Mathématiques en devenir

101. — Jacques Faraut. *Analyse sur les groupes de Lie, une introduction.*

102. — Patrice Tauvel. *Corps commutatifs et théorie de Galois.*

103. — Jean Saint Raymond. *Topologie, calcul diff. et variable complexe*

104. — Clément de Seguins Pazzis. *Invitation aux formes quadratiques*

105. — Bruno Ingrao. *Coniques projectives, affines et métriques*

106. — Wolfgang Bertram. *Calcul différentiel topologique élémentaire*

107. — Henri Lombardi & Claude Quitté. *Algèbre commutative. Méthodes constructives. Modules projectifs de type fini*

108. — Frédéric Testard. *Analyse mathématique. La maîtrise de l'implicite*

109. — Grégory Berhuy. *Modules : théorie, pratique... et un peu d'arithmétique*

110. — Bernard Candelpergher. *Théorie des probabilités. Une introduction élémentaire*

111. — Philippe Caldero et Jérôme Germoni. *Histoires hédonistes de groupes et de géométries. Tome premier*

112. — Gema-Maria Díaz-Toca, Henri Lombardi & Claude Quitté. *Modules sur les anneaux commutatifs*

113. — Philippe Caldero et Jérôme Germoni. *Histoires hédonistes de groupes et de géométries. Tome second* – encores

114. — Alain Debreil. *Groupes finis et treillis de leurs sous-groupes*

115. — François Rouvière. *Initiation à la géométrie de Riemann*

116. — Nikolaï Nikolski. *Matrices et opérateurs de Toeplitz*

117. — Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries. Tome premier*

118. — Martine Queffélec et Hervé Queffélec. *Analyse complexe et applications.*

119. — Alain Debreil, Jean-Denis Eiden, Rached Mneimné et Tuong-Huy NGuyen. *Formes quadratiques et géométrie*

120. — Christian Leruste.*Topologie algébrique–Une introduction, et au-delà*

121. — Grégory Berhuy. *Algèbre : le grand combat*

122. — Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries. Tome second*

123. — Charles-Michel Marle. *Géométrie symplectique et géométrie de Poisson*

125. — Pascal Boyer. *Petit compagnon des nombres et de leurs applications*

127. — David Chiron. *Chemins d'analyse (1) - Espace de Schwartz, distributions tempérées et transformation de Fourier*

Patrice TAUVEL

Corps commutatifs et théorie de Galois

Cours et exercices

Troisième édition, revue et bonifiée

Calvage & Mounet

Patrice Tauvel est professeur honoraire à l'Université de Poitiers. Ses recherches concernent l'algèbre non commutative et plus particulièrement la théorie des algèbres de Lie. Il est l'auteur d'une quinzaine d'ouvrages, dont plusieurs se rapportent au programme de l'agrégation. On lui doit également, en collaboration avec Rupert Yu, le monumental « Lie Algebras and Algebraic Groups », paru en 2005 chez Springer dans la collection Monographs in Mathematics.

patrice.tauvel3@orange.fr

Mathematics Subject Classification (1991) – Primary :

Mathematics Subject Classification (2000)

11R32	Galois theory
12-01	Field theory and polynomials – Instructional exposition
12F05	Field extensions – Algebraic extensions
12F20	Field extensions – Transcendental extensions
11T06	Finite fields and polynomials
34M50	Inverse problems (Riemann-Hilbert, inverse differential Galois)

ISBN 2-916352-87-9

Imprimé sur papier permanent.

Il più nobile piacere
è la gioia di capire.

Leonardo de Vinci

Préface

L'auteur de ces notes souhaite, dans cette préface, indiquer quels sont les principes qui l'ont guidé lors de la rédaction de cet ouvrage.

Tout d'abord, il a voulu que le livre soit très autonome. Pour ce faire, plusieurs chapitres sont consacrés à des révisions portant sur les groupes et les polynômes. Si l'on ne peut pas revenir sur tous les résultats que l'étudiant a vu lors de ses études universitaires, il peut lui être très profitable de pouvoir trouver dans l'ouvrage les démonstrations d'assertions que l'on va utiliser dans la suite. C'est certainement le cas pour les groupes symétriques et la résolubilité de certains de ces groupes.

L'autre souci du rédacteur a été d'écrire un livre de niveau plutôt élevé. Actuellement, une grande mode consiste à écrire des ouvrages de mathématiques assez édulcorés en ce qui concerne le niveau. Cette tendance semble avoir encore été accentuée avec la réforme du LMD et, dernièrement, on a vu dans la plupart des universités les programmes de mathématiques diminuer même dans les filières où c'est la discipline principale. Il est clair que c'est une erreur : les étudiants ne sont absolument pas moins intelligents que ceux des générations précédentes, et plutôt que de diminuer les programmes il vaut mieux essayer de leur enseigner des choses difficiles, mais qui peuvent les captiver. Ce qui est contenu dans cet ouvrage dépasse donc ce qui est enseigné dans un cours « usuel » de théorie de Galois, mais peut donner le goût à des étudiants d'aller encore plus loin dans la théorie.

Dernier point enfin, l'auteur n'a pas souhaité non plus sacrifier à une mode très tenace, et qui consiste à raconter la vie de Galois.

Table des matières

Avant-propos

Ce livre traite de la théorie des corps commutatifs. Il s'adresse aux étudiants de maîtrise ou de master en mathématiques, aux candidats au concours de l'agrégation de mathématiques, et aux enseignants.

La théorie des corps est maintenant une partie très importante des mathématiques. Elle intervient de manière fondamentale dans plusieurs domaines : géométrie algébrique, théorie des nombres, groupes arithmétiques. Signalons aussi son importance dans la théorie de Galois différentielle, qui est une branche des mathématiques en plein développement.

Le niveau de ce livre dépasse sans doute ce qu'il est possible d'enseigner dans un cours de maîtrise durant un semestre. Au risque de décourager le lecteur, précisons cependant que le texte ne fait qu'aborder certains aspects de la théorie, et ne présente pas l'ensemble de ce qui est connu sur le sujet.

Les connaissances nécessaires pour entreprendre la lecture de cet ouvrage sont celles enseignées dans un cours basique d'algèbre de licence. Afin de faciliter le travail du lecteur et de rendre ce livre très autonome, ces connaissances ont été reprises, avec démonstrations, dans les chapitres 1, 2, 3 et 14.

Dans les chapitres 4 à 8, on présente des notions qui seront la base de toute la suite du livre : différents types d'extensions et corps finis.

Les chapitres 9 et 15 traitent d'un des aspects essentiels concernant les corps commutatifs : la théorie de Galois. On en donne des applications concernant la résolubilité par radicaux et les constructions à la règle et au compas dans les chapitres 10 et 11. Dans le chapitre 11, on prouve aussi la transcendance de e et de π.

On présente dans les chapitres 16 et 17 des notions qui sont fondamentales en géométrie algébrique. En particulier, on y prouve le théorème des zéros de Hilbert.

Le chapitre 18 est un premier pas vers l'étude des corps différentiels ; c'est là un domaine en plein essor.

Nous pensons que le contenu de ce livre peut être une bonne base pour aborder l'étude de la géométrie algébrique, des groupes arithmétiques et de la théorie des nombres. En outre, il est susceptible d'intéresser les personnes curieuses de connaître la théorie de Galois.

Dans la seconde édition, nous avons corrigé certaines coquilles et erreurs. Nous remercions Vincent Beck et Roger Mansuy pour leur aide. D'autre part, nous avons complété certains chapitres par de nouveaux exercices.

Dans la troisième édition, nous avons toujours corrigé quelques coquilles et ajouté ou complété certains exercices. En ce qui concerne la théorie de Galois, tout en conservant ce qui est traité au chapitre 9, nous avons voulu traiter, au chapitre 15, le cas général, celui où les extensions considérées ne sont pas de degré fini. Cela se fait en utilisant quelques notions de topologie assez élémentaires et sans doute bien connues de la plupart des lecteurs.

Chapitre 1

Résultats divers

L'objet de ce chapitre est d'introduire des notations qui nous seront utiles dans toute la suite de l'ouvrage et aussi de rappeler des résultats variés d'algèbre générale. Pour ce qui concerne l'algèbre linéaire, le lecteur peut se reporter éventuellement à [18].

1.1. Conventions et notations

1.1.1. Les symboles

$$\mathbb{N}\,,\ \mathbb{N}^*\,,\ \mathbb{Q}\,,\ \mathbb{Q}^*\,,\ \mathbb{Z}\,,\ \mathbb{R}\,,\ \mathbb{R}_+\,,\ \mathbb{R}_-\,,\ \mathbb{R}^*\,,\ \mathbb{R}_+^*\,,\ \mathbb{R}_-^*\,,\ \mathbb{C}\,,\mathbb{C}^*$$

ont la signification habituelle, et le symbole $\mathbb{Z}^*$ désigne l'ensemble des entiers non nuls. Si $n \in \mathbb{N}$, on pose :

$$\mathbb{N}_n = \{p \in \mathbb{N}\,;\, 0 \leqslant p \leqslant n\}\,, \quad \mathbb{N}_n^* = \{p \in \mathbb{N}^*\,;\, 1 \leqslant p \leqslant n\}.$$

Si z est un nombre complexe, $\overline{z}$ est son conjugué, $\operatorname{Re} z$ sa partie réelle et $\operatorname{Im} z$ sa partie imaginaire.

1.1.2. Soient E et F des ensembles.

On note id_E l'application identique de E, $E \setminus F$ l'ensemble des éléments de E qui n'appartiennent pas à F et $\mathcal{F}(E, F)$ l'ensemble des applications de E dans F. Si E est fini, $\operatorname{card} E$ est son cardinal.

1.1.3. Soient E et I des ensembles non vides. On note E^I l'ensemble des familles $(x_i)_{i\in I}$ telles que $x_i \in E$ pour tout $i \in I$.

Supposons que E soit un groupe commutatif, de loi notée additivement. Soient $\xi = (x_i)_{i\in I} \in E^I$ et $J_\xi = \{i \in I\,;\, x_i \neq 0\}$. On note $E^{(I)}$ l'ensemble

des éléments ξ de E^I tels que J_ξ soit fini. On dit qu'un élément de $E^{(I)}$ est une famille *presque nulle* (indexée par I) d'éléments de E.

Remarques. Précisons quelques points quant à la terminologie qui suit (et qui n'est peut-être pas universelle). *Dans tout le livre, les anneaux sont supposés posséder un élément unité, et les corps ne sont pas nécessairement commutatifs. De même, un anneau intègre n'est pas supposé commutatif.* Dans la suite aussi, un sous-anneau d'un anneau contient l'élément unité de l'anneau ; un homomorphisme d'anneaux est supposé unitaire.

1.1.4. Soit A un anneau.

On note respectivement 0_A et 1_A l'élément nul et l'élément unité de A. On écrit 0 et 1 pour 0_A et 1_A s'il n'y a pas de risque de confusion. On dit que A est l'anneau nul s'il est réduit à $\{0_A\}$, c'est-à-dire si $0_A = 1_A$.

On rappelle que A est dit *intègre* s'il n'est pas nul et si le produit de deux éléments non nuls de A est non nul. Un *corps* est un anneau intègre dans lequel tout élément non nul est inversible [1].

1.1.5. Soit $n \in \mathbb{N}$. L'ensemble $n\mathbb{Z}$ des multiples entiers de n est un idéal de $\mathbb{Z}$. On peut donc former l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$. Rappelons que cet anneau quotient est un corps si et seulement si l'entier n est premier.

Si p est un nombre premier, on note encore $\mathbb{F}_p$ pour le corps $\mathbb{Z}/p\mathbb{Z}$.

1.1.6. Soient K un corps, et soit k un sous-corps commutatif de K. On munit K de sa loi de groupe additif et de la loi de composition externe, de domaine d'opérateurs k, donnée par $(\lambda, a) \mapsto \lambda a$, pour $\lambda \in k$ et $a \in K$. Il est clair que K devient ainsi un k-espace vectoriel. Sauf mention du contraire, lorsque K sera considéré comme un k-espace vectoriel, ce sera au moyen de la structure précédente.

Définition. Soit A un anneau commutatif. On appelle *A-algèbre (associative unitaire)* un quadruplet $(\mathcal{A}, +, *, \cdot)$ vérifiant les conditions suivantes.

(i) Le triplet $(\mathcal{A}, +, \cdot)$ est un A-module.

(ii) Le triplet $(\mathcal{A}, +, *)$ est un anneau non nul.

(iii) Pour tous $\lambda, \mu \in k$ et tous $a, b, x, y \in \mathcal{A}$, on a :

$$x*(\lambda\cdot a+\mu\cdot b)=\lambda\cdot(x*a)+\mu\cdot(x*b),\ \ (\lambda\cdot a+\mu b)*y=\lambda\cdot(a*y)+\mu\cdot(b*y).$$

1. Il est à noter que si A n'est pas l'anneau nul et si tout élément non nul de A est inversible, alors l'anneau A est intègre.

1.1.7. Soit A un anneau commutatif, et soit $(\mathcal{A}, +, *, \cdot)$ une A-algèbre.

Par abus de langage, on dit souvent « soit $\mathcal{A}$ une A-algèbre » au lieu de « soit $(\mathcal{A}, +, *, \cdot)$ une A-algèbre ».

L'application $\mathcal{A} \times \mathcal{A} \to \mathcal{A}$, $(x, y) \mapsto x * y$ est appelée le produit de $\mathcal{A}$. Sauf risque de confusion, on note xy pour $x * y$. De même, si $\lambda \in A$, on écrit λx pour $\lambda \cdot x$. L'algèbre $\mathcal{A}$ est dite commutative si son produit l'est.

Une sous-algèbre de $\mathcal{A}$ est un sous-A-module de $\mathcal{A}$ qui est un sous-anneau de $\mathcal{A}$. On définit de manière évidente la notion de sous-algèbre engendrée par une partie de $\mathcal{A}$.

Une partie de $\mathcal{A}$ est appelée un idéal à gauche (resp. à droite, bilatère) de $\mathcal{A}$ si c'est un sous-A-module de $\mathcal{A}$ et un idéal à gauche (resp. à droite, bilatère) de l'anneau $\mathcal{A}$. Si $\mathcal{I}$ est un idéal bilatère de $\mathcal{A}$, l'ensemble $\mathcal{A}/\mathcal{I}$ a alors une structure naturelle de A-algèbre.

Un *homomorphisme* $\mathcal{A} \to \mathcal{B}$ entre deux A-algèbres est une application linéaire des A-modules sous-jacents à $\mathcal{A}$ et $\mathcal{B}$ qui est de plus un homomorphisme des anneaux sous-jacents à $\mathcal{A}$ et $\mathcal{B}$.

1.2. Relations d'ordre

1.2.1. Soit E un ensemble. Rappelons qu'une relation d'ordre sur E est une relation binaire $\leqslant$ sur E qui vérifie les conditions suivantes.

▷ $x \leqslant x$ pour tout $x \in E$.

▷ Si $x, y \in E$ vérifient $x \leqslant y$ et $y \leqslant x$, alors $x = y$.

▷ Si x, y, z vérifient $x \leqslant y$ et $y \leqslant z$, alors $x \leqslant z$.

Un ensemble muni d'une relation d'ordre est appelé un *ensemble ordonné*.

Une relation d'ordre sur E est appelée une relation d'ordre *total* (on dit aussi que E est *totalement ordonné*) si, pour tous $x, y \in E$, on a $x \leqslant y$ ou $y \leqslant x$.

1.2.2. Soit $(E, \leqslant)$ un ensemble ordonné, et soit A une partie non vide de E. On dit que :

▷ $a \in E$ est un *majorant* de A si $x \leqslant a$ pour tout $x \in A$;

▷ $m \in A$ est un *élément maximal* de A si $x = m$ dès que $x \in A$ vérifie $m \leqslant x$.

1.2.3. Définition. Un ensemble ordonné E est dit *inductif* si toute partie totalement ordonnée de E possède un majorant dans E.

1.2.4. Exemples. Soit E un ensemble, et soit $\mathcal{E}$ un ensemble de parties de E, que l'on ordonne par la relation d'inclusion (notée indifféremment $\subset$ ou $\subseteq$). Supposons que, pour tout sous-ensemble totalement ordonné $\mathcal{F}$ de $\mathcal{E}$, la réunion $\mathcal{G}_{\mathcal{F}}$ des ensembles de $\mathcal{F}$ appartienne à $\mathcal{E}$. Alors, $(\mathcal{E}, \subset)$ est inductif.

2) Soient E, F des ensembles, et soit $\mathcal{F}$ l'ensemble des couples (A, f) où A est une partie de E et f une application de A dans F. On voit facilement que l'on ordonne $\mathcal{F}$ en convenant que :

$$(A, f) \leqslant (B, g) \quad \Leftrightarrow \quad A \subseteq B \ \text{ et } \ g|A = f.$$

Soit $\mathcal{G} = \{(A_i, f_i)\,;\, i \in I\}$ une partie totalement ordonnée de $\mathcal{F}$. Notons A la réunion des A_i pour $i \in I$.

Soit $x \in A$. Si $x \in A_i \cap A_j$, on a, par exemple, $A_i \subseteq A_j$ car $\mathcal{G}$ est totalement ordonnée, donc $f_i(x) = f_j(x)$. On peut donc définir une application f de A dans F en posant, pour $x \in A$, $f(x) = f_i(x)$, où $i \in I$ est un indice tel que $x \in A_i$. Ainsi, $(A, f) \in \mathcal{F}$, et l'ensemble ordonné $(\mathcal{F}, \leqslant)$ est inductif.

1.2.5. Théorème. (Théorème de Zorn) Tout ensemble inductif possède au moins un élément maximal.

1.2.6. Proposition. Soit E un ensemble, et soit $\mathcal{E}$ un ensemble de parties de E tel que, pour tout sous-ensemble $\mathcal{F}$ de $\mathcal{E}$, totalement ordonné par inclusion, la réunion des ensembles de $\mathcal{F}$ appartient à $\mathcal{E}$. Alors, $\mathcal{E}$ possède un élément maximal.

Démonstration. C'est une conséquence directe de 1.2.4 et 1.2.5. □

1.3. Corps des fractions

1.3.1. Théorème. *Soit A un anneau commutatif et intègre. Il existe un couple (k, ε) qui vérifie les propriétés suivantes.*

(i) *k est un corps commutatif et ε est un homomorphisme injectif d'anneaux de A dans k.*

(ii) *Si $\lambda \in k$, il existe $(a, p) \in A \times (A\backslash\{0\})$ tel que $\lambda = \varepsilon(a)[\varepsilon(p)]^{-1}$.*

De plus, si K un corps et si $\omega\colon A \to K$ est un homomorphisme injectif d'anneaux, K contient un sous-corps isomorphe à k. Enfin, si le couple (ω, K) vérifie les deux conditions précédentes, les corps k et K sont isomorphes.

Démonstration. 1) Posons $E = A \times (A\backslash\{0\})$. Définissons une relation binaire $\mathcal{R}$ sur E en convenant que $(a, p)\mathcal{R}(b, q)$ signifie que $aq - bp = 0$.

Il est immédiat que la relation $\mathcal{R}$ est réflexive et symétrique et, A étant intègre, il est clair que $\mathcal{R}$ est transitive. C'est donc une relation d'équivalence. Notons $\phi\colon E \to E/\mathcal{R} = k$ la surjection canonique.

Définissons sur E des lois internes (addition et multiplication) par :

$$(a,p)+(b,q)=(aq+bp,pq)\,,\quad (a,p)\cdot(b,q)=(ab,pq).$$

Ces lois sont commutatives, associatives, compatibles avec $\mathcal{R}$, et la multiplication est distributive par rapport à l'addition. Notons encore $+$ et $\cdot$ les lois quotients définies sur k. Elles vérifient les propriétés précédentes. De plus, $\phi(0,1)$ est élément neutre pour l'addition et $\phi(-a,p)$ est l'opposé de $\phi(a,p)$. Par conséquent, $(k,+)$ est un groupe abélien.

Pour la multiplication, $\phi(1,1)$ est élément neutre. Si $\phi(a,p)\neq\phi(0,1)$, autrement dit $a\neq 0$, alors $\phi(p,a)$ est l'inverse de $\phi(a,p)$. Par suite, k est un corps commutatif.

2) Soit $\varepsilon\colon A\to k$, $x\mapsto\phi(x,1)$. C'est un homomorphisme injectif d'anneaux et, quel que soit $(a,p)\in E$:

$$\phi(a,p)=\phi(a,1)\phi(1,p)=\phi(a,1)[\phi(p,1)]^{-1}=\varepsilon(a)[\varepsilon(p)]^{-1}.$$

3) Soit K un corps, et soit $\omega\colon A\to K$ un homomorphisme injectif d'anneaux.

Si $\phi(a,p)=\phi(b,q)$, on a $aq-bp=0$, donc $\omega(a)\omega(q)-\omega(b)\omega(q)=0$. Comme ω est une injection, $\omega(p)$ et $\omega(q)$ sont non nuls, et l'on voit donc que le produit $\omega(a)[\omega(p)]^{-1}$ ne dépend que de $\phi(a,p)$. Ainsi, on peut définir un homomorphisme d'anneaux

$$\theta\colon k\to K,\ \ \phi(a,p)\mapsto\omega(a)[\omega(p)]^{-1}.$$

Il est évident que θ est injectif. Enfin, si le couple (ω,K) vérifie (ii), θ est surjectif, donc K et k sont des corps isomorphes. □

1.3.2. Le corps k défini en 1.3.1 est appelé le *corps des fractions* de A et noté $\mathrm{Fract}(A)$. L'injection $\varepsilon\colon A\to k$ est dite *canonique*. On identifie $\varepsilon(A)$ et A au moyen de ε. L'élément $x=\phi(a,p)$ s'écrit alors ap^{-1} ou a/p, et l'on dit que la fraction a/p est un *représentant* de x.

Par exemple, $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$.

1.4. Caractéristique d'un anneau

1.4.1. Soit A un anneau. Pour $a\in A$ et $n\in\mathbb{Z}$, le symbole $n\cdot a=na$ est défini par :

$$na=\begin{cases} a+a+\cdots+a\ (n\ \text{ termes}) & \text{si } n>0,\\ 0_A & \text{si } n=0,\\ (-a)+(-a)+\cdots+(-a)\ (-n\ \text{ termes}) & \text{si } n<0.\end{cases}$$

Il est immédiat de vérifier que l'application $\varphi_A\colon\mathbb{Z}\to A$, $n\mapsto n\cdot 1_A$ est un homomorphisme d'anneaux. Son noyau est donc de la forme $c\mathbb{Z}$, pour un unique $c\in\mathbb{N}$.

On dit que l'entier c est la *caractéristique* de A, et l'on note $c = \mathrm{car}(A)$. Si A n'est pas l'anneau nul (autrement dit, la caractéristique n'est pas égale à 1), il est clair que c est le plus petit entier positif ou nul qui vérifie les conditions équivalentes suivantes :
(i) $c \cdot 1_A = 0_A$;
(ii) $c \cdot a = 0_A$ pour tout $a \in A$.

Exemples. 1) On a $\mathrm{car}(\mathbb{Z}) = \mathrm{car}(\mathbb{Q}) = \mathrm{car}(\mathbb{R}) = \mathrm{car}(\mathbb{C}) = 0$.
2) Si $n \in \mathbb{N}^*$, alors $\mathrm{car}(\mathbb{Z}/n\mathbb{Z}) = n$.

1.4.2. Proposition. *Si A est un anneau intègre, sa caractéristique est nulle ou est un nombre premier.*

Démonstration. Supposons $\mathrm{car}(A) = pq$, avec $p, q \in \mathbb{N}^*$ distincts de 1. Alors, $p \cdot 1_A$ et $q \cdot 1_A$ sont des éléments non nuls de A, dont le produit est nul. C'est absurde puisque A est intègre. □

1.4.3. Proposition. *Soit A un anneau commutatif dont la caractéristique est un nombre premier p. L'application $f_A \colon A \to A$, $x \mapsto x^p$ est un homomorphisme de l'anneau A, appelé l'*homomorphisme de Frobenius *de A.*

Démonstration. On a bien $f_A(1) = 1$ et $f_A(xy) = f_A(x)f_A(y)$, car A est commutatif. L'entier p étant premier, pour $1 \leqslant k < p$, il est immédiat que le coefficient binomial

$$\mathrm{C}_p^k = \frac{p(p-1)\cdots(p-k+1)}{k!}$$

est divisible par p. Utilisant à nouveau la commutativité de A, pour $a, b \in A$, on obtient alors :

$$(a+b)^p = \sum_{k=0}^{p} \mathrm{C}_p^k a^k b^{p-k} = a^p + b^p,$$

d'où le résultat. □

1.4.4. Si la caractéristique c de A n'est pas un nombre premier, l'application $x \mapsto x^c$ n'est pas nécessairement un endomorphisme de A. On le voit facilement avec $A = \mathbb{Z}/4\mathbb{Z}$.

1.4.5. Corollaire. *Soient K un corps commutatif de caractéristique $p > 0$, et soit f l'homomorphisme de Frobenius de K. Alors,*

(i) *si K est fini, f est un automorphisme de K ;*

(ii) *si $K = \mathbb{F}_p$, on a $f = \mathrm{id}_K$.*

Démonstration. (i) D'après 1.4.2, p est un nombre premier et f est un endomorphisme de K (1.4.3). Comme K est un corps, l'idéal $\ker f$ est réduit à $\{0\}$, et f est injectif. Si de plus K est fini, f est donc bijectif.

(ii) Le groupe multiplicatif $\mathbb{F}_p \backslash \{0\}$ étant de cardinal $p-1$, on a $x^{p-1} = 1$ pour tout $x \in \mathbb{F}_p \backslash \{0\}$. D'où, $x^p = x$ pour tout $x \in \mathbb{F}_p$. □

1.5. Corps premiers

1.5.1. Définition. Un corps K est dit *premier* s'il ne contient aucun sous-corps autre que lui-même.

1.5.2. Proposition. (i) *Le corps $\mathbb{Q}$ est premier.*

(ii) *Pour tout entier premier p, le corps $\mathbb{F}_p$ est premier.*

Démonstration. (i) Soit K un sous-corps de $\mathbb{Q}$. Il contient 1, donc le sous-corps de $\mathbb{Q}$ engendré par 1, c'est-à-dire $\mathbb{Q}$.

(ii) Si $n \in \mathbb{Z}$, notons $\overline{n}$ son image canonique dans $\mathbb{F}_p$. Si K est un sous-corps de $\mathbb{F}_p$, il contient $\overline{1}$, donc $\{\overline{n}\,;\, n \in \mathbb{Z}\} = \mathbb{F}_p$. Ainsi, $K = \mathbb{F}_p$. □

1.5.3. Définition. Soit K un corps. On appelle *sous-corps premier* de K l'intersection de tous les sous-corps de K.

1.5.4. Soit K un corps, et soit P son sous-corps premier. Le centre de K étant un sous-corps de K, il contient P. Par suite, P est commutatif. Il est clair par ailleurs que K est premier si et seulement si $K = P$.

1.5.5. Proposition. *Soit K un corps de caractéristique c, et soit P son sous-corps premier.*

(i) *Si $c = 0$, alors P est isomorphe à $\mathbb{Q}$.*

(ii) *Si $c \neq 0$, c'est un nombre premier, et P est alors isomorphe à $\mathbb{F}_c$.*

Démonstration. Soit $\varphi_K : \mathbb{Z} \to K$ comme en 1.4.1. On a $\ker \varphi_K = c\mathbb{Z}$.

▷ Si $c = 0$, l'homomorphisme d'anneaux φ_K est injectif, et se prolonge donc en un homomorphisme de corps

$$\begin{array}{rccc} \psi_K : & \mathbb{Q} & \to & K \\ & p/q & \mapsto & (p \cdot 1_K)(q \cdot 1_K)^{-1}, \end{array}$$

pour $p \in \mathbb{Z}$ et $q \in \mathbb{Z}^*$. Comme ψ_K est injectif, l'image $\psi_K(\mathbb{Q})$ est isomorphe au corps de départ $\mathbb{Q}$, si bien qu'elle est un corps premier (d'après 1.5.2). On a $P \subseteq \psi_K(\mathbb{Q})$, d'où $P = \psi_K(\mathbb{Q})$.

▷ Supposons $c \neq 0$. D'après 1.4.2, c est un entier premier. L'application φ_K induit un isomorphisme d'anneaux de $\mathbb{F}_c = \mathbb{Z}/c\mathbb{Z}$ sur l'image L de φ_K, qui est un sous-corps de K. Comme $P \subseteq L$, on a $P = L$, à nouveau d'après l'alinéa 1.5.2. □

1.5.6. Proposition. *Soit K un corps fini, et soit q son cardinal.*

(i) *Il existe $n \in \mathbb{N}^*$ et un entier premier p tels que $q = p^n$.*

(ii) *Si q est premier, alors K est isomorphe à $\mathbb{F}_q$.*

Démonstration. (i) Soit P le sous-corps premier de K. D'après 1.5.5, P est isomorphe à un corps $\mathbb{F}_p$, avec p premier. Considérons le corps K comme un P-espace vectoriel, et soit n sa dimension. Alors, K est isomorphe à P^n, si bien que $q = p^n$.

(ii) C'est immédiat d'après 1.5.5 et (i). □

1.5.7. Proposition. *Soit K un corps, et soit P son sous-corps premier. Si σ est un endomorphisme de K, on a $\sigma(x) = x$ pour tout $x \in P$. En particulier, si K est de caractéristique $p > 0$, on a $x^p = x$ pour tout $x \in P$.*

Démonstration. Le corps P étant le sous-corps de K engendré par l'élément 1, on a $\sigma(x) = x$ pour tout $x \in P$, puisque $\sigma(1) = 1$. Le second point résulte alors de 1.4.3. □

1.6. Théorème de d'Alembert

1.6.1. Nous supposons, dans ce paragraphe, que le lecteur connaît l'exponentielle complexe et ses principales propriétés.

Lemme. *Soit $f\colon \mathbb{R} \to \mathbb{C}$ une application de classe C^1, admettant 2π pour période et telle que $f(t) \neq 0$ pour tout $t \in \mathbb{R}$. Alors,*

$$I(f) = \frac{1}{2\pi i} \int_0^{2\pi} \frac{f'(t)}{f(t)}\, dt$$

est un nombre entier.

Démonstration. Si $t \in \mathbb{R}$, posons :

$$\varphi(t) = f(t) \exp\Big(-\int_0^t \frac{f'(u)}{f(u)}\, du\Big).$$

On a facilement $\varphi' = 0$. Par conséquent, pour $t \in \mathbb{R}$,

$$f(t) = f(0) \exp\Big(\int_0^t \frac{f'(u)}{f(u)}\, du\Big).$$

Comme $f(2\pi) = f(0)$, il vient $e^{2i\pi I(f)} = 1$. Écrivons $I(f) = \alpha + i\beta$, avec $\alpha, \beta \in \mathbb{R}$. On obtient $e^{2i\pi\alpha} = e^{2\pi\beta}$. La restriction de l'exponentielle à $\mathbb{R}$ est strictement croissante, et $|e^{2i\pi\alpha}| = 1$. D'où, $\beta = 0$. Alors, $\alpha \in \mathbb{Z}$. □

1.6.2. Théorème. (Théorème de d'Alembert)
Soit $n \in \mathbb{N}^*$, et soient $a_0, \ldots, a_n$ des nombres complexes tels que $a_n \neq 0$. Pour $z \in \mathbb{C}$, posons :

$$P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0.$$

Il existe un nombre complexe ζ tel que $P(\zeta) = 0$.

Démonstration. Considérons l'application

$$\begin{array}{ccc} \mathbb{R}_+ \times \mathbb{R} & \to & \mathbb{C} \\ (r,t) & \mapsto & f_r(t) = P(re^{it}) \end{array}.$$

Supposons $0 \notin P(\mathbb{C})$. Soit alors

$$g_r(t) = \frac{f_r'(t)}{f_r(t)} = \frac{iP'(re^{it})re^{it}}{P(re^{it})},$$

et soit

$$I(r) = \frac{1}{2\pi i}\int_0^{2\pi} g_r(u)\,du.$$

Fixons $a \in \mathbb{R}_+^*$. L'application $[0,a]\times[0,2\pi] \to \mathbb{C}$, $(r,t) \mapsto g_r(t)$ est continue, donc uniformément continue. Si $\varepsilon > 0$, il existe $\eta > 0$ tel que :

$$r, \rho \in [0,a],\ t \in [0,2\pi],\ |r-\rho| \leqslant \eta \Rightarrow |g_r(t) - g_\rho(t)| \leqslant \varepsilon.$$

Il en résulte que, pour $r, \rho \in [0,a]$ vérifiant $|r-\rho| \leqslant \eta$, on a alors

$$|I(r) - I(\rho)| \leqslant \frac{1}{2\pi}\int_0^{2\pi} |g_r(t) - g_\rho(t)|\,dt \leqslant \varepsilon.$$

On a ainsi prouvé que l'application $\mathbb{R}_+ \to \mathbb{C}$, $r \mapsto I(r)$ est continue. Or, $I(r)$ est entier (1.6.1). On en déduit que, pour tout $r \geqslant 0$, on a $I(r) = I(0) = 0$.

Par ailleurs, si $z \in \mathbb{C}^*$, on a

$$\frac{P'(z)z}{P(z)} = \frac{na_n + (n-1)a_{n-1}z^{-1} + \cdots + a_1 z^{1-n}}{a_n + a_{n-1}z^{-1} + \cdots + a_0 z^{-n}}.$$

Par suite, il existe $R > 0$ tel que

$$|z| > R \ \Rightarrow\ \Big|\frac{P'(z)z}{P(z)} - n\Big| < 1.$$

Il en résulte que $|I(r) - n| < 1$ si $r > R$, et l'entier $I(r)$ vérifie donc $I(r) = n$ si l'on suppose encore $r > R$. Contradiction. □

1.7. Fonction d'Euler

1.7.1. Si $m \in \mathbb{N}^*$ et $n \in \mathbb{N}$, on écrit $m \mid n$ pour signifier que m divise n, et l'on note, pour $n \in \mathbb{N}^*$, $\mathbf{P}_n$ l'ensemble des entiers $x \in \mathbb{N}_n^*$ qui sont premiers avec n. On pose $\varphi(n) = \operatorname{card}\mathbf{P}_n$. L'application $\varphi\colon \mathbb{N}^* \to \mathbb{N}^*$, $n \mapsto \varphi(n)$ ainsi définie est appelée la *fonction indicatrice d'Euler*.

1.7.2. Proposition. *Soit G un groupe cyclique d'ordre n. Le nombre de générateurs de G est égal à $\varphi(n)$.*

Démonstration. Tout groupe cyclique d'ordre n étant isomorphe au groupe additif $\mathbb{Z}/n\mathbb{Z}$, il suffit donc de prouver le résultat pour ce dernier groupe.

Soient $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la surjection canonique et $x \in \mathbb{N}_n^*$. Le groupe $\mathbb{Z}/n\mathbb{Z}$ étant engendré par $\pi(1)$, dire que $\pi(x)$ engendre $\mathbb{Z}/n\mathbb{Z}$ signifie qu'il existe un entier $p \in \mathbb{Z}$ tel que $\pi(1) = p\pi(x)$. Ceci équivaut à l'existence de $q \in \mathbb{Z}$ vérifiant $px + qn = 1$, c'est-à-dire que x et n sont premiers entre eux. □

Nous adopterons désormais la notation $\mathbb{Z}_n$ pour désigner l'anneau $\mathbb{Z}/n\mathbb{Z}$ ou son groupe additif sous-jacent.

1.7.3. Lemme. *Soient $m, n \in \mathbb{N}^*$ et G, H des groupes.*

(i) *Soient $a \in G$ et $b \in H$ d'ordres finis r et s, et Soit t le plus petit multiple commun à r et s. Alors, (a, b) est d'ordre fini t dans le groupe $G \times H$.*

(ii) *Si G, H sont cycliques et finis d'ordres m et n, le groupe $G \times H$ est cyclique si et seulement si m et n sont premiers entre eux.*

(iii) *Dire que les groupes $\mathbb{Z}_m \times \mathbb{Z}_n$ et $\mathbb{Z}_{mn}$ sont isomorphes équivaut au fait que m et n sont premiers entre eux.*

Démonstration. Notons multiplicativement les lois de G et H, et désignons par e_G, e_H leurs éléments neutres.

(i) On a $(a, b)^t = (e_G, e_H)$, donc l'ordre de (a, b) divise t.

Si $p \in \mathbb{N}^*$ vérifie $(a, b)^p = (e_G, e_H)$, alors $a^p = e_G$ et $b^p = e_H$. Par suite, $p \mid r$ et $p \mid s$, donc $p \mid t$. D'où l'assertion.

(ii) Dire que G (resp. H et $G \times H$) est cyclique signifie qu'il possède un élément d'ordre m (resp. n et mn). Le résultat est donc clair d'après (i).

(iii) Comme $\mathbb{Z}_{mn}$ est cyclique et a même cardinal que $\mathbb{Z}_m \times \mathbb{Z}_n$, ces deux groupes sont isomorphes si et seulement si $\mathbb{Z}_m \times \mathbb{Z}_n$ est cyclique. L'assertion est ainsi un cas particulier de (ii). □

1.7.4. Théorème. (i) *Si les entiers $m, n \in \mathbb{N}^*$ sont premiers entre eux, ils vérifient $\varphi(mn) = \varphi(m)\varphi(n)$.*

(ii) *Soient $d_1, \ldots, d_r \in \mathbb{N}^*$ et $p_1, \ldots, p_r$ des entiers premiers distincts, alors*

$$\varphi\big(p_1^{d_1} \cdots p_r^{d_r}\big) = \prod_{i=1}^{r} p_i^{d_i - 1}(p_i - 1).$$

(iii) *Soit $n \in \mathbb{N}^*$. Si $d \in \mathbb{N}^*$ est un diviseur de n, le groupe $\mathbb{Z}_n$ contient un et un seul sous-groupe d'ordre d.*

(iv) *Si $n \in \mathbb{N}^*$, on a :*

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

Démonstration. (i) Les groupes $\mathbb{Z}_m \times \mathbb{Z}_n$ et $\mathbb{Z}_{mn}$ étant isomorphes (1.7.3), le nombre de générateurs de $\mathbb{Z}_m \times \mathbb{Z}_n$ est $\varphi(mn)$ (1.7.2).

Si a et b sont des générateurs respectifs de $\mathbb{Z}_m$ et $\mathbb{Z}_n$, alors (a, b) est un générateur de $\mathbb{Z}_m \times \mathbb{Z}_n$ (1.7.3, (i)). D'où, $\varphi(m)\varphi(n) \leqslant \varphi(mn)$.

Réciproquement, si (a, b) est un générateur de $\mathbb{Z}_m \times \mathbb{Z}_n$, alors a et b sont respectivement des générateurs de $\mathbb{Z}_m$ et $\mathbb{Z}_n$, donc $\varphi(mn) \leqslant \varphi(n)\varphi(m)$.

(ii) Soient p un entier premier et $n \in \mathbb{N}^*$. Il est clair que $\varphi(p) = p - 1$. Dire que $r \leqslant p^n$ n'est pas premier avec p^n signifie que $r = sp$, avec $1 \leqslant s \leqslant p^{n-1}$. On a donc $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p - 1)$. L'assertion résulte alors du point (i).

(iii) Soit $x \mapsto \overline{x}$ la surjection canonique de $\mathbb{Z}$ sur $\mathbb{Z}_n$. Si $q \in \mathbb{N}^*$ vérifie $n = qd$, alors $\overline{q}$ est d'ordre d. En outre, si $\overline{r}$ est d'ordre d, dr est multiple de n, donc r est multiple de q. Alors, $\overline{r}$ appartient au sous-groupe de $\mathbb{Z}_n$ engendré par $\overline{q}$.

(iv) Un sous-groupe d'un groupe cyclique l'étant aussi, on déduit de (iii) que si $d \mid n$, le groupe $\mathbb{Z}_n$ contient exactement $\varphi(d)$ éléments d'ordre d. D'où l'assertion. □

1.7.5. Théorème. *Soit (G, e) un groupe abélien d'ordre fini N. On suppose que, pour tout diviseur d de N, le groupe G contient au plus d éléments x tels que $x^d = e$. Alors, G est cyclique.*

Démonstration. Pour $d \mid N$, soit n_d le nombre d'éléments de G d'ordre d. On va montrer que $n_d \leqslant \varphi(d)$. C'est clair si $n_d = 1$. Supposons $n_d > 1$.

Soient $x \in G$ d'ordre d, et soit H_x le sous-groupe de G engendré par x. Alors, H_x est d'ordre d, et l'on a donc $y^d = e$ pour tout $y \in H_x$. D'après l'hypothèse, tous les éléments d'ordre d de G appartiennent à H_x. Comme le sous-groupe H_x contient $\varphi(d)$ éléments d'ordre d (1.7.2), il vient $n_d \leqslant \varphi(d)$. Or, d'après 1.7.4, (iv),

$$\sum_{d|N} \varphi(d) = N = \sum_{d|N} n_d.$$

D'où, $n_d = \varphi(d)$, si $d \mid N$. En particulier, $n_N = \varphi(N) \neq 0$, et G est cyclique. □

1.7.6. Théorème. (Petit théorème de Fermat) *Si $a, n \in \mathbb{N}^*$ sont premiers entre eux, alors $a^{\varphi(n)}$ est congru à 1 modulo n.*

Démonstration. On peut supposer $n > 1$. Notons $u \mapsto \overline{u}$ la surjection canonique $\mathbb{Z} \to \mathbb{Z}_n$. Soit U l'ensemble des unités de l'anneau $\mathbb{Z}_n$. Un entier m vérifie $\overline{m} \in U$ si et seulement si m et n sont premiers entre eux. Il en découle que $\operatorname{card} U = \varphi(n) = q$. Notons $U = \{\alpha_1, \ldots, \alpha_q\}$. L'application $x \mapsto \overline{a}x$ est une bijection de U sur lui-même. Par conséquent, si $\beta = \alpha_1 \cdots \alpha_q$, il vient $\beta\overline{a}^q = \beta$. D'où, $\overline{a}^q = \overline{1}$. □

1.8. Fonction de Möbius

1.8.1. Définition. La *fonction de Möbius* est l'application $\mu\colon \mathbb{N}^* \to \mathbb{C}$ définie comme suit :

(i) $\mu(1) = 1$.

(ii) $\mu(p_1 \cdots p_k) = (-1)^k$ si $p_1, \ldots, p_k$ sont des entiers premiers distincts.

(iv) $\mu(n) = 0$ si n est divisible par le carré d'un nombre premier.

1.8.2. Théorème. (i) *On a $\mu(mn) = \mu(m)\mu(n)$ pour $m, n \in \mathbb{N}^*$ premiers entre eux.*

(ii) *La fonction de Möbius est l'unique application $\chi\colon \mathbb{N}^* \to \mathbb{C}$ qui vérifie $\chi(1) = 1$ et*

$$\sum_{d|n} \chi(d) = 0$$

pour tout entier $n \geqslant 2$.

Démonstration. (i) C'est clair par définition de μ.

(ii) Montrons que μ vérifie la relation précédente. C'est évident si n est de la forme p^m avec p premier et $m \in \mathbb{N}^*$. Sinon, l'entier n s'écrit $n = rs$, avec $r > 1, s > 1$ premiers entre eux, et les diviseurs de n sont ainsi les ab, avec $a \mid r$ et $b \mid s$. D'où, d'après (i),

$$\sum_{d|n} \mu(d) = \sum_{a|r,\, b|s} \mu(a)\mu(b) = \Big(\sum_{a|r} \mu(a)\Big)\Big(\sum_{b|s} \mu(b)\Big).$$

On obtient dès lors le résultat par récurrence.

Si χ vérifie la même relation, on a $\mu(1) = \chi(1)$ et, si $n \geqslant 2$:

$$\chi(n) + \sum_{d|n,\, d<n} \chi(d) = 0 = \mu(n) + \sum_{d|n,\, d<n} \mu(d).$$

On termine à nouveau par récurrence. □

1.8.3. Proposition. *Soient $f\colon \mathbb{R}_+^* \to \mathbb{C}$ et $g\colon \mathbb{N}^* \to \mathbb{C}$. On suppose que $f(x) = 0$ si $x < 1$. Pour $x > 0$ et $n \in \mathbb{N}^*$, on pose*

$$F(x) = \sum_{k=1}^{\infty} f\Big(\frac{x}{k}\Big) \quad \text{et} \quad G(n) = \sum_{d|n} g\Big(\frac{n}{d}\Big).$$

Alors,

$$f(x) = \sum_{k=1}^{\infty} \mu(k) F\Big(\frac{x}{k}\Big) \quad \text{et} \quad g(n) = \sum_{d|n} \mu(d) G\Big(\frac{n}{d}\Big).$$

Démonstration. Comme $f(x) = 0$ si $x < 1$, les sommes définissant F et f sont en fait finies. D'après 1.8.2, il vient :

$$\sum_{k=1}^{\infty} \mu(k) F\Big(\frac{x}{k}\Big) = \sum_{k=1}^{\infty} \sum_{q=1}^{\infty} \mu(k) f\Big(\frac{x}{qk}\Big) = \sum_{q=1}^{\infty} f\Big(\frac{x}{q}\Big)\Big(\sum_{d|q} \mu(d)\Big) = f(x).$$

Prolongeons g en $f\colon \mathbb{R}_+^* \to \mathbb{C}$ en posant $f(x) = 0$ si $x \in \mathbb{R}_+^* \setminus \mathbb{N}^*$. Il vient $F(x) = 0$ si $x \notin \mathbb{N}^*$ et $F(n) = G(n)$ si $n \in \mathbb{N}^*$. D'où la seconde formule. □

1.8.4. Corollaire. *Pour $y \in \mathbb{R}$, on note $E(y)$ la partie entière de y. Soient $n \in \mathbb{N}^*$ et $x \in \mathbb{R}_+^*$. Alors,*

$$\sum_{k=1}^{\infty} \mu(k) E\Big(\frac{x}{k}\Big) = 1 \quad \textit{et} \quad \sum_{d|n} \mu(d)\,\frac{n}{d} = \varphi(n).$$

Démonstration. Définissons $f\colon \mathbb{R}_+^* \to \mathbb{R}$ par $f(x) = 1$ si $x \geqslant 1$ et $f(x) = 0$ si $x < 1$. Avec les notations de 1.8.3, on a $F(x) = E(x)$. D'où le premier point. Le second résulte aussi de 1.8.3 en utilisant 1.7.4, (iv) avec $g = \varphi$. □

1.9. Pseudo-anneaux

1.9.1. Définition. On appelle *pseudo-anneau* un triplet $(A, +, *)$ où A est un ensemble et $+, *$ des lois de composition internes sur A, appelées respectivement addition et produit, et vérifiant les conditions suivantes.

(i) Le couple $(A, +)$ est un groupe abélien.

(ii) La loi $*$ est associative et distributive par rapport à l'addition.

1.9.2. En termes « simples », un pseudo-anneau est un anneau n'ayant pas nécessairement d'élément unité.

On dit, par abus de langage, « soit A un pseudo-anneau » plutôt que « soit $(A, +, *)$ un pseudo-anneau ». En outre, si $x, y \in A$, on note xy pour $x * y$.

Un pseudo-anneau A est dit *intègre* s'il n'est pas réduit à $\{0\}$ et si le produit de deux éléments non nuls de A est non nul.

1.9.3. Proposition. *Si A est un pseudo-anneau intègre fini, c'est un corps.*

Démonstration. On note $A^* = A \setminus \{0\}$ et, si $x \in A$, $\ell_x\colon y \mapsto xy$ est l'application de A dans lui-même. Fixons $a \in A^*$ (un tel a existe, car $A \neq \{0\}$).

Comme A est intègre, ℓ_a est une injection, donc une bijection, car A est fini. Par suite, il existe $\varepsilon \in A$ tel que $a\varepsilon = a$. On a $\varepsilon \neq 0$. Si $x \in A$, alors

$$\ell_a(\varepsilon x) = a(\varepsilon x) = (a\varepsilon)x = ax = \ell_a(x).$$

D'où, $\varepsilon x = x$. De même, $(x\varepsilon)a = x(\varepsilon a) = xa$, et A étant intègre, on a $x\varepsilon = x$. On a montré que ε est élément neutre pour le produit, donc A est un anneau.

Si $x \in A^*$, il existe $y \in A$ tel que $\ell_x(y) = \varepsilon$. On a $y \neq 0$, car $\varepsilon \neq 0$ et

$$\ell_x(yx) = x(yx) = (xy)x = \varepsilon x = x = x\varepsilon = \ell_x(\varepsilon).$$

D'où, $yx = \varepsilon$, et x est inversible dans A. □

1.10. Matrices et endomorphismes

1.10.1. Dans cette section 1.10, on désigne par A un anneau commutatif et par K un corps commutatif. On va rappeler, sans démonstration, quelques résultats d'algèbre linéaire.

Soient $n, p \in \mathbb{N}^*$. On note $\mathrm{M}_{n,p}(A)$ l'ensemble des $(n \times p)$-matrices à éléments dans A. On écrit $\mathrm{M}_n(A)$ pour $\mathrm{M}_{n,n}(A)$. On désigne par I_n l'élément unité de $\mathrm{M}_n(A)$ et par $\mathrm{GL}_n(A)$ le groupe des éléments inversibles de la A-algèbre $\mathrm{M}_n(A)$. Si $M \in \mathrm{M}_n(A)$, $\operatorname{tr} M$ (resp. $\det M$) désigne la trace (resp. le déterminant) de M. On pose

$$\mathrm{SL}_n(A) = \{M \in \mathrm{M}_n(A)\,;\, \det M = 1\}.$$

Si $\lambda_1, \ldots, \lambda_n \in A$, on note $\operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ la matrice $M = [m_{ij}] \in \mathrm{M}_n(A)$ définie par $m_{ii} = \lambda_i$, pour $1 \leqslant i \leqslant n$, et $m_{ij} = 0$, si $i \neq j$.

De même, si $M_1, \ldots, M_q$ sont des matrices carrées, $\operatorname{diag}(M_1, \ldots, M_q)$ est la matrice diagonale par blocs dont les blocs diagonaux sont les M_i.

1.10.2. Si $M \in \mathrm{M}_n(K)$, on désigne par μ_M le polynôme minimal de M et par χ_M son polynôme caractéristique. On a donc

$$\chi_M(X) = \det(X\,\mathrm{I}_n - M).$$

On rappelle que μ_M divise χ_M et que χ_M divise $(\mu_M)^n$.

Soient $P(X) = \alpha_0 + \alpha_1 X + \cdots + \alpha_{p-1}X^{p-1} + X^p$ un polynôme unitaire de degré p, à coefficients dans K, et

$$\kappa_P = \begin{pmatrix} 0 & 0 & \ldots & 0 & -\alpha_0 \\ 1 & 0 & \ldots & 0 & -\alpha_1 \\ 0 & 1 & \ldots & 0 & -\alpha_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -\alpha_{p-1} \end{pmatrix} \in \mathrm{M}_p(K).$$

On dit que κ_P est la *matrice compagnon* de P. On a

$$P(X) = \mu_{\kappa_P}(X) = \chi_{\kappa_P}(X).$$

1.10.3. Dans ce qui suit, les espaces vectoriels considérés sont des K-espaces vectoriels.

Soient E, F des espaces vectoriels. On note $\mathrm{L}(E,F)$ l'ensemble des applications linéaires de E dans F et $\mathrm{Isom}(E,F)$ l'ensemble des isomorphismes linéaires de E sur F. Pour $u \in \mathrm{L}(E,F)$, $\ker u$ est le noyau de u et $\operatorname{im} u$ son image. On pose $\mathrm{L}(E) = \mathrm{L}(E,E)$ et $\mathrm{GL}(E) = \mathrm{Isom}(E,E)$.

Dans la suite de ce paragraphe, on suppose E et F de dimension finie.

Si $u \in \mathrm{L}(E)$, on désigne par $\operatorname{tr} u$ (resp. $\det u$) la trace (resp. le déterminant) de u. On pose

$$\mathrm{SL}(E) = \{u \in \mathrm{L}(E)\,;\, \det u = 1\}.$$

Soient $v \in \mathrm{L}(E,F)$ et $\mathcal{E}, \mathcal{F}$ des bases de E et F. On note $\mathrm{Mat}(v\,;\mathcal{E},\mathcal{F})$ la matrice de v dans les bases $\mathcal{E}$ et $\mathcal{F}$. Lorsque $E = F$, on écrit $\mathrm{Mat}(v\,;\mathcal{E})$ pour $\mathrm{Mat}(v\,;\mathcal{E},\mathcal{E})$.

Pour $u \in \mathrm{L}(E)$, on désigne par χ_u (resp. μ_u) le polynôme caractéristique (resp. minimal) de u. Si $\mathcal{E}$ est une base de E, et si $M = \mathrm{Mat}(u\,;\mathcal{E})$, alors

$$\operatorname{tr} u = \operatorname{tr} M\,, \quad \det u = \det M\,, \quad \chi_u = \chi_M\,, \quad \mu_u = \mu_M.$$

1.10.4. Soient $K[X]$ l'ensemble des polynômes à une indéterminée sur K et E un K-espace vectoriel de dimension finie non nulle. Soit $u \in L(E)$.

Si $P(X) = a_0 + a_1X + \cdots + a_rX^r \in K[X]$, on note $P(u)$ l'endomorphisme de E défini par $P(u) = a_0 \operatorname{id}_E + a_1u + \cdots + a_ru^r$.

Si $x \in E$, on définit un idéal non nul de $K[X]$ en posant :

$$I_{u,x} = \{P \in K[X]\,;\, P(u)(x) = 0\}.$$

Il existe un unique polynôme unitaire $R_{u,x}$ tel que $I_{u,x}$ soit l'ensemble des multiples de $R_{u,x}$ dans $K[X]$; pour tout $x \in E$, $R_{u,x}$ divise μ_u.

Proposition. *Il existe $x \in E$ tel que $\mu_u = R_{u,x}$.*

Remarque. Soient $\mathscr{E} = (e_1, \ldots, e_n)$ une base de E et P un polynôme unitaire. Soit $u \in \mathrm{L}(E)$ vérifiant $\mathrm{Mat}(u\,;\mathscr{E}) = \kappa_P$. Avec les notations précédentes, on a $\mu_u = \chi_u = R_{u,e_1} = P$.

1.11. Exercices

Exercice 1.1. On utilise les notations de 1.10.4. Soit E un K-espace vectoriel de dimension finie, et soit $u \in \mathrm{L}(E)$.

a) Montrer que μ_u est un multiple des $R_{u,x}$ pour $x \in E$, et que tout multiple des $R_{u,x}$, pour $x \in E$, est un multiple de μ_u.

b) Soit $(e_1, \ldots, e_n)$ une base de E. Prouver que μ_u est le ppcm des R_{u,e_i}, avec $1 \leqslant i \leqslant n$.

c) Soient $x, y \in E$. Prouver que si $R_{u,x}$ et $R_{u,y}$ sont premiers entre eux, alors $R_{u,x+y} = R_{u,x}R_{u,y}$.

d) Montrer qu'il existe $x \in E$ tel que $\mu_u = R_{u,x}$.

e) On dit que E est u-monogène s'il existe un vecteur x tel que E soit l'ensemble des $P(u)(x)$, $P \in K[X]$. Montrer que E est u-monogène si et seulement si $\mu_u = \chi_u$.

f) On suppose que E est u-monogène. Soit F un sous-espace vectoriel de E stable par u. On note $v = u_{|F}$ l'endomorphisme de F induit par u. Prouver que F est v-monogène.

Exercice 1.2. Soit A un anneau commutatif. Si $\mathfrak{a}$ est un idéal de A, on note $\sqrt{\mathfrak{a}}$ l'ensemble des éléments x de A pour lesquels il existe $n \in \mathbb{N}^*$ vérifiant $x^n \in \mathfrak{a}$. Pour des idéaux $\mathfrak{a}$ et $\mathfrak{b}$ de A, établir les résultats suivants.

a) $\sqrt{\mathfrak{a}}$ est un idéal de A contenant $\mathfrak{a}$ et vérifiant $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$.

b) On a :

$$\sqrt{\mathfrak{ab}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}\,, \quad \sqrt{\mathfrak{a}+\mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}.$$

Exercice 1.3. Si $z \in \mathbb{C}$, on pose $N(z) = |z|^2 = z\overline{z}$. On désigne par A l'ensemble des nombres complexes de la forme $a + ib$, avec $a, b \in \mathbb{Z}$.

a) Prouver que A est un sous-anneau de $\mathbb{C}$. On désigne par U l'ensemble des éléments inversibles de A.

b) Si $x \in A$, montrer que $x \in U$ si et seulement si $N(x) = 1$. En déduire que l'ensemble U est constitué des éléments $-1, 1, i, -i$.

c) Soient $z \in \mathbb{C}$ et $x \in A\backslash\{0\}$. Montrer qu'il existe $\alpha \in A$ et $\beta \in \mathbb{C}$ tels que

$$z = \alpha x + \beta \quad \text{et} \quad N(\beta) < N(x).$$

d) Montrer que si $\mathfrak{a}$ est un idéal de A, il existe $x \in A$ tel que $\mathfrak{a} = Ax$.

Exercice 1.4. Soit $m \in \mathbb{N}^*$; posons $\alpha = \sqrt{1+m^2}$. On note A l'ensemble des nombres réels de la forme $a + b\alpha$, avec $a, b \in \mathbb{Z}$. Soit $\omega = m + \alpha$. Si $a, b \in \mathbb{Z}$, et $x = a + b\alpha$, on écrit $N(x) = a^2 - b^2\alpha^2$.

a) Prouver que A est un sous-anneau de $\mathbb{R}$ et que $N(xy) = N(x)N(y)$ pour $x, y \in A$.

b) Soit U l'ensemble des éléments inversibles de A. Montrer qu'un élément x de A appartient à U si et seulement si $N(x) = \pm 1$.

c) Soit $x = a + b\alpha \in U$, avec $a, b \in \mathbb{Z}$. On suppose que $x > 1$.

(i) Montrer que b est non nul et que $|a| \geqslant m$.

(ii) Prouver que $a, b \in \mathbb{N}^*$, puis que $x \geqslant \omega$.

d) Montrer que U est l'ensemble des $\pm\omega^n$, avec $n \in \mathbb{Z}$.

Exercice 1.5. Soient n un entier au moins égal à 2 et K un corps commutatif ; on note A l'anneau produit K^n.

a) Montrer que A n'est pas un corps.

b) Si $1 \leqslant i \leqslant n$, on note $p_i \colon A \to K$ l'homomorphisme d'anneaux associant à $(x_1, \ldots, x_n)$ l'élément x_i. Montrer que $\ker p_i$ est un idéal maximal de A.

c) Déterminer tous les idéaux maximaux de A.

Exercice 1.6. On désigne par k un corps commutatif. Montrer que les conditions suivantes sont équivalentes.

a) Il existe $\alpha, \beta, \gamma \in k$, non tous nuls, et tels que $\alpha^2 + \beta^2 + \gamma^2 = 0$.

b) Il existe des matrices $A, B \in \mathrm{SL}_2(k)$ telles que $ABA^{-1}B^{-1} = -I_2$.

Exercice 1.7. Soit A un anneau commutatif non nul.

a) Soit $\mathfrak{p}$ un idéal premier de A, et soient $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ des idéaux de A tels que $\mathfrak{a}_1 \cdots \mathfrak{a}_n \subset \mathfrak{p}$. Prouver qu'il existe au moins un indice i tel que $\mathfrak{a}_i \subset \mathfrak{p}$.

b) Soit $\mathfrak{a}$ un idéal non premier de A tel que $\mathfrak{a} \neq A$. Montrer qu'il existe des idéaux $\mathfrak{a}_1$ et $\mathfrak{a}_2$ vérifiant $\mathfrak{a}_1\mathfrak{a}_2 \subset \mathfrak{a}$ et contenant strictement $\mathfrak{a}$.

c) Soit $\mathfrak{a}$ un idéal de A, et soient $\mathfrak{p}_1, \ldots \mathfrak{p}_n$ des idéaux premiers de A tels que $\mathfrak{a} \subset \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$. Prouver qu'il existe un indice i tel que $\mathfrak{a} \subset \mathfrak{p}_i$.

Exercice 1.8. Soit X un espace topologique compact, et soit A l'anneau des applications continues de X dans $\mathbb{R}$. Si $f \in A$ et si I est un idéal de A, on pose

$$Z(f) = \{x \in X \,;\, f(x) = 0\}\,, \quad \text{et} \quad Z_I = \bigcap_{g \in I} Z(g).$$

a) Soit I un idéal de A, et soit $g \in I$ vérifiant $g(x) \neq 0$ pour tout $x \in X$. Montrer que $I = A$.

b) Si $a \in X$, on note $I_a = \{f \in A \,;\, f(a) = 0\}$. Montrer que I_a est un idéal maximal de A.

c) Soit I un idéal de A tel que $Z_I = \emptyset$. Montrer qu'il existe des éléments $f_1, \ldots, f_n$ de I tels que $Z(f_1) \cap \cdots \cap Z(f_n) = \emptyset$. En déduire que $I = A$.

d) Soit I un idéal maximal de A. Prouver qu'il existe $a \in X$ tel que $I = I_a$.

Exercice 1.9. Soit K un corps non nécessairement commutatif, et soit K^* l'ensemble $K \setminus \{0\}$. Montrer que les groupes $(K, +)$ et $(K^*, \times)$ ne sont pas isomorphes.

Exercice 1.10. Soit A un anneau, et soient $a, b \in A$. Montrer que $1 - ab$ est inversible si et seulement s'il en est de même de $1 - ba$.

Exercice 1.11. Soit K un corps commutatif, et soit G l'ensemble des éléments non nuls de K de la forme $a^2 + b^2$, avec $a, b \in K$. Montrer que G est un sous-groupe du groupe multiplicatif $K\backslash\{0\}$.

Exercice 1.12. Soit A un anneau non nul (non nécessairement commutatif).

a) Montrer que les conditions suivantes sont équivalentes.

(i) A est un corps.

(ii) Les seuls idéaux à gauche de A sont $\{0\}$ et A.

(iii) Les seuls idéaux à droite de A sont $\{0\}$ et A.

b) Si les seuls idéaux bilatères de A sont $\{0\}$ et A, l'anneau A est-il nécessairement un corps ?

Exercice 1.13. a) On désigne par E l'unité de $\mathrm{M}_2(\mathbb{C})$. Pour $\alpha, \beta \in \mathbb{C}$, on pose

$$M(\alpha, \beta) = \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} \in \mathrm{M}_2(\mathbb{C}).$$

Soit $\mathbb{H} = \{M(\alpha, \beta)\,;\ \alpha, \beta \in \mathbb{C}\}$. Vérifier que $\mathbb{H}$ est un sous-corps non commutatif de $\mathrm{M}_2(\mathbb{C})$. Prouver que $\mathbb{R}E$ est le centre de $\mathbb{H}$ et que si

$$I = M(i, 0)\,,\quad J = M(0, i)\,,\quad K = M(0, 1),$$

on a alors

$$I^2 = J^2 = K^2 = -E,$$

$$IJ = -JI = K\,,\quad JK = -KJ = I\,,\quad KI = -IK = J.$$

Prouver que (E, I, J, K) est une base du $\mathbb{R}$-espace vectoriel $\mathbb{H}$.

b) On note $\mathbb{H}_8$ le sous-groupe multiplicatif de $\mathbb{H}\backslash\{0\}$ engendré par I, J, K. Décrire $\mathbb{H}_8$. Donner la liste de tous les sous-groupes de $\mathbb{H}_8$, et prouver que tout sous-groupe de $\mathbb{H}_8$ est distingué dans $\mathbb{H}_8$.

Exercice 1.14. Donner un exemple d'un anneau commutatif A dont la caractéristique est un nombre premier, mais qui n'est pas intègre.

Exercice 1.15. Soit A un anneau. On suppose que $x^3 = x$ pour tout $x \in A$. On veut prouver que A est commutatif.

a) Montrer que $6A = \{0\}$ et que $2A$ et $3A$ sont des idéaux bilatères de A tels que $2A + 3A = A$ et $2A \cap 3A = \{0\}$. On déduire qu'il suffit d'étudier les cas où $2A = \{0\}$ et $3A = \{0\}$.

b) On suppose $2A=\{0\}$. Calculer $(1+x)^3$ pour $x\in A$. En déduire que $x^2=x$, puis que A est commutatif.

c) On suppose $3A = \{0\}$. Si $x, y \in A$, calculer $(x + y)^2$ et $(x - y)^2$, et montrer que $x^2y + xyx + yx^2 = 0$. Prouver que A est commutatif.

Exercice 1.16. On munit $\mathbb{Z}^n$, $n \in \mathbb{N}^*$, de sa structure usuelle d'anneau produit. Déterminer tous les homomorphismes d'anneaux de $\mathbb{Z}^n$ dans $\mathbb{Z}$.

Exercice 1.17. Soient K un corps commutatif et E un ensemble non vide. On désigne par A l'anneau des applications de E dans K. Montrer que les idéaux maximaux de A sont les parties de A de la forme $\{f \in A\,;\, f(x) = 0\}$, où x est un élément de E.

Exercice 1.18. Soit A un pseudo-anneau commutatif non nul. On suppose l'existence d'un unique $\varepsilon \in A$ tel que $a+\varepsilon-a\varepsilon \neq 0$ pour tout $a \in A$. Prouver que A est un corps.

Exercice 1.19. Soit A un pseudo-anneau commutatif non nul et sans diviseur de zéro. On note A^* pour $A\setminus\{0\}$, et l'on suppose qu'il existe une application $a \mapsto s_a$ de A^* dans le groupe symétrique de A^* possédant les propriétés suivantes.

a) L'application $a \mapsto s_a$ est injective.

b) $s_a \circ s_b = s_{ab}$ pour tous $a, b \in A^*$.

c) $s_a(b) = s_b(a)$ pour tous $a, b \in A^*$.

Prouver que A est un corps.

Exercice 1.20. Soit k un corps commutatif, et soient $a_1, \ldots, a_n$ des éléments deux à deux distincts de k. On suppose qu'il existe $\lambda_1, \ldots, \lambda_n \in k$ tels que

$$\lambda_1 a_1^r + \cdots + \lambda_n a_n^r = 0,$$

pour tout $r \in \mathbb{N}$. Prouver que les λ_i sont tous nuls.

Exercice 1.21. Soit k un corps (non nécessairement commutatif), et soit ε son élément unité.

a) On suppose que $x^{-1} = -x$ pour tout $x \in k\setminus\{0\}$.

Si k est commutatif, montrer que k est isomorphe à $\mathbb{F}_2$ (utiliser le polynôme $X^2 + 1$).

On ne suppose plus que k est commutatif. Calculer $\varepsilon + \varepsilon$. En étudiant l'application $k \to k$, $x \mapsto (x + \varepsilon)^2$, montrer que k est isomorphe à $\mathbb{F}_2$.

Dans la suite de l'exercice, on suppose $x^{-1} = -x$ pour tout $x \in k\setminus\{-\varepsilon, 0, \varepsilon\}$ et $\varepsilon + \varepsilon \neq 0$.

b) Calculer $(\varepsilon + \varepsilon)^2$. En déduire que $\mathrm{car}(k) \in \{3, 5\}$.

c) Déterminer k.

Exercice 1.22. Soit A un anneau tel que $(xy)^2 = x^2y^2$ pour tous $x, y \in A$.

a) Soient $a, b \in A$. En calculant $[(a+1)b]^2$, montrer que $ab^2 = bab$.

b) Prouver que A est commutatif.

Exercice 1.23. L'ensemble A des suites stationnaires d'entiers est muni de sa structure naturelle d'anneau commutatif. Déterminer tous les hommomorphismes d'anneaux de A dans $\mathbb{Z}$.

Exercice 1.24. Soient K, L des sous-corps d'un corps M. Montrer que si la réunion $K \cup L$ est un sous-corps de M, on a ou bien $K \subset L$, ou bien $L \subset K$.

Exercice 1.25. Pour $n \in \mathbb{N}^*$, $\mathbb{Z}_n$ désigne l'anneau $\mathbb{Z}/n\mathbb{Z}$.

a) Quels sont, si $n \in \mathbb{N}^*$, les sous-anneaux de $\mathbb{Z}_n$.

b) Si $m, n \in \mathbb{N}^*$, déterminer les homomorphismes d'anneaux $\mathbb{Z}_m \to \mathbb{Z}_n$.

Exercice 1.26. Soit A un anneau. Pour toute partie non vide P de A, on note $\mathcal{D}(P)$ l'ensemble des $x - y$, avec $x, y \in P$. On désigne par S, T des parties non vides de A telles que $A = S \cup T$.

a) Prouver que l'on a ou $T \subset \mathcal{D}(S)$ ou $S \subset \mathcal{D}(T)$.

On suppose $S \cap T = \emptyset$. Montrer que $A = \mathcal{D}(T)$ ou que $A = \mathcal{D}(T)$.

Chapitre 2

Polynômes

Les polynômes vont tenir un rôle central dans toute la suite de ce livre. On rappelle ici des résultats concernant les polynômes à une indéterminée. On va surtout s'intéresser aux polynômes à coefficients dans un corps ; il sera donc question d'anneaux principaux. Pour ce qui concerne les polynômes à coefficients dans un anneau, donc la factorialité, le lecteur pourra se reporter à [18].

Dans ce chapitre, *les anneaux considérés sont supposés commutatifs*. On désigne par A un anneau et par K un corps.

2.1. Notations

2.1.1. Soit $(X_i)_{i\in I}$ une famille d'indéterminées sur A. On note $A[(X_i)_{i\in I}]$ l'anneau des polynômes aux indéterminées X_i, $i \in I$, et à coefficients dans A. Si $I = \{1, \dots, n\}$ est fini, on écrit $A[X_1, \dots, X_n]$ pour $A[(X_i)_{i\in I}]$.

Si $(X_i)_{i\in I}$ est une famille d'indéterminées sur K, on note $K((X_i)_{i\in I})$ le corps des fractions rationnelles aux indéterminées X_i, $i \in I$, et à coefficients dans K ; c'est le corps des fractions de $K[(X_i)_{i\in I}]$. Si $I = \{1, \dots, n\}$ est fini, on écrit $K(X_1, \dots, X_n)$ pour $K((X_i)_{i\in I})$.

2.1.2. On va s'intéresser, dans ce chapitre, aux polynômes à une indéterminée. On rappelle que $A[X]$ est un A-module libre, dont une base privilégiée est $(X^n\,;\, n \in \mathbb{N})$. Un élément P de $A[X]$ sera écrit sous l'une ou l'autre des formes

$$P = \sum_{n\in\mathbb{N}} a_n X^n = \sum_{n\geqslant 0} a_n X^n = \sum a_n X^n,$$

étant entendu que $(a_n)_{n\in\mathbb{N}}$ est une famille presque nulle d'éléments de A. On dit alors que les a_n, $n \in \mathbb{N}$, sont les *coefficients* de P.

Un polynôme de la forme λX^k, où $\lambda \in A$ et $k \in \mathbb{N}$, est appelé un *monôme*.

2.1.3. Soit B un anneau, et soit $f\colon A \to B$ un homomorphisme d'anneaux. L'application

$$\widetilde{f}\colon A[X] \to B[X]\,, \quad \sum_{n\geqslant 0} a_n X^n \mapsto \sum_{n\geqslant 0} f(a_n)X^n$$

est un homomorphisme d'anneaux prolongeant f. Il est évident que $\widetilde{f}$ est injectif (resp. surjectif, bijectif) si et seulement si f l'est. En particulier, si A est un sous-anneau de B, $A[X]$ s'identifie à un sous-anneau de $B[X]$.

2.2. Degré

2.2.1. Adjoignant à $\mathbb{N}$ un élément noté $-\infty$, on prolonge l'ordre et l'addition de $\mathbb{N}$ à $\mathbb{N} \cup \{-\infty\}$, par les conventions suivantes, où $n \in \mathbb{N}$:

$$-\infty < n \quad \text{et} \quad (-\infty) + n = n + (-\infty) = (-\infty) + (-\infty) = -\infty.$$

2.2.2. Définition. Soit $P = \sum a_n X^n \in A[X]$. Le *degré* de P, noté $\deg(P)$, est défini comme suit.

(i) Si $P = 0$, $\deg(P) = -\infty$.

(ii) Si $P \neq 0$, $\deg(P) = \max\{n \in \mathbb{N}\,;\, a_n \neq 0\}$.

2.2.3. Si $P \in A[X] \setminus \{0\}$ admet pour degré n, son coefficient d'indice n est appelé son coefficient *dominant*. S'il est égal à 1, P est dit *unitaire*. Si $P = \sum a_n X^n$, on dit que $a_r X^r$ est le *terme de degré* r de P.

Dans la suite, pour $n \in \mathbb{N}$, on note :

$$A_n[X] = \{P \in A[X]\,;\, \deg(P) \leqslant n\}.$$

Le A-module $A_n[X]$ est un libre puisque $(X^k\,;\, 0 \leqslant k \leqslant n)$ est évidemment une base de ce module.

2.2.4. Proposition. *Soient* $P, Q \in A[X]$.

(i) *On a :*

$$\deg(P+Q) \leqslant \max\{\deg(P), \deg(Q)\}\,, \quad \deg(PQ) \leqslant \deg(P) + \deg(Q).$$

De plus, si $\deg(P) \neq \deg(Q)$*, alors* $\deg(P+Q) = \max\{\deg(P), \deg(Q)\}$.

(ii) *Supposons* $P \neq 0$*, de coefficient dominant* régulier *dans* A*. Alors, si l'on suppose* $Q \neq 0$*, on a alors* $PQ \neq 0$ *et* $\deg(PQ) = \deg(P) + \deg(Q)$.

Démonstration. L'assertion (i) est immédiate. Prouvons (ii).

Soient αX^p et βX^q les monômes de plus hauts degrés de P et Q. Le terme de degré $p+q$ de PQ étant $\alpha\beta X^{p+q}$, on a obtenu le résultat, car $\alpha\beta \neq 0$. □

2.2.5. Théorème. *Les conditions suivantes sont équivalentes.*

(i) *L'anneau A est intègre.*

(ii) *L'anneau $A[X]$ est intègre.*

Démonstration. L'implication (i) $\Rightarrow$ (ii) résulte de 2.2.4, (ii), et (ii) $\Rightarrow$ (i) est claire puisque A s'identifie à un sous-anneau de $A[X]$. □

2.2.6. Corollaire. *On suppose que A est intègre.*

(i) *Si P, $Q \in A[X]$, on a* $\deg(PQ) = \deg(P) + \deg(Q)$.

(ii) *L'ensemble des éléments inversibles de $A[X]$ est égal à l'ensemble des éléments inversibles de A.*

Démonstration. Le point (i) résulte de 2.2.4, (ii).

Prouvons (ii). Si $PQ = 1$, on a alors $\deg(P) = \deg(Q) = 0$ d'après (i), et donc P, $Q \in A$. Le résultat est alors clair. □

2.2.7. Corollaire. (i) *On suppose A intègre. Si $(P_i)_{i\in I}$ est une famille de polynômes non nuls de $A[X]$ tels que* $\deg(P_i) \neq \deg(P_j)$ *pour $i \neq j$, elle est libre.*

(ii) *Soit $(P_n)_{n\in\mathbb{N}}$ une suite de polynômes de $K[X]$ vérifiant* $\deg(P_n) = n$ *pour tout n. Alors, si $d \in \mathbb{N}$, $(P_0, P_1, \ldots, P_d)$ est une base de $K_d[X]$ et la famille $(P_n)_{n\geqslant 0}$ est une base de $K[X]$.*

Démonstration. (i) Soient $i_1, \ldots, i_q \in I$ et $\lambda_1, \ldots, \lambda_q \in A \setminus \{0\}$. Puisque A est intègre, on a $\deg(\lambda_j P_{i_j}) = \deg(P_{i_j})$. D'après 2.2.4, (i), on obtient :

$$\deg(\lambda_1 P_{i_1} + \cdots + \lambda_q P_{i_q}) = \max\{\deg(P_{i_j})\,;\, 1 \leqslant j \leqslant q\} \neq -\infty.$$

D'où l'assertion.

(ii) On a $\dim K_d[X] = d + 1$ et, d'après (i), $(P_0, \ldots, P_d)$ est un système libre, donc une base de $K_d[X]$. La seconde assertion est alors claire. □

2.3. Valuation

2.3.1. Adjoignant à $\mathbb{N}$ un élément noté $+\infty$, on prolonge l'ordre et l'addition de $\mathbb{N}$ à $\mathbb{N} \cup \{+\infty\}$, par les conventions suivantes, où $n \in \mathbb{N}$:

$$n < +\infty \quad \text{et} \quad (+\infty) + n = n + (+\infty) = (+\infty) + (+\infty) = +\infty.$$

2.3.2. Définition. Soit $P = \sum a_n X^n \in A[X]$. La *valuation* du polynôme P, notée $\mathrm{val}(P)$, est définie de la manière suivante.

(i) Si $P = 0$, alors $\mathrm{val}(P) = +\infty$.

(ii) Si $P \neq 0$, alors $\mathrm{val}(P) = \min\{n \in \mathbb{N}\,;\, a_n \neq 0\}$.

Remarque. Si $P \in A[X]$ est *non nul*, alors $\mathrm{val}(P) \leqslant \deg(P)$. Par ailleurs, dire que $\mathrm{val}(P) = \deg(P)$ signifie que P est un monôme.

2.3.3. Le résultat suivant se prouve comme en 2.2.4 et 2.2.7, (i).

Proposition. *Soient* $P, Q \in A[X]$.

(i) *On a :*

$$\mathrm{val}(P+Q) \geqslant \min\{\mathrm{val}(P), \mathrm{val}(Q)\} \quad \text{et} \quad \mathrm{val}(PQ) \geqslant \mathrm{val}(P) + \mathrm{val}(Q).$$

De plus, $\mathrm{val}(P+Q) = \min\{\mathrm{val}(P), \mathrm{val}(Q)\}$ *si* $\mathrm{val}(P) \neq \mathrm{val}(Q)$.

(ii) *Si A est intègre, alors* $\mathrm{val}(PQ) = \mathrm{val}(P) + \mathrm{val}(Q)$.

(iii) *Supposons A intègre. Soit $\mathcal{F} = (P_i)_{i \in I}$ une famille d'éléments non nuls de $A[X]$ tels que* $\mathrm{val}(P_i) \neq \mathrm{val}(P_i)$ *si $i \neq j$. Alors, la famille $\mathcal{F}$ est libre.*

Remarque. L'analogue de 2.2.7, (ii) pour les valuations est inexact. Par exemple, soit $P_n = X^n - X^{n+1} \in K[X]$, et soit E le K-sous-espace vectoriel de $K[X]$ engendré par les P_n et φ la forme linéaire sur $K[X]$ définie par $\varphi(X^n) = 1$. La restriction $\varphi|E$ est nulle. Par suite, $E \subset \ker \varphi \neq K[X]$. Ainsi, $(P_n)_n$ n'est pas une base de $K[X]$.

2.4. Divisions

2.4.1. Théorème. *Soit $V \in A[X] \setminus \{0\}$, de degré m et ayant son coefficient dominant* inversible *dans L'anneau A. Pour tout polynôme $U \in A[X]$, il existe $Q, R \in A[X]$ tels que*

$$U = VQ + R\,, \quad \deg(R) < m.$$

De plus, Q et R sont uniquement déterminés par ces conditions. On dit que Q est le quotient *et R le* reste *de la* division euclidienne *de U par V.*

Démonstration. Supposons que l'on ait $U = VQ+R = VS+T$, $\deg(R) < m$ et $\deg(T)\} < m$.

Comme $V(Q-S) = T-R$ et que le coefficient dominant de V est inversible, il vient (2.2.4) :

$$\deg(V) + \deg(Q-S) = \deg(T-R) < \deg(V).$$

Par conséquent, $\deg(Q-S) = -\infty$. D'où, $S = Q$, puis $T = R$.

Prouvons l'existence d'une solution en raisonnant par récurrence sur le degré p de U. Si $p < m$, le couple $(Q, R) = (0, U)$ convient. Si $p \geqslant m$, notons :

$$U = a_p X^p + \cdots + a_0\,, \quad V = b_m X^m + \cdots + b_0\,, \quad W = U - a_p b_m^{-1} V X^{p-m}.$$

Comme $\deg(W) < p$, il résulte de l'hypothèse de récurrence qu'il existe des polynômes $S, R \in A[X]$ tels que $W = VS + R$ et $\deg(R) < m$. On en déduit le résultat, car on a $U = V(a_p b_m^{-1} X^{p-m} + S) + R$. □

2.4.2. Si $U, V \in A[X]$, on dit que V *divise* U, ou que V est un *diviseur* de U, ou que U est un *multiple* de V, s'il existe $W \in A[X]$ tel que $U = VW$.

Si V est non nul et a son coefficient dominant inversible dans A, dire que V divise U signifie que le reste de la division euclidienne de U par V est nul.

2.4.3. Théorème. *Soient* $U, V \in A[X]$ *:*

$$U = a_0 + a_1 X + \cdots + a_p X^p\,, \quad V = b_0 + b_1 X + \cdots + b_m X^m.$$

Supposons b_0 *inversible dans* A*. Pour tout* $n \in \mathbb{N}$*, Il existe* $Q, R \in A[X]$ *tels que :*

$$U = VQ + X^{n+1} R\,, \quad \deg(Q) \leqslant n.$$

De plus, Q *et* R *sont uniquement déterminés par ces conditions. On dit que* Q *est le* quotient *et* R *le* reste *de la* division suivant les puissances croissantes de U par V à l'ordre n.

Démonstration. Supposons $U = VQ + X^{n+1}R = VS + X^{n+1}T$, avec $\deg(Q) \leqslant n$ et $\deg(S) \leqslant n$. D'après les hypothèses, on obtient

$$\operatorname{val}(Q - S) = \operatorname{val}(V) + \operatorname{val}(Q - S) = n + 1 + \operatorname{val}(T - R),$$

donc $\operatorname{val}(Q - S) \geqslant n + 1$. Puisque $\deg(Q - S) \leqslant n$, on a $S = Q$, puis $T = R$.

Prouvons l'existence d'une solution. Posons $m = \operatorname{val}(U)$. Si $m \geqslant n + 1$, on peut écrire $U = X^{n+1}R$; le couple $(0, R)$ convient. Supposons $U \neq 0$ et le résultat établi pour $m > p$, avec $p \leqslant n$. On termine alors comme en 2.4.1 en remarquant que l'on a $\operatorname{val}(U - a_m b_0^{-1} V X^m) > p + 1$. □

2.4.4. Supposons que A soit un sous-anneau d'un anneau B. Soient U, V dans $A[X]$, le coefficient dominant de V étant inversible dans A. On peut considérer U et V comme des éléments de $B[X]$ (2.1.3). Compte tenu des définitions, la division euclidienne de U par V est la même dans $A[X]$ et dans $B[X]$. On a le même résultat en ce qui concerne la division suivant les puissances croissantes.

2.5. Propriétés arithmétiques

2.5.1. On rappelle qu'un anneau A est dit *principal* s'il est intègre et si tout idéal de A est de la forme Aa, avec $a \in A$.