Courbes Algébriques Planes

Alain Chenciner

Courbes Algébriques Planes

Springer

Alain Chenciner
Université Paris VII
Département de Mathématiques
2, Place Jussieu
75251 Paris Cedex 05
France

and

Astronomie et Systèmes Dynamiques,
IMCCE 77,
avenue Denfert Rochereau,
75014 Paris,
France
chencine@imcce.fr

Library of Congress Control Number: 2007931602

MSC (2000): 14-01, 14H50, 14H20

Première publication: Publications Mathématiques de l'Université Paris VII, 1978

Le dessin de la couverture est inspiré par une chorégraphie de trois corps découverte par Carles Simó

ISBN 978-3-540-33707-2 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media
springer.com

Typesetting by the author
Production: SPi, India
Cover design: WMXDesign, Heidelberg

Printed on acid-free paper 41/3180/SPi 5 4 3 2 1 0

Table des matières

Préface . . . . . **ix**

Introduction **1**

0 Courbes algébriques planes **3**

1 Ensembles algébriques affines **9**
1.1 Polynômes à plusieurs indéterminées : premières propriétés 9
1.2 Ensembles algébriques affines : le théorème des zéros 12
1.3 Composantes irréductibles d'un ensemble algébrique affine 18
1.4 Idéaux ayant un nombre fini de zéros 20
1.5 Morphismes d'ensembles algébriques affines 25
1.6 Ensembles algébriques affines irréductibles : fonctions rationnelles et anneaux locaux 28
1.7 Localisation 31

2 Courbes planes affines **33**
2.1 Sous-ensembles algébriques de $\boldsymbol{K}^2$ 33
2.2 Propriétés invariantes par changement de coordonnées affines 34
2.3 Points réguliers, points singuliers, multiplicités 35
2.4 Nombres d'intersections 38

3 Ensembles algébriques projectifs **43**
3.1 L'espace projectif $P_n(K)$ 43
3.2 Topologie des espaces projectifs réels et complexes de petite dimension 44
3.3 Ensembles algébriques projectifs et idéaux homogènes 47
3.4 Traduction affine $\leftrightarrow$ projectif : homogénéisation et déhomogénéisation 49

4 Courbes projectives planes : le théorème de Bézout 53
4.1 Quelques exemples 53
4.2 Le théorème de Bézout (1ère démonstration) 57

5 Le résultant 59
5.1 Théorie élémentaire du résultant 59
5.2 Résultant et nombres d'intersection 62
5.3 Résultant et théorème de Bézout 65

6 Point de vue local : anneaux de séries formelles 67
6.0 Introduction 67
6.1 Séries formelles à une indéterminée : premières propriétés 73
6.2 Séries formelles à plusieurs indéterminées : premières propriétés 76
6.3 Le théorème de préparation de Weierstrass pour les séries formelles 78
6.4 Passage des fractions rationnelles aux séries formelles : séparé complété d'un anneau 89

7 Anneaux de séries convergentes 93
7.1 Séries entières convergentes a une indéterminée 93
7.2 Séries entières convergentes à plusieurs indéterminées 97
7.3 La méthode des séries majorantes 101
7.4 Le théorème des fonctions implicites et le théorème de préparation pour les séries convergentes à plusieurs indéterminées 104
7.5 Thème d'étude 107
7.6 Envolée 107
7.7 Lecture 107

8 Le théorème de Puiseux 109
8.1 Paramétrages et polygone de Newton (cas formel) 109
8.2 Formulation du théorème de Puiseux comme un théorème de clôture algébrique 114
8.3 Application à l'étude des éléments irréductibles de $\boldsymbol{K}((\boldsymbol{X}))[\boldsymbol{Y}]$, $\boldsymbol{K}[[\boldsymbol{X}]][\boldsymbol{Y}]$, $\boldsymbol{K}[[\boldsymbol{X}, \boldsymbol{Y}]]$ 116
8.4 Décomposition d'un polynôme distingué $\boldsymbol{P} \in \boldsymbol{K}[[\boldsymbol{X}]][\boldsymbol{Y}]$ suivant les côtés de son polygone de Newton 120
8.5 Détection locale des facteurs multiples d'un élément de $\boldsymbol{K}[\boldsymbol{X}, \boldsymbol{Y}]$ 123
8.6 Résolution des problèmes de convergence 124
8.7 Interprétation topologique du théorème de Puiseux dans le cadre de la théorie des fonctions analytiques complexes 128

9 Théorie locale des intersections de courbes **133**
9.1 Branches = places (où on fait le point sur ce qui a précédé) 133
9.2 Intersection d'une branche et d'une droite passant par l'origine . . . 136
9.3 Intersection de deux courbes formelles 138

Appendice Un critère de rationalité pour les séries formelles à coefficients dans un corps (d'après Bourbaki) **143**

Liste d'exercices et problèmes **149**

Problème 1 . . . . . **155**

Problème 2 . . . . . **157**

Index **159**

Préface

Issu d'un cours de maîtrise de l'Université Paris 7, ce livre est republié tel qu'il était paru en 1978, à la correction près de quelques phrases trop peu écrites dans l'original. Il était, m'a-t-on dit, utile aux étudiants préparant l'agrégation et c'est ce qui m'a décidé à en proposer la republication.(*) *Je remercie Catriona Byrne d'avoir accueilli cette proposition avec sa souriante efficacité, Susanne Denskus d'en avoir suivi la réalisation avec bonne humeur et Jainendra K Jain d'en avoir assuré la composition avec patience. Merci à K. Venkatasubramanian (SPi, Inde) et Ellen Kattner pour la dernière étape. Merci enfin à Carles Simó qui m'a autorisé à transformer l'une de ses « chorégraphies » de trois corps en le paisible animal qui veille sur la couverture.*

À Paris
le 29 août 2006
A. Chenciner

(*) avec un clin d'œil amical à Raymonde Lombardo qui, il y a pas mal d'années , m'avait donné "le dernier exemplaire" agrémenté d'une jolie fleur.

Introduction

Ces notes correspondent à un cours de C4 que j'ai enseigné à Paris VII et à Nice à peu de choses près ce sont les notes qui ont été distribuées aux étudiants au jour le jour. J'ai préféré (pour de bonnes et de moins bonnes raisons) conserver l'aspect informel du texte plutôt qu'écrire un mille et unième livre sur ce sujet (ce pour quoi je ne suis pas compétent).

L'idée du cours était de traiter un problème particulier (le théorème de Bézout pour les courbes) et d'introduire à son propos certains outils permettant l'étude globale et locale d'une courbe (par exemple : notions projectives, théorème de préparation de Weierstrass, théorème de Puiseux, places, etc.). Les seules originalités sont les figures du chapitre IV (où l'on "voit" que $X^3 + Y^3 + Z^3 = 0$ *est un tore) et le passage de Puiseux formel à Puiseux convergent (où les éclatements apparaissent naturellement). Les manques sont innombrables, ce qui n'empêche pas l'ensemble d'être trop long pour un cours d'1h30 annuelle.*

Très ignorant au départ en ces matières, j'ai largement profité de la science de mes collègues et amis, en particulier J. Briançon, Y. Colombé, J. Emsalem, G. Jacob, Lê Dũng Tráng[1]*, M. Lejeune et B. Teissier.*

Au soleil à Nice
le 25 Mai 1978
A. Chenciner

[1] *qui a de plus le mérite (!) de ne pas m'avoir laissé en paix jusqu'à ce que j'aie fourni les dernières corrections de ce texte (auxquelles il a d'ailleurs participé). Son efficacité ne laisse pas de m'inquiéter.*

0

Courbes algébriques planes

Sous-ensembles algébriques de C

Dans tout ce cours, les anneaux considérés sont commutatifs avec unité.

Soit K un corps, I un ensemble, et pour chaque $i \in I$, $\phi_i \in K[X]$ un polynôme à une indéterminée à coefficients dans K. Que peut-on dire de l'ensemble

$$V((\phi_i)_{i\in I}) = \{x \in K | \forall i \in I, \phi_i(x) = 0\}?$$

Tout d'abord, on a

$$V((\phi_i)_{i\in I}) = V(\mathcal{J}) = \{x \in K | \forall f \in \mathcal{J}, f(x) = 0\},$$

où $\mathcal{J}$ est l'*idéal* de $K[X]$ *engendré* par les ϕ_i, c'est-à-dire

$$\begin{aligned}\mathcal{J} =&\{f \in K[X] | \exists p \in \mathbb{N}, \exists i_1, \ldots, i_p \in I, \exists g_1, \ldots, g_p \in K[X],\\ & f = g_1\phi_{i_1} + \cdots + g_p\phi_{i_p}\}.\end{aligned}$$

Contrairement aux apparences, nous avons beaucoup gagné à augmenter ainsi le nombre des équations. Rappelons en effet que si K est un corps, $K[X]$ est un anneau *principal* : tout idéal $\mathcal{J}$ de $K[X]$ est principal, c'est-à-dire engendré par un seul élément (il suffit de prendre un élément $f \in \mathcal{J}$ de degré minimum et d'effectuer la division euclidienne par f de tous les éléments de $\mathcal{J}$; on note alors $\mathcal{J} = (f)$).

Si f est un générateur de l'idéal engendré par les $(\phi_i)_{i\in I}$, on obtient

$$V((\phi_i)_{i\in I}) = V(f) = \{x \in K | f(x) = 0\}.$$

Pour étudier $V(f)$ il faut maintenant comprendre la structure de f ; commençons par rappeler deux définitions :

Définition 0.0.1 *– Soit A un anneau intègre (i.e. sans diviseur de zéro) ; un élément $a \in A$ est dit irréductible (ou premier) si $a \neq 0$, a n'est pas une unité (i.e. un élément inversible), et si chaque fois que $a = bc$ avec $b, c \in A$, ou b ou c est une unité.*

Définition 0.0.2 – *Un anneau A est dit factoriel s'il est intègre et si tout élément $a \neq 0 \in A$ admet une unique*[1] *factorisation en éléments irréductibles : cela signifie qu'il existe une unité u et des éléments irréductibles $p_1, \ldots, p_r$ tels que $a = up_1, \ldots, p_r$, et que si $a = vq_1, \ldots, q_s$ est une autre factorisation, on a $r = s$ et, après permutation éventuelle des indices, $p_i = u_i q_i$ où les u_i sont des unités.*

Théorème 0.0.3 – *Un anneau intègre et principal est factoriel.*

Par exemple, $\mathbb{Z}$ est factoriel.

Démonstration : Soit $a_0 \neq 0 \in A$ n'admettant pas de factorisation en éléments irréductibles ; en particulier, a_0 n'est pas irréductible, et s'écrit donc $a_0 = a_1 \cdot a'_1$, où ni a_1 ni a'_1 n'est une unité et où l'un au moins, par exemple a_1, n'admet pas de factorisation en éléments irréductibles ; on construit ainsi une suite infinie d'idéaux distincts

$$(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots$$

((a_0) désigne l'idéal de A engendré par a_0).

Mais il est facile de voir qu'une telle suite devient stationnaire à un cran fini si A est principal, ce qui est une contradiction.

L'unicité vient d'un argument bien connu de divisibilité. (Voir Lang p. 71, 72).

Corollaire 0.0.4 – *Si K est un corps, $K[X]$ est factoriel*

Si $f = u \prod_{i=1}^{k} f_i^{m_i}$ est une factorisation en éléments irréductibles, on voit que

$$V(f) = \bigcup_{i=1}^{k} V(f_i^{m_i}) = \bigcup_{i=1}^{k} V(f_i).$$

Il est en particulier clair que la donnée de $V(f)$ ne permet pas de retrouver f. Si $K = \mathbb{R}$, l'exemple $f(X) = X^2 + 1 \in \mathbb{R}[X]$ montre que la situation est désespérée. Sur $\mathbb{C}$, tout se passe le mieux possible grâce au théorème de d'Alembert–Gauss. Avant d'énoncer ce dernier, énonçons une proposition (dont la démonstration est laissée en exercice).

Proposition 0.0.5 – *Soit K un corps, les trois assertions suivantes sont équivalentes.*

(a) *Tout polynôme F, de degré supérieur ou égal à 1, de $K[X]$ admet une racine dans K.*

(b) *Tout polynôme irréductible de $K[X]$ est de degré 1.*

(c) *Tout polynôme non constant de $K[X]$ se décompose en un produit de polynômes de degré 1.*

Définition 0.0.6 – *On dit qu'un corps K est algébriquement clos s'il vérifie l'une des trois propriétés équivalentes ci-dessus.*

---

[1] Il peut y avoir existence sans qu'il y ait unicité : dans $\mathbb{Z}[\sqrt{-5}]$, on a les deux décompositions $6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$; ce genre d' exemple est à la base de la théorie des idéaux de Kummer.

Remarques 0.0.7 – 1. Un corps algébriquement clos a forcément une infinité d'éléments : si $K = \{x_1, \ldots, x_n\}$, le polynôme $f = \prod_{i=1}^{n}(X - x_i) + 1$ n'a pas de racine.

2. Tout corps peut être plongé dans un corps algébriquement clos (voir Lang : Algebra, p. 169–170).

Théorème 0.0.8 – (D'Alembert-Gauss) - Le corps $\mathbb{C}$ est algébriquement clos.

Démonstration : Il y en a beaucoup ; l'une des plus intuitives se trouve en exercice dans le livre d'Algèbre de Godement (exercice 25, p. 614) ; voir aussi « Topologie algébrique » de C. Godbillon (Hermann) et « Fonctions de variables complexes » de H. Cartan (Hermann).

Remarquer que ce théorème équivaut au théorème suivant :

Théorème 0.0.8′ – *Une fonction polynôme* $F : \mathbb{C} \to \mathbb{C}$ *est constante ou surjective*.

Définition 0.0.9 – *Soit* $f \in K[X], x \in K$. *On appelle multiplicité de* x *comme racine de* f *l'entier* $m = m_x(f)$ *défini par la condition suivante :*

1. $f(X) = (X - x)^m g(X)$, *avec* $g(x) \neq 0$.

Si K *est un corps de caractéristique zéro, ceci équivaut à*

2. $\frac{\partial^i f}{\partial X^i}(x) = 0$ *pour* $i \leqslant m - 1$, $\frac{\partial^m f}{\partial X^m}(x) \neq 0$.

On déduit du théorème 0.8 que tout $f \in \mathbb{C}[X]$ s'écrit

$$f = \alpha \prod_{x \in \mathbb{C}} (X - x)^{m_x(f)} = \alpha \prod_{i=1}^{k} (X - x_i)^{m_i}$$

(où $x_1, \ldots, x_k$ sont les racines de f, $m_i = m_{x_i}(f)$, et $\alpha \in K$).

Corollaire 0.0.10 – *Soient* f *et* g *deux éléments de* $\mathbb{C}[X]$. *On suppose que* $\forall x \in V(f)$, $g(x) = 0$. *Alors il existe un entier* M *tel que* $g^M \in (f)$.

Démonstration : $f = \alpha \prod_{i=1}^{k} (X - x_i)^{m_i}$, $V(f) = (x_1, \ldots, x_k)$; l'hypothèse s'écrit donc $g(x_i) = 0$ pour $i = 1, \ldots, k$, ce qui montre que g est divisible par $X - x_i$ pour tout i. Il suffit alors de prendre pour M le sup. des m_i.

Définition 0.0.11 – *Soient* A *un anneau et* $\mathscr{A}$ *un idéal de* A. *On appelle radical (ou racine) de* $\mathscr{A}$, *et on note* rad $\mathscr{A}$, *l'idéal (vérifier que c'en est un)*

$$\text{rad } \mathscr{A} = \{a \in A | \exists n \in \mathbb{C}, a^n \in \mathscr{A}\}.$$

Si E est un sous-ensemble de K, notons

$$I(E) = \{f \in K[X] | \forall x \in E, f(x) = 0\}.$$

C'est évidemment un idéal de $K[X]$.

Le corollaire 0.0.10 s'écrit encore

Corollaire 0.0.10′ – *Si $\mathcal{J}$ est un idéal de $\mathbb{C}[X]$, on a*

$$I(V(\mathcal{J})) = rad\, \mathcal{J}.$$

Revenons maintenant sur le polynôme $f \in \mathbb{C}[X]$,

$$f(X) = \alpha \prod_{i=1}^{k} (X - x_i)^{m_i}.$$

Le degré de f est attaché *globalement* au polynôme f, alors que $m_x(f)$ est attaché au comportement *local* de f « au voisinage de x ». La relation entre global et local est donnée par

$$m = \sum_{x \in \mathbb{C}} m_x(f) = \sum_{i=1}^{k} m_i.$$

Nous allons préciser cette relation local $\leftrightarrow$ global ; pour cela, rappelons que, si $\mathscr{A}$ est un idéal de l'anneau A, on peut définir un *anneau quotient* $A/\mathscr{A}$. D'autre part, un anneau tel que $K[X]$ a une structure supplémentaire, à savoir une structure d'espace vectoriel sur K compatible avec sa structure d'anneau (on dit que $K[X]$ est une *K-algèbre*) ; en particulier, un idéal $\mathcal{J}$ de $K[X]$ est aussi un sous-espace vectoriel de $K[X]$, et $K[X]/\mathcal{J}$ est de façon naturelle une K-algèbre, ce qui permet de parler de sa dimension sur K.

Lemme 0.0.12 – *Soit K un corps, $f \in K[X]$ un polynôme de degré m, on a*

$$\dim_K K[X]/(f) = m.$$

Démonstration : Si $g \in K[X]$, on peut écrire de façon *unique* $g = qf + r$ avec un reste r tel que degré $r <$ degré f ; cela montre que les classes des m éléments $1, X, X^2, \ldots, X^{m-1}$ forment une base de $K[X]/(f)$.

Pour interpréter de façon semblable les $m_x(f)$, remarquons que d'après le lemme 0.0.12, on a

$$m_x(f) = \dim_K K[X]/(X - x)^{m_x(f)}.$$

Un moyen de concentrer l'attention sur x est de « rendre inversibles » les polynômes qui ne s'annulent pas en x. Ceci nous amène à considérer les anneaux suivants :

$K(X) =$ corps des fractions de l'anneau intègre $K[X]$, dont les éléments sont appelés « fractions rationnelles » ;

$\mathscr{O}_x(K)$ défini par

$$\mathscr{O}_x(K) = \left\{ \frac{p}{q} \in K(X) | q(x) \neq 0 \right\}.$$

On voit que $K[X] \subset \mathscr{O}_x(K) \subset K(X)$.

Lemme 0.0.13 – *Soit K un corps, $f \in K[X]$, $x \in \mathbb{C}$, $f\mathscr{O}_x(K)$ l'idéal de $\mathscr{O}_x(K)$ engendré par f ; on a*

$$\dim_K \mathscr{O}_x(K)/f\mathscr{O}_x(K) = m_x(f).$$

Démonstration : Par définition de $m_x(f)$, on peut écrire $f(X) = (X-x)^{m_x(f)}g(x)$, avec $g(x) \neq 0$. En particulier, g est une unité de $\mathscr{O}_x(K)$ et il reste à voir que $\mathscr{O}_x(K)/(X-x)^{m_x(f)}$ est engendré les classes de $1, X-x, \ldots, (X-x)^{m_x(f)-1}$ (utiliser l'algorithme de division suivant les puissances croissantes de X, après s'être ramené par translation à $x = 0$).

Nous pouvons maintenant déduire de l'égalité $m = \sum_{x\in\mathbb{C}} m_x(f) = \sum_{i=1}^{k} m_i$ (valable si k est algébriquement clos) le

Théorème 0.0.14 – *Soit K un corps algébriquement clos (par exemple $K = \mathbb{C}$), $f \in K[X]$. Soient $x_1, \ldots, x_k$ les racines de f ; il existe un isomorphisme naturel de K-algèbres*

$$K[X]/(f) \xrightarrow{\sim} \prod_{i=1}^{k} \mathscr{O}_{x_i}(K)/f\mathscr{O}_{x_i}(K).$$

Démonstration : Considérés comme e.v. sur K, les deux membres ont la même dimension (d'après les lemmes 0.0.12, 0.0.13 et l'égalité $m = \sum_{i=1}^{k} m_i$). Pour voir que la flèche est un isomorphisme d'espaces vectoriels sur K, il suffit de vérifier que c'est un homomorphisme injectif, ce qui est facile ; le fait que la structure d'anneau soit préservée est tout aussi évident.

Bien entendu, un tel isomorphisme ne peut exister pour $K = \mathbb{R}$, comme le montre l'exemple $f(X) = X^2 + 1$.

Plan du Cours :

Dans le chapitre 1, nous verrons ce qui subsiste des propriétés que nous venons de passer en revue lorsqu'on remplace $K[X]$ par $K[X_1, \ldots, X_n]$.

Dans les chapitres suivants, nous nous limiterons au cas $n = 2$. Nous démontrerons en particulier le théorème de Bézout sur les intersections des courbes planes, ce qui nous amènera à parler de l'espace projectif.

Dans la deuxième partie, nous interpréterons en termes locaux les multiplicités d'intersections, et donnerons une autre démonstration du théorème de Bézout.

Bibliographie

Pour rédiger ce cours, j'ai puisé sans vergogne dans les sources suivantes :

- Sur les rappels d'algèbre
  R. Godement, Cours d'algèbre. Hermann 1966.

S. Lang, Algebra. Addison-Wesley 1965.
N. Bourbaki, Algèbre Chapitre 7. Hermann 1964.

- Sur le point de vue global
  W. Fulton, Algebraic curves. Benjamin 1969.
  Berthelot, Cours à Paris VII, 1971–1972. (Géométrie algébrique élémentaire).
  B. Teissier, Multiplicités. Cours à l'E.N.S. 1973–1974.
- Sur le point de vue local
  R.J. Walker, Algebraic curves, 1950 (Dover 1962).
  F. Pham, cours de 3ème cycle à Paris VII.

Pour ceux qui veulent poursuivre en algèbre commutative, je recommande vivement :

M.F. Atiyah et I.G. Macdonald, Introduction to commutative algebra, Addison-Wesley 1969.

Pour ceux qui veulent poursuivre en géométrie algébrique :

Shafarevitch, Foundations of algebraic geometry.

Enfin, pour ceux qui veulent remonter aux sources :

Sir I. Newton, Méthode des fluxions, Blanchard, 1966.
J. Dieudonné, Traité de Géométrie algébrique, Vol. 1, P.U.F., 1974.

1

Ensembles algébriques affines

1.1 Polynômes à plusieurs indéterminées[1] : premières propriétés

On peut, avec Godement, définir $A[X_1, \ldots, X_n]$ par récurrence par la formule $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$ et s'apercevoir que la variable X_n ne joue pas un rôle différent des autres, ou bien, avec Lang, donner tout de suite une définition symétrique. Dans tous les cas, on arrive à une écriture formelle $\Sigma a_{i_1 i_2 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}$ où seul un nombre fini des coefficients $a_{i_1 i_2 \ldots i_n}$ est différent de 0.

Nous venons de rappeler que, si K est un corps, l'anneau $K[X]$ est intègre, principal, et donc factoriel.

Il est clair que si A est un anneau intègre, $A[X]$ est un anneau intègre ; on en déduit par récurrence le

Lemme 1.1.1 – *Si K est un corps, $K[X_1, \ldots, X_n]$ est un anneau intègre.*

Il est clair que $K[X_1, \ldots, X_n]$ n'est pas principal (considérer l'idéal engendré par X_1, X_2 dans $K[X_1, X_2]$) ; nous verrons bientôt par quoi cette propriété est remplacée. Montrons maintenant le

Théorème 1.1.2 – *Si A est un anneau factoriel, $A[X]$ est un anneau factoriel.*

Corollaire 1.1.3 – *Si K est un corps, $K[X_1, \ldots, X_n]$ est un anneau factoriel.*

Démonstration du théorème 1.1.2 (voir les détails dans Lang p. 126–128).

Puisque A est intègre, A se plonge dans son corps des fractions K et donc $A[X] \subset K[X]$ qui est factoriel (voir 0.4). Le problème est alors de comparer les notions d'irréductibilité dans $A[X]$ et dans $K[X]$.

A étant factoriel, on montre facilement que tout élément $g \in K[X]$ s'écrit $g = C_g \cdot \tilde{g}$, où $C_g \in K$ et $\tilde{g} \in A[X]$ sont bien définis, à la multiplication près par une unité de A, par la condition suivante :

$\tilde{g} = \Sigma b_i X^i$, p.g.c.d. $(b_i) = 1$ (c'est-à-dire que tout élément de A divisant tous les b_i est forcément une unité). L'élément C_g s'appelle un *contenu* de g.

[1] J'utiliserai indifféremment les mots « variable » ou « indéterminée ».

En particulier, $C_{\tilde{g}} = 1$, et $g \in A[X] \Leftrightarrow C_g \in A$.

Soit $f \in A[X]$, et soit $f = \alpha \cdot q_1 \cdot q_2, \ldots, q_r$ une décomposition en facteurs irréductibles *dans* $K[X]$ (α est une unité de K. c'est-à-dire un élément $\neq 0$).

On en déduit $f = \alpha C_{q_1} C_{q_2}, \ldots, C_{q_r} \tilde{q}_1, \ldots, \tilde{q}_r$.

Pour conclure à l'existence d'une décomposition en facteurs irréductibles *dans* $A[X]$, on va montrer que

1. $\alpha C_{q_1} C_{q_2} \ldots C_{q_r} \in A$.
2. Les $\tilde{q}_i$ sont irréductibles dans $A[X]$.

C'est une conséquence des deux lemmes suivants :

Lemme 1. – *Si* $\alpha \in K$, $g_1, g_2 \in K[X]$, *on a* :

i) $C_{\alpha g_1} = \alpha C_{g_1}$.

ii) $C_{g_1 g_2} = C_{g_1} \cdot C_{g_2}$.

Lemme 2. – $f \in A[X]$ *est irréductible dans* $A[X]$, *si et seulement si* :

Ou bien $f \in A$ *et* f *est irréductible dans* A,

Ou bien f *est irréductible dans* $K[X]$ *et* $C_f = 1$.

Démonstration du Lemme 1. (i) est trivial ; on en déduit qu'il suffit de démontrer (ii) dans le cas où $C_{g_1} = C_{g_2} = 1$. Soit $g_1 = \Sigma a_i X^i$, $g_2 = \Sigma b_j X^j$, $g_1 \cdot g_2 = \Sigma C_k X^k$; soit p un élément irréductible de A. Par hypothèse, p ne divise pas tous les a_i et de même pour les b_j.

Soit $i_0 = \sup \{i \ : \ p \text{ ne divise pas } a_i\}$, $j_0 = \sup \{j \ : \ p \text{ ne divise pas } b_j\}$

Un calcul élémentaire montre que p ne divise pas $C_{i_0 \cdot j_0}$ d'où la conclusion[2].

Démonstration du Lemme 2. Si $f = \phi \cdot \psi$ dans $A[X]$ et si f est irréductible dans $K[X]$, ou ϕ ou ψ (par exemple ϕ) est une unité de $K[X]$, c'est-à-dire un élément $\neq 0$ de K.

Alors $C_f = \phi \cdot C_\psi$. Mais $C_\psi \in A$ et si l'on suppose $C_f = 1$, on voit que ϕ est une unité de A.

La réciproque se voit de façon analogue.

Pour conclure la démonstration du théorème, il faut voir l'unicité de la factorisation dans $A[X]$; celà découle facilement de l'unicité de la factorisation dans $K[X]$.

Remarque Décomposer un élément de $A[X_1, \ldots, X_n]$ en facteurs irréductibles est en général une entreprise très difficile, même pour des polynômes à une variable.

Le seul cas facile est celui de $\mathbb{C}[X]$ car, grâce au théorème de Gauss–d'Alembert, les éléments irréductibles sont toujours du premier degré.

La proposition suivante introduit la notion fondamentale d'*anneau noethérien* : ce mot vient de Emmy Noether (la fille de Max Noether) qui fut l'une des grandes pionnières de l'algèbre « moderne » (1882–1935).

[2] Cela revient à considérer les classes de g_1 et g_2 dans l'anneau *intègre* $A/(p)[X]$.