UVSQ 2022/2023
Licence de sciences et technologie, santé
LSMA511 (structures algébriques)

Notes de cours

Table des matières

1 Ensembles, applications, relations d'équivalence

Définition Si X et Y sont deux ensembles, une *application de X dans Y* est une partie f du produit cartésien $X \times Y$ telle que

$$\forall x \in X,\ \exists! y \in Y,\ (x,y) \in f.$$

Lorsque $(x,y) \in f$, on note $y = f(x)$ – noter que cette notation est autorisée par l'axiome d'unicité dans la définition d'une application. On dit que X est *l'ensemble de départ de f* et Y son *ensemble d'arrivée*.

Remarque Cette définition formalise définitivement la définition d'une application comme *étant* son graphe. Autrement dit, $f = \{(x,y) \in X \times Y,\ y = f(x)\}$.

Remarque On confond souvent, en mathématique, les mots de *fonction* et d'application. A vrai dire, la notion de fonction généralise légèrement celle d'application ; la voici. Si X et Y sont deux ensembles, une *fonction de X dans Y* est une partie f du produit cartésien $X \times Y$ telle que pour tout $x \in X$, il existe *au plus un* $y \in Y$ tel que $(x,y) \in f$. Là encore, X est *l'ensemble de départ de f* et Y son *ensemble d'arrivée*, et l'*ensemble de définition* de f est $\{x \in X,\ \exists y \in Y,\ (x,y) \in f\}$. Bien entendu, si D est l'ensemble de définition d'une fonction $f : X \to Y$, la restriction de f à D est une application $D \to Y$.

Exemple On pourra parler de la fonction $\mathbb{C} \to \mathbb{C}$, $x \mapsto \frac{1}{x^2-1}$. Son ensemble de définition est $\mathbb{C} \setminus \{\pm 1\}$. En revanche, parler de l'application $\mathbb{C} \to \mathbb{C}$, $x \mapsto \frac{1}{x^2-1}$ n'a pas de sens.

Définitions Soit $f : X \to Y$ une application.

(i) f est *injective* lorsque $\forall x, x' \in X,\ f(x) = f(x') \Longrightarrow x = x'$.

(ii) f est *surjective* lorsque $\forall y \in Y,\ \exists x \in X,\ y = f(x)$.

(iii) f est *bijective* lorsque f est injective et surjective.

Exemples Si $A \subseteq X$, l'application $A \to X$, $a \mapsto a$ est injective (prototype d'injection). Si X et Y sont des ensembles, $X \times Y \to X$, $(x,y) \mapsto x$ est surjective (prototype de surjection). Si X est un ensemble, $\mathrm{id}_X : X \to X$, $x \mapsto x$ est bijective (prototype de bijection).

Exercice 0 Définir la composée $g \circ f$ de deux applications en tant que graphe.

Exercice 1 Une application $f : X \to Y$ est bijective si, et seulement s'il existe $g : Y \to X$ telle que $f \circ g = \mathrm{id}_Y$ et $g \circ f = \mathrm{id}_X$. Dans ces conditions, g est unique et est aussi bijective. On note alors $g = f^{-1}$ et on appelle g *l'application réciproque* de f. Elle vérifie $g^{-1} = f$.

Exercice 2 Si $f : X \to Y$ et $g : Y \to Z$ sont des bijections, alors $g \circ f : X \to Z$ est également bijective, et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Définitions Soient $f : X \to Y$ une application, $A \subseteq X$ et $B \subseteq Y$.

(i) L'*image (directe)* de A par f est

$$f(A) = \{f(x),\ x \in A\} = \{y \in Y,\ \exists x \in A,\ y = f(x)\}\,.$$

En particulier, l'*image de f* est $\mathrm{im}(f) = f(X) = \{y \in Y,\ \exists x \in X,\ y = f(x)\} = \{f(x),\ x \in X\}$.

(ii) L'*image réciproque* (ou *inverse*) de B par f est (gare à la notation !)

$$f^{-1}(B) = \{x \in X,\ f(x) \in B\}\,.$$

(iii) Si $b \in Y$, la *fibre de b*, que l'on note (dangereusement) $f^{-1}(b)$ est

$$f^{-1}(b) = f^{-1}(\{b\}) = \{x \in X,\ f(x) = b\}\,.$$

Exercice 3 Si f est bijective, alors $f^{-1}(B)$ est (aussi) l'image directe de B par l'application f^{-1}.

Définitions Si X est un ensemble, une *relation binaire* sur X est une partie de $X \times X$. Si R est une relation binaire et si $(x,y) \in R$, on note xRy. Une *relation d'équivalence* sur X est une relation binaire $\sim$ sur X qui soit

(i) *réflexive* : $\forall x \in X,\ x \sim x$

(ii) *symétrique* : $\forall x, y \in X,\ x \sim y \Longrightarrow y \sim x$

(iii) *transitive* : $\forall x, y, z \in X$, ($x \sim y$ et $y \sim z$) $\Longrightarrow x \sim z$

Si $x \in X$, la *classe d'équivalence* (ou l'*orbite*) de x est $\mathrm{cl}(x) = \{y \in X,\ y \sim x\}$. L'ensemble des classes est l'*ensemble-quotient*, noté $X/\sim$. L'application $X \to X/\sim$, $x \mapsto \mathrm{cl}(x)$ est la *surjection (ou projection) canonique.*

Exercice 4 Si un ensemble X est muni d'une relation d'équivalence, les classes définissent une partition de X. Inversement, si $(P_k)_{k\in K}$ est une partition d'un ensemble X, la relation binaire $\sim$ sur X définie par $x \sim y \Longleftrightarrow \exists k \in K, x \in P_k$ et $y \in P_k$ est une relation d'équivalence dont les classes sont exactement les parties P_k de X. Ainsi, la donnée d'une relation d'équivalence sur un ensemble équivaut à la donnée d'une partition de cet ensemble.

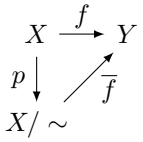
Théorème (Propriété universelle du quotient (PUQ) pour les applications)
*Soient $f : X \to Y$ une application, $\sim$ une relation d'équivalence sur X et $p : X \to X/\sim$ la projection canonique. On suppose que f est constante sur les classes de $\sim$ (*i.e. $\forall x, y \in X,\ x \sim y \Longrightarrow f(x) = f(y)$*). Alors :*

(i) il existe une unique application $\overline{f} : X/\sim \longrightarrow Y$ telle que $\overline{f} \circ p = f$

*(ii) $\overline{f}$ est injective si, et seulement si les classes de $\sim$ sont les fibres de f (*i.e. $\forall x, y \in X,\ x \sim y \Longleftrightarrow f(x) = f(y)$*)*

(iii) f et $\overline{f}$ ont la même image. En particulier, $\overline{f}$ est surjective si, et seulement si f l'est.

On résume l'affaire en disant que le diagramme ci-dessous commute.



Preuve. Par analyse-synthèse. Si $\overline{f}$ existe, elle est nécessairement définie par $\overline{f}\,(\mathrm{cl}(x)) = f(x)$. Cette formule définit bien une application grâce à l'hypothèse. Ainsi définie, $\overline{f}$ convient, et c'est la seule. ■

Exercice 5 Détailler les arguments de la preuve condensée ci-dessus.

Remarque La PUQ est le moyen universel de définir une application sur un ensemble-quotient. C'est important, car en mathématiques, on travaille sans arrêt sur des ensembles quotients (les nombres relatifs, rationnels, réels, complexes, les entiers modulo 13, les vecteurs du plan, les angles, les fonction L^p, les notations de Landau o, O, $\sim$, etc).

Le slogan *Une application constante sur les classes se factorise par la projection canonique.*

Exemple On définit sur $\mathbb{R}$ la relation binaire $x \sim y \Longleftrightarrow x - y \in \mathbb{Z}$. Soit $f : \mathbb{R} \to \mathbb{C}$ l'application $x \mapsto \exp(2i\pi x)$. D'une part, $\sim$ est une relation d'équivalence sur $\mathbb{R}$. D'autre part, les fibres de f sont exactement les classes d'équivalence de $\sim$ et l'image de f est le cercle $\mathbf{S}^1 = \{z \in \mathbb{C},\ |z| = 1\}$. En appliquant la PUQ, on en déduit que f induit une bijection $\overline{f} : \mathbb{R}/\sim \longrightarrow \mathbf{S}^1$.

[A vrai dire, les ensembles $\mathbb{R}/\sim$ et $\mathbf{S}^1$ d'une part et, d'autre part, l'application $\overline{f}$ ont de nombreuses propriétés qui, au même titre que l'exponentielle, propulsent cette bijection au rang de star des mathématiques.]

2 Anneaux de polynômes

Les définitions des structures abstraites de groupes, anneaux, corps, espaces vectoriels et algèbres sont regroupées dans le document *Axiomatique des structures abstraites* disponible en ligne sur Moodle, auquel on se référera.

Sauf mention explicite du contraire, dans tout ce cours, tous les anneaux considérés sont commutatifs.

Une question introductive : quand on parle d'un polynôme à une variable *ou à une* indéterminée*, quel est le statut mathématique exact de cette* variable *ou de cette* indéterminée *?*

Définition Soit $\mathcal{A}$ un anneau. Un *polynôme à une indéterminée* à coefficients dans $\mathcal{A}$ est une suite presque nulle $(a_0, a_1, \dots)$ d'éléments de $\mathcal{A}$ (*i.e.* $\exists N,\ \forall n \geq N,\ a_n = 0$).
On note provisoirement $\mathcal{A}^{(\mathbb{N})}$ l'ensemble de ces polynômes.

2.1 Opérations sur les polynômes à une indéterminée

(i) Somme : $(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$.

(ii) Produit externe : $x.(a_0, a_1, \dots) = (xa_0, xa_1, \dots)$.

(iii) Produit interne : $(a_0, a_1, \dots) \times (b_0, b_1, \dots) = (c_0, c_1, \dots)$ où

$$\forall n \in \mathbb{N},\ c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{p+q=n} a_p b_q.$$

Pour tout $k \in \mathbb{N}$, on définit le polynôme $e_k = (\delta_{k,n})_{n\in\mathbb{N}} = (0, \dots, 0, 1, 0, \dots)$ (le 1 à la k^{e} place).

Remarque Ces opérations miment les mêmes opérations sur les fonctions polynomiales.

Exercice 6
(i) Tout élément de $\mathcal{A}^{(\mathbb{N})}$ s'écrit comme une somme $\sum_{j\in J} a_j e_j$ où J est une partie *finie* de $\mathbb{N}$ et $a_j \in \mathcal{A}$ pour tout $j \in J$.

(ii) Soient J une partie finie de $\mathbb{N}$ et $(a_j)_{j\in J}$ une famille d'éléments de $\mathcal{A}$. Si $\sum_{j\in J} a_j e_j = 0$ alors $a_j = 0$, pour tout $j \in J$.

Proposition *Si $\mathbb{F}$ est un corps, $\left(\mathbb{F}^{(\mathbb{N})}, +, \cdot\right)$ est un espace vectoriel sur $\mathbb{F}$, de dimension infinie dénombrable, dont $(e_n)_{n\in\mathbb{N}}$ est une base.*

Preuve. Que ces lois confèrent à $\mathbb{F}^{(\mathbb{N})}$ une structure d'espace vectoriel dont le corps des scalaires est $\mathbb{F}$: exercice. Pour la base et la dimension, c'est l'exercice précédent. ■

Proposition *Si $\mathcal{A}$ est un anneau, $\left(\mathcal{A}^{(\mathbb{N})}, +, \times\right)$ est un anneau. Son unité est $e_0 = (1, 0, \dots)$.*

Preuve. Exercice - fastidieux mais élémentaire. ■

Exercice 7 Pour tout $n \geq 1$, $e_n = (e_1)^n$.

Grâce à l'exercice 7, si $a = \sum_{n\in\mathbb{N}} a_n e_n \in \mathcal{A}^{(\mathbb{N})}$ (somme presque nulle), alors $a = \sum_{n\in\mathbb{N}} a_n (e_1)^n$.

On adopte la notation (définitive) suivante : $\boxed{X = e_1 \text{ et } 1 = e_0 = X^0.}$

Avec cette notation, tout polynôme $a = (a_n)_{n\in\mathbb{N}}$ s'écrit $a = \sum_{n\in\mathbb{N}} a_n X^n$, la somme étant presque nulle. En outre, cette écriture est unique. Les a_n sont les *coefficients* de a et X est *l'indéterminée*.

On note définitivement $\boxed{\mathcal{A}^{(\mathbb{N})} = \mathcal{A}[X].}$

Proposition *Soient $d \in \mathbb{N}$ et $(a_0, a_1, \dots, a_d) \in \mathcal{A}^{d+1}$. Alors,*

$$a_0 + a_1 X + \cdots + a_d X^d = 0 \Longleftrightarrow a_0 = a_1 = \cdots = a_d = 0.$$

Preuve. Immédiat. ■

Le slogan *Un polynôme* est *la suite de ses coefficients.*

Remarque La réponse à la question introductive est maintenant acquise : l'indéterminée est la suite presque nulle $X = (0, 1, 0, 0, \dots)$.

2.2 Degré d'un polynôme non nul

Définitions si $P = \sum_n a_n X^n \in \mathcal{A}[X] \setminus \{0\}$, le *degré* de P est $\deg(P) = \max\{n \in \mathbb{N},\ a_n \neq 0\}$. Si $P = \sum_{0\leq n\leq d} a_n X^n$ et si $a_d \neq 0$, alors a_0 est le *terme constant* de P et a_d son *coefficient dominant*. On dit qu'un polynôme est *unitaire* lorsque son coefficient dominant est 1.

A noter Pour des raisons d'économie d'énoncés, souvent un peu snob, on attribue parfois le degré $-\infty$ ou $+\infty$ au polynôme nul. Dans ce cours, on ne le fera pas.

Proposition *Soient $P, Q \in \mathcal{A}[X] \setminus \{0\}$.*

(i) $P + Q = 0$ ou $\deg(P+Q) \leq \max\{\deg(P), \deg(Q)\}$.

(ii) $PQ = 0$ ou $\deg(PQ) \leq \deg(P) + \deg(Q)$.

Preuve. On note $P = \sum_{0\leq n\leq p} a_n X^n$ et $Q = \sum_{0\leq n\leq q} b_n X^n$ avec $a_p \neq 0 \neq b_q$.

(i) On suppose que $P+Q \neq 0$. Quitte à échanger P et Q, on peut supposer que $p \leq q$. Si $p < q$, alors le coefficient dominant de $P+Q$ est $b_q \neq 0$ et $\deg(P+Q) = q$. Si $p = q$, alors $P+Q = (a_p+b_p)X^p + \{\text{termes de degré } < p\}$ et $\deg(P+Q) \leq p$ (attention, l'égalité $\deg(P+Q) = p$ est fausse, comme le montre l'exemple $P = 1 - X$ et $Q = X$).

(ii) $PQ = a_p b_q X^{p+q} + \{\text{termes de degré } < p+q\}$. Ainsi, si $PQ \neq 0$, on obtient $\deg(PQ) \leq p+q$. ■

Exercice 8 Montrer que si $\deg P \neq \deg Q$, alors $\deg(P+Q) = \max\{\deg(P), \deg(Q)\}$.

Attention $a_p \neq 0$ et $b_q \neq 0$ n'entraîne pas que $a_p b_q \neq 0$. C'est la raison de la non égalité dans (ii).

Exemples

(i) Dans $\mathbb{Z}/6\mathbb{Z}$, $2 \times 3 = 0$ alors que $2 \neq 0$ et $3 \neq 0$.

(ii) Soit $\mathcal{F}(\mathbb{R}, \mathbb{R})$ l'anneau des fonctions $\mathbb{R} \to \mathbb{R}$ (les lois sont les lois usuelles). Si $f = \mathbf{1}_{]0,1]}$ est la fonction indicatrice de l'intervalle $]0, 1]$ et si $g = \mathbf{1}_{\mathbb{R}_-}$ est celle de $\mathbb{R}_-$, alors $fg = 0$ alors que $f \neq 0$ et $g \neq 0$ (on a noté 0 la fonction nulle).

Définitions Soient $\mathcal{A}$ un anneau et $a \in \mathcal{A}$. On dit que a est un *diviseur de zéro* lorsque $a \neq 0$ et $\exists b \in \mathcal{A} \setminus \{0\}$, $ab = 0$. Un *anneau intègre* est un anneau sans diviseur de zéro.

Exemples Tout corps est un anneau intègre (en particulier, $\mathbb{C}$). Tout sous-anneau d'un anneau intègre est intègre. L'anneau $Z/n\mathbb{Z}$ est intègre si, et seulement si n est un nombre premier (et dans ce cas, $Z/n\mathbb{Z}$ est un corps). L'anneau $\mathcal{M}_n(\mathbb{C})$ est un anneau non commutatif et non intègre. L'anneau $\mathcal{C}(\mathbb{R}, \mathbb{R})$ des applications continues $\mathbb{R} \to \mathbb{R}$ n'est pas intègre. L'anneau $\mathbb{Z}/8\mathbb{Z}[X]$ n'est pas intègre.

Exercice 9 Soient P et Q deux polynômes non nuls. Si le coefficient dominant de P n'est pas un diviseur de zéro, alors $PQ \neq 0$ et $\deg(PQ) = \deg(P) + \deg(Q)$. En particulier, si $\mathcal{A}$ est un anneau intègre, cette égalité est toujours vraie.

Proposition *Soit $\mathcal{A}$ un anneau. Si $\mathcal{A}$ est intègre, alors $\mathcal{A}[X]$ est intègre.*

Preuve. Le produit de deux polynômes non nuls est non nul, puisque son coefficient dominant n'est pas 0. ■

2.3 Spécialisation, racines, fonction polynomiale, substitution

Définitions Soient $\mathcal{A}$ un anneau, $a \in \mathcal{A}$ et $P = \sum_{0\leq n\leq d} p_n X^n \in \mathcal{A}[X]$, où $d \in \mathbb{N}$. On note alors

$$P(a) = \sum_{0\leq n\leq d} p_n a^n.$$

Cet élément de $\mathcal{A}$ est la *spécialisation de P en a*. On dit que a est *racine de P* lorsque $P(a) = 0$. La fonction $\widetilde{P} : \mathcal{A} \to \mathcal{A}$, $x \mapsto P(x)$ est la *fonction polynomiale associée à P*.

Exercice 10 L'application $\mathcal{A}[X] \to \mathcal{F}(\mathcal{A}, \mathcal{A})$, $P \mapsto \widetilde{P}$ est un homomorphisme d'anneaux (d'algèbres si $\mathcal{A}$ est un corps).

Exercice 11 Faire dessiner par une machine des graphes de fonctions polynomiales $\mathbb{R} \to \mathbb{R}$ définies par des polynômes de degrés $0, 1, 2, 3, \ldots$

Exemple Si $P = X(X+1) \in \mathbb{Z}/2\mathbb{Z}[X]$, alors $\widetilde{P}$ est la fonction nulle $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. Cela montre que $P \mapsto \widetilde{P}$ n'est en général pas injectif.

Exemple Toute fonction polynomiale $\mathbb{R} \to \mathbb{R}$ non constante tend vers $\pm\infty$ en $+\infty$. On voit ainsi que la fonction sinus n'est pas polynomiale, puisqu'elle est bornée et non constante. Donc $P \mapsto \widetilde{P}$ n'est en général pas surjectif.

Théorème de substitution
Soient $\mathcal{A}$ et $\mathcal{B}$ des anneaux et $b \in \mathcal{B}$. Soit $g : \mathcal{A} \to \mathcal{B}$ un homomorphisme d'anneaux. Alors, il existe un unique homomorphisme d'anneaux $\overline{g} : \mathcal{A}[X] \to \mathcal{B}$ qui prolonge g et qui vérifie et $\overline{g}(X) = b$.

Preuve. (i) Unicité : si $\overline{g}$ existe, alors $\overline{g}\left(\sum a_n X^n\right) = \sum \overline{g}\left(a_n\right) b^n = \sum g\left(a_n\right) b^n$. (ii) Existence : il suffit de montrer que $\mathcal{A}[X] \to \mathcal{B}$, $\sum a_n X^n \mapsto \sum g\left(a_n\right) b^n$ est un homomorphisme d'anneaux. C'est facile (exercice). ■

Définition Dans les conditions du théorème, $\overline{g}$ est l'*homomorphisme de substitution* (de b à X, qui prolonge g à $\mathcal{A}[X]$).

Remarque Lorsque $g = \mathrm{id}_{\mathcal{A}}$, la substitution $\overline{g}$ est la spécialisation en b.

Notation Soient $\mathcal{A}$ un anneau, $Q \in \mathcal{A}[X]$ et $c_Q : \mathcal{A}[X] \to \mathcal{A}[X]$ l'homomorphisme de substitution qui prolonge l'inclusion $\mathcal{A} \to \mathcal{A}[X]$, $a \mapsto a$ et qui envoie X sur Q. Pour tout $P \in \mathcal{A}[X]$, on note $P \circ Q$ le polynôme $P \circ Q = c_Q(P) = P(Q(X))$.

Exercice 12 Montrer que si $P, Q \in \mathcal{A}[X]$, alors $\widetilde{P \circ Q} = \widetilde{P} \circ \widetilde{Q}$ (le premier symbole $\circ$ de l'égalité est le symbole de substitution qui vient d'être défini, le second est celui de la composition des applications).

2.4 Division euclidienne des polynômes

Définition Soient $\mathcal{A}$ un anneau et $a \in \mathcal{A}$. On dit que a est *inversible* lorsqu'il existe $b \in \mathcal{A}$ tel que $ab = 1$.

Exercice 13 Un inversible n'est jamais un diviseur de zéro.

Exercice 14 L'ensemble des éléments inversibles d'un anneau $\mathcal{A}$ est un groupe abélien pour la multiplication de l'anneau. On l'appelle le *groupe des unités de* $\mathcal{A}$ et on le note souvent $\mathcal{A}^\times$.

Exercice 15
(i) $\mathbb{Z}^\times = \{\pm 1\}$
(ii) Si $\mathcal{A}$ est un anneau intègre, $\mathcal{A}[X]^\times = \mathcal{A}^\times$ (les polynômes inversibles sont les polynômes constants inversibles).
(iii) Si $\mathcal{A}$ est un anneau quelconque et si $P = \sum_n a_n X^n \in \mathcal{A}[X]$, alors P est inversible dans $\mathcal{A}[X]$ si, et seulement si $a_0 \in \mathcal{A}^\times$ et $a_1, a_2, \ldots$ sont tous nilpotents (un élément a d'un anneau est dit *nilpotent* lorsqu'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$). Par exemple, dans $\mathbb{Z}/16\mathbb{Z}[X]$, $(1+2X)(1-2X+4X^2-8X^3) = 1$.
[Eléments de preuve. D'abord, $Q \in \mathcal{A}[X]$ est nilpotent si, et seulement si tous ses coefficients le sont. Le sens direct peut se faire par récurrence sur le degré de Q, en s'appuyant sur le fait que si $\deg Q \leq d-1$, alors $Q + aX^d$ est nilpotent si, et seulement si Q et a le sont (si $\left(Q + aX^d\right)^n = 0$, alors $a^n = 0$ et Q^n, qui est de la forme aR, est lui-même annulé par sa puissance n). Le sens réciproque est élémentaire. Ainsi, il suffit de montrer que $1 - XQ$ est inversible si, et seulement si Q est nilpotent, ce qui vient du fait que l'inverse, s'il existe, est nécessairement $\sum_{n \geq 0} X^n Q^n$. Pour voir cette nécessité, le plus simple est de passer par les séries formelles. Sinon, par récurrence sur n, on montre que si $1 - XQ$ est inversible dans $\mathcal{A}[X]$, pour tout n, il existe R_n tel que $(1-XQ)^{-1} = 1 + XQ + \cdots + X^n Q^n + X^{n+1} R_n$; alors, si $n \geq \deg(1-XQ)^{-1}$, cela impose que $R_n = 0$, c'est-à-dire que l'inverse de $1 - XQ$ égale $1 + XQ + \cdots + X^n Q^n$, ce qui entraîne que $Q^{n+1} = 0$.]

Théorème de division euclidienne des polynômes sur un corps
Soit $\mathbb{F}$ un corps. Soient $A, B \in \mathbb{F}[X]$. On suppose que $B \neq 0$. Alors, il existe un unique couple $(Q, R) \in \mathbb{F}[X]^2$ tel que

$$\begin{cases} A = BQ + R, \\ R = 0 \quad \text{ou} \quad \deg(R) \leq \deg(B) - 1. \end{cases}$$

Preuve. (i) Unicité. On suppose que $A = BQ + R = BQ' + R'$ avec les conditions sur les restes. Alors, $B(Q - Q') = R' - R$. Par l'absurde, on suppose que $R \neq R'$. Alors, d'une part, $\deg(R - R') \leq \deg B - 1$. D'autre part, $Q \neq Q'$ et $\deg(R - R') = \deg(B) + \deg(Q - Q') \geq \deg(B)$ puisque le coefficient dominant de B

est non nul donc inversible. L'hypothèse $R \neq R'$ ne tient pas. Donc $R = R'$, et par conséquent, à nouveau puisque le coefficient dominant de B est inversible, $Q = Q'$.
(ii) Existence : si $A = 0$, prendre $Q = R = 0$. On suppose que $A \neq 0$ et on procède par récurrence sur $d = \deg(A)$.
• Si $d = 0$, alors $A = a_0 \in \mathbb{F}$. Ou bien $\deg(B) = 0$. Alors, $B = b_0 \in \mathbb{F} \setminus \{0\}$ est inversible et $a_0 = b_0 \left(b_0^{-1} a_0\right) + 0$: prendre $Q = b_0^{-1} a_0$ et $R = 0$. Ou bien $\deg(B) \geq 1$ et $a_0 = B \times 0 + a_0$: prendre $Q = 0$ et $R = a_0$.
• On suppose $d \neq 0$. Ou bien $\deg B \geq d + 1$; alors, puisque $A = B \times 0 + A$, prendre $Q = 0$ et $R = A$. Ou bien, enfin, $\deg B \leq d$. On note $A = \sum_{k=0}^{d} a_k X^k$ et $B = \sum_{k=0}^{e} b_k X^k$ où $e = \deg B$. Comme $b_e \neq 0$, on peut diviser par b_e dans le corps $\mathbb{F}$. Soit alors, comme dans l'algorithme posé, $C = A - b_e^{-1} B a_d X^{d-e}$. Si $C = 0$, prendre $Q = b_e^{-1} B a_d X^{d-e}$ et $R = 0$. Si $C \neq 0$, par hypothèse de récurrence, soient $Q_1 \in \mathbb{F}[X]$ et $R \in \mathbb{F}[X]$ tels que $C = BQ_1 + R$ avec $R = 0$ ou $\deg R < \deg B$. Alors, $A = B\left(Q_1 + b_e^{-1} a_d X^{d-e}\right) + R$ et il suffit de prendre $Q = Q_1 + b_e^{-1} a_d X^{d-e}$. ■

Définitions Avec les notations du théorème, Q est le *quotient* et R le *reste de la division euclidienne de A par B*.

Remarque La preuve est une formalisation de l'algorithme de division euclidienne des entiers enseignée à l'Ecole élémentaire, dont le mécanisme s'applique à la division des polynômes à une indéterminée.

Exercice 16 Prendre des exemples simples de divisions euclidiennes de polynômes.

Théorème général de division euclidienne des polynômes
Soit $\mathcal{A}$ un anneau. Soient $A, B \in \mathcal{A}[X]$. On suppose que $B \neq 0$ et que le coefficient dominant de B est inversible. Alors, il existe un unique couple $(Q, R) \in \mathcal{A}[X]^2$ tel que

$$\begin{cases} A = BQ + R, \\ R = 0 \quad \text{ou} \quad \deg(R) \leq \deg(B) - 1. \end{cases}$$

PREUVE. Comme dans le cas des corps. ■

Définitions Soient $\mathcal{A}$ un anneau, $a, b \in \mathcal{A}$. On dit que a *divise* b lorsqu'il existe $c \in \mathcal{A}$ tel que $ac = b$. On note alors $a|b$. On dit aussi que a est un *diviseur de* b, ou que b *est un multiple* de a.

Exemple Dans $\mathbb{R}[X]$, $X^4+1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$ (le voir à partir de $X^4+1 = (X^2+1)^2 - 2X^2$). Ainsi, $X^2 - \sqrt{2}X + 1 | X^4 + 1$ dans $\mathbb{R}[X]$.

Proposition *Soient $\mathcal{A}$ un anneau, $a \in \mathcal{A}$ et $P \in \mathcal{A}[X]$. Alors, a est racine de P si, et seulement si $X - a$ divise P.*

PREUVE. On fait la division euclidienne de P par le polynôme unitaire $X - a$. Soient $Q \in \mathcal{A}[X]$ et $b \in \mathcal{A}$ tels que $P = (X - a)Q + b$. En spécialisant, nécessairement, $b = P(a)$. Cela conduit au résultat. ■

Corollaire *Soient $\mathcal{A}$ un anneau intègre, $P \in \mathcal{A}[X]$ et $a_1, \ldots, a_d \in \mathcal{A}$, distincts. Alors, $a_1, \ldots, a_d$ sont des racines de P si, et seulement si $\prod_{k=1}^{d}(X - a_k)$ divise P.*

PREUVE. Par récurrence sur d. Si $d = 1$, c'est la proposition précédente. Si $d \geq 2$, puisque a_d est racine, soit $Q \in \mathcal{A}[X]$ tel que $P = (X - a_d)Q$. Puisque $\mathcal{A}$ est intègre, $a_1, \ldots, a_{d-1}$ sont des racines distinctes de Q à qui on applique l'hypothèse de récurrence. ■

Exemple Sur $\mathbb{Z}/4\mathbb{Z}$ qui n'est pas intègre, 0 et 2 sont racines de X^2. Pourtant, X^2 n'est pas multiple de $X(X - 2)$.

Exercice 17 Pourquoi $X(X - 2)$ ne divise-t-il pas X^2 dans $\mathbb{Z}/4\mathbb{Z}[X]$ comme on l'affirme ci-dessus ?

Exemple Si p est un nombre premier

$$X^p - X = \prod_{k=0}^{p-1}(X - k) \text{ dans } \mathbb{Z}/p\mathbb{Z}.$$

[Noter que ce polynôme non nul définit une fonction polynomiale nulle sur $\mathbb{Z}/p\mathbb{Z}$.]

Preuve de cette égalité : le polynôme $P = X^p - X$ vérifie $P(0) = 0$ et $P(X - 1) = P(X)$, grâce au théorème de Gauss sur les entiers qui assure que, puisque p est premier, p divise les coefficients du binôme $\binom{p}{k}$, $1 \leq k \leq p-1$.

Ainsi, P a-t-il pour racines tous les éléments de $\mathbb{Z}/p\mathbb{Z}$. Donc, d'après le corollaire ci-dessus, $\prod_{k=0}^{p-1}(X-k)|P$, puisque $\mathbb{Z}/p\mathbb{Z}$ est intègre. Par conséquent, comme les polynômes $\prod_{k=0}^{p-1}(X-k)$ et P sont unitaires et de même degré, ils sont égaux.

N.B. En considérant le coefficient de X dans cette égalité, on obtient que $(p-1)! = -1$ $[p]$: c'est le théorème de Wilson.

Théorème de prolongement analytique pour les polynômes
Soient $\mathcal{A}$ un anneau intègre *et $P \in \mathcal{A}[X]$.*

(i) Si $P \neq 0$, alors P a au plus $\deg(P)$ *racines.*

(ii) Si P a une infinité de racines, alors $P = 0$.

(iii) Si $\mathcal{A}$ est infini et si $P(x) = 0$ pour tout $x \in \mathcal{A}$, alors $P = 0$.

Preuve. Il suffit de montrer (i), les points (ii) et (iii) en sont des conséquences directes. On procède par récurrence sur $d = \deg(P)$. Si $d = 0$, alors P n'a pas de racine (rien à dire). On suppose $d \geq 1$. Si P n'a pas de racine, il n'y a rien à faire ; sinon, soit $a \in \mathcal{A}$ tel que $P(a) = 0$. Soit alors $Q \in \mathcal{A}[X]$ tel que $P = (X-a)Q$. Comme $\mathcal{A}$ est intègre, $x \in \mathcal{A}$ est racine de P si, et seulement si $x = a$ ou x est racine de Q. Or, par hypothèse de récurrence, Q a au plus $d-1$ racines. Donc P a au plus d racines. ■

Exercice 18 Montrer que l'homomorphisme d'anneaux $\mathbb{R}[X] \to \mathcal{F}(\mathbb{R},\mathbb{R})$, $P \mapsto \widetilde{P}$ est injectif. Par quel anneau peut-on remplacer $\mathbb{R}$ pour que cette assertion reste vraie ?

2.5 Polynômes à plusieurs indéterminées

Définition Soit $\mathcal{A}$ un anneau. On note $\mathcal{A}[X,Y]$ l'anneau $(\mathcal{A}[X])[Y]$ qui est l'anneau des polynômes (à une indéterminée) à coefficients dans l'anneau $\mathcal{A}[X]$. C'est l'*anneau des polynômes à 2 indéterminées à coefficients dans $\mathcal{A}$.*

Notation Soit $Q = \sum_{n\geq 0} P_n(X)Y^n$, où $P_n = \sum_{m\geq 0} a_{m,n}X^m \in \mathcal{A}[X]$. Alors, $Q = \sum_{m,n\geq 0} a_{m,n}X^mY^n$, la famille $(a_{m,n})_{m,n\geq 0}$ n'ayant qu'un ensemble fini de termes non nuls – on dit encore qu'elle est *presque nulle.*

Remarque Le nom des indéterminées X et Y n'a pas d'importance : $\mathcal{A}[X,Y] = \mathcal{A}[Y,X] = \mathcal{A}[s,t]$ (ces anneaux ne sont pas seulement isomorphes, ils sont égaux).

Exercice 19 Si $\mathbb{F}$ est un corps, la famille $(X^mY^n)_{m,n\geq 0}$ (ordonnée comme on veut) est une base du $\mathbb{F}$-espace vectoriel $\mathbb{F}[X,Y]$.

Définition Soit $\mathcal{A}$ un anneau. Par récurrence sur $n \in \mathbb{N}^*$, on définit

$$\mathcal{A}[X_1,\ldots,X_n] = \mathcal{A}[X_1,\ldots,X_{n-1}][X_n],$$

anneau des polynômes à n indéterminées à coefficients dans $\mathcal{A}$.

Les règles de calcul relatives à l'addition, la soustraction et la multiplication dans $\mathcal{A}[X_1,\ldots,X_n]$ se font comme si les X_j étaient des éléments de $\mathcal{A}$.

Notation Si $i = (i_1,\ldots,i_n) \in \mathbb{N}^n$, on note

$$X^i = X_1^{i_1}X_2^{i_2}\ldots X_n^{i_n}$$

Exercice 20 Tout élément de $\mathcal{A}[X_1,\ldots,X_n]$ s'écrit de manière unique sous la forme $\sum_{i\in\mathbb{N}^n} a_iX^i$ où $(a_i)_{i\in\mathbb{N}^n}$ est une famille presque nulle d'éléments de $\mathcal{A}$.

Définition Tout polynôme de la forme a_iX^i où $i \in \mathbb{N}^n$ et $a_i \in \mathcal{A}$ est un *monôme* de $\mathcal{A}[X_1,\ldots,X_n]$.

Définition Soient $a \in \mathcal{A}\setminus\{0\}$ et $i = (i_1,\ldots,i_n) \in \mathbb{N}^n$. Le *degré* du monôme a_iX^i est $\deg\left(a_iX^i\right) = |i| = i_1+\cdots+i_n$. Le degré (total) d'un polynôme non nul est le degré de son monôme de plus haut degré :

$$\deg\left(\sum_{i\in\mathbb{N}^n} a_iX^i\right) = \max\{|i|,\ a_i \neq 0\}.$$

Exercice 21

(i) Si P et Q sont des polynômes à n indéterminées tels que ni P, ni Q, ni $P+Q$, ni PQ ne soient nuls, alors $\deg(P+Q) \leq \max\{\deg P, \deg Q\}$ et $\deg(PQ) \leq \deg P + \deg Q$.

(ii) Si $\mathcal{A}$ est intègre, alors $\mathcal{A}[X_1, \ldots, X_n]$ est intègre.

Définition Si $P \in \mathcal{A}[X_1, \ldots, X_n]$ est non nul et si $j \in \{1, \ldots, n\}$, le *degré partiel* de P par rapport à X_j est le degré de P vu dans $\mathcal{A}[X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n][X_j]$.

Autrement dit, si $P = \sum_{k \geq 0} P_k \left(X_1, \ldots, \widehat{X_j}, \ldots, X_n\right) X^k$, alors $\deg_{X_j}(P) = \max\{i,\ P_i \neq 0\}$. Dans cette formule, le chapeau signifie qu'on oublie l'indéterminée X_j.

Théorème de substitution (n variables)
Soient $\mathcal{A}$ et $\mathcal{B}$ des anneaux, $b_1, \ldots, b_n \in \mathcal{B}$ et $g : \mathcal{A} \to \mathcal{B}$ un homomorphisme d'anneaux. Alors, il existe un unique homomorphisme d'anneaux $\overline{g} : \mathcal{A}[X_1, \ldots, X_n] \to \mathcal{B}$ qui prolonge g et que vérifie $\overline{g}(X_j) = b_j$ pour tout j.

PREUVE. Par récurrence sur n avec le théorème de substitution à une indéterminée. ■

Ce prolongement est le suivant : $\overline{g}\left(\sum_{i \in \mathbb{N}^n} a_i X^i\right) = \sum_{i \in \mathbb{N}^n} g(a_i)\, b_1^{i_1} \ldots b_n^{i_n}$.

Dans le cas où $\mathcal{A}$ est un sous-anneau de $\mathcal{B}$ et g l'inclusion, on note $\overline{g}(P) = P(b_1, \ldots, b_n)$. Dans ces condtions, $\overline{g}$ est l'homomorphisme de *substitution* des b_j aux indéterminées.

Si $\mathcal{B} = \mathcal{A}$ et si g est l'identité, $P(a_1, \ldots, a_n) \in \mathcal{A}$ est la *spécialisation* de P en les a_j.

Définitions Soient $\mathcal{A}$ un anneau, $P \in \mathcal{A}[X_1, \ldots, X_n]$

(i) L'application $\widetilde{P} : \mathcal{A}^n \to \mathcal{A}$, $(x_1, \ldots, x_n) \mapsto P(x_1, \ldots, x_n)$ est la *fonction polynomiale* associée à P.

(ii) Si $(a_1, \ldots, a_n) \in \mathcal{A}^n$ vérifie $P(a_1, \ldots, a_n) = 0$, on dit que $(a_1, \ldots, a_n)$ est une *racine* de P.

Exercice 22 L'application $\mathcal{A}[X_1, \ldots, X_n] \to \mathcal{F}(\mathcal{A}^n, \mathcal{A})$, $P \mapsto \widetilde{P}$ est un homomorphisme d'anneaux. Il n'est en général ni injectif, ni surjectif (donner des exemples).

Théorème de prolongement analytique pour les polynômes (n indéterminées)
Soient $\mathcal{A}$ un anneau intègre *et $P \in \mathcal{A}[X_1, \ldots, X_n]$. Pour chaque $j \in \{1, \ldots, n\}$, soit $E_j \subseteq \mathcal{A}$ tel que*
(i) $\mathrm{Card}(E_j) \geq 1 + \deg_{X_j}(P)$
(ii) $\forall (x_1, \ldots, x_n) \in E_1 \times \cdots \times E_n$, $P(x_1, \ldots, x_n) = 0$.
Alors, $P = 0$.

PREUVE. Par récurrence sur n. Si $n = 1$, c'est déjà vu. On suppose $n \geq 2$. Pour tout $(a_1, \ldots, a_{n-1}) \in E_1 \times \cdots \times E_{n-1}$, le polynôme $P(a_1, \ldots, a_{n-1}, X) \in \mathcal{A}[X]$, s'il était non nul, aurait strictement plus de racines que son degré puisqu'il s'annule sur E_n. Donc il est nul. Alors, comme $\mathcal{A}[X_n]$ est intègre, on applique l'hypothèse de récurrence à $P \in \mathcal{A}[X_n][X_1, \ldots, X_{n-1}]$ qui s'annule sur $E_1 \times \cdots \times E_{n-1}$ avec les mêmes conditions de degrés. Donc $P = 0$. ■

Corollaire *Si $\mathcal{A}$ est infini et intègre et si $\forall a \in \mathcal{A}^n$, $P(a) = 0$, alors $P = 0$.*

PREUVE. Exercice. ■

Exercice 23 Donner des conditions suffisantes pour que $P \mapsto \widetilde{P}$ soit injectif. Même question pour surjectif.

3 Théorème de Bézout dans $\mathbb{Z}$ et $\mathbb{F}[X]$, anneaux principaux

3.1 Idéaux et sous-anneaux engendrés

Proposition *Si $\mathcal{A}$ est un anneau et si $(\mathcal{B}_i)_{i\in I}$ est une famille de sous-anneaux de $\mathcal{A}$, alors $\bigcap_{i\in I}\mathcal{B}_i$ est un sous-anneau de $\mathcal{A}$.*

Preuve. D'abord, $1\in\bigcap_{i\in I}\mathcal{B}_i$ puisque $1\in\mathcal{B}_i$ pour tout $i\in I$. Ensuite, soient $x,y\in\bigcap_{i\in I}\mathcal{B}_i$ et $i\in I$. Alors, $x,y\in\mathcal{B}_i$. Puisque $\mathcal{B}_i$ est un sous-anneau de $\mathcal{A}$, $x-y$ et xy sont aussi dans $\mathcal{B}_i$. Comme cela est vrai pour tout $i\in I$, il en résulte que $x-y$ et xy sont dans $\bigcap_{i\in I}\mathcal{B}_i$. ■

Définition Si $\mathcal{A}$ est un anneau et si E est une partie de $\mathcal{A}$, le *sous-anneau de $\mathcal{A}$ engendré par E* est l'intersection des sous-anneaux de $\mathcal{A}$ contenant E. On le note $\langle E\rangle$.

Proposition *Soit $\mathcal{A}$ un anneau E une partie de $\mathcal{A}$. Alors, le sous-anneau engendré $\langle E\rangle$ est le plus petit sous-anneau de $\mathcal{A}$ contenant E au sens de l'inclusion,* i.e. *si $\mathcal{B}$ est un sous-anneau de $\mathcal{A}$, alors $E\subseteq\mathcal{B}\Longrightarrow\langle E\rangle\subseteq\mathcal{B}$.*

Preuve. D'abord, $\langle E\rangle$ est un sous-anneau de $\mathcal{A}$ grâce à la proposition précédente. Si $\mathcal{B}$ est un sous-anneau de $\mathcal{A}$ contenant E, il contient (évidemment) l'intersection de tous les sous-anneaux de $\mathcal{A}$ contenant E, c'est-à-dire $\langle E\rangle$. ■

Proposition (caractérisation des sous-anneaux engendrés)
Soient $\mathcal{B}$ un anneau, $b_1,\ldots,b_n\in\mathcal{B}$ et $\mathcal{A}$ un sous-anneau de $\mathcal{B}$. Alors, le sous-anneau de $\mathcal{B}$ engendré par $\mathcal{A}\cup\{b_1,\ldots,b_n\}$ est $\{P(b_1,\ldots,b_n),\ P\in\mathcal{A}[X_1,\ldots,X_n]\}$.

Preuve. On montre d'abord que $\mathcal{E}=\{P(b_1,\ldots,b_n),\ P\in\mathcal{A}[X_1,\ldots,X_n]\}$ est un sous-anneau de $\mathcal{B}$. Il contient $\mathcal{A}$ (prendre pour P des polynômes constants) et les b_k (prendre pour P les indéterminées X_k) ; donc il contient $\langle\mathcal{A}\cup\{b_1,\ldots,b_n\}\rangle$. Enfin, puisque $\langle\mathcal{A}\cup\{b_1,\ldots,b_n\}\rangle$ est un sous-anneau de $\mathcal{A}$, il est stable pour l'addition et la multiplication, et contient $\mathcal{A}$ et les b_k ; donc il contient $\mathcal{E}$ (pour fabriquer un élément de $\mathcal{E}$, on part de $\mathcal{A}$ et des b_k et on effectue des additions et des multiplications). ■

Exercice 24 Détailler la preuve ci-dessus.

Notation (dangereuse) Dans ces conditions, on note $\langle\mathcal{A}\cup\{b_1,\ldots,b_n\}\rangle=\mathcal{A}[b_1,\ldots,b_n]$.

Exemples de sous-anneaux de $\mathbb{C}$
(i) $\mathbb{Z}[i]=\{a+bi,\ a,b\in\mathbb{Z}\}$
(ii) $\mathbb{Q}[\sqrt{2}]=\left\{a+b\sqrt{2},\ a,b\in\mathbb{Q}\right\}$
(iii) $\mathbb{Z}[\sqrt{2},\sqrt{3}]=\left\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6},\ a,b,c,d\in\mathbb{Z}\right\}$
(iv) $\mathbb{Z}[\omega]=\{a+b\omega,\ a,b\in\mathbb{Z}\}$ si $\omega\in\mathbb{C}$ vérifie une équation du type $\omega^2+\alpha\omega+\beta=0$ où α et β sont entiers
(v) $\mathbb{Q}[\sqrt[4]{3}]=\left\{a+b\sqrt[4]{3}+c\left(\sqrt[4]{3}\right)^2+d\left(\sqrt[4]{3}\right)^3,\ a,b,c,d\in\mathbb{Q}\right\}$

Exercice 25 Prouver toutes les égalités des exemples (i) à (v) ci-dessus.

Définition Soit $\mathcal{A}$ un anneau. Un *idéal* de $\mathcal{A}$ est une partie I de $\mathcal{A}$ qui soit un sous-groupe pour l'addition et qui vérifie $\mathcal{A}I\subseteq I$, *i.e.* $\forall a\in\mathcal{A}$, $\forall x\in I$, $xa\in I$ (voir le document *Structures abstraites*).

Exemples
(i) Les idéaux un peu stupides : l'idéal nul $\{0\}$, l'idéal plein $\mathcal{A}$.
(ii) Si $a\in\mathcal{A}$, l'ensemble $a\mathcal{A}$ de ses multiples est un idéal de $\mathcal{A}$.
(iii) Les idéaux d'annulation d'un homomorphisme de substitution. Par exemple, $\left\{P\in\mathbb{Q}[X],\ P\left(\sqrt{2}\right)=0\right\}$, ou $\{P\in\mathbb{Z}[X],\ P(M)=O_3\}$ où M est une matrice de $\mathcal{M}_3(\mathbb{Z})$, ou encore $\{f\in\mathcal{F}(\mathbb{R},\mathbb{R}),\ \forall x\in[0,1],\ f(x)=0\}$.

Exercice 26 Prouver toutes les assertions des exemples (i) à (iii) ci-dessus.

Proposition *Si $\mathcal{A}$ est un anneau et si $(I_j)_{j\in J}$ est une famille d'idéaux de $\mathcal{A}$, alors $\bigcap_{j\in J}I_i$ est un idéal de $\mathcal{A}$.*

Preuve. Exercice. ■

Définition Si $\mathcal{A}$ est un anneau et si E est une partie de $\mathcal{A}$, l'*idéal de $\mathcal{A}$ engendré par E* est l'intersection des idéaux de $\mathcal{A}$ contenant E. On le note (E).

Proposition *Soit $\mathcal{A}$ un anneau E une partie de $\mathcal{A}$. Alors, l'idéal engendré (E) est le plus petit idéal de $\mathcal{A}$ contenant E au sens de l'inclusion,* i.e. *si I est un idéal de $\mathcal{A}$, alors $E \subseteq I \Longrightarrow (E) \subseteq I$.*

PREUVE. Exercice. ■

Proposition (caractérisation des idéaux engendrés)
Soit $\mathcal{A}$ un anneau et $x_1, \ldots, x_n$ des éléments de $\mathcal{A}$. Alors, l'idéal de $\mathcal{A}$ engendré par $\{x_1, \ldots, x_n\}$ est $(\{x_1, \ldots, x_n\}) = \mathcal{A}x_1 + \cdots + \mathcal{A}x_n = \{a_1x_1 + \cdots + a_nx_n,\ \forall k \in \{1, \ldots, n\},\ a_k \in \mathcal{A}\}$.

PREUVE. Le schéma de la preuve copie celui de l'énoncé jumeau pour les sous-anneaux engendrés : on montre que $\mathcal{A}x_1 + \cdots + \mathcal{A}x_n$ est un idéal de $\mathcal{A}$ qui contient $(\{x_1, \ldots, x_n\})$ et qui est également contenu dedans. ■

Exercice 27 Détailler les arguments de la preuve ci-dessus.

Notation Dans ces conditions, on note $(\{x_1, \ldots, x_n\}) = (x_1, \ldots, x_n)$.

Exemples
(i) Soit I un idéal d'un anneau $\mathcal{A}$. Alors, $I = \mathcal{A}$ si, et seulement si $1 \in I$.
(ii) Si $a \in \mathbb{Z}$, l'idéal de $\mathbb{Z}$ engendré par a est l'ensemble $a\mathbb{Z}$ des multiples de a.
(iii) Soit $\mathcal{A}$ un anneau, $a, b \in \mathcal{A}$. Alors, $(a) \subseteq (b)$ si, et seulement si b divise a.

Exercice 28 Prouver les trois assertions des exemples ci-dessus.

3.2 Principalité de $\mathbb{Z}$ et $\mathbb{F}[X]$

Définition Soient $\mathcal{A}$ un anneau et I un idéal de $\mathcal{A}$. On dit que I est *un idéal principal* lorsqu'il existe $a \in \mathcal{A}$ tel que $I = (a)$. On dit que $\mathcal{A}$ est *un anneau principal* lorsqu'il est intègre et lorsque tous ses idéaux sont principaux.

Exemple important L'idéal $(2, X)$ de l'anneau $\mathbb{Z}[X]$ n'est pas principal. En particulier, l'anneau $\mathbb{Z}[X]$ n'est pas principal.

PREUVE. Supposons que $(2, X) = (P)$ où $P \in \mathbb{Z}[X]$. D'abord, 2 est multiple de P. Donc P est un polynôme constant puisque $\mathbb{Z}$ est intègre (degrés). Par ailleurs, X est multiple de P. En regardant les coefficients dominants, on obtient que $P = \pm 1$. Donc $(2, X) = (1) = \mathbb{Z}[X]$. Soient alors $Q, R \in \mathbb{Z}[X]$ tels que $1 = 2Q + XR$. En spécialisant, on obtient que $1 = 2Q(0)$ ce qui est impossible dans $\mathbb{Z}$. L'hypothèse $(2, X) = (P)$ ne tient pas. ■

Théorème
(i) L'anneau $\mathbb{Z}$ est principal.
(ii) Si $\mathbb{F}$ est un corps, l'anneau $\mathbb{F}[X]$ est principal.

PREUVE. [Cette preuve est à retenir. La division euclidienne en est l'ingrédient principal.] (i) Soit I un idéal de $\mathbb{Z}$. Si $I = \{0\}$, alors $I = (0)$ est principal. Sinon, $I_+ = \{|x|,\ x \in I,\ x \neq 0\}$ est une partie non vide de $\mathbb{N}$. Soit alors $b \in I$ tel que $|b| = \min I_+$ (b existe puisque toute partie non vide de $\mathbb{N}$ admet un minimum). On montre alors que $I = (b)$. D'abord, $b \in I$ et I est un idéal ; donc $(b) \subseteq I$. Inversement, soit $x \in I$. On fait la division euclidienne de x par b : soient q et r dans $\mathbb{Z}$ tels que $x = bq + r$ et $0 \leq r \leq |b| - 1$. Alors, $r = x - bq \in I$ et $r \geq 0$. Donc $r = 0$ ou $r \in I_+$. Mais puisque $r \leq |b| - 1$, la minimalité de $|b|$ interdit que $r \in I_+$. Donc $r = 0$ et parz conséquent, $x = bq \in b\mathbb{Z}$. On a montré que $I \subseteq (b)$.
(ii) Preuve similaire, en utilisant la division euclidienne des polynômes à coefficients dans un corps. ■

Exercice 29 Ecrire soigneusement une preuve de (ii).

Exemple d'application Soient E un $\mathbb{F}$-espace vectoriel de dimension finie et $u \in \mathrm{End}(E)$. L'ensemble $\{P \in \mathbb{F}[X],\ P(u) = 0\}$ est un idéal de $\mathbb{F}[X]$ – on a noté 0 l'endomorphisme nul. Il existe donc un unique polynôme unitaire $\mu_u \in \mathbb{F}[X]$ tel que $\{P \in \mathbb{F}[X],\ P(u) = 0\} = (\mu_u)$. Ce polynôme est le *polynôme minimal* de u. Il vérifie : pour tout $P \in \mathbb{F}[X]$, si $P(u) = 0$, alors μ_u divise P.

3.3 PGCD, PPCM, théorème de Bézout, anneaux principaux

Définitions Soient $\mathcal{A}$ un anneau, $a, b \in \mathcal{A}$.

• Lorsqu'il existe, *un PGCD* (*plus grand diviseur commun*) de a et b est un $d \in \mathcal{A}$ qui vérifie

(i) $d|a$ et $d|b$

(ii) $\forall x \in \mathcal{A}$, $\big(x|a \text{ et } x|b\big) \Longrightarrow x|d$

• Lorsqu'il existe, *un PPCM* (*plus petit multiple commun*) de a et b est un $m \in \mathcal{A}$ qui vérifie

(i) $a|m$ et $b|m$

(ii) $\forall x \in \mathcal{A}$, $\big(a|x \text{ et } b|x\big) \Longrightarrow m|x$.

Remarque Ces définitions s'étendent aux PGCD et PPCM d'une partie finie $\{a_1, \ldots, a_n\}$ de $\mathcal{A}$.

Théorème de Bézout Soient $\mathcal{A}$ un anneau principal, $a, b \in \mathcal{A}$.

(i) a et b admettent des PGCD, qui sont exactement les générateurs de l'idéal $(a, b) = a\mathcal{A} + b\mathcal{A}$.

(ii) a et b admettent des PPCM, qui sont exactement les générateurs de l'idéal $(a) \cap (b)$.

Preuve. (i) Soit d un générateur de (a, b). Alors, d est un PGCD de a et b. (ii) Soit m un générateur de $(a) \cap (b)$. Alors, m est un PPCM de a et b. ■

Exercice 30 Ecrire les détails de cette preuve du théorème de Bézout.

Définition Dans un anneau $\mathcal{A}$, deux éléments a et b sont *associés* lorsqu'il existe $u \in \mathcal{A}^\times$ tel que $b = au$.

Exercice 31 La relation binaire sur un anneau $\mathcal{A}$ définie par $\big(a \sim b\big) \Longleftrightarrow \big(a \text{ et } b \text{ sont associés}\big)$ est une relation d'équivalence. La classe de 1 est le groupe $\mathcal{A}^\times$ des inversibles de $\mathcal{A}$.

Proposition *Soient $\mathcal{A}$ un anneau intègre, $a, b \in \mathcal{A}$. Alors, $(a) = (b)$ si, et seulement si a et b sont associés.*

Preuve. Si a ou b vaut 0, c'est évident puisque $(0) = \{0\}$ (indépendamment de l'intégrité de $\mathcal{A}$). On suppose donc que a et b sont non nuls. On suppose que $(a) = (b)$. Alors, $a \in (b)$: soit $u \in \mathcal{A}$ tel que $a = ub$. De manière analogue, puisque $b \in (a)$, soit $v \in \mathcal{A}$ tel que $b = va$. Alors, $a = uva$, ce qui s'écrit encore $a(1 - uv) = 0$. Puisque $\mathcal{A}$ est intègre et $a \neq 0$, cela entraîne que $uv = 1$, et donc que u est inversible. Réciproquement, si $a = ub$ où u est inversible, alors $b = u^{-1}a$. On a simultanément $(a) \subseteq (b)$ et $(b) \subseteq (a)$, ce qui entraîne que $(a) = (b)$. ■

Une paraphrase du théorème de Bézout : *dans un anneau principal, les PGCD (*resp. *les PPCM) existent toujours et sont tous associés.*

A noter Dans la liste d'exercices numéro 5, on trouvera un exemple d'anneau (non intègre) contenant deux élements non associés qui engendrent le même idéal.

Définition Dans $\mathbb{Z}$, ***le*** PGCD (*resp.* ***le*** PPCM) de deux entiers est l'unique PGCD (*resp.* PPCM) qui soit positif ou nul. Dans $\mathbb{F}[X]$, ***le*** PGCD (*resp.* ***le*** PPCM) de deux polynômes est l'unique PGCD (*resp.* PPCM) qui soit nul ou unitaire.

Définition Dans un anneau, deux éléments sont dits *étrangers* ou *premiers entre eux* lorsqu'ils admettent un PGCD qui soit inversible.

Théorème (relation de Bézout dans les anneaux principaux) *Soit $\mathcal{A}$ un anneau principal, $a, b \in \mathcal{A}$. Alors, a et b sont premiers entre eux si, et seulement s'il existe $u, v \in \mathcal{A}$ tels que $1 = au + bv$.*

Exercice 32 Prouver ce théorème à la lumière des résultats précédents.

Pour mémoire Dans $\mathbb{Z}$ ou dans $\mathbb{F}[X]$, les PGCD se calculent avec l'algorithme d'Euclide.

Exercice 33 Soit $\mathcal{A}$ un anneau intègre. Alors, $\mathcal{A}[X]$ est principal si, et seulement si $\mathcal{A}$ est un corps.

Exercice 34 Soient A un anneau, $a, b, d, m \in \mathcal{A}$. Montrer que

$$(a) \cap (b) = (m) \Longleftrightarrow m \text{ est un PPCM de } a \text{ et } b.$$

Montrer que

$$(a, b) = (d) \Longrightarrow d \text{ est un PGCD de } a \text{ et } b$$

et que la réciproque est fausse (voir les exercices de TD sur ce sujet).

4 Théorème de Gauss dans $\mathbb{Z}$ et $\mathbb{F}[X]$, anneaux factoriels

4.1 Factorialité de $\mathbb{Z}$ et de $\mathbb{F}[X]$

Définition Soient $\mathcal{A}$ un anneau et $a \in \mathcal{A}$. On dit que a est *irréductible* lorsque
(i) $a \notin \mathcal{A}^\times$;
(ii) $\forall b, c \in \mathcal{A}$, $\big(a = bc\big) \Longrightarrow \big(b \in \mathcal{A}^\times \text{ ou } c \in \mathcal{A}^\times\big)$.
Dans $\mathbb{Z}$, un *nombre premier* est un irréductible positif.

Exemple Le polynôme $2X$ est irréductible dans $\mathbb{Q}[X]$, mais pas dans $\mathbb{Z}[X]$.

Exercice 35 Tout associé d'un irréductible est encore irréductible.

Proposition
(i) Les irréductibles de $\mathbb{Z}$ sont les $\pm p$ où p est un nombre premier.
(ii) Si $\mathbb{F}$ est un corps, les irréductibles de $\mathbb{F}[X]$ sont les aP où $a \in \mathbb{F} \setminus \{0\}$ et où P est irréductible et unitaire.

Preuve. On a déjà caractérisé la liste des inversibles des anneaux $\mathbb{Z}$ et $\mathbb{F}[X]$, en exercice au début de la section 2.4. La proposition en résulte directement. ■

Exercice 36 Détailler la preuve de cette proposition.

Théorème (Factorialité de $\mathbb{Z}$)
Pour tout $x \in \mathbb{Z} \setminus \{0\}$, il existe un unique ensemble fini $\{(p_1, \alpha_1), \dots, (p_r, \alpha_r)\}$ où les p_k sont des nombres premiers distincts et les α_k des entiers naturels non nuls, tel que $x = \pm \prod_{k=1}^r p_k^{\alpha_k}$.

Preuve. Déjà connu. C'est une conséquence de la division euclidienne. On en refera une preuve juste dessous. ■

Vocabulaire Les p_k sont les *facteurs premiers* de x. L'unicité permet de noter $\alpha_k = v_{p_k}(x)$, *valuation p_k-adique* de x. On a ainsi la formule générale

$$x = \operatorname{sgn}(x) \prod_{p \in \mathcal{P}} p^{v_p(x)}$$

où $\mathcal{P}$ désigne l'ensemble des nombres premiers.

Exercice 37 Si x et y sont des entiers non nuls, x divise y si, et seulement si $v_p(x) \leq v_p(y)$ pour tout nombre premier p.

Théorème (Factorialité de $\mathbb{F}[X]$)
Soit $\mathbb{F}$ un corps. Pour tout $A \in \mathbb{F}[X] \setminus \{0\}$, il existe un unique $u \in \mathbb{F} \setminus \{0\}$ et un unique ensemble fini $\{(P_1, \alpha_1), \dots, (P_r, \alpha_r)\}$ où les P_k sont des polynômes irréductibles unitaires distincts et les α_k des entiers naturels non nuls, tel que $A = u \prod_{k=1}^r P_k^{\alpha_k}$.

Preuve. Résulte encore de la division euclidienne dans $\mathbb{F}[X]$, preuve semblable à celle de $\mathbb{Z}$. On en reverra un preuve. ■

Là encore, on note

$$A = u \prod_{\substack{P \text{ irréductible} \\ \text{et unitaire}}} P^{v_p(A)}.$$

La valuation P-adique $v_P(A)$ est aussi appelée *multiplicité* de P dans A.

4.2 Anneaux factoriels

Définition Un anneau $\mathcal{A}$ est dit *factoriel* lorsque
(i) $\mathcal{A}$ est intègre ;
(ii) (Existence d'une décomposition en produit d'irréductibles)
$\forall a \in \mathcal{A} \setminus \{0\}$, $\exists u \in \mathcal{A}^\times$, $\exists r \in \mathbb{N}$, $\exists (p_1, \dots, p_r) \in \mathcal{A}^r$ tels que les p_k soient irréductibles et $a = u \prod_{k=1}^r p_k$;
(iii) (Unicité d'une décomposition en produit d'irréductibles)

Pour tous $u, v \in \mathcal{A}^\times$, $p_1, \ldots, p_r, q_1, \ldots, q_s \in \mathcal{A}$, irréductibles, si $up_1 \ldots p_r = vq_1 \ldots q_s$, alors $r = s$ et $\forall k \in \{1, \ldots, r\}$, $\exists \ell \in \{1, \ldots, r\}$, p_k et q_ℓ sont associés.

Exemples $\mathbb{Z}$ et $\mathbb{F}[X]$ lorsque $\mathbb{F}$ est un corps, comme on vient de le voir. La factorialité de ces deux anneaux a été montrée à l'aide de la division euclidienne. On a le résultat plus général suivant.

Théorème *Tout anneau principal est factoriel.*

PREUVE. Soit $\mathcal{A}$ principal (donc intègre). (i) Existence d'une décomposition. Soit $\mathcal{E} = \{(x),\ x \in \mathcal{A} \setminus \{0\},\ x \text{ indécomposable}\}$. Par l'absurde, on suppose que $\mathcal{E} \neq \emptyset$. Alors, $\mathcal{E}$ contient un élément maximal (a) pour l'inclusion. [En effet, par l'absurde, sinon, soit $(a_1) \in \mathcal{E}$ et soit $(a_1) \subset (a_2) \subset \ldots$ une suite strictement croissante d'éléments de $\mathcal{E}$. Comme $\mathcal{A}$ est principal, soit $a \in \mathcal{A}$ tel que $(a) = \bigcup_{k \geq 1}(a_k)$. Puisque $a \in (a)$, soit $n \geq 1$ tel que $a \in (a_n)$. Alors, $(a) \subseteq (a_n) \subseteq (a)$; ainsi, $(a) \in \mathcal{E}$ et la suite des idéaux emboîtés est stationnaire, ce qui contredit sa croissance stricte.] Puisque $(a) \in \mathcal{E}$, a n'est pas irréductible. Soient $b, c \in \mathcal{A}$, non inversibles, tels que $a = bc$. Comme $(a) \subset (b)$ et $(a) \neq (b)$ (et *idem* pour c), la maximalité de (a) impose que (b) et (c) ne soient pas dans $\mathcal{E}$. Donc b et c sont décomposables. Donc a aussi, ce qui contredit $(a) \in \mathcal{E}$: l'hypothèse $\mathcal{E} \neq \emptyset$ ne tient pas.
(ii) Unicité d'une décomposition.

Lemme *Soient $\mathcal{A}$ un anneau principal, et $p, p_1, \ldots, p_r$ des irréductibles de $\mathcal{A}$. Alors, si $p | p_1 \ldots p_r$, alors il existe $k \in \{1, \ldots, r\}$ tel que p et p_k soient associés.*
[Preuve du lemme plus bas]

Avec le lemme, on fait une preuve par récurrence sur r de l'unicité.
H(r) : Pour tout $a = up_1 \ldots p_r \in \mathcal{A}$, si $a = vq_1 \ldots q_s$, alors $s = r$ et tout p_k est associé à un q_ℓ. Si $r = 1$, $a = up = vq_1 \ldots q_s$; avec le lemme, quitte à renuméroter, p est associé à q_1. En simplifiant par q_1, on obtient que $q_2 \ldots q_s$ est inversible, donc q_2 aussi, ce qui est impossible à moins que $s = 1$. On suppose $r \geq 2$ et $a = up_1 \ldots p_r = vq_1 \ldots q_s \in \mathcal{A}$. Alors, p_r divise $q_1 \ldots q_s$. Grâce au lemme, quitte à renuméroter, p_r est associé à q_s. En simplifiant ($\mathcal{A}$ est intègre), les produits $p_1 \ldots p_{r-1}$ et $q_1 \ldots q_{s-1}$ sont associés. Par récurrence, $r = s$ et chaque p_k est associé à un q_ℓ.

PREUVE DU LEMME Par récurrence sur r. Si $r = 1$, $p | p_1$ et p_1 est irréductible et p n'est pas inversible. Donc p et p_1 sont associés. On suppose que $r \geq 2$ et que $p | p_1 \ldots p_r$. Si p et p_r sont associés, c'est fini. Sinon, puisqu'ils sont irréductibles, leur PGCD est (1) puisqu'ils n'ont pas de diviseur commun non inversible. Soient u et v dans A tels que $1 = ap + bp_r$. Alors, $p_1 \ldots p_{r-1} = app_1 \ldots p_{r-1} + bp_1 \ldots p_r$. Donc p divise $p_1 \ldots p_{r-1}$; par récurrence, p est associé à un p_k, $1 \leq k \leq r-1$. ■

Exercice 38 La relation d'association est une relation d'équivalence sur l'anneau.

Définition Soit $\mathcal{A}$ un anneau. Une partie $\mathcal{I}$ de $\mathcal{A}$ est un *système de représentants d'irréductibles* de $\mathcal{A}$ (en abrégé, SRI) lorsque

$$\forall x \in \mathcal{A},\ x \text{ irréductible } \implies \exists! u \in \mathcal{A}^\times,\ \exists! y \in \mathcal{I},\ x = uy.$$

Autrement dit, lorsque tout élément irréductible de $\mathcal{A}$ est associé à un unique élément de $\mathcal{I}$.

Exemples Dans $\mathbb{Z}$, l'ensemble des nombres premiers, mais aussi l'ensemble des opposés des nombres premiers. Dans $\mathbb{F}[X]$, les polynômes irréductibles unitaires.

Proposition (caractérisation des anneaux factoriels) *Soit $\mathcal{A}$ un anneau intègre. Alors, $\mathcal{A}$ est factoriel si, et seulement si $\mathcal{A}$ contient un SRI $\mathcal{I}$ tel que pour tout $x \in \mathcal{A} \setminus \{0\}$, il existe un unique $u \in \mathcal{A}^\times$ et une unique famille presque nulle d'entiers $(v_p(x))_{p \in \mathcal{I}}$ tels que*

$$x = u \prod_{x \in \mathcal{I}} p^{v_p(x)}.$$

PREUVE. Exercice (utilisant, à vrai dire, l'axiome du choix qui assure, en toute généralité, l'existence d'un SRI). Cela équivaut aussi à l'existence et l'unicité d'une décomposition dans n'importe quel SRI. ■

Le nombre entier naturel $v_p(x)$ est la *valuation p-adique* de x dans $\mathcal{A}$ (elle est relative au SRI choisi).

Exemples
(i) $\mathbb{Z}$ et $\mathbb{F}[X]$ sont factoriels (si $\mathbb{F}$ est un corps), puisqu'ils sont principaux. On a déjà pointé cela plusieurs fois.

(ii) Soit $\mathcal{A} = \left\{a + ib\sqrt{5},\ a, b \in \mathbb{Z}\right\} = \mathbb{Z}[i\sqrt{5}]$ (exercice : montrer la dernière égalité), sous-anneau de $\mathbb{C}$. On montre ci-dessous que $\mathcal{A}$ n'est pas factoriel en montrant que $9 = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ sont deux factorisations distinctes de 9 en produits d'irréductibles.
⋆ $\mathcal{A}^\times = \{\pm 1\}$. [En effet, on montre que $a + ib\sqrt{5} \in \mathcal{A}^\times$ si, et seulement si $a^2 + 5b^2 = 1$ et on résout cette équation diophantienne.]
⋆ 3 est irréductible. [En effet, si $3 = xy$, alors $9 = |x|^2|y|^2$ où $|x|$ et $|y|$ sont entiers. Or,$|z|^2 \neq 3$ pour tout $z \in \mathcal{A}$ puisque l'équation diophantienne $a^2 + 5b^2 = 3$ n'a pas de solution entière. Donc x ou y est inversible.]
⋆ $2 \pm i\sqrt{5}$ est irréductible. [Même raisonnement puisque $|2 \pm i\sqrt{5}|^2 = 9$.]
⋆ Enfin, $2 \pm i\sqrt{5}$ et 3 ne sont pas associés.

Exercice 39 Détailler minutieusement tous les arguments de cet exemple.

4.3 Divisibilité dans les anneaux factoriels

Proposition *Soient $\mathcal{A}$ un anneau factoriel, $a, b \in \mathcal{A} \setminus \{0\}$, $\mathcal{I}$ un SRI de $\mathcal{A}$. Alors,*
(i) a divise b si, et seulement si $v_p(a) \leq v_p(b)$ pour tout $p \in \mathcal{I}$
(ii) a et b sont associés si, et seulement si $v_p(a) = v_p(b)$ pour tout $p \in \mathcal{I}$
(iii) si $a + b \neq 0$, alors $v_p(a + b) \geq \min\{v_p(a), v_p(b)\}$ pour tout $p \in \mathcal{I}$
(iv) $v_p(ab) = v_p(a) + v_p(b)$ pour tout $p \in \mathcal{I}$.

Preuve. Tout vient de l'unicité de la décomposition. ■

Exercice 40 Faire une preuve détaillée de cette proposition.

Exercice 41 Si $v_p(a) \neq v_p(b)$, alors $v_p(a + b) = \min\{v_p(a), v_p(b)\}$ (alors que $v_2(4 + 12) > \min\{v_2(4), v_2(12)\}$).

Proposition *Soient $\mathcal{A}$ un anneau factoriel, $a, b \in \mathcal{A} \setminus \{0\}$, $\mathcal{I}$ un SRI de $\mathcal{A}$. Alors,*
(i) a et b ont des PGCD qui sont les associés de $\prod_{p\in\mathcal{I}} p^{\min\{v_p(a),v_p(b)\}}$
(ii) a et b ont des PPCM qui sont les associés de $\prod_{p\in\mathcal{I}} p^{\max\{v_p(a),v_p(b)\}}$.

Preuve. Les produits écrits sont respectivement un PGCD et un PPCM. ■

Exercice 42 Faire une preuve détaillée de cette proposition.

Exercice 43 Dans un anneau factoriel, si d est un PGCD de a et b et si m en est un PPCM, alors ab et dm sont associés.

Théorème (lemme d'Euclide)
Soient $\mathcal{A}$ un anneau factoriel, $a, b, p \in \mathcal{A}$, p irréductible. Alors, $p|ab \Longrightarrow p|a$ ou $p|b$.

Preuve. $v_p(ab) = v_p(a) + v_p(b) \geq 1$. Donc $v_p(a) \geq 1$ ou $v_p(b) \geq 1$. ■

Théorème de Gauss
Soient $\mathcal{A}$ un anneau factoriel, $a, b, c \in \mathcal{A}$. Si a divise bc et si a et b sont étrangers, alors a divise c.

Preuve. Comme a et b sont étrangers, pour tout irréductible p, $v_p(a) = 0$ ou $v_p(b) = 0$. Si $a|bc$, pour tout p irréductible, $v_p(a) \leq v_p(b) + v_p(c)$, ce qui entraîne que $v_p(a) \leq v_p(c)$. ■

Exercice 44 Dans un anneau factoriel, si a et b sont premiers entre eux, si $a|c$ et si $b|c$, alors $ab|c$.

Exemple $3|12$ et $6|12$ mais 3×6 ne divise pas 12.

4.4 Théorème de transfert de Gauss

Théorème de transfert de Gauss
Si $\mathcal{A}$ est factoriel, alors $\mathcal{A}[X]$ est factoriel.

Preuve. Voir la feuille de TD numéro 8, ou le livre *Cours d'algèbre* de Daniel Perrin. ■

Corollaire *Si $\mathcal{A}$ est factoriel, $\mathcal{A}[X_1, \ldots, X_n]$ est factoriel pour tout $n \geq 1$.*

Preuve. Récurrence sur n. ■

Exercice 45 Détailler cette récurrence.

5 Anneaux-quotients

– Ce chapitre est un des chapitres majeurs de tout le cours –

5.1 Quotient d'un anneau par un idéal

Définition Soient $\mathcal{A}$ un anneau et I un idéal de $\mathcal{A}$. Pour tous $x, y \in \mathcal{A}$, on dit que x *égale* y *modulo* I lorsque $x - y \in I$. On note parfois $x = y\ [I]$. Cela définit une relation d'équivalence sur $\mathcal{A}$ (exercice). Si $x \in \mathcal{A}$, la classe de x pour cette relation, appelée *classe de* x *modulo* I est

$$\overline{x} = \{y \in \mathcal{A},\ x = y\ [I]\} = \{x + i,\ i \in I\} = x + I.$$

On note $\mathcal{A}/I$ l'ensemble quotient, *i.e.* l'ensemble des classes modulo I. Si $y \in \overline{x}$, on dit que y est un *représentant* de $\overline{x}$. Bien entendu, les classes modulo I forment une partition de $\mathcal{A}$.

L'anneau $\mathcal{A}/I$
Les applications $\mathcal{A}/I \times \mathcal{A}/I \to \mathcal{A}/I$, $(\overline{x}, \overline{y}) \mapsto \overline{x+y}$ et $\mathcal{A}/I \times \mathcal{A}/I \to \mathcal{A}/I$, $(\overline{x}, \overline{y}) \mapsto \overline{xy}$ ont un sens. En effet, si $x = x'\ [I]$ et $y = y'\ [I]$, alors $(x+y) - (x'+y') \in I$ et $(xy - x'y') = x(y-y') + (x-x')y' \in I$. Ces applications définissent des lois de compositions internes sur $\mathcal{A}/I$ *via* les formules

$$\overline{x} + \overline{y} = \overline{x+y} \quad \text{et} \quad \overline{x} \times \overline{y} = \overline{x \times y}.$$

Proposition *Soient $\mathcal{A}$ un anneau et I un idéal de $\mathcal{A}$, différent de $\mathcal{A}$. Alors $(\mathcal{A}/I, +, \times)$ est un anneau commutatif. Son zéro est $\overline{0}$, son unité est $\overline{1}$. Si $x \in \mathcal{A}$, alors l'opposé de $\overline{x}$ est $-\overline{x} = \overline{-x}$. Si $x \in \mathcal{A}$ est inversible, alors $\overline{x}$ est inversible dans $\mathcal{A}/I$, et $(\overline{x})^{-1} = \overline{x^{-1}}$.*

Preuve. Exercice (comme pour $\mathbb{Z}/n\mathbb{Z}$). ■

Proposition *Soient $\mathcal{A}$ un anneau et I un idéal de $\mathcal{A}$, différent de $\mathcal{A}$. Alors, la* projection canonique *$p : \mathcal{A} \to \mathcal{A}/I$, $x \mapsto x + I$ est un homomorphisme d'anneaux surjectif, dont le noyau est I.*

Preuve. C'est une paraphrase de la définition des lois sur $\mathcal{A}/I$. ■

Théorème (Propriété universelle du quotient pour les anneaux)
Soient $\mathcal{A}$ et $\mathcal{B}$ des anneaux (commutatifs unitaires), I un idéal de $\mathcal{A}$ différent de $\mathcal{A}$ et $f : \mathcal{A} \to \mathcal{B}$ un homomorphisme d'anneaux. On note $p : \mathcal{A} \to \mathcal{A}/I$ la projection canonique. On suppose que $I \subseteq \ker f$. Alors,
(i) Il existe un unique homomorphisme d'anneaux $\overline{f} : \mathcal{A}/I \to \mathcal{B}$ tel que $f = \overline{f} \circ p$;
(ii) $\operatorname{im}(\overline{f}) = \operatorname{im}(f)$ *et* $\ker(\overline{f}) = p(\ker(f))$.
En particulier, $\overline{f}$ est surjectif si, et seulement si f est surjectif ; $\overline{f}$ est injectif si, et seulement si $I = \ker f$.

Le diagramme commutatif (et même cartésien) standard est le suivant :

$$\begin{array}{ccc} \mathcal{A} & \xrightarrow{f} & \mathcal{B} \\ {\scriptstyle p}\downarrow & \nearrow_{\overline{f}} & \\ \mathcal{A}/I & & \end{array}$$

Preuve. C'est la PUQ pour les applications appliquée à cette situation. Par ailleurs, $\overline{f}$ est un homomorphisme d'anneaux (exo). Le calcul du noyau de $\overline{f}$ est immédiat. ■

Exercice 46 Prendre le temps de faire une preuve détaillée de la PUQ pour les anneaux.

Exemple Soient a et b dans un anneau $\mathcal{A}$. Si $a|b$, alors $(b) \subseteq (a)$. La projection canonique $\mathcal{A} \to \mathcal{A}/(a)$ se factorise en un homomorphisme d'anneaux surjectif $\mathcal{A}/(b) \to \mathcal{A}/(a)$ dont le noyau est $\{x + (b),\ x \in (a)\} = \{a\alpha + (b),\ \alpha \in \mathcal{A}\} = q((a))$, si $q : \mathcal{A} \to \mathcal{A}/(b)$ est la projection canonique sur (b).

Théorème (Premier théorème d'isomorphisme pour les anneaux)
Tout homomorphisme d'anneaux $f : \mathcal{A} \to \mathcal{B}$ induit un isomorphisme d'anneaux $\overline{f} : \mathcal{A}/\ker f \xrightarrow{\sim} \operatorname{im} f$.

Preuve. Corollaire direct de la PUQ. ■

Exemples

(i) Soit $\mathbb{F}$ un corps commutatif et $a \in \mathbb{F}$. La spécialisation $\mathbb{F}[X] \to \mathbb{F}$, $P \mapsto P(a)$ est un homomorphisme surjectif d'anneaux dont le noyau est $(X-a)$. Il se factorise en l'isomorphisme $\mathbb{F}[X]/(X-a) \simeq \mathbb{F}$ qui envoie la classe de X sur a. En particulier, le quotient $\mathbb{F}[X]/(X-a)$ est un corps.

(ii) Imaginons qu'on ait une construction du corps $\mathbb{C}$ des nombres complexes (par des matrices réelles de dimension 2, par exemple). La spécialisation $\mathbb{R}[X] \to \mathbb{C}$, $P \mapsto P(i)$ se factorise en un isomorphisme d'anneaux $\mathbb{R}[X]/(X^2+1) \xrightarrow{\sim} \mathbb{C}$. Cela fournit une définition intrinsèque de $\mathbb{C}$, qui permet d'écrire définitivement

$$\mathbb{C} = \mathbb{R}[X]/(X^2+1)$$

(iii) La même spécialisation $\mathbb{Z}[X] \to \mathbb{C}$ se factorise en un isomorphisme d'anneaux $\mathbb{Z}[X]/(X^2+1) \xrightarrow{\sim} \mathbb{Z}[i]$.

Exercice 47 Montrer que si l'entier naturel d n'est pas un carré d'entier, les anneaux $\mathbb{Z}[\sqrt{d}]$ et $\mathbb{Z}[X]/(X^2-d)$ sont isomorphes.

Théorème (Idéaux d'un quotient)
Soient $\mathcal{A}$ un anneau, I un idéal de $\mathcal{A}$ différent de I et $p : \mathcal{A} \to \mathcal{A}/I$ la projection canonique. Alors, l'application

$$\begin{array}{ccc} \{\text{idéaux de } \mathcal{A}/I\} & \longrightarrow & \{\text{idéaux de } \mathcal{A} \text{ contenant } I\} \\ \mathcal{I} & \longmapsto & p^{-1}(\mathcal{I}) \end{array}$$

est une bijection dont la réciproque est l'application $J \longmapsto J/I := p(J) = \{p(j),\ j \in J\} = \{j+I,\ j \in J\}$.

Attention à la notation J/I qui n'est pas le quotient d'un *anneau* par un idéal, même si cela y ressemble beaucoup.

Preuve. $p(p^{-1}(\mathcal{I})) = \mathcal{I}$ car p est surjectif. Par ailleurs, $p^{-1}(p(J)) = J + I = J$ puisque $I \subseteq J$. ■

Exercice 48 S'attarder sur ce théorème. En écrire une preuve plus détaillée.

Exemple Les idéaux de $\mathbb{R}[X]/(X^4-1)$ sont tous principaux, engendrés par les diviseurs de $X^4-1 = (X^2+1)(X-1)(X+1)$ sur $\mathbb{R}$. Il y en a 8.

Exercice 49 Détailler les arguments qui permettent les assertions de l'exemple ci-dessus. Décrire les huit idéaux de $\mathbb{R}[X]/(X^4-1)$.

Théorème (Deuxième théorème d'isomorphisme pour les anneaux)
Soient $\mathcal{A}$ un anneau, I et J des idéaux de $\mathcal{A}$ tels que $I \subseteq J \neq \mathcal{A}$. Alors, la projection canonique $\mathcal{A} \to \mathcal{A}/J$ induit un isomorphisme d'anneaux $(\mathcal{A}/I)\,/\,(J/I) \xrightarrow{\sim} \mathcal{A}/J$.

Preuve. Grâce à la PUQ pour les anneaux, on factorise la projection canonique $\mathcal{A} \to \mathcal{A}/J$ en un homomorphisme d'anneaux surjectif $\mathcal{A}/I \to \mathcal{A}/J$, dont le noyau est J/I (notation définie dans le théorème d'idéaux d'un quotient). On conclut avec le premier théorème d'isomorphisme. ■

Corollaire *Soit $\mathcal{A}$ un anneau.*

(i) Soient I et J deux idéaux de $\mathcal{A}$ tels que $I + J \neq \mathcal{A}$. Alors, les anneaux $\mathcal{A}/(I+J)$ et $\big(\mathcal{A}/I\big)/\big(I+J\big)/I$ sont isomorphes.

(ii) Soient $\mathcal{A}$ un anneau, a et b deux éléments de $\mathcal{A}$ tels que $\mathcal{A} \neq (a,b)$. Alors, les anneaux $\mathcal{A}/(a,b)$ et $\big(\mathcal{A}/(a)\big)/(b) = \big(\mathcal{A}/(a)\big)/b\mathcal{A}/(a)$ sont isomorphes.

Preuve. $(a,b)/(a) = bA/(a)$. ■

Exercice 50 Faire une preuve détaillée de ce corollaire en décryptant l'argument elliptique écrit ci-dessus.

Exemple En appliquant successivement le second théorème d'isomorphisme et le premier théorème d'isomorphisme appliqué à la spécialisation des polynômes en 0, on obtient les isomorphismes entre anneaux suivants :

$$\mathbb{Z}[X]/(2,X) \simeq \mathbb{Z}[X]/(X)/(2) \simeq \mathbb{Z}/2\mathbb{Z}.$$

Cela apporte une deuxième démonstration du fait que $(2,X) \neq \mathbb{Z}[X]$.

Exercice 51 Détailler les mécanismes qui amènent aux isomorphismes d'anneaux de l'exemple précédent.

Théorème (Réduction des polynômes)
Soient $\mathcal{A}$ un anneau et I un idéal de $\mathcal{A}$ différent de $\mathcal{A}$. On note encore I l'idéal engendré par I dans l'anneau de polynômes $\mathcal{A}[X]$. Alors, l'homomorphisme de réduction

$$\begin{array}{ccc} \mathcal{A}[X] & \longrightarrow & \mathcal{A}/I[X] \\ \displaystyle\sum_{n\geq 0} a_n X^n & \longmapsto & \displaystyle\sum_{n\geq 0} \overline{a_n} X^n, \end{array}$$

où $\overline{a}_n$ désigne la classe de a_n modulo I, induit un isomorphisme d'anneaux entre $\mathcal{A}[X]/I$ et $\mathcal{A}/I[X]$.

Preuve. L'application définie dans l'énoncé est un homomorphisme d'anneaux surjectif dont le noyau est I. On applique le premier théorème d'isomorphisme pour les anneaux. ■

Exercice 52 Détailler les arguments des éléments de preuve ci-dessus.

Exemple En reprenant l'exemple précédent, on peut combiner le second théorème d'isomorphisme pour les anneaux, le théorème de réduction et le premier théorème d'isomorphisme appliqué à la spécialisation des polynômes en 0 pour aboutir à la même conclusion via les trois étapes successives suivantes :

$$\mathbb{Z}[X]/(2,X) \simeq \mathbb{Z}[X]/(2)/(X) \simeq \mathbb{Z}/2\mathbb{Z}[X]/(X) \simeq \mathbb{Z}/2\mathbb{Z}.$$

5.2 Idéaux premiers, idéaux maximaux

Définitions Soient $\mathcal{A}$ un anneau et I un idéal de $\mathcal{A}$, différent de $\mathcal{A}$.
(i) On dit que I est un *idéal premier* de $\mathcal{A}$ lorsque

$$\forall i \in I, \forall a, b \in \mathcal{A},\ i = ab \Longrightarrow a \in I \text{ ou } b \in I.$$

(ii) On dit que I est un *idéal maximal* de $\mathcal{A}$ lorsque I est élément maximal parmi les idéaux non triviaux de $\mathcal{A}$. Autrement dit, lorsque pour tout idéal J de $\mathcal{A}$,

$$I \subsetneq J \Longrightarrow J = \mathcal{A}.$$

Théorème de Krull *Soit $\mathcal{A}$ un anneau et I un idéal de $\mathcal{A}$, différent de $\mathcal{A}$. Alors, il existe un idéal maximal de $\mathcal{A}$ qui contienne I.*

Preuve. Ce théorème est une conséquence de l'axiome du choix, sous sa version Zorn. En trouver une preuve dans la littérature. ■

Proposition *Soient $\mathcal{A}$ un anneau et I un idéal de $\mathcal{A}$, différent de $\mathcal{A}$.*
(i) I est un idéal premier si, et seulement si $\mathcal{A}/I$ est un anneau intègre.
(ii) I est un idéal maximal si, et seulement si $\mathcal{A}/I$ est un corps.

Preuve. Ce sont des paraphrases des définitions d'idéal premier et d'idéal maximal. ■

Exercice 53 Détailler en quoi cette proposition est une simple redite des définitions d'idéal premier et d'idéal maximal.

Exercice 54 Cela montre en particulier que tout idéal maximal est premier. Faire une preuve directe de cela sans utiliser le passage au quotient.

Exercice 55 Dans $\mathbb{Z}[X]$, l'idéal $(2,X)$ est maximal (donc premier).

Exercice 56 Dans un anneau principal, tout idéal premier non nul est maximal.

Exercice 57 Si (p) est un idéal premier, alors p est irréductible. La réciproque est vraie dans les anneaux factoriels, fausse en général.

5.3 Anneau produit, théorème chinois

Définition Si $\mathcal{A}$ et $\mathcal{B}$ sont des anneaux, l'*anneau produit* est la structure d'anneau sur le produit cartésien $\mathcal{A}\times\mathcal{B}$ défini par les loi suivantes : pour tous (a,b) et (a',b') dans $\mathcal{A}\times\mathcal{B}$,

$$(a,b)+(a',b')=(a+a',b+b') \text{ et } (a,b)\times(a',b')=(a\times a',b\times b').$$

On note $\mathcal{A}^2$ l'anneau produit $\mathcal{A}\times\mathcal{A}$.

Exercice 58 Les lois définies par les formules ci-dessus confèrent à $\mathcal{A}\times\mathcal{B}$ une structure d'anneau dont le zéro est $(0_\mathcal{A},0_\mathcal{B})$ et l'unité $(1_\mathcal{A},1_\mathcal{B})$ (notations évidentes).

Exercice 59 Un anneau produit n'est jamais intègre.

Exercice 60 Si $n\geq 2$ et si $\mathcal{A}_1,\mathcal{A}_2,\dots,\mathcal{A}_n$ sont des anneaux, on définit de façon similaire l'anneau produit $\mathcal{A}_1\times\mathcal{A}_2\times\cdots\times\mathcal{A}_n$ où l'addition et la multiplication se font coordonnée par coordonnée. On obtient bien un anneau. On note encore $\mathcal{A}^n$ l'anneau produit $\mathcal{A}\times\cdots\times\mathcal{A}$ (n fois).

Exercice 61 Si $\mathcal{A}$, $\mathcal{B}$ et $\mathcal{C}$ sont des anneaux, les anneaux produits

$$(\mathcal{A}\times\mathcal{B})\times C,\ \mathcal{A}\times(\mathcal{B}\times\mathcal{C}) \text{ et } \mathcal{A}\times\mathcal{B}\times\mathcal{C}$$

sont isomorphes. Généraliser cet énoncé aux parenthésages de produits finis arbitraires d'anneaux.

Théorème (Théorème chinois forme générale)
Soient $\mathcal{A}$ un anneau, I et J des idéaux de $\mathcal{A}$ différents de $\mathcal{A}$. On suppose que $I+J=\mathcal{A}$. Alors, l'homomorphisme d'anneaux $\mathcal{A}\to\mathcal{A}/I\times\mathcal{A}/J$, $x\mapsto(x+I,x+J)$ induit un isomorphisme d'anneaux $\mathcal{A}/I\cap J\xrightarrow{\sim}\mathcal{A}/I\times\mathcal{A}/J$.

Preuve. Soit f le produit des projections canoniques, $\mathcal{A}\to\mathcal{A}/I\times\mathcal{A}/J$, $x\mapsto f(x)=(x+I,x+J)$. Son noyau est $I\cap J$. Soient $i\in I$ et $j\in J$ tels que $1=i+j$. Alors, pour tout $(\overline{x},\overline{y})\in\mathcal{A}/I\times\mathcal{A}/J$, $(\overline{x},\overline{y})=f(x+(y-x)i)=f(y+(x-y)j)$ ce qui montre que f est surjectif puisque $x+(y-x)i=y+(x-y)j$. ■

Exercice 62 Détailler la preuve ci-dessus.

Exemples

(i) Soient n et m deux entiers premiers entre eux. Alors, $\mathbb{Z}/nm\mathbb{Z}\simeq\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$.

(ii) Soient $\mathbb{F}$ un corps commutatif, a et b deux éléments distincts de $\mathbb{F}$. Les polynômes $X-a$ et $X-b$ sont étrangers. Pour s'en persuader, s'il faut, voici une relation de Bézout : $\frac{1}{b-a}(X-a)+\frac{1}{a-b}(X-b)=1$. En outre (ou par conséquent), $(X-a)\cap(X-b)=((X-a)(X-b))$. On est dans les hypothèses du chinois qui fournit

$$\mathbb{F}[X]/(X-a)(X-b)\simeq\mathbb{F}[X]/(X-a)\times\mathbb{F}[X]/(X-b)\simeq\mathbb{F}^2$$

(la structure de $\mathbb{F}^2$ est ici celle de l'anneau produit).

(iii) $\mathbb{C}[X]/(X^2+1)\simeq\mathbb{C}[X]/(X-i)\times\mathbb{C}[X]/(X+i)\simeq\mathbb{C}^2$ qui n'est pas intègre. Cette situation est très différente du quotient $\mathbb{R}[X]/(X^2+1)\simeq\mathbb{C}$.

(iv) Par récurrence, si $a_1,\dots a_n$ sont distincts dans un corps $\mathbb{F}$, alors $\mathbb{F}[X]/(X-a_1)\dots(X-a_n)\simeq\mathbb{F}^n$.

(v) L'anneau $\mathbb{F}[X]/\left(X^2\right)$ est un $\mathbb{F}$-espace vectoriel de dimension 2, dont une base est $(\overline{1},\overline{X})$. En tant que $\mathbb{F}$-espace vectoriel, $\mathbb{F}[X]/\left(X^2\right)\simeq\mathbb{F}^2$. En revanche, en tant qu'anneaux, il n'y a pas d'isomorphisme entre $\mathbb{F}[X]/\left(X^2\right)$ et $\mathbb{F}^2$, puisque $\mathbb{F}[X]/\left(X^2\right)$ a $\overline{X}$ pour nilpotent[♫] alors que $\mathbb{F}^2$ ne contient aucun nilpotent non nul (si $(x,y)^n=(0,0)$ pour $n\geq 1$, alors $x=y=0$).

(vi) $\mathbb{R}[X]/(X^4-1)\simeq\mathbb{C}\times\mathbb{R}^2$ en tant qu'anneau.

Exercice 63 Détailler tous les arguments des exemples (i) à (vi) ci-dessus.

Exercice 64 Au regard de l'isomorphisme d'anneaux de l'exemple (vi), faire la liste des idéaux des deux anneaux et établir la correspondance entre ces idéaux que cet isomorphisme induit.

[♫] Dans un anneau, un élément a est *nilpotent* lorsqu'il existe $n\in\mathbb{N}$ tel que $a^n=0$.

6 Fractions

6.1 Corps des fractions d'un anneau intègre

Soit $\mathcal{A}$ un anneau intègre. En mimant l'égalité de deux fractions, on définit sur $\mathcal{A} \times \mathcal{A} \setminus \{0\}$ la relation d'équivalence $(n,d) \sim (n',d') \iff nd' = n'd$ (la transitivité utilise l'intégrité). On note l'ensemble quotient

$$\mathrm{Fr}(\mathcal{A}) = (\mathcal{A} \times \mathcal{A} \setminus \{0\}) / \sim .$$

C'est l'ensemble des *fractions* d'éléments de $\mathcal{A}$. [On peut aussi écrire la relation avec un déterminant.]

Exercice 65 Montrer que la relation binaire définie ci-dessus est une relation d'équivalence.

En mimant l'addition et la multiplication des fractions, on définit sur $\mathcal{A} \times \mathcal{A} \setminus \{0\}$ les lois internes suivantes :

$$(n,d) + (n',d') = (nd' + n'd, dd') \quad \text{et} \quad (n,d) \times (n',d') = (nn', dd').$$

Exercice 66 Ces lois sur $\mathcal{A} \times \mathcal{A} \setminus \{0\}$ sont associatives, commutatives, admettent respectivement $(0,1)$ et $(1,1)$ comme neutres pour $+$ et $\times$. En outre, $\times$ est distributive par rapport à $+$ (que manque-t-il pour avoir un anneau ?).

Ces lois sont *compatibles* avec la relation d'équivalence : si $q = (m,d)$, $q' = (m',d')$, $r = (n,e)$ et $r' = (n',e')$ sont dans $\mathcal{A} \times \mathcal{A} \setminus \{0\}$ et si $q \sim q'$ et $r \sim r'$, alors $q + r \sim q' + r'$ et $qr \sim q'r'$.

Exercice 67 Prouver la compatibilité de $\sim$ pour l'addition et la multiplication définies sur $\mathcal{A} \times \mathcal{A} \setminus \{0\}$ ci-dessus.

On définit alors une addition et une multiplication internes sur $\mathrm{Fr}(\mathcal{A})$ par :

$$\overline{q} + \overline{r} = \overline{q+r} \quad \text{et} \quad \overline{q} \times \overline{r} = \overline{qr}.$$

Bien noter que sans la compatibilité, ces définitions n'auraient pas de sens.

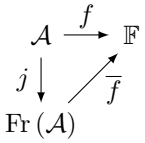
Proposition *Si $\mathcal{A}$ est un anneau (commutatif) intègre, $(\mathrm{Fr}(\mathcal{A}), +, \times)$ est un corps (commutatif) et l'application $j : \mathcal{A} \to \mathrm{Fr}(\mathcal{A})$, $x \mapsto \overline{(x,1)}$ est un homomorphisme injectif d'anneaux.*

Preuve. Associativités, commutativités, neutres ($j(0)$ et $j(1)$) et distributivité viennent des exercices précédents. L'opposé de $\overline{(n,d)}$ est $\overline{(-n,d)} = \overline{(n,-d)}$ puisque $\overline{(n,d)} + \overline{(-n,d)} = \overline{(0,d^2)} = \overline{(0,1)}$. L'addition fait de $\mathrm{Fr}(\mathcal{A})$ un groupe abélien. Ainsi, $\mathrm{Fr}(\mathcal{A})$ est un anneau commutatif. Si $\overline{(n,d)} \neq \overline{(0,1)}$, *i.e.* si $n \neq 0$, alors $\overline{(n,d)} \times \overline{(d,n)} = \overline{(nd,nd)} = \overline{(1,1)}$. D'où le corps. Que j soit un homomorphisme d'anneaux est une paraphrase des lois sur $\mathrm{Fr}(\mathcal{A})$. Il est injectif puisque $(x,1) \sim (0,1)$ si et seulement si $x = 0$. ■

Notation On note $(n,d) = \frac{n}{d}$, avec les règles habituelles de calcul sur les fractions. On note aussi $a = j(a) = \frac{a}{1}$ lorsque $a \in \mathcal{A}$. Par exemple, $\frac{n}{d} = 0$ si, et seulement si $n = 0$, ou encore $\frac{n}{d} \in \mathcal{A}$ si, et seulement si $d|n$.

Proposition (Propriété universelle du corps des fractions)
Soient $\mathcal{A}$ un anneau intègre et $\mathbb{F}$ un corps. Alors, tout homomorphisme injectif d'anneaux $f : \mathcal{A} \to \mathbb{F}$ se prolonge de manière unique en un homomorphisme d'anneaux (de corps) $\overline{f} : \mathrm{Fr}(\mathcal{A}) \to \mathbb{F}$.

Le diagramme commutatif (et même cartésien) correspondant est le suivant :



Que $\overline{f}$ "prolonge" f s'écrit $\overline{f} \circ j = f$, puisque la notation $j(a) = a \in \mathrm{Fr}\,(\mathcal{A})$ revient à considérer j comme une inclusion.

Preuve. Unicité : on n'a pas le choix, $\overline{f}\left(\frac{a}{b}\right) = \frac{f(a)}{f(b)}$ (cela a du sens car $f(b) \neq 0$ puisque f est injectif). Existence : la formule $\overline{f}\left(\frac{a}{b}\right) = \frac{f(a)}{f(b)}$ a du sens et répond à la question. ■

Exercice 68 Détailler tous les arguments de la preuve ci-dessus.

Corollaire *Soient $\mathbb{F}$ un corps et $\mathcal{A}$ un sous-anneau de $\mathbb{F}$. Alors, $\mathbb{F}$ contient $\mathrm{Fr}(\mathcal{A})$ (ou plutôt un sous-corps isomorphe à $\mathrm{Fr}(\mathcal{A})$).*

PREUVE. On applique la propriété universelle du corps des fractions à l'injection $\mathcal{A} \subseteq \mathbb{F}$. ■

Exemple $\mathbb{Q} = \mathrm{Fr}\,(\mathbb{Z})$. Cela fournit une définition intrinsèque de $\mathbb{Q}$.

6.2 Fractions rationnelles

Définition Si $\mathcal{A}$ est intègre, $\mathcal{A}[X_1, \ldots, X_n]$ l'est aussi et on note $\mathcal{A}(X_1, \ldots, X_n)$ le corps des fractions de $\mathcal{A}[X_1, \ldots, X_n]$. C'est le corps des *fractions rationnelles à n indéterminées* (formelles) sur $\mathcal{A}$.

Exercice 69 Si $\mathcal{A}$ est intègre, $\mathcal{A}(X_1, \ldots, X_n) = \mathrm{Fr}(\mathcal{A})(X_1, \ldots, X_n)$.

Exercice 70 $\mathrm{Fr}\,(\mathbb{Z}[X]/(2)) \simeq \mathbb{Z}/2\mathbb{Z}(X)$.

Remarque Si $\mathbb{F}$ est un corps, l'anneau $\mathbb{F}[X, Y]$ est factoriel (transfert de Gauss) mais pas principal. Il est souvent utile de le considérer comme sous-anneau de $\mathbb{F}(X)[Y]$ qui, lui, est principal puisque $\mathbb{F}(X)$ est un corps.

Définition Soit $\mathbb{F}$ un corps. Une fraction rationnelle de $\mathbb{F}(x)$ est dite *simple* lorsqu'elle est de la forme $\frac{N}{D^n}$ où $n \in \mathbb{N}^*$, $D \in \mathbb{F}[X]$ est unitaire et irréductible, et où $N \in \mathbb{F}[X] \setminus \{0\}$ vérifie $\deg(N) \leq \deg(D) - 1$.

Théorème (Décomposition des fractions rationnelles en éléments simples)
Soit $\mathbb{F}$ un corps. Toute fraction rationnelle de $\mathbb{F}(X)$ s'écrit de manière unique comme la somme d'un polynôme de $\mathbb{F}[X]$ et de fractions rationnelles simples.

PREUVE. Utilisations itérées de la division euclidienne dans $\mathbb{F}[X]$. ■

Exercice 71 Faire une preuve détaillée de ce théorème en suivant la suggestion ci-dessus.

Remarque La pratique de la décomposition sur $\mathbb{R}$ et sur $\mathbb{C}$ sert notamment au calcul de primitives des fractions rationnelles réelles et au calcul de résidus en analyse complexe.

Exemples Soit $F = \frac{X^5}{X^4-4} = X + \frac{4X}{X^4-4}$. La décomposition en éléments simples de F s'écrit :

(i) $F = X + \frac{1/2}{X-\sqrt{2}} + \frac{1/2}{X+\sqrt{2}} - \frac{1/2}{X-i\sqrt{2}} - \frac{1/2}{X+i\sqrt{2}}$ sur $\mathbb{C}$

(ii) $F = X + \frac{1/2}{X-\sqrt{2}} + \frac{1/2}{X+\sqrt{2}} - \frac{X}{X^2+2}$ sur $\mathbb{R}$

(iii) $F = X + \frac{X}{X^2-2} - \frac{X}{X^2+2}$ sur $\mathbb{Q}$.

Exercice 72 Justifier tout cela minutieusement.

7 Factorisation des polynômes

7.1 Polynôme dérivé, formule de Taylor

Dans tout le chapitre, $\mathcal{A}$ est un anneau commutatif unitaire.

Définition Si $P = \sum_{n\geq 0} a_n X^n \in \mathcal{A}[X]$, le *polynôme dérivé* de P est le polynôme $P' = \sum_{n\geq 1} n a_n X^{n-1} = \sum_{n\geq 0}(n+1)a_{n+1}X^n$. On le note aussi $\frac{dP}{dX}$.

Définition *Dérivés d'ordres supérieurs* : si $P \in \mathcal{A}[X]$, on note $P^{(0)} = P$, $P^{(1)} = P'$, et par récurrence $P^{(n)} = \left(P^{(n-1)}\right)' = \frac{d^n P}{dX^n}$ pour tout entier naturel n (*polynôme dérivé n-ième* de P).

Remarque La définition est formelle, par opposition à la définition de la dérivation en un point d'une fonction de la variable réelle. Les règles de dérivation des fonctions polynomiales sont encore valides pour les polynômes (preuves élémentaires à faire en exercice) : $(P+Q)' = P' + Q'$, $(\lambda P)' = \lambda P'$, $(PQ)' = P'Q + PQ'$ et $(P \circ Q)' = P' \circ Q \times Q'$.

Exercice 73 Prouver les assertions de la remarque ci-dessus.

Théorème (formule de Taylor pour les polynômes)
On suppose que $\mathcal{A}$ est un sous-anneau de $\mathbb{C}$.

(i) Si $P \in \mathcal{A}[X]$, alors $P = \displaystyle\sum_{n\geq 0} \frac{1}{n!} P^{(n)}(0) X^n$.

(ii) Si $P \in \mathcal{A}[X]$ et $a \in \mathcal{A}$, alors

$$P(X+a) = \sum_{n\geq 0} \frac{1}{n!} P^{(n)}(a) X^n \quad \text{et} \quad P(X) = \sum_{n\geq 0} \frac{1}{n!} P^{(n)}(a)(X-a)^n.$$

Preuve. Une récurrence immédiate montre que pour tous entiers naturels n et p,

$$\frac{d^p}{dX^p}(X^n) = \begin{cases} 0 \ \text{ si } p \geq n+1 \ ; \\ n(n-1)\dots(n-p+1)X^{n-p} \ \text{ si } p \leq n. \end{cases}$$

Ainsi, si $P = \sum_n a_n X^n$, a-t-on $P^{(p)}(0) = p! a_p$. D'où le (i) puisqu'on peut diviser par $p!$ qui n'est pas nul. Si $a \in \mathcal{A}$, soit $Q \in \mathcal{A}[X]$ défini par $Q(X) = P(X+a)$. On applique (i) à Q : $Q = \sum_n Q^{(n)}(0)/n! X^n = \sum_n P^{(n)}(a)/n! X^n$ puisque $\forall n$, $Q^{(n)}(X) = P^{(n)}(X+a)$. La dernière égalité est conséquence de la deuxième en substituant $X - a$ à X. ∎

Exercice 74 Trouver un anneau (ou même un corps) et un polynôme à une indéterminée à coefficients dans cet anneau pour lequel la formule de Taylor n'est pas valide.

Définition (caractéristique d'un anneau) Soit $\mathcal{A}$ un anneau. L'application

$$\begin{array}{rccc} \chi : & \mathbb{Z} & \to & \mathcal{A} \\ & n & \mapsto & n.1 \end{array}$$

est un homomorphisme d'anneaux. La *caractéristique* de $\mathcal{A}$, notée $\operatorname{car}(\mathcal{A})$ est l'unique entier naturel tel que $\ker(\chi) = \operatorname{car}(\mathcal{A})\,\mathbb{Z}$.

Autrement dit, $\operatorname{car}(\mathcal{A})$ est le plus petit entier positif ou nul n tel que $1 + 1 + \dots + 1$ [n fois] est nul.

Exercice 75
(i) Quelle est la caractéristique de $\mathbb{Z}/n\mathbb{Z}$? Celle de $\mathbb{C}$?

(ii) Si B est un sous-anneau de A, calculer la caractéristique de B en fonction de celle de A.

(iii) Calculer la caractéristique de $A[X]$ en fonction de celle de A.

(iv) Si A est intègre, $\operatorname{car}(A)$ est nulle ou un nombre premier.

(v) Si A est intègre, calculer caractéristique de $\operatorname{Fr}(A)$ en fonction de celle de A.

(vi) Calculer la caractéristique de l'anneau produit $A \times B$ en fonction de celles de A et B.

(vii) Si A est un anneau et si I est un idéal de A, la caractéristique de A/I divise celle de A.

(viii) Un anneau de caractéristique nulle est infini.

(ix) Les formules de Taylor pour les polynômes sont valides sur les corps de caractéristique nulle.

7.2 Factorisation des polynômes sur un anneau intègre

Rappel : dans un anneau intègre, tout polynôme unitaire de degré 1 est irréductible (exercice : on peut enlever "intègre" dans l'assertion). Sur un corps, tout polynôme de degré 1 est irréductible.

Exercice 76 Soit $n \in \mathbb{N}^*$. Pour tout $k \in \{0, \dots, n-1\}$, $\exp(2ik\pi/n)$ est racine de $X^n - 1$ dans $\mathbb{C}$, et ces n nombres sont distincts. Ainsi, $\prod_{k=0}^{n-1}(X - \exp(2ik\pi/n))$ divise-t-il $X^n - 1$. Ces deux polynômes ont le même degré, le même coefficient dominant et l'un divise l'autre : ils sont égaux. La factorisation de $X^n - 1$ dans $\mathbb{C}[X]$ est donc

$$X^n - 1 = \prod_{k=0}^{n-1}(X - e^{2ik\pi/n}).$$

Cas $n = 3$: on note $j = \exp(2i\pi/3)$. Factorisation de $X^3 - 1$ sur $\mathbb{C}$: $X^3 - 1 = (X-1)(X-j)(X-j^2)$. En regroupant les facteurs non réels, on obtient la factorisation dans $\mathbb{R}[X]$: $X^3 - 1 = (X-1)(X^2+X+1)$. C'est aussi la factorisation rationnelle (dans $\mathbb{Q}[X]$).

Cas $n = 4$: $X^4 - 1 = (X-1)(X-i)(X+1)(X+i) = (X-1)(X+1)(X^2+1)$ (factorisation réelle et rationnelle).

Cas $n = 5$: on pose $\omega = \exp(2i\pi/5)$. Alors, $X^5 - 1 = (X-1)(X-\omega)(X-\omega^2)(X-\omega^3)(X-\omega^4)$, c'est la factorisation sur $\mathbb{C}$. En regroupant, $X^5 - 1 = (X-1)(X - e^{2i\pi/5})(X - e^{-2i\pi/5})(X - e^{4i\pi/5})(X - e^{-4i\pi/5}) = (X-1)(X^2 - 2\cos\frac{2\pi}{5}X + 1)(X^2 + 2\cos\frac{2\pi}{5}X + 1)$, c'est la factorisation sur $\mathbb{R}$. Comme $\cos\frac{2\pi}{5} \notin \mathbb{Q}$ (exercice), on continue : $X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1)$, c'est la factorisation sur $\mathbb{Q}$.

Définition Soient $\mathcal{A}$ un anneau intègre, $P \in \mathcal{A}[X]$, $a \in \mathcal{A}$ et n un entier naturel. La *multiplicité* (ou l'*ordre*) *de a dans P* est la $(X-a)$-valuation de P dans l'anneau factoriel $\mathcal{A}[X]$.

Exercice 77 Soient $\mathcal{A}$ un anneau intègre et $P \in \mathcal{A}[X]$, $a \in \mathcal{A}$ et $n \in \mathbb{N}$. Alors, a est racine de P de multiplicité n si, et seulement si $(X-a)^n | P$ et $(X-a)^{n+1} \not| P$.

Exemple La multiplicité de la racine 1 de $(X^2-1)(X^5-1)^3(X^2+X+1)$ est 4.

Proposition *Soient $\mathcal{A}$ un anneau intègre, $P \in \mathcal{A}[X]$, $a \in \mathcal{A}$ et $n \geq 1$ un entier.*
(i) a est racine d'ordre $\geq n$ de P si, et seulement si $P(a) = 0$ et a est racine d'ordre $\geq n-1$ de P'.
(ii) Si a est racine d'ordre $\geq n$ de P, alors $\forall k \in \{0, \dots, n-1\}$, $P^{(k)}(a) = 0$.
(iii) Si $\mathcal{A}$ est un sous-anneau de $\mathbb{C}$, il y a équivalence entre (i) et (ii). En outre, dans ces conditions, a est racine d'ordre n si, et seulement si $\forall k \in \{0, \dots, n-1\}$, $P^{(k)}(a) = 0$ et $P^{(n)}(a) \neq 0$.

Preuve. (i) On fait la division euclidienne de P par $(X-a)^n$: $P = (X-a)^n Q + R$ avec $R = 0$ ou $\deg(R) \leq n-1$. Alors, $P' = (X-a)^{n-1}[nQ + (X-a)Q'] + R'$ est la division euclidienne de P' par $(X-a)^{n-1}$. Si $(X-a)^n | P$ alors $R = 0$; d'où $R' = 0$ et $(X-a)^{n-1} | P'$.
(ii) On fait un récurrence sur n.
(iii) Si $\mathcal{A}$ est un sous-anneau de $\mathbb{C}$, la formule de Taylor est valide. Ainsi, si $P(a) = P'(a) = \cdots = P^{(n-1)}(a) = 0$, alors $(X-a)^n | P$. La fin de la preuve est laissée en exercice (avec la formule de Taylor). ■

Exemples
(i) $\mathcal{A} = \mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier, $P = X^p - 1 = (X-1)^p$ et $a = 1$. Dans cet exemple, 1 est racine de multiplicité p de P. Par ailleurs, comme $P' = 0$, $P^{(k)}(1) = 0$ pour tout $k \geq 0$: il n'y a en général pas d'équivalence dans le (ii) du théorème.
(ii) Dans $\mathbb{Z}[X]$, $(X-1)^3 | P = X^7 + 7X^4 - 4X^3 - 3X^6 - 6X^2 + 7X - 2$ puisque $P(1) = 0$, $P'(1) = 0$ et $P''(1) = 0$ (faire le calcul).

7.3 Irréductibilité de polynômes sur $\mathbb{R}$ et $\mathbb{C}$

7.3.1 Sur $\mathbb{C}$

Théorème de d'Alembert-Gauss *Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine.*

PREUVE. On l'admet ici. Toute preuve contient de l'analyse et s'appuie sur les propriétés de $\mathbb{R}$, notamment sa complétude. Voir par exemple le cours d'analyse complexe. ■

Corollaire *$P \in \mathbb{C}[X]$ est irréductible si, et seulement si* $\deg(P) = 1$.

PREUVE. Si P est constant, il est nul ou inversible, donc réductible. Si $\deg(P) = 1$, alors P est irréductible (le voir sur le degré). Enfin, si $\deg(P) \geq 2$, soit a une racine (complexe) de P. Alors, $P = (X-a)Q$ où $\deg(Q) \geq 1$. Comme Q n'est pas inversible (il n'est pas constant), P est réductible.

Corollaire *Tout polynôme de $\mathbb{C}[X] \setminus \{0\}$ est produit de polynômes de degré un.*

PREUVE. Récurrence sur $\deg(P)$. ■

Autrement dit, si $P \in \mathbb{C}[X]$ a $u \in \mathbb{C}$ pour coefficient dominant, il existe $a_1, \ldots, a_n \in \mathbb{C}$ tels que

$$P = u \prod_{1 \leq k \leq n} (X - a_k).$$

Définition Soit $\mathbb{F}$ un corps. Un polynôme de $\mathbb{F}[X]$ est dit *scindé* lorsqu'il est produit de polynômes de degré un (ainsi, tout polynôme complexe est-il scindé).

7.3.2 Sur $\mathbb{R}$

Si $P \in \mathbb{R}[X]$, on peut voir P comme élément de $\mathbb{C}[X]$. Si $z \in \mathbb{C}$ est racine de P, alors $\overline{z}$ est aussi racine de P ; en effet, puisque les coefficients de P sont réels, $P(\overline{z}) = \overline{P(z)}$. Par ailleurs,

$$\forall z \in \mathbb{C},\ (X - z)(X - \overline{z}) = X^2 - 2\Re(z)X + |z|^2.$$

Proposition *Soient $P \in \mathbb{R}[X]$ et $z \in \mathbb{C} \setminus \mathbb{R}$. Alors, z est racine de P si, et seulement si $X^2 - 2\Re(z)X + |z|^2$ divise P.*

PREUVE. ($\Longleftarrow$) résulte de la formule ci-dessus.
($\Longrightarrow$) : si z est racine, alors $\overline{z}$ aussi, avec $z \neq \overline{z}$. Alors, le produit $(X - z)(X - \overline{z})$ divise P. ■

Corollaire *Les polynômes irréductibles de $\mathbb{R}[X]$ sont :*
(i) les polynômes de degré un ;
(ii) les polynômes de degré deux qui n'ont pas de racine réelle, i.e. dont le discriminant est strictement négatif.

PREUVE. Ceux-ci sont irréductibles (un polynôme réductible de degré deux sur un corps a toujours une racine). Inversement, si P est irréductible et de degré ≥ 2, il n'a pas de racine réelle. Soit z une racine complexe non réelle de P. Alors, $X^2 - 2\Re(z)X + |z|^2$ divise P. Comme P est irréductible, il existe $u \in \mathbb{C}$ non nul tel que $P = u(X^2 - 2\Re(z)X + |z|^2)$. ■

Exercice 78 Tout polynôme réel de degré impair a au moins une racine (utiliser par exemple le théorème des valeurs intermédiaires).

Corollaire *Soit $P \in \mathbb{R}[X]$, non nul. Alors, P se décompose de manière unique en produit de facteurs irréductibles sous la forme*

$$P = u \prod_{1 \leq k \leq r} (X - a_k) \prod_{1 \leq k \leq s} Q_k$$

où $u \neq 0$ et les a_k sont des nombres réels et les Q_k des polynômes unitaires irréductibles de degré deux.

PREUVE. Décomposer dans $\mathbb{C}[X]$ et regrouper les facteurs conjugués. ■

Exercice 79 Ecrire les détails d'une démonstration du corollaire.

7.4 Polynômes d'interpolation de Lagrange

Question introductive Etant donnés $a_1, a_2, \ldots, a_n$ distincts dans $\mathbb{R}$ et $b_1, b_2, \ldots, b_n$ dans $\mathbb{R}$, existe-t-il des fonctions polynomiales dont le graphe passe par les points (a_1, b_1), (a_2, b_2), $\ldots$, (a_n, b_n) ?

Proposition (Théorème d'interpolation de Lagrange)

Soit $\mathbb{F}$ un corps (commutatif). *Soient $a_0, a_1, \ldots, a_n \in \mathbb{F}$, distincts, et $b_0, b_1, \ldots, b_n \in \mathbb{F}$ ($n \geq 0$). Alors, il existe un unique polynôme $P \in \mathbb{F}[X]$ tel que*

(i) $\forall k \in \{0, \ldots, n\}$, $P(a_k) = b_k$;

(ii) $P = 0$ ou $\deg(P) \leq n$.

En outre, P s'écrit explicitement sous la forme

$$P = \sum_{k=1}^{n} b_k \prod_{j \neq k} \frac{X - a_j}{a_k - a_j}.$$

PREUVE. Existence : la formule la prouve. Unicité : si P et Q sont solutions de (i) et (ii), alors $P - Q$ est nul ou a un degré $\leq n$. Comme $P - Q$ a $n + 1$ racines distinctes (les a_i), cela impose que $P - Q = 0$. ■

Exercice 80 Dans la situation de la proposition, trouver tous les polynômes qui vérifient (i) (on pourra utiliser la division euclidienne par le produit des $X - a_k$).

Exercice 81 Si $\mathbb{F}$ est un corps fini, $\mathbb{F}[X] \to \mathcal{F}(\mathbb{F}, \mathbb{F})$, $P \mapsto \widetilde{P}$ est surjectif – autrement dit, toute fonction $\mathbb{F} \to \mathbb{F}$ est polynomiale.

8 Eléments sur les corps de nombres [pas en 2022/2023 ?]

Sous-corps premier d'un anneau intègre. Elément algébrique vs transcendant. Extension de corps, théorie linéaire, degré d'une extension.