Introduction à l'algèbre commutative

Cédric Lecouvey

Université François Rabelais Master I

Chapitre 1

Proprietés arithmétique des anneaux

1.1 Un peu d'histoire

Comme l'indique son éthymologie ($\alpha\rho\iota\tau\mu o\varsigma$ signifiant nombre en grec), l'arithmétique est la science des nombres et son origine remonte au moins à l'antiquité grecque. Elle s'est longtemps développée autour des différentes tentatives pour résoudre certaines équations diophantiennes. Rappelons qu'il s'agit d'équations algébriques à une ou plusieurs inconnues dont on cherche à déterminer les éventuelles solutions entières ou au contraire à établir l'absence de solution. Le début de leur étude systématique remonte au moins à Diophante (aux alentours du III-ième sciècle de notre ère). La plus connue est sans doute l'équation

$$x^n + y^n = z^n \tag{1.1}$$

où $n \geq 2$ est un entier et $x, y, z \in \mathbb{Z}$. L'existence d'une infinité de solutions à l'équation $x^2 + y^2 = z^2$ est généralement attribuée à l'école de Pythagore (vers 570 avant notre ère) bienqu'il semble que sa résolution ait déjà été connue par les Babyloniens 1000 auparavant. Les solutions sont les triplets Pythagoriciens

$$(x, y, z) = (r^2 - s^2, 2rs, r^2 + s^2)$$

où r, s sont des entiers positifs, premiers entre eux et de parité opposée.

Les notions de *corps et d'anneaux* sont quant à elles beaucoup plus récentes. Elles émergent progressivement de l'étude des équations algébriques et de la recherche d'une démonstration du grand théorème de Fermat infirmant l'existence d'un triplet d'entiers non nuls solution à l'équation (1.1) dès lors que $n \geq 3$. Les anneaux sont alors essentiellement vus comme des ensembles de nombres généralisant les nombres entiers. En 1753, Leonhard Euler $(1707 - 1783)$ pense avoir trouvé une preuve du grand théorème de Fermat pour $n = 3$. Elle se fonde sur l'utilisation de l'anneau $\mathbb{Z}[i\sqrt{3}]$des nombres de la forme $a + bi\sqrt{3}$ où a et b sont des entiers relatifs et i l'unité imaginaire. Sa preuve s'avère fausse car, contrairement à ce que croit Euler, un tel anneau n'est pas *factoriel* c'est à dire que le *théorème fondamental de l'artithmétique* (tout nombre se décompose de façon unique en un produit de nombres premiers) n'y est plus vérifié. Ainsi

$$4 = 2 \times 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$$

admet deux telles décompositions. Néanmoins, l'idée d'utiliser des généralisations des nombres entiers s'avère très fructueuse. Carl Friedrich Gauss $(1777 - 1855)$ étudie les nombres de la forme

$a + ib$ où a et b sont dans $\mathbb{Z}$ ce qui lui permet notamment de fournir des preuves élégantes du théorème des deux carrés de Fermat caractérisant les nombres entiers se décomposant comme la somme de deux carrés d'entiers. L'ensemble $\mathbb{Z}[i]$ de ces nombres est maintenant dénommé ensemble des entiers de Gauss. Ferdinand Eisenstein $(1823 - 1852)$ analyse l'anneau des entiers $\mathbb{Z}[j]$ de la forme $a + bj$ où $j = \exp(\frac{2i\pi}{3})$ portant désormais son nom ce qui lui permet de donner une preuve rigoureuse du grand théorème de Fermat pour $n = 3$ très analogue à celle (éronnée) proposée par Euler. La différence essentielle entre les anneaux $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$ d'une part, et $\mathbb{Z}[i\sqrt{3}]$ d'autre part est qu'il y existe un analogue de la division euclidienne des entiers seulement pour les deux premiers. Il semble que le mérite puisse être attribué à Gauss d'avoir le premier compris que l'existence d'une telle division suffisait à garantir la validité du théorème fondamental de l'arithmétique dans l'anneau considéré. De tels anneaux sont dit *euclidiens* et nous verrons qu'en effet, ils sont nécessairement factoriels.

La recherche d'une résolution générale du dernier théorème de Fermat amène l'étude d'autres anneaux d'entiers. Pour $n = 5$, Johann Peter Gustav Lejeune Dirichlet $(1805-1859)$ utilise l'anneau maintenant appelé anneau des entiers de Dirichlet formé des nombres $\mathbb{Z}[\Phi]$ de la forme $a + b\Phi$ où $\Phi = \frac{1+\sqrt{5}}{2}$ est le nombre d'or. Il comprend qu'une première obstruction va rendre la démonstration plus difficile. Cette obstruction réside dans le fait que, si l'anneau est bien euclidien, l'ensemble des éléments inversibles encore appelé groupe des unités devient infini. Pour ces éléments inversibles, aucun outil classique de la théorie des anneaux, comme la décomposition en facteurs premiers n'est possible. Il propose néanmoins une preuve du Théorème de Fermat pour $n = 5$ complétée quelques mois plus tard par Adrien-Marie Legendre $(1752 - 1833)$. Gabriel Lamé $(1795 - 1870)$ prouve bien, quatorze ans après Dirichlet, l'absence de solution pour $n = 7$ à l'aide d'un anneau d'entiers quadratiques mais sa preuve est très complexe et non généralisable.

Un progrès décisif est accompli par Ernst Kummer $(1810-1893)$ qui, en travaillant dans l'anneau des entiers $\mathbb{Z}[\xi_p]$ où p est un nombre premier impair et $\xi = \exp(\frac{2i\pi}{p})$ parvient à démontrer le théorème de Fermat pour tous les nombres premiers dits "réguliers". Il prouve que l'anneau $\mathbb{Z}[\xi_p]$ n'est en général pas factoriel mais son idée majeure consiste à raisonner non plus avec les éléments de $\mathbb{Z}[\xi_p]$ mais avec des sous ensembles de $\mathbb{Z}[\xi_p]$ qu'il dénomme "nombres idéaux". Cette idée est alors systématisée par Richard Dedekind $(1831 - 1916)$ à qui l'on doit la notion moderne d'*idéal* dans un anneau commutatif unitaire et le développement d'une arithmétique non plus sur les éléments d'un anneau de nombres algébriques mais sur les idéaux de cet anneau.

L'étude des anneaux commutatifs et notamment des anneaux de polynômes et de leurs idéaux se pousuit alors en lien avec le développement de la *géométrie algébrique* et notamment avec les travaux de Hilbert $(1862 - 1943)$. Elle donne naissance à toute une branche des mathématiques connue sous le nom *d'algèbre commutative* encore en plein développement de nos jours. Signalons que l'intérêt de la notion d'anneau ne se limite pas bien sûr aux seuls anneaux commutatifs. Il suffit pour s'en convaincre de garder en tête l'importance des anneaux et algèbres de matrices à la fois en mathématique mais aussi en physique.

L'objectif de ce chapitre est de présenter les définitions et propriétés basiques liée aux anneaux commutatifs. Nous n'étudierons en détail que les propriétés des anneaux factoriels et n'aborderons les définitions et propriétés des anneaux Noetheriens ou des anneaux de Dedekind que superficiellement. Le lecteur plus curieux pourra consulter les références en fin de texte. Dans la suite tous les anneaux considérés seront *unitaires et commutatifs*. Les définitions et notions de bases sur les groupes et les anneaux sont également supposées connues par le lecteur que nous renvoyons par exemple à [5] pour celles qui ne seraient pas rappelées.

1.2 Autour de la notion d'idéal

On se donne un *anneau* $A = A(+, \cdot, 0, 1)$ unitaire et commutatif (c'est à dire que la multiplication est commutative). On rappelle que l'addition est toujours commutative dans un anneau. On dit qu'un élément $a \in A$ est inversible dans A si il existe un élément $a' \in A$ telle que $aa' = 1 (= a'a)$. Il est facile de vérifier qu'un tel élément a' est nécessairement unique. On note alors $a' = a^{-1}$. L'ensemble $A^\times := \{a \in A, \text{ inversible}\}$ forme le groupe des éléments inversibles de A. Lorsque $A^\times = A \setminus \{0\}$, on dit que A est un *corps*.

Exemple 1.2.1
- *Pour* $\mathbb{Z}[i] := \{a + ib \mid (a, b) \in \mathbb{Z}^2\}$, $\mathbb{Z}[i]^\times = \{-1 - i, 1, i\}$.
- *Dans* $\mathbb{Z}/n\mathbb{Z}$ *les éléments inversibles sont les classes* $\overline{k}$ *telles que* k *soit premier avec* n.

Exercice 1.2.2
- *Détermier* $A^\times$ *pour* $\mathbb{Z}[i\sqrt{3}]$ *et* $\mathbb{Z}[\Phi]$.
- *Caractériser le groupe* $(\mathbb{Z}/n\mathbb{Z})^\times$ *pour* $n = 121\,000$.

Comme mentioné dans l'introduction, la notion d'*idéal* est centrale en algèbre commutative. Nous allons voir que la plupart des propriétés arithmétiques des anneaux peuvent s'exprimer comme des propriétés sur leurs idéaux. On dit que $I \subset A$ est un idéal si I est un sous-groupe de $(A, +)$ tel que $aI \subset I$ pour tout $a \in A$. Cela signifie que tous les produits de la forme ax avec $a \in A$ et $x \in I$ sont dans I. Pour tout $a \in A$, on note $\overline{a} := a + I$ la classe de a pour la relation d'équivalence $a \sim a'$ ssi $a - a' \in I$. La preuve du lemme suivant est laisée au lecteur

Lemme 1.2.3 *L'addition et la multiplication*

$$\overline{a} + \overline{b} = \overline{a + b} \text{ et } \overline{a}\overline{b} = \overline{ab}$$

sont bien définies dans $A/\sim$. *Elles confèrent à* $A/\sim$ *un structure d'anneau commutatif unitaire appelé quotient de* A *par* I *et noté* A/I.

La projection canonique $p : A \to A/I$ qui associe à tout $a \in A$ sa classe $\overline{a}$ est alors un morphisme surjectif d'anneaux tel que $\ker f = I$. Noter que les idéaux de l'anneau quotient A/I sont de la forme I/J où J est un idéal de A contenant I.

Plus généralement si $f : A \to B$ est un morphisme d'anneaux, alors $\ker f$ est un idéal et l'application

$$\overline{f} : \begin{cases} A/\ker f \to B \\ \overline{a} \longmapsto f(a) \end{cases}$$

est bien définie (vérifier que $f(a)$ ne dépend pas du représentant $a \in \overline{a}$ choisi !) et donne un morphisme d'anneau.

Exemple 1.2.4
- *Les idéaux de* $\mathbb{Z}$ *sont de la forme* $n\mathbb{Z}$ *où* n *est un entier. Ceci est du au fait que les sous-groupes additifs de* $\mathbb{Z}$ *sont eux-mêmes de la forme* $n\mathbb{Z}$ *ce qui se montre facilement en considérant le plus petit élément positif d'un tel sous-groupe* $G \neq \{0\}$ *à l'aide de la division euclidienne.*

– *Soit A un anneau fini et $f : \mathbb{Z} \to A$ le morphisme d'anneaux défini par $f(k) = \underbrace{1_A + \cdots + 1_A}_{k \text{ fois}}$.*
Comme A est fini, $\ker f = n\mathbb{Z}$ avec $n \neq 0$. L'anneau A contient un sous-anneau isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
– *Si $A = \mathbb{K}$ est un corps, les seuls idéaux de $\mathbb{K}$ sont $\mathbb{K}$ et $\{0\}$.*

Les propriétés ci-dessous sont laissées en exercice (à faire !). Soient I et J deux idéaux d'un anneau A. Alors

1. $I + J := \{x + y \mid x \in I \text{ et } y \in J\}$ est un idéal,
2. $I \cap J$ est un idéal (mais pas $I \cup J$ en général),
3. $IJ := \langle xy \mid x \in I, y \in J\rangle$ l'idéal engendré par les produits d'éléments de I et J est contenu dans $I \cap J$,
4. $\sqrt{I} := \{a \in A \mid \exists n \in \mathbb{N}, a^n \in I\}$ est un idéal,
5. l'idéal $(a) := aA$ engendré par a est égal à A ssi $a \in A^\times$.

On dit qu'un idéal I de l'anneau A est
– *principal* si il existe $a \in A$ tel que $I = (a)$ et dans ce cas, $(a) = A$ ssi $a \in A^\times$
– *maximal* si I est maximal pour la relation d'ordre sur les idéaux définie par l'inclusion (autrement dit $I \subset J$ avec J idéal implique que $J = I$ ou $J = A$),
– *premier* si pour toute paire (a, b) d'élements de A, on a $ab \in I$ ssi $a \in I$ ou $b \in I$,
– *de type fini* si il existe un nombre fini d'éléments $x_1, \ldots, x_n$ dans A tel que $I = \langle x_1, \ldots, x_n\rangle$ soit l'idéal engendré par $x_1, \ldots, x_n$ (cela généralise la notion d'idéal principal).

1.3 Divisibilité

Soient a et b deux éléments d'un anneau A. On dit que a divise b et on écrit $a \mid b$ si il existe $c \in A$ tel que $b = ac$. Cette propriété peut se réécrire en termes d'idéaux. On a en effet

$$a \mid b \Longleftrightarrow (b) \subset (a).$$

La relation de divisibilité n'a d'intérêt que si A n'est pas un corps. Dans le cas contraire, elle se réduit à $a \mid 0$ pour tout $a \in A$. La relation de divisibilité est un *préordre*, c'est à dire qu'elle est réflexive et transitive mais pas symétrique. Il est alors naturel d'introduire la relation d'équivalence aRb ssi $a \mid b$ et $b \mid a$. Cette relation peut se caractériser facilement lorsque A est un anneau *intègre*, c'est à dire sans diviseur de 0, i.e.

$$ab = 0 \Longrightarrow a = 0 \text{ ou } b = 0.$$

Lemme 1.3.1 *Si A est intègre, aRb ssi il existe $u \in A^\times$ tel que $a = ub$*

Preuve. Comme $a \mid b$ et $b \mid a$, il existe c et d tels que $b = ac$ et $a = db$. Cela donne $a = dca$ et donc $a(1 - dc) = 0$. Or $a \neq 0$ car $a \mid b$. Puisque A est intègre, on en déduit que $dc = 1$, donc $c \in A^\times$. ■

Deux éléments figurant dans la même classe d'équivalence pour la relation R sont dits *associés*. On note $\mathcal{I}_{pr}(A)$ l'ensemble des idéaux principaux de l'anneau **intègre** A. Soit $[a]$ la classe de $a \in A$

dans A/R. Dans A/R, la relation de divisibilité devient un ordre. On vérifie alors aisément que l'application

$$\begin{cases} A/R \to \mathcal{I}_{pr}(A) \\ [a] \longmapsto (a) \end{cases} \tag{1.2}$$

est une bijection de l'ensemble A/R ordonné par $|$ dans $\mathcal{I}_{pr}(A)$ ordonné par la relation d'inclusion. Cela signifie essentiellement qu'en identifiant les éléments qui diffèrent entre eux par multiplication d'un inversible, on peut traiter la divisibilité en termes d'inclusion d'idéaux principaux.

On dit qu'un élément $p \in A$ est *irréductible* ssi p n'est pas inversible et toute égalité $p = ab$ avec a, b dans A implique $a \in A^\times$ ou $b \in A^\times$. Ainsi les diviseurs de p sont exactement les élements de $[p]$. Noter que 0 n'est pas irréductible. Par ailleurs si A n'est pas un corps, p est irréductible équivaut à (p) est maximal dans $\mathcal{I}_{pr}(A) \setminus \{A\}$.

Deux éléments a et b de A sont dits premiers entre eux ssi pour tout $d \in A$, $d \mid a$ et $d \mid b$ implique que $d \in A^\times$. Autrement dit, les seuls diviseurs communs à a et b sont les inversibles.

Exemple 1.3.2

1. *Les éléments irréductibles de $\mathbb{Z}$ sont les nombres premiers.*
2. *Dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{2}$ n'est pas un élément irréductible puisque $\overline{2} = \overline{2} \times \overline{4}$ d'une part et que d'autre part, ni $\overline{2}$ ni $\overline{4}$ ne sont inversibles.*

Lemme 1.3.3 *On suppose que A est intègre. Soit $p \in A$ tel que (p) soit un idéal premier. Alors p est irréducible.*

La preuve de ce lemme est laissée en exercice.

Proposition 1.3.4 *Soit A un anneau et I un idéal.*

1. *A/I est un corps ssi I est maximal.*
2. *A/I est intègre ssi I est premier.*

En particulier un idéal maximal est premier.

Preuve. On sait que les idéaux de A/I sont les J/I tels que J soit un idéal de A contenant I. Dire que A/I est un corps revient à dire que ces seuls idéaux sont A et I puisqu'un idéal contenant un inversible est égal à l'anneau tout entier. Donc A/I est un corps ssi les seuls idéaaux J contenant I sont I et A, c'est à dire pour I maximal. L'assertion 2 découle immédiatement de la définition d'un anneau intègre. ■

1.4 Zoologie des anneaux

L' anneau A est dit
- *intègre* si il est sans diviseur de 0
- *noetherien* si tout idéal de A est de type fini
- *factoriel* si il est intègre et tout $a \in A$ non nul admet
  (E) : une décomposition sous la forme

$$a = up_1 \cdots p_r \tag{1.3}$$

  où $u \in A^\times$ et $p_1, \ldots, p_r$ sont des irréductibles
  (U) : la décomposition est unique au sens où $a = vq_1 \cdots q_r$ ssi il existe une permutation $\sigma \in S_r$ telle que p_i et $q_{\sigma(i)}$ soient associés.

– *principal* si il est intègre et si tout idéal de A est principal
– *euclidien* si A est intègre et si il est muni d'une application $v : A \setminus \{0\} \to \mathbb{N}$ telle que pour tout couple a, b dans $A \setminus \{0\}$, il existe q et r dans A vérifiant

$$a = bq + r \text{ et } \begin{cases} r = 0 \text{ ou} \\ v(r) < v(b) \end{cases} \tag{1.4}$$

La notion d'anneau factoriel offre une généralisation naturelle du théorème fondamental de l'arithmétique dans $\mathbb{Z}$. Malheureusement, comme Kummer l'a le premier compris, elle est encore trop restrictive pour permettre l'étude d'anneaux d'entiers aussi simples que $\mathbb{Z}[i\sqrt{3}]$ qui n'est pas factoriel puisque $4 = 2 \times 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ dans cet anneau. Pour étudier ce type d'anneaux non factoriels, il faut introduire une classe d'anneaux plus vaste : les *annneaux de Dedekind*. Nous renvoyons le lecteurs à [3] ou [6] pour leur définition et propriétés qui ne seront pas abordées dans la suite. Noter également la présence d'une condition d'existence et d'une condition d'unicité dans la définition des anneaux factoriels. Avant d'étudier les relations entre tous ces types d'anneaux dans le paragraphe suivant, nous allons en donner quelques propriétés.

Proposition 1.4.1 *Soit A un anneau. Les propriétés suivantes sont équivalentes :*

1. *A est noetherien (i.e. tout idéal de A est de type fini),*
2. *Toute suite croissante $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ d'idéaux de a est stationnaire, i.e. il existe un rang N tel que $I_n = I_N$ pour tout $n \geq N$.*
3. *Tout ensemble non vide d'idéaux de A a un élément maximal pour l'inclusion.*

Preuve. (1) $\Longrightarrow$ (2) : Comme la suite est croissante $I = \cup_{n \geq 1} I_n$ est un idéal de A. Comme A est noetherien, il existe $a_1, \ldots, a_k$ dans A tels que $I = \langle a_1, \ldots, a_k \rangle$. Il est alors clair que $I = I_N$ où N est le plus petit entier tel que $a_1, \ldots, a_k$ soient dans I_N.

(2) $\Longrightarrow$ (3) : On raisonne par l'absurde. Soit E un ensemble d'idéaux sans élément maximal et $I_1 \in E$. Comme E n'a pas d'élément maximal, il existe $I_2 \in E$ tel que $I_1 \subsetneq I_2$. Par récurrence, on construit une suite croissante d'idéaux qui n'est pas stationnaire.

(3) $\Longrightarrow$ (1) : Soit I un idéal de A et $E_I := \{$idéaux J de A contenus dans I et de type fini$\}$. Puisque $\{0\} \in E_I$, E_I est non vide. Soit J un élément maximal de E_J. Si $I \neq J$, il existe $a \in I$ tel que $a \notin J$. Alors l'idéal $J + (a)$ est de type fini, contenu dans I. Par ailleurs $J \subsetneq J + (a)$. On a donc $I = J$ et I est de type fini. ■

Proposition 1.4.2 *Supposons que A est intègre et Noetherien. Alors tout élément $a \in A$ non nul admet une décomposition sous la forme*

$$a = up_1 \cdots p_r \tag{1.5}$$

où $u \in A^\times$ et $p_1, \ldots, p_r$ sont des irréductibles.

Preuve. Considérons l'ensemble $F = \{$idéaux (a) principaux$|$ $a \neq 0$ et a n'est pas de la forme $a = up_1 \cdots p_r$. Noter que pour tout (a) dans F, a n'est ni inversible ni irréductible. Si A est non vide, il doit admettre un élément maximal (a) d'après la proposition précédente. Puisque a n'est pas irréductible, on peut l'écrire sous la forme $a = bc$ avec b, c non inversibles. On a donc $(a) \subsetneq (b)$ et $(a) \subsetneq (c)$. En effet si on a par exemple $(a) = (b)$, il existe $u \in A^\times$ tel que $a = ub$. Mais alors, $b(c - u) = 0$ et $c = u$ serait inversible. Comme (a) est maximal dans F, ni (b) ni (c) ne sont dans

F. On peut donc décomposer $b = up_1 \cdots p_s$ et $c = vq_1 \cdots q_t$ ce qui donne une contradiction car on a alors $a = uvp_1 \cdots p_s q_1 \cdots q_t$. L'ensemble A est donc vide. ■

Soit A un anneau intègre. On se donne un ensemble P des irréductibles dans A, c'est à dire que l'on fixe un représentant dans chaque classe $[p]$ où p est irréductible. Alors A est un anneau factoriel ssi chaque élément a non nul admet une décomposition unique sous la forme

$$a = u \prod_{p \in P} p^{v_p(a)}$$

où u inversible et les $v_p(a)$ son nuls sauf un nombre fini d'entre eux. L'entier $v_p(a)$ s'appelle la *valuation p-adique* de a. Il est alors clair que

$$a \mid b \Longleftrightarrow v_p(a) \leq v_p(b) \text{ pour tout } p \in P.$$

On dispose alors d'une notion naturelle de ppcm et de pgcd en posant

$$\text{ppcm}(a,b) = \prod_{p \in P} p^{\sup(v_p(a), v_p(b))} \text{ et } \text{pgcd}(a,b) = \prod_{p \in P} p^{\inf(v_p(a), v_p(b))}.$$

Noter que l'on a $(a) \cap (b) = (\text{ppcm}(a,b))$ mais seulement $(a) + (b) \subset (\text{pgcd}(a,b))$ en général si aucune autre hypothèse n'est faite sur l'anneau A.

Proposition 1.4.3 *Soit A un anneau intègre où chaque élément a non nul admet une décomposition $a = up_1 \cdots p_r$ du type (1.3). Les assertions suivantes sont équivalentes :*

1. *La décomposition est unique (au sens (U) ci-dessous),*
2. *Si p est irréductible et $p \mid ab$, alors $p \mid a$ ou $p \mid b$ (lemme d'Euclide).*
3. *L'élément p est irréductible ssi (p) est premier.*
4. *Si $a \mid bc$ et si a est premier avec b alors $b \mid c$.*

Preuve. (1) $\Longrightarrow$ (2) : l'assertion 1 signifie que A est factoriel. Dans ce cas $p \mid ab$ signifie que $v_p(ab) > 0$. Comme $v_p(ab) = v_p(a) + v_p(b)$, l'une des deux valuations $v_p(a)$ ou $v_p(b)$ doit être non nulle.

(2) $\Longrightarrow$ (1) : Si $a = up_1 \cdots p_r = vq_1 \cdots q_s$ avec u, v inversibles et $p_1, \ldots, p_r, q_1, \ldots, q_s$ irréductibles, chaque p_i divise l'un des q_j. Comme il s'agit d'irréductibles, cela montre que modulo les inversibles les ensembles $\{p_1, \ldots, p_r\}$ et $\{q_1, \ldots, q_s\}$ sont les mêmes, c'est à dire que la décomposition est unique.

(2) $\Longrightarrow$ (3) : d'après le Lemme 1.3.3, il suffit de montrer que (p) est premier. Soit donc a et b tels que $ab \in (p)$. Alors $p \mid ab$ donc $a \in (p)$ ou $b \in (p)$.

(3) $\Longrightarrow$ (2) : Si p est irréductible et divise ab, $ab \in (p)$. Puisque (p) est premier, on a $a \in (p)$ ou $b \in (p)$. Donc $p \mid a$ ou $p \mid b$.

(4) $\Longrightarrow$ (2) est immédiat.

(2) $\Longrightarrow$ (4) : Puisque 2 est vrai, les décompositions des éléments a, b, c sont uniques ce qui entraîne facilement (4) en considérant les valuations. ■

Exercice 1.4.4

1. *Montrer que le quotient d'un anneau noetherien est un anneau noetherien.*
2. *Montrer que l'anneau $A = \mathbb{Z}[i\sqrt{5}]$ est noetherien mais pas factoriel.*

1.5 Liens unissant les différents types d'anneaux

Proposition 1.5.1 *Soit A un anneau euclidien. Alors A est principal.*

Preuve. Soit I un idéal non réduit à $\{0\}$ de A et $a \in A$ non nul tels que $v(a) = \min_{\alpha \in A}\{v(\alpha)\}$. Considérons $\alpha \in I$. La division euclidienne de α par a implique l'existence de q, r dans A tels que $\alpha = aq + r$ et, $v(r) = 0$ ou $v(r) < v(a)$. Comme $r = \alpha - aq$, r est dans I. Par définition de a, on a donc $r = 0$. Cela montre que $I \subset (a)$. La réciproque étant évidente, $I = (a)$ est un anneau principal. ■

Proposition 1.5.2 *Soit A un anneau principal. Alors A est factoriel.*

Preuve. Tout d'abord, A étant en particulier noetherien, tout élément non nul dans A admet une décomposition du type (1.3) d'après la Proposition 1.4.2. Soit p irrédutible. Soit E_p l'ensemble des idéaux premiers contenant p. Puisque p est irréductible, cet ensemble ne contient que (p). Par ailleurs, d'après la Proposition 1.4.1, il contient un élément maximal. Donc (p) est maximal et en particulier il est premier. La proposition 1.4.3 permet alors de conclure que A est bien factoriel. ■

Noter que la preuve précédente montre que **dans un anneau principal** les équivalences ci-dessous sont vraies :

$$p \text{ irréductible} \iff (p) \text{ premier} \iff (p) \text{ maximal.}$$

Cela simplifie énormément les choses. Notamment, le théorème de Bezout est vérifié.

Corollaire 1.5.3 *Soit A un anneau principal. Considérons a, b deux éléments non nuls et $d = \text{pgcd}(a, b)$. Alors $(a) + (b) = (d)$. En particulier, $(a) + (b) = A$ si a et b sont premiers entre eux.*

Preuve. On a déjà vu que $(a) + (b) \subset (d)$ car $a \in (d)$ et $b \in (d)$. Par ailleurs, comme A est principal, il existe e tel que $(a) + (b) = (e)$. On a donc $(e) \subset (d)$ et donc $d \mid e$, $e \mid a$ et $e \mid b$. Par définition de $\text{pgcd}(a, b)$, cela impose que $e = d$. ■

Exemple 1.5.4 *L'anneau des entiers $\mathbb{Z}$ est euclidien relativement à $v = |\ \ |$ la valeur absolue.*

Exercice 1.5.5 *L'anneau $\mathbb{Z}[i]$ des entiers de Gauss est euclidien relativement à l'application v telle que $v(z) = a^2 + b^2$ pour tout $z = a + ib$. En particulier $\mathbb{Z}[i]$ est principal et factoriel. Noter que la paire (p, r) obtenus lors de la décomposition $a = bq + r$ n'est pas nécessairement unique.*

Il existe des anneaux principaux non euclidiens comme par exemple $\mathbb{Z}[\alpha]$ où $\alpha = \frac{1+i\sqrt{19}}{2}$ (voir [5] pour la preuve qui n'est pas immédiate). Comme mentionné dans l'introduction, les anneaux d'entiers quadratiques ou cyclotomiques ne sont même pas factoriels en général. La notion pertinente d'anneaux à considérer pour les étudier et celle d'anneaux de Dedekind. Nous ne poursuivrons pas dans cette voie. Nous verrons dans le chapitre suivant, qu'il existe une large classe d'anneaux euclidiens très naturels : les anneaux de polynômes $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps.

Chapitre 2

Anneaux de polynômes

2.1 Introduction

L'idée d'associer une lettre par exemple X à un ensemble de nombres date au moins des travaux de Diophante au III-ième siècle. A l'origine les nombres considérés sont des entiers ou des rationnels. Cette idée est généralisée aux nombres irrationnels par la civilisation arabe, à partir du VIII-ième siècle. Bienque la contruction soit encore rudimentaire, elle permet aux mathématiciens de la Renaissance de résoudre toutes les équations polynomiales jusqu'au degré 4. Au XVIIe siècle apparaît un premier formalisme, celui des fonctions. Le symbole X est vu comme une variable et le polynôme comme une fonction. Cette approche permet notamment à Gauss d'obtenir la première preuve complète du théorème de d'Alembert-Gauss montrant qu'un polynôme à coefficients complexe de degré n a exacatement n racines (éventuellement multiples) dans $\mathbb{C}$.

Une question de Vandermonde au XVIIIe siècle remet à l'honneur le concept de polynôme formel faisant usage d'une indéterminée X pouvant s'additionner et se multiplier, mais qui n'est pas vu comme une fonction. Il cherche sans succès à résoudre l'équation cyclotomique $X^n = 1$ à l'aide de radicaux, c'est-à-dire de nombres rationnels, de l'unité imaginaire i, des quatre opérations adjointes et des fonctions racines n-ièmes. C'est finalement Gauss qui y parvient en considérant les polynômes comme des équivalents de nombres entiers, avec une division euclidienne, l'équivalent des nombres premiers et une décomposition unique en facteurs premiers. En langage moderne, Gauss considère l'anneau des polynômes $\mathbb{C}[X]$. Ce n'est qu'au XX-ième siècle que la notion d'anneau de polynômes est dégagée de façon totalement rigoureuse.

Dans ce qui suit, on suppose connues les définitions et propriétés basiques sur les anneaux de polynômes (structure d'anneau, degré, racines etc.). En cas de doute, consulter [3].

2.2 Quelques définitions et propriétés élémentaires

Etant un A un anneau, on note $A[X]$ l'anneau des polynômes en l'indéterminée X à coefficients dans A. On note $d(P)$ le degré du polynôme $P \in A[X]$. Par convention $d(0) = -\infty$.

De façon plus générale si $X_1, \ldots, X_n$ est un ensemble d'indéterminées (supposées indépendantes), $A[X_1, \ldots, X_n]$ est l'anneau des polynômes sur A en les variables $X_1, \ldots, X_n$.

Exemple 2.2.1 *$P(X, Y) = X^2Y + XY + Y^2$ peut être vu comme un élément de $\mathbb{Z}/2\mathbb{Z}[X, Y]$.*

Proposition 2.2.2 (division euclidienne) *Soit P non nul dans $A[X]$ de **coefficient dominant inversible**. Alors pour tout $F \in A[X]$, il existe $Q, R \in A[X]$ tels que $F = PQ + R$ et $d(R) < d(Q)$.*

Preuve. On peut supposer que P est unitaire (i.e son coefficient dominant vaut 1). Posons $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Soit $B := A/(P)$ et x l'image de X par la projection canonique. Il suffit de montrer que tout élément de B est combinaison linéaire à coefficients dans A de $1, x, \ldots, x^{n-1}$. En fait, il suffit même de le faire pour tous les monômes $x^i, i \geq 0$. Cela découle immédiatement par récurrence de la relation $x^n = -(a_{n-1}X^{n-1} + \cdots + a_0)$ vraie dans B. ■

Puisque tous les éléments non nuls d'un corps sont inversibles, on obtient le corollaire fondamental suivant.

Corollaire 2.2.3 *Si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est euclidien relativement au degré des polynômes, donc en particulier principal et factoriel.*

Supposons que A soit **factoriel**. Soit $P(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X]$. On note $c(P)$ le *contenu* de P défini par $c(P) := \text{pgcd}(a_n, \ldots, a_0)$. On dit que P est *primitif* lorsque $c(P) = 1$.

Lemme 2.2.4 (dit lemme de Gauss) *Soit P, Q dans $A[X]$ avec A factoriel. Alors $c(PQ) = c(P)C(Q)$ (modulo $A^\times$).*

Preuve. Supposons tout d'abord $c(P) = c(Q) = 1$. Posons $P(X) = a_nX^n + \cdots + a_0$, $Q(X) = b_mX^m + \cdots + b_0$ et $PQ(X) = v_{n+m}X^{n+m} + \cdots + v_0$. Supposons tout d'abord que $c(PQ) \neq 1$. Alors, comme A est factoriel, il existe p irréductible tels que $p \mid c(PQ)$. Puisque $c(P) = c(Q) = 1$ il existe i_0 tel que $p \mid a_i$ pour $i < i_0, p \not| a_{i_0}$ et j_0 tel que $p \mid b_j$ pour $j < j_0, p \not| b_{j_0}$. Alors

$$p \mid c_{i_0+j_0} = \sum_{i+j=i_0+j_0} a_ib_j = a_{i_0}b_{j_0} + \sum_{i+j=i_0+j_0,(i,j)\neq(i_0,j_0)} a_ib_j.$$

Dans la dernière somme on a $i < i_0$ ou $j < j_0$ ce qui implique que p divise cette somme. il s'ensuit que p divise $a_{i_0}b_{j_0}$ et donc, d'après le lemme d'Euclide (vrai dans les anneaux factoriels), $p \mid a_{i_0}$ ou $p \mid b_{i_0}$. Ce qui mène à une contradiction.

Dans le cas général, on pose $d = c(P)$, $e = c(Q)$, $P' = P/d$ et $Q' = Q/e$. Ainsi $c(P') = c(Q') = 1$ donc d'après ce qui précède $c(P'Q') = 1$. Or $PQ = deP'Q'$. Donc $c(PQ) = dec(P'Q') = de$ comme souhaité. ■

2.3 Propriétés de transfert

Le but de se paragraphe est d'étudier dans quelle mesure l'anneau $A[X]$ hérite des propriétés de l'anneau A. Tout d'abord, il est clair que si A est intègre, il en est de même pour $A[X]$. Ce n'est plus le cas en général si A est principal.

Proposition 2.3.1 *L'anneau $A[X]$ est principal ssi $A = \mathbb{K}$ est un corps (cas où il est donc euclidien).*

Preuve. Si $A = \mathbb{K}$, $A[X]$ est euclidien donc principal. Si $A[X]$ est principal, il est intègre donc A est intègre. Cela implique que X est irréductible dans $A[X]$. En effet, si $X = PQ$, on doit avoir $d(P) + d(Q) = 1$. Donc l'un des deux polynômes est de degré 1 et l'autre de degré 0. On peut supposer $P(X) = aX + b$ et $Q(X) = c$. Comme A est intègre, on doit avoir $a = 0$ et $bc = 1$ ce qui montre que X est irréductible. Or, dans un anneau principal, X irréductible implique que (X) est maximal. Il s'ensuit que $A[X]/(X) = A$ est un corps. ■

Théorème 2.3.2 *Soit A un anneau noetherien. Alors $A[X]$ est noetherien.*

Preuve. Soit I un idéal de $A[X]$. Pour tout $n \in \mathbb{N}$, soit $d_n(I)$ l'ensemble des coefficients dominants des éléments de degré n dans I augmenté de l'élément 0. Il est clair que $d_n(I)$ est un idéal. Il vérifie de plus les propriétés suivantes. Si $I \subset J$, $d_n(I) \subset d_n(J)$. Pour tout n, on obtient en multipliant par X, $d_n(I) \subset d_{n+1}(I)$. Si $I \subset J$, $I = J$ ssi $d_n(I) = d_n(J)$ pour tout $n \in \mathbb{N}$. En effet si $I \neq J$ et $d_n(J) = d_n(I)$ pour tout n, il existe P dans $J \setminus I$ de degré minimal k et Q dans I de degré k ayant les mêmes coefficients dominants. Alors $P - Q$ est non nul, dans $J \setminus I$ et de degré inférieur à k ce qui est contradictoire.

Soit $I_0 \subset \cdots \subset I_n$ une suite croissante d'ideaux dans $A[X]$. Comme A est noetherien, la famille des idéaux $d_k(I_n)$ avec $k, n \in \mathbb{N}$ admet un élément maximal $d_\ell(I_m)$. Pour $k \leq \ell$ la suite $d_k(I_n)$ est croissante par rapport à n donc il existe n_k tel que $d_k(I_n) = d_k(I_{n+1})$ pour $n \geq n_k$. *Soit* $N = \sup(m, n_0, \ldots, n_\ell)$. Nous allons montrer que $I_n = I_N$ pour tout $n \geq N$. Comme $I_N \subset I_n$ pour $n \geq N$, il suffit de montrer d'après ce qui précède que $d_k(I_n) = d_k(I_N)$ pour tout $k \in \mathbb{N}$ et tout $n \geq N$. Si $k \geq \ell$, on a $d_\ell(I_m) \subset d_k(I_m) \subset d_k(I_N)$ et $d_\ell(I_m) \subset d_k(I_m) \subset d_k(I_n)$. Donc $d_k(I_N) = d_k(I_n) = d_\ell(I_m)$ puisque $d_\ell(I_m)$ est maximal. Si $k < \ell$, on $d_k(I_N) = d_k(I_{n_k}) = d_k(I_n)$. ■

Corollaire 2.3.3 *Si A est noetherien, $A[X_1, \ldots, X_n]$ l'est aussi.*

Proposition 2.3.4 *Soit A un anneau factoriel et $\mathbb{K}$ son corps des fractions. Alors les polynômes irréductibles dans $A[X]$ sont les constantes $p \in A$ irréductibles et les polynômes $P \in A[X]$ primitifs de degré au moins 1 et irréductibles dans $\mathbb{K}[X]$.*

Preuve. Montrons que les éléments proposés sont effectivement irréductibles. Si p est irréductible dans A et $p = P(X)Q(X)$ dans $A[X]$, on doit avoir $d(P) = d(Q) = 0$ car A est intègre. Donc p reste irréductible dans $A[X]$. Si $P \in A[X]$ est irréductible non constant dans $K[X]$ et vérifie $P = QR$ dans $A[X]$, Q ou R est dans $\mathbb{K} \setminus \{0\}$. Supposons qu'il s'agisse de R. Comme R est dans $A[X]$, on doit avoir $R \in A$. Mais alors $c(P) = c(Q)C(R) = 1$ donc $c(R) = R \in A^\times$ et P est bien irréductible.

Montrons qu'il s'agit des seuls irréductibles. Si P est irréductible de degré 0, il s'agit nécessairement d'un irréductible de A. Si P est irréductible de degré au moins 1, on doit avoir $c(P) = 1$. Supposons que l'on ait $P(X) = Q(X)R(X)$ dans $\mathbb{K}[X]$. On peut écrire $Q(X) = \frac{a}{b}Q'(X)$ et $R(X) = \frac{c}{d}R'(X)$ où Q', R' sont dans $A[X]$ et de contenu égal à 1 et a, b, c, d sont dans A avec $\text{pgcd}(a, b) = \text{pgcd}(c, d) = 1$. On en déduit que $bdP(X) = abQ'(X)R'(X)$. En passant aux contenus, on obtient puisque A est intègre $bd = ac$ modulo $A^\times$. Il existe donc $u \in A^\times$ telle que $P(X) = uQ'(X)R'(X)$. Or, P étant irréductible dans $A[X]$ Q' ou R' est dans $A^\times$. Les polynômes irréductibles de $A[X]$ doivent donc nécessairement le rester dans $\mathbb{K}[X]$ ce qui termine la preuve. ■

Théorème 2.3.5 (Gauss) *Soit A un anneau factoriel. Alors $A[X]$ est factoriel.*

Preuve. On commence par montrer l'existence d'une décomposition dans $A[X]$. Considérons $P \in A[X]$ primitif. Soit $\mathbb{K}$ le corps des fractions de A. Comme $\mathbb{K}[X]$ est euclidien, il est factoriel. On peut donc écrire $P(X) = P_1(X)^{r_1} \cdots P_k(X)^{r_k}$ où les P_i sont irréductibles dans $\mathbb{K}[X]$. Posons comme dans la preuve précédente $P_i(X) = \frac{a_i}{b_i} P_i'(X)$ avec $P'(X) \in A[X]$ de contenu égal à 1. D'après la proposition précédente, chaque P_i' est irréductible dans $A[X]$. On obtient $\prod b_i P(X) = \prod a_i \prod P_i'(X)^{r_i}$. En passant aux contenus, cela implique l'existence de $u \in A^\times$ tel que $P(X) = u \prod P_i(X)^{r_i}$ c'est à dire l'existence d'une décomposition en irréductibles dans $A[X]$ pour P. Si P n'est pas primitif, on écrit $P = c(P)P'$ et on décompose P' en irréductibles dans $A[X]$ puis $c(P)$ en irréductibles dans A factoriel.

L'unicité de la décomposition dans $A[X]$ découle immédiatement de l'unicité de la décomposition dans $\mathbb{K}[X]$ et du fait que A est factoriel. ■

Corollaire 2.3.6 *Si A est factoriel, $A[X_1, \ldots, X_n]$ l'est aussi.*

2.4 Critères d'irréductibilité

Soit A un anneau intègre. Il peut être difficile de prouver qu'un polynôme de $A[X]$ est irréductible. Rappelons quelque faits élémentaires mais très utiles.

1. Les polynômes $X - a$ avec $a \in A$ sont irréductibles dans $A[X]$.
2. Si $P(X) \in A[X]$ et $a \in A$ sont tels que $P(a) = 0$, alors $X - a$ divise P dans $A[X]$ (cela découle de la division euclidienne de P par $X - a$ dont le reste est une constante).
3. Un polynôme qui n'a pas de racine peut ne pas être irréductible. Par exemple $P(X) = (X^2 + 1)^2$ n'a pas de racine dans $\mathbb{Z}[X]$ mais n'est pas irréductible.
4. Un polynôme de degré 3 qui n'est pas irréductible dans $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps possède nécessairement une racine.
5. Un polynôme de degré n admet au plus n racines.
6. Un polynôme $P \in \mathbb{C}[X]$ (où plus généralement à coefficients dans un corps algébriquement clos voir le Chapitre 3) a toutes ces racines simples ssi P et son polynôme dérivé P' sont premiers en eux.

Une première méthode pour étudier l'irréductibilité d'un polynôme dans $\mathbb{A}[X]$ consiste à étudier celle de son image dans $A/I[X]$ où I est un idéal premier. En effet sous cette hypothèse, on sait que A/I est intègre donc également $A/I[X]$. Si $P(X) = a_n X^n + \cdots + a_0 \in A[X]$, on note $\overline{P}(X) = \overline{a}_n X^n + \cdots + \overline{a}_0$ son image dans $A/I[X]$.

Proposition 2.4.1 *Soit A un anneau factoriel et $\mathbb{K}$ son corps des fractions (voir chapitre 3). On considère I un idéal premier de A. Soit $P \in A[X]$ de degré n et $\overline{P}$ son image dans $A/I[X]$. On suppose de plus que $d(\overline{P}) = n$. Finalement on note $\mathbb{L}$ le corps des fractions de A/I.*

*Si $\overline{P}$ est irréducitble sur A/I ou $\mathbb{L}$, alors P est irréductible **sur** $\mathbb{K}$.*

Preuve. Laissée en exercice. ■

On prendra garde que l'irréductibilité de P obtenue est sur $\mathbb{K}$ et pas sur A en général. Par exemple $2X$ n'est pas irréductible dans $\mathbb{Z}[X]$ mais l'est dans $\mathbb{Z}/3\mathbb{Z}[X]$.

Exemple 2.4.2

1. *Le polynôme* $P(X) = X^2+Y^2+1$ *est irréductible dans* $\mathbb{R}[X,Y]$. *On le voit en prenant* $I = (Y)$.
2. *Le polynôme* $P(X) = X^3 + 462X^2 + 2433X - 67691$ *est irréductible sur* $\mathbb{Z}$. *En effet, modulo* 2, *on a* $P(X) = X^3 + X + 1$ *qui est irréductible dans* $\mathbb{Z}/2\mathbb{Z}[X]$ *puisque de degré* 3 *sans racine.*

Voici un autre critère permettant de démontrer l'irréductibilité d'un polynôme.

Proposition 2.4.3 (critère d'Eisenstein) *Soit* A *un anneau factoriel,* $\mathbb{K}$ *son corps des fractions. On considère un polynôme* $P(X) = a_nX^n + \cdots + a_0 \in A[X]$ *et* $p \in A$ *un irréductible tel que* $p \not| a_n$, $p \mid a_i$ *pour* $i = 1, \ldots, n-1$ *et* $p^2 \not| a_0$. *Alors* P *est irréductible dans* $\mathbb{K}[X]$ *(donc aussi dans* $A[X]$ *si* $c(P) = 1$).

Preuve. Si P n'est pas irréductible dans $\mathbb{K}[X]$, on peut écrire $P(X) = Q(X)R(X)$ avec P, Q dans $A[X]$ non constants. On a donc $Q(X) = b_qX^q + \cdots + b_0$ et $R(X) = c_rX^r + \cdots + c_0$ avec $0 < q, r < n$. Puisque A est factoriel et p irréductible, l'idéal (p) est premier d'après la Proposition 1.4.3. Donc $B := A/(p)$ est intègre. Dans $B[X]$ on a donc

$$\overline{P}(X) = \overline{a}_nX^n = (\overline{b}_qX^q + \cdots + \overline{b}_0)(\overline{c}_rX^r + \cdots + \overline{c}_0).$$

Mais cette égalité reste vraie dans $\mathbb{L}[X]$ où $\mathbb{L}$ est le corps des fractions de B. Comme $\mathbb{L}[X]$ est euclidien, il est factoriel. L'unicité de la décomposition et les inégalités $0 < q, r < n$ montrent que X divise à la fois $\overline{Q}$ et $\overline{R}$. Donc $\overline{b}_0 = \overline{c}_0 = 0$. Mais alors p^2 divise $a_0 = b_0c_0$ contrairement à l'hypothèse. ■

Exemple 2.4.4

1. *Soit* p *un nombre premier. Alors* $P(X) = X^{p-1} + \cdots + X + 1$ *est irréductible sur* $\mathbb{Z}[X]$. *Il suffit de poser* $X = Y + 1$ *et d'appliquer le critère précédent avec* p.
2. *Soit* $a \in \mathbb{Z}$ *tel que* $v_p(a) = 1$ *pour au moins un nombre premier* p. *Alors* $X^n - a$ *est irréductible dans* $\mathbb{Z}[X]$.
3. *Soit* $\lambda \in \mathbb{R} \setminus \{0, 1\}$. *Le polynôme* $Y^2 - X(X-1)(X-\lambda)$ *est irréductible sur* $\mathbb{R}[X,Y]$. *Cela implique que la cubique d'équation* $Y^2 = X(X-1)(X-\lambda)$ *(dite cubique de Weiserstrass) est connexe dans le plan.*

Chapitre 3

Théorie élémentaire des corps commutatifs

3.1 Généralités

La notion moderne de *corps* est due à Richard Dedekind. Il s'agit d'un anneau dans lequel tous les éléments non nuls sont inversibles. Dans ce qui suit, nous ne considérerons que des corps commutatifs. La théorie des corps non commutatifs est plus complexe mais également très utile notamment en physique avec le corps des quaternions (voir [3] pour la déinition de ce corps non commutatif généralisant $\mathbb{C}$). On peut déjà noter que la notion d'idéal dans un corps est essentiellement triviale : les seuls idéaux du corps $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$ lui-même. Il s'ensuit que tout morphisme non nul d'un corps dans un autre est **nécessairement injectif**.

Il existe par ailleurs une façon canonique de construire un corps à partir d'un anneau intègre que nous allons maintenant brièvement rappeler. Soit A un anneau intègre. On définit que $A \times A \setminus \{0\}$ une relation d'équivalence en posant

$$(a, b) \sim (c, d) \iff ad = bc.$$

On note $\mathbb{K} := A \times A \setminus \{0\}/\sim$ et $\frac{a}{b}$ la classe de (a, b).

Proposition 3.1.1

1. *L'addition* $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ *et la multiplication* $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$ *sont bien définies sur* $\mathbb{K}$.
2. *Elles confèrent à* $\mathbb{K}$ *une structure de corps.*
3. *L'application* $\iota : A \to \mathbb{K}$ *définie par* $\iota(a) = (a, 1)$ *est un morphisme injectif d'anneaux.*
4. *On a la propriété universelle suivante. Pour tout corps* $\mathbb{L}$ *et tout morphisme injectif d'anneaux* f *de* A *dans* $\mathbb{L}$*, il existe un unique morphisme de corps* $\widetilde{f}$ *de* $\mathbb{K}$ *dans* $\mathbb{L}$ *tel que* $f = \widetilde{f} \circ i$

Preuve. Laissée en exercice. ■

Exemple 3.1.2

1. $\mathbb{Q}$ *est le corps des fractions de* $\mathbb{Z}$.
2. *Si* $\mathbb{K}$ *est un corps,* $\mathbb{K}(X)$ *le corps des fractions rationnelles en* X *est le corps des fractions de* $\mathbb{K}[X]$.

Si $\mathbb{K}$ est un corps, l'application $f : \mathbb{Z} \to \mathbb{K}$ définie par

$$f(k) = \underbrace{1_A + \cdots + 1_A}_{k \text{ fois}} \tag{3.1}$$

est un morphisme d'anneaux. On rencontre l'une des deux situations suivantes :

1. Soit $\ker f = \{0\}$ et dans ce cas $\mathbb{K}$ contient un sous-corps isomorphe à $\mathbb{Q}$ (donc en particulier $\mathbb{K}$ est infini). On dit que $\mathbb{K}$ est de caractéristique nulle.
2. Soit $\ker f = p\mathbb{Z}$ avec p premier dans $\mathbb{Z}$. En effet, si $\ker f \neq \{0\}$, $\ker f = p\mathbb{Z}$ est un idéal principal de l'anneau principal $\mathbb{Z}$. Par ailleurs $\mathbb{K}$ contient un sous anneau isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Puisque $\mathbb{K}$ est intègre, ce sous-anneau doit également être intègre ce qui implique que p est premier. On dit alors que le corps $\mathbb{K}$ est de caractéristique p.

Le plus petit sous-corps de $\mathbb{K}$ contenant 1 s'appelle le *sous-corps premier* de $\mathbb{K}$. D'après de qui précède, il est égal à $\mathbb{Q}$ si $\mathbb{K}$ est de caractéristique 0 et à $\mathbb{Z}/p\mathbb{Z}$ si $\mathbb{K}$ est de caractéristique p.

Exemple 3.1.3 *$\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier dans $\mathbb{Z}$.*

Exercice 3.1.4 *Soit $f : \mathbb{K} \to \mathbb{L}$ un morphisme de corps. Montrer que f est injectif et que les deux corps ont la même caractéristique.*

Proposition 3.1.5 (morphisme de Frobenius) *Soit $\mathbb{K}$ un corps de caractéristique p. L'application $F : x \mapsto x^p$ de $\mathbb{K}$ dans $\mathbb{K}$ définit un morphisme (injectif) de corps. On l'appelle le morphisme de Frobenius. En particulier, F est un isomorphisme si $\mathbb{K}$ est fini et $F = id$ si $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$.*

Preuve. Il est clair que $F(xy) = F(x)F(y)$. La formule du binôme donne

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}.$$

Mais pour $k \in \{1, \ldots, p-1\}$, p divise $\binom{p}{k}$. Donc puisque la caractéristique vaut p, on a bien $(x+y)^p = x^p + y^p$. Comme tout morphisme de corps, F est injectif. Si $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$, on a bien sûr $x^p = x$ d'après le petit théorème de Fermat. ■

3.2 Extensions de corps, éléments algébriques et transcendants

3.2.1 Dégré d'une extension

Si $\mathbb{K}$ et $\mathbb{L}$ sont deux corps tels que $\mathbb{K} \subset \mathbb{L}$, $\mathbb{L}$ est un $\mathbb{K}$ espace vectoriel. On dit que $\mathbb{L}$ est une *extension* de $\mathbb{K}$. Lorsque $\dim_{\mathbb{K}}(\mathbb{L})$ est finie on dit que l'extension est finie de *degré* $[\mathbb{L} : \mathbb{K}] = \dim_{\mathbb{K}}(\mathbb{L})$. Dans le cas où $\mathbb{K}$ est un corps fini, on a alors $|\mathbb{L}| = |\mathbb{K}|^n$.

Théorème 3.2.1 (de la base téléscopique) *Soient $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ une tour d'extention de corps. On suppose données $(e_i)_{i\in I}$ et $(f_j)_{j\in J}$ respectivement des bases de $\mathbb{L}$ sur $\mathbb{K}$ et de $\mathbb{M}$ sur $\mathbb{L}$. Alors la famille $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$.*

Preuve. En décomposant un élément $x \in \mathbb{M}$ sur la base (f_j) puis chaque f_j sur la base (e_i), on obtient la décomposition de x sur la famille $(e_i f_j)$ qui est donc génératrice. Si $\sum_i \sum_j \lambda_{i,j} e_i f_j = 0$ avec $\lambda_{i,j} \in \mathbb{K}$, on a $\sum_j \left(\sum_i \lambda_{i,j} e_i\right) f_j = 0$. Comme (f_j) est libre, cela donne $\sum_i \lambda_{i,j} e_i$ pour tout i et donc $\lambda_{i,j} = 0$ pour tout i et tout j puisque (e_i) est libre. La famille $(e_i f_j)$ est donc bien une base de $\mathbb{M}$ sur $\mathbb{K}$. ■

Corollaire 3.2.2 *On a* $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

3.2.2 Eléments algébriques et transcendants

Soit $\mathbb{K} \subset \mathbb{L}$ une extension et E un sous-ensemble de $\mathbb{L}$. On note $\mathbb{K}(E)$ le plus petit sous-corps de $\mathbb{L}$ contenant les éléments de E et on l'appelle sous-corps engendré par E. L'extension $\mathbb{L}$ est dite *monogène* si il existe $\alpha \in \mathbb{L}$ telle que $\mathbb{L} = \mathbb{K}(\alpha)$. On dit alors que α est un élément *primitif* dans $\mathbb{L}$.

Si $\mathbb{K} \subset \mathbb{L}$ est une extension et $\alpha \in \mathbb{L}$, on peut considérer le morphisme d'anneaux

$$\theta_\alpha : \begin{cases} \mathbb{K}[X] \to \mathbb{L} \\ P(X) \longmapsto P(\alpha) \end{cases}$$

Deux situations peuvent alors se produire :

1. Soit θ_α est injectif. Dans ce cas $\mathbb{K}[\alpha]$ est isomorphe à $\mathbb{K}[X]$ et en particulier $\mathbb{L}$ est une extension infinie (i.e. de degré infini) sur $\mathbb{K}$. On dit alors que le nombre α est *transcendant*.
2. Soit $\ker \theta_\alpha = (P)$ où (P) est un idéal principal non réduit à $\{0\}$ de $\mathbb{K}[X]$. En effet $\mathbb{K}[X]$ est euclidien donc principal. Le corps $\mathbb{L}$ contient alors un sous-anneau isomorphe à $\mathbb{K}[X]/(P)$, ce dernier doit être intègre ce qui force le polynôme P à être irréductible. On dit alors que le nombre α est *algébrique*. L'unique polynôme unitaire dans (P) s'appelle le *polynôme minimal* de α et on le note $\mu_\alpha(X)$.

Proposition 3.2.3 *Soient* $\mathbb{K} \subset \mathbb{L}$ *et* $\alpha \in \mathbb{L}$. *Les propriétés suivantes sont équivalentes :*

1. α *est algébrique sur* $\mathbb{K}$, *de polynôme minimal* μ_α *de degré* n,
2. $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$,
3. $\dim_{\mathbb{K}} \mathbb{K}[\alpha]$ *est finie est égale au degré de* n.

Preuve. (1) $\Longrightarrow$ (2) : Si α est algébrique, on a d'après ce qui précède un isomorphisme d'anneaux entre $\mathbb{K}[\alpha]$ et $\mathbb{K}[X]/(P)$. Mais puisque P est irréductible et $\mathbb{K}[X]$ principal, $\mathbb{K}[X]/(P)$ est un corps. Ainsi $\mathbb{K}[\alpha]$ est un corps contenant α. Le plus petit sous-corps de ce type est $\mathbb{K}(\alpha)$ et donc $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.

(2) $\Longrightarrow$ (1) : Si $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$, on ne peut pas avoir $\mathbb{K}[\alpha] = \mathbb{K}[X]$ car $\mathbb{K}[X] \neq \mathbb{K}(X)$. Donc α est algébrique.

(3) $\Longrightarrow$ (1) : Découle aussi du fait que $\mathbb{K}[\alpha] = \mathbb{K}[X]$ si α est transcendant.

(1) $\Longrightarrow$ (3) : Puisque μ_α est le polynôme minimal de α, $1, \alpha, \ldots, \alpha^{n-1}$ forme une base de $\mathbb{K}(\alpha) = \mathbb{K}[\alpha]$ (dans le cas contraire on aurait un polynôme annulateur de α de degré inférieur à n). ■

Exemple 3.2.4 *Les nombres* e *et* π *sont transcendants. La preuve n'est pas immédiate et utilise des méthodes analytiques (voir par exemple [3]).*

Exercice 3.2.5

1. *Montrer que les nombres $e+\pi$ et $e\pi$ ne peuvent pas être simutanément algébriques. Noter que l'on ignore encore si $e+\pi$ ou $e\pi$ sont transcendants !*
2. *Montrer que $1+\sqrt{2}+\sqrt{3}$ est algébrique sur $\mathbb{Q}$ de degré 4.*

Une extension $\mathbb{K} \subset \mathbb{L}$ est *finie* lorsque $[\mathbb{K} : \mathbb{L}]$ est fini. Dans ce cas, il découle de la proposition précédente que tous les éléments de $\mathbb{L}$ sont algébriques sur $\mathbb{K}$. Plus généralement, une extention $\mathbb{K} \subset \mathbb{L}$ est dite *algébrique* si tous les éléments de $\mathbb{L}$ sont algébriques sur $\mathbb{K}$.

Théorème 3.2.6 *Soit $\mathbb{K} \subset \mathbb{L}$ une extension. On note $\mathbb{M} := \{x \in L \mid x \text{ est algébrique sur } \mathbb{K}\}$. Alors $\mathbb{M}$ est un sous-corps algèbrique de $\mathbb{L}$.*

Preuve. Soient α, α' dans $\mathbb{M}$. On a $\mathbb{K}[\alpha, \alpha'] = \mathbb{K}[\alpha][\alpha']$. Comme α et α' sont algébriques sur $\mathbb{K}$, la proposition précédente montre que $\mathbb{K}[\alpha]$ et $\mathbb{K}[\alpha, \alpha']$ sont des corps et plus précisément des extensions finies de $\mathbb{K}$. Comme $\mathbb{K}[\alpha\alpha']$ et $\mathbb{K}[\alpha+\alpha']$ sont contenus dans $\mathbb{K}[\alpha, \alpha']$, ils sont de dimension finie ce qui montre que $\alpha\alpha'$ et $\alpha + \alpha'$ sont algébriques. ■

3.2.3 Clôture algébrique

On dit qu'un corps $\mathbb{K}$ est algébriquement clos si l'une des propriétés équivalentes suivantes est vérifiées :

1. Tout polynôme de $\mathbb{K}[X]$ de degré au moins 1 admet une racine dans $\mathbb{K}$.
2. Tout polynôme de $\mathbb{K}[X]$ de degré au moins 1 se décompose en un produit de polynômes de degré 1.
3. Les irréductibles de $\mathbb{K}[X]$ sont les polynômes de la forme $X - a$ avec $a \in \mathbb{K}$.
4. Si $\mathbb{L}$ est une extension de $\mathbb{K}$ algébrique, $\mathbb{K} = \mathbb{L}$.

Le célèbre théorème suivant formulé par Dalembert n'a été complètement prouvé qu'un peu plus tard par Gauss. Nous en donnons une preuve élémentaire n'utilisant que des outils d'analyse de niveau licence.

Théorème 3.2.7 *Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.*

Preuve. Il s'agit de montrer que tout polynôme $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ unitaire de degré n dans $\mathbb{C}$ a au moins une racine. Cela revient à montrer que l'équation $P(z) = 0$ possède toujours une solution complexe.

Considérons tout d'abord l'équation $x^n = a$ avec $n \geq 1$ un entier et $a \in \mathbb{C}$. Dans ce cas, on sait trouver les solutions. En particulier $z = \sqrt[n]{|a|}\exp(\frac{2i\pi\theta}{n})$ avec $\theta = \arg a$ est solution.

Soit maintenant la fonction $f : \mathbb{C} \to \mathbb{R}_{\geq 0}$ telle que $f(z) = |P(z)|$. Il s'agit d'une fonction continue non identiquement nulle puisque $P \neq 0$. L'ensemble $E := f(\mathbb{C})$ est non vide minoré par 0 donc admet une borne inférieure m. Par ailleurs l'inégalité triangulaire montre que

$$|P(z)| \geq |z^n| - \left|a_{n-1}z^{n-1} + \cdots + a_0\right| \geq |z|^n \left(1 - \frac{\left|a_{n-1}z^{n-1} + \cdots + a_0\right|}{|z|^n}\right).$$

On voit donc que $\lim_{|z|\to+\infty} f(z) = +\infty$. La fonction f étant continue, il existe un rayon $r > 0$ tel que $f(z) > m$ dès que z sort de $D(0, r)$ le disque de centre 0 et de rayon r. Ce dernier étant

compact, f atteint son minimum m en une valeur z_0, i.e. $f(z_0) = m$. Quitte à remplacer $P(X)$ par $P(X + z_0)$ ce qui ne change rien aux valeurs prises par f, on peut supposer que $z_0 = 0$.

On peut alors écrire $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_kX^k + a_0$ avec $k > 0$ minimal tel que $a_k \neq 0$. On a alors $m = a_0$. Soit c tel que $c^k = -m\overline{a_k}$. Un tel complexe existe puisque les équations de la forme $z^n = a$ ont toujours au moins une solution.

Supposons $m \neq 0$. On définit maintenant la fonction g sur l'intervalle $[0, 1]$ par $g(t) = f(tc)$. Cela donne

$$g(t) = \left| m - m \times |a_k|^2 t^k + c_{k+1}t^{k+1} + \cdots + c_nt^n \right| \text{ où } c_r = a_rc^r, r = k+1, \ldots, n.$$

On a donc en utilisant l'inégalité triangulaire et pour tout $t \in [0, 1]$

$$g(t) \leq m(1-|a_k|^2 t^k)+t^{k+1}(\left|c_{k+1} + \cdots + c_nt^{n-k-1}\right| \leq m(1-|a_k|^2 t^k)+t^{k+1}M \leq m-|a_k|^2 t^k \left(1 - \frac{tM}{m|a_k|^2}\right).$$

où $M = |c_{k+1}| + \cdots + |c_n| > 0$. Pour $0 < t \leq \min(1, \frac{m|a_k|^2}{M})$, on voit que $g(t) < m$ ce qui fournit une contradiction. Cela signifie que notre supposition $m \neq 0$ est fausse. Donc $m = 0$ et P admet bien une racine dans $\mathbb{C}$. ■

La proposition suivante montre que les nombres complexe algébriques sont plutôt rares parmi tous les nombres complexes. Paradoxalement, il est souvent difficile de montrer qu'un nombre donné est transcendant.

Proposition 3.2.8 *Le corps $\mathbb{A}$ des nombres complexes algèbriques sur $\mathbb{Q}$ est dénombrable.*

Preuve. Pour tout n, on note $\mathbb{A}(n)$ l'ensemble des nombres complexes algébriques sur $\mathbb{Q}$ dont le polynôme minimal est de degré n. L'ensemble des polynômes de degré n de $\mathbb{Q}[X]$ est dénombrable. Il s'ensuite que l'ensemble de leur racines l'est aussi, donc $\mathbb{A}(n)$ est dénombrable. Comme $\mathbb{A} = \cup_{n\geq 1}\mathbb{A}_n$, $\mathbb{A}$ est dénombrable. ■

On dit que l'extension $\overline{\mathbb{K}}$ de $\mathbb{K}$ est *clôture algèbrique* de $\mathbb{K}$ si $\overline{\mathbb{K}}$ est algébriquement clos et $\overline{\mathbb{K}}$ est algébrique sur $\mathbb{K}$. D'après le théorème de Gauss, $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$. Nous renvoyons à [3] pour la preuve du théorème fondamental suivant.

Théorème 3.2.9 *Un corps admet une clôture algébrique qui est unique à isomorphisme près.*

Exercice 3.2.10 *Montrer que la clôture algébrique de $\mathbb{Q}$ est le corps $\overline{\mathbb{Q}}$ des nombres algébriques sur $\mathbb{Q}$.*

3.2.4 Construction à la règle et au compas

Etant donné A un ensemble de points du plan, quels sont les points pouvant être contruits à partir de A en n'utilisant qu'une règle (non graduée) et un compas ? Ce problème est historiquement très important car il contient trois problèmes majeurs de géométrie déjà formulés par les grecs dans l'antiquité, à savoir :

1. Peut-on construire un cube dont le volume est le double de celle d'une cube donné (*duplication du cube*) ?

2. Peut-on diviser un angle quelconque en trois angles égaux (*trisection de l'angle*) ?
3. Peut-on construire un carré (à la règle et au compas) dont l'aire est égale à celle d'un cercle (*quadrature du cercle*) ?

Dans les trois cas, la réponse est négative. On a en effet le théorème suivant :

Théorème 3.2.11 *Le point $(x, 0)$ est constructible ssi il existe n tel que $[\mathbb{Q}(x) : \mathbb{Q}] = 2^n$.*

Nous renvoyons le lecteur à [5] pour une preuve détaillée (tout particulièrement les futurs candidats au Capes ou à l'Agrégation). L'idée essentielle est que les équations de droites étant de degré 1 et les équations de cercles de degré 2, les points contructibles à partir d'un point donné doivent être dans une extension de $\mathbb{Q}$ de degré une puissance de 2. On peut alors en déduire facilement que la réponse aux trois problèmes précédents est négative.

1. $\sqrt[3]{2}$ n'est pas constructible car $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ puisque $\mu_{\sqrt[3]{2}}(X) = X^3 - 2$.
2. On ne peut pas couper à la règle et au compas $\frac{\pi}{3}$. En effet, cela voudrait dire que l'on peu construire $x = \cos\frac{\pi}{9}$ à partir de $\cos\frac{\pi}{3} = \frac{1}{2} \in \mathbb{Q}$. Mais le polynôme minimal de x est $\mu_x(X) = X^3 - \frac{3}{4}X^2 - \frac{1}{8}$. On a donc encore $[\mathbb{Q}(x) : \mathbb{Q}] = 3$
3. Le nombre π est transcendant, donc également $\sqrt{\pi}$. On a donc $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = +\infty$.

3.3 Corps de rupture et corps de décomposition

Soit $P \in \mathbb{K}[X]$ un polynôme irréductible de degré $d > 1$. Le but de ce paragraphe est de construire une extension de $\mathbb{K}$ dans laquelle P possède au moins une racine (*corps de rupture* de P) et une extension dans laquelle P se décompose en un produit de facteurs de degré 1 (*corps de décomposition*).

Plus précisément, une extension $\mathbb{K} \subset \mathbb{L}$ est un corps de rupture de P si $\mathbb{L} = \mathbb{K}(\alpha)$ est une extension monogène avec $P(\alpha) = 0$.

Proposition 3.3.1 *Soit $P \in \mathbb{K}[X]$ un polynôme irréduible de degré $d > 1$. Il existe un corps de rupture de P unique à isomorphisme près.*

Preuve. Un tel corps existe. Il suffit en effet de prendre $\mathbb{L} = \mathbb{K}[X]/(P)$ qui est bien un corps puisque P est irréducible (donc (P) est maximal). Le corps $\mathbb{K}$ s'injecte dans $\mathbb{L}$ et si x est l'image de X par la projection canonique, on a $P(x) = 0$ dans $\mathbb{L} = \mathbb{K}(x)$.

Soit $\mathbb{L} = \mathbb{K}(\alpha)$ un corps de rupture de P. On considère le morphisme d'anneaux $\phi : \mathbb{K}[X] \to \mathbb{L}$ tel que $\phi(X) = \alpha$. Alors ϕ est surjectif puisque $\mathbb{L} = \mathbb{K}(\alpha)$. Par ailleurs $\ker\phi = (P)$ puisqu'il s'agit d'un idéal contenant l'idéal (P) qui est maximal. On a donc $\mathbb{L} \simeq \mathbb{K}[X]/(P)$ ce qui montre l'unicité. ■

Exemple 3.3.2 *On vérifie facilement que $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$ et que $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[X]/(X^3 - 2)$.*

Ce dernier exemple montre que toutes les racines de P ne sont pas dans son corps de rupture en général (ici $X^3 - 2$ admet des racines complexes alors que $\mathbb{Q}(\sqrt[3]{2})$ est un sous-corps de $\mathbb{R}$). Cela conduit à la définition suivante. Soit $P \in \mathbb{K}[X]$ un polynôme (pas nécessairement irréductible) de degré n. Un *corps de décomposition* de P est une extension $\mathbb{L}$ de $\mathbb{K}$ telle que P soit un produit de facteurs de degré 1 dans $\mathbb{L}[X]$ (i.e. toutes les racines de P sont dans $\mathbb{L}$) et soit minimal avec cette propriété (les racines de P engendrent $\mathbb{L}$ sur $\mathbb{K}$).

Proposition 3.3.3 *Pour tout $P \in \mathbb{K}[X]$, il existe un corps de décomposition de P, unique à isomorphisme près.*

Preuve. Pour l'existence, on raisonne par récurrence sur $d = d(P)$. Si $d = 1$, $\mathbb{L} = \mathbb{K}$ convient. De même si P est un produit de facteurs de degré 1 dans $\mathbb{K}[X]$, $\mathbb{L} = \mathbb{K}$ convient. Dans le cas contraire, P possède un facteur irréductible Q avec $d(Q) > 1$ et on peut considérer $\mathbb{K}'$ le corps de rupture de Q sur $\mathbb{K}$. On a donc dans $\mathbb{K}'[X]$, $P = (X - \alpha_1)P'(X)$ où α_1 est une racine de P dans $\mathbb{K}'$. Par hypothèse de récurrence, il existe un corps de décomposition $\mathbb{L}$ de P' sur $\mathbb{K}'$. Si $\alpha_2, \ldots, \alpha_r$ sont les racines de P' dans $\mathbb{L}$, on a $\mathbb{L} = \mathbb{K}'(\alpha_2, \ldots, \alpha_r)$. Donc $\mathbb{L} = \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_r)$ est un corps de décomposition de P au dessus de $\mathbb{K}$.

Soient $\mathbb{L}$ et $\mathbb{L}'$ deux corps de décomposition de P. Pour montrer qu'ils sont isomorphes, on procède par induction sur $[\mathbb{L} : \mathbb{K}]$. Si $[\mathbb{L} : \mathbb{K}] = 1$, toutes les racines de P sont dans $\mathbb{K}$, donc par minimalité de $\mathbb{L}'$, on a aussi $\mathbb{L}' = \mathbb{K}$. Sinon, P possède un facteur irréductible Q. Soit α une racine de Q et $\mathbb{M} = \mathbb{K}(\alpha)$. Alors $\mathbb{M}$ est un sous-corps de $\mathbb{L}$ et de $\mathbb{L}'$ puisque ces deux corps contiennent la racine α. Dans $\mathbb{M}[X]$, on a $P(X) = (X-\alpha)P'(X)$. Puisque $\mathbb{L}$ et $\mathbb{L}'$ sont des corps de décomposition de P au dessus de $\mathbb{K}$, ce sont aussi des corps de décomposition de P' au dessus de $\mathbb{M}$. Ils sont donc isomorphes d'après l'hypothèse de récurrence puisque $[\mathbb{L} : \mathbb{M}] < [\mathbb{L} : \mathbb{K}]$. ■

Exemple 3.3.4 *Le corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt[3]{2}, j)$ avec $j = \exp(\frac{2i\pi}{3})$. Celui de $X^4 - 2$ est $\mathbb{Q}(\sqrt[4]{2}, i)$.*

3.4 Corps finis

On a déjà vu que la caractéristique d'un corps fini $\mathbb{K}$ est non nulle, égale à p un nombre premier. Le sous-corps premier de $\mathbb{K}$ est alors $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Il s'ensuite que $\mathbb{K}$ est une extension finie de $\mathbb{F}_p$. Si on note $n := [\mathbb{K} : \mathbb{F}_p]$, on a donc $|\mathbb{K}| = p^n$.

Théorème 3.4.1 *Soit p un nombre premier et $n \geq 1$ un entier. On pose $q = p^n$.*

1. *Le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$ est un corps fini à q éléments.*
2. *il n'existe, à isomorphisme près, qu'un corps fini à q éléments. On le note $\mathbb{F}_q$.*

Preuve. 1 : Soit $\mathbb{K}$ le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$ et $\mathbb{J}$ l'ensemble des racines du polynôme $X^q - X$ dans $\mathbb{K}$. Puisque $G : x \to x^q$ est l'itération du morphisme de Frobenius, $\mathbb{J}$ est un corps contenant toutes les racines de $X^q - X$. On a donc $\mathbb{J} = \mathbb{K}$. De plus le polynôme dévivé de $P(X) = X^q - X$ vaut $P('X) = qX^{q-1} - 1 = -1$. Donc P et P' sont premiers entre eux et P possède q racines distinctes dans $\mathbb{K}$. Finalement $\mathbb{K}$ contient exactement les q racines distintes de P.

2 : Si $\mathbb{K}$ est un corps à q éléments, $\mathbb{K}^\times$ est un groupe d'ordre $q - 1$. Donc tout $x \in \mathbb{K}$ est racine du polynôme $X^q - X$ à coefficients dans $\mathbb{F}_p$ le sous-corps premier de $\mathbb{K}$. Donc $\mathbb{K}$ est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$ deux tels corps de décomposition sont isomorphes d'après la Proposition 3.3.3. ■

Exercice 3.4.2 *Donner les tables d'addition et de multiplication du corps $\mathbb{F}_4$.*

Théorème 3.4.3 *$\mathbb{F}_q^\times$ est un groupe cyclique à $q - 1$ éléments.*

Preuve. Notons E l'ensemble (nécessairement fini) de tous les ordres des élements de $\mathbb{F}_q^\times$ et μ le ppcm des éléments de E. Soit $\mu = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la décomposition de μ en facteurs premiers. Pour tout $i = 1, \ldots, r$, il existe au moins un élément a_i dans $\mathbb{F}_q^\times$ dont l'ordre est de la forme $p_i^{\alpha_i} m_i$ avec $p_i \not| m_i$. Alors $b_i = a_i^{m_i}$ est d'ordre $p_i^{\alpha_i}$. On en déduit que $b = b_1 \cdots b_r$ est d'ordre μ puisque les p_i sont distincts et que $\mathbb{F}_q^\times$ est abélien. Le sous-groupe $\langle b \rangle$ de $\mathbb{F}_q^\times$ engendré par b est d'ordre μ. D'un autre côté, tout élément $a \in \mathbb{F}_q^\times$ vérifie $a^\mu = 1$ donc est racine du polynôme $X^\mu - 1$ à coefficients dans $\mathbb{F}_p$. Ce polynôme possède au plus μ racines ce qui implique que $\left|\mathbb{F}_q^\times\right| \leq \mu$. On en déduit donc que $\mathbb{F}_q^\times = \langle b \rangle$ est cyclique. ■

Attention :

1. Une erreur répandue consiste à confondre le corps $\mathbb{F}_q$ avec l'anneau $\mathbb{Z}/q\mathbb{Z}$. Les deux ne coïncident uniquement que lorsque $q = p$ est un nombre premier et pas pour $q = p^n$ avec $n > 1$ comme on peut facilement s'en convaincre grâce à l'exercice précédent.
2. Ce qui précède ne permet pas de conclure que tout corps fini est commutatif puisqu'isomorphe à un corps de décomposition sur $\mathbb{F}_p$. En effet, toutes les constructions précédentes supposent déjà que les corps considérés sont commutatifs. Nous verrons que le théorème de Wedderburn affirmant que tout corps fini est commutatif peut se prouver en utilisant la notion de polynômes cyclotomiques qui fait l'objet du paragraphe suivant

3.5 Polynômes cyclotomiques

Soit $\mathbb{K}$ un corps et $n \geq 1$ un entier. On considère le polynôme $P_n(x) = X^n - 1$. On suppose que la **caractéristique de $\mathbb{K}$ ne divise pas** n, autrement dit qu'elle est nulle ou égale à un nombre premier p premier avec n. Dans ce cas, $P_n'(X) = nX^{n-1}$ est premier avec $P_n(X)$, donc ce dernier n'admet que des racines simples dans un corps de décomposition. Les racines de P_n sont les *racines n-ième de l'unité* (sur $\mathbb{K}$). Elles forment un groupe de $\mathbb{K}^\times$ que nous noterons $U_{n,\mathbb{K}} := \{\xi \in \mathbb{K} \mid \xi^n = 1\}$.

Proposition 3.5.1 *$U_{n,\mathbb{K}}$ est un groupe cyclique et $|U_{n,\mathbb{K}}| \leq n$. Le corps $\mathbb{K}$ contient un corps isomorphe au corps de décomposition de P_n ssi on a $U_{n,\mathbb{K}} \simeq \mathbb{Z}/n\mathbb{Z}$.*

Preuve. On a bien sûr $|U_{n,\mathbb{K}}| \leq n$ puisque P_n a au plus n racines dans $\mathbb{K}$. Il suffit alors de reprendre la preuve du Théorème 3.4.3. On note E l'ensemble des ordre des éléments de $U_{n,\mathbb{K}}$ et μ le ppcm de ces ordres. On en déduit l'existence d'un sous-groupe cyclique G d'ordre μ dans $U_{n,\mathbb{K}}$. Comme les éléments de ce groupe sont racines de $X^\mu - 1$ à coefficients dans $\mathbb{K}$, on a $|U_{n,\mathbb{K}}| \leq \mu$ ce qui montre que $G = U_{n,\mathbb{K}}$ est cyclique. ■

Exemple 3.5.2 *Le groupe $U_{4,\mathbb{Q}}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ alors que $U_{4,\mathbb{C}}$ est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.*

On suppose jusqu'à la fin de cette section sur les polynômes cyclotomiques, que $\mathbb{K}$ **contient un sous-corps isomorphe au corps de décomposition de** P_n. Dans ce cas $U_{n,\mathbb{K}} \simeq \mathbb{Z}/n\mathbb{Z}$. Une racine $\xi \in U_{n,\mathbb{K}}$ d'ordre n est dite *primitive*. C'est alors un générateur de $U_{n,\mathbb{K}}$. on notera $U_{n,\mathbb{K}}^\times$ le sous-ensemble des racines primitives. D'après la proposition précédente, on doit avoir $\left|U_{n,\mathbb{K}}^\times\right| = \varphi(n)$. On appelle n-ième *polynôme cyclotomique* sur $\mathbb{K}$ le polynôme $\phi_{n,\mathbb{K}} \in \mathbb{K}[X]$ défini par

$$\phi_{n,\mathbb{K}}(X) := \prod_{\xi \in U_{n,\mathbb{K}}^\times} (X - \xi).$$

Il s'agit donc d'un polynôme unitaire de degré $\varphi(n)$. Par ailleurs, l'ordre d'une racine ξ de P_n est un diviseur d de n. Cela découle de la proposition précedente. En regroupant les racines n-ième ayant le même ordre d, on obtient immédiatement l'identité

$$X^n - 1 = \prod_{d|n} \phi_{d,\mathbb{K}}(X). \tag{3.2}$$

En comparant les dégrés, on retrouve l'identité bien connue

$$n = \sum_{d|n} \varphi(d)$$

où φ *est la fonction indicatrice d'Euler*. En outre, (3.2) permet le calcul des polynômes cyclotomiques par récurrence. On a en effet $\phi_{1,\mathbb{K}}(X) = X - 1$. Ensuite l'identité $X^2 - 1 = \phi_{1,\mathbb{K}}(X)\phi_{2,\mathbb{K}}(X)$ donne $\phi_{2,\mathbb{K}}(X) = X + 1$. De façon générale, nous avons

$$\phi_{n,\mathbb{K}}(X) = \frac{X^n - 1}{\prod_{d|n,d<n} \phi_{d,\mathbb{K}}(X)}.$$

Exercice 3.5.3 *Vérifier que* $\phi_{2,\mathbb{K}}(X) = X^2 + X + 1$, $\phi_{4,\mathbb{K}}(X) = X^2 + 1$, $\phi_{5,\mathbb{K}}(X) = X^4 + X^3 + X^2 + X + 1$, $\phi_{6,\mathbb{K}}(X) = X^2 - X + 1$.

Proposition 3.5.4 *Pour tout entier* $n \geq 1$,

1. $\phi_{n,\mathbb{Q}}(X) \in \mathbb{Z}[X]$,
2. $\phi_{n,\mathbb{K}}(X) = f(\phi_{n,\mathbb{Q}}(X))$ *où* $f : \mathbb{Z} \to \mathbb{K}$ *est le morphisme canonique (3.1). Ainsi* $\phi_{n,\mathbb{K}}(X) = \phi_{n,\mathbb{Q}}(X)$ *si* $\mathbb{K}$ *est de caractéristique nulle et dans le cas contraire* $\phi_{n,\mathbb{K}}(X)$ *s'obtient à partir de* $\phi_{n,\mathbb{Q}}(X)$ *par réduction modulo* p.

Preuve. 1 : On raisonne par récurrence sur n. On a $\phi_{1,\mathbb{Q}}(X) = X - 1$. Si on suppose que $\phi_{d,\mathbb{Q}}(X) \in \mathbb{Z}[X]$ pour tout $d < n$, $F(X) = \prod_{d|n,d<n} \phi_{d,\mathbb{Q}}(X) \in \mathbb{Z}[X]$ et F est unitaire. On peut alors, d'après la Proposition 2.2.2, effectuer la division euclidienne de $X^n - 1$ par $F(X)$ dans $\mathbb{Z}[X]$. Elle s'écrit $X^n - 1 = F(X)Q(X) + R(X)$ dans $\mathbb{Z}[X]$. Mais dans $\mathbb{Q}[X]$, on doit avoir $X^n - 1 = F(X)\phi_{n,\mathbb{Q}}(X)$. Donc dans $\mathbb{Q}[X]$, $R(X) = F(X)(\phi_{n,\mathbb{Q}}(X) - Q(X))$. Mais $d(R) < d(F)$. Cela impose que $\phi_{n,\mathbb{Q}}(X) = Q(X) \in \mathbb{Z}[X]$.

2 : Là encore on raisonne par récurrence. Le cas $n = 1$ est immédiat. Dans $\mathbb{Z}[X]$, on a d'après le 1, $X^n - 1 = F(X)\phi_{n,\mathbb{Q}}(X)$. En appliquant le morphisme f, cela donne $X^n - 1 = f(F(X))f(\phi_{n,\mathbb{Q}}(X))$. Or par hypothèse de récurrence $f(F(X)) = \prod_{d|n,d<n} \phi_{d,\mathbb{K}}(X)$. Puisque $\mathbb{K}[X]$ est intègre, on en déduit que $f(\phi_{n,\mathbb{Q}}(X)) = \phi_{n,\mathbb{K}}(X)$. ■

Pour alléger les notations, on pose $\phi_{n,\mathbb{K}} = \phi_n$ lorsque $\mathbb{K}$ est de caractéristique 0 et $\phi_{n,\mathbb{K}} = \phi_{n,p}$ lorsque $\mathbb{K}$ est de caractéristique p.

Théorème 3.5.5 *Les polynômes cyclotomiques* ϕ_n *sont irréductibles sur* $\mathbb{Z}$ *(donc aussi sur* $\mathbb{Q}$*).*

Preuve. Soit $P \in \mathbb{Z}[X]$ un facteur irréductible de P. Il existe $Q \in \mathbb{Z}[X]$ tel que $\phi_n = PQ$. Soit E l'ensemble des racines de P dans $\mathbb{C}$. Ces racines sont des racines n-ième de 1 de polynôme minimal P.

On va montrer par l'absurde que pour tout $\xi \in E$ et tout p premier ne divisant pas n, $\xi^p \in E$. Supposons qu'il existe $\xi \in E$ et p premier avec n tel que $\xi^p \notin E$, i.e. $P(\xi^p) \neq 0$. Comme $\phi(\xi^p) = 0$ (ξ^p est racine primitive de 1 puisque n et p sont premiers entre eux), on doit avoir $Q(\xi^p) = 0$. Ainsi ξ est racine de $Q(X^p)$. Comme P est le polynôme minimal de ξ, et qu'il est unitaire, il existe $R \in \mathbb{Z}[X]$ tel que $Q(X^p) = P(X)R(X)$. Dans $\mathbb{Z}/p\mathbb{Z}[X]$ (i.e. en passant aux classes modulo p), on obtient $\overline{Q}(X^p) = \overline{Q}(X)^p = \overline{P}(X)\overline{R}(X)$. Soit $\mathbb{L}$ un corps de décomposition de $\overline{P}$ sur $\mathbb{Z}/p\mathbb{Z}$ et α une racine de $\overline{P}$ dans $\mathbb{L}$. Alors $\overline{Q}$ admet également α comme racine dans $\mathbb{L}$. Cela implique que $\phi_{n,p} = \overline{\phi_n} = \overline{PQ}$ admet une racine d'ordre au moins 2 dans $\mathbb{L}$ ce qui est impossible car toutes les racines de $X^n - 1$ sont simples dans $\mathbb{L}$ à cause de l'hypothèse p ne divise pas n.

Ainsi pour tout nombre premier p ne divisant pas n, E est stable par le passage à la puissance p. Il s'ensuit qu'il est stable par passage à n'importe quelle puissance r première avec n (en décomposant r en facteur premiers) et donc que E contient toutes les racines primitives n-ièmes. Donc $\phi_n = P$ est bien irréductible sur $\mathbb{Z}$. ■

Puisque ϕ_n est irréductible sur $\mathbb{Q}$ et ses racines sont les racines primitives n-ièmes de 1, on a le corrolaire suivant.

Corollaire 3.5.6 *Si ξ est une racine primitive n-ième de 1 dans un corps de caractéristique nulle, son polynôme minimal sur $\mathbb{Q}$ est ϕ_n et donc $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$.*

Les polynômes cyclotomiques ont de nombreuses appplications, notamment en cryptographie. Ils permettent également de démontrer le théorème fondamental qui suit.

Théorème 3.5.7 (de Wedderburn) *Tout corps fini est commutatif.*

Preuve. Soit $\mathbb{K}$ un corps fini (éventuellement non commutatif). On note k son centre, i.e. $k := \{x \in \mathbb{K} \mid xy = yx, \forall y \in \mathbb{K}\}$. On vérifie facilement que k est un corps commutatif fini et que $\mathbb{K}$ est un k-espace vectoriel de dimension finie n. Ainsi si $|k| = q$, on a $|\mathbb{K}| = q^n$. Le groupe $\mathbb{K}^\times$ opère sur $\mathbb{K}$ par automorphismes intérieurs. On note pour tout $x \in \mathbb{K}$, $\omega(x)$ l'orbite de x sous cette action. Soit $k_x := \{y \in \mathbb{K} \mid xy = yx\}$. Alors k_x est un sous-corps (éventuellement non commutatif) de $\mathbb{K}$. C'est aussi un espace vectoriel sur k de dimension, disons d. Le stabilisateur de x est $k_x^\times$. Puisque $k_x^\times \subset \mathbb{K}^\times$, on doit avoir $q^d - 1 \mid q^n - 1$ ce qui implique que $d \mid n$. Il s'ensuite que $|\omega(x)| = \frac{q^n-1}{q^d-1}$. En utilisant la relation (3.2), on obtient alors $|\omega(x)| = \prod_{m|n, m|\not d} \phi_m(q)$. Lorsque $d < n$, on a donc $\phi_n(q) \mid |\omega(x)|$. Par ailleurs, l'équation des classes s'écrit

$$\left|\mathbb{K}^\times\right| = \left|k^\times\right| + \sum_{x \notin k} |\omega(x)| .$$

On en déduit que $\phi_n(q)$ divise $|k^\times| = q - 1$, en particulier $\phi_n(q) \leq q - 1$. Posons $\phi_n(q) = (q - \xi_1) \cdots (q - \xi_r)$. On montre facilement que, les racines de 1 étant de norme 1 dans $\mathbb{C}$ et q étant un nombre entier, on a $|q - \xi_i| > q - 1$ si $\xi_i \neq 1$. Cela implique que $\phi_n(q) = \phi_1(q) = q - 1$ car sinon $|\phi_n(q)| > q - 1$. Donc $n = 1$ et $\mathbb{K} = k$ est commutatif. ■

Chapitre 4

Théorie de Galois

4.1 Introduction

La théorie de Galois naît, vers la fin des années 1820, de la résolution par Evariste Galois (1811-1832) du problème suivant : étant donné un polynôme $P = a_0 + a_1X + \cdots + a_dX^d$ a coefficients rationnels,peut-on résoudre l'équation $P = 0$ par radicaux ? Ce qui, grossièrement, revient à répondre à la question suivante : existe-t-il des formules exprimant les d racines complexes de P en fonction de ses coefficients, formules n'impliquant, outre les opérations élémentaires $+$ et $\times$, que des radicaux $\sqrt[n]{z}$ avec $n \geq 2$?

Pour $d = 2$, la réponse via le discriminant de l'équation, est bien connue. Pour $d = 3$ et $d = 4$ il existe des formules analogues quoique plus compliquées. Lorsque $d \geq 5$, la réponse de Galois est la suivante : il n'existe pas de formule générale, c'est- à-dire de formule qui serait valable pour tous les polynômes de degré d.

L'argument de Galois est révolutionnaire : il s'agit du premier exemple de dictionnaire entre deux théories, en l'occurrence la théorie des corps et la théorie des groupes. Ce n'est pas un dictionnaire parfait, c'est- a-dire qu'il ne concerne pas n'importe quel corps ni n'importe quel groupe, et surtout c'est une théorie relative : elle ne concerne pas les corps en tant que tels mais les extensions d'un corps fixé. Le principe est d'associer au polynôme P un sous-groupe $G(P)$ du groupe des permutations des des racines complexes de P. En langage moderne, il s'agit du groupe des automorphismes du corps $\mathbb{Q}(P)$ engendré par les racines complexes de P. La théorie de Galois montre que les sous-corps de $\mathbb{Q}(P)$ sont en correspondance bijective avec les sous-groupes de $G(P)$. C'est ce qu'on appelle la correspondance de Galois.

Si l'équation générale du d-ième degré n'est pas résoluble par radicaux, certaines équations particulières, comme $X^d = 0$, sont résolubles, et ce quelque soit la valeur de d. On aimerait donc avoir un critère, portant sur P, permettant de décider dans quels cas l' equation $P = 0$ est résoluble par radicaux. La correspondance de Galois permet de traduire la question dans des termes de la théorie des groupes, ce qui donne le critère suivant. L'équation $P = 0$ est résoluble par radicaux si et seulement s'il existe une suite finie décroissante :

$$G(P) = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$$

de sous-groupes de $G(P)$ tels que, pour tout $i > 0$, d'une part G_{i+1} soit distingué dans G_i et d'autre part le groupe quotient G_i/G_{i+1} soit cyclique.

Depuis sa création il y a près de deux siècles, la théorie de Galois qui n'était, à l'origine qu'un moyen de résoudre un problème donné est devenu une théorie jouant un rôle important dans

plusieurs domaines des mathématiques. En particulier, La théorie de Galois classique des extensions finies d'un corps quelconque qui fait l'objet de ce qui va suivre.

4.2 Séparabilité et théorème de l'élément primitif

Soit $\mathbb{K} \subset \mathbb{L}$ une extension. On rappelle que $\mathbb{L}$ est monogène lorsqu'il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(\alpha)$. Il est souvent facile de construire explicitement un élément primitif. Ainsi, prenons $\mathbb{K} = \mathbb{Q}$, et $\mathbb{L} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Montrons que $\mathbb{L} = \mathbb{Q}(\alpha)$, avec $\alpha = \sqrt{2} + \sqrt{3}$. Il est clair qu'il suffit de démontrer que $\sqrt{2}$ et $\sqrt{3}$ sont dans $\mathbb{Q}(\alpha)$, or un calcul direct montre que $\sqrt{2} = \dfrac{\alpha^3 - 9\alpha}{2}$ et que $\sqrt{3} = \dfrac{11\alpha - \alpha^3}{2}$ Le théorème de l'élément primitif qui fait l'objet de cette section, garantit en particulier l'existence d'un élément primitif dans toutes les extension finies de $\mathbb{Q}$. Il est valable plus généralement dans les *extensions séparables* que nous allons maintenant définir.

On dit que le polynôme $P \in \mathbb{K}[X]$ est *séparable* si il n'admet que des racines simples dans un corps de décomposition.

Proposition 4.2.1

1. *P est séparable ssi P et P' sont premiers entre eux.*
2. *Si $\mathbb{K}$ est de caractéristique nulle, tout polynôme irréductible de $\mathbb{K}[X]$ est séparable.*
3. *Si $\mathbb{K}$ est de caractéristique $p > 0$, $P \in \mathbb{K}[X]$ irréductible est inséparable sur $\mathbb{K}$ ssi $P \in \mathbb{K}[X^p]$.*

Preuve. Découle facilement du fait que P et P' ont un facteur commun ssi $P' = 0$ (car dans ce cas $P' \in (P)$). ■

Exemple 4.2.2 *Le polynôme $X^3 - 2$ est séparable sur $\mathbb{Q}$.*

Soit $\mathbb{K} \subset \mathbb{L}$ une extension. Un élément $x \in \mathbb{L}$ est dit séparable si son polynôme minimal est séparable. L'extention $\mathbb{L}$ est dite séparable sur $\mathbb{K}$ si elle est algébrique sur $\mathbb{K}$ et tous ces éléments sont séparables. En particulier, toutes les extensions algébriques sont séparables en caractéristique nulle et le corps fini $\mathbb{F}_q$ avec $q = p^n$ est une extension séparable de $\mathbb{F}_p$ (tout polynôme minimal divise $X^q - X$ qui n'a que des racines simples). Si $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ est une tour d'extensions avec $\mathbb{M}$ séparable sur $\mathbb{K}$, alors $\mathbb{L}$ est séparable sur $\mathbb{K}$ et $\mathbb{M}$ est séparable sur $\mathbb{L}$.

Le théorème de l'élément primitif peut s'énoncer ainsi :

Théorème 4.2.3 (de l'élément primitif) *Soit $\mathbb{K} \subset \mathbb{L}$ une extension de dimension finie n et Ω la clôture algébrique de $\mathbb{K}$. Les quatre conditions suivantes sont équivalentes :*

1. *L'extension $\mathbb{L}$ est séparable sur $\mathbb{K}$*
2. *L'extension est engendrée par des éléments séparables.*
3. *Il existe exactement n morphismes de $\mathbb{L}$ dans Ω laissant invariant $\mathbb{K}$.*
4. *L est une extension monogène engendrée par un élément séparable (appelé élément primitif).*

Pour prouver ce théorème, nous aurons besoin de plusieurs propositions intermédiaires.

Proposition 4.2.4 *On considère la tour d'extensions $\mathbb{K} \subset \mathbb{L} \subset \Omega$ où Ω est la clôture algébrique de $\mathbb{L}$. On suppose qu'il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(\alpha)$ et que $n = [\mathbb{K}(\alpha) : \mathbb{K}]$ est finie.*

1. *Il existe au plus n morphismes de $\mathbb{L}$ dans Ω laissant $\mathbb{K}$ invariant.*
2. *α est séparable ssi ce nombre vaut exactement n.*

Preuve. 1 : Soit P le polynôme minimal de α dans $\mathbb{K}$. Pour toute racine β de P dans Ω, il existe un morphisme de $\mathbb{L}$ dans Ω laissant $\mathbb{K}$ invariant qui à α associe β. Ceci est du au fait que $\mathbb{K}(\alpha) \simeq \mathbb{K}(\beta) \simeq \mathbb{K}[X]/(P)$. Réciproquement, si f est un tel morphisme alors $P(f(\alpha)) = f(P(\alpha))) = 0$. Donc α a pour image par f une racine de P. En conclusion, il existe exactement autant de morphismes que de racines de P dans Ω. Dans le cas général il n'existe donc jamais plus de morphismes que le degré de P, lequel est égal à la dimension de $\mathbb{K}(\alpha)$.

2 : Une condition nécessaire et suffisante d'égalité entre le nombre de morphismes et la dimension de $\mathbb{L}$ est la séparabilité de α. ■

Proposition 4.2.5 *On considère la tour d'extensions $\mathbb{K} \subset \mathbb{L} \subset \Omega$.*

1. *Soit S un ensemble de morphismes distincts de $\mathbb{L}$ dans Ω laissant $\mathbb{K}$ invariant. Alors les éléments de S sont linéairements indépendants sur Ω.*
2. *Supposons $[\mathbb{L} : \mathbb{K}] = n$. Alors, le nombre de morphismes $\mathbb{L}$ dans Ω laissant $\mathbb{K}$ invariant est inférieur à n.*

Preuve. 1 : Soient $f_1, \ldots, f_n \in S$ et $a_1, \ldots, a_n$ dans Ω tels que $\sum_{i=1}^n a_i f_i = 0$. On suppose de plus que n est choisi minimal parmi toutes les combinaisons linéaires nulles d'éléments de S à coefficients dans Ω non tous nuls. On a donc $n \geq 2$ et $a_i \neq 0$ pour tout $i = 1, \ldots, n$. Comme $f_1 \neq f_2$, il existe $y \in \mathbb{L}^\times$ tel que $f_1(y) \neq f_2(y)$. Pour tout $x \in \mathbb{L}$, on a alors $\sum_{i=1}^n a_i f_i(xy) = 0$. Ainsi $\sum_{i=1}^n a_i f_i(x) f_i(y) = 0$ et $\sum_{i=1}^n a_i f_i(x) f_1(y) = 0$. En retranchant ces deux égalités, on obtient $\sum_{i=2}^n a_i f_i(x)(f_i(y) - f_1(y)) = 0$. Cela contredit le choix de n. Les éléments de S sont donc bien linéairement indépendants.

2 : Soit E l'espace vectoriel sur le corps Ω des applications linéaires sur $\mathbb{K}$ de $\mathbb{L}$ dans Ω. Si $B = \{l_1, \ldots, l_n\}$ est une base de $\mathbb{L}$, $f \in E$ est complétement déterminé par $f(B) \in \Omega^n$. Cela montre qu'en tant qu'espace sur Ω, E est de dimension n. En effet l'application

$$\theta : \begin{cases} E \to \Omega^n \\ f \longmapsto (f(l_1), \ldots, f(l_n)) \end{cases}$$

est un isomorphisme de Ω espace vectoriels. D'après le 1, tout sous-ensemble de morphismes de $\mathbb{L}$ dans Ω laissant $\mathbb{K}$ invariant forme une famille libre sur Ω. Donc l'ensemble de tels morphismes est fini et son cardinal est inférieur ou égal à n. ■

Proposition 4.2.6 *Soit $\mathbb{L}$ un corps et Ω sa cloture algébrique. On considère la tour d'extensions $\mathbb{K} \subset \mathbb{K}_1 \subset \mathbb{L} \subset \Omega$.*

1. *Supposons que $\mathbb{L}$ soit une extension finie de $\mathbb{K}_1$. Alors tout morphisme f de $\mathbb{K}_1$ dans Ω laissant invariant $\mathbb{K}$ se prolonge en un morphisme de $\mathbb{L}$ dans Ω laissant $\mathbb{K}$ invariant et laissant fixe une base de $\mathbb{L}$ sur $\mathbb{K}_1$.*
2. *Supposons que $\mathbb{L}$ soit une extension finie de $\mathbb{K}_1$ contenant n_1 morphismes de $\mathbb{L}$ dans Ω laissant invariant $\mathbb{K}_1$ et telle que $\mathbb{K}_1$ soit une extension de $\mathbb{K}$ contenant n_2 morphismes de $\mathbb{K}_1$ dans Ω laissant invariant $\mathbb{K}$. Alors, il existe au moins $n_1 n_2$ morphismes de $\mathbb{L}$ dans Ω laissant $\mathbb{K}$ invariant.*

3. *Supposons que $\mathbb{L}$ soit une extension finie de $\mathbb{K}$ de dimension n. Si $\mathbb{L}$ est engendrée par des éléments séparables, alors il existe exactement n morphismes de $\mathbb{L}$ dans Ω laissant invariant $\mathbb{K}$.*

Preuve. 1 : $\mathbb{K}$ est un espace vectoriel sur $\mathbb{K}_1$ de dimension m. Il existe donc une base $B = (l_1, l_2, \ldots, l_m)$ où $l_1 = 1$ de $\mathbb{L}$ sur $\mathbb{K}_1$. On considère l'application g de $\mathbb{K}_1$ dans Ω définie par

$$g(l) = \sum_{i=1}^{m} f(\lambda_i) l_i \text{ pour tout } l = \sum_{i=1}^{m} \lambda_i l_i \in \mathbb{L} \text{ avec } \lambda_i \in \mathbb{K}_1, i = 1, \ldots, m.$$

Ces égalités montrent que g définit un morphisme qui laisse $\mathbb{K}$ invariant.

2 : Soit $m : \mathbb{K}_1 \to \Omega$ laissant $\mathbb{K}$ invariant et $m' : \mathbb{L} \to \Omega$ laissant $\mathbb{K}_1$ invariant. Il est facile de construire un morphisme $m * m'$ de $\mathbb{L} \to \Omega$ laissant $\mathbb{K}$ invariant. Pour tout $l = \sum_{i=1}^{m} \lambda_i l_i \in \mathbb{L}$ avec $\lambda_i \in \mathbb{K}_1, i = 1, \ldots, m$, posons

$$m * m'(l) = \sum_{i=1}^{m} m'(\lambda_i) m(l_i). \tag{4.1}$$

L'application $m * m'$ est linéaire sur $\mathbb{K}_1$. De plus si $l' = \sum_{j=1}^{m} \lambda'_j l_j$, on a

$$m * m'(ll') = m * m' \left(\sum_{j=1}^{m} \sum_{i=1}^{m} \lambda_i \lambda'_j l_i l_j \right) = \sum_{j=1}^{m} \sum_{i=1}^{m} m'(\lambda_i \lambda'_j) m(l_i l_j) = m * m'(l) \times m * m'(l')$$

puisque m et m' sont des morphismes de corps. L'application $m * m'$ définit donc bien un morphisme de corps. Noter que $l_1 = 1$, donc $m(l_1) = 1$. Il s'ensuit que la restriction $m * m'_{|\mathbb{K}_1}$ coincide avec m'. Donc $m * m'$ laisse $\mathbb{K}$ invariant puisque m' laisse $\mathbb{K} \subset \mathbb{K}_1$ invariant. Cela montre également que si m'_1 et m'_2 sont deux morphismes de $\mathbb{K}_1$ dans Ω, les morphismes $m * m'_1$ et $m * m'_2$ sont disctincts. D'un autre côté, la restriction $m * m'_{|B}$ de m à la base B coincide avec m sur B. Donc si m_1 et m_2 sont deux morphismes de $\mathbb{L}$ dans Ω disctints, $m_1 * m'$ et $m_2 * m'$ sont disctincts ce qui termine la preuve de l'assertion 2.

3 : Montrons la proposition $P(k)$ suivante par récurrence sur k : "Si une extension finie $\mathbb{L}$ d'un corps $\mathbb{K}_1$ est générée par k éléments séparables de $\mathbb{L}$, alors le nombre de morphismes de $\mathbb{L}$ dans Ω laissant invariant $\mathbb{K}_1$ est au moins égal à la dimension de $\mathbb{L}$ sur $\mathbb{K}_1$". Si $k = 0$, la proposition est trivialement vraie. Supposons le résultat vrai pour k et supposons que $\mathbb{L}$ est généré par une famille $\{l_1, \ldots, l_{k+1}\}$ de $k+1$ éléments. Posons $\mathbb{K}_1 = \mathbb{K}(l_{k+1})$. $\mathbb{L}$ est alors une extension de $\mathbb{K}(l_{k+1})$ générée par k éléments séparables. L'hypothèse de récurrence montre qu'il existe au moins $[\mathbb{L} : \mathbb{K}(l_{k+1})]$ morphismes de $\mathbb{L}$ dans Ω laissant invariant $\mathbb{K}(l_{k+1})$. Par ailleurs, d'après la Proposition 4.2.4, le nombre de morphismes de $\mathbb{K}(l_{m+1})$ dans Ω laissant invariant $\mathbb{K}$ vaut exactement $[\mathbb{K}(l_{k+1}) : \mathbb{K}]$ puisque l_{k+1} est séparable. Maintenant, d'après le 2, il existe au moins $[\mathbb{L} : \mathbb{K}(l_{k+1})][\mathbb{K}(l_{m+1}) : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]$ morphismes de $\mathbb{L}$ dans Ω laissant invariant $\mathbb{K}$ ce qui prouve la proposition $P(k)$. Donc si $\mathbb{L}$ est séparable, il existe au moins n morphismes. Or d'après le point 2 de la proposition précédente il en existe au plus n. Cela termine la preuve. ■

Nous aurons encore besoin d'un lemme général sur les espaces vectoriels.

Lemme 4.2.7 *Soit $\mathbb{K}$ un corps **infini** et E un $\mathbb{K}$-espace vectoriel. Soit $F_1, \ldots, F_r$ une famille finie de sous-espaces de E disctincts de E. Alors $\bigcup_{i=1}^{r} F_i \neq E$.*

Preuve. On procède par récurrence sur r. La cas $r = 1$ est immédiat. Supposons par l'absurde que $E = \bigcup_{i=1}^{r} F_i$. Par hypothèse de récurrence, il existe x tel que $x \notin \bigcup_{i=1}^{r-1} F_i$. On a donc $x \in F_r$. Soit $y \notin F_r$. Alors $y \in \bigcup_{i=1}^{r-1} F_i$. L'ensemble des vecteurs $\{x + \lambda y\}$ étant infini puisque $\mathbb{K}$ est infini, il existe $i \in \{1, \ldots, r\}$ et deux scalaires λ et μ tels que $x + \lambda y \in F_i$ et $x + \mu y \in F_i$. Cela implique que x et y sont dans F_i ce qui est impossible compte tenu des hypothèses sur x et y. ■

Proposition 4.2.8 *Soit $\mathbb{L}$ une extension séparable sur $\mathbb{K}$ et Ω sa clôture algébrique. On suppose que $[\mathbb{L} : \mathbb{K}] = n$. Alors il existe $\alpha \in \mathbb{L}$ ayant n images disctinctes par les morphismes de la Proposition 4.2.6.*

Preuve. Si $\mathbb{L}$ est fini, alors le groupe $\mathbb{L}^\times$ est un groupe cyclique. Si α est choisi parmi les éléments générateurs du groupe, il possède n images distinctes par les n morphismes. Sinon, il existerait des morphismes confondus. Cela démontre la proposition dans le cas fini.

Si $\mathbb{L}$ est infini, soit $V_{i,j}$ l'ensemble des vecteurs de $\mathbb{L}$ ayant même image par le i-ième et le j-ième morphisme. C'est un sous-espace vectoriel différent de $\mathbb{L}$. D'après le lemme précédent, l'union des $V_{i,j}$ n'est pas égale à $\mathbb{L}$. Il existe donc un élément α de $\mathbb{L}$ qui n'est élément d'aucun $V_{i,j}$ et la proposition est démontrée. ■

Preuve du théorème de l'élément primitif. Nous sommes maintenant en mesure de terminer la preuve du théorème de l'élémént primitif. Il s'agit de démontrer l'équivalence des quatre assertions du Théorème 4.2.3.

$1 \Longrightarrow 2$: Ce résultat découle de la définition d'une extension séparable et du fait que l'extension est finie.

$2 \Longrightarrow 3$: Il s'agit de l'assertion 3 de la Proposition 4.2.6.

$3 \Longrightarrow 4$: D'après la Proposition ci-dessus, il existe un élément $\alpha \in \mathbb{L}$ ayant n images distinctes par les n morphismes de l'assertion 3. Alors son polynôme minimal est de degré n puisque ces n images en sont des racines. Cela implique que $\mathbb{K}(\alpha)$ est un espace vectoriel inclus dans $\mathbb{L}$ et de même dimension. Ainsi $\mathbb{L} = \mathbb{K}(\alpha)$.

$4 \Longrightarrow 1$: Soit α un générateur de $\mathbb{L}$. D'après la Proposition 4.2.4, comme α est séparable, son polynôme minimal possède n racines disctinctes et il existe exactement n morphismes de $\mathbb{L}$ dans Ω laissant $\mathbb{K}$ invariant. Soit $\beta \in \mathbb{L} = \mathbb{K}(\alpha)$. Il découle de la preuve de la Proposition 4.2.6, que α étant séparable, tout morphisme de $\mathbb{L}$ dans Ω laissant $\mathbb{K}$ invariant se décompose sous la forme $m * m'$ (voir 4.1) où $m : \mathbb{K}(\beta) \to \Omega$ laisset $\mathbb{K}$ invariant et $m' : \mathbb{K}(\alpha) \to \Omega$ laissant $\mathbb{K}(\beta)$ invariant. D'après la Proposition 4.2.4 le nombre q de morphismes m est inférieur ou égal à $[\mathbb{K}(\beta) : \mathbb{K}]$ et le nombre de morphismes m' vaut $[\mathbb{K}(\alpha) : \mathbb{K}(\beta)]$ puisque α est séparable. On a donc

$$n = q[\mathbb{K}(\alpha) : \mathbb{K}(\beta)] \leq [\mathbb{K}(\beta) : \mathbb{K}][\mathbb{K}(\alpha) : \mathbb{K}(\beta)] = n.$$

Donc $[\mathbb{K}(\beta) : \mathbb{K}] = q$ et β est séparable. ■

Corollaire 4.2.9 *Toute extension de dimension finie sur un corps fini ou de caractéristique 0 est monogène.*

Preuve. Cela découle du théorème de l'élément primitif puisqu'une telle extension est séparable. ■

4.3 Correspondence de Galois

Commençons par définir la notion d'extension **normale**.

Proposition 4.3.1 (et définition) *Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie. Si $\mathbb{L}$ vérifie l'une des deux propositions suivantes, on dit qu'elle est **normale**.*

1. *Tout morphisme de corps de $\mathbb{L}$ laissant invariant $\mathbb{K}$ et à valeurs dans Ω, la clôture algébrique de $\mathbb{K}$ contenant $\mathbb{L}$, est un automorphisme de $\mathbb{L}$.*
2. *Tout polynôme irréductible à coefficients dans $\mathbb{K}$ ayant au moins une racine dans $\mathbb{L}$ a toutes ses racines dans $\mathbb{L}$ (ie. que tout polynôme irréductible de $\mathbb{K}[X]$ ayant une racine dans $\mathbb{L}$ se décompose en facteurs linéaires dans $\mathbb{K}[X]$).*

Preuve. $1 \Longrightarrow 2$: Soit $P \in \mathbb{K}[X]$ irréductible ayant au moins une racine α dans $\mathbb{L}$. On a vu dans la preuve de la Proposition 4.2.4 que pour toute racine β de P dans Ω, il existe au moins un morphisme $f : \mathbb{L} \to \Omega$ laissant $\mathbb{K}$ invariant. Comme un tel morphisme est un automorphisme de $\mathbb{L}$, $\beta \in \mathbb{L}$ et donc toutes les racines de P sont dans $\mathbb{L}$.

$2 \Longrightarrow 1$: Soit $f : \mathbb{L} \to \Omega$ un morphisme laissant invariant $\mathbb{K}$. Considérons $\alpha \in \mathbb{L}$ et P son polynôme minimal. Le polynôme P est irréductible et toute ses racines sont dans $\mathbb{L}$ donc $f(\alpha)$ qui est une racine de P est dans $\mathbb{L}$. Cela montre que l'image des morphismes f est dans $\mathbb{L}$. Un tel morphisme étant injectif, il s'agit d'un automorphisme de $\mathbb{L}$. ■

Soit $\mathbb{K} \subset \mathbb{L}$ une extension finie. Le groupe de Galois de $\mathbb{L}$ sur $\mathbb{K}$ est le groupe $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ est le groupe des automorphismes de $\mathbb{L}$ laissant $\mathbb{K}$ invariant. On note alors $\mathbb{K}_0$ le corps des éléments de $\mathbb{L}$ fixés par tous les éléments du groupe de Galois $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$, c'est à dire

$$\mathbb{K}_0 := \{x \in \mathbb{L} \mid g(x) = x, \forall g \in g\}.$$

Exercice 4.3.2 *Vérifier que $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ est bien un groupe et que $\mathbb{K}_0$ est bien un corps.*

L'extension $\mathbb{K} \subset \mathbb{L}$ est *galoisienne* lorsque $\mathbb{K}_0 = \mathbb{K}$.

Exemple 4.3.3

1. *Soit $\mathbb{L} = \mathbb{Q}(\sqrt[3]{2})$. Pour tout $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$, on doit avoir $\sigma(\sqrt[3]{2})^3 = 2$. Donc $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ et le groupe de Galois est réduit à l'identité. On a donc $\mathbb{K}_0 = \mathbb{L}$ et $\mathbb{L}$ n'est pas une extension galoisienne.*
2. *Soit $\mathbb{L} = \mathbb{Q}(\sqrt[3]{2}, i)$ le corps de décomposition de $P(X) = X^4 - 2$ sur $\mathbb{Q}$. $\mathbb{L}$ est une extension normale de $\mathbb{Q}$ de degré 8 et contient (avec $\alpha = \sqrt[3]{2}$), $\pm\alpha, \pm i\alpha, \pm i$. Si $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$, on doit avoir $\sigma(\alpha) \in \{\pm\alpha, \pm i\alpha\}$ et $\sigma(i) = \pm i$ donc on a au plus 8 automorphismes. En définissant σ et τ par $\sigma(\alpha) = i\alpha, \sigma(i) = i$ et $\tau(\alpha) = \alpha, \tau(i) = -i$, on voit que σ est d'ordre 4 et τ est d'ordre 2. De plus $\tau\sigma\tau = \sigma^{-1}$. On en conclut que $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ est isomorphe au groupe diédral d'ordre 8.*

Proposition 4.3.4 *Soit $\mathbb{L}$ une extension algébrique finie de $\mathbb{K}$. Les assertions suivantes sont équivalentes.*

1. *$\mathbb{L}$ est une extension galoisienne de $\mathbb{K}$.*
2. *$\mathbb{L}$ est une extension normale et séparable.*

3. $|\mathrm{Gal}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$.

Preuve. $1 \Longrightarrow 2$: Soit $\alpha \in \mathbb{L}$ et P son polynôme minimal. On note E l'ensemble des racines de P appartenant à $\mathbb{L}$. Soit $Q(X) = \prod_{\beta \in E}(X - \beta)$. Il est clair que pour tout $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, on a $\sigma(Q) = Q$. Donc les coefficients de $Q \in \mathbb{L}[X]$ sont dans $\mathbb{K}_0$. Mais comme $\mathbb{K}_0 = \mathbb{K}$, $Q \in \mathbb{K}[X]$ et annule α. Il s'agit donc d'un multiple de P mais comme $d(Q) \leq d(P)$, on a en fait $P = Q$ et l'extension est normale. Elle est également séparable car $P = Q$ a toutes ses racines distinctes.

$2 \Longrightarrow 1$: Soit $\mathbb{K}_0$ le corps fixe de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Comme $\mathbb{L}$ est séparable, il existe d'après le théorème 4.2.3 $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(\alpha)$. Soit $\beta \in \mathbb{K}_0$. On peut écrire $\beta = P(\alpha)$ avec $P \in \mathbb{K}[X]$ et $d(P) < [\mathbb{L} : \mathbb{K}]$. Posons $Q(X) = P(X) - \beta \in \mathbb{K}_0[X]$ et soit μ le polynôme minimal de α. Si α' est racine de μ, on a $\alpha' \in \mathbb{L}$ car l'extension est normale. De plus, il existe un unique élément $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ tel que $\sigma(\alpha) = \alpha'$. Comme Q est à coefficients dans $\mathbb{K}_0$, il s'ensuit que $Q(\alpha') = Q(\sigma(\alpha)) = \sigma(Q(\alpha)) = 0$. Donc Q' et μ sont deux polynômes à coefficients dans $\mathbb{K}_0$ ayant les même racines dans $\mathbb{L}$. Il existe $c \in \mathbb{K}_0$ telle que $P(X) - \beta = c\mu(X)$. Mais $d(P) < [\mathbb{L} : \mathbb{K}]$ alors que $d(\mu) = [\mathbb{L} : \mathbb{K}]$. On doit donc avoir $c = 0$ et $\beta = P(X) \in \mathbb{K}$. Cela montre que $\mathbb{K}_0 = \mathbb{K}$.

$2 \Longrightarrow 3$: Si L est normale et séparable, il découle immédiatement du théorème 4.2.3 et de la Proposition 4.3.1 que $|\mathrm{Gal}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$.

$3 \Longrightarrow 2$: Supposons $|\mathrm{Gal}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$. Le nombre q de morphismes de $\mathbb{L}$ dans Ω laissant $\mathbb{K}$ invariant est supérieur ou égal à $n = |\mathrm{Gal}(\mathbb{L}/\mathbb{K})|$. Par ailleurs la Proposition 4.2.5, implique que $q \leq n$.Donc $q = n$ et d'après le théorème 4.2.3, l'extension est séparable. De plus, la proposition 4.3.1 implique qu'elle est normale. ■

Corollaire 4.3.5 *Soit $\mathbb{K} \subset \mathbb{L}$ une extension galoisienne. Alors pour tout corps intermédiaire $\mathbb{K} \subset \mathbb{E} \subset \mathbb{L}$, $\mathbb{L}$ est une extension de Galois de $\mathbb{E}$. De plus $\mathrm{Gal}(\mathbb{L}/\mathbb{E})$ est alors un sous-groupe de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$.*

Preuve. L'extension $\mathbb{L}$ reste normale et séparable sur $\mathbb{E}$. Par ailleurs tout automorphisme de $\mathbb{L}$ qui stabilise $\mathbb{E}$ stabilise $\mathbb{K}$. ■

Exemple 4.3.6

1. *Le corps $\mathbb{F}_{p^n}$ est une extension finie de $\mathbb{F}_p$. Par ailleurs l'homomorphisme de Frobenius $F : x \longmapsto x^p$ est dans $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ qui est un groupe d'ordre n. Comme F est d'ordre n, $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ est cyclique d'ordre n engendré par F.*
2. *Soit ξ une racine primitive n-ième de l'unité. Alors $\mathbb{L} = \mathbb{Q}(\xi)$ est une extension galoisienne de $\mathbb{Q}$ de degré $\varphi(n)$. Si $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, σ est déterminé par $\sigma(\xi) = \xi^k$ où k est premier avec n. On a donc $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$.*

Soit $\mathbb{K} \subset \mathbb{L}$ une extension de $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Si H est un sous-groupe de G, on note $\mathbb{L}^H := \{x \in \mathbb{L} \mid h(x) = x, \forall h \in H\}$ le sous-corps des invariants de $\mathbb{L}$ par H. De façon duale, à tout sous-corps $\mathbb{E}$ de $\mathbb{L}$ contenant $\mathbb{K}$, on peut associer $H = \mathrm{Gal}(\mathbb{L}/\mathbb{E})$. Soit $\mathcal{G}$ l'ensemble des sous-groupes de G et $\mathfrak{C}$ l'ensemble des sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$. D'après de ce qui précède, on dispose des deux applications suivantes :

$$\Gamma : \begin{cases} \mathcal{G} \to \mathfrak{C} \\ \Gamma(H) = \mathbb{L}^H \end{cases} \quad \text{et } \Phi : \begin{cases} \mathfrak{C} \to \mathcal{G} \\ \Phi(\mathbb{E}) = H = \mathrm{Gal}(\mathbb{L}/\mathbb{E}) \end{cases} \tag{4.2}$$

toutes deux décroissantes pour l'inclusion. De plus, pour tout $H \in \mathcal{G}$, on a $H \subset \Phi \circ \Gamma(H)$ et pour tout $\mathbb{E} \in \mathfrak{C}$, $\mathbb{E} \subset \Gamma \circ \Phi(\mathbb{E})$.

Exemple 4.3.7 *Pour* $\mathbb{L} = \mathbb{Q}(\sqrt[3]{2})$, *on a vu que* $G = \{id\}$ *et* $\Phi(\mathbb{Q}) = \{id\}$, $\Gamma \circ \Phi(\mathbb{Q}) = \mathbb{L}$. *On voit donc que les applications* Γ *et* Φ *ne sont en général pas réciproques l'une de l'autre. Noter qu'ici,* $\mathbb{L}$ *n'est pas une extension galoisienne de* $\mathbb{Q}$.

Nous admettrons le résultat suivant du à Artin (1898-1962) dont la preuve, un peu technique, utilise essentiellement les mêmes arguments que celle de la Proposition 4.2.5.

Théorème 4.3.8 *Soit* H *un groupe fini d'automorphismes d'un corps* $\mathbb{L}$. *Alors* $\mathbb{L}$ *est une extension finie de* $\mathbb{L}^H$ *et* $[\mathbb{L} : \mathbb{L}^H] = |H|$.

On dit que deux sous-corps $\mathbb{E}$ et $\mathbb{E}'$ de $\mathfrak{C}$ sont *conjugués* sur $\mathbb{K}$ si il existe $\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ tel que $\tau(\mathbb{E}) = \mathbb{E}'$.

Lemme 4.3.9 *Supposons que* $\mathbb{K} \subset \mathbb{L}$ *est galoisienne.*

1. *Pour tout* $\mathbb{E} \in \mathfrak{C}$ *et* $\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, *on a* $\mathrm{Gal}(\mathbb{L}/\tau(\mathbb{E})) = \tau\mathrm{Gal}(\mathbb{L}/\mathbb{E})\tau^{-1}$.
2. *Deux sous-corps* $\mathbb{E}$ *et* $\mathbb{E}'$ *de* $\mathfrak{C}$ *sont* conjugués *sur* $\mathbb{K}$ *si* $\mathrm{Gal}(\mathbb{L}/\mathbb{E})$ *et* $\mathrm{Gal}(\mathbb{L}/\mathbb{E}')$ *sont des sous-groupes conjugués dans* $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$.

Preuve. 1 : Posons $\mathbb{E}' = \tau(\mathbb{E})$. On a $\tau' \in \mathrm{Gal}(\mathbb{L}/\mathbb{E}')$ ssi $\tau'(e') = e'$ pour tout $e' \in \mathbb{E}'$. Mais on peut poser $e' = \tau(e)$ avec $e \in \mathbb{E}$. Ainsi $\tau' \in \mathrm{Gal}(\mathbb{L}/\mathbb{E}')$ ssi $\tau'(\tau(e)) = \tau(e)$ pour tout $e \in \mathbb{E}$, c'est à dire que $\tau^{-1}\tau'\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{E})$ d'où le résultat.

2 : Si $\mathbb{E}$ et $\mathbb{E}'$ de $\mathfrak{C}$ sont *conjugués*, leurs groupes de Galois le sont dans $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ d'après le 1. Réciproquement, supposons qu'il existe $\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ tel que $\mathrm{Gal}(\mathbb{L}/\mathbb{E}') = \tau\mathrm{Gal}(\mathbb{L}/\mathbb{E})\tau^{-1}$. Posons $H = \mathrm{Gal}(\mathbb{L}/\mathbb{E}') = \tau\mathrm{Gal}(\mathbb{L}/\mathbb{E})\tau^{-1} = \mathrm{Gal}(\mathbb{L}/\tau(\mathbb{E}))$ où la dernière égalité découle de 1. L'extension $\mathbb{L}$ étant galoisienne sur $\mathbb{E}'$, on a $\mathbb{L}^H = \mathbb{E}'$. De même $\mathbb{L}$ étant galoisienne sur $\tau(\mathbb{E})$, on a $\mathbb{L}^H = \tau(\mathbb{E})$. D'où $\mathbb{E}' = \tau(\mathbb{E})$. ■

Théorème 4.3.10 *Soit* $\mathbb{K} \subset \mathbb{L}$ *une extension finie et galoisienne et* $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$.

1. $|G| = [\mathbb{L} : \mathbb{K}]$
2. *Les applications* Φ *et* Γ *définies en (4.2) sont bijectives et réciproques l'unes de l'autres.*
3. *Pour tout* $\mathbb{E}$ *dans* $\mathfrak{C}$, *on a*

$$[\mathbb{L} : \mathbb{E}] = |\mathrm{Gal}(\mathbb{L}/\mathbb{E})| \text{ et } [\mathbb{E} : \mathbb{K}] = \frac{|\mathrm{Gal}(\mathbb{L}/\mathbb{K})|}{|\mathrm{Gal}(\mathbb{L}/\mathbb{E})|} = |[\mathrm{Gal}(\mathbb{L}/\mathbb{K}) : \mathrm{Gal}(\mathbb{L}/\mathbb{E})]|.$$

4. $\mathbb{E}$ *est une extension normale de* $\mathbb{K}$ *ssi* $\mathrm{Gal}(\mathbb{L}/\mathbb{E})$ *est un sous-groupe normal (distingué) de* $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. *Dans ce cas,* $\mathrm{Gal}(\mathbb{E}/\mathbb{K}) \simeq \mathrm{Gal}(\mathbb{L}/\mathbb{K})/\mathrm{Gal}(\mathbb{L}/\mathbb{E})$.

Preuve. 1 : Découle de la Proposition 4.3.4.

2 : Comme $\mathbb{E}$ est une extension galoisienne de $\mathbb{L}$, on a $\mathbb{E} = \mathbb{F}^{G'}$ où $G' = \mathrm{Gal}(\mathbb{L}/\mathbb{E}) = \Phi(\mathbb{E})$. Cela signifie que $\mathbb{E} = \Gamma \circ \Phi(\mathbb{E})$. Maintenant pour tout $H \in \mathcal{G}$, on a déjà vu que $H \subset \Phi \circ \Gamma(H)$. Par ailleurs $\mathbb{L}$ reste galoisienne sur $\mathbb{E}' = \Gamma(H) = \mathbb{F}^H$ de groupe de Galois $\Phi \circ \Gamma(H)$. On a donc $[\mathbb{L} : \mathbb{E}'] = |\Phi \circ \Gamma(H)| \geq |H|$. Mais d'après le Théorème 4.3.8, $[\mathbb{L} : \mathbb{E}'] = |H|$. Donc $H = \Phi \circ \Gamma(H)$ ce qui, avec l'égalité $\mathbb{E} = \Gamma \circ \Phi(\mathbb{E})$, montre bien que Φ et Γ sont réciproques l'une de l'autre.

3 : Découle du fait que $\mathbb{E} \subset \mathbb{L}$ est galoisienne et de l'égalité $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{E}][\mathbb{E} : \mathbb{K}]$.

4 : Comme $\mathbb{E}$ est normale, $\mathbb{E}$ est une extension galoisienne de $\mathbb{K}$. Si $\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, $\tau(\mathbb{E}) = \mathbb{E}$. En effet si $\alpha \in \mathbb{E}$ a pour polynôme minimal $P \in \mathbb{K}[X]$, $\tau(\alpha)$ est encore une racine de P donc

appartient à $\mathbb{E}$. On a alors $\mathrm{Gal}(\mathbb{L}/\mathbb{E}) = \mathrm{Gal}(\mathbb{L}/\tau(\mathbb{E})) = \tau\mathrm{Gal}(\mathbb{L}/\mathbb{E})\tau^{-1}$ d'après le lemme précédent. Donc $\mathrm{Gal}(\mathbb{L}/\mathbb{E})$ est distingué dans $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Réciproquement, si $\mathrm{Gal}(\mathbb{L}/\mathbb{E})$ est distingué, on a pour tout $\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, $\mathrm{Gal}(\mathbb{L}/\mathbb{E}) = \mathrm{Gal}(\mathbb{L}/\tau(\mathbb{E}))$. Autrement dit $\Gamma(\mathbb{E}) = \Gamma(\tau(\mathbb{E}))$. Mais comme Γ est une bijection, on a $\tau(\mathbb{E}) = \mathbb{E}$ et donc $\mathbb{E}$ est une extension normale de $\mathbb{K}$. Maintenant, soit $G' = \mathrm{Gal}(\mathbb{E}/\mathbb{K})$. On a vu que la restriction $\tau_{\mathbb{E}}$ de n'importe quel $\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ à $\mathbb{E}$ donnait un élément de G'. Soit θ l'application de G dans G' qui à τ associe $\tau_{\mathbb{E}}$. Il s'agit d'un morphisme surjectif de groupes puisque l'on peut toujours prolonger les morphismes d'après la Proposition 4.2.6. Par ailleurs $\tau \in \ker\theta$ ssi $\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{E})$, d'où $\mathrm{Gal}(\mathbb{E}/\mathbb{K}) \simeq \mathrm{Gal}(\mathbb{L}/\mathbb{K})/\mathrm{Gal}(\mathbb{L}/\mathbb{E})$. ■

4.4 Groupes et équations résolubles

4.4.1 Groupes résolubles

Soit G un groupe. On utilise la notation classique $H \lhd G$ pour signifier que H est un sous-groupe distingué de G, c'est à dire que H est un sous-groupe de G tel que $gHg^{-1} = H$ pour tout $g \in G$. Nous renvoyons à [2] pour les notions de base sur les groupes. On dit que G est *résoluble* si il existe une suite décroissante (pour l'inclusion) finie de sous-groupes

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{r+1} = \{1\} \tag{4.3}$$

telle que chaque quotient $G_i/G_{i+1}, i = 0, \ldots r-1$ est un groupe abélien.

On rappelle que le *groupe dérivé* de G se note $D(G)$. Il s'agit du groupe engendré par les commutateurs $[x, y] = xyx^{-1}y^{-1}$, $x, y \in G$ du groupe G. On vérifie facilement que $D(G) \lhd G$ et que $G/D(G)$ est le plus grand quotient abélien de G, c'est à dire que si G/H avec $H \lhd G$ est abélien, alors, $D(G) \lhd H$. Par ailleurs, $D(G) = \{1\}$ si et seulement si G est abélien. La série dérivée de G est la suite des groupes $D^i(G), i \geq 0$ définie par la relation de récurrence

$$D^0(G) = G \text{ et } D^{i+1}(G) = D(D^i(G)) \text{ pour tout } i \geq 0.$$

Il est clair que l'on a

$$G = D^0(G) \rhd D^1(G_1) \rhd D^2(G) \rhd \cdots .$$

Proposition 4.4.1 *Le groupe G est résoluble si et seulement si il existe un entier r tel que $D^r(G) = 1$.*

Preuve. Il est clair, d'après la définition d'un groupe résoluble, que la condition $D^r(G) = 1$ implique que G est résoluble. Réciproquement, suppose que G est résoluble. Il existe une suite finie comme en (4.3). Comme G_i/G_{i+1} est abélien, $D(G_i) \subset G_{i+1}$ pour tout $i = 0, \ldots, r-1$. Cela entraîne que $D^i(G) \subset G_{i+1}$ pour tout $i = 1, \ldots, r$. Donc $D^r(G) = \{1\}$. ■

Exemple 4.4.2

1. *Pour tout $n \geq 2$, $D(S_n) = A_n$.*
2. *En particulier $D(S_3) = A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ est résoluble puisque $D^2(S_3) = \{1\}$.*
3. *De même $D(S_4) = A_4$. Le sous-groupe $H = \{1, (12)(34), (13(24), (14)(23)\}$ de A_4 est distingué et abélien. Comme A_4 est d'ordre 12, A_4/H est d'ordre 3, il est donc abélien. On dispose donc de la suite décroissante $S_4 \rhd A_4 \rhd A_4/H \rhd \{1\}$. Donc S_4 est résoluble.*

Proposition 4.4.3 *Pour tout $n \geq 5$, on a $D(A_n) = A_n$. Donc S_n n'est pas résoluble pour tout $n \geq 5$.*

Preuve. Soit (abc) un 3-cycle de S_n. Comme $n \geq 5$, on peut choisir dans $\{1, \ldots, n\} \setminus \{a, b, c\}$ deux entiers c et d distincts. Posons

$$\tau = [(adc), (bec)] = (adc)(bec)(acd)(bce) \in D(A_n).$$

On vérifie facilement que $\tau = (abc)$ en calculant sont action sur $\{a, b, c, d, e\}$ (les autres élements étants invariants). Cela montre que tous les trois cycles sont dans $D(A_n)$. Or les 3-cycle engendre A_n. Donc $D(A_n) = A_n$. ■

4.4.2 Equations résolubles par radicaux

Dans la suite de ce chapitre, nous nous limiterons aux sous-corps de $\mathbb{C}$.

Chapitre 5

Introduction à la géométrie algébrique

5.1 Notion de variété algébrique

L'introduction de la géométrie analytique par Descartes permet de faire un lien entre certains objets géométriques et certaines équations algébriques. Ainsi les droites du plan ou les plans de l'espace peuvent être vus comme les ensemble des zéros des polynômes de degré 1 à coefficients dans $\mathbb{R}$ en deux ou trois variables. De même les cercles du plan ou les sphères de l'espace coïncident avec l'ensemble des zéros de polynômes de degré 2 à coefficients dans $\mathbb{R}$. La géométrie algébrique s'intéresse à l'étude des variétés affines, c'est à dire à l'étude de l'ensemble des zéros communs à une famille de polynômes à plusieurs variables sur un corps donné.

Plus précisément, soit $\mathbb{K}$ un corps et $n \geq 1$ un entier. On note $\mathbf{A}= \mathbb{K}[X_1, \ldots, X_n]$. Si $P \in \mathbf{A}$, on dit que $(x_1, \ldots, x_n) \in \mathbb{K}^n$ est un zéro de P si $P(x_1, \ldots, x_n) = 0$. Soit S une partie de $\mathbf{A}$. On note $V(S)$ le sous-ensemble de $\mathbb{K}^n$ des zéros communs à tous les éléments de S. Un tel sous-ensemble s'appelle une *variété (algébrique) affine* de $\mathbb{K}^n$.

Exemple 5.1.1

1. *On a $V(1) = \emptyset$ et $V(0) = \mathbb{K}^n$, le vide et l'espace sont des variétés de $\mathbb{K}^n$.*
2. *Le point $M = \{x = (x_1, \ldots, x_n)\}$ est une variété correspondant à $S = \{X_1 - x_1, \ldots, X_n - x_n\}$.*
3. *Tout sous-espace de $\mathbb{K}^n$ est une sous-variété.*

Exercice 5.1.2 *L'ensemble des x tel que $\sin x = 0$ n'est pas une sous-variété affine de $\mathbb{R}^2$.*

Les propriétés suivantes se vérifient aisément :

1. Si $S \subset S'$, alors $V(S) \supset V(S')$.
2. Si $\langle S \rangle$ est l'idéal engendré par S, $V(S) = V(\langle S \rangle)$.
3. L'anneau A étant noetherien (Theorème 2.3.2), l'idéal $\langle S \rangle$ est engendré par un nombre fini de polynômes $P_1, \ldots, P_n$ de sorte que $V(S) = V(P_1, \ldots, P_n)$. Toute sous-variété de $\mathbb{K}^n$ peut donc être définie par un nombre fini d'équations.
4. On a $V(S_1) \cap V(S_2) = V(S_1 \cup S_2)$. Plus généralement l'intersection d'une famille de sous-variétés est une sous-variété.
5. On a $V(S_1) \cup V(S_2) = V(S_1 S_2)$. Plus généralement la réunion d'une famille finie de sous-variétés est une sous-variété.

6. Il découle du 5 que tout sous-ensemble fini de $\mathbb{K}^n$ est une sous-variété.
7. On peut définir une topologie (la *topologie de Zariski*) sur $\mathbb{K}^n$ en prenant comme fermés l'ensemble des sous-variétés.

5.2 Idéal associé à une variété affine

Une variété V peut être définie par différents ensembles d'équations. Il existe néanmoins une façon naturelle d'associer un idéal à n'importe quel sous-ensemble V de $\mathbb{K}^n$ (pas forcément à une variété). On Note $I(V)$ *l'idéal de* $\mathbf{A}$ *des polynômes qui s'annulent en tous les points de* V. On a les propriétés suivantes :

1. $V \subset V(I(V))$ avec égalité ssi V est une variété affine. En fait, $V(I(V))$ est l'adhérence de V pour la topologie de Zariski.
2. $S \subset I(V(S))$ mais il n'y a en général pas égalité même lorsque S est un idéal. Par exemple $I(V(X^2)) = (X)$. La relation entre les idéaux I et $I(V(I))$ fait l'objet du *Nullstellensatz* et sera étudiée dans le prochain paragraphe.
3. L'anneau $\mathbf{A}$ étant noetherien, toute suite décroissante (pour l'inclusion) de sous-variétés est stationnaire (la suite des idéaux associés est croissante).
4. Si $V = V_1 \cup V_2$ où V_1, V_2 sont deux variétés affines, $I(V) = I(V_1) \cap I(V_2)$.
5. Si $V = V_1 \cap V_2$ où V_1, V_2 sont deux variétés affines, $I(V) \supset I(V_1)I(V_2)$.

La sous-variété de $\mathbb{R}^2$ définie par $X_1X_2 = 0$ se décompose en les deux sous-variétés $X_1 = 0$ et $X_2 = 0$ qui ne peuvent être à leur tour décomposées. On dit qu'une sous-variété est irréductible si elle n'est pas vide et n'est pas la réunion de deux fermés distincts (pour la topologie de Zariski).

Proposition 5.2.1 *La sous-variété V est irréductible ssi $I(V)$ est un idéal premier.*

Preuve. Supposons V irréductible et soit P_1P_2 dans $I(V)$. On a $V \subset V(P_1P_2) = V(P_1) \cup V(P_2)$. Donc V est la réunion des fermés $V \cap V(P_1)$ et $V \cap V(P_2)$. Mais comme V est irréductible, on a $V = V \cap V(P_1)$ ou $V = V \cap V(P_2)$ c'est à dire $P_1 \in I(V)$ ou $P_2 \in I(V)$.

Réciproquement, supposons que $I(V)$ est un idéal premier et que $V = V_1 \cup V_2$ est la réunion de deux fermés propres. Alors pour $i = 1, 2$, il existe un polynôme P_i tel que P_i soit nul sur V_i mais pas sur V. Mais alors P_1P_2 s'annule sur V donc $P_1P_2 \in I(V)$ ce qui implique que P_1 ou P_2 est dans $I(V)$. On obtient bien une contradiction. ■

La condition de la proposition revient à dire que $\mathbf{A}(V) := \mathbf{A}/I(V)$ est un idéal intègre. La proposition implique donc que $\mathbb{K}^n$ est irréductible puisque $I(\mathbb{K}^n) = \{0\}$.

Théorème 5.2.2 *Toute sous-variété affine V non vide se décompose de façon unique (à permutation près) en une r éunion finie de sous-variétés affines irréductibles, non contenues l'une dans l'autre.*

Preuve. Existence : Supposons qu'il existe une sous-variété V non vide qui ne se décompose pas en une réunion finie d'irréductibles. D'après le point 3 ci-dessus, l'ensemble de ces sous-variétés admet un élément minimal V , qui est forcément réductible. On écrit $V = V_1 \cup V_2$ avec V_1, V_2 fermés non vides et distincts de V. Par minimalité, V_i est réunion finie d'irréductibles, d'où contradiction.

L'unicité est laissée en exercice. ■

Les sous-variétés irréductibles $V_1, \ldots, V_r$ apparaissant dans la décomposition du théorème sont appelées les composantes irréductibles de la sous-variété affine V. On a $I(V) = I(V_1) \cap I(V_2) \cap \cdots \cap I(V_r)$ et les idéaux $I(V_i)$ sont premiers.

5.3 Théorème des zéros de Hilbert

Le théorème des zéros de Hilbert, aussi appelé *Nullstellensatz*, précise le lien entre les idéaux et les variétés algébriques. Il a été démontré par le mathématicien allemand David Hilbert. Commençons par un lemme général concernant les algèbres sur un anneau. On se donne un corps $\mathbb{K}$ et $\mathcal{A}$ une $\mathbb{K}$-algèbre, c'est à dire que $\mathcal{A}$ est un anneau muni d'une structure de $\mathbb{K}$ espace vectoriel. On dit que $\mathcal{A}$ est de type fini, si il existe un entier $n \in \mathbb{N}$ et des éléments $x_1, \ldots, x_n$ dans $\mathcal{A}$ tels que tout élément de $\mathcal{A}$ s'écrive comme un polynôme en $x_1, \ldots, x_n$ à coefficients dans $\mathbb{K}$. Autrement dit $\mathcal{A}$ est de type fini si $\mathcal{A} \simeq \mathbb{K}[X_1, \ldots, X_n]/I$ où I est un idéal de $\mathbb{K}[X_1, \ldots, X_n]/I$.

Soient $A \subset B$ deux anneaux. On dit que B est entier sur A si tout élément de B est solution d'une équation polynomiale à coefficients dans A.

Lemme 5.3.1 *Soient $A \subset B$ deux anneaux tels que B est entier sur A. Si B est un corps, alors A est un corps.*

Preuve. Soit x un élément non nul de A. Son inverse y dans B est entier sur A, donc on a une relation du type $y^m + a_{m-1}y^{m-1} + \cdots + a_1 y + a_0 = 0$ avec $m \in \mathbb{N}$ et $a_i \in A$). En multipliant cette relation par x^{m-1}, on obtient $y = -(a_{m-1} + \cdots + a_1 x^{m-2} + a_0 x^{m-1})$ et donc $y \in A$. ■

Proposition 5.3.2 *Soit $\mathbb{K}$ un corps et soit $\mathcal{A}$ une $\mathbb{K}$-algèbre de type fini. Si $\mathcal{A}$ est un corps, alors $\mathcal{A}$ est une extension algébrique finie de $\mathbb{K}$.*

Preuve. Pour tout $n \in \mathbb{N}$, notons $P(n)$ la propriété suivante : "Si $\mathbb{K}$ est un corps et si $\mathcal{A}$ est une $\mathbb{K}$-algèbre de type fini engendrée par n éléments qui est un corps, alors $\mathcal{A}$ est une extension algèbrique finie (donc un corps) de $\mathbb{K}$ ". On raisonne par récurrence sur n. La propriété $P(0)$ est vraie car dans ce cas $\mathcal{A} = \mathbb{K}$. Si $n = 1$, on a $\mathcal{A} = \mathbb{K}[x_1]$. Si x_1 était transcendant sur $\mathbb{K}$, on aurait $\mathcal{A} \simeq \mathbb{K}[X]$ qui nest pas un corps. Donc x_1 est algébrique et par suite $\mathcal{A}$ est une extension algébrique finie de $\mathbb{K}$.

Supposons maintenant que $n > 1$ et que $P(n-1)$ est vraie. Soit $\mathcal{A}$ une $\mathbb{K}$-algèbre de type fini engendrée en tant que $\mathbb{K}$-algèbre par des éléments $x_1, \ldots, x_n$ de $\mathcal{A}$. On a donc $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_n]$. Soit $A = \mathbb{K}[x_1]$ et soit $\mathbb{L}$ le corps des fractions de A ; on a $\mathbb{L} \subset \mathcal{A}$ (car $\mathcal{A}$ est un corps) de sorte que $\mathcal{A}$ est aussi une $\mathbb{L}$-algèbre de type fini engendrée par $n-1$ éléments. Par hypothèse de récurrence, $\mathcal{A}$ est une extension algébrique finie de $\mathbb{L}$. En particulier, les éléments x_i, pour $i = 2, \ldots, n$, sont algébriques sur $\mathbb{L}$, donc il existe des polynomes unitaires $P_2, \ldots, P_n$ dans $\mathbb{L}[X]$ tels que $P_i(x_i) = 0$ pour tout $i = 2, \ldots, n$. Soit $\delta \in \mathbb{K}[x_1]$ le produit de tous les dénominateurs des coefficients des P_i, de sorte que les éléments $x_2, \ldots, x_n$ sont entiers sur $A_\delta = A[1/\delta]$. Ainsi, $\mathcal{A}$ est entier sur A_δ (puisque ses générateurs le sont tous) et comme $A_\delta \subset \mathcal{A}$ (car $\mathcal{A}$ est un corps), on déduit du lemme précédent que A_δ est un corps. Maintenant, supposons que x_1 est transcendant sur $\mathbb{K}$. Alors $A_\delta \simeq \mathbb{K}[X][1/P]$, où $P \in \mathbb{K}[X]$ est un polynome non nul. L´elément $1 - XP$ est non nul dans A_δ (P est un polynôme en X) et il n'est pas inversible (car si il existe Q dans A_δ tel que $(1 - XP)Q = 1$, en substituant $1/P$ à X on a une contradiction). Ceci contredit le fait que A_δ est un corps. Donc x_1 est algébrique

sur $\mathbb{K}$. Par suite $\mathbb{L}$ est une extension algébrique finie de $\mathbb{K}$. Or on sait que $\mathcal{A}$ est une extension algébrique finie de $\mathbb{L}$ ce qui conduit au résultat. ■

Théorème 5.3.3 (Nullstellensatz faible I) *Soit $\mathbb{K}$ un corps algébriquement clos. Les idéaux maximaux de $\mathbb{K}[X_1, \ldots, X_n]$ propres (i.e distincts de $\mathbb{K}[X_1, \ldots, X_n]$) sont de la forme*

$$J = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$$

où les a_i sont des éléments de $\mathbb{K}$.

Preuve. Montrons d'abord que les idéaux de la forme $J = \langle X - a_1, \ldots, X - a_n \rangle$ sont maximaux. L' application $\theta : \mathbb{K}[X_1, \ldots, X_n] \to \mathbb{K}$ définie par $\theta(P) = P(a_1, \ldots, a_n)$ est un morphisme surjectif d'anneaux. Soit $P \in \ker \theta$. En écrivant la division euclidienne de P par $X_1 - a_1$, puis celle du reste par $X_2 - a_2$ etc. on obtient $P = (X_1 - a_1)Q_1 + \cdots + (X_n - a_n)Q_n + P(a_1, \ldots, a_n)$ avec $Q_j \in \mathbb{K}[X_j, \ldots, X_n]$ pour $j = 1, \ldots, n$. Comme $P \in \ker \theta$, on en déduit que $P \in J$. Donc $\ker \theta \subset J$. L'inclusion réciproque est évidente, donc $\ker \theta = J$. On en déduit que $\mathbb{K}[X_1, \ldots, X_n]/I \simeq \mathbb{K}$, donc J est maximal. Noter que ce résultat reste vrai même si $\mathbb{K}$ n'est pas algébriquement clos.

Soit M un idéal maximal de $\mathbb{K}[X_1, \ldots, X_n]$ distinct de $\mathbb{K}[X_1, \ldots, X_n]$. Alors $\mathbb{K}[X_1, \ldots, X_n]/M$ est une $\mathbb{K}$-algèbre de type fini qui est un corps. D'après la proposition précédente, c'est une extension algébrique finie de $\mathbb{K}$ et comme $\mathbb{K}$ est algébriquement clos, on a $\mathbb{K}[X_1, \ldots, X_n]/M = \mathbb{K}$. Pour tout $i = 1, \ldots, n$, il existe donc $a_i \in \mathbb{K}$ tel que $X_i - a_i \in M$. Ainsi, l'idéal $J = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ est contenu dans M. Mais comme on vient de le voir, J est maximal. Donc $J = M$. ■

Théorème 5.3.4 (Nullstellensatz faible II) *Soit $\mathbb{K}$ un corps algébriquement clos et soit I un idéal de $\mathbb{K}[X_1, \ldots, X_n]$. On a $V(I) = \emptyset$ ssi $I = \mathbb{K}[X_1, \ldots, X_n]$.*

Preuve. Il est clair que $V(I) = \emptyset$ si $1 \in I$. Réciproquement, si $I \neq \mathbb{K}[X_1, \ldots, X_n]$, il existe un idéal maximal M qui contient I. Daprès le théorème précédent, M est de la forme $M = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$. Pour tout $P \in I$, on a $P \in M$, donc $P(a_1, \ldots, a_n) = 0$, ce qui montre que $(a_1, \ldots, a_n) \in V(I)$. Ainsi, $V(I) \neq \emptyset$. ■

Le théorème suivant précise la relation entre I et $I(V(I))$.

Théorème 5.3.5 (Nullstellensatz) *Soit $\mathbb{K}$ un corps algébriquement clos et soit I un idéal de $\mathbb{K}[X_1, \ldots, X_n]$. Alors $I(V(I)) = \sqrt{I} = \{P \mid \exists n \in \mathbb{N}, P^n \in I\}$.*

Preuve. Soit $P \in \sqrt{I}$. Il existe un entier $r > 1$ tel que $P^r \in I$. Par conséquent, pour tout $x \in V(I)$, on a $P^r(x) = 0$ et donc $P(x) = 0$. Ainsi, $P \in I(V(I))$. Réciproquement, soit $P \in I(V(I))$. Dans $\mathbb{K}[X_1, \ldots, X_n, T]$, l'idéal J engendré par I et $1 - TP$ définit un ensemble algébrique **vide** car si $x \in V(J)$, on a $x \in V(I)$, donc $P(x) = 0$ (car $P \in I(V(I))$. Par suite, $(1 - TP)(x) = 1 \neq 0$. Posons $I = \langle P_1, \ldots, P_m \rangle$ où les P_i sont dans $\mathbb{K}[X_1, \ldots, X_n]$ (c'est possible car $\mathbb{K}[X_1, \ldots, X_n]$ est noetherien). D'après le théorème précédent, on a $J = \mathbb{K}[X_1, \ldots, X_n, T]$ et donc il existe des polynomes $Q_0, \ldots, Q_m \in \mathbb{K}[X_1, \ldots, X_n, T]$ tels que

$$\sum_{i=1}^{m} P_i Q_i + (1 - TP)Q_0 = 1.$$

En substituant $1/P$ à T dans cette égalité, on obtient dans $\mathbb{K}[X_1, \ldots, X_n, T]$

$$\sum_{i=1}^{m} P_i(X_1, \ldots, X_m) Q_i(X_1, \ldots, X_m, 1/P) = 1.$$

Il existe un entier $r > 1$ assez grand pour que $P^r Q_j(X_1, \ldots, X_n, 1/P)$ soit dans $\mathbb{K}[X_1, \ldots, X_n]$ pour tout $j = 1, \ldots, n$. On a alors

$$P^r = \sum P_i(X_1, \ldots, X_m) Q_i(X_1, \ldots, X_m, 1/P) P^r.$$

Donc $P^r \in I$. ■

Bibliographie

[1] J. Calais, Extension de corps, théorie de Galois, Ellipse (2006).

[2] F. Combes, Algèbre et géométrie, Bréal (2004).

[3] S. Lang, Algèbre, Dunod (2004).

[4] S. Mac Lane et G. Birkoff, algèbre tomes I et II, Gauthiers Villars (1971).

[5] D. Perrin, Cours d'algère, Ellipse (1996).

[6] J-P Serre, Cours d'arithmétique, PUF (1995)