Cours “Anneaux”

L3 Mathématiques

Université de Poitiers

Olivier Frécon

Année 2023-2024 – 2e version

Table des matières

Chapitre 1

Introduction

Ce polycopié est consacré au cours “Anneaux” donné aux étudiant·es de 3^e année de la licence de mathématiques de l'université de Poitiers durant le second semestre des années universitaires 2022-2023 et 2023-2024. Ce cours est d'une durée de 20h accompagné de 30h de Travaux Dirigés donnés par Lionel Ducos.

Le programme est le suivant :
Anneaux, idéaux, morphismes, quotient d'un anneau, théorèmes d'isomorphisme. Idéaux premiers et maximaux. Corps et corps de fractions. Caractéristique d'un anneau. Anneau des polynômes. Anneaux euclidiens, principaux et factoriels.

Le polycopié comprend quelques parties hors programme, notamment celles consacrées à l'axiome du choix et aux anneaux noethériens. Les étudiant·es sont invité·es à les lire attentivement pour leur culture mathématique, en sachant qu'elles ne seront pas aux programme de l'épreuve de contrôle continu ni de l'examen terminal.

Chapitre 2

Anneaux : Généralités

2.1 Définitions

De nombreux ensembles que l'on connaît ne sont pas munies d'une seule loi de composition interne, mais souvent de deux. C'est le cas, par exemple, de $\mathbb{Z}$, $\mathbb{Q}$ *et* $\mathbb{R}$ *qui sont munies de l'addition et de la multiplication (la soustraction et la division se déduisent de ces deux-là). La structure algébrique munie de deux lois de composition interne la plus souvent rencontrée est l'*anneau *:*

Définition 2.1.1 –

Remarque 2.1.2 –

— La première loi est traditionnellement notée $+$ et, pour tout $x \in A$, on note $-x$ le symétrique de x pour la loi $+$ et on dit que $-x$ est l'*opposé* de x. On note aussi $x - y = x + (-y)$ pour tout $(x, y) \in A \times A$. De plus, l'élément neutre de $(A, +)$ se note généralement 0 (*ou* 0_A).
On réserve généralement le mot inverse *au symétrique d'un élément* x *de* A *pour la loi* $\times$ *(lorsqu'il existe).*

— La seconde loi, lorsqu'elle est notée $\cdot$ ou $\times$, peut être omise : on peut écrire xy au lieu de $x \times y$ ou $x \cdot y$.
— Il y a unicité de l'élément neutre pour la seconde loi, il est généralement noté 1 (ou 1_A).
[En effet, si e et f sont deux éléments neutres pour la seconde loi, on a $e = e \times f = f$.]
— Par convention, si $(A, +, \times)$ est un anneau, alors la loi $\times$ est prioritaire par rapport à la loi $+$, ce qui permet de ne pas écrire certaines parenthèses :

pour tout $(x, y, z) \in A \times A \times A$, $(x \times y) + z = x \times y + z$ *et* $x + (y \times z) = x + y \times z$

— Si $(A, +, \times)$ est un anneau alors on a $0 \times x = x \times 0 = 0$ pour tout $x \in A$.
[En effet, par distributivité de la loi $\times$ par rapport à $+$, on a

$$0 \times x = (0 - 0) \times x = 0 \times x - 0 \times x = 0$$

et, de même, $x \times 0 = 0$.].
— En particulier, si $1_A = 0_A$, alors $A = \{0_A\}$ (*car, alors, tout $x \in A$ vérifie $x = 1_A x = 0_A x = 0_A$*). Cet anneau est appelé *anneau nul* ou *anneau trivial*.
— Si $(A, +, \times)$ est un anneau alors, pour tout $(x, y) \in A$, l'opposé de $x \times y$ est $-(x \times y) = (-x) \times y = x \times (-y)$.
[En effet, d'après ci-dessus on a $0 \times y = 0$ et $x \times 0 = 0$ donc, par distributivité de $\times$: $x \times y + (-x) \times y = (x + (-x)) \times y = 0 \times y = 0$, d'où $-(x \times y) = (-x) \times y$. De même on obtient $-(x \times y) = x \times (-y)$].

Exemples 2.1.3 –

(a) $(\mathbb{Z}, +, \times)$ est un anneau.

De même, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux.
(b) Pour tout entier $n \in \mathbb{N}^*$ et tout anneau $(A, +, \times)$, l'ensemble des matrices $\mathscr{M}_n(A)$, muni de l'addition $+$ et de la multiplication $\cdot$, est un anneau.

(c) Si $(G, +)$ est un groupe abélien d'élément neutre noté e, on considère l'ensemble $E = \mathrm{End}(G)$ des endomorphismes du groupe G. On muni E d'une loi notée $+_E$ et définie par $(f +_E g)(x) = f(x) + g(x)$ pour tout $x \in G$ et tous f et g dans E. On note 0_E l'élément de E qui vérifie $0_E(x) = e$ pour tout $x \in G$.

(d) Pour tout ensemble E, le triplet $(\mathscr{P}(E), \Delta, \cap)$ est un anneau, où $\mathscr{P}(E)$ est l'ensemble des parties de E et où, pour toutes parties A et B de E, on note $A\Delta B = (A \cup B) \setminus (A \cap B)$. L'élément neutre pour Δ est l'ensemble vide $\emptyset$ et l'élément neutre pour $\cap$ est E.

(e) Si $(A_1, +_1, \times_1)$,..., $(A_n, +_n, \times_n)$ forment une famille de $n \in \mathbb{N}^*$ anneaux, alors le produit direct $A_1 \times \cdots \times A_n$ muni de la somme naturelle et du produit naturel est un anneau. Son élément neutre pour l'addition est $(0_{A_1}, \cdots, 0_{A_n})$ et celui pour la multiplication est $(1_{A_1}, \cdots, 1_{A_n})$.

Notation 2.1.4 – *Soit $(A, +, \times)$ un anneau. Pour tout élément x de A on note :*
— $0x = 0_A$, $(n+1)x = nx + x$ *pour tout* $n \in \mathbb{N}$, *puis* $(-n)x = -(nx)$ *pour tout* $n \in \mathbb{N}$;
— $x^0 = 1_A$ *et* $x^{n+1} = x^n \times x$ *pour tout* $n \in \mathbb{N}$.

Remarque 2.1.5 –

2.2 Corps

Définition 2.2.1 – *Soit $(A, +, \times)$ un anneau. Un élément x de A est dit* inversible *s'il existe $y \in A$ tel que $x \times y = y \times x = 1_A$.*

Remarque 2.2.2 –

Définition 2.2.3 – *Un* corps *est un anneau non nul dans lequel tous les éléments non nuls sont inversibles.*

Remarque 2.2.4 – Généralement, les corps auxquels on s'intéresse sont *commutatifs* : tous leurs éléments x et y vérifient $x \times y = y \times x$. Cependant il existe des corps non commutatifs, l'exemple le plus connu étant le *corps* $\mathbb{H}$ *des quarternions.*

Théorème 2.2.5 – **(Théorème de Wedderburn)** *Tout corps fini est commutatif.*

Démonstration – ADMIS, au moins provisoirement, il sera démontré si le temps le permet. □

Proposition 2.2.6 – *Soit A un ensemble muni de deux lois de composition internes $+$ et $\times$. Le triplet $(A, +, \times)$ est un corps si et seulement si*

— $(A, +)$ *est un groupe abélien ;*
— $(A^*, \times)$ *est un groupe* - où $(A^*, \times)$ est l'ensemble des éléments non nuls de A muni de la restriction de la loi $\times$ à A^* *;*
— *la loi* $\times$ *est distributive par rapport à* $+$*.*

Démonstration –

□

2.3 Sous-anneaux

Définition 2.3.1 – *Un* sous-anneau *d'un anneau* $(A, +, \times)$ *est une partie* B *de* A *qui, munie des restrictions des lois* $+$ *et* $\times$ *à* B *est un anneau ayant les mêmes élément neutres pour* $+$ *et* $\times$ *que* $(A, +, \times)$*.*

Remarque 2.3.2 – Soit $(A, +, \times)$ un anneau.
— A est un sous-anneau de $(A, +, \times)$.
— La partie $B = \{0_A\}$ n'est un sous-anneau de $(A, +, \times)$ que si A est l'anneau nul.

Proposition 2.3.3 –

Démonstration –

□

Corollaire 2.3.4 –

Démonstration –

□

Corollaire 2.3.5 –

Définition 2.3.6 – *Soient* $(A, +, \times)$ *un anneau et* X *est une partie quelconque de* A*. Le plus petit sous-anneau de* A *contenant* X *est appelé* sous-anneau de A engendré par X*.*

Exemples 2.3.7 –

Définition 2.3.8 – *Un* sous-corps *d'un corps* $(K, +, \times)$ *est une partie* L *de* K *qui, munie des restrictions des lois* $+$ *et* $\times$ *à* L *est un corps.*

Remarque 2.3.9 – Un sous-corps L d'un corps $(K, +, \times)$ contient les éléments neutres 0_K et 1_K. C'est donc un sous-anneau. En revanche un sous-anneau d'un corps n'est pas forcément un sous-corps : par exemple $\mathbb{Z}$ n'est pas un sous-corps de $\mathbb{Q}$.

Exemples 2.3.10 –

- $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$;
- $\mathbb{C}$ est un sous-corps du corps des quaternions $\mathbb{H}$.

2.4 Idéaux

Définition 2.4.1 –

Remarque 2.4.2 –

- Tout idéal contient 0_A.
- $\{0_A\}$ et A sont des idéaux de A (*un idéal différent de A est dit* propre).
- Le seul idéal de A qui contient 1_A est A. Plus généralement, si un élément inversible de A appartient à un idéal I de A, alors $I = A$.
- Par conséquent, si A est un corps, ses seuls idéaux sont $\{0_A\}$ et A.
  [*Nous verrons que cette propriété caractérise les corps parmi les* anneaux commutatifs *que nous étudierons plus loin. En revanche, dans le contexte général, cette propriété ne caractérise pas les corps : si A est un corps, les seuls idéaux de $\mathscr{M}_n(A)$ sont $\{0_{\mathscr{M}_n(A)}\}$ et $\mathscr{M}_n(A)$, pourtant $\mathscr{M}_n(A)$ n'est pas un corps.*]

Exemples 2.4.3 – Les idéaux de $\mathbb{Z}$ sont les ensembles de la forme $n\mathbb{Z}$ pour $n \in \mathbb{N}$.

Lemme 2.4.4 – *Si E est un ensemble et $(I_k)_{k\in E}$ est une famille, éventuellement infinie, d'idéaux d'un anneau $(A, +, \times)$, alors $\cap_{k\in E} I_k$ est aussi un idéal de A.*

Démonstration –

□

Corollaire 2.4.5 – *Soit $(A, +, \times)$ un anneaux. Si X est une partie quelconque de A, alors l'intersection des idéaux de A contenant X est un idéal de A, c'est le plus petit idéal de A contenant X.*

Définition 2.4.6 –

Lorsque $X = \{x\}$ est un singleton ou $X = \{x_1, \ldots, x_n\}$ ou ne contient qu'un nombre fini d'éléments, on note plutôt (x) ou $(x_1, \ldots, x_n)$ l'idéal engendré par X.

Exemples 2.4.7 –

Proposition 2.4.8 – *Soit $(A, +, \times)$ un anneaux. Si I et J sont deux idéaux de A, alors l'ensemble $I + J = \{x + y\,;\, x \in I,\ y \in J\}$ est un idéal de A. De plus, on a $I + J$ est le plus petit idéal de A contenant I et J : $I + J = (I \cup J)$.*

Démonstration –

□

Définition 2.4.9 – *Soit $(A, +, \times)$ un anneaux. Si I et J sont deux idéaux de A, on note IJ l'idéal de A engendré par les produits de la forme xy pour $x \in I$ et $y \in J$.*

Remarque 2.4.10 –

— En général, pour des idéaux Iet J quelconques, on a $IJ \neq \{xy \ ; \ x \in I, \ y \in J\}$.

— Pour des idéaux Iet J quelconques, on a $xy \in I \cap J$ pour tous $x \in I$ et $y \in J$, donc comme $I \cap J$ est un idéal de A, on a $IJ \subseteq I \cap J$.

Lemme 2.4.11 – *Soit $(A, +, \times)$ un anneaux. Si I et J sont deux idéaux de A, alors*

$$IJ = \{x_1y_1 + \cdots + x_ny_n \ |; \ n \in \mathbb{N}^*, \ x_1, \ldots, x_n \in I, \ y_1, \ldots, y_n \in J\}.$$

Démonstration – On note $P = \{x_1y_1 + \cdots + x_ny_n \mid n \in \mathbb{N}^*, \ x_1, \ldots, x_n \in I, \ y_1, \ldots, y_n \in J\}$. Comme, pour tout $n \in \mathbb{N}^*$, tous $x_1, \ldots, x_n \in I$ et tous $y_1, \ldots, y_n \in J$, on a $x_iy_i \in IJ$ pour chaque $i \in \{1, \ldots, n\}$, on a $P \subseteq IJ$. De plus P contient tous les produits de la forme xy pour $x \in I$ et $y \in J$, donc il suffit de montrer que P est un idéal de A.

D'abord P contient $0_A = 0_A0_A \in IJ$, donc P est non vide. Soient $n \in \mathbb{N}^*$, $m \in \mathbb{N}^*$, $x_1, \ldots, x_n, u_1, \ldots, u_m \in I$ et $y_1, \ldots, y_n, v_1, \ldots, v_m \in J$. On note $x = x_1y_1 + \cdots + x_ny_n$ et $y = u_1v_1 + \cdots + u_mv_m$. Alors on a $-u_1, \ldots, -u_m \in I$ donc $x - y = x_1y_1 + \cdots + x_ny_n + (-u_1)v_1 + \cdots + (-u_m)v_m$ appartient à P et $(P, +$ est un sous-groupe de $A, +)$.

Aussi, pour tout $a \in A$, on a $ax_1, \ldots, ax_n \in I$ et $y_1a, \ldots, y_na \in J$, donc $ax = (ax_1)y_1 + \cdots + (ax_n)y_n$ et $xa = x_1(y_1a) + \cdots + x_n(y_na)$ appartiennent à P, et P est bien un idéal de A. $\square$

2.5 Anneaux quotients

Remarque 2.5.1 – Les sous-anneaux et idéaux des anneaux rappellent les sous-groupes et sous-groupes normaux des groupes. En effet, nous pouvons comparer les situations :

	Groupes	Anneaux	Corps
Sous-structures	Sous-groupes	Sous-anneaux	Sous-corps
Objets permettant de quotienter	Sous-groupes normaux	Idéaux	$\{0\}$

Notons les principales différences :
— pour les groupes, les objets permettant de quotienter sont des sous-structures (*les sous-groupes normaux sont des sous-groupes*) ;
— pour les anneaux, à l'exception de l'anneau entier, les objets permettant de quotienter ne sont pas des sous-structures (*les idéaux propres ne sont jamais des sous-anneaux*) ;
— les corps n'admettent pas de quotients non-triviaux (*cependant, en tant qu'anneau, on peut quotienter un corps par lui-même, mais on obtient alors l'anneau nul et ce n'est pas un corps*).

2.6 Morphismes d'anneaux

Définition 2.6.1 –

Remarque 2.6.2 –
— La première condition dit que f est un morphisme de groupes de $(A, +)$ vers $(B, \oplus)$. En particulier on a $f(0_A) = 0_B$.
— Si B est un anneau non nul, par exemple si B est un corps, alors f n'est pas identiquement nulle.
— Si A, B et C sont trois anneaux et $f : A \to B$ et $g : B \to C$ des morphismes d'anneaux, alors $g \circ f : A \to C$ est un morphisme d'anneaux.

Exemples 2.6.3 –
— Si I est un idéal d'un anneau A, l'application $f : A \to A/I$ définie par $f(x) = \overline{x}$ est un morphisme d'anneaux. Il est surjectif et s'appelle la *surjection canonique* de A sur A/I.

— Pour tout sous-anneau B d'un anneau A, l'application $\iota : B \to A$ définie par $\iota(x) = x$ est un morphisme d'anneaux injectif.

— Si $A = A_1 \times \cdots \times A_n$ est un produit direct d'anneaux, on peut définir pour chaque $i \in \{1, \ldots, n\}$ une application $p_i : A \to A_i$ appelée *projection* par $p_i(a_1, \ldots, a_n) = a_i$; cette application est un morphisme d'anneaux surjectif.

Lemme 2.6.4 – *Soient A et B deux anneaux et $f : A \to B$ un morphisme d'anneaux. L'image par f de tout sous-anneau de A est un sous-anneau de B.*

Démonstration –

□

Remarque 2.6.5 –

Néanmoins on a le résultat suivant.

Lemme 2.6.6 –

Démonstration –

□

Définition 2.6.7 – *Soient A et B deux anneaux et $f : A \to B$ un morphisme d'anneaux. Le sous-anneau* $\operatorname{Im} f = f(A)$ *de B est appelé* image de f.

Remarque 2.6.8 – Le morphisme f est surjectif si et seulement si $\mathrm{Im}\, f = B$.

Lemme 2.6.9 – *Soient A et B deux anneaux et $f : A \to B$ un morphisme d'anneaux. L'image réciproque par f de tout sous-anneau de B est un sous-anneau de A.*

Démonstration –

□

Cette propriété est également vérifiée par les idéaux.

Lemme 2.6.10 –

Démonstration –

□

Corollaire 2.6.11 –

Démonstration –

□

Définition 2.6.12 – *L'image réciproque* $\text{Ker } f = f^{-1}(\{0_B)\}$ *de l'idéal nul de* B *est appelée* noyau de f*, c'est un idéal de* A*.*

Exemples 2.6.13 – Soit I un idéal d'un anneau A. Le noyau de la surjection canonique de A vers A/I est I.

Proposition 2.6.14 – *Soient* A *et* B *deux anneaux. Un morphisme d'anneaux* $f : A \to B$ *est injectif si et seulement si* $\text{Ker } f = \{0_A\}$.

Démonstration – Le morphisme d'anneaux f est en particulier un morphisme de groupes entre $(A, +)$ et $(B, +)$, il est donc injectif si et seulement si $\text{Ker } f = \{0_A\}$. □

Corollaire 2.6.15 – *Tout morphisme de corps est injectif.*

Démonstration –

□

Définition 2.6.16 –

Lemme 2.6.17 –

Démonstration –

□

Définition 2.6.18 – *S'il existe un isomorphisme entre deux anneaux A et B, on dit que les anneaux A et B sont* isomorphes *et on note $A \simeq B$.*

Théorème d'isomorphisme. –

Démonstration –

□

Corollaire 2.6.19 – *Soient I et J deux idéaux d'un anneau A tels que $I \subseteq J$. Alors J/I est un idéal de A/I et les anneaux A/J et $(A/I)/(J/I)$ sont isomorphes.*

Démonstration – D'après le corollaire 2.6.11, l'ensemble J/I est un idéal de A/I. Soit $f : A \to A/I$ et $g : A/I \to (A/I)/(J/I)$ les surjections canoniques. Alors $g \circ f : A \to (A/I)/(J/I)$ est un morphisme d'anneaux, il est surjectif puisque f et g sont surjectives. De plus le noyaux de $g \circ f$ est $f^{-1}(\operatorname{Ker} g) = f^{-1}(J/I) = J$, le théorème d'isomorphisme permet donc de conclure. □

2.7 Caractéristique d'un anneau

Définition 2.7.1 – *La* caractéristique *d'un anneau $(A, +, \times)$ est 0 si $n1_A \neq 0_A$ pour tout $n \in \mathbb{N}^*$, sinon c'est le plus petit entier $n \in \mathbb{N}^*$ tel que $n1_A = 0_A$. On la note* $\operatorname{char}(A)$.

Remarque 2.7.2 – Tout sous-anneau d'un anneau A a la même caractéristique que A.

Exemples 2.7.3 –
- L'anneau trivial (ou *nul*) est la seul anneau de caractéristique 1.
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique nulle.
- Pour tout $n \in \mathbb{N}$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n.
- Tout anneau booléen non trivial est de caractéristique 2.
  [*En effet, dans un tel anneau A on a $a \times a = a$ pour tout $a \in A$. En particulier on a $(2 \cdot 1_A) \times (2 \cdot 1_A) = 2 \cdot 1_A$, autrement dit $4 \cdot 1_A = 2 \cdot 1_A$ d'où $2 \cdot 1_A = 0_A$.*]

Lemme 2.7.4 – *Si $(A, +, \times)$ un anneau de caractéristique c, alors on a $ca = 0_A$ pour tout $a \in A$.*

Démonstration – On peut supposer $c \neq 0$. Par définition on a $c1_A = 0_A$, d'où $ca = c(1_A a) = (c1_A)a = 0_A a = 0_A$. Soit $f : \mathbb{Z} \to A$ l'unique morphisme d'anneaux de $\mathbb{Z}$ dans A. □

On peut caractériser autrement la caractéristique d'un anneau.

Proposition 2.7.5 – *Pour tout anneau $(A, +, \times)$, il existe un unique morphisme d'anneaux $f : \mathbb{Z} \to A$.*

Démonstration –

□

Remarque 2.7.6 – Comme f est un morphisme d'anneaux, son image est un sous-anneau de A. De plus $\mathbb{Z}$ a la particularité de n'avoir aucun sous-anneau propre, l'anneau $\operatorname{Im} f$ a donc la même propriété. Par conséquent $\operatorname{Im} f$ est le plus petit sous-anneau de A, ce sous-anneau est donc engendré par 1_A.

Définition 2.7.7 – *Pour tout anneau $(A, +, \times)$, le plus petit sous-anneau de A est appelé le* sous-anneau premier *de A.*

Lemme 2.7.8 – *Soit $(A, +, \times)$ un anneau de caractéristique c. Si $f : \mathbb{Z} \to A$ est l'unique morphisme d'anneaux de $\mathbb{Z}$ dans A, alors* $\operatorname{Ker} f = c\mathbb{Z}$.

Démonstration – On a $f(1) = 1_A$, donc $f(c) = cf(1) = c1_A = 0_A$ d'où $c \in \operatorname{Ker} f$ et $c\mathbb{Z} \subseteq \operatorname{Ker} f$.

Aussi, pour tout $n \in \operatorname{Ker} f$ on a $n1_A = 0_A$, donc n est un multiple de l'ordre de c et appartient donc à $c\mathbb{Z}$, d'où le résultat. □

Corollaire 2.7.9 – *Le sous-anneau premier d'un anneau A est isomorphe à $\mathbb{Z}/\operatorname{char}(A)\mathbb{Z}$.*

Démonstration – Ceci découle du théorème d'isomorphisme et du lemme précédent. □

Proposition 2.7.10 – *La caractéristique d'un corps est soit* 0*, soit un nombre premier.*

Démonstration –

□

Lemme 2.7.11 – *Toute intersection de sous-corps d'un corps K est un sous-corps de K. En particulier, tout corps a un plus petit sous-corps.*

Démonstration –

□

Définition 2.7.12 – *Pour tout corps $(K, +, \times)$, le plus petit sous-corps de K est appelé le* sous-corps premier *de K.*

Chapitre 3

L'axiome du choix

3.1 Introduction

Le *théorème de Krull*, dont l'énoncé est rappelé ci-dessous, figure au programme du cours. Sa démonstration est basée sur le *lemme de Zorn* qui est lui-même une conséquence de l'*axiome du choix*, ce qui n'est pas anodin et nécessite des explications, tant mathématiques qu'historiques.

L'axiome du choix sera ensuite mentionné plusieurs autres fois dans le cours en fin de semestre. Ce sera d'abord dans la partie *anneaux factoriels* lorsque nous parlerons des *systèmes représentatifs d'éléments irréductibles*, une notion est au programme mais indépendante du reste du cours. Ce sera ensuite lorsque nous démontrerons que *tout anneau principal est factoriel* : comme le théorème de Krull, le résultat est à connaître mais indépendant du reste du cours. Enfin, ce sera lorsque nous étudierons les *anneaux noethériens* en toute fin de cours. Précisons que ces deux derniers cas ne nécessiteront pas toute la force de l'axiome du choix, il s'agira d'applications directes d'une forme faible de l'axiome du choix : l'*axiome du choix dépendant* qui sera vu vers la fin de cette note.

Nous commençons en rappelant les énoncés et définitions utiles. Le premier énoncé nécessite de savoir ce qu'est un *idéal maximal* : *un idéal propre d'un anneau A est dit* maximal *s'il n'est contenu dans aucun autre idéal propre de A que lui-même.*

Théorème de Krull – *Dans tout anneau commutatif, chaque idéal propre est contenu dans un idéal maximal.*

Le deuxième énoncé nécessite de définir un *ensemble inductif* : *un* ensemble inductif *est un ensemble ordonné dans lequel chaque sous-ensemble totalement ordonné admet un majorant.*

Lemme de Zorn – *Tout ensemble inductif non vide admet au moins un élément maximal.*

Le dernier énoncé est celui justifiant cette note.

Axiome du choix – *Toute famille d'ensembles admet une fonction de choix.*

Ici on appelle *fonction de choix* sur une famille d'ensembles $\mathscr{A}$ une application $f : \mathscr{A}\setminus\{\emptyset\} \to$

$\bigcup_{E\in\mathscr{A}} E$ telle que $f(E) \in E$ pour tout $E \in \mathscr{A} \setminus \{\emptyset\}$.

Dans cette note, nous allons évoquer deux variantes de l'axiome du choix :

— l'*axiome du choix dépendant* – seulement vers la fin de cette note – qui peut paraître quelque peu technique mais sera utile en fin de semestre ;

— l'*axiome du choix dénombrable* – régulièrement mentionné ci-dessous – qui est à peu près aussi ancien que l'axiome du choix et a une importance historique.

Axiome du choix *dénombrable* – *Toute famille* dénombrable *d'ensembles admet une fonction de choix.*

Nous en profitons pour rappeler qu'une *famille* est la donnée d'un ensemble I et d'un élément x_i pour chaque élément i de I (appelé *indice*). Ainsi, lorsque nous parlons de *familles*, nous restons dans le cadre de la théorie des ensembles. Les termes *ensemble* et *famille* ne doivent pas être confondus avec le terme *classe* qui, lui, sort du cadre de de la théorie des ensembles : par exemple, on peut parler de la *classe* des anneaux, mais pas de l'*ensemble* des anneaux, ni de la *famille* des anneaux.

Nous terminons cette introduction en donnant deux exemples d'applications de l'axiome du choix. L'un est une construction très naturelle qui utilise pourtant de façon cruciale l'axiome du choix, l'autre en est une conséquence particulièrement déroutante.

Exemple 1 : les ensembles de Vitali

Considérons le groupe quotient $\mathbb{R}/\mathbb{Q}$ du groupe $(\mathbb{R}, +)$. Ses classes à gauche sont les ensembles de la forme $x + \mathbb{Q}$ pour $x \in \mathbb{R}$. Aussi, pour chaque $x \in \mathbb{R}$, si on note $\lfloor x \rfloor$ sa partie entière, alors $x - \lfloor x \rfloor \in x + \mathbb{Q}$ est un représentant de la classe $x + \mathbb{Q}$ appartenant à l'intervalle $[0, 1]$. Choisissons alors, pour chaque classe à gauche de $\mathbb{R}$ modulo $\mathbb{Q}$, un représentant appartenant à l'intervalle $[0, 1]$. On forme ainsi un ensemble V. Les ensembles construits de la sorte sont appelés *ensembles de Vitali*. Notre construction utilise l'axiome du choix : notre fonction de choix est l'application $f : \mathbb{R}/\mathbb{Q} \to \cup_{E\in\mathbb{R}/\mathbb{Q}} E = \mathbb{R}$ qui, à toute classe à gauche $x + \mathbb{Q} \in \mathbb{R}/\mathbb{Q}$ associe son représentant choisi précédemment (celui appartenant à V).

On peut montrer que, pour que les ensembles de Vitali existent, ce qui parait très naturel, on ne peut pas se passer de l'axiome du choix, et même qu'aucune des deux variantes considérées dans cette note n'est suffisante [1].

Exemple 2 : le paradoxe de Banach-Tarski

Il s'agit d'un exemple célèbre de phénomène allant à l'encontre du sens commun. Il affirme que, grâce à l'axiome du choix, il est possible de découper une boule en 8 morceaux puis de réassembler ces morceaux de façon à obtenir deux boules identiques à la première.

1. En fait, les ensemble de Vitali ont la *propriété de Baire*, or le mathématicien israélien Saharon Shelah a démontré que, même avec l'axiome du choix dépendant, qui est plus fort que l'axiome du choix dénombrable, il n'est pas possible de construire un ensemble n'ayant pas cette propriété (voir Conclusion 7.17 de l'article https ://shelah.logic.at/files/95333/176.pdf qui fait suite à un travail du théoricien des ensembles américain Robert Martin Solovay).

Paradoxe de Banach-Tarski [2] **(1924)** – Soit B une boule de l'espace centrée en O. Il existe une partition $B\setminus\{O\} = B_1\cup\cdots\cup B_8$ de $B\setminus\{O\}$ de telle sorte que $r_1(B_1)\cup\cdots\cup r_4(B_4)$ et $r_5(B_5)\cup\cdots\cup r_8(B_8)$ soient deux autres partitions de $B\setminus\{O\}$ où $r_1,\ldots,r_8$ désignent des rotations de centre O.

Notons que ce paradoxe ne comporte aucune contradiction logique. Il s'agit plutôt d'un théorème illustrant le fait que l'axiome du choix a des conséquences particulièrement surprenantes. Il a été démontré en 1924 par les mathématiciens polonais Stefan Banach (1892-1945) et Alfred Tarski (1901-1983).

3.2 Historique

3.2.1 Origines

Les premiers questionnements liés aux fonctions de choix ont lieu dans les années 1890, quand des mathématiciens de Turin décèlent des raisonnements suspects dans des écrits antérieurs [3]. L'un d'eux, Rodolfo Bettazzi (1861-1941), introduit une "loi de choix" dans une démonstration dès 1892, avant de dire explicitement en 1896, en faisant référence à des travaux datant de 1887 de Richard Dedekind [4], qu'il n'est pas rigoureux de choisir arbitrairement un élément dans chacun des ensembles d'une famille infinie d'ensembles, *à moins de l'admettre comme postulat.*

Le mathématicien allemand Ernst Zermelo (1871-1953) démontre en 1904 que *tout ensemble peut être bien ordonné* (c'est-à-dire muni d'un ordre tel que toute partie non vide admet un plus petit élément, *l'ensemble* $\mathbb{N}$ *est l'exemple typique d'un tel ensemble*) [5] ; ainsi il répond positivement à une question posée en 1883 par le mathématicien allemand Georg Cantor (1845-1918). Dans son article, il formule et utilise l'axiome du choix, il préconise de l'appliquer partout. Mais son résultat déconcerte car l'idée que $\mathbb{R}$ puisse être bien ordonné semble contre-intuitive.

Il s'ensuit une vigoureuse opposition de la part de plusieurs grands mathématiciens qui contestent cet axiome, parmi eux les français Henri-Léon Lebesgue (1875-1941), René Baire (1874-1932) et Émile Borel (1871-1956) [6]. En réalité, entre 1872 et 1904, de nombreux travaux ont implicitement utilisé l'axiome du choix sans que cela ait choqué [7], et Lebesgue et Baire l'ont aussi utilisé sous sa forme *dénombrable*. En effet, l'axiome du choix dénombrable ne rencontre pas la même opposition et, par exemple, c'est le cas *non dénombrable* que

2. https ://www.math.ucla.edu/~tao/preprints/Expository/banach-tarski.pdf.

3. Pierre Ageron, *L'autre axiome de choix.* Rev. Histoire Math. 8 (2002), no. 1, 113–140.

4. Jean Cassinet, *Rodolfo Bettazzi (1861–1941), précurseur oublié de l'axiome du choix.* Atti Accad. Sci. Torino Cl. Sci. Fis. Mat. Natur. 116 (1982), no. 1-2, 169–179 (1984).

5. Ernst Zermelo, *Beweis, daß jede Menge wohlgeordnet werden kann.* Math. Ann. 59 (1904), no. 4, 514–516.

6. Jacques Hadamard, *Cinq lettres sur la théorie des ensembles.* Bull. Soc. Math. France 33 (1905), 261–273.

7. Jean Cassinet, *L'axiome du choix avant l'article de E. Zermelo de 1904.* Séminaire de Philosophie et Mathématiques, 1981, fascicule 2, p. 1-19.

récuse explicitement Émile Borel [8]. En revanche, le mathématicien français Jacques Salomon Hadamard (1865-1963) "ne voi[t] pas de différence [...] entre le cas d'une infinité non dénombrable et celui d'une infinité dénombrable" [6]. Ces discussions auront des conséquences importantes pour la suite : l'axiome du choix dénombrables sera accepté de la grande majorité des mathématicien·nes, alors que l'axiome du choix n'est toujours pas admis de la même façon dans toutes les branches des mathématiques.

Signalons que l'axiome du choix a été illustré de façon humoristique en 1919 par le logicien et philosophe britannique Bertrand Arthur William Russell (1872-1970) avec une anecdote pouvant aider à se le représenter : *si on a une infinité de paires de chaussures et qu'on veut choisir une chaussure de chaque paire, on peut le faire en prenant, par exemple, la chaussure gauche de chaque paire : l'obtention d'une fonction de choix se fait ici sans faire appel à l'axiome du choix. En revanche, si on a une infinité de paires de chaussettes, la seule façon de choisir une chaussette de chaque paire est de le faire arbitrairement : on a besoin de l'axiome du choix.*

3.2.2 Naissance des axiomes de la théorie des ensembles

Durant la même période où ont lieu les controverses sur l'axiome du choix, et même un peu avant, différents paradoxes sont mis en lumière, le plus célèbre étant dû à Bertrand Russell.

Paradoxe de Russell (1903) – *L'ensemble des ensembles n'appartenant pas à eux-mêmes appartient-il à lui-même ?*

Ainsi, les mathématicien·nes se rendent compte qu'une théorie "naïve" des ensembles, basée sur une définition trop proche du sens commun, mène à des contradictions. Toutes ces discussions ayant trait à l'axiome du choix, ainsi que ces paradoxes, font émerger la nécessité de faire reposer la théorie des ensembles, et donc les mathématiques, sur des bases plus solides que celles existantes : ce qu'est un *ensemble au sens mathématique* doit être précisé.

Zermelo propose alors en 1908 un système de sept axiomes pour la théorie des ensembles. Ce système sera modifié et réécrit de façon plus formelle dans les années 1920 par le mathématicien allemand (puis israélien) Abraham Adolf Halevi Fraenkel (1891-1965), ainsi que le norvégien Thoralf Skolem (1887-1963), un pionnier de la *théorie des modèles* [9]. Leur axiomatisation est aujourd'hui celle qui est généralement admise : il s'agit du *système* ZF. Notons qu'en raison des controverses durant la période 1904-1908, le système ZF ne comporte pas l'axiome du choix (on écrit ZFC lorsqu'on lui ajoute l'axiome du choix), ni l'axiome du choix dénombrable. Il peut être utile de préciser que, d'après le 1^{er} axiome de ZF, dit *d'extensionnalité*, si deux ensembles ont les mêmes éléments, ils sont égaux. On peut donc toujours choisir un élément dans un ensemble non vide, ou même dans chaque ensemble d'une famille *finie* d'ensembles non vides : l'axiome du choix n'est utile qu'en présence d'une famille infinie d'ensembles.

8. Émile Borel, *Quelques remarques sur les principes de la théorie des ensembles.* Math. Ann. 60 (1905), no. 2, 194–195.

9. Branche de la logique mathématique consacrée à l'étude et la classification des structures.

3.2.3 Des fondations inébranlables ?

Il est naturel de se demander pourquoi avoir choisi de fonder les mathématiques sur ces axiomes et pas d'une autre façon, et aussi si on est sûr que le système ZF n'est pas sujet lui aussi à des contradictions. Si ces questions, et bien d'autres, sont entièrement naturelles, elles relèvent en partie de la philosophie des mathématiques, or ce n'est pas l'objet de cette note. Nous pouvons cependant signaler que c'est peu à peu que le système ZF s'est imposé comme une sorte de norme acceptée de la grande majorité des mathématicien·nes. Plutôt que de définir les ensembles (mais est-ce possible ?), le système ZF fournit une liste d'axiomes naturels, qui formalisent les propriétés à partir desquelles se sont développées les mathématiques ; s'agissant de propriétés (quasiment) universellement admises, cette façon de procéder apparait comme susceptible d'être acceptée de tous et toutes, tout en empêchant les paradoxes tels que celui de Russell. L'idée est que, s'il était possible des définir les ensembles, il serait difficilement imaginable qu'ils ne vérifient pas ces axiomes. Cette méthode permet donc d'assoir les mathématiques sur des bases solides, tout en ne perdant rien de leur généralité.

Néanmoins, la méthode axiomatique a deux limites, comme l'a démontré le logicien autrichien (puis américain) Kurt Gödel (1906-1978) en 1931 avec ses célèbres *théorèmes d'incomplétude*. Le premier de ces théorèmes affirme, grosso modo, que, dès qu'une théorie mathématique est assez puissante, il y a des énoncés "indécidables" (des propositions qu'il est impossible de démontrer mais aussi de réfuter, qui ne sont ni justes ni fausses), ce qui met fin à l'espoir d'avoir une liste d'axiomes permettant de tout démontrer. Le second théorème dit qu'aucune théorie mathématiques ne peut démontrer qu'elle n'engendre aucune contradiction, *i. e.* qu'elle est "cohérente". Il est donc permis d'espérer que le système ZF fonde les mathématiques sur des bases inébranlables, mais il faut avoir conscience que, si tel est le cas, on ne pourra jamais le démontrer !

Serait-il alors possible de fonder autrement les mathématiques ? Cette question relève plus de la philosophie des mathématiques. Disons toutefois que quelques rares mathématicien·nes n'acceptent pas le système ZF, on peut notamment citer les *constructivistes* : ils reconnaissent seulement les objets mathématiques que l'on peut effectivement construire et rejettent même le *principe du tiers exclu* (le principe du tiers exclu énonce qu'une proposition est soit vraie soit fausse) : les démonstrations par l'absurde ne sont alors pas possibles [10]. Le prix à payer d'une telle approche est le rejet d'une grande partie des mathématiques classiques.

Pour en revenir à l'axiome du choix, dans ce contexte les seules questions importantes deviennet : *peut-on démontrer l'axiome du choix à partir du système ZF, ou au contraire, peut-on démontrer qu'il est faux ?* Qu'en est-il de l'axiome du choix *dénombrable*

10. Un raisonnement direct ou par contraposée est toujours plus élégant qu'une démonstration par l'absurde, mais dans certains cas il est très difficile de faire autrement.

3.3 Le lemme de Zorn

C'est en 1935 que le mathématicien allemand (puis américain) Max Zorn (1906-1993) énonce le célèbre *Lemme de Zorn*[11]. Sa démonstration repose sur l'axiome du choix, il a été démontré qu'il est en réalité équivalent à l'axiome du choix. Cependant, la formulation du lemme de Zorn le rend bien plus facile à manier que l'axiome du choix, d'où son intérêt, il est donc beaucoup plus utilisé dans les démonstrations que l'axiome du choix.

Notons que Zorn avait formulé le résultat comme un "principe", pas un lemme, et surtout, il n'a pas été pas le premier à l'énoncer, loin de là ; il est ainsi parfois appelé "Lemme de Kuratowski-Zorn" puisque le polonais Kazimierz Kuratowski (1896-1980) l'avait déjà obtenu en 1922[12].

Il est remarquable que, dans son article, la première application que donne Zorn du lemme est le *théorème de Krull*, précisément le théorème qui nous intéresse dans notre étude des anneaux. Il s'agit d'un résultat qui était déjà connu auparavant puisque c'est l'algébriste allemand Wolfgang Krull (1899-1971) qui l'avait d'abord démontré en 1929.

Notons aussi que, de même que le lemme de Zorn, le théorème de Krull est équivalent à l'axiome du choix. Ceci n'a été démontré qu'en 1979 par Wilfrid Augustine Hodges, un théoricien des modèles britannique, aujourd'hui professeur émérite à l'université de Londres.

Théorème (Hodges, 1979) – *Le théorème de Krull est équivalent à l'axiome du choix.*

Il y a beaucoup d'autres résultats équivalents à l'axiome du choix ; en algèbre on peut notamment mentionner l'existence d'une base dans tout espace vectoriel[13] sachant que, sans l'axiome du choix, il peut aussi exister des espaces vectoriels ayant deux bases de cardinalités différentes[14].

3.4 L'indépendance de l'axiome du choix

Nous en revenons aux questions sur lesquelles nous avons clôturé la section 2 : *peut-on démontrer l'axiome du choix à partir du système ZF, ou au contraire, peut-on démontrer qu'il est faux ?* Qu'en est-il de l'axiome du choix *dénombrable*

3.4.1 Les théorèmes de Gödel et Cohen

Kurt Gödel a démontré en 1938 que,

si le système ZF est cohérent, celui obtenu en ajoutant l'axiome du choix (ZFC) l'est aussi.

11. Max Zorn, *A remark on method in transfinite algebra.* Bull. Amer. Math. Soc. 41 (1935), no. 10, 667–670.

12. On peut consulter l'article de Paul J. Campbell, *The origin of "Zorn's lemma"* (Historia Math. 5 (1978), no. 1, 77–89) pour un historique du Lemme de Zorn.

13. Theorem 4.44 du livre *Axiome of choice* de Horst Herrlich paru à Lecture Notes in Mathematics (n° 1876).

14. Voir l'article *Auswahlaxiom in der Algebra* écrit par von H. Läuchli et paru à Comment. Math. Helv. en 1963.

Autrement dit, en partant du système ZF, il n'est pas possible de démontrer que l'axiome du choix est faux. Cependant, le résultat de Gödel ne dit pas que l'axiome du choix est vrai. Bien plus tard en 1963, le mathématicien américain Paul Joseph Cohen (1934-2007) démontre que

si le système ZF est cohérent, celui obtenu en ajoutant la négation de l'axiome du choix l'est aussi.

Ainsi, le système ZF ne permet pas non plus de démontrer l'axiome du choix ! Ce que ces résultats permettent d'affirmer c'est

— d'une part, qu'une fois qu'on travaille dans ZF, il est scientifiquement autant cohérent d'admettre l'axiome du choix que d'admettre sa négation ;
— d'autre part, qu'en travaillant avec aucune de ces deux hypothèses, on est incapable de démontrer le théorème de Krull, et tout aussi incapable de démontrer qu'il est faux !

Autrement dit, en n'admettant ni l'axiome du choix ni sa négation, on n'a pas suffisamment précisé ce qu'est un ensemble pour pouvoir dire si le théorème de Krull est vrai ou faux.

La situation peut surprendre. Si on a du mal à se la représenter, on peut regarder un problème similaire qui à l'avantage de se rapporter à un objet plus concret. En effet, parallèlement à l'axiome du choix, et même un peu plus tôt, les mathématicien·nes ont été confronté·es au problème de l'*hypothèse du continu* détaillé plus loin qui concerne l'ensemble $\mathbb{R}$ des nombres réels.

3.4.2 L'hypothèse du continu

En 1874 Georg Cantor a démontré que le cardinal de l'ensemble $\mathbb{R}$ est strictement plus grand que celui de l'ensemble $\mathbb{N}$. Il a ensuite formulé vers 1890 un très célèbre problème :

Hypothèse du continu – *Il n'existe aucun ensemble dont le cardinal est strictement compris entre celui de l'ensemble des entiers naturels et celui de l'ensemble des nombres réels.*

À Paris en 1900, au 2^e congrès international des mathématiciens, le mathématicien allemand David Hilbert (1862-1943) a énoncé une liste restée célèbre de 23 problèmes ouverts, appelés *problèmes de Hilbert*. Le premier d'entre eux était justement l'hypothèse du continu.

La situation avec l'axiome du choix, c'est-à-dire avec ZFC, est la suivante : l'ensemble $\mathbb{R}$ a un cardinal, et ce cardinal est strictement plus grand que celui de $\mathbb{N}$. En notant $\aleph_1$ le plus petit cardinal strictement plus grand que celui de $\mathbb{N}$, la question revient à se demander si le cardinal de $\mathbb{R}$ est $\aleph_1$ (hypothèse du continu), ou s'il est strictement plus grand que $\aleph_1$.

En 1938, Gödel a démontré que, *si le système ZFC est cohérent, celui obtenu lorsqu'on ajoute l'hypothèse du continu l'est aussi.* Ensuite en 1964, par la *méthode du forcing*, Cohen a démontré que, *si le système ZFC est cohérent, celui obtenu en ajoutant la négation de l'hypothèse du continu l'est aussi.* Ainsi Paul Cohen a apporté une réponse complète au 1^{er} problème de Hilbert.

Ces résultats montrent que, même avec l'axiome du choix et pas seulement avec le système ZF, on n'est pas suffisamment précis sur ce qu'est un ensemble pour pouvoir

dire quel est cardinal de l'ensemble $\mathbb{R}$, pourtant celui-ci existe et est unique ! Cependant, contrairement à l'axiome du choix qui est couramment admis dans une grande partie des mathématiques, au moins sous des formes affaiblies comme l'axiome du choix dénombrable ou l'axiome du choix dépendant, en général on n'admet ni l'hypothèse du continu, ni sa négation.

Nous terminons cette discussion en signalant que, pour ses travaux sur l'axiome du choix et l'hypothèse du continu, Paul Cohen a reçu la médaille Fields en 1966.

3.5 Deux variantes courantes de l'axiome du choix

Comme nous l'avons vu plus haut en retraçant l'historique de l'axiome du choix, c'est sa forme générale qui a donné lieu à controverse tandis que sa version dénombrable avait même déjà été couramment utilisée dans de nombreux travaux précédents. Nous terminons cette note en disant quelques mots sur l'axiome du choix dénombrable et sur une autre forme faible de l'axiome du choix qui est également couramment utilisée : l'*axiome du choix dépendant*.

3.5.1 L'axiome du choix dénombrable

L'axiome du choix dénombrable est généralement admis par les mathématicien·nes et, comme on l'a vu plus haut, ce dès le départ des controverses liées à l'axiome du choix. Il a plus tard été démontré qu'à la fois,

— cet axiome n'est, comme l'axiome du choix, pas conséquence de ZF ;
— il est strictement plus faible que l'axiome du choix (il a été démontré que, si ZF est cohérent, alors le système obtenu en ajoutant l'axiome du choix dénombrable et la négation de l'axiome du choix est aussi cohérent).

Il est important d'avoir conscience que c'est l'axiome du choix dénombrable qui est utilisé pour montrer que toute réunion dénombrable d'ensembles dénombrables est dénombrable [15], avec le système ZF seul, il est même impossible de démontrer que l'ensemble des nombres réels n'est pas une union dénombrable d'ensembles dénombrables [16].

Si nous nous contentons du système ZF sans axiome supplémentaire, nous permettons également à un ensemble infini de ne contenir aucun sous-ensemble dénombrable [17], alors que cela ne se produit pas avec l'axiome du choix dénombrable. *Notons cependant que la réciproque de ce résultat est fausse : le fait que tout ensemble infini contienne un ensemble dénombrable n'implique pas l'axiome du choix dénombrable* [18]. Tout cela illustre à quel point les mathématicien·nes ont besoin d'un tel axiome pour travailler.

15. https ://www.lmno.cnrs.fr/archives/dehornoy/Surveys/DehornoyChap4.pdf
16. Voir Theorem 10.6 de https ://gwern.net/doc/math/1973-jech-theaxiomofchoice.pdf
17. Voir Theorem 10.1 de https ://gwern.net/doc/math/1973-jech-theaxiomofchoice.pdf
18. Voir Theorem 8.9 de https ://gwern.net/doc/math/1973-jech-theaxiomofchoice.pdf

3.5.2 L'axiome du choix dépendant

Après avoir remarqué que les fondements de l'analyse ne nécessitent pas la pleine force de l'axiome du choix, le logicien suisse Paul Bernays (1888-1977) a introduit en 1942 un axiome plus faible que l'axiome du choix appelé *axiome du choix dépendant*[19].

Axiome du choix *dépendant* – *Pour tout ensemble non vide X et toute relation R sur X, si pour tout $x \in X$ il existe $y \in X$ tel que xRy, alors il existe une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de X telle qu'on ait x_nRx_{n+1} pour tout $n \in \mathbb{N}$.*

Son énoncé peut paraître compliqué, il est pourtant si naturel que, comme nous le verrons en cours, il peut être utilisé sans même s'en rendre compte, notamment lorsqu'on construit une suite *par récurrence*.

Il est possible de démontrer que cet axiome est strictement plus fort que l'axiome du choix dénombrable et strictement plus faible que l'axiome du choix[20]. À titre d'exemple, cet axiome est insuffisant pour construire les ensembles de Vitali (voir Exemple 1 ci-dessus ainsi que la note de bas de page).

L'axiome du choix dépendant sera utilisé deux fois dans le cours, en fin de semestre : d'abord pour montrer que tout anneau *principal* est *factoriel*, puis dans l'étude des anneaux *noethériens*. En réalité, le théoricien des modèles Wilfrid Hodges a démontré que les axiomes du système ZF sont insuffisants pour démontrer que tout anneau principal est factoriel[21].

Théorème (Hodges, 1976) – *Il n'est pas possible de démontrer que tout anneau principal est factoriel en utilisant seulement les axiomes du système ZF.*

Il a également démontré en 1973 que les axiomes du système ZF sont insuffisants pour démontrer certains résultats du cours sur les anneaux noethériens[22], alors que l'axiome du choix dépendant permettra leur démonstration.

19. Paul Bernays, *A system of axiomatic set theory. III. Infinity and enumerability. Analysis.* J. Symbolic Logic 7 (1942), 65,Äì89.

20. Voir la section 8 de les théorème 8.9 et 8.12 de https ://gwern.net/doc/math/1973-jech-theaxiomofchoice.pdf

21. Voir Corollaire 10 (a) de l'article de Wilfried Hodges intitulé *Läucli's algebraic closure of Q* paru dans Math. Proc. Camb. Phil. Soc. en 1976.

22. Voir Ring 1 de l'article de Wilfried Hodges intitulé *Six impossible rings* paru au Journal of Algebra en 1974.

Chapitre 4

Anneaux intègres

4.1 Généralités

Définition 4.1.1 – *Un anneau* $(A, +, \times)$ *est dit* commutatif *si la loi* $\times$ *est commutative.*

Remarque 4.1.2 –
- Les sous-anneaux et quotients des anneaux commutatifs sont commutatifs.
- Si $(A, +, \times)$ est un anneau commutatif, un sous-groupe I de $(A, +)$ est un idéal de A si et seulement si, pour tout $(x, a) \in I \times A$, on a $xa \in I$.

Exemples 4.1.3 –
- Les anneaux $(\mathbb{Z}, +\times)$, $(\mathbb{Q}, +\times)$, $(\mathbb{R}, +\times)$ et $(\mathbb{C}, +\times)$ sont commutatifs.
- Si $(A, +\times)$ est un anneau, l'anneau $\mathscr{M}_n(A)$ n'est commutatif que dans le cas où A est commutatif et où $n = 1$.
- Si $(G, +)$ est un groupe abélien, l'anneau $(\mathrm{End}(G), +, \circ)$ n'est commutatif que dans des cas très particuliers.
- Pour tout ensemble E, l'anneau $(\mathscr{P}(E), \Delta, \cap)$ est commutatif.
  Plus généralement, les anneaux de Boole sont tous commutatifs.

- Un produit direct d'anneaux $A_1, \cdots, A_n$ est commutatif si et seulement si les anneaux $A_1, \cdots, A_n$ sont tous commutatifs.

Définition 4.1.4 –

Remarque 4.1.5 – Un sous-anneau d'un anneau intègre est intègre.

Exemples 4.1.6 –
— Les anneaux $(\mathbb{Z}, +\times)$, $(\mathbb{Q}, +\times)$, $(\mathbb{R}, +\times)$ et $(\mathbb{C}, +\times)$ sont intègres.
— L'anneau $(\mathscr{P}(E), \Delta, \cap)$ n'est intègre que si E est un singleton.

Plus généralement, parmi les anneaux de Boole, seuls ceux ayant exactement deux éléments sont intègres.

— Un produit direct d'anneaux $A_1, \cdots, A_n$ n'est intègre que si tous les anneaux A_i sont nuls sauf un qui est intègre.

Le résultat suivant montre que les corps commutatifs sont des exemples particuliers d'anneaux intègres.

Lemme 4.1.7 – *Tout corps commutatif est un anneau intègre.*

Démonstration – Soit $(K, +, \times)$ un corps commutatif. Par définition, c'est un anneau non nul. Soit a un élément non nul de K. Si on a $ab = 0$ pour un élément b de K, alors on a $b = 1_K b = a^{-1}ab = a^{-1}0_A = 0_A$ et a n'est donc pas un diviseur de zéro. Ainsi $(K, +, \times)$ est un anneau intègre. □

Proposition 4.1.8 – *La caractéristique d'un anneau intègre est soit* 0*, soit un nombre premier.*

Démonstration –

□

Rappel (théorème de Gauss) : si a, b et c sont trois entiers relatifs tels que a divise bc et est premier avec b, alors a divise c.

Proposition 4.1.9 – *Soit $(A, +, \times)$ un anneau commutatif de caractéristique un nombre premier p. Alors l'application $f : A \to A$ définie par $f(x) = x^p$ est un endomorphisme d'anneaux.*

En particulier, on a $(x + y)^p = x^p + y^p$ pour tous x et y dans A.

Démonstration –

□

Définition 4.1.10 – *Si $(A, +, \times)$ un anneau intègre dont la caractéristique est un nombre premier p, l'endomorphisme $f : A \to A$ définie par $f(x) = x^p$ est appelé* morphisme de Frobenius.

4.2 Le corps des fractions d'un anneau intègre

Proposition 4.2.1 – *Pour tout anneau intègre A, il existe un plus petit corps contenant A, unique à isomorphisme près, appelé* corps des fractions de A. *Il est commutatif*

Exemples 4.2.2 – La construction ci-dessus appliquée à l'anneau $A = \mathbb{Z}$ donne $K_A = \mathbb{Q}$: le corps des fractions de $\mathbb{Z}$ est donc $\mathbb{Q}$.

Supposons maintenant que K est un corps de carcatéristique nulle, et notons K_0 son sous-corps premier. Le sous-anneau premier A_0 de K est isomorphe à $\mathbb{Z}/0\mathbb{Z} \simeq \mathbb{Z}$ d'après le Corollaire 2.7.9 du chapitre précédent, or K_0 est le plus petit sous-corps de K contenant A_0, il est donc isomorphe au corps des fractions de $A_0 \simeq \mathbb{Z}$ qui est $K_{A_0} \simeq \mathbb{Q}$.

Proposition 4.2.3 – *Le sous-corps premier d'un corps de caractéristique nulle est isomorphe à* $\mathbb{Q}$.

4.3 Idéaux premiers

Définition 4.3.1 –

Nous montrons que cette définition est équivalente à la nôtre.

Proposition 4.3.2 –

Démonstration –

□

Définition 4.3.3 – *Soient x et y deux éléments d'un anneau commutatif A. On dit que x* divise *y s'il existe $a \in A$ tel que $y = ax$. On note alors $x|y$ et on dit que x est un* diviseur *de y, ou encore que y est* multiple *de x.*

Remarque 4.3.4 –
— Tous les éléments d'un anneau commutatif A divisent 0_A : ce sont tous des diviseurs de 0_A.
Attention, il ne faut pas confondre "diviseur de 0_A" et "diviseur de zéro" [1]
— 1_A divise tous les éléments de A.

Lemme 4.3.5 – *Soit $(A, +, \times)$ un anneau commutatif. On a $(x) = xA$ pour tout élément x de A.*

Autrement dit, l'idéal engendré par x est l'ensemble des multiples de x.

Démonstration –

□

Définition 4.3.6 – *Un idéal I d'un anneau commutatif $(A, +, \times)$ est dit* principal *s'il est de la forme $I = (x)$ pour $x \in A$.*

Corollaire 4.3.7 – *Soit $(A, +, \times)$ un anneau commutatif. Un élément x de A est inversible si et seulement si $(x) = A$.*

Démonstration –

□

1. Cette distinction peut surprendre, cependant il y a le même genre de distinction dans d'autres domaines : en course à pied, courir un 10000m est différent de courir un 10km (pourquoi ?).

Définition 4.3.8 –

Remarque 4.3.9 –

— Nous verrons que, dans l'anneau $\mathbb{Z}$, les éléments premiers sont les nombres premiers et leurs opposés.
— Les corps n'ont pas d'élément premier.

Proposition 4.3.10 – *Soit $(A, +, \times)$ un anneau commutatif et x un élément non nul de A. Alors l'élément x est premier si et seulement si l'idéal (x) est premier.*

Démonstration –

□

4.4 Idéaux maximaux

Définition 4.4.1 – *Un idéal propre d'un anneau A est dit* maximal *s'il n'est contenu dans aucun autre idéal propre de A que lui-même.*

Proposition 4.4.2 – *Un idéal M d'un anneau commutatif $(A, +, \times)$ est maximal si et seulement si A/M est un corps.*

Démonstration –

□

Corollaire 4.4.3 – *Tout idéal maximal est premier.*

Démonstration – Si M est un idéal maximal d'un anneau A, alors A/M est un corps d'après la proposition 4.4.2, donc A/M est un anneau intègre (lemme 4.1.7). La proposition 4.3.2 dit alors que M est un idéal premier. □

Nous allons démontré le *théorème de Krull*, sa démonstration nécessite l'utilisation du *Lemme de Zorn*, et donc de l'*Axiome du choix*. Nous commençons donc par quelques "rappels".

Définition 4.4.4 –
- *Un ensemble E muni d'une relation d'ordre $\leqslant$ est dit* ordonné.
- *Un* majorant *d'une partie X de E est un élément m de E qui vérifie $x \leq m$ pour tout $x \in X$.*
- *On dit que E est* totalement ordonné *si l'ordre $\leqslant$ est total (c'est-à-dire qu'il vérifie $x \leqslant y$ ou $y \leqslant x$ pour tout $(x, y) \in E \times E$).*
- *Enfin, un ensemble ordonné est dit* inductif *si tout ses sous-ensembles totalement ordonnés admettent un majorant.*

Lemme 4.4.5 – **(Lemme de Zorn)** *Tout ensemble inductif non vide admet au moins un élément maximal.*

Démonstration – ADMIS, voir feuille à part pour des explications concernant ce lemme.
□

Théorème 4.4.6 – **(Théorème de Krull)** *Dans tout anneau commutatif, chaque idéal propre est contenu dans un idéal maximal.*

Démonstration –

□

Remarque 4.4.7 – Le théorème de Krull est évidemment à connaître. Cependant, nous verrons dans la suite du cours que, lorsqu'on a un idéal propre I d'un anneau commutatif, dans la pratique il est rare d'avoir besoin du théorème de Krull pour trouver un idéal maximal M contenant I.

4.5 L'anneau $\mathbb{Z}$

Rappel 4.5.1 – *Les idéaux de l'anneau $\mathbb{Z}$ sont les sous-ensembles de la forme $n\mathbb{Z}$ pour $n \in \mathbb{N}$.*

Remarque 4.5.2 – Pour tous m et n dans $\mathbb{Z}$, l'idéal $m\mathbb{Z}$ est contenu dans $n\mathbb{Z}$ si et seulement si n divise m.

[*En effet, si $m\mathbb{Z}$ est contenu dans $n\mathbb{Z}$, alors $m = na$ pour $a \in \mathbb{Z}$, donc n divise m et, réciproquement si n divise m, alors on a $m = na$ pour $a \in \mathbb{Z}$, d'où $m\mathbb{Z} = na\mathbb{Z} \subseteq n\mathbb{Z}$.*]

En particulier, on a $m\mathbb{Z} = n\mathbb{Z}$ si et seulement si m et n se divisent l'un l'autre, autrement dit si $m = \pm n$.

Proposition 4.5.3 – *Les idéaux maximaux de l'anneau $\mathbb{Z}$ sont les idéaux de la forme $p\mathbb{Z}$ pour un entier premier p.*

En particulier, un quotient $\mathbb{Z}/n\mathbb{Z}$ de $\mathbb{Z}$ est un corps si et seulement si n est premier.

Démonstration – Soit $n \in \mathbb{N}$ un entier non premier. Alors soit $n = 0$ et $n\mathbb{Z} = 0\mathbb{Z} \subsetneq 2\mathbb{Z}$ n'est pas maximal, soit $n = 1$ et $n\mathbb{Z} = \mathbb{Z}$ n'est pas maximal, soit un entier premier p divise n et $n\mathbb{Z} \subsetneq p\mathbb{Z}$ n'est pas maximal. On en déduit que $n\mathbb{Z}$ ne peut être maximal que si n est un entier premier.

Si n est premier, comme le seul entier naturel différent de n qui divise n est 1, et comme $1\mathbb{Z} = \mathbb{Z}$, l'idéal $n\mathbb{Z}$ est maximal. □

Corollaire 4.5.4 – *Le sous-corps premier d'un corps de caractéristique p non nulle est son sous-anneau premier, et il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

Démonstration –

□

Remarque 4.5.5 – Sans faire appel au théorème de Krull (et donc à l'axiome du choix), on en déduit que tout idéal propre $I = n\mathbb{Z}$ de $\mathbb{Z}$ est contenu dans un idéal maximal de $\mathbb{Z}$: il suffit de considérer $p\mathbb{Z}$ pour un entier premier p qui divise n.

Corollaire 4.5.6 – *Les idéaux premiers de $\mathbb{Z}$ sont $0\mathbb{Z}$ et les idéaux de la forme $p\mathbb{Z}$ pour un entier premier p ; les éléments premiers de $\mathbb{Z}$ sont les entiers premiers et les opposés des entiers premiers.*

Démonstration –

□

Remarque 4.5.7 –

- Dans l'anneau $\mathbb{Z}$, pour tout $n \in \mathbb{N}$, au lieu de parler de la congruence modulo $n\mathbb{Z}$, on parle plus simplement de la *congruence modulo* n et, pour tout $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, avec $x - y \in n\mathbb{Z}$, on note $x \equiv y \pmod{n}$ ou $x \equiv y\ [n]$ au lieu de $x \equiv y \pmod{n\mathbb{Z}}$.
- La congruence modulo 0 est une relation d'équivalence "*triviale*" (comme "="). En effet, pour tout $(x, y) \in \mathbb{Z}\times\mathbb{Z}$, on a $x \equiv y \pmod{0}$ si et seulement si $x-y \in 0\mathbb{Z} = \{0\}$, c'est-à-dire $x = y$. Autrement dit, $\mathbb{Z}/0\mathbb{Z}$ s'identifie à $\mathbb{Z}$.
- Comme tous les éléments de $\mathbb{Z}$ sont congrus modulo 1, l'anneau $\mathbb{Z}/1\mathbb{Z}$ n'a qu'un élément.
- Pour tout $n \in \mathbb{N}^*$ et tout $a \in \mathbb{Z}$, si r désigne le reste de la division euclidienne de a par n, alors on a $a = nq + r$ pour $q \in \mathbb{Z}$, donc $\overline{a} = \overline{r}$. Les seuls éléments de $\mathbb{Z}/n\mathbb{Z}$ sont donc $\overline{0},\ \overline{1}, \ldots, \overline{n-1}$, et ils sont tous distincts puisque n ne divise aucun entier de la forme $y - x$ avec x et y dans $\{0, \ldots, n-1\}$. En particulier $\mathbb{Z}/n\mathbb{Z}$ a exactement n éléments.

Chapitre 5

Anneaux de polynômes

5.1 Anneau $A[X]$ des polynômes sur A

Dans toute cette section, on fixe un anneau commutatif A.

5.1.1 Définition

Vous connaissez depuis longtemps les fonctions polynomiales, nous allons généraliser cette notion.

Définition 5.1.1 – *Un* polynôme sur A *(ou* à coefficients dans A*) est une suite presque nulle* $P = (a_i)_{i\in\mathbb{N}} = (a_0, a_1, a_2, ..., a_i, ...)$ *d'éléments de* A. Autrement dit, la suite n'a qu'un nombre fini de termes non nuls : il existe un entier $n \in \mathbb{N}$ tel que $a_i = 0_A$ pour tout $i > n$.

Les éléments a_i *de* A *pour* $i \in \mathbb{N}$ *sont appelés les* coefficients *du polynôme* P.

On définit naturellement l'addition des polynômes et la multiplication des polynômes par des éléments de A : si $P = (a_i)_{i\in\mathbb{N}}$ et $Q = (b_i)_{i\in\mathbb{N}}$ sont deux polynômes sur A, et λ un élément de A, on définit $P + Q = (a_i + b_i)_{i\in\mathbb{N}}$ et $\lambda P = (\lambda a_i)_{i\in\mathbb{N}}$.

Le produit $\times$ de deux polynômes $P = (a_i)_{i\in\mathbb{N}}$ et $Q = (b_j)_{j\in\mathbb{N}}$ sur A est défini de façon un peu différente par $P \times Q = PQ = (\sum_{i+j=k} a_i b_j)_{k\in\mathbb{N}}$.

Remarque 5.1.2 –

Notation 5.1.3 – *Pour tous les entiers naturels m et n, on définit le* symbole de Kronecker *δ_{mn} par $\delta_{mn} = 1_A$ si $m = n$ et $\delta_{mn} = 0_A$ si $m \neq n$.*

On note $0 = (0_A, 0_A, \cdots)$ la suite nulle et 1 la suite $(\delta_{0i})_{i\in\mathbb{N}} = (1_A, 0_A, 0_A, \cdots)$. Ces deux suites sont des polynômes, le premier est appelé *polynôme nul*.

Théorème 5.1.4 – *L'ensemble des polynômes sur A muni des lois $+$ et $\times$ est un anneau commutatif. Ses éléments neutres sont 0 pour la loi $+$ et 1 pour la loi $\times$.*

Démonstration – On a vu que les lois $+$ et $\times$ sont des lois de composition internes commutatives. Elles sont associatives puisque, pour tous les polynômes $(a_i)_{i\in\mathbb{N}}$, $(b_i)_{i\in\mathbb{N}}$ et $(c_i)_{i\in\mathbb{N}}$, on a

$$((a_i)_i + (b_i)_i) + (c_i)_i = ((a_i + b_i) + c_i)_i = (a_i + (b_i + c_i))_i = (a_i)_i + ((b_i)_i + (c_i)_i)$$

et

$$\begin{array}{rcl} ((a_i)_{i\in\mathbb{N}} \times (b_i)_{i\in\mathbb{N}}) \times (c_i)_{i\in\mathbb{N}} & = & (\sum_{i+j=k} a_i b_j))_{k\in\mathbb{N}} \times (c_i)_{i\in\mathbb{N}} \\ & = & (\sum_{k+l=m} (\sum_{i+j=k} a_i b_j) c_l)_{m\in\mathbb{N}} \\ & = & (\sum_{i+j+l=m} a_i b_j c_l)_{m\in\mathbb{N}} \\ & = & (a_i)_{i\in\mathbb{N}} \times ((b_i)_{i\in\mathbb{N}} \times (c_i)_{i\in\mathbb{N}}) \end{array} .$$

Les éléments neutres sont respectivement 0 et 1 puisque, pour tout polynôme $(a_i)_{i\in\mathbb{N}}$, on a

$$0 + (a_i)_{i\in\mathbb{N}} = (0 + a_i)_{i\in\mathbb{N}} = (a_i)_{i\in\mathbb{N}} = (a_i)_{i\in\mathbb{N}} + 0$$

et

$$1 \times (a_i)_{i\in\mathbb{N}} = (\delta_{0i})_{i\in\mathbb{N}} \times (a_i)_{i\in\mathbb{N}} = (\sum_{i+j=k} \delta_{0i} a_j))_{k\in\mathbb{N}} = (a_k)_{k\in\mathbb{N}} = (a_i)_{i\in\mathbb{N}} \times 1.$$

De plus, pour tout polynôme $(a_i)_{i\in\mathbb{N}}$, la suite $-(a_i)_{i\in\mathbb{N}} = (-a_i)_{i\in\mathbb{N}}$ est un polynôme sur A qui vérifie

$$(a_i)_{i\in\mathbb{N}} + (-(a_i)_{i\in\mathbb{N}}) = (a_i - a_i)_{i\in\mathbb{N}} = 0 = -(a_i)_{i\in\mathbb{N}} + (a_i)_{i\in\mathbb{N}}.$$

Il reste donc juste à montrer que la loi $\times$ est distributive par rapport à la loi $+$. Considérons trois polynômes $(a_i)_{i\in\mathbb{N}}$, $(b_i)_{i\in\mathbb{N}}$ et $(c_i)_{i\in\mathbb{N}}$. On a

$$\begin{aligned}
(a_i)_{i\in\mathbb{N}}((b_i)_{i\in\mathbb{N}} + (c_i)_{i\in\mathbb{N}}) &= (a_i)_{i\in\mathbb{N}}(b_i + c_i)_{i\in\mathbb{N}} \\
&= (\textstyle\sum_{i+j=k} a_i(b_j + c_j))_{k\in\mathbb{N}} \\
&= ((\textstyle\sum_{i+j=k} a_i b_j) + (\sum_{i+j=k} a_i c_j))_{k\in\mathbb{N}} \\
&= (\textstyle\sum_{i+j=k} a_i b_j)_{k\in\mathbb{N}} + (\sum_{i+j=k} a_i c_j)_{k\in\mathbb{N}} \\
&= (a_i)_{i\in\mathbb{N}}(b_i)_{i\in\mathbb{N}} + (a_i)_{i\in\mathbb{N}}(c_i)_{i\in\mathbb{N}}
\end{aligned}$$

La loi $\times$ étant commutative, on a aussi $((a_i)_i + (b_i)_i)(c_i)_i = (a_i)_i(c_i)_i + (b_i)_i(c_i)_i$, donc l'ensemble des polynômes sur A muni des lois $+$ et $\times$ est bien un anneau commutatif. □

Remarque 5.1.5 – Pour tout $a \in A$ et tout polynôme $P = (a_i)_{i\in\mathbb{N}}$, on a $aP = (a1) \times P$.
[*En effet, on a* $(a1) \times P = (a\delta_{0i})_{i\in\mathbb{N}}(a_i)_{i\in\mathbb{N}} = (\sum_{i+j=k} a\delta_{0i}a_j)_{k\in\mathbb{N}} = (aa_j)_{j\in\mathbb{N}} = aP$.]

Proposition 5.1.6 – *Soit ι l'application de A dans l'ensemble des polynômes sur A définie par $\iota(a) = a1 = (a, 0, 0, \cdots)$ pour tout $a \in A$. Alors ι est un morphisme d'anneaux injectif.*

Démonstration –

□

Remarque 5.1.7 – On en déduit qu'on peut identifier l'anneau A au sous-anneau $\operatorname{Im}\iota$ de l'ensemble des polynômes sur A en notant de la même façon l'élément a de A et son image $\iota(a) = a1$: on notera $\iota(a) = a$.

Les polynômes de la forme a sont appelés les *polynômes constants*.

Notation 5.1.8 – *On note X le polynôme $X = (\delta_{1i})_{i\in\mathbb{N}} = (0_A, 1_A, 0_A, 0_A, \cdots)$.*

Lemme 5.1.9 – *Pour tout $n \in \mathbb{N}$, on a $X^n = (\delta_{ni})_{i\in\mathbb{N}}$.*

Démonstration –

□

Corollaire 5.1.10 – *Tout polynôme $P = (a_i)_{i\in\mathbb{N}}$ s'écrit de façon unique sous la forme $P = \sum_{i\in\mathbb{N}} a_i X^i$. En outre il existe $n \in \mathbb{N}$ tel que $P = \sum_{i=0}^{n} a_i X^i$.*

Démonstration –

□

Notation 5.1.11 – *L'ensemble des polynômes sur A est noté $A[X]$.*

5.1.2 Degré d'un polynôme

Définition 5.1.12 – *Soit $P = \sum_{i\in\mathbb{N}} a_i X^i \in A[X]$. Si $P = 0$, on dit que le* degré *de P est $-\infty$. Sinon, il existe un plus grand entier $n \in \mathbb{N}$ pour lequel $a_n \neq 0_A$. On dit alors que le* degré *de P est n et on note* $\deg P$ *le degré de P.*

Remarque 5.1.13 –
- Si $n \in \mathbb{N}$ est le degré d'un polynôme $P = \sum_{i\in\mathbb{N}} a_i X^i$, alors on a $P = \sum_{i=0}^{n} a_i X^i$.
- Les polynômes constants non nuls sont ceux de degré 0.
- On a les conventions suivantes : pour tout $n \in \mathbb{N}$, $-\infty < n$, $(-\infty) + (-\infty) = -\infty$ et $n + (-\infty) = (-\infty) + n = -\infty$.

Définition 5.1.14 – *Pour tout polynôme $P = \sum_{i\in\mathbb{N}} a_i X^i$, les polynômes $a_i X^i$ sont appelés* termes *de P.*

Si P est non nul, son terme de plus haut degré *est son terme de degré* $\deg P$.

Si P est non nul, le coefficient de son terme de plus haut degré est appelé coefficient dominant.

Un polynôme P sur A est dit unitaire *s'il est non nul et si coefficient dominant est 1_A.*

Proposition 5.1.15 – *Pour tous polynômes P et Q sur A, on a* $\deg(PQ) \leqslant \deg P + \deg Q$ *et* $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$.

De plus, si P est nul ou si son coefficient dominant n'est pas un diviseur de zéro, alors $\deg(PQ) = \deg P + \deg Q$.

Démonstration –

□

Corollaire 5.1.16 – *Si l'anneau A est intègre, alors pour tous polynômes P et Q sur A, on a* $\deg(PQ) = \deg P + \deg Q$.

Corollaire 5.1.17 – *L'anneau $A[X]$ est intègre si et seulement si A est intègre.*

Démonstration –

□

Corollaire 5.1.18 – *Si l'anneau A est intègre, les éléments inversibles de $A[X]$ sont les polynômes constants de la forme $P = a$ pour $a \in A^\times$.*

Démonstration –

□

Remarque 5.1.19 – Le *théorème de la division euclidienne* ci-dessous est notamment utile lorsque A est un corps, ainsi que lorsque le polynôme B de l'énoncé est unitaire.

Théorème 5.1.20 – **(Théorème de la division euclidienne)**

Démonstration –

□

5.1.3 Racines d'un polynôme

Définition 5.1.21 –

Exemples 5.1.22 – Si $A = \mathbb{Z}/6\mathbb{Z}$ et $P = X^2 - X$, alors l'application polynomiale associée à P est définie par $P(\overline{x}) = \overline{0}$ si $\overline{x} \in \{\overline{0}, \overline{1}, \overline{3}, \overline{4}\}$ et $P(\overline{x}) = \overline{2}$ si $\overline{x} \in \{\overline{2}, \overline{5}\}$. Ainsi P a 4 racines : $\overline{0}, \overline{1}, \overline{3}, \overline{4}$.

Remarque 5.1.23 – Pour tout $\alpha \in A$, l'évaluation en α est un morphisme d'anneaux.

[*En effet, on a* $\mathrm{ev}_\alpha(1) = 1_A$ *et, pour tous polynômes* P *et* Q *sur* A*, on a* $\mathrm{ev}_\alpha(P+Q) = (P+Q)(\alpha) = P(\alpha) + Q(\alpha) = \mathrm{ev}_\alpha(P) + \mathrm{ev}_\alpha(Q)$ *et* $\mathrm{ev}_\alpha(PQ) = (PQ)(\alpha) = P(\alpha)Q(\alpha) = \mathrm{ev}_\alpha(P)\mathrm{ev}_\alpha(Q)$.]

Proposition 5.1.24 – *Soit* P *un polynôme sur* A*. Un élément* r *de* A *est une racine de* P *si et seulement si le polynôme* $X - r$ *divise* P*.*

Démonstration –

□

Théorème 5.1.25 – *Si* A *est intègre, alors tout polynôme de degré* $n \in \mathbb{N}$ *admet au plus* n *racines.*

Démonstration –

□

Corollaire 5.1.26 – **(Théorème d'identification)**

Démonstration –

□

Remarque 5.1.27 –
— Si A est fini, alors même si c'est un corps, deux polynômes distincts peuvent avoir la même fonction polynomiale associée.

— De la même façon, si A est infini sans être intègre, deux polynômes distincts peuvent avoir la même fonction polynomiale associée.

5.2 Anneaux euclidiens et anneaux principaux

Comme cela a été dit à la remarque 5.1.19, le théorème de la division euclidienne (théorème 5.1.20) est notamment utile dans le cas où l'anneau commutatif A est un corps. La division euclidienne est une propriété commune à $\mathbb{Z}$ et aux anneaux de polynômes $\mathbb{K}[X]$ lorsque $\mathbb{K}$ est un corps commutatif quelconque. Elle engendrent de nombreuses autres propriétés vérifiées par tous les *anneaux euclidiens*.

Définition 5.2.1 – *Soit A un anneau intègre.*
— *Un* stathme euclidien *(du grec $\sigma\tau\alpha\theta\mu\eta$, qui signifie "fil de plomb, règle, mesure", et avec un* th *venant de* thêta *qui se prononce* t*) est une application $\varphi : A^* \to \mathbb{N}$ qui vérifie les deux conditions suivantes :*

— *Si un tel stathme euclidien existe, on dit que A est un* anneau euclidien.

Remarque 5.2.2 –

— Un tel stathme n'est généralement pas unique.
— Les éléments q et r de la condition (1) ne sont généralement pas unique, même pour un stathme fixé.
— Certains auteurs définissent un stathme euclidien comme une application $\varphi : A^* \to \mathbb{N}$ vérifiant seulement la condition (1) de la définition 5.2.1. La proposition ci-dessous montre que les anneaux euclidiens obtenus de cette façon sont exactement les mêmes que ceux à partir de notre définition.

Proposition 5.2.3 – *Soit A un anneau intègre. S'il y a une application $\nu : A^* \to \mathbb{N}$ vérifiant la condition (1) de la définition 5.2.1, alors l'anneau A est euclidien.*

Démonstration –

□

Exemples 5.2.4 – On a vu que $\mathbb{Z}$ et $\mathbb{K}[X]$ sont euclidiens lorsque $\mathbb{K}$ est un corps commutatif, tout corps commutatifs $\mathbb{K}$ est également euclidien puisque l'application constante $\varphi : \mathbb{K}^* \to \mathbb{N}$ égale à 0 est un stathme euclidien sur $\mathbb{K}$.

Beaucoup d'autres anneaux sont euclidiens, comme l'*anneau des entiers de Gauss* défini par $\mathbb{Z}[i] = \{a + ib \mid (a, b) \in \mathbb{Z}\}$ puisque l'application $N : \mathbb{Z}[i] \to \mathbb{N}$ définie par $N(a + ib) = |a + ib|^2$ est un stathme euclidien (*ceci sera vu en TD*).

De même $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid (a, b) \in \mathbb{Z}\}$ est un anneau euclidien ; l'application N :

$\mathbb{Z}[\sqrt{3}]^* \to \mathbb{N}$ définie par $N(a+b\sqrt{3}) = |a^2 - 3b^2|$ est un stathme euclidien.

Une particularité importante des anneaux euclidiens est que tous leurs idéaux sont *principaux*.

Définition 5.2.5 – *Un anneau intègre est dit* principal *si tous ses idéaux sont principaux.*

Remarque 5.2.6 – Il y a de nombreux anneaux intègres qui ne sont pas principaux. Par exemple, si A est un anneau intègre qui n'est pas un corps, alors l'anneau intègre $A[X]$ n'est pas principal.

Théorème 5.2.7 – *Tout anneau euclidien est principal.*

Démonstration –

□

Remarque 5.2.8 – En revanche, il existe des anneaux principaux non euclidiens, comme par exemple $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}] = \{a + b\frac{1+i\sqrt{19}}{2} \ ; \ (a,b) \in \mathbb{Z}^2\}$: un exercice de l'une des fiches de TD est consacré à l'étude de cet anneau.

5.3 Polynômes à plusieurs indéterminées

Dans cette section, on fixe un anneau commutatif A et un entier $n \in \mathbb{N}^*$.

Remarque 5.3.1 – Une suite $(a_i)_{i\in\mathbb{N}}$ d'éléments de A, c'est une application $\mathbb{N} \to A$ définie par $i \mapsto a_i$. Or on a défini un polynôme sur A comme une une suite presque nulle $P = (a_i)_{i\in\mathbb{N}}$ d'éléments de A : un polynôme est donc une application $f : \mathbb{N} \to A$ *à support fini*, autrement dit telle que $f(i) \neq 0_A$ seulement pour un nombre fini d'entiers $i \in \mathbb{N}$.

La définition d'un polynôme à plusieurs indétrminées part de ce point de vue.

Définition 5.3.2 – *Un* polynôme à n indéterminées *est une application $f : \mathbb{N}^n \to A$ à support fini.*

Les images des éléments de $\mathbb{N}^n$ sont appelés les coefficients *du polynôme.*

On définit l'addition de ces polynômes et leur multiplication par des éléments de A en posant, pour tous polynômes P et Q à n indéterminées, tout $\lambda \in A$ et tout $\overline{u} \in \mathbb{N}^n$:

$$(P + Q)(\overline{u}) = P(\overline{u}) + Q(\overline{u}) \quad \text{et} \quad (\lambda P)(\overline{u}) = \lambda P(\overline{u}).$$

Le produit $\times$ de P et Q est défini simillairement à celui de deux polynômes de $A[X]$ en posant $(P \times Q)(\overline{u}) = \sum_{\overline{x}+\overline{y}=\overline{u}} P(\overline{x})Q(\overline{y})$.

Remarque 5.3.3 – Pour tout $(a, b) \in A \times A$ et tout polynôme P à n indéterminées, on a $(a + b)P = aP + bP$ et $(ab)P = a(bP)$.

Notation 5.3.4 – *On note 0 polynôme à n indéterminées défini par $0(\overline{u}) = 0_A$ pour tout $\overline{u} \in \mathbb{N}^n$ et par 1 celui défini par $1((0, \dots, 0)) = 1_A$ et $1(\overline{u}) = 0_A$ pour tout $\overline{u} \in \mathbb{N}^n$ distinct de $(0, \dots, 0)$.*

Théorème 5.3.5 – *L'ensemble des polynômes à n indéterminées sur A muni des lois $+$ et $\times$ est un anneau commutatif. Ses éléments neutres sont 0 pour la loi $+$ et 1 pour la loi $\times$.*

Démonstration – Similaire à celle du théorème 5.1.4. □

Remarque 5.3.6 –

- Pour tout $a \in A$ et tout polynôme P à n indéterminées, on a $aP = (a1) \times P$.
- L'application ι de A dans l'ensemble des polynômes à n indéterminées sur A, définie par $\iota(a) = a1$ est un morphisme d'anneaux injectif.
  Ainsi on peut identifier l'anneau A au sous-anneau $\operatorname{Im}\iota$ de l'ensemble des polynômes à n indéterminées sur A en notant $\iota(a) = a$ pour tout $a \in A$.
- Les polynômes de la forme a sont appelés les *polynômes constants.*

Notation 5.3.7 – *Pour tout $i \in \{1, \dots, n\}$, si $\overline{a}_i = (0, \dots, 0, 1, 0, \dots, 0)$ désigne l'élément de $\mathbb{N}^n$ ayant toutes ses coordonnées nulles sauf la i^e qui vaut 1, alors on note X_i le polynôme à n indéterminées sur A défini par $X_i(\overline{a}_i) = 1_A$ et $X_i(\overline{u}) = 0_A$ pour $\overline{u} \neq \overline{a}_i$.*

On peut alors démontrer des résultats analogues au lemme 5.1.9 et au corollaire 5.1.10.

Proposition 5.3.8 –
- *Pour tout $i \in \{1, \dots, n\}$ et tout $k \in \mathbb{N}$, le polynôme X_i^k associe 0_A à tout $\overline{u} \in \mathbb{N}^n$ distinct de l'élément $(0, \dots, 0, k, 0, \dots, 0)$ de $\mathbb{N}^n$ ayant toute ses coordonnées nulles sauf la i^e qui vaut k, et on a alors $X_i^k((0, \dots, 0, k, 0, \dots, 0)) = 1_A$.*
- *Tout polynôme à n indéterminées sur A s'écrit de façon unique sous la forme d'une somme finie de* monômes*, c'est-à-dire d'éléments de la forme $aX_1^{k_1} \cdots X_n^{k_n}$ avec $a \in A$.*

On peut alors adopter une notation similaire à celle des polynômes sur A (notation 5.1.11).

Notation 5.3.9 – *On note $A[X_1, \dots, X_n]$ l'ensemble des polynômes à n indéterminées sur A.*

On peut abréger la notation en notant $X^{\overline{\alpha}} = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ pour tout $\overline{\alpha} = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$. Alors tout $P \in A[X_1, \dots, X_n]$ s'écrit de façon unique sous la forme $P = \sum_{\overline{\alpha} \in \mathbb{N}^n} a_{\overline{\alpha}} X^{\overline{\alpha}}$ où $a_{\overline{\alpha}}$ désigne un élément de A pour tout $\overline{\alpha} \in \mathbb{N}^n$.

Théorème 5.3.10 – *Soient B un anneau commutatif et $f : A \to B$ un morphisme d'anneaux. Pour tout n-uple $(b_1, \dots, b_n) \in B^n$, il existe un unique morphisme d'anneaux $g : A[X_1, \dots, X_n] \to B$ satisfaisant*
- *$g(a) = f(a)$ pour tout $a \in A$;*
- *$g(X_i) = b_i$ pour tout $i \in \{1, \dots, n\}$.*

Démonstration – (résumé) Par unicité de l'écriture $P = \sum_{\overline{\alpha} \in \mathbb{N}^n} a_{\overline{\alpha}} X^{\overline{\alpha}}$ pour tout $P \in A[X_1, \dots, X_n]$, on peut définir une application $g : A[X_1, \dots, X_n] \to B$ par

$$g(\sum_{\overline{\alpha} \in \mathbb{N}^n} a_{\overline{\alpha}} X^{\overline{\alpha}}) = \sum_{\overline{\alpha} \in \mathbb{N}^n} f(a_{\overline{\alpha}}) b_1^{\alpha_1} \cdots b_n^{\alpha_n}.$$

On a alors bien $g(a) = f(a)$ pour tout $a \in A$ et $g(X_i) = b_i$ pour tout $i \in \{1, \dots, n\}$. De plus, il n'est pas difficile de montrer que g est un morphisme d'anneaux, cela suit essentiellement du fait que f est un morphisme d'anneaux. Ceci démontre l'existence de g.

En outre, tout morphisme $h : [X_1, \dots, X_n] \to B$ satisfaisant $g(a) = f(a)$ pour tout $a \in A$ et $g(X_i) = b_i$ pour tout $i \in \{1, \dots, n\}$ vérifie

$$h(\sum_{\overline{\alpha} \in \mathbb{N}^n} a_{\overline{\alpha}} X^{\overline{\alpha}}) = \sum_{\overline{\alpha} \in \mathbb{N}^n} f(a_{\overline{\alpha}}) b_1^{\alpha_1} \cdots b_n^{\alpha_n} = g(\sum_{\overline{\alpha} \in \mathbb{N}^n} a_{\overline{\alpha}} X^{\overline{\alpha}})$$

pour tout $\sum_{\overline{\alpha} \in \mathbb{N}^n} a_{\overline{\alpha}} X^{\overline{\alpha}}) \in A[X_1, \dots, X_n]$, d'où l'unicité de g. □

Proposition 5.3.11 – *Si $n \geqslant 2$, les anneaux $A[X_1, \dots, X_n]$ et $A[X_1, \dots, X_{n-1}][X_n]$ sont isomorphes.*

DÉMONSTRATION – Soit $f : A \to A[X_1, \ldots, X_{n-1}][X_n]$ le morphisme défini par $f(a) = a$. D'après le théorème 5.3.10, il y a un unique morphisme d'anneaux $g : A[X_1, \ldots, X_n] \to A[X_1, \ldots, X_{n-1}][X_n]$ satisfaisant $g(a) = a$ pour tout $a \in A$ et $g(X_i) = X_i$ pour tout $i \in \{1, \ldots, n\}$.

De même, en considère le morphisme $f_1 : A \to A[X_1, \ldots, X_n]$ défini par $f(a) = a$, on obtient un unique morphisme d'anneaux $g_1 : A[X_1, \ldots, X_{n-1}] \to A[X_1, \ldots, X_n]$ satisfaisant $g_1(a) = a$ pour tout $a \in A$ et $g_1(X_i) = X_i$ pour tout $i \in \{1, \ldots, n-1\}$. Le théorème 5.3.10 appliqué à g_1 donne ensuite un unique morphisme d'anneaux $h : A[X_1, \ldots, X_{n-1}][X_n] \to A[X_1, \ldots, X_n]$ satisfaisant $h(P) = g_1(P)$ pour tout $P \in A[X_1, \ldots, X_{n-1}]$ et $h(X_n) = X_n$.

On remarque que, pour tout $a \in A$ on a $h(g(a)) = h(a) = g_1(a) = a$, pour tout $i \in \{1, \ldots, n-1\}$ on a $h(g(X_i)) = h(X_i) = g_1(X_i) = X_i$ et que $h(g(X_n)) = h(X_n) = X_n$. Ainsi $h \circ g$ est l'unique endomorphisme de $A[X_1, \ldots, X_n]$ satisfaisant $(h \circ g)(a) = a$ pour tout $a \in A$ et $(h \circ g)(X_i) = X_i$ pour tout $i \in \{1, \ldots, n\}$, c'est donc l'identité et g est donc un isomorphisme. □

Remarque 5.3.12 – L'isomorphisme g ainsi construit vérifie $g(a) = a$ pour tout $a \in A$.

Corollaire 5.3.13 – *L'anneaux $A[X_1, \ldots, X_n]$ est intègre si et seulement si A est intègre.*

DÉMONSTRATION – Ceci découle du corollaire 5.1.17 et de la proposition précédente. □

Corollaire 5.3.14 – *Si l'anneau A est intègre, les éléments inversibles de $A[X_1, \ldots, X_n]$ sont les polynômes constants de la forme $P = a$ pour $a \in A^\times$.*

DÉMONSTRATION – On procède par récurrence sur $n \in \mathbb{N}^*$. D'après le corollaire 5.1.18, le résultat est vrai si $n = 1$. Supposons le résultat vrai pour $n \in \mathbb{N}^*$. Alors les éléments inversibles de $A[X_1, \ldots, X_n]$ sont les polynômes constants de la forme $P = a$ pour $a \in A^\times$. D'aprés le corollaire 5.1.18, les éléments inversibles de $A[X_1, \ldots, X_n][X_{n+1}]$ sont les éléments inversibles de $A[X_1, \ldots, X_n]$, ce sont donc les polynômes constants de la forme $P = a$ pour $a \in A^\times$. Comme $A[X_1, \ldots, X_{n+1}]$ et $A[X_1, \ldots, X_n][X_{n+1}]$ sont isomorphes par un isomorphisme g tel que $g(a) = a$ pour tout $a \in A$, on en déduit que le résultat est vrai pour $n + 1$. Ceci fini notre démonstration. □

Chapitre 6

Arithmétique dans les anneaux

Dans ce chapitre, on fixe un anneau *intègre* A.

6.1 Éléments irréductibles

Définition 6.1.1 – *Soit x un élément non inversible de l'anneau intègre A. On dit que x est* irréductible *s'il n'est pas le produit de deux éléments non inversibles.*

Remarque 6.1.2 – Les éléments irréductibles sont non nuls *(car 0_A n'est pas inversible et $0_A = 0_A \cdot 0_A$).*

Proposition 6.1.3 – *Tout élément premier de A est irréductible.*

Démonstration –

□

Remarque 6.1.4 –

Définition 6.1.5 – *Deux éléments a et b de A sont dits* premiers entre eux *si leurs seuls diviseurs communs sont les éléments inversibles de A.*

Remarque 6.1.6 – Ne pas confondre *premiers entre eux* et *étrangers* : deux éléments a et b sont *étrangers* s'il existe $(u, v) \in A^2$ tel que $au + bv = 1_A$.

En effet, si deux éléments a et b sont étrangers, ils sont premiers entre eux (*car leurs diviseurs communs divisent 1_A et sont donc inversibles*), mais la réciproque est fausse. *Par exemple*

Lemme 6.1.7 – *Soit a un élément irréductible de A. Alors tout $b \in A$ est soit premier avec a, soit divisible par a.*

Démonstration – Si b n'est pas premier avec a, alors a et b ont un diviseur commun non inversible d. En particulier, il existe $u \in A$ tel que $a = du$, et comme a est irréductible, u est inversible. On obtient $d = au^{-1}$, donc a divise d. Comme d divise b, on en déduit que a divise b. □

Définition 6.1.8 – *Deux éléments a et b de A sont* associés *si $a|b$ et $b|a$.*

Exemples 6.1.9 – Tout élément de A est associé à son opposé.

Lemme 6.1.10 – *Les conditions suivantes sont équivalentes pour tous les éléments a et b de A :*

- *a et b sont associés ;*
- *$(a) = (b)$.*
- *il existe $u \in U(A)$ tel que $b = ua$;*

Démonstration – Si a et b sont associés, alors comme $a|b$, on a $b \in aA = (a)$ d'où $(b) \subseteq (a)$, et comme on a aussi $b|a$, alors on a aussi $(a) \subseteq (b)$, et ainsi $(a) = (b)$.

Si $(a) = (b)$, alors on a $b \in (a) = aA$ et il existe $u \in A$ tel que $b = au$. Or on a aussi $a \in bA$, donc il existe $v \in A$ tel que $a = bv$. On a donc $b = (bv)u$, d'où $b(1_A - vu) = 0_A$. Comme A est intègre, on en déduit que soit $vu = 1_A$ et u est inversible, soit $b = 0_A$, et dans ce cas on a aussi $a = 0_A$ puisque $(a) = (b)$, d'où $b = ua$ pour $u = 1_A \in U(A)$. Dans les deux cas, il existe $u \in U(A)$ tel que $b = ua$.

Si $b = ua$ pour $u \in U(A)$, alors $a|b$ et on a aussi $a = u^{-1}b$, donc $b|a$. Ainsi a et b sont associés. □

Remarque 6.1.11 – Tout élément associé à un élément irréductible est irréductible.

Proposition 6.1.12 – *Si A est euclidien, tous ses éléments non nuls se décomposent en un produit d'un élément inversible par un produit d'éléments irréductibles.*

Démonstration –

□

6.2 $PGCD$ et $PPCM$

6.2.1 Généralités

Définition 6.2.1 – *Soient a et b deux éléments de A.*

- *Un $PGCD$ (ou* plus grand diviseur commun*) de a et b est un diviseur commun à a et b tel que tout autre diviseur de a et b divise d.*
- *Un $PPCM$ (ou* plus petit multiple commun*) de a et b est un multiple commun à a et b tel que tout autre multiple de a et b est un multiple de m.*
- Plus généralement, on dit que d (resp. m) est un $PGCD$ (resp. $PPCM$) d'un nombre fini d'éléments $a_0, \ldots, a_n$ de A si d est un diviseur (resp. m est un multiple) commun à $a_0, \ldots, a_n$ tel que tout autre diviseur (resp. multiple) de $a_0, \ldots, a_n$ divise d (resp. est un multiple de m).

Remarque 6.2.2 –

- En général, deux éléments d'un anneau intègre n'ont ni $PGCD$ ni $PPCM$. Par exemple

— Dire que a et b sont premiers entre eux équivaut à dire que 1_A est un $PGCD$ de a et b.
— Si $a = 0_A$, alors b est un $PGCD$ de a et b et 0_A est un $PPCM$ de a et b.
— Si d est un $PGCD$ de a et b, alors tout autre $PGCD$ de a et b est associé à d.
— Si m est un $PPCM$ de a et b, alors tout autre $PPCM$ de a et b est associé à m.

Proposition 6.2.3 – *Si deux éléments a et b de A admettent un $PGCD$ et un $PPCM$ notés respectivement d et m, alors dm et ab sont associés.*

Démonstration – Si $a = 0_A$, alors $m = 0_A$ d'où $dm = 0_A = ab$. On peut donc supposer $a \neq 0_A$ et, de même, $b \neq 0_A$. En particulier d est non nul.

Comme d divise a et b, il existe u et v dans A tels que $a = ud$ et $b = vd$. On en déduit que uvd est un multiple de a et b, donc c'est un multiple de m, et il existe $q \in A$ tel que $mq = uvd$. Or m est un multiple de a et b, donc il existe x et y dans A tels que $m = ax = by$. On a donc $(ax)q = mq = uvd = av$, d'où $a(xq - v) = 0_A$. Or a est non nul et A est intègre, donc $xq = v$. De même, on montre que $yq = u$. Ainsi q divise u et v, donc qd divise $a = ud$ et $b = vd$ et il divise alors d puisque c'est un $PGCD$ de a et b. Comme d divise qd, on en déduit que d et qd sont associés, d'où $d = rqd$ pour $r \in U(A)$ d'après le lemme 6.1.10. On a donc $d(1_A - rq) = 0_A$, et comme $d \neq 0_A$, on obtient $rq = 1_A$ et q est inversible.

Comme on a $mq = uvd$, on a $(dm)q = duvd = ab$, ce qui démontre que dm et ab sont associés. □

Remarque 6.2.4 –
— Dire que m est un $PPCM$ de $a_0, \ldots, a_n$ est équivalent à dire que $(m) = \cap_{i=0}^{n}(a_i)$. [*En effet, les multiples communs à $a_0, \ldots, a_n$ sont les éléments de $\cap_{i=0}^{n}(a_i)$.*]

— Dire que d est un $PGCD$ de $a_0, \ldots, a_n$ est équivalent à dire qu'on a $(a_0)+\cdots+(a_n) \subseteq (d) \subseteq (d^*)$ pour tout diviseur commun d^* à $a_0, \ldots, a_n$.
[*En effet, pour tout $d^* \in A$, être un diviseur commun à $a_0, \ldots, a_n$ équivaut à diviser tous les éléments de $(a_0) + \cdots + (a_n)$, c'est-à-dire vérifier $(a_0) + \cdots + (a_n) \subseteq (d^*)$. Dire que l'élément d est, de plus, un $PGCD$ signifie que tout tel élément d^* divise d, c'est-à-dire vérifie $(d) \subseteq (d^*)$.*]

6.2.2 L'algorithme d'Euclide

L'algorithme d'Euclide pour les entiers relatifs se généralise naturellement aux anneaux euclidiens. On fixe A un anneau euclidien et φ un stathme sur A. Considèrons deux éléments a et b de A. Si a et b sont nuls, l'élément $d = 0_A$ est leur unique $PGCD$. Sinon,

6.2.3 Le théorème des restes chinois

Définition 6.2.5 – Ici A est un anneau commutatif quelconque. *Deux éléments a et b de A sont dits* étrangers *s'il existe deux éléments u et v de l'anneau tels que $au + bv = 1_A$.*

Remarque 6.2.6 –
- Comme cela a déjà été dit plus haut, deux éléments étrangers sont premiers entre eux (*car tout diviseur commun à a et b divise $1_A = au + bv$ et est donc inversible*).
- La réciproque est vraie dans les anneaux principaux puisque, dans un tel anneau, tous deux éléments a et b premiers entre eux vérifient $(a) + (b) = (1_A)$: autrement dit, *dans un anneau principal, deux éléments a et b sont premiers entre eux si et seulement s'il existe des éléments u et v tels que $au + bv = 1_A$* (Identité de Bézout).

Définition 6.2.7 – *On dit que deux idéaux I et J d'un anneau commutatif quelconque A sont* premiers entre eux *si $I + J = A$.*

Remarque 6.2.8 – Soient u et v deux éléments d'un anneau commutatif quelconque A. Alors u et v sont étrangers si et seulement si les idéaux (u) et (v) sont premiers entre eux.

Proposition 6.2.9 – **(Théorème des restes chinois *pour un anneau commutatif*)** Ici A est un anneau commutatif quelconque. *Si $I_0, \ldots, I_n$ sont des idéaux de A deux à deux premiers entre eux, alors on a $I_0 \cdots I_n = \cap_{k=0}^n I_k$ et les anneaux $A/I_0 \cdots I_n$ et $A/I_0 \times \cdots \times A/I_n$ sont isomorphes.*

Démonstration – On considère l'application $f : A \to A/I_0 \times \cdots \times A/I_n$ définie par $f(x) = (\overline{x}^0, \ldots, \overline{x}^n)$ où, pour tout $i \in \{0, \ldots, n\}$, on note $\overline{x}^i$ la classe de x modulo I_i. Il s'agit d'un morphisme d'anneaux et son noyau est $\mathrm{Ker}\, f = \cap_{k=0}^n I_k$.

Si I et J sont deux idéaux premiers entre eux, alors on a $1_A = u + v$ pour $(u, v) \in I \times J$, donc tout $x \in I \cap J$ s'écrit sous la forme $x = ux + xv \in IJ$ (*on rappelle que IJ désigne l'idéal engendré par les éléments de la forme xy pour $x \in I$ et $y \in J$*). Comme on a $IJ \subseteq I \cap J$, on en déduit que $I \cap J = IJ$.

Si un idéal I est premier avec des idéaux J_1 et J_2, alors on a $A = (I + J_1)(I + J_2) = I + J_1J_2$ et I est premier avec J_1J_2.

Ces deux remarques impliquent d'une part que $\mathrm{Ker}\, f = \cap_{k=0}^n I_k = I_0 \cdots I_n$, d'autre part que, pour tout $k \in \{0, \ldots, n\}$, l'idéal I_k est premier avec le produit J_k des idéaux I_l pour $l \neq k$. Ainsi on a $1_A = x + y$ pour $(x, y) \in I_k \times J_k$. Alors, pour tout $a \in A$, on a $a = ax + ay$ et

$$\begin{aligned} f(a - ax) &= f(ay) \\ &= (\overline{ay}^0, \ldots, \overline{ay}^{k-1}, \overline{a - ax}^k, \overline{ay}^{k+1}, \ldots, \overline{ay}^n) \\ &= (\overline{0_A}^0, \ldots, \overline{0_A}^{k-1}, \overline{a}^k, \overline{0_A}^{k+1}, \ldots, \overline{0_A}^n). \end{aligned}$$

Comme ceci est valable pour tout $k \in \{0, \ldots, n\}$, l'application f est surjective. □

Corollaire 6.2.10 – **(Théorème des restes chinois (seconde version))**

Démonstration –

□

Corollaire 6.2.11 – **(Théorème des restes chinois *pour un anneau principal*)** On suppose que A est un anneau principal. *Si $a_0, \ldots, a_n$ sont des éléments de A deux à deux premiers entre eux, alors les anneaux $A/(a_0 \cdots a_n)$ et $A/(a_0) \times \cdots \times A/(a_n)$ sont isomorphes.*

Démonstration – Comme A est principal, les éléments $a_0, \ldots, a_n$ sont deux à deux étrangers, et la seconde version du théorème des restes chinois donne le résultat. □

Exemples 6.2.12 – **(Application aux systèmes de congruences)**

6.3 Anneaux à $PGCD$

6.3.1 Généralités

Définition 6.3.1 –

Remarque 6.3.2 –

— Un tel anneau est parfois appelé *anneau de Gauss*.
— Certains auteurs remplacent le mot *intègre* de la définition par *commutatif*.
— Il suit de la proposition 6.2.3 que, si deux éléments a et b de A sont premiers entre eux, alors tout $PPCM$ de a et b est associé à ab, donc ab est un $PPCM$ de a et b.

Exemples 6.3.3 –

Lemme 6.3.4 – *Si $a_0, \ldots, a_n$ sont des éléments d'un anneau à $PGCD$, ils admettent un $PGCD$.*

Démonstration – On obtient un tel $PGCD$ par récurrence sur n. On peut supposer $n \geqslant 1$. Soit d' est un $PGCD$ de $a_0, \ldots, a_{n-1}$. Comme l'anneau est à $PGCD$, il existe un $PGCD$ d à d' et a_n. En particulier, d est un diviseur commun à $a_0, \ldots, a_n$.

Si d^* est un autre diviseur commun à $a_0, \ldots, a_n$, alors d^* est en particulier un diviseur commun à $a_0, \ldots, a_{n-1}$, et il divise donc d'. Ainsi d^* est un diviseur commun à d' et a_n, et il divise donc d. Ceci montre que d est un $PGCD$ de $a_0, \ldots, a_n$. □

Lemme 6.3.5 – On suppose que A est un anneau à $PGCD$. *Soient a, b et d trois éléments de A avec d non nul. Alors d est un $PGCD$ de ad et bd si et seulement si a et b sont premiers entre eux.*

Démonstration –

□

Les trois résultats ci-dessous montrent l'intérêt de ces anneaux.

Proposition 6.3.6 – **(Lemme de Gauss)** On suppose que A est un anneau à $PGCD$. *Soient a, b et c trois éléments de A. Si a et b sont premiers entre eux et si a divise bc, alors a divise c.*

Démonstration – On peut supposer c non nul. C'est alors un $PGCD$ de ac et bc d'après le lemme 6.3.5. Or, comme a divise bc, c'est un diviseur commun de ac et bc, donc a divise c. □

Corollaire 6.3.7 – On suppose que A est un anneau à $PGCD$. *Soient a, b et c trois éléments de A. Alors a est premier avec bc si et seulement si a est premier avec b et c.*

Démonstration – Supposons a premier avec bc. Comme un diviseur commun à a et b est un diviseur commun à a et bc, a est premier avec b. De même il est premier avec c.

Réciproquement, supposons que a soit premier avec b et c, et notons d un diviseur commun à a et bc. Comme d divise a, il est premier avec b et c, et le lemme de Gauss appliqué à bc puis $c1_A$ montre que d est inversible, donc a est premier avec bc. □

Corollaire 6.3.8 – On suppose que A est un anneau à $PGCD$. *Soit $n \in \mathbb{N}^*$. Si $a_0, \ldots, a_n$ sont $n+1$ éléments de A deux à deux premiers entre eux, alors $a_0 \cdots a_n$ est un $PPCM$ de $a_0, \ldots, a_n$.*

Démonstration – On montre le résultat par récurrence sur $i \in \{1, \ldots, n\}$. Pour $i = 1$, le résultat découle de la remarque 6.3.2. Si le résultat est vrai pour $n \in \mathbb{N}^*$, alors $a_0 \cdots a_n$ est un $PPCM$ de $a_0, \ldots, a_n$, et on a donc $\cap_{i=0}^{n}(a_i) = (a_0 \cdots a_n)$. Or le corollaire 6.3.7 montre

que a_{n+1} est premier avec $a_0 \dots a_n$, donc d'après la remarque 6.3.2, le produit $a_0 \cdots a_{n+1}$ est un $PPCM$ de $a_0 \cdots a_n$ et a_{n+1}, d'où $(a_0 \cdots a_n) \cap (a_{n+1}) = (a_0 \cdots a_{n+1})$. Finalement on a $\cap_{i=0}^{n+1}(a_i) = (a_0 \cdots a_{n+1})$ et $a_0 \cdots a_{n+1}$ est un $PPCM$ de $a_0 \cdots a_{n+1}$. □

Proposition 6.3.9 – Dans un anneau à $PGCD$, *les éléments irréductibles sont ceux qui sont premiers.*

Démonstration –

□

Nous finissons par deux résultats donnés seulement pour information.

Proposition 6.3.10 – *Dans un anneau à $PGCD$, tous les couples d'éléments de A admettent un $PPCM$.*

Démonstration – Supposons d'abord que l'anneau A est à $PGCD$. Soient a et b deux éléments de A. Montrons qu'ils admettent un $PPCM$. Si a ou b est nul, ils admettent 0_A comme $PPCM$, donc on peut supposer a et b non nuls.

Soit d un $PGCD$ de a et b. Comme a et b sont non nuls, l'élément d est aussi non nul. Aussi d divise a, donc d divise ab et il existe $m \in A$ tel que $ab = dm$. Comme d divise a et b, il existe u et v dans A tels que $a = ud$ et $b = vd$. On a alors $(ud)b = dm$ et $d(ub - m) = 0_A$. Comme A est intègre et d est non nul, $m = ub$ et m est un multiple de b. De la même façon, $m = va$ est un multiple de a.

Soit m' un autre multiple commun à a et b. Soient μ un $PGCD$ de m et m', et $q \in A$ tel que $m = q\mu$. Comme a et b divisent m et m', on en déduit que μ est un multiple commun à a et b, il existe donc α et β dans A tels que $\mu = \alpha a = \beta b$. Ainsi on a $ab = dm = d(q\mu) = dq\alpha a$, et comme a est non nul, $b = dq\alpha$. Or on a vu que $b = vd$ et que d est non nul, donc on a $v = q\alpha$. De même on a $u = q\beta$. Ceci montre que q divise u et v, donc qd divise a et b, et ainsi qd divise d. Comme d divise qd, on en déduit que d et qd sont associés, d'où $d = rqd$ pour $r \in U(A)$ d'après le lemme 6.1.10. On a donc $d(1_A - rq) = 0_A$, et comme $d \neq 0_A$, on obtient $rq = 1_A$ et q est inversible. Ceci montre que $\mu = q^{-1}m$, donc m divise μ, et aussi m' puisque $\mu | m'$. On a montré que m est un $PPCM$ de a et b. □

Corollaire 6.3.11 – *Si $a_0, \dots, a_n$ sont des éléments d'un anneau à $PGCD$, ils admettent un $PPCM$.*

DÉMONSTRATION – Comme tout couple d'éléments de A admet un $PPCM$, on peut définir des éléments $m_0, \ldots, m_n$ par $m_0 = a_0$ et $(m_{i+1}) = (m_i) \cap (a_{i+1})$ pour tout $i \in \{0, \ldots, n-1\}$. Alors on a $(m_n) = \cap_{i=0}^{n}(a_i)$ et m_n est un $PPCM$ de $a_0, \ldots, a_n$. □

6.3.2 Une propriétés des racines des polynômes unitaires

Nous commençons par un résutat généralisant l'écriture d'un nombre rationnel sous forme d'une fraction irréductible.

Proposition 6.3.12 – On suppose que A est un anneau à $PGCD$. *Tout élément x du corps des fractions de A s'écrit sous la forme $x = \frac{a}{b}$ pour des éléments a et b de A premiers entre eux.*

DÉMONSTRATION – Soit x un élément du corps des fractions de A. Alors $x = \frac{a'}{b'}$ pour des éléments a' et b' de A avec b' non nul. Soit d un $PGCD$ de a' et b'. Alors il existe a et b dans A tels que $a' = ad$ et $b' = bd$. Comme on a $a'b = abd = ab'$, on a $x = \frac{a}{b}$, et a et b sont premiers entre eux d'après le lemme 6.3.5. □

Définition 6.3.13 –

Proposition 6.3.14 –

Démonstration –

□

Exemples 6.3.15 – Comme $\mathbb{Z}$ est un anneau à $PGCD$, il est intégralement clos d'après la proposition 6.3.14. Ceci généralise le résultat bien connu suivant : pour tout $a \in \mathbb{N}$ et tout $n \in \mathbb{N}^*$, *comme* $\sqrt[n]{a}$ *est une racine du polynôme unitaire* $X^n - a \in \mathbb{Z}[X]$, le nombre $\sqrt[n]{a}$ est soit un entier, soit un irrationnel.

Chapitre 7

Anneaux factoriels

Dans ce chapitre, on fixe un anneau *intègre* A.

7.1 Définition

Définition 7.1.1 – *L'anneau intègre A est* factoriel *si*

1. *ses éléments non nuls se décomposent tous en un produit d'un élément inversible u par un produit d'éléments irréductibles $p_1, \ldots, p_r$;*

2. *cette décomposition est unique* à permutation près et à multiplication par des inversibles près. *Autrement dit, si $vq_1 \cdots q_s$ est une autre telle décomposition du même élément, alors il y a une bijection $\pi : \{p_1, \ldots, p_r\} \to \{q_1 \cdots q_s\}$ telle que p_i et $\pi(p_i)$ sont associés pour tout $i \in \{1, \ldots, r\}$.*

Proposition 7.1.2 – *Si l'anneau intègre A vérifie la première condition et que ses éléments irréductibles sont tous premiers, alors il est factoriel.*

Démonstration –

□

Corollaire 7.1.3 – *Tout anneau euclidien est factoriel.*

Démonstration –

□

7.1.1 Qu'en est-il des anneaux principaux ?

On a vu que tout anneau principal est un anneau à $PGCD$ (exemple 6.3.3). Vous êtes vivement invités à lire la remarque 7.1.5 ci-dessous au sujet du théorème suivant.

Théorème 7.1.4 – *Tout anneau principal est factoriel.*

Démonstration – **(attention : cette démonstration comporte un point délicat)** Comme A est un anneau à $PGCD$, ses éléments irréductibles sont premiers (proposition 6.3.9) et, d'après la proposition 7.1.2, il suffit de montrer que A vérifie la 1re condition de la définition 7.1.1. Par l'absurde, supposons que ce ne soit pas le cas. Alors l'ensemble B formé des éléments non nuls de A qui ne satisfont pas la 1re condition de la définition 7.1.1 est non vide.

Comme les éléments de B sont non nuls, non inversibles et non irréductibles, tout $x \in B$ se décompose en un produit $x = ab$ de deux éléments non inversibles a et b, qui sont non nuls puisque $x \neq 0_A$. Aussi, comme tout multiple de x est un multiple de a et b, on a $(x) \subseteq (a) \cap (b)$.

Montrons que (a) et (b) contiennent strictement (x). Si on a $(x) = (a)$, alors d'après le lemme 6.1.10, x et a sont asociés et il existe $u \in U(A)$ tel que $x = ua$. On a donc $ua = x = ab$, et comme a est non nul, l'élément $b = u$ est inversible, ce qui contredit le choix de b. On obtient $(x) \neq (a)$ et, de même, $(x) \neq (b)$. Ainsi (a) et (b) contiennent strictement (x).

Notons qu'au moins un des deux éléments a et b appartient à B, sinon les décompositions de a et b fourniraient une décomposition de x conforme à la 1re condition de la définition 7.1.1.

On en déduit qu'on peut construire une suite $(x_i)_{i\in\mathbb{N}}$ d'éléments de B telle que $x_0 = x$ et, pour tout $i \in \mathbb{N}$, l'idéal (x_i) est strictement contenu dans (x_{i+1}) (**voir le commentaire ci-dessous concernant cette phrase**). Notons $I = \cup_{i\in\mathbb{N}}(x_i)$ l'union de tous ces idéaux. C'est un idéal de A car :

- on a $0_A \in (x_0) \subseteq I$;
- pour tout $(u, v) \in I \times I$, il existe $j \in \mathbb{N}$ tel que u et v appartiennent à (x_j), donc
  - $u - v \in (x_j) \subseteq I$ (ainsi I est un sous-groupe de $(A, +)$), et
  - on a $\alpha u \in (x_j) \subseteq I$ pour tout $\alpha \in A$.

Comme A est principal, il existe $y \in A$ tel que $I = (y)$, mais comme $I = \cup_{i\in\mathbb{N}}(x_i)$, il existe $k \in \mathbb{N}$ tel que $y \in (x_k)$, d'où $I = (x_k)$, ce qui contredit le fait que (x_k) soit strictement contenu dans (x_{k+1}). □

Remarque 7.1.5 –

- La phrase ci-dessous, extraite de la démonstration, utilise l'axiome du choix :

  on peut construire une suite $(x_i)_{i\in\mathbb{N}}$ d'éléments de B telle que $x_0 = x$ et, pour tout $i \in \mathbb{N}$, l'idéal (x_i) est strictement contenu dans (x_{i+1}).

  En effet, nous choisissons ici une infinité d'éléments de B. Il s'agit d'une infinité dénombrable d'éléments, mais comme le choix de chaque élément dépend du précédent, on utilise quelque chose de plus fort que l'axiome du choix dénombrable. Nous utilisons précisément l'**axiome du choix dépendant** qui stipule que :

  pour tout ensemble non vide X et toute relation R sur X, si pour tout $x \in X$ il existe $y \in X$ tel que xRy, alors il existe une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de X telle qu'on ait x_nRx_{n+1} pour tout $n \in \mathbb{N}$.

L'existence de la suite $(x_i)_{i\in\mathbb{N}}$ de notre démonstration découle de cet axiome en prenant $X = B$ et R la relation définie sur X par :

$$xRy \text{ lorsque } (x) \text{ est strictement contenu dans } (y).$$

— L'axiome du choix dépendant a été introduit en 1942 par le logicien suisse Paul Bernays (1888-1977). Il est démontré que cet axiome est strictement plus fort que l'axiome du choix dénombrable et strictement plus faible que l'axiome du choix. Tout comme l'axiome du choix dénombrable, cet axiome est généralement admis, et souvent il n'est pas mentionné lorsqu'il est utilisé.

— L'axiome est équivalent au "lemme de König", qui affirme que *tout arbre infini à branchement fini a une branche infinie*; il s'agit d'un résultat démontré en 1927 par le mathématicien hongrois Dénes König (1884-1944), et donc antérieur à l'axiome du choix dépendant.

— L'axiome du choix dépendant n'est pas à connaître, en revanche avoir conscience que la construction faite dans la démonstration ci-dessus n'est pas une simple récurrence serait bien.

— En particulier, il ne faut pas confondre ce qui est fait ci-dessus avec ce qu'on a fait, par exemple, lorsqu'on écrit l'algorithme d'Euclide : dans ce cas-ci, on a juste choisi un élément de $(r_0, \dots, r_{\varphi(b)+1})$ de $A^{\varphi(b)+2}$ satisfaisant la condition "*pour tout* $i \in \{0, \dots, \varphi(b) - 1\}$*, si* $r_{i+1} = 0_A$ *alors* $r_{i+2} = 0_A$*, si* r_{i+1} *divise* r_i *alors* $r_{i+2} = 0_A$*, sinon* r_{i+2} *vérifie* $\varphi(r_{i+2}) < \varphi(r_{i+1})$ *et* $r_i = r_{i+1}q + r_{i+2}$ *pour* $q \in A$."

— Le théoricien des modèles Wilfrid Hodges a démontré en 1976 que **les axiomes du système ZF sont insuffisants pour démontrer que tout anneau principal est factoriel**. À ma connaissance il n'est pas démontré que le théorème est équivalent à l'axiome du choix dépendant, mais je ne connais pas de démonstration ne faisant pas usage de cet axiome.

7.2 Valuation

Dans la suite de cette section, on suppose que A est un anneau factoriel.

Remarque 7.2.1 – Le "*produit d'éléments irréductibles* $p_1, \dots, p_r$" peut éventuellement être vide : par convention un produit vide vaut 1_A, c'est ce qui se passe pour les éléments inversibles de A.

Définition 7.2.2 – *Pour tout $a \in A$ non nul et tout élément irréductible p de A, on appelle* valuation de a en p *le nombre déléments irréductibles associés à p dans une décomposition de a en un produit d'un élément inversible u par un produit d'éléments irréductibles. La valuation de a en p se note $v_p(a)$.*

Remarque 7.2.3 – Il suit de l'unicité de la décomposition que $v_p(a)$ ne dépend pas de la décomposition choisie.

Lemme 7.2.4 – *Pour tous éléments a et b non nuls de A et tout élément irréductible p de A, on a $v_p(ab) = v_p(a) + v_p(b)$.*

DÉMONSTRATION – Soient $a = up_1 \cdots p_r$ et $b = vq_1 \cdots q_s$ des décompositions de a et b pour des éléments inversibles u et v et des éléments irréductibles $p_1, \ldots, p_r, q_1, \ldots, q_s$. Alors ab se décompose sous la forme $ab = (uv)(p_1 \cdots p_r q_1 \cdots q_s)$ avec uv inversible, d'où $v_p(ab) = v_p(a) + v_p(b)$. □

Proposition 7.2.5 – *Pour tout $a \in A$ non nul et tout élément irréductible p de A, il y a une plus grande puissance de p qui divise a, c'est $p^{v_p(a)}$.*

DÉMONSTRATION – Soit $a = uq_1 \cdots q_s$ une décomposition de a en un produit d'un élément inversible u par un produit d'éléments irréductibles $q_1, \ldots, q_s$. Par définition de la valuation, il y a $v_p(a)$ éléments parmi $q_1, \ldots, q_s$ qui sont associés à p ; pour chaque tel élément q_j, il y a un inversible v_{q_j} de A tel que $q_j = v_{q_j} p$, on note v le produit des tels éléments u_{q_j}. Alors $vp^{v_p(a)}$ est égal au produit des éléments q_j associés à p, ce qui montre que $p^{v_p(a)}$ divise a.

Si $p^{v_p(a)+1}$ divise a, il existe $d \in A^*$ tel que $a = dp^{v_p(a)+1}$. Soit $d = wp_1 \cdots p_r$ une décomposition de d en un produit d'un élément inversible w et d'un produit d'éléments irréductibles $p_1, \ldots, p_r$. Comme $a = wp_1 \cdots p_r p^{v_p(a)+1}$ est une décomposition de a en un produit d'un élément inversible w par un produit d'éléments irréductibles, cette décomposition doit comporter $v_p(a)$ éléments associés à p. Or elle en comporte au moins $v_p(a) + 1$, ce qui est impossible. Ainsi $p^{v_p(a)}$ est bien la plus grande puissance de p qui divise a. □

Corollaire 7.2.6 – *Tout $a \in A$ non nul se décompose sous la forme $a = u \prod_{i=1}^{r} p_i^{v_{p_i}(a)}$ pour un élément inversible u et des éléments irréductibles $p_1, \ldots, p_r$ deux à deux non associés.*

DÉMONSTRATION – Par définition d'un anneau factoriel, on peut décomposer a sous la forme $a = v \prod_{j=1}^{s} q_j$ pour un élément inversible v et des éléments irréductibles $q_1, \ldots, q_s$. On choisit des éléments $p_1, \ldots, p_r$ deux à deux non associés de telle sorte que, pour tout $j \in \{1, \ldots, s\}$, l'élément q_j soit associé à un élément p_i pour $i \in \{1, \ldots, r\}$: on a alors $q_j = v_j p_i$ pour un élément inversible v_j. Par définition de la valuation, on obtient $a = u \prod_{i=1}^{r} p_i^{v_{p_i}(a)}$ où $u = v \prod_{j=1}^{s} v_j$. □

Corollaire 7.2.7 – *Pour tous éléments a et b non nuls de A, l'élément a divise b si et seulement si $v_p(a) \leqslant v_p(b)$ pour tout irréductible p de A.*

DÉMONSTRATION – Si a divise b, alors pour tout irréductible p de A, la plus grande puissance de p qui divise a est $p^{v_p(a)}$ d'après la proposition 7.2.5, donc $p^{v_p(a)}$ divise b et on a $v_p(a) \leqslant v_p(b)$ d'après la proposition 7.2.5.

Réciproquement, supposons $v_p(a) \leqslant v_p(b)$ pour tout irréductible p de A. D'après le corollaire 7.2.6, on a $b = u \prod_{i=1}^{r} p_i^{v_{p_i}(b)}$ pour un élément inversible u et des éléments irréductibles $p_1, \ldots, p_r$ deux à deux non associés. On décompose a sous la forme $a = v \prod_{j=1}^{s} q_j$ pour un élément inversible u et des éléments irréductibles $q_1, \ldots, q_s$. Alors, pour tout $j \in \{1, \ldots, s\}$, il existe un unique $i \in \{1, \ldots, r\}$ tel que q_j soit associé à p_i. On a alors $q_j = v_j p_i$ pour un élément inversible v_j, et on obtient $a = u \prod_{i=1}^{r} p_i^{v_{p_i}(a)}$ où $u = v \prod_{j=1}^{s} v_j$. Comme on a $v_p(a) \leqslant v_p(b)$ pour tout irréductible p, on en déduit que a divise b. □

Théorème 7.2.8 – *Tout anneau factoriel est un anneau à PGCD.*

DÉMONSTRATION – Soient a et b deux éléments de A. Montrons qu'ils admettent un $PGCD$. On peut supposer a et b non nuls. D'après le corollaire 7.2.6, on peut décomposer a et b sous la forme $a = u\prod_{i=1}^{r} p_i^{v_{p_i}(a)}$ et $b = v\prod_{j=1}^{s} q_j^{v_{q_j}(b)}$ pour des éléments inversibles u et v et des éléments irréductibles $p_1, \dots, p_r, q_1, \dots, q_s$. On fixe des éléments irréductibles $r_1, \dots, r_t$ deux à deux non associés tels que chaque élément $p_1, \dots, p_r, q_1, \dots, q_s$ soit associé à l'un des éléments $r_1, \dots, r_t$. On peut alors écrire $a = u'\prod_{i=1}^{t} r_i^{v_{r_i}(a)}$ et $b = v'\prod_{i=1}^{t} r_i^{v_{r_i}(b)}$ pour des éléments inversibles u' et v'.

On note $d = \prod_{i=1}^{t} r_i^{\min(v_{r_i}(a),v_{r_i}(b))}$ et $m = \prod_{i=1}^{t} r_i^{\max(v_{r_i}(a),v_{r_i}(b))}$. Alors d est un diviseur de a et b et m est un multiple de a et b. De plus, d'après le corollaire 7.2.7, tout diviseur commun de a et b divise d et tout multiple commun de a et b est un multiple de m, donc d est un $PGCD$ de a et b et m est un $PPCM$ de a et b. □

Remarque 7.2.9 – Il existe des anneaux à $PGCD$ qui ne sont pas factoriels, vous verrez notamment en TD que $A = \mathbb{Z} + X\mathbb{Q}[X]$ est un tel anneau.

Il en existe d'autres, notamment l'*anneau des entiers algébriques* (l'ensemble des nombres complexes qui sont racines d'un polynôme unitaire à coefficients dans $\mathbb{Z}$) et l'*anneau des fonctions holomorphes sur* $\mathbb{C}$, mais il n'est pas possible de démontrer ces propriétés en quelques lignes.

7.3 Une autre approche

Il existe une autre méthode pour analyser les anneaux factoriels. Il s'agit de commencer en fixant un *système représentatif d'éléments irréductibles*, ce qui permet de simplifier certaines démonstrations. L'inconvénient de cette méthode est qu'elle nécessite l'axiome du choix : sans lui, un tel système n'existe pas forcément.

Définition 7.3.1 – *Un* système représentatif d'éléments irréductibles *de A est une famille $\mathscr{P}$ d'éléments irréductibles de A ayant la propriété que tout élément irréductible de A est associée à un unique élément de $\mathscr{P}$.*

Exemples 7.3.2 –

- Les éléments irréductibles de $\mathbb{Z}$ sont les nombres premiers et leurs opposés, donc l'ensemble des nombres premiers est un système représentatif d'éléments irréductibles de $\mathbb{Z}$.
- Si $\mathbb{K}$ est un corps commutatif, tout polynôme non nul de $\mathbb{K}[X]$ est associé à un unique polynômes unitaire, donc l'ensemble des polynômes unitaires irréductibles sur $\mathbb{K}$ est un système représentatif d'éléments irréductibles de $\mathbb{K}[X]$.

Remarque 7.3.3 – L'exemple ci-dessus montre que, dans certains cas particuliers, on peut naturellement extraire un système représentatif d'éléments irréductibles. Dans le cas général, même si l'anneau A est euclidien, *il faut l'axiome du choix* pour assurer l'existence d'un tel système.

Proposition 7.3.4 – *Si $\mathscr{P}$ est un système représentatif d'éléments irréductibles de A, alors pour tout élément non nul a de A, il existe un élément inversible $\varepsilon(a)$ de A tel que $a = \varepsilon(a)\prod_{i=1}^{r} p_i^{v_{p_i}(a)}$ où $p_1, \dots, p_r$ sont les éléments de $\mathscr{P}$ pour lesquels la valuation de a en ces éléments est non nulle. Cette écriture est unique* à permutation près.

DÉMONSTRATION – On considère une décomposition $a = uq_1 \cdots q_s$ de a en un produit d'un élément inversible u par un produit d'éléments irréductibles $q_1, \dots, q_s$. On note $p_1, \dots, p_r$ les éléments de $\mathscr{P}$ pour lesquels au moins l'un des éléments de $\{q_1, \dots, q_s\}$ est associé à l'un des éléments de $\{p_1 \dots p_r\}$. Par définition de la valuation, pour chaque $i \in \{1, \dots, r\}$, il y a $v_{p_i}(a)$ éléments parmi $q_1, \dots, q_s$ qui sont associés à p_i ; pour chaque tel élément q_j, il y a un inversible u_{q_j} de A tel que $p_i = u_{q_j} q_j$, on note u_i le produit des tels éléments u_{q_j}. On a alors $a = u\prod_{i=1}^{r} u_i p_i^{v_{p_i}(a)}$, et en notant $\varepsilon(a) = u\prod_{i=1}^{r} u_i$, on obtient $a = \varepsilon(a)\prod_{i=1}^{r} p_i^{v_{p_i}(a)}$.

L'unicité de l'écriture *à permutation près* suit de la factorialité de A et de la définition d'un système représentatif d'éléments irréductibles. □

Remarque 7.3.5 – Dans ce contexte, au lieu de parler d'un $PGCD$ et d'un $PPCM$ de deux éléments $a = \varepsilon(a)\prod_{i=1}^{r} p_i^{v_{p_i}(a)}$ et $b = \varepsilon(b)\prod_{i=1}^{s} q_i^{v_{p_i}(b)}$, on peut définir le $PGCD$ et le $PPCM$ de a et b (*par rapport au système $\mathscr{P}$*) par $d = \prod_{i=1}^{t} r_i^{\min(v_{r_i}(a), v_{r_i}(b))}$ et $m = \prod_{i=1}^{t} r_i^{\max(v_{r_i}(a), v_{r_i}(b))}$ où $r_1, \dots, r_t$ sont les différents éléments de $\mathscr{P}$ pour lesquels au moins l'une des valuations de a ou b est non nulle.

7.4 Anneaux factoriels et polynômes

Dans cette section, on suppose que A est un anneau factoriel.

7.4.1 Polynômes primitifs et contenus

Définition 7.4.1 – *Un polynôme $P \in A[X]$ est dit* primitif *si 1_A est un $PGCD$ de ses coefficients.*

Remarque 7.4.2 –
- Le polynôme nul n'est pas un polynôme primitif puisque 0_A est un $PGCD$ de ses coefficients.
- Tout polynôme unitaire est primitif.
- Un polynôme P est primitif si et seulement si αP est primitif pour tout $\alpha \in U(A)$.

Proposition 7.4.3 – *Le produit de deux polynômes primitifs est un polynôme primitif.*

DÉMONSTRATION – Soient $P = \sum_{i=0}^{m} a_i X^i$ et $Q = \sum_{i=0}^{n} b_i X^i$ deux polynômes primitifs. Soit p un élément irréductible de A. Comme P et Q sont primitifs, ils ne sont pas nuls et on peut supposer $m = \deg P$ et $n = \deg Q$. Aussi p ne peut pas diviser tous les coefficients $a_0, \dots, a_m$, ni tous les coefficients $b_0, \dots, b_n$. Il existe donc un plus petit entier entier $r \in \{0, \dots, m\}$ et un plus petit entier $s \in \{0, \dots, n\}$ tels que p ne divise pas a_r ni b_s. D'après

le lemme 7.2.4, p ne divise pas leur produit $a_r b_s$. Or le coeffcient du terme de degré $r+s$ de PQ est

$$c_{r+s} = \sum_{\substack{i+j=r+s \\ 0\leqslant i\leqslant m, 0\leqslant j\leqslant n}} a_i b_j = \sum_{\substack{i=0 \\ 0\leqslant r+s-i\leqslant n}}^{r-1} a_i b_{r+s-i} + a_r b_s + \sum_{\substack{i=r+1 \\ 0\leqslant r+s-i\leqslant n}}^{m} a_i b_{r+s-i},$$

et p divise la première somme par minimalité de r, ainsi que la seconde somme par minimalité de s (car on a $r+s-i<s$ lorsque $i>r$). On en déduit que p ne divise pas c_{r+s}. Ceci démontre qu'aucun élément irréductible de A ne divise tous les coefficients de PQ, donc tout $PGCD$ de PQ est inversible et PQ est primitif. □

Lemme 7.4.4 – *Soit $P \in A[X]$. Un élément c de A est un $PGCD$ des coefficients de P équivaut à dire qu'il existe un polynôme primitif P^* tel que $P = cP^*$.*

Démonstration – Soit c un $PGCD$ des coefficients de $P = \sum_{i=0}^n a_i X^i$. Si $c = 0_A$, alors P est nul et on peut prendre $P^* = 1_A$, donc on peut supposer $c \neq 0_A$. Pour tout $i \in \{0,\dots,n\}$, il existe $u_i \in A$ tel que $a_i = cu_i$, donc en posant $P^* = \sum_{i=0}^n u_i X^i$, on obtient $P = cP^*$. Si c^* est un $PGCD$ des coefficients de P^*, alors cc^* est un diviseur commun à $a_0,\dots,a_n$, donc il divise c et il existe $q \in A$ tel que $cc^*q = c$. Comme A est intègre et $c \neq 0_A$, on obtient $c^*q = 1_A$ et c^* est inversible, ce qui montre que P^* est primitif.

Réciproquement, si $P = cP^*$ pour un polynôme primitif $P^* = \sum_{i=0}^n u_i X^i$, alors c est un diviseur commun des coefficients de $P = \sum_{i=0}^n cu_i X^i$. Si $c = 0_A$, alors P est le polynôme nul et c est bien un $PGCD$ des coefficients de P, donc on peut supposer $c \neq 0_A$. Soit d un $PGCD$ des coefficients de P. Alors c divise d et il existe $q \in A$ tel que $d = cq$. Soit $P^{**} = \sum_{i=0}^n v_i X^i$ un polynôme primitif tel que $P = dP^{**}$. Alors on a $cu_i = cqv_i$ pour tout $i \in \{0,\dots,n\}$, et comme $c \neq 0_A$, on obtient $u_i = qv_i$ pour tout $i \in \{0,\dots,n\}$ et q est un diviseur commun à $u_0,\dots,u_n$. Comme P^* est primitif, on en déduit que q est inversible, donc $c = dq^{-1}$ est aussi un $PGCD$ des coefficients de P. □

Dans la suite, on note K_A le corps des fractions de A.

Lemme 7.4.5 – *Pour tout polynôme $P \in K_A[X]$, il existe $c \in K_A$ et un polynôme primitif P^* de $A[X]$ tel que $P = cP^*$. De plus, si $P = c'P^{**}$ pour $c' \in K_A$ et un polynôme primitif P^{**} de $A[X]$, alors il existe $u \in U(A)$ tel que $c' = cu$.*

Démonstration – Soit $P = \sum_{i=0}^n a_i X^i$ un polynôme sur K_A. Alors il existe dans A des éléments $u_0,\dots,u_n,v_0,\dots,v_n$, avec $v_0,\dots,v_n$ non nuls, tels que $a_i = \frac{u_i}{v_i}$ pour tout $i \in \{0,\dots,n\}$. En notant $v = v_0\cdots v_n \in A^*$, on obtient $vP = \sum_{i=0}^n b_i X^i \in A[X]$. D'après le lemme 7.4.4, si d un $PGCD$ des coefficients de vP, il existe un polynôme primitif P^* tel que $vP = dP^*$. On obtient $P = cP^*$ pour $c = \frac{d}{v} \in K_A$ et, d'après la remarque 7.4.2, tout autre élément de la forme cu pour $u \in U(A)$ convient.

Supposons $P = c'P^{**}$ pour $c' \in K_A$ et un polynôme primitif P^{**} de $A[X]$. Alors on a $vP = vc'P^{**}$, et vc' est un $PGCD$ des coefficients de vP (lemme 7.4.4). On en déduit que vc' et d sont associés, et il existe $u \in U(A)$ tel que $vc' = du$ d'où $c' = \frac{d}{v}u = cu$. □

Définition 7.4.6 – *Pour tout polynôme $P \in K_A[X]$, on appelle* contenu *de P tout élément $C(P)$ de K_A tel que $P = C(P)P^*$ pour un polynôme primitif P^* de $A[X]$.*

Remarque 7.4.7 –
- Les polynômes primitifs sont ceux pour lesquels 1_A est un contenu.
- Si $C(P)$ est un contenu de $P \in K_A[X]$, alors d'après le lemme 7.4.5, l'ensemble des contenus de P sont les éléments de la forme $C(P)u$ pour $u \in U(A)$. *Ainsi, un contenu de P appartient à A si et seulement si tous ses contenus appartiennent à A.*
- D'après les lemmes 7.4.4, les polynômes $P \in K_A[X]$ appartenant à $A[X]$ sont ceux dont les contenus appartiennent à A, on en déduit que
  pour tout** $P \in A[X]$**, les** $PGCD$ **des coefficients de** P **sont les contenus de** P**.

7.4.2 Le lemme des Gauss et ses conséquences

Lemme 7.4.8 – **(Lemme de Gauss)** *Soient P et Q deux polynômes sur K_A et $C(P)$ et $C(Q)$ des contenus de P et Q. Alors $C(P)C(Q)$ est un contenu de PQ.*

Démonstration – Par définition d'un contenu, il y a des polynômes primitifs P^* et Q^* tels que $P = C(P)P^*$ et $Q = C(Q)Q^*$. On a alors $PQ = C(P)C(Q)P^*Q^*$. Or P^*Q^* est un polynôme primitif d'après la proposition 7.4.3, donc $C(P)C(Q)$ est un contenu de PQ. □

Corollaire 7.4.9 – *Si P, U et V sont trois polynômes sur A avec P primitif et $P = UV$, alors U et V sont primitifs.*

Démonstration – Soient $C(U)$ et $C(V)$ des contenus de U et V. D'après le lemme de Gauss, leur produit est inversible donc $C(U)$ et $C(V)$ sont inversibles et U et V sont primitifs. □

Corollaire 7.4.10 – *Si un polynôme primitif $P \in A[X]$ divise $Q \in A[X]$ dans $K_A[X]$, alors P divise Q dans $A[X]$.*

Démonstration – Dire que P divise Q dans $K_A[X]$ signifie qu'il existe $U \in K_A[X]$ tel que $Q = UP$. Soit $C(U)$ un contenu de U. Comme P est primitif, alors $C(U)$ est un contenu de Q d'après le lemme de Gauss. Or les contenus de Q sont des éléments de A d'après la remarque 7.4.7, donc $C(U)$ appartient à A et $U \in A[X]$ d'après la même remarque. On en déduit que P divise Q dans $A[X]$. □

Exemples 7.4.11 – Si le produit UV de deux polynômes unitaires U et V sur $K_A = \mathbb{Q}$ appartient à $\mathbb{Z}[X]$, alors U et V sont à coefficients dans $A = \mathbb{Z}$.

[*En effet, si on note $C(U)$ et $C(V)$ des contenus de U et V, U^* et V^* des polynômes primitifs tels que $U = C(U)U^*$ et $V = C(V)V^*$ et a et b les coefficients des termes de plus haut degré de U^* et V^*, alors comme U et V sont unitaires, on a $C(U) = a^{-1}$ et $C(V) = b^{-1}$. Le fait que U et V soient unitaires implique aussi que $UV \in \mathbb{Z}[X]$ est unitaire, donc UV est un polynôme primitif. Le lemme de Gauss donne alors $a^{-1}b^{-1} = \pm 1$, d'où $a = \pm 1$ et $b = \pm 1$. On en déduit que $U = C(U)U^*$ et $V = C(V)V^*$ appartiennent à $\mathbb{Z}[X]$.*]

7.4.3 Le théorème principal

Pour démontrer le théorème 7.4.15, qui sera le dernier résultat du cours, nous étudions d'abord les polynômes irréductibles de $A[X]$.

Lemme 7.4.12 – *Si un polynôme primitif $P \in A[X]$ est premier dans $K_A[X]$, alors il est premier dans $A[X]$.*

Démonstration – Si P est premier dans $K_A[X]$, alors P n'est ni nul, ni constant. En particulier, il n'est pas inversible dans $A[X]$. Supposons que P divise dans $A[X]$ un produit UV de polynômes sur A. Alors P divise UV dans $K_A[X]$ et, comme P est premier dans $K_A[X]$, il divise U ou V dans $K_A[X]$.

Comme P est primitif, le corollaire 7.4.10 dit qu'il divise U ou V dans $A[X]$. On en déduit que P est premier dans $A[X]$. □

Proposition 7.4.13 – *Les éléments irréductibles de $A[X]$ sont*
- *les polynômes constants $P = a$ pour $a \in A$ irréductible ;*
- *les polynômes primitifs non constants de $A[X]$ qui sont irréductibles dans $K_A[X]$.*

Démonstration – Soit $P = a$ un polynôme constant pour $a \in A$. Il faut montrer que P est irréductible dans $A[X]$ si et seulement si a est irréductible dans A. On peut supposer $a \in A$ non nul et non inversible. On suppose d'abord a irréductible dans A et $P = UV$ pour U et V dans $A[X]$. Alors U et V sont des polynômes constants, et on a $U = u$ et $V = v$ pour u et v dans A, d'où $a = uv$. Or a est irréductible, donc u ou v est inversible dans A, et soit $U = u$ soit $V = v$ est inversible dans $A[X]$, ce qui montre que P est irréductible dans $A[X]$.

Réciproquement, si P est irréductible dans $A[X]$ et $a = uv$ pour u et v dans A, alors on a $P = UV$ où U et V désigne les polynômes constants $U = u$ et $V = v$. Comme P est irréductible, alors U ou V est inversible dans $A[X]$, et donc u ou v est inversible dans A, ce qui montre que a est irréductible dans $A[X]$.

Soient $P \in A[X]$ un polynôme non constant, $C(P)$ un contenu de P et P^* un polynôme primitif tel que $P = C(P)P^*$. Il faut montrer que P est irréductible dans $A[X]$ si et seulement si P est primitif dans $A[X]$ et irréductible dans $K_A[X]$. Si $C(P)$ n'est pas inversible, alors $P = C(P)P^*$ n'est ni irréductible dans $A[X]$, ni primitif, donc on peut supposer que $C(P)$ est inversible, autrement dit que P est primitif.

Si $P \in A[X]$ est irréductible dans $K_A[X]$ et si $P = UV$ pour deux polynômes U et V de $A[X]$, alors soit U soit V est un polynôme constant. Comme P est primitif, ce polynôme constant est inversible dans $A[X]$, donc P est aussi irréductible dans $A[X]$. On peut donc supposer P irréductible dans $A[X]$, et on doit montrer que P est irréductible dans $K_A[X]$.

Supposons que $P \in A[X]$ s'écrive sous la forme $P = UV$ pour deux polynômes U et V de $K_A[X]$. Soient $C(U)$ et $C(V)$ des contenus de U et V, et U^* et V^* des polynômes primitifs tels que $U = C(U)U^*$ et $V = C(V)V^*$. D'après la proposition 7.4.3, le polynômes U^*V^* est primitif, or on a $P = (C(U)C(V))(U^*V^*)$, donc $C(U)C(V)$ est un contenu de P et la remarque 7.4.7 dit que $C(U)C(V)$ appartient à A. Comme P est irréductible dans

$A[X]$, on en déduit que U^* ou V^* est un polynôme constant, donc U ou V est constant et non nul, c'est-à-dire inversible dans $K_A[X]$. Ainsi P est irréductible dans $K_A[X]$. □

Lemme 7.4.14 – *Les éléments irréductibles de $A[X]$ sont premiers.*

Démonstration – Soit P un éléments irréductibles de $A[X]$. Si P est constant, alors d'après la proposition 7.4.13, il existe $a \in A$ irréductible tel que $P = a$. En particulier, d'une part a est premier dans A puisque A est factoriel, d'autre part a est un contenu de P. Si P divise un produit UV de polynômes sur A, on note $C(U)$ et $C(V)$ des contenus de U et V, et U^* et V^* des polynômes primitifs tels que $U = C(U)U^*$ et $V = C(V)V^*$. Alors a divise $C(U)C(V)$ dans A d'après le lemme de Gauss, donc a divise $C(U)$ ou $C(V)$ puisque a est premier dans A. On en déduit que P divise U ou V, donc P est premier dans $A[X]$.

Si P n'est pas constant, alors d'après la proposition 7.4.13, le polynôme P est primitif et il est irréductible dans $K_A[X]$. Or $K_A[X]$ est un anneau euclidien, donc il est principal (théorème 2.7 du chapitre précédent) et ses éléments irréductibles sont premiers (exemple 6.3.3 et proposition 6.3.9). On déduit du lemme 7.4.12 que P est premier dans $A[X]$. □

Théorème 7.4.15 – *Si A est factoriel, l'anneau $A[X_1, \ldots, X_n]$ est aussi factoriel.*

Démonstration – D'après la proposition 3.11 du chapitre précédent, il suffit de montrer que $A[X]$ est factoriel. Aussi, le corollaire 3.13 du chapitre précédent dit que $A[X]$ est un anneau intègre. Comme on a vu que les éléments irréductibles de $A[X]$ sont tous premiers (lemme 7.4.14), d'après la proposition 7.1.2, il suffit de montrer que les éléments de $A[X]$ se décomposent tous en un produit d'un élément inversible par un produit d'éléments irréductibles.

On montre par récurrence sur le $n = \deg P$ la proposition $\mathscr{P}(n)$: "tout $P \in A[X]$ non nul de degré au plus n se décompose en un produit d'un élément inversible par un produit de facteurs irréductibles".

Initialisation : Si $n = 0$, alors P est constant et on a $P = a$ pour $a \in A$. Comme A est factoriel, on peut écrire $a = up_1 \cdots p_r$ pour $u \in U(A)$ et des éléments irréductibles $p_1, \ldots, p_r$ de A. Les polynômes constants $P_1 = up_1$, $P_2 = p_2$,..., $P_r = p_r$ sont irréductibles d'après la proposition 7.4.13, donc comme on a $P = P_1 \cdots P_r$, la proposition est vraie pour $n = 0$.

Hérédité : Supposons $\mathscr{P}(n)$ vraie pour $n \in \mathbb{N}$. Soient $P \in A[X]$ de degré $n+1$, $C(P)$ un contenu de P et P^* un polynôme primitif tel que $P = C(P)P^*$. Comme le polynôme constant $Q = C(P)$ se décompose en un produit de facteurs irréductibles d'après $\mathscr{P}(0)$, il suffit de montrer que P^* se décompose en un produit de facteurs irréductibles.

On peut supposer P^* non irréductible. Supposons $P^* = UV$ pour des polynômes non inversibles U et V dans $A[X]$. D'après le corollaire 7.4.9, comme P^* est primitif, U et V sont primitifs. En particulier, si l'un des deux est constant, il est inversible, ce qui contredit notre choix de U et V. Alors U et V sont non constants, et comme $\deg P^* = \deg U + \deg V$ puisque A est intègre, on a $\deg U \leqslant n$ et $\deg V \leqslant n$. Comme $\mathscr{P}(n)$ est vraie, on en déduit que $\mathscr{P}(n+1)$ est vraie.

Conclusion : on a montré que $\mathscr{P}(n)$ est vraie pour tout $n \in \mathbb{N}$, donc tout $P \in A[X]$ non nul se décompose en un produit de facteurs irréductibles, et $A[X]$ est un anneau factoriel. □

Nous finissons en remarquant que la réciproque du théorème précédent est vraie.

Proposition 7.4.16 – *Soit B un anneau commutatif quelconque. Si $B[X_1, \ldots, X_n]$ est un anneau factoriel, alors B est aussi factoriel.*

Démonstration – D'après le corollaire 3.13 du chapitre précédent, l'anneau B est intègre. Aussi, la proposition 3.11 du chapitre précédent permet de supposer que $B[X]$ est factoriel.

Si p est un élément irréductible de B, alors le polynômes constant $P = p$ est irréductible dans $B[X]$ d'après la proposition 7.4.13. Or si p divise un produit uv d'éléments u et v de B, alors $P = p$ divise dans $B[X]$ le produit UV des polynômes contants $U = u$ et $V = v$. Comme $P = p$ est irréductible dans $B[X]$, il divise $U = u$ ou $V = v$, et donc p dans u ou v dans A. Ceci montre que p est premier dans B.

Soit b un élément non nul de B. Alors le polynôme constant $P = b$ se décompose en un produit d'un polynôme inversible U par un produit de polynômes irréductibles $P_1, \ldots, P_r$. Or P est constant et non nul, donc $U, P_1, \ldots, P_r$ aussi, et il existe un élément inversible u de B et des éléments non nuls $p_1, \ldots, p_r$ de B tels que $U = u$, $P_1 = p_1$,...,$P_r = p_r$. Comme la proposition 7.4.13 dit que $p_1, \ldots, p_r$ sont irréductibles, l'élément b se décompose en un produit d'un élément inversible par un produit d'élément irréductibles, et la proposition 7.1.2 permet de conclure. □

Conclusion :

pour tout anneau, on a les implications suivantes :
corps commutatif $\Longrightarrow$ *euclidien* $\Longrightarrow$ *principal* $\Longrightarrow$ *factoriel*
$\Longrightarrow$ *à PGCD* $\Longrightarrow$ *intégralement clos* $\Longrightarrow$ *intègre* $\Longrightarrow$ *commutatif*

En revanche, aucune réciproque n'est vraie :
- $\mathbb{Z}$ est un anneau euclidien mais n'est pas un corps ;
- $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est un anneau principal qui n'est pas euclidien ;
- $\mathbb{Z}[X]$ est un anneau factoriel qui n'est pas principal ;
- $\mathbb{Z} + X\mathbb{Q}[X]$ est un anneau à $PGCD$ qui n'est pas factoriel ;
- Si ζ_{23} désigne une racine 23^e de l'unité, alors $\mathbb{Z}[\zeta_{23}]$ est un anneau intégralement clos sans être un anneau à $PGCD$.
- $\mathbb{Z}[\sqrt{5}]$ est un anneau intègre qui n'est pas intégralement clos ($\frac{1+\sqrt{5}}{2}$ *appartient au corps des fractions de* $\mathbb{Z}[\sqrt{5}]$ *et est racine de* $X^2 - X - 1$, *mais* $\frac{1+\sqrt{5}}{2}$ *n'appartient pas à* $\mathbb{Z}[\sqrt{5}]$) ;
- $\mathbb{Z}/4\mathbb{Z}$ est un anneau commutatif qui n'est pas intègre.

Cependant, on a vu que la démonstration de l'implication "*principal* $\Longrightarrow$ *factoriel*" utilise l'axiome du choix dépendant et n'est pas démontrable dans le système ZF ; en revanche les autres implications n'utilisent pas cet axiome, dont les implications "*principal* $\Longrightarrow$ *à PGCD*" (exemple 6.3.3) et "*euclidien* $\Longrightarrow$ *factoriel*" (corollaire 7.1.3).

Chapitre 8

L'anneau des fonctions arithmétiques

8.1 Les fonctions arithmétiques

Définition 8.1.1 –
- *Une* fonction arithmétique *est une application* $f : \mathbb{N}^* \to \mathbb{C}$.
  Dans la suite, nous noterons $\mathscr{A}$ l'ensemble des fonctions arithmétiques.
- *Une fonction arithmétique non nulle* f *est dite* multiplicative *si, pour tous entiers naturels non nuls* m *et* n *premiers entre eux, on a* $f(mn) = f(m)f(n)$.
- *Une fonction arithmétique non nulle* f *est dite* complètement multiplicative *si, pour tous entiers naturels non nuls* m *et* n, *on a* $f(mn) = f(m)f(n)$.

Remarque 8.1.2 –
- Les fonctions complètement multiplicatives sont multiplicatives.
- Toute fonction multiplicative f satisfait $f(1) = 1$.
- Pour tout sous-anneau A de $\mathbb{C}$, on notera $\mathscr{A}_A$ l'ensemble des fonctions arithmétiques f satisfaisant $f(n) \in A$ pour tout $n \in \mathbb{N}^*$. *On s'intéressera particulièrement au cas* $A = \mathbb{Z}$.
- *Les sections 1 et 3 restent valables si on remplace* $\mathbb{C}$ *par un autre corps commutatif.*

Exemples 8.1.3 –
- Toute fonction constante est une fonction arithmétique.
- Pour tout $s \in \mathbb{R}$ (ou même $s \in \mathbb{C}$), la fonction $e_s : \mathbb{N}^* \to \mathbb{C}$ définie par $e_s(n) = \frac{1}{n^s}$ est une fonction complètement multiplicative. *La fonction* e_0 *est la fonction constante* $\mathbb{1}$ *égale à 1.*
- L'*indicatrice d'Euler* φ est une fonction arithmétique multiplicative (proposition 8.2.4).

8.1.1 La structure d'anneau de $\mathscr{A}$

Définition 8.1.4 –

— *La* convolution de Dirichlet $f * g : \mathbb{N}^* \to \mathbb{C}$ *de deux fonctions arithmétiques* f *et* g *est définie par* $(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$.
— *On note* δ_1 *la fonction définie par* $\delta_1(1) = 1$ *et* $\delta_1(n) = 0$ *pour tout* $n \neq 1$.
— *Pour toute fonction* $f \in \mathscr{A}$ *non nulle, on note* $N(f)$ *le plus petit* $n \in \mathbb{N}^*$ *tel que* $f(n) \neq 0$.

Lemme 8.1.5 – *Pour toutes fonctions arithmétiques non nulles* f *et* g*, la fonction* $f * g$ *est non nulle et satisfait* $N(f * g) = N(f)N(g)$.

Démonstration – Soient $m = N(f)$ et $n = N(g)$. Pour tout $a \in \mathbb{N}^*$ satisfaisant $a < mn$ et tout entier d, on a soit $d < m$, soit $d \geqslant m$ et $\frac{a}{d} < n$, donc $(f * g)(a) = \sum_{d|a} f(d)g(\frac{a}{d}) = 0$ et soit $N(f * g) \geqslant mn$ soit $f * g = 0$.

Pour tout diviseur $d \in \mathbb{N}^*$ de mn satisfaisant $d > m$, on a $\frac{mn}{d} < n$, donc $g(\frac{mn}{d}) = 0$. Comme, pour tout diviseur $d \in \mathbb{N}^*$ de mn tel que $d < m$, on a $f(d) = 0$, on obtient $(f * g)(mn) = \sum_{d|mn} f(d)g(\frac{mn}{d}) = f(m)g(n) \neq 0$. Ceci montre que $f * g$ est non nul et que $N(f * g) = mn$. □

Théorème 8.1.6 – *Le triplet* $(\mathscr{A}_A, +, *)$ *est un anneau intègre ayant pour éléments neutres la fonction nulle et* δ_1*. Une fonction* f *est inversible dans* $\mathscr{A}_A$ *si et seulement si* $f(1)$ *est inversible dans* A.

Démonstration – Comme A est un sous-anneau de $\mathbb{C}$, il est stable pour l'addition et par symétrie. La somme est donc une loi de composition interne sur $\mathscr{A}_A$ qui est associative, commutative, ayant pour élément neutre la fonction nulle, et l'opposé de tout $f \in \mathscr{A}_A$ appartient à $\mathscr{A}_A$. Ainsi $(\mathscr{A}_A, +)$ est un groupe abélien.

Il suit de la définition de la loi $*$ qu'il s'agit d'une loi de composition interne sur $\mathscr{A}_A$. Montrons qu'elle est associative. Pour toutes fonctions f, g et h dans $\mathscr{A}_A$ et tout $n \in \mathbb{N}^*$, on a $((f * g) * h)(n) = \sum_{d|n}(f * g)(d)h(\frac{n}{d}) = \sum_{d|n}(\sum_{d'|d} f(d')g(\frac{d}{d'}))h(\frac{n}{d})$. En posant $a = d'$, $b = \frac{d}{d'}$ et $c = \frac{n}{d}$, on obtient $((f * g) * h)(n) = \sum_{abc=n} f(a)g(b)h(c)$. De même on montre que $(f * (g * h))(n) = \sum_{abc=n} f(a)g(b)h(c)$, donc on a bien $(f * g) * h = f * (g * h)$ et la loi $*$ est associative.

La loi $*$ est commutative sur $\mathscr{A}_A$. En effet, dire que $d \in \mathbb{N}^*$ est un diviseur de $n \in \mathbb{N}^*$ équivaut à dire que $\frac{n}{d}$ appartient à $\mathbb{N}^*$, ou encore que $d' = \frac{n}{d}$ est un diviseur de n, donc on obtient $(f * g)(n) = \sum_{d'|n} f(\frac{n}{d'})g(d') = (g * f)(n)$.

Pour tout $f \in \mathscr{A}_A$ et tout $n \in \mathbb{N}^*$, on a $(f * \delta_1)(n) = \sum_{d|n} f(d)\delta_1(\frac{n}{d}) = f(n)$, donc on a $f * \delta_1 = f$ et, par commutativité de $*$, on a aussi $\delta_1 * f = f$. Ainsi δ_1 est l'élément neutre de $\mathscr{A}_A$ pour la loi $*$.

La loi $*$ est distributive par rapport à $+$ car, pour tous f, g et h dans $\mathscr{A}_A$ et tout $n \in \mathbb{N}^*$, on a $(f * (g + h))(n) = \sum_{d|n} f(d)(g + h)(\frac{n}{d}) = \sum_{d|n} f(d)g(\frac{n}{d}) + \sum_{d|n} f(d)h(\frac{n}{d}) = (f * g)(n) + (f * h)(n)$ d'où $f * (g + h) = f * g + f * h$. Par commutativité de $*$, on a aussi $(f + g) * h = f * h + g * h$, ce qui démontre la distributivité de $*$.

On a montré que $(\mathscr{A}_A, +, *)$ est un anneau commutatif, et il est intègre d'après le lemme 8.1.5.

Il nous reste à caractériser les éléments inversibles de $\mathscr{A}_A$. Soit $f \in \mathscr{A}_A$ tel que $f(1)$ est non inversible. Alors pour tout $g \in \mathscr{A}_A$, on a $(f*g)(1) = f(1)g(1)$ non inversible, donc $f*g$ est distinct de δ_1 et f n'est pas inversible.

Réciproquement, soit $f \in \mathscr{A}_A$ tel que $f(1)$ est inversible. On peut définir par récurrence (forte) une fonction $g \in \mathscr{A}_A$ en posant $g(1) = f(1)^{-1}$ et $g(n) = -f(1)^{-1} \sum_{d|n, d\neq 1} f(d)g(\frac{n}{d})$ pour tout $n > 1$. On a alors $(f*g)(1) = f(1)g(1) = 1$ et $(f*g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}) = f(1)g(n) + \sum_{d|n, d\neq 1} f(d)g(\frac{n}{d}) = f(1)g(n) - f(1)g(n) = 0$ pour tout $n > 1$. On en déduit que $f*g = \delta_1$, donc f est inversible. □

8.1.2 Le groupe des unités de $\mathscr{A}$

Remarque 8.1.7 – Pour tout sous-anneau A de $\mathbb{C}$ et tout $f \in \mathscr{A}_A$ vérifiant $f(1) = 1$, il y a une unique fonction multiplicative $\overline{f} \in \mathscr{A}_A$ telle que $\overline{f}(p^k) = f(p^k)$ pour tout nombre premier p et tout $k \in \mathbb{N}^*$.

[*Si une fonction multiplicative $\overline{f} \in \mathscr{A}_A$ vérifie $\overline{f}(p^k) = f(p^k)$ pour tout nombre premier p et tout $k \in \mathbb{N}^*$, alors elle satisfait $\overline{f}(1) = 1$ et $\overline{f}(p_1^{k_1} \cdots p_r^{k_r}) = f(p_1^{k_1}) \cdots f(p_r^{k_r})$ pour tout $r \in \mathbb{N}^*$, tous nombres premiers $p_1, \ldots, p_r$ distincts et tous entiers $k_1, \ldots, k_r$ dans $\mathbb{N}^*$, or une telle fonction est unique.*]

Proposition 8.1.8 – *Pour tout sous-anneau A de $\mathbb{C}$, l'ensemble des fonctions multiplicatives de $\mathscr{A}_A$ est un sous-groupe du groupe $U(\mathscr{A}_A)$ des éléments inversibles de $\mathscr{A}_A$.*

Démonstration – Comme δ_1 est une fonction multiplicative, et que toute fonction multiplicative f est inversible car $f(1) = 1$, les fonctions multiplicatives forment une partie non vide de $U(\mathscr{A}_A)$.

Montrons que, si f et g sont deux fonctions multiplicatives, la fonction $f*g$ est aussi multiplicative. Comme f et g sont multiplicatives, on a $(f*g)(1) = f(1)g(1) = 1$. Soient m et n des entiers naturels non nuls premiers entre eux. Alors tout diviseur $d \in \mathbb{N}^*$ de mn se décompose d'une unique façon en un produit $d = a(d)b(d)$ d'un diviseur $a(d) \in \mathbb{N}^*$ de m et d'un diviseur $b(d) \in \mathbb{N}^*$ de n, et les entiers $a(d)$ et $b(d)$ sont premiers entre eux puisque m et n sont premiers entre eux. Réciproquement, tout produit d'un diviseur de m et d'un diviseur de n est un diviseur de mn. On en déduit que

$$\begin{aligned}
(f*g)(mn) &= \textstyle\sum_{d|mn} f(d)g(\frac{mn}{d}) \\
&= \textstyle\sum_{d|mn} f(a(d)b(d))g(\frac{mn}{a(d)b(d)}) \\
&= \textstyle\sum_{d|mn} f(a(d))f(b(d))g(\frac{m}{a(d)})g(\frac{n}{b(d)}) \\
&= \textstyle\sum_{a|m, b|n} f(a)g(\frac{m}{a})f(b)g(\frac{n}{b}) \\
&= \textstyle\sum_{a|m} f(a)g(\frac{m}{a}) \sum_{b|n} f(b)g(\frac{n}{b}),
\end{aligned}$$

donc on a $(f*g)(mn) = (f*g)(m)(f*g)(n)$ et la fonction $f*g$ est multiplicative.

Soient f une fonction multiplicative et g son inverse. Alors on a $g(1) = f(1)g(1) = (f*g)(1) = \delta_1(1) = 1$ et, d'après la remarque 8.1.7, il existe une unique fonction multiplicative $\overline{g}$ satisfaisant $\overline{g}(p^k) = g(p^k)$ pour tout nombre premier p et tout $k \in \mathbb{N}^*$. Alors on a $(f*\overline{g})(1) = f(1)\overline{g}(1) = 1 = \delta_1(1)$ et, pour tout nombre premier p et tout $k \in \mathbb{N}^*$, on a

$(f * \overline{g})(p^k) = \sum_{d|p^k} f(d)\overline{g}(\frac{p^k}{d})$. Or les quotients de p^k sont des puissances de p, donc on $\overline{g}(\frac{p^k}{d}) = g(\frac{p^k}{d})$ pour tout diviseur d de p^k, d'où $(f*\overline{g})(p^k) = \sum_{d|p^k} f(d)g(\frac{p^k}{d}) = (f*g)(p^k) = \delta_1(p^k)$. On déduit de la remarque 8.1.7 que $f * \overline{g} = \delta_1 = f * g$, ce qui implique $g = \overline{g}$, donc g est multiplicative. □

Remarque 8.1.9 – En revanche, la convolution de deux fonctions complètement multiplicatives n'est généralement pas complètement multiplicative.

[*Par exemple, la fonction* $\mathbb{1} * \mathbb{1}$ *associe à tout* $n \in \mathbb{N}^*$ *le nombre de diviseurs de* n *car* $(\mathbb{1} * \mathbb{1})(n) = \sum_{d|n} \mathbb{1}(d)\mathbb{1}(\frac{n}{d}) = \sum_{d|n} 1$. *On a donc* $(\mathbb{1} * \mathbb{1})(2) = 2$ *et* $(\mathbb{1} * \mathbb{1})(4) = 3 \neq ((\mathbb{1} * \mathbb{1})(2))^2$.]

8.2 La fonction de Möbius

8.2.1 Définition et indicatrice d'Euler

Définition 8.2.1 – *La* fonction de Möbius*, notée* μ*, est l'inverse de la fonction constante* $\mathbb{1}$.

Lemme 8.2.2 – *La fonction de Möbius vérifie* $\mu(1) = 1$, $\mu(n) = 0$ *pour tout* $n \geqslant 2$ *divisible par le carré d'un nombre premier et* $\mu(p_1 \cdots p_r) = (-1)^r$ *lorsque* $p_1, \ldots, p_r$ *sont des nombres premiers distincts.*

Démonstration – Soit f l'unique fonction multiplicative satisfaisant $f(p) = -1$ et $f(p^k) = 0$ pour tout nombre premier p et tout entier $k \geqslant 2$. Pour tout nombre premier p, on a $(f * \mathbb{1})(p) = \sum_{d|p} f(d) = f(1) + f(p) = 0 = \delta_1(p)$, et pour tout entier $k \geqslant 2$, on a $(f * \mathbb{1})(p^k) = \sum_{d|p^k} f(d) = f(1) + f(p) + \cdots + f(p^k) = 0 = \delta_1(p^k)$. Comme $f * \mathbb{1}$ et δ_1 sont deux fonctions multiplicatives, on obtient $f * \mathbb{1} = \delta_1$ (remarque 8.1.7) et $f = \mu$. Le résultat suit de cette égalité. □

Proposition 8.2.3 – **(Formule d'inversion de Möbius)** *Soient* $f \in \mathscr{A}$ *et* $g \in \mathscr{A}$ *la fonction arithmétique définie par* $g(n) = \sum_{d|n} f(d)$*, alors on a* $f(n) = \sum_{d|n} \mu(d)g(\frac{n}{d})$ *pour tout* $n \in \mathbb{N}^*$.

Démonstration – Comme g est définie par $g(n) = \sum_{d|n} f(d)$, on a $g = \mathbb{1} * f$, et comme μ est l'inverse de $\mathbb{1}$, on a $f = \mu * g$. □

Considérons l'*indicatrice d'Euler*, c'est-à-dire la fonction $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ qui, à tout $n \in \mathbb{N}^*$, associe le nombre d'entiers $k \in \{1, \ldots, n\}$ premiers avec n. Alors la fonction de Möbius permet de retrouver rapidement ses principales propriétés.

Proposition 8.2.4 – *Pour tout* $n \in \mathbb{N}^*$*, on a* $\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$*, autrement dit on a* $\varphi = \mu * \mathrm{id}_{\mathbb{N}^*}$. *En particulier, la fonction* φ *est multiplicative.*

DÉMONSTRATION – Pour tout $n \in \mathbb{N}^*$, on a $\sum_{d|n} \mu(d) = \sum_{d|n} \mu(d)\mathbb{1}(\frac{n}{d}) = (\mu * \mathbb{1})(n) = \delta_1(n)$ donc $\varphi(n) = \sum_{\substack{1\leqslant k\leqslant n \\ k\wedge n=1}} 1 = \sum_{1\leqslant k\leqslant n} \delta_1(k\wedge n) = \sum_{1\leqslant k\leqslant n} \sum_{d|k\wedge n} \mu(d) = \sum_{1\leqslant k\leqslant n} \sum_{\substack{d|k \\ d|n}} \mu(d) = \sum_{d|n} \sum_{\substack{1\leqslant k\leqslant n \\ d|k}} \mu(d) = \sum_{d|n} \mu(d)\frac{n}{d}$. Ainsi $\varphi = \mu * \mathrm{id}_{\mathbb{N}^*}$ est la convolution de deux fonctions multiplicatives, c'est donc une fonction multiplicative d'après la proposition 8.1.8. □

Corollaire 8.2.5 – *Pour tout $n \in \mathbb{N}^*$, on a $n = \sum_{d|n} \varphi(d)$.*

DÉMONSTRATION – D'après la proposition 8.2.4, on a $\varphi = \mu * \mathrm{id}_{\mathbb{N}^*} = \mathrm{id}_{\mathbb{N}^*} * \mu$, donc en multipliant à droite par $\mathbb{1}$, on obtient $\mathrm{id}_{\mathbb{N}^*} = \varphi * \mathbb{1}$ et $n = \sum_{d|n} \varphi(d)$ pour tout $n \in \mathbb{N}^*$. □

Corollaire 8.2.6 – *Soient $p_1, \ldots, p_r$ des nombres premiers distincts et $\alpha_1, \ldots, \alpha_r$ des entiers naturels non nuls. Alors on a $\varphi(n) = n\prod_{i=1}^r (1 - \frac{1}{p_i})$ où $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.*

DÉMONSTRATION – Le résultat suit de la multiplicativité de φ (proposition 8.2.4) et du lemme 8.2.2 qui donne, pour tout nombre premier p et tout $\alpha \in \mathbb{N}^*$, les égalités suivantes : $\varphi(p^\alpha) = (\mu * \mathrm{id}_{\mathbb{N}^*})(p^\alpha) = \sum_{d|p^\alpha} \mu(p^\alpha)\frac{p^\alpha}{d} = \mu(1)p^\alpha + \mu(p)\frac{p^\alpha}{p} = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$. □

Exercice 8.2.7 – a) *Montrer que tout entier $n \geqslant 2$ vérifie $\sum_{\substack{1\leqslant k\leqslant n \\ k\wedge n=1}} k = \frac{n}{2}\varphi(n)$.*
b) *Montrer qu'on a $\sum_{k=1}^n \mu(k)\lfloor \frac{n}{k} \rfloor = 1$ pour tout $n \in \mathbb{N}^*$, où $\lfloor \frac{n}{k} \rfloor$ désigne la partie entière de $\frac{n}{k}$.*
c) *Montrer que $\sum_{d|n} \frac{\mu(d)^2}{\varphi(d)} = \frac{n}{\varphi(n)}$ pour tout $n \in \mathbb{N}^*$ (indication : on peut utiliser la remarque 8.1.7).*

8.2.2 Application aux polynômes cyclotomiques

Remarque 8.2.8 – Soit $(G, +)$ est un groupe abélien. On rappelle que, pour tout $x \in G$, on note $0x = e_G$ l'élément neutre de G, $(n+1)x = nx + x$ pour tout $n \in \mathbb{N}$ et $(-n)x = -(nx)$.

Pour toute application $f : \mathbb{N}^* \to G$ et tout $u \in \mathscr{A}_{\mathbb{Z}}$, on définit $u * f : \mathbb{N}^* \to G$ par $(u * f)(n) = \sum_{d|n} u(d)f(\frac{n}{d})$. Alors, de même que dans la démonstration du théorème 8.1.6, pour tout $n \in \mathbb{N}^*$ et tous u et v dans $\mathscr{A}_{\mathbb{Z}}$, on a $((u * v) * f)(n) = \sum_{abc=n} (u(a)v(b)f(c) = (u * (v * f))(n)$.

Ainsi, si $g : \mathbb{N}^* \to G$ désigne la fonction définie par $g(n) = \sum_{d|n} f(d)$, autrement dit par $g = \mathbb{1} * f$ où $\mathbb{1}$ est la fonction constante égal à 1, alors on a $f = \mu * g$ où μ est la fonction de Möbius.

Si la loi du groupe G est notée multiplicativement, cela donne pour tout $n \in \mathbb{N}^*$:

$$g(n) = \prod_{d|n} f(d) \iff f(n) = \prod_{d|n} g(\frac{n}{d})^{\mu(d)} \qquad (1).$$

Définition 8.2.9 – *Pour tout* $n \in \mathbb{N}^*$, *le* n^{e} polynôme cyclotomique *est* $\Phi_n(X) = \prod_{\substack{k=1 \\ k\wedge n=1}}^{n} (X - e^{\frac{2ik\pi}{n}})$.

Remarque 8.2.10 – Pour tout $n \in \mathbb{N}^*$, le polynôme $\Phi_n(X)$ est unitaire de degré $\varphi(n)$.

Proposition 8.2.11 – *Pour tout* $n \in \mathbb{N}^*$, *on a* $\prod_{d|n} \Phi_d(X) = X^n - 1$.

Démonstration – Si $d \in \mathbb{N}^*$ divise n, on a $\Phi_d(X) = \prod_{\substack{1\leqslant k\leqslant d \\ k\wedge d=1}} (X - e^{\frac{2ik\pi}{d}}) = \prod_{\substack{1\leqslant k\leqslant d \\ k\frac{n}{d}\wedge n=\frac{n}{d}}} (X - e^{\frac{2ik\frac{n}{d}\pi}{n}}) = \prod_{\substack{1\leqslant l\leqslant n \\ l\wedge n=\frac{n}{d}}} (X - e^{\frac{2il\pi}{n}})$, donc $\prod_{d|n} \Phi_d(X) = \prod_{d|n} \prod_{\substack{1\leqslant l\leqslant n \\ l\wedge n=\frac{n}{d}}} (X - e^{\frac{2il\pi}{n}}) = \prod_{1\leqslant l\leqslant n} (X - e^{\frac{2il\pi}{n}}) = X^n - 1$. □

Corollaire 8.2.12 – *Pour tout* $n \in \mathbb{N}^*$, *on a* $\Phi_n(X) = \prod_{d|n}(X^{\frac{n}{d}} - 1)^{\mu(d)}$.

Démonstration – Le corps $\mathbb{C}(X)$ des fractions rationnelles sur $\mathbb{C}$ est commutatif, donc $\mathbb{C}(X)^*$ muni de la multiplication est un groupe abélien. Soient $f : \mathbb{N}^* \to \mathbb{C}(X)^*$ et $g : \mathbb{N}^* \to \mathbb{C}(X)^*$ définies par $f(n) = \Phi_n(X)$ et $g(n) = X^n - 1$. La proposition 8.2.11 donne $g(n) = \prod_{d|n} f(d)$ pour tout $n \in \mathbb{N}^*$, et la formule (1) ci-dessus permet de conclure. □

Corollaire 8.2.13 – *Si un nombre premier* p *ne divise pas* $n \in \mathbb{N}^*$, *on a* $\Phi_{pn}(X) = \dfrac{\Phi_n(X^p)}{\Phi_n(X)}$.

Démonstration – On a $\Phi_{pn}(X) = \prod_{d|pn}(X^{\frac{pn}{d}} - 1)^{\mu(d)} = \prod_{\substack{d|pn \\ p|d}} (X^{\frac{pn}{d}} - 1)^{\mu(d)} \prod_{\substack{d|pn \\ p\nmid d}} (X^{\frac{pn}{d}} - 1)^{\mu(d)} = \prod_{d'|n}(X^{\frac{n}{d'}} - 1)^{\mu(pd')} \prod_{d|n}(X^{\frac{pn}{d}} - 1)^{\mu(d)} = \prod_{d|n}(X^{\frac{n}{d}} - 1)^{-\mu(d)} \prod_{d|n}((X^p)^{\frac{n}{d}} - 1)^{\mu(d)} = \frac{\Phi_n(X^p)}{\Phi_n(X)}$. □

Corollaire 8.2.14 – *Si un nombre premier* p *divise* $n \in \mathbb{N}^*$, *on a* $\Phi_{pn}(X) = \Phi_n(X^p)$.

Démonstration – Comme p divise n, on a $n = pn'$ pour $n' \in \mathbb{N}^*$. Soit $d \in \mathbb{N}^*$ un diviseur de $pn = p^2n'$ satisfaisant $\mu(d) \neq 0$. Alors p^2 ne divise pas d et, soit p ne divise pas d et d divise n (par le lemme de Gauss) ; soit p divise d et $p \not| \frac{d}{p}$, donc $\frac{d}{p}$ divise n' (par le lemme de Gauss) et d divise n. Ainsi, pour tout $d \in \mathbb{N}^*$ tel que $\mu(d) \neq 0$, on a $d|pn \iff d|n$. On obtient : $\Phi_{pn}(X) = \prod_{d|pn}(X^{\frac{pn}{d}} - 1)^{\mu(d)} = \prod_{d|n}(X^{p\frac{n}{d}} - 1)^{\mu(d)} = \prod_{d|n}((X^p)^{\frac{n}{d}} - 1)^{\mu(d)} = \Phi_n(X^p)$. □

Proposition 8.2.15 – *Pour tout* $n \in \mathbb{N}^*$, *le polynôme* $\Phi_n(X)$ *est à coefficients dans* $\mathbb{Z}$.

DÉMONSTRATION – On procède par récurrence (forte) sur $n \in \mathbb{N}^*$. On a $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$. Si, pour un entier $n \geqslant 2$, on a $\Phi_d(X) \in \mathbb{Z}[X]$ pour tout $d \in \mathbb{N}^*$ vérifiant $d < n$, alors $P = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(X) \in \mathbb{Z}[X]$ est unitaire. Il existe donc un unique couple $(Q, R) \in \mathbb{Z}[X]^2$ tel que $X^n - 1 = QP + R$ avec $\deg R < \deg P$. Comme ce couple est également unique dans $\mathbb{C}[X]$ et que $X^n - 1 = \Phi_n(X)P$ dans $\mathbb{C}[X]$ (proposition 8.2.11), on a $\Phi_n(X) = Q \in \mathbb{Z}[X]$. Ainsi on a $\Phi_n(X) \in \mathbb{Z}[X]$ pour tout $n \in \mathbb{N}^*$. □

Exercice 8.2.16 – a) *Calculer $\Phi_n(X)$ pour $n \in \{1, \ldots, 6\}$, puis $\Phi_{14}(X)$, $\Phi_{30}(X)$, $\Phi_{72}(X)$ et $\Phi_{80}(X)$.*
b) *Montrer que $\Phi_{2n}(X) = \Phi_n(-X)$ pour tout $n \in \mathbb{N}^*$ impair.*
c) *Soient $n \in \mathbb{N}^*$, p un nombre premier et $x \in \mathbb{Z}$ tel que p divise $\Phi_{pn}(x)$. Montrer que p divise $\Phi_n(x)$. Montrer aussi que, si p ne divise pas n, alors n divise $p - 1$* (difficile).

8.3 Étude de l'anneau $\mathscr{A}$

Nous montrons que l'anneau des fonctions arithmétiques est un exemple d'anneau factoriel non noethérien, et que sa structure est très liée à celle des *anneaux de séries formelles* (§8.3.2).

8.3.1 $\mathscr{A}$ n'est pas un anneau noethérien

Proposition 8.3.1 – *L'anneau $\mathscr{A}$ n'est pas noethérien. En particulier, ce n'est pas un anneau principal.*

DÉMONSTRATION – Pour tout $n \in \mathbb{N}$, on note I_n l'ensemble des fonctions $f \in \mathscr{A}$ satisfaisant $f(k) = 0$ pour tout $k \in \mathbb{N}^*$ divisible par aucun nombre premier inférieur ou égal à n.

Soit $n \in \mathbb{N}$. Montrons que I_n est idéal de $\mathscr{A}$. La fonction nulle appartient à I_n et, si f et g sont deux éléments de I_n, alors $f - g$ aussi. De plus, pour tout $\alpha \in \mathscr{A}$, on a $(\alpha * f)(k) = \sum_{d|k} \alpha(d) f(\frac{k}{d}) = 0$ donc $\alpha * f \in I_n$. Ceci montre que I_n est un idéal de $\mathscr{A}$.

Or la suite $(I_n)_{n \in \mathbb{N}}$ est croissante et non stationnaire, donc l'anneau $\mathscr{A}$ n'est pas noethérien. □

Néanmoins $\mathscr{A}$ partage avec les anneaux noethériens, et donc principaux, la propriété suivante.

Proposition 8.3.2 – *Si A est factoriel, toute fonction arithmétique $f \in \mathscr{A}_A$ non nulle est le produit d'un élément inversible de $\mathscr{A}_A$ et d'un produit fini d'éléments irréductibles de $\mathscr{A}_A$.*

DÉMONSTRATION – Soit $f \in \mathscr{A}_A^*$. Si $N(f) = 1$, alors $f(1)$ est un élément non nul de A, il se décompose donc en un produit d'un élément inversible de A par un produit fini d'éléments irréductibles de A, de plus toute telle décomposition comporte le même nombre $n_{f(1)}$ d'éléments irréductibles. Si $n_{f(1)} = 0$, alors $f(1)$ est inversible, donc f aussi. Supposons que, pour un entier $N \in \mathbb{N}^*$, toute fonction $g \in \mathscr{A}_A$ vérifiant $n_{g(1)} < N$ a une décomposition de la forme voulue. Si f vérifie $n_{f(1)} = N$, alors f n'est pas inversible, donc soit f est

irréductible, soit $f = u * v$ pour u et v dans $\mathscr{A}_A^*$ non inversibles. En particulier, on a $N(u) = N(v) = 1$. On a aussi $f(1) = u(1)v(1)$ et, comme u et v ne sont pas inversibles dans $\mathscr{A}_A$, alors $u(1)$ et $v(1)$ ne sont pas inversibles dans A. Ils se décomposent donc chacun en un produit d'un élément inversible de A par un produit fini d'éléments irréductibles de A, et on obtient $n_{f(1)} = n_{u(1)} + n_{v(1)}$ avec $n_{u(1)}$ et $n_{v(1)}$ non nuls. Par minimalité de N, on en déduit que u et v ont une décomposition de la forme voulue, donc $f = u * v$ aussi.

Supposons $N(f) > 1$ et que toute fonction $g \in \mathscr{A}_A$ non nulle et vérifiant $N(g) < N(f)$ a une décompositon de la forme voulue.

— Si $f = u * v$ pour u et v dans $\mathscr{A}_A$ non inversibles, on a $N(f) = N(u)N(v)$ d'après le lemme 8.1.5, et comme $N(u)$ et $N(v)$ sont distincts de 1, on a $N(u) < N(f)$ et $N(v) < N(f)$. L'hypothèse sur f entraîne que u et v ont une décomposition de la forme voulue, donc aussi $f = u * v$.

— Si $f \neq u * v$ quelles que soient u et v dans $\mathscr{A}_A$ non inversibles, alors f est irréductible.

On en déduit que tout $f \in \mathscr{A}_A$ non nul a une décomposition de la forme voulue. □

8.3.2 Les séries formelles

Avant de poursuivre notre analyse de l'anneau des fonctions arithmétique, nous devons dire quelques mots sur les *séries formelles* (à plusieurs indéterminées), une généralisation des polynômes (à plusieurs indéterminées).

Définition 8.3.3 – *Une* série formelle *à n indéterminées sur un anneau commutatif A est une application de $\mathbb{N}^n$ dans A. L'ensemble des séries formelles est noté $A[[X_1, \ldots, X_r]]$.*

Le produit de deux séries formelles R et S est défini par $(RS)(\overline{x}) = \sum_{\overline{u}+\overline{v}=\overline{x}} R(\overline{u})S(\overline{v})$.

Remarque 8.3.4 – Exactement de la même manière que pour l'ensemble $A[X_1, \ldots, X_r]$, on montre que l'ensemble $A[[X_1, \ldots, X_r]]$ muni de l'addition et du produit ci-dessus est un anneau commutatif, qui est intègre si si A est intègre. De même, si $A[[X_1, \ldots, X_r]]$ est factoriel, alors A est factoriel (en revanche, la réciproque est fausse).

Désormais A désigne un sous-anneau de $\mathbb{C}$ tel que l'anneau $A[[X_1, \ldots, X_r]]$ est factoriel. D'après le fait suivant, cette hypothèse est vérifiée si A est principal, par exemple si $A = \mathbb{C}$ ou $A = \mathbb{Z}$.

Fait 8.3.5 – **(Samuel, 1961 – admis)** *Si A est un anneau principal, alors $A[[X_1, \ldots, X_r]]$ est factoriel.*

8.3.3 $\mathscr{A}$ est un anneau factoriel

On rappelle que A est un sous-anneau de $\mathbb{C}$ tel que l'anneau $A[[X_1, \ldots, X_r]]$ est factoriel. Nous démontrons que l'anneau $\mathscr{A}_A$ est factoriel.

Remarque 8.3.6 – Pour tout $n \in \mathbb{N}$, on note J_n l'ensemble des $f \in \mathscr{A}_A$ satisfaisant $f(k) = 0$ pour tout $k \in \mathbb{N}^*$ divisible par aucun nombre premier supérieur ou égal à n. De la même façon que les ensembles I_n vus dans la démonstration de la proposition 8.3.1, ce

sont des idéaux de $\mathscr{A}_A$, et $(J_n)_n$ **est une suite décroissante d'idéaux de** $\mathscr{A}_A$. De plus, **l'intersection** $\cap_{n\in\mathbb{N}} J_n$ **est l'idéal nul**.

Lemme 8.3.7 – *Pour tout entier $n \geqslant 3$, s'il y a r nombres premiers strictement inférieurs à n, les anneaux $\mathscr{A}_A/J_n$ et $A[[X_1,\dots,X_r]]$ sont isomorphes. En particulier, l'anneau $\mathscr{A}_A/J_n$ est factoriel.*

Démonstration – Soient $p_1,\dots,p_r$ les nombres premiers strictement inférieurs à n et $\mathscr{P}_r$ l'ensemble des entiers naturels divisibles par aucun nombre premier supérieur ou égal à n : c'est l'ensemble des entiers de la forme $p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ pour des entiers naturels $\alpha_1,\dots,\alpha_r$, de plus cette écriture est unique.

On définit des applications $F : \mathscr{A}_A \to A[[X_1,\dots,X_r]]$ et $G : A[[X_1,\dots,X_r]] \to \mathscr{A}_A$ par :
- $F(f)(\alpha_1,\dots,\alpha_r) = f(p_1^{\alpha_1}\cdots p_r^{\alpha_r})$ pour tout $f \in \mathscr{A}_A$ et tout $(\alpha_1,\dots,\alpha_r) \in \mathbb{N}^r$;
- $G(S)(p_1^{\alpha_1}\cdots p_r^{\alpha_r}) = S(\alpha_1,\dots,\alpha_r)$ pour tout $S \in A[[X_1,\dots,X_r]]$ et tout $p_1^{\alpha_1}\cdots p_r^{\alpha_r} \in \mathscr{P}_r$.

L'application composée $G\circ F$ étant l'identité de $A[[X_1,\dots,X_r]]$, on en déduit que F est surjective.

Aussi, on a $F(\delta_1) = 1$ et, pour tous f et g dans $\mathscr{A}_A$, on a $F(f+g) = F(f)+F(g)$. De plus, pour tous f et g dans $\mathscr{A}_A$ et tout $(\alpha_1,\dots,\alpha_r) \in \mathbb{N}^r$, on a

$$\begin{array}{rcl}(F(f)F(g))((\alpha_1,\dots,\alpha_r) & = & \sum_{(u_1,\dots,u_r)+(v_1,\dots,v_r)=(\alpha_1,\dots,\alpha_r)} F(f)(u_1,\dots,u_r)F(g)(v_1,\dots,v_r)\\ & = & \sum_{(u_1+v_1,\dots,u_r+v_r)=(\alpha_1,\dots,\alpha_r)} f(p_1^{u_1}\cdots p_r^{u_r})g(p_1^{v_1}\cdots p_r^{v_r}).\end{array}$$

Or si on pose $m = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$, on a $m = p_1^{u_1}\cdots p_r^{u_r}p_1^{v_1}\cdots p_r^{v_r}$ si et seulement si $(u_1+v_1,\dots,u_r+v_r) = (\alpha_1,\dots,\alpha_r)$, donc on obtient $(F(f)F(g))(\alpha_1,\dots,\alpha_r) = \sum_{d|m} f(d)g(\frac{m}{d}) = (f*g)(m) = F(f*g)((\alpha_1,\dots,\alpha_r))$. Ainsi F est un morphisme d'anneaux. Comme son noyau est $\operatorname{Ker} F = \{f \in \mathscr{A}_A \mid f(m) = 0 \ \ \forall m \in \mathscr{P}_r\} = J_n$, le théorème d'isomorphisme donne le résultat. □

Lemme 8.3.8 – *Soient p et u deux éléments de $\mathscr{A}_A$. On suppose que la classe de p divise la classe de u dans $\mathscr{A}_A/J_n$ pour tout $n \in \mathbb{N}$ avec $n \geqslant 3$. Alors p divise u dans $\mathscr{A}_A$.*

Démonstration – Si p est nulle, alors la classe de u dans $\mathscr{A}_A/J_n$ est nulle pour tout $n \geqslant 3$, donc on a $u \in \cap_{n\in\mathbb{N}} J_n$ et u est la fonction nulle. Ainsi p divise u dans $\mathscr{A}_A$ et on peut supposer p non nulle.

On peut aussi supposer p non inversible.

Notons que, pour tous α et β dans $\mathscr{A}_A$, si $\overline{\alpha} = \overline{\beta}$ dans $\mathscr{A}_A/J_n$ pour un entier $n \geqslant 3$, alors il existe $\omega \in J_n$ tel que $\alpha = \beta + \omega$. On en déduit que, pour tout $k \in \mathbb{N}^*$ divisible par aucun nombre premier supérieur ou égal à n, on a $\omega(k) = 0$ et $\alpha(k) = \beta(k)$.

On construit alors une fonction arithmétique u^* de la façon suivante. On pose $u^*(1) = 1$ puis, pour tout entier $k \geqslant 2$, on considère le plus grand nombre premier p_k divisant k et on pose $m = \max(N(p), p_k) + 1$. On note alors $u^*(k) = v(k)$ où v est un élément de $\mathscr{A}_A$ satisfaisant $\overline{u} = \overline{p} * \overline{v}$ dans $J_m/\mathscr{A}_A$. On remarque que, si w est un élément quelconque de $\mathscr{A}_A$ parmi ceux satisfaisant $\overline{u} = \overline{p} * \overline{w}$ dans $J_n/\mathscr{A}_A$ pour un entier n quelconque parmi ceux qui sont strictement supérieurs à p_k et à $N(p)$, alors J_m contient J_n, et on a donc

$\overline{u} = \overline{p} * \overline{v} = \overline{p} * \overline{w}$ dans $\mathscr{A}_A/J_m$. Le paragraphe précédent donne $w(k) = v(k) = u^*(k)$. Cette remarque appliquée à v montre que $v(l) = u^*(l)$ pour tout entier $l \in \mathbb{N}^*$ divisible par aucun nombre premier supérieur ou égal à m, autrement dit que $v - u^*$ appartient à J_m. Comme $u - p * v$ appartient à J_m, on en déduit $u - p * u^* \in J_m$. Or $k \geqslant 2$ étant quelconque, ceci vaut pour tout $m > N(p)$, donc on a $u - p * u^* \in \cap_{m>N(p)} J_m$, d'où $u = p * u^*$ et p divise u dans $\mathscr{A}_A$. □

Théorème 8.3.9 – **(Cashwell-Everett, 1959)** *L'anneau $\mathscr{A}_A$ est factoriel.*

Démonstration – Il suit des propositions 7.1.2 et 8.3.2 qu'il suffit de montrer que tout élément irréductible de $\mathscr{A}_A$ est premier. Soit $p \in \mathscr{A}_A$ irréductible. On suppose que p divise un produit $u * v$ d'éléments de $\mathscr{A}_A$, et on montre que p divise u ou v. On peut supposer que $p \not| u$. D'après le lemme 8.3.8, il existe $m \in \mathbb{N}$ tel que la classe de p ne divise pas celle de u dans $\mathscr{A}_A/J_m$, et comme la suite $(J_n)_{n\in\mathbb{N}}$ est décroissante, la classe de p ne divise pas celle de u dans $\mathscr{A}_A/J_n$ pour tout $n \geqslant m$. Or $\mathscr{A}_A/J_n$ est factoriel pour tout $n \geqslant m$ d'après le lemme 8.3.7, et la classe de p divise la classe de $u * v$ dans $\mathscr{A}_A/J_n$ pour tout $n \in \mathbb{N}$. Alors la classe de p divise celle de v dans $\mathscr{A}_A/J_n$ pour tout $n \geqslant m$, et même pour tout $n \in \mathbb{N}$ puisque la suite $(J_n)_{n\in\mathbb{N}}$ est décroissante. Ainsi p divise v d'après le lemme 8.3.8. □

Chapitre 9

Complément : les anneaux noethériens

9.1 Quelques mots sur Emmy Noether

Emmy Noether (1882-1935) était une mathématicienne allemande connue pour ses contributions essentielles à l'algèbre, notamment à la théorie des anneaux, et à la physique théorique. En raison de la place des femmes à cette époque dans la société, ses études et sa carrière ont été extrêmement compliquées, et elle a dû combattre la misogynie durant toute sa vie.

Elle a intégré l'université d'Erlangen (Allemagne) en 1900, elles étaient seulement deux femmes parmi 956 étudiant·e·s et elles devaient demander à chaque professeur son autorisation personnelle pour suivre ses cours. Elle a soutenu une thèse d'algèbre en 1907 puis a enseigné durant sept ans à l'université d'Erlangen, bénévolement et sous le nom de son père, qui était professeur à l'université.

En 1915, elle a rejoint l'université de Göttingen (Allemagne), mais malgré les soutiens appuyés de David Hilbert et de Félix Klein, elle n'a pas pu obtenir de poste officiel et travaillait sans rémunération : elle s'en sortait grâce à l'aide de sa famille. De plus, durant les première années elle devait donner ses cours sous le nom de David Hilbert car la faculté de philosophie était très opposée à ce qu'une femme soit nommée professeure ("Que penseront nos soldats, quand ils reviendront à l'université et verront qu'ils doivent apprendre aux pieds d'une femme ?"). Cette attitude indignait profondément Hilbert.

En 1915, elle a démontré un théorème en physique, qui est fondamental pour la physique mathématique, et qui a même été qualifié de "monument de la pensée mathématiques" par Albert Einstein.

Il y avait un contraste extrême entre ses multiples résultats scientifiques dans des domaines variés, ses approches particulièrement novatrices des problèmes, et sa situation académique : c'est seulement en 1919 qu'elle a obtenu l'autorisation d'enseigner à l'université de Göttingen, et il ne s'agissait même pas d'un poste fixe, seulement d'une autorisation à enseigner bénévolement. Elle a encore dû travailler plusieurs années sans salaire, continuant donc à dépendre financièrement de sa famille.

En 1921, elle a publié un article concernant la "théorie des idéaux dans les anneaux", qui a eu une influence majeure sur le développement de la théorie des anneaux en raison de sa généralité, sa simplicité et son efficacité. En effet, elle posait dans cet article les fondations de la théorie abstraite des anneaux et de leurs idéaux : auparavant les anneaux étaient surtout étudiés séparément ; la théorie abstraite générale est principalement due à Emmy Noether.

C'est en 1923, après plusieurs interventions d'Albert Einstein, qu'elle a enfin obtenu un poste, du plus bas niveau existant et qu'elle a reçu son premier salaire.

Ensuite elle a publié plusieurs autres articles fondamentaux traitant des anneaux et encore bien d'autres concernant, plus généralement, l'algèbre théorique. Ses nombreux travaux ont eu une très forte influence sur le développement de plusieurs branches de l'algèbre, dont la théorie des représentations (en théorie des groupes) et la topologie algébrique.

À partir de 1911, elle a dirigé une quinzaine de thèse, dont celles de mathématicien·ne·s célèbres comme Grete Hermann (une femme dont la thèse a posé les fondations du *calcul formel*, un domaine à l'interface des mathématiques et de l'informatique), Hans Fitting (théoricien des groupes) ou Ernst Witt (algébriste).

En raison de ses origines juives, elle a été congédiée de son université en 1933 à la suite de l'élection d'Adolf Hitler, et des étudiants l'ont faite évincer de son logement. La situation étant devenue trop dangereuse, elle a rejoint les États-Unis cette même année. Comme beaucoup d'autres scientifiques fuyaient également l'Allemagne pour les États-Unis, l'obtention d'un poste n'était pas évidente. Malgré l'influence de ses recherches, qui faisaient d'elle l'une des personnes les plus importantes parmi les mathématicien·ne·s, et les appuis d'Albert Einstein et de nombreux mathématiciens, elle n'a obtenu qu'une invitation d'un an en Pennsylvanie qui sera ensuite renouvelée. Elle est décédée en 1935 lors d'une opération bénigne.

Après sa mort, Albert Einstein a écrit une lettre élogieuse sur Emmy Noether qui a été publiée au *New-York Times* en mai 1935. En son honneur, un cratère de la Lune et un astréroïde portent son nom.

C'est Emmy Noether qui a défini les anneaux noethériens ci-dessous, son travail sur ces anneaux, et sur les anneaux en générales, va infiniment plus loin que les deux pages qui suivent (d'autant plus que le théorème ci-dessous est dû à Hilbert, c'est le résultat sur ces anneaux le plus lié au programme du cours). Le fait que ces anneaux portent son nom était l'occasion de dire quelques mots à son sujet, ainsi que sur le fait qu'il y ait si peu de scientifiques femmes célèbres (consulter le site femmes-et-maths.fr pour des portraits de mathématiciennes contemporaines).

9.2 Anneaux noethériens

On fixe désormais un anneau commutatif A.
Les *anneaux noethériens* sont définis comme des anneaux non nécessairement commutatifs, et leur définition nécessite d'introduire les *idéaux à gauche* et *à droite*. Cependant, le contexte qui nous intéresse étant celui des anneaux commutatifs, nous nous restreindrons à ces anneaux-ci.

Définition 9.2.1 –
- *Un idéal I de A est dit être* de type fini *(ou* finiment engendré*) s'il existe une partie finie X de A telle que $I = (X)$.*
- *L'anneau A est dit* noethérien *si tous ses idéaux sont* de type fini*.*

Remarque 9.2.2 –
- Les anneaux principaux sont noethériens.
- Un anneau noethérien n'est pas supposé être intègre.
- Tout quotient d'un anneau noethérien est noethérien.

Le résultat ci-dessous est indispensable pour la suite. Notons que sa démonstration utilise l'axiome du choix dépendant : l'étude des anneaux noethériens nécessite cet axiome.

Proposition 9.2.3 – *Les conditions suivantes sont équivalentes :*
(1) *A est noethérien ;*
(2) *toute suite croissante (*pour l'inclusion*) d'idéaux de A est stationnaire ;*
(3) *toute famille non vide d'idéaux de A a un élément maximal (*pour l'inclusion*).*

Démonstration – Si A est noethérien et si $(I_i)_{i\in\mathbb{N}}$ est une suite croissante d'idéaux de A, alors l'union $J = \cup_{i\in\mathbb{N}} I_i$ est également un idéal de A. Comme A est noethérien, il y a un ensemble fini X d'éléments de A tel que $J = (X)$. Or les éléments de X appartiennent tous à des éléments de la suite $(I_i)_{i\in\mathbb{N}}$, et comme la suite est croissante, il existe $j \in \mathbb{N}$ tel que I_j contient X. On en déduit que $I_i = I_j$ pour tout $i \geqslant j$, la suite est donc stationnaire et (1) implique (2).

Si A a une famille non vide $\mathfrak{F}$ d'idéaux de A n'ayant aucun élément maximal, alors pour tout $I \in \mathfrak{F}$, il existe $J \in \mathfrak{F}$ tel que $I \subsetneq J$. **D'après l'axiome du choix dépendant**, il existe une suite $(I_i)_{i\in\mathbb{N}}$ d'éléments de $\mathfrak{F}$ telle qu'on ait $I_i \subsetneq I_{i+1}$ pour tout $i \in \mathbb{N}$. Ainsi, il y a une suite croissante d'idéaux de A qui n'est pas stationnaire et (2) implique (3).

Si toute famille non vide d'idéaux de A a un élément maximal, alors pour tout idéal I de A, la famille des idéaux de type fini contenus dans I a un élément maximal J. Si on a $J \neq I$, il existe $x \in I \setminus J$, mais l'idéal $(x) + J$ contient strictement J, est de type fini et est contenu dans I, ce qui contredit la maximalité de J. On en déduit que $I = J$ est de type fini, et (3) implique (1). □

Corollaire 9.2.4 – *Dans un anneau noethérien intègre, tout élément non nul se décompose en un produit d'un élément inversible u par un produit d'éléments irréductibles $p_1, \ldots, p_r$.*

Démonstration – Soit A un anneau noethérien intègre. Soit X l'ensemble des éléments de A^* n'admettant pas de décomposition de cette forme. Si X est non vide, alors d'après la proposition 9.2.3, l'ensemble $\mathfrak{F}$ des idéaux de la forme (x) pour $x \in X$ a un élément maximal (a) pour $a \in X$. En particulier, a n'est ni inversible, ni irréductible, donc $a = uv$ pour deux éléments non inversibles u et v. Si u appartient à X, alors par maximalité de (a) et comme u divise a, on a $(u) = (a)$ et a divise u. Comme A est intègre, cela implique que v est inversible, ce qui contredit le choix de v. On en déduit que u n'appartient pas à X et, de même, v n'appartient pas à X. Ainsi u et v admettent une décomposition de la forme voulue, donc $a = uv$ en admet aussi une, ce qui contredit le choix de a. □

Corollaire 9.2.5 – *Si A est un anneau noethérien intègre dans lequel tous les éléments irréductibles sont premiers, alors A est un anneau factoriel.*

Démonstration – Ce résultat découle de la proposition suivant la définition d'un anneau factoriel et du corollaire 9.2.4 □

Corollaire 9.2.6 – *Tout anneau qui est à la fois noethérien et à $PGCD$ est factoriel.*

Démonstration – Un anneau à $PGCD$ est intègre par définition. Or on a vu que, dans tout anneau à $PGCD$, les éléments irréductibles sont premiers, donc si un tel anneau est noethérien, il est factoriel d'après le corollaire 9.2.5. □

Théorème 9.2.7 – **(théorème de la base de Hilbert)** *Si A est un anneau noethérien, l'anneau $A[X_1, \ldots, X_n]$ est aussi noethérien.*

Démonstration – Comme les anneaux $A[X_1, \ldots, X_i][X_{i+1}]$ et $A[X_1, \ldots, X_i, X_{i+1}]$ sont isomorphes pour tout $i \in \mathbb{N}$, il suffit de montrer que $A[X]$ est nothérien. Soit I un idéal de $A[X]$. On doit montrer que I est de type fini. On peut supposer que I est non nul.

Pour tout $n \in \mathbb{N}$, on note J_n l'ensemble formé de 0_A et des coefficients dominants des éléments de I de degré n. Soient $(x, y) \in J_n^2$ et $a \in A$. Montrons que $x + y \in J_n$ et que $ax \in J_n$. On peut supposer x, y, $x + y$ et ax non nuls. Il existe donc des polynômes P et Q dans I tels que $P = a_n X^m n + \cdots + a_0 \in I$ avec $a_n = x$ et $Q = b_n X^n + \cdots + b_0$ avec $b_n = y$. On a donc $P + Q = \sum_{i=0}^{n}(a_i + b_i)X^i$, et comme on a $a_n + b_n = x + y \neq 0_A$, le coefficient dominant de $P + Q$ est $a_n + b_n = x + y$. Ainsi $x + y$ appartient à J_n. Aussi, le polynôme $aP = (a1)P$ est un polynôme de I de degré n, et son coefficient dominant est $aa_n = ax$, donc on a $ax \in J_n$. Ceci montre que J_n est un idéal de A.

Aussi, pour tout $n \in \mathbb{N}$ et tout $x \in J_n$ non nul, il existe $P \in I$ de degré n et de coefficient dominant x. Alors XP est un polynôme de I de degré $n + 1$ et de coefficient dominant x, donc on a $x \in J_{n+1}$. Ainsi la suite $(J_n)_{n\in\mathbb{N}}$ est croissante et, d'après la proposition 9.2.3, il existe $N \in \mathbb{N}$ tel que $J_n \subseteq J_N$ pour tout $n \in \mathbb{N}$.

Comme A est noethérien, chaque idéal J_i pour $i \in \mathbb{N}$ est de type fini, et il existe un ensemble fini X_i formé d'éléments non nuls de A tel que $J_i = (X_i)$. On associe à chaque $x \in X_i$ un polynôme $P_x \in I$ de degré i ayant x pour coefficient dominant. Soit Y l'ensemble des polynômes de la forme P_x pour $x \in X_j$ avec $j \geqslant N$. Alors Y est une famille finie de polynômes de I.

Montrons que $I = (Y)$. Si ce n'est pas le cas, il existe $P \in I \setminus (Y)$ qu'on peut choisir de degré minimal d. Nécessairement P est non nul, on note a_d son coefficient dominant. On a $a_d \in J_d$ et, si on note $m = \min(d, N)$, on a $a_d \in J_m = (X_m)$. Il existe alors des polynômes $P_1, \ldots, P_k$ de Y de degré m avec pour coefficients dominant $x_1, \ldots, x_k$, et des éléments $\alpha_1, \ldots, \alpha_k$ de A tels que $a_d = \alpha_1 x_1 + \cdots + \alpha_k x_k$. Alors $Q = \alpha_1 P_1 + \cdots + \alpha_k P_k$ est un polynôme de degré m, appartenant à (Y) et ayant pour coefficient dominant a_d. Ainsi $P - X^{d-m}Q \in I$ est de degré strictement inférieur à d, et par minimalité de d, on a $P - X^{d-m}Q \in (Y)$. Comme Q appartient à (Y), on en déuit que P appartient à (Y), ce qui contredit la minimalité de d et démontre que $I = (Y)$. □

Exemples 9.2.8 – Tous les anneaux de la forme $\mathbb{Z}[X_1, \ldots, X_n]$, et $\mathbb{K}[X_1, \ldots, X_n]$ pour un corps commutatif $\mathbb{K}$, sont à la fois factoriels et noethériens.

Corollaire 9.2.9 – *Pour tout $\alpha \in \mathbb{C}$, les anneaux $\mathbb{Z}[\alpha]$ et $\mathbb{Q}[\alpha]$ sont noethériens. Un tel anneau est factoriel si et seulement si ses éléments irréductibles sont premiers.*

Démonstration – Pour tout sous-anneau A de $\mathbb{C}$ et tout $\alpha \in \mathbb{C}$, l'application $\mathrm{ev}_\alpha : A[X] \to \mathbb{C}$ définie par $\mathrm{ev}_\alpha(P) = P(\alpha)$ est un morphisme d'anneaux, et son image est le sous-anneau $A[\alpha] = \{P(\alpha) \mid P \in A[X]\}$ de $\mathbb{C}$.

Ainsi, si on note I le noyau de ev_α, alors d'après le théorème d'isomorphisme, les anneaux $A[X]/I$ et $A[\alpha]$ sont isomorphes. Or, si A est noethérien, l'anneau $A[X]$ est nothérien d'après le théorème de la base de Hilbert, donc $A[\alpha] \simeq A[X]/I$ est noethérien (remarque 9.2.2).

Comme $\mathbb{Z}$ est un anneau principal et $\mathbb{Q}$ un corps, ce sont des anneaux noethériens d'après la remarque 9.2.2, d'où la première partie du corollaire. La seconde partie suit du corollaire 9.2.5. □

Ce résultat explique pourquoi il est difficile de trouver un anneau à $PGCD$ qui n'est pas factoriel.