Chapitre 1
Équations, corps et polynômes

Sommaire

1 Les équations algébriques, des origines à Galois

L'oeuvre de Galois marque le passage de l'étude classique des équations algébriques à celle d'objets plus conceptuels (les « structures algébriques »). 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.

L'exposé vise à donner une idée assez large du sujet et de son développement historique. Même si le point de vue adopté est celui de Dedekind-Noether-Artin [1], j'ai souvent indiqué des démonstrations alternatives plus anciennes, fondées sur les polynômes symétriques. Je n'ai pas hésité à faire des digressions

1. Cette présentation, bien adaptée à ce niveau, gagne d'ailleurs à être complétée par la reformulation qu'a donnée Grothendieck de la théorie de Galois autour de 1960.

naturelles et ai présenté bon nombre d'exemples, d'illustrations et d'exercices. Ce cours est donc loin d'une géodésique vers la correspondance de Galois.

Ce premier chapitre, qui n'est pas conçu pour être lu linéairement, présente une mise perspective historique et un certain nombre de résultats utilisés dans la suite : polynômes irréductibles, racines de l'unité, polynômes symétriques, théorème de d'Alembert-Gauss.

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 :*

$$\sum_{k=0}^{4} z^k = 0 \quad \textit{et que} \quad 2\cos\left(\frac{2\pi}{5}\right) = z + \frac{1}{z},$$

trouver une équation de degré 2 *satisfaite par* $2\cos\left(\frac{2\pi}{5}\right)$ *et montrer que*

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

Déterminer 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]

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 actuelles [3], la *méthode de Cardan* pour la résolution des équations de degré 3. Une remarque préliminaire est qu'une équation polynomiale de degré n :

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

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 directement géométrique.

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.

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

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

où $b_{n-1} = a_{n-1} + nh$. Il suffit donc de choisir $h = -\dfrac{a_{n-1}}{n}$ pour que (2) n'ait 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

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

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

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

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

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

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 :

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

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

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

Posons alors [4] :

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

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

$$u - \frac{p}{3u}$$

4. Le choix du signe $-$, qui peut sembler stupide ici, est lié au fait que Δ ainsi défini est le *discriminant* du polynôme $X^3 + pX + q$; cf. **4.3**.

où u est l'une des racines cubiques de $\dfrac{-q}{2}+\dfrac{\sqrt{-\Delta}}{6\sqrt{3}}$. Traditionnellement et un peu abusivement, on dit que les racines sont données par les *formules de Cardan* :

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

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 :

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

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

Exercice 4. ③ *Soit* $P=X^3+pX+q$ *un élément de* $\mathbb{C}[X]$*. Montrer, sans utiliser les formules de Cardan, que* P *est à racines simples si et seulement si* $\Delta\neq 0$*. On pourra appliquer l'algorithme d'Euclide à* P *et* P'*.*

Exercice 5. ③ *Soit* $P=X^3+pX+q$ *un élément de* $\mathbb{R}[X]$*. Discuter le nombre de racines réelles de* P *en fonction du signe de* Δ *(cf. aussi exercice 63,* **4.3***). Cf* **4.3** *pour une généralisation.*

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 :*

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

a) Soit λ *un nombre complexe. Expliciter un polynôme complexe* T_λ *de degré au plus* 2 *tel que :*

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

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. Hölder a montré à la fin du dix-neuvième siècle comment la théorie de Galois expliquait ce phénomène.

b) Montrer que T_λ est le carré d'un polynôme de degré au plus 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, montrant que cette équation peut se résoudre par 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 » :

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

L'exercice suivant étudie le cas des *équations réciproques*.

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

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

Montrer qu'il existe Q dans $\mathbb{C}[X]$ de degré n tel que $P(X) = X^n Q\left(X + \dfrac{1}{X}\right)$. 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 algébrique[6], 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 dégageant 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*

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

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.

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 aux nôtres.

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 ...

Exercice 10. ⑤ *a) Soient P dans $\mathbb{R}[X]$ 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 $\delta(b)-\delta(a)-2\,m$ avec $m \in \mathbb{N}$.*

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

Nous allons donner quelques indications sommaires sur l'évolution de la théorie des équations chez Lagrange et Gauss. Ce choix, très partiel, est justifié par le fait que Lagrange et Gauss font progresser de manière décisive deux aspects différents de la théorie, que Galois saura unifier.

Lagrange et l'équation générale

Dans ses *Réflexions sur la résolution algébrique des équations* (1770), Lagrange étudie l'« équation générale » [8] de degré n. Son travail part d'une analyse des méthodes de résolution des équations de degré 3 et 4 connues à l'époque, qui met en lumière le rôle du groupe des permutations des racines.

Voici l'approche de Lagrange de la méthode de Cardan. Par commodité, nous trahissons Lagrange. Plutôt que d'étudier l'équation générale, nous 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 on peut supposer que $3y_1y_4 = -p$. Quitte à réindexer, z_1, z_2, z_3 sont donc donnés par

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

Par suite

$$y_1 = \frac{z_1 + j^2z_2 + jz_3}{3} \qquad y_4 = \frac{z_1 + jz_2 + j^2z_3}{3}.$$

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.

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 $\mathbb{K}$.

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

$$\alpha = z_1 + jz_2 + j^2 z_3 \qquad \text{et} \qquad \beta = z_1 + j^2 z_2 + jz_3,$$

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 $\alpha^3 + \beta^3$:

$$\alpha\ \beta = z_1^2 + z_2^2 + z_3^2 - (z_1z_2 + z_2z_3 + z_3z_1) = (z_1 + z_2 + z_3)^2 - 3(z_1z_2 + z_2z_3 + z_3z_1),$$

$$\text{soit} \qquad \alpha\ \beta = -3p \quad \text{puis} \qquad \alpha^3\ \beta^3 = -27p^3.$$

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'intuition 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 p en les x_i ne prend que m valeurs lorsque l'on permute les x_i, elle vérifie une équation de degré m sur le corps de base.* Cet énoncé, que nous établirons en **4.2**, est une application et une généralisation du théorème des polynômes symétriques.

La méthode de Cardan repose en définitive sur la mise en évidence de fonctions polynomiales des racines prenant seulement deux valeurs distinctes par permutation des x_i, à partir desquelles on peut calculer les x_i par opérations de corps et extraction de radicaux. Lagrange examine d'autres méthodes de résolution des équations de degré 3 et 4 et constate que leur succès repose sur des faits analogues ; nous présenterons son étude de l'équation de degré 4 en **4.2**. Il établit que ces méthodes ne s'étendent pas aux degrés supérieurs et en vient à douter de la résolubilité par radicaux des équations de degré 5.

Le travail de Lagrange contient d'autres résultats intéressants. Sa leçon principale est que la théorie des équations entretient des rapports étroits avec celle des permutations. Poursuivant dans cette voie, 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.

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 ».

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.

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* $x^n - 1 = 0$. Gauss donne une analyse profonde de cette équation. Son résultat le plus spectaculaire est la construction à la règle et au compas du polygone régulier à 17 côtés, liée à la formule suivante [10] pour $\cos\left(\frac{2\pi}{17}\right)$:

$$\frac{1}{16}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}\right).$$

En fait, $\cos\left(\frac{2\pi}{17}\right)$ est racine d'une équation de degré 8 à coefficients dans $\mathbb{Q}$ que l'on peut ramener à trois équations de degré 2 bien choisies. Gauss montre plus généralement que, si p est un nombre premier de la forme $2^m + 1$ avec $m \in \mathbb{N}^*$, alors on peut calculer $\cos\left(\frac{2\pi}{p}\right)$ en résolvant m équations de degré 2.

Exercice 11. ③ *Écrire une équation de degré* 8 *à coefficients dans* $\mathbb{Z}$ *admettant* $2\cos\left(\frac{2\pi}{17}\right)$ *pour solution.*

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**.

1.3 Galois et la transformation de l'algèbre

Galois

Galois s'inscrit dans la double filiation de Lagrange et de Gauss. [11] 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. [12] 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* $\mathbb{K}$. [13]

Qu'entend-on par symétries algébriques ? Soit P dans $\mathbb{K}[X]$ de degré n, admettant n racines distinctes $x_1, \ldots, x_n$ 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, mais pas les seuls. Par exemple, si P est de degré 4 et « bicarré », c'est-à-dire de la forme $X^4 + aX^2 + b$, l'opposé

10. Noter l'apparition de $\sqrt{17}$, à relier à celle de $\sqrt{5}$ pour le pentagone. Explication en **4.3**.
11. Même si, curieusement, il cite Gauss mais pas Lagrange.
12. 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.
13. Insistons sur le fait que le groupe dépend du corps de base. La façon dont le groupe varie lorsque l'on change $\mathbb{K}$ (qui n'est a priori assujetti qu'à contenir les coefficients de l'équation) est justement le thème fondamental de la théorie.

d'une racine est également une racine : les racines se regroupent donc en deux paires $\{x, -x\}$. Autrement dit, on a deux relations

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

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

Après Galois

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 un cadre plus vaste, une « classification des irrationnelles » fondée sur la correspondance susmentionnée ;

- crée un nouveau champ d'études, la théorie des groupes.

Une fois le travail de Galois assimilé, l'intérêt des algébristes se déplace des équations vers d'autres objets et des problèmes plus « structurels ». [14] Indiquons deux directions, dont chacune a conduit à des reformulations d'une partie du travail de Galois et, parallèlement, à des résultats importants ne relevant pas de la théorie des équations.

- Le premier véritable continuateur de Galois est Jordan, qui précise et approfondit les notions relatives aux groupes. Son monumental *Traité des Substitutions et des équations algébriques*, paru en 1870, se présente comme un « commentaire des idées de Galois ». Ce livre, qui contient une foule de résultats concernant les groupes de permutations et ce que nous appelons maintenant les « groupes classiques » sur les corps $\mathbb{F}_p$, a considérablement stimulé l'étude des groupes et des matrices. Jordan a le souci de rattacher ses résultats aux équations, mais la théorie des groupes commence chez lui à devenir autonome.

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 ...).

- Motivé par l'arithmétique des corps de nombres (factorisation des idéaux), Dedekind initie, à la fin du dix-neuvième siècle, la présentation moderne de la théorie de Galois. Dans le onzième supplément aux *Vorlesungen über Zahlentheorie* de Dirichlet, paru en 1894, les extensions, les morphismes et la correspondance prennent le pas sur les équations ; la linéarisation de la théorie commence. Cette approche est reprise et axiomatisée un peu avant 1930 par Emmy Noether, qui tire également parti d'une grande synthèse sur la théorie des corps due à Steinitz (1910). Van der Waerden en rédige aussitôt le premier exposé didactique, dans un des livres d'algèbre les plus influents du vingtième siècle.[15] Quelques années plus tard, Emil Artin donne à ces idées une forme radicale : dans la théorie de Galois « à la Artin », les arguments utilisant le théorème des fonctions symétriques et celui de l'élément primitif disparaissent complètement.

2 Polynômes à coefficients dans un corps

Il est préférable d'aborder la théorie de Galois avec une certaine pratique des polynômes irréductibles. Rappels et compléments sur ce sujet sont l'objectif de cette section. 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 $\mathbb{K}(X)$ ($\mathbb{K}$ étant lui-même un corps), $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier. Nous en rencontrerons beaucoup d'autres.

Les corps donnent un bon cadre à 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 $\mathbb{H}$.

Exercice 12. ② *Vérifier les propriétés ci-dessus de l'algèbre des quaternions.*

Exercice 13. 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, tandis que **2.5** est un divertissement.

15. *Moderne Algebra*, paru en 1930-1931 et ayant connu à ce jour (2018) sept éditions.

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

Si $\mathbb{K}$ est un corps, l'étude de l'arithmétique de $\mathbb{K}[X]$ est élémentaire. Elle 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 $\mathbb{K}[X]$. Notons 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 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.

- On définit la notion de polynôme irréductible et 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 14. 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 du paragraphe précédent ramène l'arithmétique de $\mathbb{K}[X]$ à la détermination des irréductibles de $\mathbb{K}[X]$. Cette détermination dépend fortement du corps $\mathbb{K}$. Les polynômes de degré 1, cependant, 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 $\mathbb{K}$.

On montre que le corps $\mathbb{C}$ des nombres complexes est algébriquement clos (*théorème de d'Alembert-Gauss*, cf. section **5**). On établit également que tout corps admet un surcorps algébriquement clos (*théorème de Steinitz*, cf. chapitre **2**). On peut souvent substituer à cet énoncé un résultat plus simple, à

savoir l'existence d'un surcorps de $\mathbb{K}$ scindant un polynôme fixé de $\mathbb{K}[X]$. Nous utiliserons ces résultats librement dès maintenant.

Exercice 15. 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 16. 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 $\overline{\lambda}$. Or :

$$(X - \lambda)\,(X - \overline{\lambda}) = X^2 - 2\mathrm{Re}(\lambda)X + |\lambda|^2$$

appartient à $\mathbb{R}[X]$.

Exercice 17. ③ *Soit P dans $\mathbb{R}[X]$. Montrer qu'il existe A et B dans $\mathbb{R}[X]$ tels que $P = A^2 + B^2$ si et seulement si*

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

Exercice 18. 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 $P = A/B$ si et seulement si*

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

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

Si l'élément P de $\mathbb{K}[X]$ 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, comme on le voit en prenant $\mathbb{K} = \mathbb{R}$ et $P = X^4 + 1$.

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

Lemme 1. *Soit $P = a_n X^n + \cdots + a_0$ 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 $\dfrac{p}{q}$ 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. 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, $q|a_n$. L'autre démonstration est analogue.

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

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

Ce résultat peut être démontré de manière un peu différente : si $\sqrt[m]{n} = \dfrac{u}{v}$ 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. La première méthode est bien entendu plus générale.

Exercice 19. ② *Montrer que $X^3 - X - 1$ est irréductible sur $\mathbb{Q}$.*

Exercice 20. 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 un nombre premier et a un élément de $\mathbb{K}$. Alors les deux assertions suivantes sont équivalentes :*

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 : $d \in \{1, \ldots, p-1\}$. 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. On en déduit que le terme constant de P est de la forme $\pm\varepsilon u^d$ où ε est une racine p-ième de 1 dans $\mathbb{L}$. On a donc :

$$\varepsilon u^d \in \mathbb{K}.$$

La relation de Bézout fournit d'autre part $(\alpha, \beta) \in \mathbb{Z}^2$ tel que : $\alpha d + \beta p = 1$. Mais alors :

$$\left(\varepsilon u^d\right)^{\alpha} a^{\beta} = \varepsilon^{\alpha} u \in \mathbb{K}$$

est une 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 dans $\mathbb{N}^*$, $X^n - 2$ 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 $d \in \{1, \ldots, n-1\}$. 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 21. ② *À quels binômes $X^n - m$ de $\mathbb{Z}[X]$ peut-on généraliser la démonstration ci-dessus ?*

Un polynôme de $\mathbb{Q}[X]$ a des associés dans $\mathbb{Z}[X]$. Pour P dans $\mathbb{Z}[X]$, nous donnerons en **2.4** un outil puissant, dû à Gauss, qui ramène l'étude de l'irréductibilité P sur $\mathbb{Q}$ à celle de son irréductibilité sur $\mathbb{Z}$ et permet de montrer l'existence d'un « algorithme de factorisation » dans $\mathbb{Q}[X]$. Établir l'irréductibilité d'un polynôme de $\mathbb{Q}[X]$ reste souvent délicat, même si un polynôme non constant de $\mathbb{Q}[X]$ est « en général » irréductible, cf. **2.5**.

Le corps $\mathbb{F}_p$

On démontre que, si p est un nombre premier et n un élément de $\mathbb{N}^*$, 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 p^n/n d'irréductibles.[16] Contentons nous du cas des polynômes de degré 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 $\dfrac{p(p-1)}{2}$ polynômes de degré 2 unitaires irréductibles.

Exercice 22. 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 23. ④ *Soient p un nombre premier, $\mathbb{K}$ un corps de caractéristique p, a un élément de $\mathbb{K}$ 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 $\mathbb{K}$.

16. 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. [17]

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 et son degré est 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 $\mathbb{K}$, alors le pgcd de A et B est le même vu dans $\mathbb{K}[X]$ ou $\mathbb{L}[X]$. Ce point résulte du fait que le pgcd s'obtient par l'algorithme d'Euclide.
2. *Dérivation et racines simples*
   Si $\mathbb{K}$ est un corps de caractéristique nulle, P un élément non nul de $\mathbb{K}[X]$, x un élément de $\mathbb{K}$, 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
   $$\forall P \in \mathbb{K}[X], \qquad P' = 0 \Longleftrightarrow P \in \mathbb{K}[X^p].$$
   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 $p > 0$, 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 fausse 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 *un nombre premier,* $\mathbb{K}$ *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* $\mathbb{K}[X^p]$.

17. Le lecteur qui souhaite se borner à la théorie de Galois en caractéristique 0 peut laisser de côté la suite de ce paragraphe.

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.

Exercice 24. ③ *Soit P dans $\mathbb{Z}[X]$ un polynôme séparable. Montrer que, si p est un nombre premier assez grand, la réduction modulo p de P est séparable.*

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 $\mathrm{Frob}_{\mathbb{K}}$ l'*endomorphisme de Frobenius* de $\mathbb{K}$, défini par

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

Théorème 1. *Soient p un nombre premier, $\mathbb{K}$ un corps de caractéristique p. Alors $\mathbb{K}$ est parfait si et seulement si $Frob_{\mathbb{K}}$ est surjectif.*

Preuve. Soient $a_0, \ldots, a_n$ 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 $\mathrm{Frob}_{\mathbb{K}}$ 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 $\mathrm{Frob}_{\mathbb{K}}$ 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 un élément de $\mathbb{K}$ 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, en un certain sens, aussi simple que possible.

Corollaire 1. *Tout corps fini est parfait.*

Preuve. Le résultat est une conséquence immédiate du lemme suivant, que nous utiliserons beaucoup dans l'exposé de la théorie de Galois proprement dite.

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 $x \in \mathbb{K}^*$, $x \times \dfrac{1}{x} = 1$, donc $\varphi(x) \times \varphi(1/x) = 1$, donc $\varphi(x) \neq 0$.

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

Comme annoncé en **2.2**, nous allons ramener l'étude des irréductibles de $\mathbb{Q}[X]$ à celle des irréductibles de $\mathbb{Z}[X]$. Les arguments sont en fait plus généraux : on peut, sans changement, remplacer $\mathbb{Z}$ par un anneau factoriel $\mathbb{A}$ et $\mathbb{Q}$ 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 de base de ce paragraphe est le lemme suivant.

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

Preuve. Soient P_1 et P_2 dans $\mathbb{Z}[X]$, $P = P_1P_2$. 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

$$0_{\mathbb{F}_p[X]} = \overline{P} = \overline{P_1}\,\overline{P_2}.$$

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 2 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 $C(P_1P_2)$. 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_1P_2 est congru à a_kb_ℓ 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 2 en l'énoncé suivant, nommé *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 est un élément de $\mathbb{Z}[X] \setminus \{0\}$, une factorisation de P dans $\mathbb{Q}[X]$ se relève en une factorisation de P dans $\mathbb{Z}[X]$.

Théorème 2. *Soit P dans $\mathbb{Z}[X]\setminus\{0\}$. Si P s'écrit P_1P_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 $P_i = (u_i/v_i)Q_i$ où u_i, v_i sont des éléments non nuls de $\mathbb{Z}$ et Q_i un polynôme primitif de $\mathbb{Z}[X]$. Alors : $u_1u_2Q_1Q_2 = v_1v_2P$ et, grâce au lemme de Gauss : $u_1u_2 = \pm C(P)v_1v_2$.

Remarques

1. *Point de vue algorithmique*

   On déduit du théorème 2 l'« existence » d'un algorithme de factorisation dans $\mathbb{Q}[X]$. Il suffit en effet d'établir que, si P est un élément de $\mathbb{Z}[X]$, on peut expliciter une partie finie de $\mathbb{Z}[X]$ contenant tous les éventuels diviseurs de P dans $\mathbb{Z}[X]$. Rappelons à cet effet un résultat élémentaire sur la localisation des racines.

   Lemme 4. *Soient* $n \in \mathbb{N}^*$, $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$, *avec* $a_n \neq 0$. *Alors 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, 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 relations entre coefficients et racines 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 2 que $\mathbb{Z}[X]$ (qui n'est pas principal, cf exercice 14, **2.1**) est factoriel, ses irréductibles étant les $\pm p$ où p est un nombre premier 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. ② *Détailler le raisonnement de la remarque 2.*

18. Cet argument donne des bornes prohibitives. Voici un algorithme légèrement moins naïf, dû à Kronecker. Si Q est un diviseur de P dans $\mathbb{Z}[X]$ de degré majoré par $n/2$ 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 $\lfloor n/2 \rfloor + 1$ 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 maintenant 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.Lovàsz en 1982 ont découvert l'« algorithme LLL », fondé sur la géométrie des réseaux, qui a sur ses prédécesseurs l'avantage -essentiellement théorique- d'être polynomial.

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

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

b) On suppose que $\frac{p}{q}$ *est racine de multiplicité* d *de* P. *Montrer que* q^d *divise* a_n.

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

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

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

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

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

c) Montrer que, pour k *dans* $\{0, \ldots, d\}$ *:* $|p_k| \leq \binom{d}{k} m(P)$.

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

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

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 29. ② *a) Soient* P *un élément non constant de* $\mathbb{Z}[X]$, p *un nombre premier 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 23, que, si p *est un nombre premier,* $X^p - X - 1$ *est irréductible sur* $\mathbb{Q}$.

Exercice 30. ③ *Soient $n \in \mathbb{N}^*$, $a_1, \ldots, a_n$ des entiers relatifs deux à deux distincts. Montrer l'irréductibilité sur $\mathbb{Q}$ de $P = \prod_{i=1}^{n}(X - a_i) - 1$.*

Exercice 31. ④ *a) Soit P un polynôme de $\mathbb{Z}[X]$ 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 de $\mathbb{Z}[X]$ de degré n prenant les valeurs ± 1 pour au moins $\lfloor \frac{n}{2} \rfloor + 1$ entiers est irréductible sur $\mathbb{Q}$ (Dorwart et Ore, 1933).

Exercice 32. ⑤ *Soit $n \in \mathbb{N}^*$.*

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

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

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

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

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

Exercice 33. ④ *a) Soit $P \in \mathbb{Z}[X]$ unitaire, non constant, tel que $|P(0)|$ soit premier et 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 $|a_0|$ est premier, que $|a_0| > \sum_{i=1}^{n} |a_i|$. Montrer que P est irréductible sur $\mathbb{Q}$.

Exercice 34. ④ *Soient n dans $\mathbb{N}^*$, p un nombre premier. Montrer aue le polynôme $P = \sum_{i=1}^{n} X^i + p$ est irréductible sur $\mathbb{Q}$.*

Exercice 35. ④ *Soient $P \in \mathbb{Z}[X]$ unitaire de degré $n \geq 1$, M dans $\mathbb{R}^{+*}$. Supposons les racines $z_1, \ldots, z_n$ de P dans $\mathbb{C}$ de module au plus M. Montrer que, s'il existe k dans $\mathbb{Z}$ tel que $|k| > M + 1$ et que $|P(k)|$ soit premier, alors P est irréductible sur $\mathbb{Q}$ (Brillhart, 1980).*

Exercice 36. ④ *a) Soit $P \in \mathbb{Z}[X]$ unitaire de degré $n \geq 2$ tel que $P(0) \neq 0$. On suppose que P a exactement $n-1$ racines de module strictement inférieur à 1. Montrer que P est irréductible sur $\mathbb{Q}$.*

b) Soient $a_0, \ldots, a_{n-1}$ 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 37. ⑤ *Notons E l'ensemble des polynômes non constants de $\mathbb{C}[X]$ ne s'annulant pas en 0. Si P est dans E, de degré n et s'écrit :*

$$P = \sum_{i=0}^{n} a_i X^i = \prod_{j=1}^{n} (X - z_j),$$

posons :

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

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 $\mathbb{Z}$. [19]

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

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

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

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

Voici une conséquence immédiate mais utile du théorème 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 $\mathbb{Z}[X]$.*

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

Proposition 5. *Soient p un nombre premier, $a_0, \ldots, a_n$ des entiers tels que p divise $a_0, \ldots, a_{n-1}$ mais pas a_n, et que p^2 ne divise pas a_0. Alors*

$$P = \sum_{i=0}^{n} a_i X^i$$

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

$$\overline{P_1 P_2} = \overline{a_n} X^n.$$

Il s'ensuit que $\overline{P_1}$ et $\overline{P_2}$ sont des monômes, puis que $\overline{P_1} = \overline{b} X^r$ et $\overline{P_2} = \overline{c} X^s$. Comme r et s sont ≥ 1, les termes constants de P_1 et P_2 sont divisibles par p. Leur produit a_0 est donc divisible par p^2, ce qui est 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 5).

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

Exercice 38. 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 39. ④ *Soit $n \geq 2$ un entier. On rappelle qu'il existe un nombre premier p tel que $n \leq p < 2n$.*[20] *En déduire l'irréductibilité sur $\mathbb{Q}$ du polynôme*

$$E_n = \sum_{k=0}^{n} \frac{X^k}{k!}.$$

Exercice 40. ④ *Soit P un élément de $\mathbb{Z}[X]$. Montrer que si p est un nombre premier assez grand, $P + 1/p$ est irréductible sur $\mathbb{Q}$.*

Exercice 41. ③ *Soient $n \in \mathbb{N}^*$, p un nombre premier, $P = \sum_{k=0}^{n} a_k X^k$ dans $\mathbb{Z}[X]$, d dans $\{1, \ldots, n\}$. 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.*

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 $\mathbb{N}^*$, on note $\mathcal{P}_n^t$ l'ensemble des P de $\mathbb{Z}[X]$ de degré n tels que $H(P) \leq t$. Alors, si n est fixé

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

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 2, 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 3. *Si $n \geq 3$, on a*

$$\pi_{n,t} \underset{t \to +\infty}{=} O\left(\frac{1}{t}\right).$$

Par ailleurs

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

20. Ce résultat se déduit des encadrements de Tchebychev sur les nombres premiers.

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*

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

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

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

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*

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

Preuve du théorème 3. Pour k dans $\{1,\dots,n-1\}$, soit $\mathcal{R}_{n,k}^t$ l'ensemble des éléments de $\mathcal{R}_n^t$ de la forme UV ou 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 $1 \leq k \leq n-1$,

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

et que

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

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 $H(U)\,H(V) \leq \dfrac{t}{c_{k,n-k}}$.

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

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

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 3 résulte donc en fin de compte du lemme suivant.

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

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

$$a \neq b \Longrightarrow S_{a,b}(T) \underset{T\to+\infty}{=} O(T^{\max(a,b)+1})\ ;$$

$$S_{a,a}(T) \underset{T\to+\infty}{=} O(T^{a+1}\ \ln(T)).$$

Preuve du lemme 7. On peut supposer $a \geq b$. 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

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

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

Exercice 42. ③ *Donner un équivalent de $S_{a,b}(T)$ lorsque T tend vers $+\infty$.*

Les estimations du théorème sont optimales. Pour $n \geq 3$, on le voit immédiatement en considérant l'ensemble des polynômes nuls en 0, qui donne $\pi_{n,t} \geq \dfrac{1}{2t+1}$. Pour $n = 2$, l'optimalité subsiste, mais la démonstration est plus délicate. [22]

Exercice 43. ⑤ *Montrer que*

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

Exercice 44. 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 $\dfrac{|\mathcal{E}_{n,p}^t|}{|\mathcal{P}_n^t|}$.* [23]

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.

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 $\dfrac{|\bigcup_{p\in\mathcal{P}} \mathcal{E}_{n,p}^t|}{|\mathcal{P}_n^t|}$ converge, lorsque $\to +\infty$ 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.

3.1 Groupes de racines de l'unité

Le théorème ci-après est bien connu pour $\mathbb{K} = \mathbb{C}$.[24] La démonstration ne donne pas un algorithme produisant un générateur. 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 $\{1, \ldots, p-1\}$ dont la classe modulo p engendre $(\mathbb{F}_p^*, \times)$.[25]

Théorème 4. *Soit $\mathbb{K}$ un corps. Tout sous-groupe fini de $(\mathbb{K}^*, \times)$ est cyclique.*

Voici deux preuves de ce résultat. La première utilise 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_g est non vide. On va en fait établir que, pour tout d de$D$, 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 classique[26] :

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

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.

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 abrègera :

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

24. Dans ce cas, la démonstration habituelle est fondée sur la description des racines de l'unité via l'exponentielle complexe, donc « transcendante ».

25. 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 ».

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

Il se peut que $\mathbb{U}_n(\mathbb{K})$ soit réduit à $\{1\}$; tel est par exemple le cas si $\mathbb{K}$ est un sous-corps de $\mathbb{R}$ et si 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 $p > 0$, 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

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

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 45. ③ *Soit $\mathbb{K}$ un corps algébriquement clos. Pour quels entiers n existe-t-il un sous-groupe fini de $(\mathbb{K}^*, \times)$ de cardinal n ?*

Exercice 46. ④ *Soit $\mathbb{K}$ un corps algébriquement clos de caractéristique nulle.*

a) Montrer que le groupe multiplicatif 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 47. ④ *Si $\mathbb{K}$ est un corps algébriquement clos de caractéristique p première, montrer que le groupe Tor$(\mathbb{K}^*)$ est isomorphe à la somme directe des C_q pour q premier différent de p.*

Exercice 48. ④ *Soit $\mathbb{H}$ l'anneau à division des quaternions réels, introduit au début du paragraphe* **2**. *Montrer que, pour tout m de $\mathbb{N}^*$, $\mathbb{H}^*$ 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)

Littéralement, « 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 $\varphi(n)$.

Ainsi : $\Phi_1 = X - 1$, $\Phi_2 = X + 1$, $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$,
$\Phi_5 = X^4 + X^3 + X^2 + X + 1$, $\Phi_6 = X^2 - X + 1$.

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

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

Lemme 8. *On a*[28] *:*

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

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 de l'égalité est unitaire.

Le théorème ci-après est fondamental. Nous l'établissons ici dans un cas particulier, la démonstration du cas général sera donnée plus loin.

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

Théorème 5. *Pour tout n de $\mathbb{N}^*$, le polynôme Φ_n est irréductible sur $\mathbb{Q}$.* [29]

Preuve pour $n = p$ premier. 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 $\{1, \ldots, p-1\}$.

Exercice 49. ③ *Si p est premier et si α est dans $\mathbb{N}^*$, montrer que Φ_{p^α} est irréductible sur $\mathbb{Q}$.*

Exercice 50. ③ *Préciser le terme constant de Φ_n.*

Exercice 51. 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

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

Exercice 52. ③ *Si μ est la fonction de Moebius, établir, pour n dans $\mathbb{N}^*$:*

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

Exercice 53. 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 54. 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 55. 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 56. ④ *Soient m et n deux éléments distincts de $\mathbb{N}^*$, q dans $\mathbb{Z}$. On pose*

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

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.

a) Montrer que ℓ divise $(m \vee n)q^{(m\vee n)-1}$. On pourra dériver la factorisation de $X^{m\vee n} - 1$ donnée 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 ; cf. aussi exercice 51. L'exercice suivant montre qu'il n'en est rien : tout entier relatif apparaît comme coefficient d'un polynôme cyclotomique. [30]

Exercice 57. ⑤ *Soient m un entier impair, $p_1, \ldots, p_m$ une suite strictement croissante de nombres premiers, $n = \prod_{i=1}^{m} p_i$.*

a) Montrer

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

b) On suppose : $p_m < p_1 + p_2$. 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 $(p_k)_{1\le k\le m}$ de nombres premiers possédant les propriétés précédentes.

d) Démontrer que, pour tout entier relatif ℓ, il existe N dans $\mathbb{N}^*$ tel que ℓ soit un coefficient de Φ_N (Suzuki, 1987).

Exercice 58. 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 :

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

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) :

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

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

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

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

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 vu son importance relativisée par l'approche de Dedekind de la théorie de Galois. Il garde cependant un intérêt véritable, notamment par son caractère effectif. Nous lui préfèrerons en général des arguments plus abstraits fondés sur la notion d'extension, mais signalerons la possibilité de l'utiliser lorsqu'elle se présente. En **4.2**, on utilise ce théorème pour en dire un peu plus sur le travail de Lagrange abordé en **1.2**.

Autre outil important : le résultant. Nous introduisons en **4.3** uniquement le cas particulier du discriminant, qui nous servira dans la suite.

Nous terminerons cette section par un complément qui ne sera pas utilisé dans la suite, relatif aux sommes de Newton. 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 $\mathbb{A}[X_1, \ldots, X_n]$ l'anneau des polynômes en les indéterminées indépendantes $X_1, \ldots, X_n$ à coefficients dans $\mathbb{A}$. Si $\alpha = (\alpha_1, \ldots, \alpha_n)$ est dans $\mathbb{N}^n$, on note

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

Par définition, si $(\alpha, c) \in \mathbb{N}^n \times \mathbb{A} \setminus \{0\}$, le degré de $c\, X^\alpha$ est $\sum_{i=1}^{n} \alpha_i$. Le degré d'un élément de $\mathbb{A}[X_1, \ldots, X_n] \setminus \{0\}$ est le maximum des degrés de ses monômes.

4.1 Le théorème des polynômes symétriques

Ordre lexicographique sur les monômes

On munit $\mathbb{N}^n$ de l'ordre lexicographique $\leq_{\text{lex}}$. 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 $\leq$.[31] Les bons ordres permettent donc d'effectuer des démonstrations par récurrence.

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

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

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

Soit A une partie non vide de $\mathbb{N}^n$. Par hypothèse de récurrence, $\pi(A)$ admet un plus petit élément $(a_1, \ldots, a_{n-1})$. On choisit alors $a = (a_1, \ldots, a_n)$ dans A tel que a_n soit minimal. Il est clair que a est le plus petit élément de A.

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

Pour

$$P = \sum_{\alpha \in \mathbb{N}^n} c_\alpha \, X^\alpha$$

dans $\mathbb{A}[X_1, \ldots, X_n] \setminus \{0\}$, on note $M(P)$ le plus grand monôme de P pour $\leq_{\text{lex}}$. Par exemple

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

Pour P et Q dans $\mathbb{A}[X_1, \ldots, X_n] \setminus \{0\}$ tels que le coefficient dominant de P soit inversible, on a :

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

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 $\{1, \ldots, n\}$, soit

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

Pour tout k, Σ_k est homogène de degré k. Si T est une nouvelle indéterminée indépendante, on a donc

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

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

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

Polynômes symétriques

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

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

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

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

Exemples

1. Si P est dans $\mathbb{A}[X_1, \ldots, X_n]$, les polynômes
$$\sum_{\sigma \in \mathcal{S}_n} \sigma.P \quad \text{et} \quad \prod_{\sigma \in \mathcal{S}_n} \sigma.P$$
sont symétriques.
2. Les $\Sigma_k, 1 \leq k \leq n$ sont des polynômes symétriques. Il en est de même de $Q(\Sigma_1, \ldots, \Sigma_n)$ pour tout polynôme Q à n indéterminées à coefficients dans $\mathbb{A}$.

Le théorème des polynômes symétriques est la réciproque de l'exemple 2. [32] Il détermine ainsi les fonctions polynomiales des racines d'une équation auxquelles on accède via les coefficients. La démonstration de la partie « existence » est un algorithme, qui repose sur le fait que $\leq_{\text{lex}}$ est un bon ordre et sur la remarque suivante.

Lemme 10. *Soit P dans $\mathbb{A}[X_1, \ldots, X_n] \setminus \{0\}$ un polynôme symétrique. Posons $M(P) = c_\alpha \, X^\alpha$ avec $c_\alpha \in \mathbb{A} \setminus \{0\}$. Alors*
$$\alpha_1 \geq \ldots \alpha_2 \geq \cdots \geq \alpha_n.$$

Preuve. Puisque P est symétrique, P contient tous les monômes déduits de $c_\alpha \, X^\alpha$ par permutation.

Théorème 6. *Soient P dans $\mathbb{A}[X_1, \ldots, X_n]$ un polynôme symétrique, $Y_1, \ldots, Y_n$ des indéterminées indépendantes. Il existe un unique Q dans $\mathbb{A}[Y_1, \ldots, Y_n]$ tel que*
$$P(X_1, \ldots, X_n) = Q(\Sigma_1, \ldots, \Sigma_n).$$

Preuve du théorème 6 : existence. Soit P dans $\mathbb{A}[X_1, \ldots, X_n] \setminus \{0\}$ un polynôme symétrique. Posons $M(P) = c_\alpha \, X^\alpha$ avec $c_\alpha \in \mathbb{A} \setminus \{0\}$. Comme $\leq_{\text{lex}}$ est un bon ordre sur $\mathbb{N}^n$, il suffit, pour conclure par récurrence, d'établir que l'on peut trouver S dans $\mathbb{A}[X_1, \ldots, X_n]$ tel que, si $T = P - S(\Sigma_1, \ldots, \Sigma_n)$, l'une des deux propriétés suivantes soit vraie :

- $T = 0$;
- le degré de T est strictement inférieur (pour $\leq_{\text{lex}}$) à celui de P.

Construisons S. Le lemme 10 assure que
$$\alpha_1 \geq \ldots \alpha_2 \geq \cdots \geq \alpha_n.$$

L'observation-clé est alors que
$$M(c_\alpha \, \Sigma_1^{\alpha_1 - \alpha_2} \Sigma_2^{\alpha_2 - \alpha_3} \ldots \Sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \Sigma_n^{\alpha_n}) = c_\alpha \, X^\alpha.$$

Le polynôme
$$P - c_\alpha \, \Sigma_1^{\alpha_1 - \alpha_2} \Sigma_2^{\alpha_2 - \alpha_3} \ldots \Sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \Sigma_n^{\alpha_n}$$

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

est symétrique ; s'il n'est pas nul, son monôme de plus haut degré est de degré strictement inférieur à α.

Preuve du théorème 6 : unicité. En faisant la différence de deux éventuelles écritures de P, on est ramené à établir que le seul Q de $\mathbb{A}[X_1, \ldots, X_n]$ vérifiant

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

est le polynôme nul. Notons τ l'application qui à Q associe $Q(\Sigma_1, \ldots, \Sigma_n)$. Alors, pour tout α de $\mathbb{N}^n$ et tout c de $\mathbb{A} \setminus \{0\}$, le monôme dominant de $\tau(cX^\alpha)$ est

$$c \prod_{j=1}^{n} X_j^{\sum_{i=j}^{n} \alpha_i}.$$

Pour conclure, il suffit de noter l'injectivité de l'application

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

Remarques

1. *Homogénéité*
   Si P est homogène de degré k, il en est de même de $P - Q(\Sigma_1, \ldots, \Sigma_n)$: l'algorithme s'effectue composante homogène par composante homogène.
2. *Un exemple*
   En pratique, on peut utiliser des raccourcis au lieu d'appliquer brutalement l'algorithme. Prenons ainsi $n = 4$ et

   $$P = (X_1X_2 + X_3X_4)\ (X_1X_3 + X_2X_4)\ (X_1X_4 + X_2X_3).$$

   Le plus grand monôme de P est $X_1^3X_2X_3X_4$. 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 8) $\alpha_1 \geq \cdots \geq \alpha_4$. Seuls $(2, 2, 2, 0)$ et $(2, 2, 1, 1)$ conviennent, ce qui assure que P est combinaison linéaire à coefficients dans $\mathbb{Z}$ 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 dans $\mathbb{A}[X_1, \ldots, X_n] \setminus \{0\}$ symétrique et

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

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

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

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

$$S = P - R(\Sigma_1, \ldots, \Sigma_n).$$

Le polynôme S de $\mathbb{A}[X_1, \ldots, X_n]$ 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 :

$$P = R(\Sigma_1, \ldots, \Sigma_n) + \Sigma_n\, U,$$

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

Les exposés de la théorie de Galois « pré-Dedekind-Noether-Artin » utilisent le théorème 6 à travers le corollaire suivant, qui ne requiert que la partie « existence » de l'énoncé.

Corollaire 3. *Soient $\mathbb{K}$ un corps, $\mathbb{A}$ un sous-anneau de $\mathbb{K}$, P dans $\mathbb{K}[X]$ 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 $\mathbb{A}[X_1, \ldots, X_n]$ symétrique, on a

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

Preuve. Comme $\Sigma_k(x_1, \ldots, x_n)$ sont dans $\mathbb{A}$, il suffit d'appliquer le théorème 6 à U pour conclure.

Fractions rationnelles symétriques

On peut donner une version « fractions rationnelles » du théorème 6. Nous supposons ici que l'anneau de base est un corps, ce qui permet de définir $\mathbb{K}(X_1, \ldots, X_n)$ comme le corps des fractions de $\mathbb{K}[X_1, \ldots, X_n]$.

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

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

si et seulement si

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

Preuve. Seule l'implication réciproque mérite démonstration. Soit F dans $\mathbb{K}(X_1, \ldots, X_n)$ 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 5. On écrit $F = P/Q$ où P et Q sont dans $\mathbb{K}[X_1, \ldots, X_n]$ et $Q \neq 0$. Posons

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

Le polynôme $\tilde{Q}$ est évidemment symétrique. Il en est de même de l'élément $U = \tilde{Q}\, F$ de $\mathbb{K}[X_1, \ldots, X_n]$, d'où le résultat.

4.2 Retour à Lagrange

Nous pouvons maintenant prouver le résultat de Lagrange mentionné dans la section **1.2**, important jalon du chemin qui mène à Galois.

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

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

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

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

Lagrange a démontré des résultats plus généraux de même nature, sur lesquels nous reviendrons dans le chapitre **4**. [33]

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 $\mathbb{A}[X_1, \ldots, X_n]$,

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

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 $V(x_1, \ldots, x_n)$ 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 :

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

33. Incidemment, Lagrange a établi que, si G_U désigne le stabilisateur de U,

$$|\omega(U)|\ |G_U| = n!,$$

par 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.

Posons

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

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 59. ④ *Expliciter les calculs.*

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

Soient $X_1, \ldots, X_n$ 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 $\mathbb{K}[X_1, \ldots, X_n]$

- 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 $< n$. Or, on peut démontrer que, pour $n \geq 5$, $\mathcal{S}_n$ admet un seul sous groupe de ce type, le groupe alterné $\mathcal{A}_n$. Ce fait laisse suspecter 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.* [34] Le théorème 5 montre qu'il existe un polynôme R à n indéterminées à coefficients dans $\mathbb{A}$ tel que

$$\Delta = R(\Sigma_1, \ldots, \Sigma_n).$$

34. On trouve dans la littérature plusieurs définitions du discriminant, qui coïncident pour les polynômes unitaires. Celle présentée ici n'est pas la plus satisfaisante, mais est adaptée à notre sujet.

Soient $\mathbb{K}$ un corps, P un polynôme unitaire scindé sur $\mathbb{K}$:

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

On pose alors

$$\Delta(P) = \Delta(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_j - x_i)^2.$$

L'existence de R (ou le corollaire 3) entraîne le résultat suivant, que l'on pourrait également établir par l'algèbre linéaire. [35]

Corollaire 6. *Soient $\mathbb{K}$ un corps, $\mathbb{A}$ un sous-anneau de $\mathbb{K}$, P dans $\mathbb{A}[X]$ unitaire scindé sur $\mathbb{K}$. Alors*

$$\Delta(P) \in \mathbb{A}.$$

Si P n'est pas scindé sur $\mathbb{K}$, on peut calculer $\Delta(P)$ en travaillant dans un surcorps Ω de $\mathbb{K}$ sur lequel P est scindé : l'existence de R ci-dessus montre que le résultat ne dépend pas de Ω.

Le discriminant généralise le « $b^2 - 4ac$ » de l'équation du second degré. La définition entraîne en effet le résultat suivant.

Lemme 11. *Soient $\mathbb{K}$ un corps, P dans $\mathbb{K}[X]$ unitaire. Alors P est séparable si et seulement si $\Delta(P) \neq 0$.*

Le résultat suivant est immédiat et utile.

Proposition 9. *Avec les notations précédentes, on a*

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

Exemples

1. *Second degré*
   Si $P = aX^2 + bX + c$ avec $(a, b, c) \in \mathbb{K}^* \times \mathbb{K} \times \mathbb{K}$,

   $$\Delta(P) = -(2ax_1 + b)\,(2ax_2 + b) = -4a^2x_1x_2 - 2ab(x_1 + x_2) - b^2 = b^2 - 4ac.$$

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

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

35. La théorie du résultant permet de voir le discriminant comme un déterminant à coefficients dans $\mathbb{A}$.

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

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

Prenons $\mathbb{K} = \Omega = \mathbb{C}$, $n = p$ premier impair et $a = 1$. On déduit du calcul précédent 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 le calcul de $\cos\left(\frac{2\pi}{5}\right)$ (**1.1**), celle de $\sqrt{17}$ dans le calcul de $\cos\left(\frac{2\pi}{17}\right)$ (**1.2**), se trouvent ainsi justifiées.

Exercice 60. 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 61. ③ *On suppose $\mathbb{A}$ intègre. Soient U et V des éléments unitaires non constants de $\mathbb{A}[X]$. Montrer que $\Delta(UV)$ est divisible par $\Delta(U)\,\Delta(V)$.*

Exercice 62. ③ *Pour $n \in \mathbb{N}^*$, soit E_n l'élément $\displaystyle\sum_{k=0}^{n} \frac{X^k}{k!}$ de $\mathbb{C}[X]$. Calculer $\Delta(E_n)$.*

Exercice 63. ④ *Pour $n \in \mathbb{N}^*$, $a \in \mathbb{C}$, calculer $\Delta(X^n - X - a)$.*

Exercice 64. ⑤ *Soit $n \geq 3$ un entier. Démontrer la formule*

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

Exercice 65. ③ *a) Soit P un polynôme séparable non constant de $\mathbb{R}[X]$. Déterminer le signe de $\Delta(P)$ en fonction du nombre de paires de racines irréelles conjuguées de P.*

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

Exercice 66. ④ *Soit P dans $\mathbb{Z}[X]$ unitaire de degré $n \geq 1$. On écrit*

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

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 67. ③ *Soient P dans $\mathbb{Z}[X]$ 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.*

Exercice 68. ③ *On suppose que $\mathbb{A}$ est un anneau intègre. Un élément P de $\mathbb{A}[X_1, \ldots, X_n]$ est dit antisymétrique si*

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

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

Exercice 69. ④ *On suppose que $\mathbb{A}$ est un anneau intègre de caractéristique différente de 2. On se propose de décrire les P de $\mathbb{A}[X_1, \ldots, X_n]$ tels que*

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

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

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

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

4.4 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 dans $\mathbb{N}^*$, soit

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

Les N_j sont des polynômes symétriques. On complète la définition en posant $N_0 = n$. Newton a donné en 1666 des relations de récurrence qui permettent d'exprimer les N_j en fonction des Σ_i. Dans ses *Meditationes Algebricae* (1770), Waring a explicité N_j.[36] Ce sont ces résultats, marginaux pour la théorie de Galois, mais emblématiques d'une époque de l'algèbre, que nous prouvons ici.

Les formules de Newton

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

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

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

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

Proposition 10. *Pour $k \geq n$,*

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

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

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

Preuve de la seconde partie de la proposition. Le cas $k = n$ est déjà établi. On s'y ramène 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 et s'écrit donc $\displaystyle\sum_{\substack{\alpha \in \mathbb{N}^n \\ |\alpha| = k}} c_\alpha\, X^\alpha$ 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

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

Il s'ensuit que c_α est nul dès que $\alpha_{k+1}, \ldots, \alpha_n$ sont non tous nuls. Par symétrie, tous les c_α sont nuls.

Ces formules montrent que, si $k \leq n$ et si la caractéristique de $\mathbb{A}$ ne divise pas $n!$, Σ_k est un polynôme à coefficients dans $\mathbb{A}$ en $N_1, \ldots, N_k$. En particulier, les n premières sommes de Newton $N_1, \ldots, N_n$ déterminent les Σ_k, donc P.

Les formules de Waring

Nous utiliserons librement les séries formelles. En effet, il est 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 :

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

Par suite

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

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

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

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

$$\sum_{i=1}^{k} L(1-X_iY) = L\left(1-\Sigma_1 Y+\Sigma_2 Y^2+\cdots+(-1)^n\Sigma_n Y^n\right).$$

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

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

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

Proposition 11. *Avec les notations précédentes, on a*

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

L'exercice ci-après fait établir le jeu de formules inverse de celui de la proposition 11, également dû à Waring.

Exercice 70. 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 $k\in\{1,\ldots,n\}$, exprimer Σ_k en fonction des N_i pour $1\le i\le k$.

5 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 présenterons 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, très tôt conjecturé, a été complètement établi par Gauss après une tentative de d'Alembert.

Théorème 7. *Le corps $\mathbb{C}$ est algébriquement clos.* [37]

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 7 utilisent essentiellement des arguments 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 d'une racine carrée pour un élément de $\mathbb{R}^+$, d'une racine réelle pour un polynôme à coefficients réels de degré impair.

Cette section 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 plus loin une dernière approche, fondée sur la théorie de Galois. [38]

5.1 Démonstrations topologiques et/ou analytiques

Dans les preuves 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

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

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 élémentaire suppose connue l'exponentielle complexe.

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

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

Étape 2. Si z_0 est un nombre complexe tel que $|P|$ atteigne un minimum local en z_0 alors $P(z_0) = 0$.

On suppose par l'absurde $P(z_0) \neq 0$. 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 : $|P(z)| < |P(z_0)|$.

37. Ce résultat est connu comme « théorème de d'Alembert-Gauss » ou comme « théorème fondamental de l'algèbre ».

38. Il existe également des preuves du théorème de d'Alembert-Gauss fondées sur la géométrie riemannienne et des preuves probabilistes utilisant le mouvement brownien !

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 :

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

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 :

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

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

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

d'où

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

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 $1/f$.

Exercice 71. ⑤ *Donner une version de cette preuve ne faisant pas appel à 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 $1/P$ est entière[39] 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 72. 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 73. 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.*

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

Preuve 3 : inversion locale

Identifions $\mathbb{C}$ et $\mathbb{R}^2$. Alors P est différentiable en tout point de $\mathbb{R}^2$, sa différentielle $\mathrm{d}P(z)$ au point z de $\mathbb{C}$ étant la multiplication par $P'(z)$. En particulier, l'ensemble des z de $\mathbb{C}$ tels que $\mathrm{d}P(z)$ ne soit pas inversible est l'ensemble des zéros de P', donc fini. Le théorème résulte de la proposition ci-après.

Proposition 12. *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 $C = \{x \in E,\ \mathrm{d}f(x) \notin GL(E)\}$ 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 »). Si $(y, y') \in I^2$, on a $[y, e] \cap [y', e] = \{e\}$ et le résultat.

Exercice 74. ① *La proposition 12 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 le nombre complexe z_0 n'appartient pas à $\gamma(S)$, on peut définir le nombre de tours orientés que fait γ autour de z_0, ou *indice de γ par rapport à z_0*.

Plutôt que de définir brutalement l'indice par une formule intégrale, nous allons motiver la définition. Si $\rho = |\gamma - z_0|$, alors $u = (\gamma - z_0)/\rho$ 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 $\mathrm{Ind}_\gamma(z_0)$ de γ par rapport à z_0 en posant :

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

Puisque $u(a) = u(b)$, cet indice appartient à $\mathbb{Z}$.[40]

40. Le lecteur connaissant le théorème de relèvement continu pourra noter que ce qui précède vaut si l'application γ est seulement continue.

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 $[\ln \rho]_a^b = 0$:

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

Ceci nous suffira. Signalons cependant que la fonction qui à z_0 dans $\mathbb{C} \setminus \gamma(S)$ associe $\mathrm{Ind}_\gamma(z_0)$ est continue (intégrale à paramètre) et à valeurs dans $\mathbb{Z}$, donc constante sur chaque composante connexe de $\mathbb{C} \setminus \gamma(S)$, et tend vers 0 quand $|z_0| \to +\infty$, donc est nulle sur la composante non bornée de $\mathbb{C} \setminus \gamma(S)$. [41]

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

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

On a :

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

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

$$\frac{z\, P'(z)}{P(z)} \underset{|z| \to +\infty}{\longrightarrow} n,$$

on déduit $\varphi(r) \to n$ quand $r \to +\infty$. Contradiction. [42]

Exercice 75. 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 f'/f sur ce cercle parcouru une fois dans le sens direct ? En déduire le théorème 7.*

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 :

$$f(z_0) = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(z_0 + re^{it})\, \mathrm{d}t.$$

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 $\mathbb{C}$, alors $\ln(|f|)$ est harmonique sur Ω.

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

42. 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.

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

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

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 :

$$\frac{1}{2\pi}\int_{-\pi}^{\pi} \ln(|P(re^{it})|)\,\mathrm{d}t \underset{r\to+\infty}{\longrightarrow} +\infty.$$

C'est la contradiction désirée.

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

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

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

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

Soient u et v deux éléments de $\mathbb{R}^{+*}$. Nous allons appliquer le théorème de Cauchy à la fonction holomorphe $1/Q$ 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 $\displaystyle\int_\gamma \frac{\mathrm{d}z}{Q(z)} = 0$, c'est-à-dire

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

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

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

convergent. De plus, par convergence uniforme

$$\int_0^v \frac{\mathrm{d}t}{Q(\pm u+it)} \underset{u\to+\infty}{\longrightarrow} 0.$$

On en déduit

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

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

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

C'est contradictoire avec la stricte positivité de de Q sur $\mathbb{R}$.

Preuve 7 : fonctions implicites et discriminant

Fixons $n \in \mathbb{N}^*$ et 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 $\mathcal{U}_n$ admettant au moins une racine complexe (resp. l'ensemble des P de $\mathcal{U}_n$ admettant au moins une racine complexe de multiplicité supérieure ou égale à 2). 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.

Notons $\Delta(P)$ le discriminant d'un élément P de $\mathcal{U}_n$; alors $\mathcal{M}_n$ 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

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

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

Lemme 12. *Soient D un élément non nul de $\mathbb{C}[X_1, \ldots, X_n] \setminus \{0\}$,*

$$V_D = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \ ;\ D(x_1, \ldots, x_n) = 0\}.$$

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

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

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

on définit une fonction polynomiale qui ne s'annule pas en 0 et 1 ; l'ensemble des nombres complexes t qui annulent G est donc fini, en particulier de complémentaire connexe par arcs, d'où le résultat.

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

Ouvert. Soit Φ l'application de $\mathbb{C}_n[X] \times \mathbb{C}$ dans $\mathbb{C}$ définie par

$$\forall (Q, t) \in \mathbb{C}_n[X] \times \mathbb{C}, \qquad \Phi(Q, t) = Q(t).$$

L'application Φ est de classe C^1 et

$$\forall (Q, t) \in \mathbb{C}_n[X] \times \mathbb{C}, \qquad \partial_2\Phi(Q, t) = Q'(t).$$

Soient P un polynôme complexe de degré n, $z \in \mathbb{C}$ une racine simple de P, V un ouvert de $\mathbb{C}$ contenant z. En appliquant le théorème des fonctions implicites à Φ au point (P, z), on obtient que tout polynôme de degré n de $\mathbb{C}[X]$ suffisamment voisin de P a une racine simple dans V. On déduit aisément de ce fait que $\mathcal{S}_n \setminus \mathcal{M}_n$ est un ouvert de $\mathcal{U}_n \setminus \mathcal{M}_n$ (noter $z_1, \ldots, z_n$ les racines de $P \in \mathcal{S}_n \setminus \mathcal{M}_n$ et choisir, si $1 \leq i \leq n$, un voisinage V_i de z_i dans $\mathbb{C}$ de sorte que $V_1, \ldots, V_n$ soient deux à deux disjoints).

Fermé. Soit $(P_k)_{k \geq 1}$ une suite d'éléments de $\mathcal{S}_n$ convergeant vers P dans $\mathcal{U}_n \setminus \mathcal{M}_n$. Pour $k \geq 1$, on dispose de z_k dans $\mathbb{C}$ tel que $P_k(z_k) = 0$. Le lemme 4

de **2.4** assure que $(z_k)_{k\geq 1}$ est bornée. On dispose donc d'une valeur d'adhérence z de $(z_k)_{k\geq 1}$, qui vérifie $P(z) = 0$. Il s'ensuit que $P \in \mathcal{S}_n$.

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 13. *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 :

$$\begin{array}{rccc} q\ : & \mathbb{A}\setminus\{0\} & \to & \mathbb{A}\setminus\{0\} \\ & x & \mapsto & x^2 \end{array}$$

L'application q est de classe C^1. Sa différentielle en un point de $\mathbb{A}\setminus\{0\}$ 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

$$x^2 = y^2 \Longleftrightarrow x = \pm y$$

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 des résultats fondamentaux de la théorie des algèbres de Banach, le *théorème de Gelfand-Mazur.* [43]

Théorème 8. *Toute $\mathbb{R}$-algèbre de Banach commutative qui est un corps est isomorphe à $\mathbb{R}$ ou à $\mathbb{C}$.*

Exercice 76. 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 », c'est-à-dire, pour nous, l'existence d'un corps de décomposition (cf. chapitre **2**) ; à ce point près, sa démonstration est complète.

43. 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.

a) Il suffit de prouver 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 $\overline{P} = \sum_{k=0}^{n} \overline{a_k} X^k$, $Q = P\overline{P}$ 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 $\mathbb{C}$. »

Le cas $m = 0$ provient du théorème des valeurs intermédiaires, car alors

$$a_n P(x) \underset{x\to+\infty}{\longrightarrow} +\infty, \qquad a_n P(x) \underset{x\to+\infty}{\longrightarrow} -\infty.$$

Supposons $\mathcal{A}_m$ établie, soient P dans $\mathbb{R}[X]$ unitaire de degré $n = 2^{m+1}q$ avec q impair, $\mathbb{K}$ un surcorps de $\mathbb{C}$ sur lequel P est scindé, et $x_1, \ldots, x_n$ 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 dans $\mathbb{R}$, le polynôme :

$$P_c = \prod_{1\leq i<j\leq n} \left(X - (x_i + x_j + c\, x_i x_j)\right).$$

Si $\sigma \in \mathcal{S}_n$, σ induit une permutation de l'ensemble des parties à deux éléments de $\{1, \ldots, n\}$. Par conséquent :

$$P_c = \prod_{1\leq i<j\leq n} \left(X - (x_{\sigma(i)} + x_{\sigma(j)} + c\, x_{\sigma(i)} x_{\sigma(j)})\right).$$

Chaque coefficient de P_c est ainsi de la forme $U(x_1, \ldots, x_n)$ où U est un polynôme symétrique de $\mathbb{R}[X_1, \ldots, X_n]$; le corollaire 3 de **4.1** entraîne que P_c est à coefficients dans $\mathbb{R}$. De plus, le degré $\dfrac{n(n-1)}{2}$ de P_c est de la forme $2^m q'$ avec q' impair. Grâce à $\mathcal{A}_m$, le polynôme P_c a une racine dans $\mathbb{C}$: il existe deux éléments distincts i_c et j_c de $\{1, \ldots, n\}$ 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) la valeur commune de (i_c, j_c) et $(i_{c'}, j_{c'})$, $s = x_i + x_j$ 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.