
**Département de Mathématiques et Informatique**

**Master 1 Mathématiques**

# *Arithmétique et Algèbre*

***Notes de cours***

R. Taillefer

Rachel.Taillefer@math.univ-bpclermont.fr

2016-2017

version du 12 décembre 2016, 11:53am

# *Table des matières*

**Chapitre 0 Rappels de base sur les anneaux** **1**

**Chapitre 1 Rappels et compléments sur les anneaux** **5**
I Idéaux premiers et maximaux. . . . . 5
II Ensembles ordonnés et lemme de Zorn . . . . . 6
III Corps des fractions d'un anneau intègre . . . . . 7
IV Rappels d'arithmétique. . . . . 9
V Anneaux factoriels . . . . . 10

**Chapitre 2 Anneaux de polynômes** **17**
I Anneaux de polynômes en plusieurs indéterminées . . . . . 17
II Fonctions polynomiales. . . . . 20
III Arithmétique dans les anneaux de polynômes . . . . . 21

**Chapitre 3 Polynômes symétriques** **27**
I L'anneau des polynômes symétriques . . . . . 27
II Polynômes symétriques élémentaires . . . . . 28
III Structure des polynômes symétriques . . . . . 29
IV Coefficients et racines de polynômes . . . . . 31
V Exemple : le discriminant . . . . . 34
VI Complément : résultant de deux polynômes . . . . . 34

Voici quelques références utiles.

- D. Guin :
  - Groupes et anneaux (tome 1), ou
  - Algèbre tome 2, Anneaux, modules et algèbre multilinéaire.
- S. Lang : Algèbre.
- M. Demazure : Cours d'algèbre. Primalité, divisibilité, codes. (Partie II).
- Tauvel : Mathématiques générales pour l'agrégation.
- Escoffier : Théorie de Galois.

## CHAPITRE 0

# *Rappels de base sur les anneaux*

On rappelle un certain nombre de définitions et propriétés de base sur les anneaux. Pour plus de détails, on renvoie au cours de L3 ou aux références données sur les cours en ligne.

**Définition.** *Un **anneau** est un groupe abélien $(A, +)$ muni d'une deuxième loi interne, la **multiplication** ou le **produit** $\cdot : A \times A \to A$, tel que :*

- *le produit est associatif : $\forall (a, b, c) \in A^3$, $(ab)c = a(bc)$;*
- *le produit est distributif par rapport à l'addition : $\forall (a, b, c) \in A^3$, $a(b + c) = ab + ac$ et $(a + b)c = ac + bc$.*

*Si de plus le produit possède un élément neutre $1$, on dit que l'anneau $A$ est **unitaire** et $1$ est appelé **élément unité** de $A$. Il vérifie $1a = a = a1$ pour tout $a \in A$.*

*Enfin, si le produit est commutatif, c'est-à-dire que $ab = ba$ pour tout $(a, b) \in A^2$, on dit que l'anneau $A$ est commutatif.*

*Pour mémoire, un groupe abélien est un ensemble non vide $A$ muni d'une loi interne $+ : A \times A \to A$ qui est associative ( $\forall (a, b, c) \in A^3$, $(a + b) + c = a + (b + c)$), possède un élément neutre noté $0$ ($\forall a \in A$, $a + 0 = a = 0 + a$), est telle que tout élément $a \in A$ possède un inverse $-a$ appelé opposé ($\forall a \in A$, $\exists b \in A$ tq. $a + b = 0 = b + a$ ; $b = -a$) et qui est commutative ($\forall (a, b) \in A^2$, $a + b = b + a$).*

**Dans tout ce cours, anneau signifie anneau commutatif unitaire, sauf mention expresse du contraire.**

**Définition.** *Un **corps** est un anneau (commutatif unitaire) tel que tout élément non nul possède un inverse : $\forall a \in A \setminus \{0\}$, $\exists b \in A$ tel que $ab = 1$.*

**Définition.** *Un **sous-anneau** $B$ d'un anneau $A$ est une partie non vide $B$ de $A$ qui, munie des opérations de $A$, est un anneau.*

*On peut vérifier que $B$ est un sous-anneau de $A$ si, et seulement si,*

- *$(B \neq \varnothing)$;*
- *$\forall (a, b) \in B^2$, on a $a - b \in B$ (ou $a + b \in B$ et $-a \in B$) – d'où $B$ est un sous-groupe (abélien) de $A$ ;*
- *$1 \in B$ ;*
- *$\forall (a, b) \in B$, on a $ab \in B$.*

**Définition.** *Un **morphisme d'anneaux** $f$ d'un anneau $A$ vers un anneau $B$ est une application $f : A \to B$ vérifiant, pour tout $(a, b) \in A^2$,*

- *$f(a + b) = f(a) + f(b)$,*
- *$f(ab) = f(a)f(b)$ et*
- *$f(1) = 1$.*

*On peut vérifier que si un morphisme d'anneaux $f$ est bijectif, alors l'application réciproque $f^{-1}$ est aussi un morphisme d'anneaux. On dit alors que $f$ est un* ***isomorphisme*** *d'anneaux.*

**Définition.** *Soit $A$ un anneau.*

- *Un élément $a \in A$ est dit* ***inversible*** *s'il possède un inverse, noté $a^{-1}$, pour le produit. On note $A^\times$ l'ensemble des éléments inversibles de $A$.*
- *Un élément $a \in A$ est un* ***diviseur de zéro*** *si $a \neq 0$ s'il existe $b \in A$ avec $b \neq 0$ tel que $ab = 0$.*
- *Un anneau $A$ est dit* ***intègre*** *si $A \neq 0$ et s'il ne contient pas de diviseur de zéro.*

*Un anneau intègre n'est pas nul.*
*Un corps est en particulier un anneau intègre.*

**Définition.** *Soit $A$ un anneau. Un* ***idéal*** *de $A$ est un sous-groupe abélien $I$ de $A$ qui vérifie*

$$\forall a \in A,\ \forall x \in I,\ \text{on a } ax \in I.$$

*Une partie $I$ de $A$ est un idéal de $A$ si, et seulement si,*

- $I \neq \varnothing$ ;
- $\forall (x, y) \in I^2,\ x + y \in I$ *et*
- $\forall (a, x) \in A \times I,\ ax \in I$.

**Propriétés.**
- Un idéal $I$ de $A$ est égal à $A$ si, et seulement si, $1 \in I$.
- Un idéal $I$ de $A$ est égal à $A$ si, et seulement s'il contient un élément inversible de $A$.
- Une intersection d'idéaux est un idéal.
- Soit $f : A \to B$ un morphisme d'anneaux.
  - Si $I$ est un idéal de $B$, alors $f^{-1}(I)$ est un idéal de $A$. En particulier, $\operatorname{Ker} f = f^{-1}(\{0\})$ est un idéal de $A$.
  - Si $f$ est *surjectif* et si $J$ est un idéal de $A$, alors $f(J)$ est un idéal de $B$.
  - Si $C$ est un sous-anneau de $A$, alors $f(C)$ est un sous-anneau de $B$. En particulier, $\operatorname{Im} f = f(A)$ est un sous-anneau de $B$.
  - Si $D$ est un sous-anneau de $B$, alors $f^{-1}(D)$ est un sous-anneau de $A$.

**Définition-Proposition.** *Soit $A$ un anneau et soit $X$ une partie de $A$. L'idéal* ***engendré*** *par $X$ est le plus petit idéal contenant $X$. Celui-ci existe et il est égal à l'intersection de tous les idéaux contenant $X$.*

**Théorème.** Soit $A$ un anneau et soit $I$ un idéal de $A$. On définit une relation d'équivalence $\sim$ sur $A^2$ en posant

$$a \sim b \iff a - b \in I.$$

L'ensemble quotient $A/\sim$ est alors un anneau pour les lois

$$\overline{a} + \overline{b} = \overline{a + b};$$
$$\overline{a}\,\overline{b} = \overline{ab}$$

où $\overline{a}$ désigne la classe d'équivalence de $a$ dans $A/\sim$ (celle-ci est parfois notée $a + I$). Cet anneau est appelé **anneau quotient** de $A$ par $I$ et noté $A/I$.

L'application $\pi : A \to A/I$ définie par $\pi(a) = \overline{a}$ est un morphisme d'anneaux surjectif, appelé **projection canonique**.

**Théorème** (Théorème de passage au quotient)**.** Soit $f\colon A \to B$ un morphisme d'anneaux. Soit $I$ un idéal de $A$ et soit $J$ un idéal de $B$ tel que $f(I) \subset J$. On note $\pi_A\colon A \to A/I$ et $\pi_B\colon B \to B/I$ les projections canoniques.

Alors il existe un unique morphisme d'anneaux $\bar{f} : A/I \to B/J$ tel que $\bar{f} \circ \pi_A = \pi_B \circ f$ (on a donc $\bar{f}(\overline{a}) = \overline{f(a)}$).

Schématiquement, on a

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle \pi_A}\downarrow & & \downarrow{\scriptstyle \pi_B} \\ A/I & \xrightarrow[\bar{f}]{} & B/J. \end{array}$$

Réciproquement, si un tel $\bar{f}$ existe, alors $f(I) \subset J$.

*Démonstration.* ✦ Supposons que $\bar{f}$ existe. Soit $b \in f(I)$. Alors il existe $a \in I$ tel que $b = f(a)$. On a alors $\pi_B(b) = \pi_B(f(a)) = \bar{f}(\pi_A(a)) = \bar{f}(0) = 0$ donc $b \in \operatorname{Ker} \pi_B = J$. Donc $f(I) \subset J$.

✦ Réciproquement, supposons que $f(I) \subset J$. On doit avoir $\bar{f}(\pi_A(a)) = \pi_B(f(a))$ pour tout $a \in A$. Soit $x \in A/I$. Il existe $a \in A$ tel que $\pi_A(a) = x$. Posons donc $\bar{f}(x) = \pi_B(f(a))$.

Il faut vérifier que $\bar{f}$ est bien définie, c'est-à-dire que si on choisit un autre représentant $a'$ de $x$ dans $A$, on a bien $\pi_B(f(a')) = \pi_B(f(a))$. Puisque $a$ et $a'$ sont deux représentants de $x$ dans $A$, on a $a' - a \in \operatorname{Ker} \pi_A = I$, donc $f(a' - a) \in J$ et donc $\pi_B(f(a' - a)) = 0$. Or $\pi_B$ et $f$ sont des morphismes d'anneaux donc $\pi_B(f(a')) - \pi_B(f(a)) = 0$. On a donc bien défini une application $\bar{f}$.

De plus, $\bar{f}$ est un morphisme d'anneaux. Soit $(x, y) \in (A/I)^2$ et soit $(a, b) \in A^2$ tel que $x = \pi_A(a)$ et $y = \pi_B(b)$. Alors

✧ $\bar{f}(x + y) = \bar{f}(\pi_A(a + b)) = \pi_B(f(a + b)) = \pi_B(f(a)) + \pi_B(f(b)) = \bar{f}(x) + \bar{f}(y)$;

✧ $\bar{f}(xy) = \bar{f}(\pi_A(ab)) = \pi_B(f(ab)) = \pi_B(f(a))\pi_B(f(b)) = \bar{f}(x)\bar{f}(y)$;

✧ $\bar{f}(1) = \bar{f}(\pi_A(1)) = \pi_B(f(1)) = 1$.

Enfin, la condition $\bar{f} \circ \pi_A = \pi_B \circ f$ nous a imposé la définition de $\bar{f}$, donc un tel morphisme d'anneaux est unique. ✓

***Remarque.*** Dans le cas particulier où $J = 0$, la condition "$f(I) \subset J$" devient "$I \subset \operatorname{Ker} f$". Ainsi, si $f : A \to B$ est un morphisme d'anneaux et si $I$ est un idéal de $A$ tel que $I \subset \operatorname{Ker} f$, alors $f$ induit un unique morphisme d'anneaux $\bar{f} : A/I \to B$ tel que $f = \bar{f} \circ \pi_A$ (c'est-à-dire que $\bar{f}(\overline{a}) = f(a)$).

**Théorème** (Premier théorème d'isomorphisme)**.** Soit $f\colon A \to B$ un morphisme d'anneaux. Le morphisme $f$ induit un isomorphisme d'anneaux

$$\bar{f}\colon A/\operatorname{Ker} f \to \operatorname{Im} f.$$

**Théorème** (Deuxième théorème d'isomorphisme)**.** Soit $A$ un anneau, soit $B$ un sous-anneau de $A$ et soit $I$ un idéal de $A$. Alors l'ensemble $B + I = \{b + x;\ (b, x) \in B \times I\}$ est un sous-anneau de $A$, l'ensemble $B \cap I$ est un idéal de $B$ et on a un isomorphisme d'anneaux

$$(B + I)/I \cong B/(B \cap I).$$

**Théorème** (Troisième théorème d'isomorphisme)**.** Soit $A$ un anneau. Soit $I$ un idéal de $A$. Notons $\pi : A \to A/I$ la projection canonique. Soit $J$ un idéal de $A$ contenant $I$ ($I \subset J$). Alors on a un isomorphisme d'anneaux

$$(A/I)/\pi(J) \cong A/J$$

ce que l'on peut également écrire $(A/I)/(J/I) \cong A/J$.

**Définition.** *Soit $A$ un anneau. Soient $I$ et $J$ deux idéaux de $A$. On note $IJ$ l'idéal engendré par les produits $xy$ avec $(x,y) \in I \times J$ et $I+J$ l'idéal engendré par $I \cup J$. On a donc*

$$IJ = \left\{ \sum_{k=1}^{n} x_k y_k;\ n \in \mathbb{N},\ (x_k, y_k) \in I \times J \right\}$$

$$I + J = \left\{ \sum_{k=1}^{n} a_k x_k;\ n \in \mathbb{N},\ x_k \in I \cup J,\ a_k \in A \right\} = \{x + y;\ (x,y) \in I \times J\}.$$

**Théorème** (Théorème Chinois)**.** Soit $A$ un anneau. Soient $I$ et $J$ deux idéaux de $A$ tels que $I + J = A$. Alors

**(a)** $IJ = I \cap J$ ;

**(b)** les anneaux $A/IJ$ et $A/I \times A/J$ sont isomorphes.

*Démonstration.* **(a)** Il est clair que $IJ \subset I \cap J$ (sans hypothèse sur les idéaux $I$ et $J$).
Réciproquement, soit $x \in I \cap J$. Puisque $I + J = A$ il existe $a \in I$ et $b \in J$ tels que $1 = a + b$. On a alors $x = ax + bx$ et $ax \in IJ$ puisque $(a, x) \in I \times J$ et $bx \in IJ$ puisque $(b, x) \in J \times I$. Donc $x \in IJ$.
On a bien $I \cap J = IJ$.

**(b)** Notons $\pi_I \colon A \to I$ et $\pi_J \colon A \to A/J$ les projections canoniques (morphismes d'anneaux) et considérons $\varphi : A \to A/I \times A/J$ définie par $\varphi(x) = (\pi_I(x), \pi_J(x))$. C'est un morphisme d'anneaux.
Il est clair que $\operatorname{Ker} \varphi = I \cap J = IJ$.
Démontrons que $\varphi$ est surjective. Soit $(\overline{y}, \overline{z}) \in A/I \times A/J$, et soit $(x, y) \in A^2$ tel que $\overline{y} = \pi_I(y)$ et $\overline{z} = \pi_J(z)$. On cherche $x \in A$ tel que $\varphi(x) = (\overline{y}, \overline{z})$.
Comme dans la première partie, il existe $a \in I$ et $b \in J$ tels que $1 = a + b$. Posons $x = yb + za$. Alors $\pi_I(x) = \pi_I(yb) = \pi_I(y - ya) = \pi_I(y) = \overline{y}$ et $\pi_J(x) = \pi_J(za) = \pi_J(z - zb) = \pi_J(z) = \overline{z}$ donc $\varphi(x) = (\overline{y}, \overline{z})$.
Finalement, d'après le premier théorème d'isomorphisme, $\varphi$ induit un isomorphisme $\overline{\varphi} : A/IJ \to A/I \times A/J$ (donné par $\varphi(\overline{x}) = (\pi_I(x), \pi_J(x))$). ✓

**Corollaire.** Soit $A$ un anneau principal. Soient $m$ et $n$ deux éléments de $A$ premiers entre eux. Alors les anneaux $A/(m) \times A/(n)$ et $A/(mn)$ sont isomorphes.

***Remarque.*** L'isomorphisme est donné par $\overline{\varphi}(\overline{x}) = (\pi_m(x), \pi_n(x))$ où $\pi_m : A \to A/(m)$ et $\pi_n : A \to A/(n)$ sont les projections canoniques. Pour exprimer $\overline{\varphi}^{-1}$, on applique la propriété de Bézout, qui donne $(u, v) \in A^2$ tel que $mu + nv = 1$. Alors $\overline{\varphi}^{-1}(\pi_m(y), \pi_n(z)) = \overline{zmu + ynv}$.

Ceci permet, dans le cas où $A = \mathbb{Z}$, de résoudre des systèmes de congruences du type

$$\begin{cases} x \equiv a \pmod{m} \\ y \equiv b \pmod{n} \end{cases}$$

avec $m$ et $n$ deux entiers premiers entre eux.

# CHAPITRE 1

# *Rappels et compléments sur les anneaux*

## I IDÉAUX PREMIERS ET MAXIMAUX.

Dans tout ce cours, anneau signifie anneau commutatif unitaire, sauf mention expresse du contraire.

**Définition 1.** *Soient $A$ un anneau et $I$ un idéal de $A$.*

**(1)** *L'idéal $I$ est dit **premier** s'il est distinct de $A$ et vérifie la condition suivante : pour tous $a, b \in A$, $ab \in I \Longrightarrow a \in I$ ou $b \in I$.*

**(2)** *L'idéal $I$ est dit **maximal** s'il est distinct de $A$ et vérifie la condition suivante : pour tout idéal $J$ de $A$, $I \subset J \subset A \Longrightarrow J = I$ ou $J = A$.*

On peut caractériser la primalité ou la maximalité de l'idéal $I$ d'un anneau $A$ à l'aide de l'anneau quotient $A/I$.

**Proposition 2.** Soient $A$ un anneau et $I$ un idéal de $A$.

**(1)** L'idéal $I$ est premier si et seulement si l'anneau $A/I$ est intègre.

**(2)** L'idéal $I$ est maximal si et seulement si l'anneau $A/I$ est un corps.

*Démonstration.* Exercice (L3). ✓

***Remarque.*** ✦ Il est clair d'après la proposition 2 que tout idéal maximal est premier.

✦ Par contre, il est facile de démontrer que $\{0\}$ est un idéal premier et non maximal de l'anneau $\mathbb{Z}$. (En effet, $\mathbb{Z}/\{0\} \cong \mathbb{Z}$ est intègre mais n'est pas un corps).

**Proposition 3.** Soient $A$ un anneau, $I$ un idéal de $A$ et $\pi : A \longrightarrow A/I$ la projection canonique. On note $\mathbf{I}_{A/I}$ l'ensemble de tous les idéaux de $A/I$ et $\mathbf{J}_{A,I}$ l'ensemble de tous les idéaux de $A$ contenant $I$. Alors :

**(1)** les applications

$$\begin{array}{ccc} \mathbf{J}_{A,I} & \xrightarrow{\alpha} & \mathbf{I}_{A/I} \\ K & \mapsto & \pi(K) \end{array} \quad \text{et} \quad \begin{array}{ccc} \mathbf{I}_{A/I} & \xrightarrow{\beta} & \mathbf{J}_{A,I} \\ L & \mapsto & \pi^{-1}(L) \end{array}$$

sont des bijections réciproques l'une de l'autre. Elles établissent donc une correspondance bijective entre idéaux de $A/I$ et idéaux de $A$ contenant $I$.

**(2)** la correspondance bijective ci-dessus induit des correspondances bijectives entre idéaux premiers (resp. maximaux) de $A/I$ et idéaux premiers (resp. maximaux) de $A$ contenant $I$.

*Démonstration.* **(1)** Puisque $\pi$ est un morphisme d'anneaux, $\pi^{-1}(L)$ est un idéal de $A$ pour tout idéal $L$ de $A/I$. De plus, 0 est dans $L$ donc $I = \pi^{-1}(\{0\}) \subset \pi^{-1}(L)$.
Puisque $\pi$ est un morphisme d'anneaux surjectif, $\pi(K)$ est un idéal de $A/I$ pour tout idéal $K$ de $A$.
On a $\alpha \circ \beta = \mathrm{id}_{\mathbf{I}_{A/I}}$ car $\pi \circ \pi^{-1}(L) = L$ pour tout idéal $L$ de $A/I$.
Il reste à vérifier que $\beta \circ \alpha = \mathrm{id}_{\mathbf{J}_{A,I}}$ pour tout idéal $K$ de $A$ contenant $I$. Soit $K$ un tel idéal. On a toujours $\pi^{-1}(\pi(K)) \supset K$. Soit maintenant $x \in \pi^{-1}(\pi(K))$. Alors $\pi(x) \in \pi(K)$ donc il existe $a \in K$ tel que $\pi(x) = \pi(a)$. Mais alors $x - a \in I \subset K$ donc $x \in K$. On a donc bien $\pi^{-1}(\pi(K)) = K$.

**(2)** Le troisième théorème d'isomorphisme précise que pour tout idéal $K$ de $A$ contenant $I$, on a un isomorphisme d'anneaux

$$A/K \cong (A/I)/\pi(K).$$

Ainsi, d'après la proposition 2, pour tout idéal $K$ de $A$ contenant $I$, $K$ est premier (resp. maximal) dans $A$ si et seulement si $\pi(K)$ est premier (resp. maximal) dans $A/I$. ✓

Il est clair par définition que l'anneau nul ne contient pas d'idéaux premiers (et donc pas d'idéaux maximaux). La première question légitime est alors la suivante : étant donné un anneau non nul $A$, existe-t-il toujours des idéaux premiers, des idéaux maximaux, dans $A$ ? La réponse est donnée par le *théorème de Krull*.

## II Ensembles ordonnés et lemme de Zorn

Ce lemme est utilisé pour faire certaines démonstrations où une récurrence est impossible (si l'ensemble d'indices n'est pas dénombrable). Il est équivalent à l'axiome du choix (indépendant des autres axiomes, Cohen 1963). Vous le verrez également dans le cours de topologie.

***Axiome du choix.*** Un produit d'une famille non vide d'ensembles non vides est non vide. Autrement dit, si $(A_i)_{i\in I}$ est une famille non vide d'ensembles non vides, on peut choisir simultanément $x_i \in A_i$ pour tout $i \in I$.

Nous nous contenterons d'énoncer le lemme de Zorn, et admettrons qu'il est équivalent à l'axiome du choix.

### II.1. Lemme de Zorn

**Définition 4.** *Soit $E$ un ensemble. Un **ordre** sur $E$ est une relation binaire $\preccurlyeq$, réflexive, antisymétrique et transitive, c'est-à-dire telle que :*

- ✦ $\forall\, x \in E,\ x \preccurlyeq x$ ;
- ✦ $\forall\, x, y \in E$, *si* $x \preccurlyeq y$ *et* $y \preccurlyeq x$, *alors* $x = y$ ;
- ✦ $\forall\, x, y, z \in E$, *si* $x \preccurlyeq y$ *et* $y \preccurlyeq z$ *alors* $x \preccurlyeq z$.

*On dit alors que l'ensemble $(E, \preccurlyeq)$ est un **ensemble ordonné**.*

***Remarque.*** Il est clair que, si $F$ est un sous-ensemble de l'ensemble $E$ et si $\preccurlyeq$ est un ordre sur $E$, alors $\preccurlyeq$ induit un ordre sur $F$.

**Définition 5.** *Si $(E, \preccurlyeq)$ est un ensemble ordonné et si, pour tous $x, y \in E$, on a $x \preccurlyeq y$ ou $y \preccurlyeq x$, on dit que $\preccurlyeq$ est un **ordre total** ou que $(E, \preccurlyeq)$ est un **ensemble totalement ordonné**. Dans le cas contraire, un dit que $\preccurlyeq$ est un **ordre partiel** ou que $(E, \preccurlyeq)$ est un **ensemble partiellement ordonné**.*

**Définition 6.** *Soit $(E, \preccurlyeq)$ un ensemble ordonné.*

- ✦ *Un **élément maximal** de $(E, \preccurlyeq)$ est un élément $x \in E$ tel que, pour tout $y \in E$, si $x \preccurlyeq y$, alors $x = y$.*
- ✦ *Soit $F$ un sous-ensemble de $E$. Un **majorant** de $F$ dans $E$ est un élément $m$ de $E$ tel que pour tout $x \in F$, $x \preccurlyeq m$.*
- ✦ *On dit que $(E, \preccurlyeq)$ est un **ensemble inductif** si tout sous-ensemble non-vide $F$ de $E$ tel que $(F, \preccurlyeq)$ soit totalement ordonné admet un majorant dans $E$.*

***Remarque.*** Soient $A$ un anneau et $\mathcal{E}$ l'ensemble de tous les idéaux de $A$ distincts de $A$. L'inclusion définit une relation d'ordre (partiel) sur $\mathcal{E}$ et on note $(\mathcal{E}, \subset)$ l'ensemble ordonné ainsi obtenu. Alors, $I$ est un idéal maximal de $A$ si et seulement si $I$ est un élément maximal de $(\mathcal{E}, \subset)$.

**Théorème 7** (Lemme de Zorn)**.** Soit $(E, \preccurlyeq)$ un ensemble ordonné, inductif et non vide. Alors il existe un élément maximal dans $E$.

*Démonstration.* (admis) ✓

## II.2. Applications

**Théorème 8.** Soit $\mathbb{K}$ un corps. Tout espace vectoriel non nul sur $\mathbb{K}$ a une base.

*Démonstration.* Soit $E$ un espace vectoriel sur $\mathbb{K}$. Soit $\mathcal{S}$ l'ensemble des parties libres de $E$ muni de l'ordre fourni par l'inclusion. Comme $E \neq \{0\}$, on a $\mathcal{S} \neq \varnothing$.
$\mathcal{S}$ muni de cet ordre est inductif : soit $(S_i)_{i\in I}$ une partie totalement ordonnée de $\mathcal{S}$. Alors $\cup_{i\in I} S_i$ est libre. En effet, soit $\sum_{j\in J} \lambda_j x_j = 0$ une relation de dépendance avec $J$ une partie finie de $I$, $x_j \in S_j$ et $\lambda_j \in \mathbb{K}$. Puisque $J$ est fini et $(S_i)_{i\in I}$ est totalement ordonné, on peut choisir $i_0 \in J$ tel que $S_j \subset S_{i_0}$ pour tout $j \in J$. Alors $x_j \in S_{i_0}$ pour tout $j \in J$. Or $S_{i_0}$ est libre, donc $\lambda_j = 0$ pour tout $j \in J$.
D'après le lemme de Zorn, il existe une partie libre maximale dans $\mathcal{S}$, notons-la $B$. Il reste à démontrer que $B$ est un système générateur : sinon, il existe $y \in E$ tel que $y \notin \text{vect}\{B\}$, donc $\{y\} \cup B$ est libre, ce qui contredit la maximalité de $B$. ✓

**Théorème 9** (Théorème de Krull)**.** Soit $A$ un anneau unitaire. Alors tout idéal de $A$ distinct de $A$ est contenu dans un idéal maximal.

*Démonstration.* Soit $I$ un idéal de $A$ distinct de $A$. Soit $\mathcal{S}$ l'ensemble des idéaux de $A$ qui contiennent $I$ et qui sont distincts de $A$, ordonné par l'inclusion. Puisque $I \in \mathcal{S}$, cet ensemble est non vide. De plus, $\mathcal{S}$ muni de cet ordre est inductif : soit $(I_j)_{j\in J}$ une famille totalement ordonnée d'idéaux qui contiennent $I$ et qui sont distincts de $A$. Alors $\cup_{j\in J} I_j$ est encore un idéal distinct de $A$ et contenant $I$. En effet, $1 \notin \cup_{j\in J} I_j$ donc $\cup_{j\in J} I_j \neq A$. Il est clair que $I \subset \cup_{j\in J} I_j$. De plus, si $x$ et $y$ sont dans $\cup_{j\in J} I_j$, il existe $j_0$ tel que $x$ et $y$ soient dans $I_{j_0}$ (puisque la famille des $I_j$ est totalement ordonnée). Alors $x + y \in I_{j_0} \subset \cup_{j\in J} I_j$ et $ax \in I_{j_0} \subset \cup_{j\in J} I_j$ pour tout $a \in A$, donc c'est bien un idéal.
D'après le lemme de Zorn, $\mathcal{S}$ contient un élément maximal. C'est un idéal maximal de $A$ contenant $I$. ✓

***Remarque.*** Vous verrez également le théorème de Hahn-Banach qui se démontre à l'aide du lemme de Zorn.

# III Corps des fractions d'un anneau intègre

Soit $A$ un anneau *intègre*. Notons $S = A \setminus \{0\}$.

On veut construire un corps $K$ contenant $A$ comme sous-anneau (d'où la nécessité d'avoir un anneau intègre) et qui soit minimal pour cette propriété. La construction est la même que celle de $\mathbb{Q}$ à partir de $\mathbb{Z}$ : on va considérer un ensemble de quotients de la forme $\frac{a}{s}$ avec $(a, s) \in A^2$ et $s \neq 0$, et le munir d'une structure d'anneau (qui se trouvera être un corps).

On définit une relation d'équivalence sur $A \times S$ par

$$(a, s) \sim (a', s') \iff as' - a's = 0.$$

C'est bien une relation d'équivalence :

- ✦ $(a, s) \sim (a, s)$ car $as - sa = 0$.
- ✦ Si $(a, s) \sim (a', s')$, alors $as' - a's = 0$, donc $a's - as' = 0$ et donc $(a', s') \sim (a, s)$.
- ✦ Si $(a, s) \sim (a', s')$ et $(a', s') \sim (a'', s'')$, alors $as' - a's = 0$ et $a's'' - a''s' = 0$. Donc $as's'' - a'ss'' + a's''s - a''s's = 0$ et donc $as'' - a''s = 0$. Donc $(a, s) \sim (a'', s'')$.

On forme le quotient $A \times S/\sim$, dont les éléments sont notés $\frac{a}{s}$. On note ce quotient $\mathrm{Frac}(A)$.

**Définition-Proposition 10.** $\mathrm{Frac}(A)$ *est un corps (commutatif), dit* ***corps des fractions*** *de* $A$*, pour les opérations suivantes :*

- $\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}$
- $\frac{a}{s}\frac{a'}{s'} = \frac{aa'}{ss'}$.

*L'unité est* $\frac{1}{1}$ *et l'élément nul est* $\frac{0}{1}$.

*Démonstration.* Les opérations sont bien définies : si $\frac{a}{s} = \frac{a_1}{s_1}$ et $\frac{a'}{s'} = \frac{a'_1}{s'_1}$, on doit vérifier que

$$\frac{a_1 s'_1 + a'_1 s_1}{s_1 s'_1} = \frac{as' + a's}{ss'} \qquad \text{(III.1)} \qquad \text{et que} \qquad \frac{aa'}{ss'} = \frac{a_1 a'_1}{s_1 s'_1}. \qquad \text{(III.2)}$$

Par hypothèse, on a $a_1 s - a s_1 = 0$ et $a'_1 s' - a' s'_1 = 0$. On a donc $0 = (a_1 s - a s_1)s' s'_1 + (a'_1 s' - a' s'_1)ss_1 = ss'(s'_1 a_1 + s_1 a'_1) - s_1 s'_1(as' + sa')$, ce qui démontre (III.1), et $0 = (a_1 s - a s_1)a'_1 s' + (a'_1 s' - a' s'_1)as_1 = a_1 a'_1 ss' - aa' s_1 s'_1$, ce qui démontre (III.2).

Il reste à vérifier que $A$ est bien un anneau, commutatif et unitaire, et que tout élément non nul est inversible (exercice). ✓

***Remarque.*** L'application $\varphi : A \to \mathrm{Frac}(A)$ définie par $\varphi(a) = \frac{a}{1}$ est un morphisme d'anneaux injectif. Ainsi $A$ peut être identifié à un sous-anneau de $\mathrm{Frac}(A)$.

**Proposition 11.** Soit $A$ un anneau intègre et soit $\varphi : A \to \mathrm{Frac}(A)$ le morphisme d'anneaux ci-dessus. Pour tout anneau $B$ et pour tout morphisme d'anneaux $f : A \to B$ tel que pour tout $s \in S$, $f(s)$ est inversible dans $B$ (autrement dit, $f(S) \subset B^\times$), il existe un unique morphisme d'anneaux $g : \mathrm{Frac}(A) \to B$ tel que $g \circ \varphi = f$.

*Démonstration.* Commençons par démontrer l'unicité. Supposons que $g$ existe. Alors on doit avoir $f(a) = g(\varphi(a)) = g\left(\frac{a}{1}\right) = g\left(\frac{a}{s}\frac{s}{1}\right) = g\left(\frac{a}{s}\right)g\left(\frac{s}{1}\right) = g\left(\frac{a}{s}\right)g(\varphi(s)) = g\left(\frac{a}{s}\right)f(s)$, d'où l'unicité pour $g\left(\frac{a}{s}\right)$.

Maintenant, posons $g\left(\frac{a}{s}\right) = (f(s))^{-1} f(a)$. Alors

- $g$ est bien défini : si $\frac{a}{s} = \frac{a'}{s'}$, alors $as' - a's = 0$, d'où $f(a')f(s) - f(a)f(s') = 0$. En multipliant par $f(s)^{-1}f(s')^{-1}$, on obtient $f(s)^{-1}f(a) = f(s')^{-1}f(a')$.
- $g$ est un morphisme. En effet, on a
  - $g\left(\frac{a}{s} + \frac{a'}{s'}\right) = g\left(\frac{as' + a's}{ss'}\right) = f(as' + a's)f(ss')^{-1} = f(a)f(s')f(s)^{-1}f(s')^{-1} + f(a')f(s)f(s)^{-1}f(s')^{-1} = f(a)f(s)^{-1} + f(a')f(s')^{-1} = g\left(\frac{a}{s}\right) + g\left(\frac{a'}{s'}\right)$;
  - $g\left(\frac{a}{s}\frac{a'}{s'}\right) = g\left(\frac{aa'}{ss'}\right) = f(aa')f(ss')^{-1} = f(a)f(a')f(s)^{-1}f(s')^{-1} = f(a)f(s)^{-1}f(a')f(s')^{-1} = g\left(\frac{a}{s}\right)g\left(\frac{a'}{s'}\right)$;
  - $g\left(\frac{1}{1}\right) = f(1)f(1)^{-1} = 1$.
- $g \circ \varphi = f : g \circ \varphi(a) = g\left(\frac{a}{1}\right) = f(1)^{-1}f(a) = f(a)$. ✓

***Remarque.*** Le morphisme $g$ est nécessairement injectif.

**Conséquence 12** ("Minimalité" du corps des fractions)**.** Soit $K$ un corps contenant $A$ comme sous-anneau. Alors $\mathrm{Frac}(A)$ est (s'identifie à) un sous-corps de $K$.

Autrement dit, $\mathrm{Frac}(A)$ est le plus petit corps contenant $A$.

Pour vérifier cela, il suffit d'appliquer la proposition avec $f$ l'inclusion de $A$ dans $K$.

***Exemple.*** Si $A = \mathbb{Z}$ on obtient $\mathrm{Frac}(A) = \mathbb{Q}$.

***Exemple.*** Soit $K$ un corps. Le corps des fractions de l'anneau de polynômes $K[X]$ est le corps des fractions rationnelles $K(X)$.

## IV Rappels d'arithmétique.

Dans cette partie, on étudie et rappelle des propriétés arithmétiques des anneaux, c'est-à-dire des propriétés des anneaux liées à la divisibilité.

Dans toute cette partie, sauf mention expresse du contraire, $A$ désigne un anneau (commutatif, unitaire) intègre (et donc non nul). On note alors $A^\times$ le groupe des éléments inversibles de $A$.

**Définition 13.** *Soient $a, b \in A$.*

**(1)** *On dit que $a$ **divise** $b$, et on note $a|b$, s'il existe un élément $c$ de $A$ tel que $b = ac$.*

**(2)** *On dit que $a$ et $b$ sont **associés** si $a|b$ et $b|a$. On note $a \sim b$.*

***Remarque.*** Soient $a, b \in A$. Les points suivants sont clairs :

**(1)** $a$ divise $b$ si et seulement si $(b) \subset (a)$ ;

**(2)** $a$ et $b$ sont associés si et seulement si $(a) = (b)$ ;

**(3)** $a$ et $b$ sont associés si et seulement s'il existe $u \in A^\times$ tel que $a = ub$.

**Définition 14.** *Soit $p$ un élément de $A$.*

✦ *On dit que $p$ est **irréductible** s'il satisfait aux conditions suivantes :*

- **(i)** $p \notin A^\times$ ;
- **(ii)** *$p = ab$ avec $a, b \in A$ entraîne que $a$ ou $b$ est un élément inversible.*

✦ *On dit que $p$ est **premier** s'il n'est pas nul et si l'idéal engendré $(p)$ est premier.*

***Remarque.*** **(1)** Le produit d'un élément irréductible par un élément inversible est un élément irréductible.

**(2)** L'élément 0 n'est pas irréductible car $0 = 0.0$. Ainsi, un corps n'a pas d'éléments irréductibles.

**(3)** Soit $p$ un élément de $A$ ; $p$ est irréductible si et seulement si :

- **(i)** $p \notin A^\times$ ;
- **(ii)** $p \neq 0$ et les seuls diviseurs de $p$ sont les éléments inversibles de $A$ et les éléments de $A$ associés à $p$.

**(4)** Soit $p \in A$ un élément non nul. Alors $p$ est premier si et seulement s'il n'est pas inversible et si pour tout $(a, b) \in A^2$, $p|ab \Rightarrow (p|a$ ou $p|b)$.

**(5)** Soit $p \in A$ ; si $p$ est premier, alors $p$ est irréductible.

**Définition 15.** *Soient $I$ un ensemble non vide et $(a_i)_{i\in I}$ une famille d'éléments de $A$.*

**(1)** *On dit que $a \in A$ est un **diviseur** (resp. **multiple**) **commun** de $(a_i)_{i\in I}$ si, pour tout $i \in I$, $a|a_i$ (resp. $a_i|a$).*

**(2)** *On suppose que les $a_i$, $i \in I$, ne sont pas tous nuls. On dit que $d \in A$ est un **plus grand commun diviseur** (en abrégé pgcd) de $(a_i)_{i\in I}$ si c'est un divieur commun de $(a_i)_{i\in I}$ et si tout diviseur commun de $(a_i)_{i\in I}$ divise $d$.*

**(3)** *On suppose que tous les $a_i$, $i \in I$, sont non nuls. On dit que $m \in A$ est un* ***plus petit commun multiple*** *(en abrégé ppcm) de $(a_i)_{i\in I}$ si c'est un multiple commun de $(a_i)_{i\in I}$ qui divise tout multiple commun de $(a_i)_{i\in I}$.*

**(4)** *On dit que les $a_i$, $i \in I$ sont* ***premiers entre eux*** *si $1$ est un pgcd de $(a_i)_{i\in I}$.*

***Remarque.*** Soit $I$ un ensemble non vide et $\mathcal{A} = (a_i)_{i\in I}$ une famille d'éléments de $A$. On suppose que les $a_i$, $i \in I$, ne sont pas tous nuls (resp. sont tous non nuls). On démontre facilement que si $a \in A$ est un pgcd (resp. ppcm) de $\mathcal{A}$, un élément $b$ est un pgcd (resp. ppcm) de $\mathcal{A}$ si et seulement s'il est associé à $a$.

On notera donc $d \sim \text{pgcd}(a_i, i \in I)$ (resp. $m \sim \text{ppcm}(a_i, i \in I)$) si $d$ (resp. $m$) est un pgcd (resp. ppcm) de $(a_i)_{i\in I}$.

***Remarque.*** Soit $a \in A \setminus \{0\}$ ; $a$ et $0$ sont premiers entre eux si et seulement si $a$ est un élément inversible de $A$.

**Proposition 16.** Soit $(a, b) \in A^2$, $ab \neq 0$. Soit $d$ un pgcd de $a$ et $b$ et soit $m$ un ppcm de $a$ et $b$. Alors $ab$ et $dm$ sont associés.

*Démonstration.* Puisque $a$ et $b$ divisent $ab$, leur ppcm $m$ divise $ab$. Posons $ab = me$ pour un $e \in A$. Pour conclure, il suffit de démontrer que $e$ est associé à $d$.
Posons $a = da'$, $b = db'$, et $m = aa'' = bb''$.
On a $ab = me = aa''e$ donc $b = a''e$ et donc $e$ divise $b$. De même, $e$ divise $a$, donc $e$ divise $d$ qui est un pgcd de $a$ et $b$.
Puisque $d$ divise $a$ et $b$, il divise $ab$, posons $ab = dx$. On a alors $dx = ab = da'b = dab'$ donc $x = ab' = a'b$ et donc $a$ et $b$ divisent tous deux $x$, donc $m$ divise $x$. Posons $x = my$. On a alors $me = ab = dx = dmy$ donc $e = dy$ est un multiple de $d$.
On en déduit finalement que $d$ est associé à $e$ et donc que $ab = me$ est associé à $md$. ✓

**Proposition 17.** Soit $a$ un élément irréductible de $A$ et $b$ un élément de $A$. Alors, $a$ et $b$ sont premiers entre eux si et seulement si $a$ ne divise pas $b$.

*Démonstration.* Si $a$ divise $b$, alors $a$ est un diviseur commun à $a$ et $b$ qui n'est pas inversible, donc $a$ et $b$ ne sont pas premiers entre eux.
Si $a$ et $b$ ne sont pas premiers entre eux, ils admettent un diviseur commun $x$ qui n'est pas inversible. Or $x$ divise $a$ qui est irréductible donc $x$ est associé à $a$. Comme $x$ divise $b$, on en déduit que $a$ divise $b$. ✓

# V Anneaux factoriels

## V.1. Anneaux factoriels.

**Définition 18.** **(1)** *On dit que $A$ satisfait la condition (E) si tout élément non nul et non inversible $a \in A$ admet une décomposition en produit d'éléments irréductibles, c'est-à-dire qu'il existe $r \in \mathbb{N}^*$ et des éléments irréductibles $p_1, \dots, p_r$ tels que $a = p_1 \dots p_r$.*

**(2)** *On dit que $A$ satisfait la condition (U) si pour tout élément non nul et non inversible de $A$, une décomposition en produit d'éléments irréductibles (si elle existe) est essentiellement unique, c'est-à-dire que, si $a = p_1 \dots p_r = q_1 \dots q_s$ où $r, s \in \mathbb{N}^*$ et $p_1, \dots, p_r, q_1, \dots, q_s$ sont des éléments irréductibles de $A$, alors $r = s$ et il existe $\sigma \in \mathfrak{S}_r$ tel que, pour $1 \leqslant i \leqslant r$, $p_i$ et $q_{\sigma(i)}$ soient associés.*

**(3)** *On dit que $A$ est* ***factoriel*** *s'il est intègre et s'il satisfait aux conditions (E) et (U).*

***Exemple.*** Tout corps est un anneau factoriel.

On va donner une définition équivalente d'un anneau factoriel, dans laquelle on a vraiment unicité de la décomposition. Pour cela on introduit la définition suivante.

**Définition 19.** *Soit $A$ un anneau. Une partie $\mathcal{P}$ de $A$ est un* ***système de représentants des irréductibles*** *de $A$ si c'est un système de représentants des classes d'équivalence des éléments irréductibles de $A$ pour la relation $\sim$ (association), autrement dit,*

- ✦ *tout élément de $\mathcal{P}$ est irréductible ;*
- ✦ *si $a \in A$ est irréductible alors il existe $p \in \mathcal{P}$ tel que $a \sim p$ ;*
- ✦ *deux éléments distincts de $\mathcal{P}$ ne sont pas associés.*

***Exemple.*** L'anneau $\mathbb{Z}$ est factoriel (les éléments irréductibles de $\mathbb{Z}$ sont les nombres premiers et leurs opposés). Si $A = \mathbb{Z}$, on peut prendre l'ensemble des nombres premiers (positifs) pour $\mathcal{P}$, ou bien l'ensemble des opposés de nombres premiers.

**Définition-Proposition 20.** *Un anneau $A$ est factoriel si, et seulement s'il est intègre et si tout élément non nul $a \in A$ se décompose de manière unique sous la forme $a = u_a \prod_{p\in\mathcal{P}} p^{v_p(a)}$ avec $u_a \in A^\times$, $v_p(a) \in \mathbb{N}$ pour tout $p \in \mathcal{P}$ et les $v_p(a)$ sont nuls sauf pour un nombre fini de $p \in \mathcal{P}$.*
*Pour $p \in \mathcal{P}$, l'entier $v_p(a)$ est appelé* ***valuation $p$-adique*** *de $a$.*

*Démonstration.* C'est clair. ✓

**Propriétés 21.** Soit $A$ un anneau factoriel et soient $a$ et $b$ deux éléments non nuls de $A$. Alors
**(1)** pour tout $p \in \mathcal{P}$ on a $v_p(ab) = v_p(a) + v_p(b)$.
**(2)** $a$ divise $b$ si, et seulement si, $v_p(a) \leqslant v_p(b)$ pour tout $p \in \mathcal{P}$.
**(3)** $a$ et $b$ sont premiers entre eux si, et seulement si, $v_p(a)v_p(b) = 0$ pour tout $p \in \mathcal{P}$.

*Démonstration.* **(1)** On a $ab = u_a u_b \prod_{p\in\mathcal{P}} p^{v_p(a)+v_p(b)} = u_{ab} \prod_{p\in\mathcal{P}} p^{v_p(ab)}$. Par unicité de la décomposition on en déduit que $u_{ab} = u_a u_b$ et $v_p(ab) = v_p(a) + v_p(b)$ pour tout $p \in \mathcal{P}$.

**(2)** ($\Leftarrow$) Si $v_p(a) \leqslant v_p(b)$ pour tout $i$, alors $b = au_a^{-1}u_b \prod_{p\in\mathcal{P}} p^{v_p(b)-v_p(a)}$ donc $a$ divise $b$. *[Les hypothèses sur $A$ ne servent pas ici.]*

($\Rightarrow$) Si $b = ac$, alors pour tout $p \in \mathcal{P}$ on a $v_p(b) = v_p(a) + v_p(c) \geqslant v_p(a)$.

**(3)** ($\Rightarrow$) S'il existe $p$ tel que $v_p(a)v_p(b) \neq 0$, alors $p$ divise $a$ et $b$ donc $a$ et $b$ ne sont pas premiers entre eux. *[Les hypothèses sur $A$ ne servent pas ici.]*

($\Leftarrow$) Supposons que l'on ait, pour tout $p \in \mathcal{P}$, $v_p(a)v_p(b) = 0$. Soit $d$ un diviseur commun de $a$ et $b$. On a donc $0 \leqslant v_p(d) \leqslant \min(v_p(a), v_p(b)) = 0$ pour tout $p \in \mathcal{P}$ donc $v_p(d) = 0$ pour tout $p \in \mathcal{P}$ et donc $d \in A^\times$. ✓

Dans un anneau intègre quelconque, les pgcd et ppcm n'existent pas toujours. Cependant, dans un anneau factoriel, c'est le cas.

**Proposition 22.** Supposons $A$ factoriel. Si $a_1, \ldots, a_r$ ($r \in \mathbb{N}^*$) sont des éléments non nuls de $A$, alors ils admettent un pgcd et un ppcm.

*Démonstration.* Posons $a_i = u_{a_i} \prod_{p\in\mathcal{P}} p^{v_p(a_i)}$ pour tout $i$.

Pour tout $p \in \mathcal{P}$, posons $\delta_p = \min\{v_p(a_i); i \in [\![1\,;r]\!]\}$ et considérons $d = \prod_{p\in\mathcal{P}} p^{\delta_p}$ (notons que c'est bien le produit d'un nombre fini d'éléments distincts de 1).

- ✦ Il est clair que $d$ est un diviseur de chacun des $a_i$ (pour tout $p \in \mathcal{P}$ on a $v_p(d) = \delta_p \leqslant v_p(a_i)$).
- ✦ Soit $x \in A$ un diviseur commun des $a_i$. Puisque $x$ divise tous les $a_i$, on a $v_p(x) \leqslant \min\{v_p(a_i); i \in [\![1\,;r]\!]\} = \delta_p = v_p(d)$ pour tout $p \in \mathcal{P}$, donc $x$ divise $d$.

L'élément $d$ est donc bien un pgcd des $a_i$.

Pour le ppcm on fait un raisonnement similaire.
Pour tout $p \in \mathcal{P}$, posons $\mu_p = \max\{v_p(a_i); i \in [\![1\,;r]\!]\}$ et considérons $m = \prod_{p\in\mathcal{P}} p^{\mu_p}$.

- ✦ Il est clair que $m$ est un multiple de tous les $a_i$.

✦ Soit $y \in A$ un multiple commun des $a_i$. Puisque $a_i$ divise $y$ pour tout $i$, on a $v_p(y) \geqslant \max\{v_p(a_i); i \in [\![1;r]\!]\} = \mu_p = v_p(m)$ pour tout $p \in \mathcal{P}$, donc $m$ divise $y$.

L'élément $m$ est donc bien un ppcm de $a$ et $b$. ✓

**Lemme 23.** Soit $A$ un anneau factoriel, soit $\{a_i; i \in I\}$ une famille finie d'éléments non tous nuls de $A$ et soit $b \in A$, $b \neq 0$.

**(1)** Soit $d$ un pgcd des $a_i$. Alors $bd$ est un pgcd des $ba_i$, $i \in I$.

**(2)** Si $d$ est un pgcd des $a_i$ alors pour tout $i \in I$ il existe $a_i' \in A$ tel que les $a_i'$, $i \in I$, soient premiers entre eux et $a_i = da_i'$ pour tout $i \in I$.

*Démonstration.* **(1)** Soit $c$ un pgcd des $ba_i$. Il est clair que $bd$ est un diviseur commun des $ba_i$ donc $bd$ divise $c$. Réciproquement, puisque $b|ba_i$ pour tout $i \in I$, on en déduit que $b|c$ donc $c = bc'$ avec $c' \in A$. Puisque $c = bc'|ba_i$ pour tout $i \in I$, on a $c'|a_i$ pour tout $i$ et donc $c'|d$. Finalement, $c = bc'$ divise $bd$. Donc $bd \sim c$ est un pgcd des $ba_i$.

*Remarquons qu'on n'utilise pas ici le fait que $A$ est factoriel, mais seulement le fait que les $a_i$, $i \in I$, et les $ba_i$, $i \in I$, admettent des pgcd. Mais on peut aussi utiliser les décompositions en produits de facteurs irréductibles pour démontrer ce résultat, on utilise alors vraiment le fait que $A$ est factoriel.*

**(2)** Puisque $d$ est un diviseur commun des $a_i$, il existe $a_i'$ tel que $a_i = da_i'$ pour tout $i \in I$. D'après ce qui précède, si $d'$ est un pgcd des $a_i'$, alors $dc$ est un pgcd des $a_i$ donc il est associé à $d$ et donc $c$ est inversible. ✓

**Théorème 24.** Soit $A$ un anneau intègre satisfaisant la condition (E). Alors les assertions suivantes sont équivalentes :

**(a)** $A$ est factoriel

**(b)** $A$ satisfait la condition (U).

**(c)** Pour tout triplet $(a,b,c)$ d'éléments de $A$ tel que $a \neq 0$, si $a$ et $b$ sont premiers entre eux et si $a|bc$, alors $a|c$ (condition de Gauss).

**(d)** Pour tout triplet $(a,b,c)$ d'éléments de $A$, si $a$ est irréductible et divise $bc$, alors $a$ divise $b$ ou $a$ divise $c$ (condition d'Euclide).

**(e)** Pour $p$ dans $A$, $p$ est premier si et seulement si $p$ est irréductible (condition de primalité).

*Démonstration.* **(a)⇔(b)** par définition d'un anneau factoriel.

**(b)⇒(c)** Soient $a$ et $b$ premiers entre eux divisant $bc$.

✦ Si $b = 0$, puisque $a$ et $b$ sont premiers entre eux on en déduit que $a$ est inversible (voir remarque page 10) donc $a$ divise $c$.

✦ Si $c = 0$, alors $a$ divise $c$.

✦ Supposons donc que $a$, $b$ et $c$ ne sont pas nuls. Puisque $A$ est factoriel, on peut décomposer $a$, $b$ et $c$ de manière unique sous la forme $a = u_a \prod_{p\in\mathcal{P}} p^{v_p(a)}$, $b = u_b \prod_{p\in\mathcal{P}} p^{v_p(b)}$ et $c = u_c \prod_{p\in\mathcal{P}} p^{v_p(c)}$. Alors, puisque $a$ et $b$ sont premiers entre eux, on a $v_p(a)v_p(b) = 0$ pour tout $p \in \mathcal{P}$. Puisque $a$ divise $bc$ on a $v_p(a) \leqslant v_p(b) + v_p(c)$ pour tout $p \in \mathcal{P}$. On en déduit facilement que $v_p(a) \leqslant v_p(c)$ pour tout $p \in \mathcal{P}$ et donc que $a$ divise $c$.

**(c)⇒(d)** Soit $a$ un élément irréductible divisant $bc$. Si $a$ ne divise pas $b$, alors d'après la proposition **17** $a$ et $b$ sont premiers entre eux, donc d'après la condition de Gauss $a$ divise $c$.

**(d)⇒(e)** C'est clair.

**(e)⇒(b)** Soit $a \in A$ et supposons que $a = p_1 \dots p_m = q_1 \dots q_n$ avec $m \leqslant n$. On raisonne par récurrence sur $m$.

✦ Si $m = 1$, on a $a = p_1 = q_1 \dots q_n$. Donc $q_1 \mid p_1$, $p_1$ est irréductible et $q_1 \notin A^\times$, donc $q_1 = up_1$ avec $u \in A^\times$. Donc $uq_2 \dots q_n \in A^\times$ et donc $n = 1$.

✦ Supposons que le résultat soit vrai jusqu'au rang $m-1$ et démontrons-le au rang $m$. On a $p_1(p_2 \dots p_m) = q_1 \dots q_n$. Puisque $p_1$ est irréductible, $p_1$ est premier d'après **(d)**, et il divise $q_1 \dots q_n$, donc il existe $i$ tel que $p_1 \mid q_i$ : on a $q_i = u_1 p_1$ avec $u_1 \in A$. Puisque $q_i$ est irréductible, $u_1 \in A^\times$.

On a donc $p_1(p_2 \dots p_m) = u_1 p_1 (q_1 \dots q_{i-1} q_{i+1} \dots q_n)$, donc $p_2 \dots p_m = u_1 q_1 \dots q_{i-1} q_{i+1} \dots q_n$ et par hypothèse de récurrence on a $m - 1 = n - 1$, donc $m = n$, et il existe $u_j \in A^\times$ pour tout $j = 2, \dots, m$ et une bijection $\tau : \{2, \dots, m\} \to \{1, \dots, m\} \setminus \{i\}$ tels que $p_j = u_j q_{\tau(j)}$ pour tout $j = 2, \dots, m$. On conclut en définissant $\sigma \in \mathfrak{S}_m$ par $\sigma(1) = i$ et $\sigma(j) = \tau(j)$ pour $j = 2, \dots, m$. ✓

## V.2. Exemples d'anneaux factoriels.

Dans cette partie, on étudie les anneaux principaux et les anneaux euclidiens. Ce sont des exemples d'anneaux factoriels.

On commence par l'étude des anneaux principaux. On rappelle qu'un anneau $A$ est dit principal s'il est intègre et si tout idéal de $A$ est principal, c'est-à-dire que pour tout idéal $I$ de $A$, il existe $a \in A$ tel que $I = (a)$.

**Lemme 25.** Soit $A$ un anneau principal et soit $I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots \subset A$ une suite croissante d'idéaux de $A$. Alors cette suite stationne, c'est-à-dire qu'il existe $N \in \mathbb{N}^*$ tel que pour tout $n \geqslant N$ on ait $I_n = I_N$.

*Démonstration.* Posons $I = \cup_{n\in\mathbb{N}^*} I_n$. Alors $I$ est un idéal de $A$ (exercice), donc comme $A$ est principal il existe $a \in A$ tel que $I = (a)$. Alors $a \in \cup_{n\in\mathbb{N}^*} I_n$, donc il existe $N \in \mathbb{N}^*$ tel que $a \in I_N$. Par conséquent, $(a) \subset I_N \subset I = (a)$, donc $I = I_N$. De plus, pour tout $n \geqslant N$, on a $I_N \subset I_n \subset I = I_N$ donc $I_n = I_N$. ✓

**Proposition 26.** Soit $A$ un anneau principal qui n'est pas un corps. Soit $a \in A$. Alors $a$ est irréductible si et seulement si $(a)$ est maximal.

En particulier, un anneau principal satisfait la condition de primalité. De plus, les idéaux premiers non nuls d'un anneau principal sont maximaux.

*Démonstration.* On sait déjà que l'on a les implications suivantes :

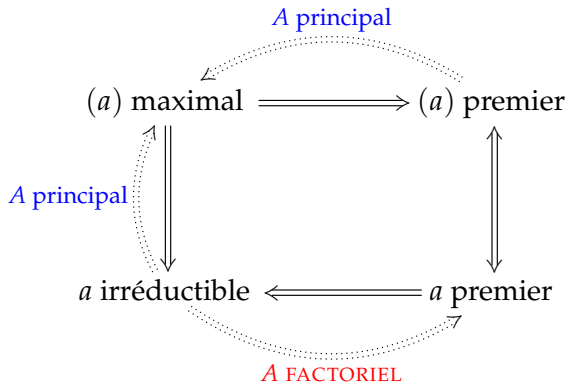
$$(a) \text{ maximal} \implies (a) \text{ premier} \overset{\text{def}}{\iff} a \text{ premier} \overset{\text{p. 9}}{\implies} a \text{ irréductible}$$

Il suffit donc de démontrer que si $a$ est irréductible alors $(a)$ est maximal.

Supposons donc $a$ irréductible. Soit $I$ un idéal de $A$ tel que $(a) \subsetneq I \subset A$. Puisque $A$ est principal, il existe $b \in A$ tel que $I = (b)$. Donc $b \mid a$ et comme $a$ est irréductible et que $b$ n'est pas associé à $a$ (puisque $(a) \neq (b)$), $b$ est inversible et donc $I = (b) = A$. Donc $(a)$ est maximal.

Le reste est clair. ✓

***Remarque.*** Soit $A$ un anneau intègre et soit $a \in A$ un élément non nul. On a les implications suivantes :




**Théorème 27.** Si $A$ est principal, alors il est factoriel.

*Démonstration.* On sait déjà que $A$ est intègre.

Si $A$ est un corps, il est factoriel (voir **p. 10**). Supposons donc que $A$ n'est pas un corps.

D'après la proposition **26**, la condition de primalité est satisfaite par $A$. Il suffit donc d'après le théorème **24** de démontrer que tout élément non nul et non inversible de $A$ est un produit d'éléments irréductibles.

Soit $\mathcal{S}$ l'ensemble des idéaux $(a)$ engendrés par les éléments $a$ non nuls, non inversibles et n'admettant pas de factorisation en produit d'éléments irréductibles. Supposons par l'absurde que $\mathcal{S} \neq \varnothing$.

Démontrons que $\mathcal{S}$ admet un élément maximal. Si ce n'est pas le cas, soit $(a_1) \in \mathcal{S}$. Alors $(a_1)$ n'est pas maximal dans $\mathcal{S}$ donc il existe $(a_2) \in \mathcal{S}$ tel que $(a_1) \subsetneq (a_2)$. De même, $(a_2)$ n'est pas maximal donc il

existe $(a_3) \in \mathcal{S}$ tel que $(a_2) \subsetneq (a_3)$. En procédant ainsi, on construit une suite strictement croissante d'idéaux dans $A$, contredisant ainsi le lemme 25.
Donc $\mathcal{S}$ admet un élément maximal, notons-le $(a_0)$. En particulier, comme $(a_0) \in \mathcal{S}$, l'élément $a_0$ n'est pas irréductible, donc on peut écrire $a_0 = bc$ avec $b$ et $c$ non nuls et non inversibles. On a alors $(a_0) \subsetneq (b)$ et $(a_0) \subsetneq (c)$ donc par maximalité de $(a_0)$ dans $\mathcal{S}$, on a $(b) \notin \mathcal{S}$ et $(c) \notin \mathcal{S}$. Par définition de $\mathcal{S}$ il existe donc des éléments irréductibles $p_1, \dots, p_r$ et $q_1, \dots, q_s$ tels que $b = p_1 \cdots p_r$ et $c = q_1 \cdots q_s$. Mais alors $a_0 = p_1 \cdots p_r q_1 \cdots q_s$ ce qui contredit le fait que $(a_0) \in \mathcal{S}$.
Finalement, $\mathcal{S} = \varnothing$ et donc la propriété (E) est bien vérifiée. ✓

***Remarque.*** On suppose $A$ principal.

**(1)** Si $A$ est un corps, son unique idéal premier est $\{0\}$.

**(2)** Si $A$ n'est pas un corps, ses idéaux premiers sont $\{0\}$ (qui n'est pas maximal) et les idéaux $(p)$ où $p$ est irréductible (et un tel idéal est maximal d'après la proposition 26).

Le théorème 27 montre que toute famille finie d'éléments non tous nuls d'un anneau principal admet un pgcd et un ppcm (voir proposition 22) ; on peut les caractériser au moyen d'idéaux.

**Proposition 28.** Supposons $A$ principal et soient $a_1, \dots, a_r$ ($r \in \mathbb{N}^*$) des éléments de $A$.

- ✦ Si les $a_1, \dots, a_r$ ne sont pas tous nuls, alors un élément de $A$ est un pgcd de $\{a_1, \dots, a_r\}$ si et seulement s'il engendre l'idéal $a_1A + \cdots + a_rA$.
- ✦ Si les $a_1, \dots, a_r$ sont tous non nuls, alors un élément de $A$ est un ppcm de $\{a_1, \dots, a_r\}$ si et seulement s'il engendre l'idéal $a_1A \cap \cdots \cap a_rA$.

*Démonstration.* ✦ Soit $d$ un pgcd de $\{a_1, \dots, a_n\}$. Alors pour tout $i$ on a $(a_i) \subset (d)$, donc $(a_1, \dots, a_n) = (a_1) + \cdots + (a_n) \subset (d)$.
Puisque $A$ est principal, il existe $b \in A$ tel que $(a_1, \dots, a_n) = (b)$. Pour tout $i$, on a $(a_i) \subset (b)$ donc $b$ divise $a_i$ pour tout $i$ et donc $b$ divise $d$ qui est un pgcd des $a_i$. Par conséquent, $(d) \subset (b)$ et finalement $(a_1, \dots, a_n) = (b) = (d)$.

Réciproquement, si $d \in A$ est tel que $(d) = (a_1, \dots, a_r)$, alors $d$ est un diviseur commun des $a_i$, et pour tout autre diviseur commun $b$ des $a_i$, on a $(d) = (a_1, \dots, a_r) \subset (b)$ donc $b$ divise $d$ et donc $d$ est un pgcd des $a_i$.

✦ Soit $m$ un ppcm de $\{a_1, \dots, a_n\}$. Alors pour tout $i$ on a $(m) \subset (a_i)$, donc $(m) \subset (a_1) \cap \cdots \cap (a_n)$.
Puisque $A$ est principal, il existe $b \in A$ tel que $(a_1) \cap \cdots \cap (a_n) = (b)$. Pour tout $i$, on a $(b) \subset (a_i)$ donc $a_i$ divise $b$ pour tout $i$ et donc $m$, qui est un ppcm des $a_i$, divise $b$. Par conséquent, $(b) \subset (m)$ et finalement $(a_1) \cap \cdots \cap (a_n) = (b) = (m)$.

Réciproquement, si $m \in A$ est tel que $(m) = (a_1) \cap \cdots \cap (a_r)$, alors $m$ est un multiple commun des $a_i$, et pour tout autre multiple commun $c$ des $a_i$, on a $(m) = (a_1) \cap \cdots \cap (a_r) \supset (c)$ donc $m$ divise $c$ et donc $m$ est un ppcm des $a_i$. ✓

**Corollaire 29** (Propriété de Bézout)**.** Supposons $A$ principal et soient $a_1, \dots, a_r$ ($r \in \mathbb{N}^*$) des éléments non tous nuls de $A$. Alors, les éléments $a_1, \dots, a_r$ sont premiers entre eux si et seulement s'il existe $x_1, \dots, x_r \in A$ tels que $a_1x_1 + \cdots + a_rx_r = 1$.

*Démonstration.* C'est une conséquence immédiate de la proposition 28. ✓

On passe maintenant au cas des anneaux euclidiens. Ce sont des exemples d'anneaux principaux.

**Définition 30.** *L'anneau $A$ est dit* ***euclidien*** *s'il est intègre et s'il existe une application $\nu : A \setminus \{0\} \longrightarrow \mathbb{N}$ vérifiant : pour tout couple $(a, b)$ d'éléments de $A$ tel que $b \neq 0$, il existe un couple $(q, r)$ d'éléments de $A$ tel que $a = bq + r$ et ou bien $r = 0$, ou bien $\nu(r) < \nu(b)$.*
*L'application $\nu$ s'appelle un* ***stathme euclidien****.*

***Remarque.*** Dans la littérature, un tel $\nu$ s'appelle parfois un *pré-stathme euclidien*, et il faut ajouter la condition que pour tout $(a,b) \in A^2$ avec $ab \neq 0$, on a $\nu(a) \leqslant \nu(ab)$ pour avoir un *stathme euclidien*. Mais on peut démontrer que si un pré-stathme existe, il existe aussi un stathme, donc les deux définitions d'*anneau* euclidien sont équivalentes.

**Théorème 31.** Si $A$ est euclidien, il est principal.

*Démonstration.* cf. cours de L3.
Soit $I$ un idéal de $A$. Si $I = \{0\}$, il est principal. Sinon, l'ensemble $I \setminus \{0\}$ est non vide et par suite l'ensemble $\{\nu(a),\ a \in I \setminus \{0\}\}$ est une partie non vide de $\mathbb{N}$ qui admet donc un plus petit élément $m$. Soit alors $a \in I \setminus \{0\}$ tel que $\nu(a) = m$. Pour tout $b \in I$, il existe $q, r \in A$ tels que $b = aq + r$ et ou bien $r = 0$, ou bien $\nu(r) < \nu(a)$. Si l'on suppose que $r \neq 0$, alors $r$ est un élément non nul de $I$ tel que $\nu(r) < \nu(a)$. Ceci contredit la définition de $a$ et par suite, on doit avoir $r = 0$. On a démontré que $I = (a)$. ✓

***Exemple.*** L'anneau $\mathbb{Z}$ est euclidien (considérer l'application $\nu : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}$ définie par $\nu(n) = |n|$).
Si $K$ est un corps, l'anneau $K[X]$ est euclidien (considérer l'application $\nu : K[X] \setminus \{0\} \longrightarrow \mathbb{N}$ définie par $\nu(P) = \deg P$).

**Corollaire 32.** Soit $A$ un anneau commutatif unitaire quelconque (*ie.* non nécessairement intègre). L'anneau $A[X]$ est principal si et seulement si $A$ est un corps.

*Démonstration.* D'après le théorème 31 et l'exemple ci-dessus, si $A$ est un corps, alors $A[X]$ est principal.
Réciproquement, supposons que $A[X]$ est principal. Alors $A$ est intègre car c'est un sous-anneau de $A[X]$ qui est principal donc intègre.
L'application $\varphi : A[X] \to A$ définie par $\varphi(P) = P(0)$ est un morphisme d'anneaux surjectif et de noyau $(X)$, donc d'après le premier théorème d'isomorphisme on a $A[X]/(X) \cong A$. Or $A$ est intègre, donc $A[X]/(X)$ est intègre, donc $(X)$ est un idéal premier et non nul, donc maximal puisque $A[X]$ est principal, et donc $A \cong A[X]/(X)$ est un corps. ✓

# CHAPITRE 2

# *Anneaux de polynômes*

Dans tout ce chapitre, $A$ désigne un anneau (commutatif unitaire).

## I ANNEAUX DE POLYNÔMES EN PLUSIEURS INDÉTERMINÉES

Vous avez défini en L3 l'anneau de polynômes $A[X]$ en une indéterminée. Pour mémoire, il s'agit de l'ensemble des suites $(a_n)_{n\in\mathbb{N}}$ finies d'éléments de $A$, muni de l'addition composante à composante et du produit défini par $(a_n)\cdot(b_n) = (c_n)$ avec $c_n = \sum_{k=0}^{n} a_k b_{n-k}$. On note $(a_n)_{n\in\mathbb{N}} = \sum_{k=0}^{d} a_k X^k$ où $d \geqslant \max\{k; a_k \neq 0\}$ et $\max\{k; a_k \neq 0\} = \deg\left(\sum_{k=0}^{d} a_k X^k\right)$ est le degré du polynôme $\sum_{k=0}^{d} a_k X^k$.

On définit alors récursivement les anneaux de polynômes en plusieurs indéterminées.

**Définition 1.** *Soit $n \in \mathbb{N}$ un entier avec $n > 1$. L'**anneau de polynômes en $n$ indéterminées** $X_1, \dots, X_n$, noté $A[X_1, \dots, X_n]$, est défini récursivement par*

$$A[X_1, \dots, X_n] := A[X_1, \dots, X_{n-1}][X_n].$$

***Remarque.*** On a une inclusion naturelle $A \to A[X]$ qui à un élément $a \in A$ associe le polynôme $a$. C'est un morphisme d'anneaux. Il découle de la définition qu'il existe des morphismes injectifs d'anneaux naturels

- $A \hookrightarrow A[X_1, \dots, X_n]$ et
- $A[X_1, \dots, X_p] \hookrightarrow A[X_1, \dots, X_n]$ pour tout $p \leqslant n$ tel que $X_i$ a pour image $X_i$ pour tout $i \in [\![1\,;p]\!]$.

**Proposition 2.** Tout élément de $A[X_1, \dots, X_n]$ s'écrit, de façon unique, sous la forme

$$\sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n},$$

où $a_{(i_1,\dots,i_n)} \in A$, pour tout $(i_1, \dots, i_n) \in \mathbb{N}^n$ (somme finie).

*Démonstration.* On raisonne par récurrence sur $n$.

- C'est vrai pour $n = 1$ (L3).
- Soit $n \geqslant 1$. Supposons le résultat vrai pour l'anneau de polynômes en $n$ indéterminées. Soit $P \in A[X_1, \dots, X_n, X_{n+1}]$. Posons $B = A[X_1, \dots, X_n]$. Alors, puisque $A[X_1, \dots, X_n, X_{n+1}] = B[X_{n+1}]$, le résultat au rang 1 nous permet d'écrire $P = \sum_{i=0}^{d} Q_i X_{n+1}^i$ avec $d \in \mathbb{N}$ et $Q_i \in B$, $Q_d \neq 0$. Par hypothèse de récurrence, on a, pour tout $j$, $Q_j = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a^{(j)}_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}$ avec où $a^{(j)}_{(i_1,\dots,i_n)} \in A$ (somme finie). On en déduit que

$$P = \sum_{j=0}^{d} \sum_{(i_1,\dots,i_n)} a^{(j)}_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n} X_{n+1}^{j} = \sum_{(i_1,\dots,i_n,i_{n+1})} b_{(i_1,\dots,i_n,i_{n+1})}.X_1^{i_1}\dots X_n^{i_n} X_{n+1}^{i_{n+1}}$$

où $b_{(i_1,\dots,i_n,i_{n+1})} = a^{(j)}_{(i_1,\dots,i_n)}$. On a démontré l'existence. Démontrons maintenant l'unicité. Il suffit pour cela de démontrer que si $P = \sum_{(i_1,\dots,i_n,i_{n+1})} a_{(i_1,\dots,i_n,i_{n+1})}.X_1^{i_1}\dots X_n^{i_n}X_{n+1}^{i_{n+1}}$ est le polynôme nul, alors tous les coefficients $a_{(i_1,\dots,i_n,i_{n+1})}$ sont nuls.

On peut écrire $0 = \sum_{i_{n+1}\in\mathbb{N}}\left(\sum_{(i_1,\dots,i_n)} a_{(i_1,\dots,i_n,i_{n+1})}.X_1^{i_1}\dots X_n^{i_n}\right)X_{n+1}^{i_{n+1}} = \sum_{i_{n+1}\in\mathbb{N}} Q_{i_{n+1}}X_{n+1}^{i_{n+1}}$ avec $Q_{i_{n+1}} \in B$. Le résultat au rang 1 donne $Q_j = 0$ pour tout $j$. L'hypothèse de récurrence implique que tous les coefficients de tous les $Q_j$ sont nuls, c'est-à-dire que tous les coefficients de $P$ sont nuls. ✓

**Définition 3.** ✦ *Un élément de $A[X_1,\dots,X_n]$ de la forme $X_1^{i_1}\dots X_n^{i_n}$, avec $(i_1,\dots,i_n)\in\mathbb{N}^n$ s'appelle un* ***monôme*** *de $A[X_1,\dots,X_n]$ (en $X_1,\dots,X_n$).*

✦ *Soit $P = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}$. Alors $a_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}$ est le* ***terme monomial*** *correspondant au monôme $X_1^{i_1}\dots X_n^{i_n}$.*

*La proposition ci-dessus dit que tout polynôme de $A[X_1,\dots,X_n]$ s'écrit de manière unique comme somme finie de termes monomiaux.*

✦ *Le* ***degré****, ou* ***degré total****, du monôme $X_1^{i_1}\dots X_n^{i_n}$ ou du terme monomial $a_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}$ (avec $a_{(i_1,\dots,i_n)}\neq 0$) est $\sum_{k=1}^n i_k$.*

*Le* ***degré****, ou* ***degré total****, du polynôme $P$ est le maximum des degrés des termes monomiaux non-nuls qui constituent $P$ :*

$$\deg P := \max\left\{\sum_{k=1}^n i_k ; a_{(i_1,\dots,i_n)}\neq 0\right\}.$$

**Proposition 4.** Soit $A$ un anneau intègre et $n\in\mathbb{N}^*$. L'anneau de polynômes $A[X_1,\dots,X_n]$ en $n$ indéterminées est intègre.

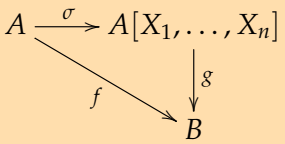
*Démonstration.* On procède par récurrence sur $n$.

✦ Le résultat est connu si $n=1$. Pour mémoire, si $P=\sum_{i=0}^d a_iX^i$ et $Q=\sum_{j=0}^t b_jX^j$ ne sont pas nuls, avec $a_d\neq 0$ et $b_t\neq 0$, alors $PQ = a_db_tX^{d+t}+R$ avec $\deg R < d+t$. Puisque $A$ est intègre, $a_db_t\neq 0$ et donc $PQ\neq 0$.

✦ Supposons que $B = A[X_1,\dots,X_n]$ est intègre pour un $n\geqslant 1$. Alors $A[X_1,\dots,X_{n+1}] = B[X_{n+1}]$ est intègre d'après le résultat au rang 1. ✓

**Théorème 5** (Propriété universelle des anneaux de polynômes)**.** Soient $B$ un anneau, $f : A\longrightarrow B$ un morphisme d'anneaux et $b_1,\dots,b_n\in B$. On note $\sigma : A\to A[X_1,\dots,X_n]$ l'inclusion naturelle.

Alors il existe un morphisme d'anneaux $g : A[X_1,\dots,X_n]\longrightarrow B$ et un seul tel que, pour $1\leqslant j\leqslant n$, $g(X_j)=b_j$ et tel que $g\circ\sigma = f$, c'est-à-dire que le diagramme suivant soit commutatif :




***Remarque.*** La condition $g\circ\sigma = f$ s'écrit $g_{|A} = f$ lorsqu'on identifie $A$ et $\sigma(A)$. Autrement dit, $g$ est un prolongement de $f$ à $A[X_1,\dots,X_n]$.

*Démonstration.* Si $g$ existe, on doit avoir

$$\begin{aligned} g\left(\sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}\right) &= \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} g\left(a_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}\right)\\ &= \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} f(a_{(i_1,\dots,i_n)}).g(X_1)^{i_1}\dots g(X_n)^{i_n}\\ &= \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} f(a_{(i_1,\dots,i_n)})b_1^{i_1}\dots b_n^{i_n}\end{aligned}$$

donc $g$ est nécessairement unique.
De plus, on vérifie facilement que l'application $g\colon A[X_1,\dots,X_n] \longrightarrow B$ définie par

$$g\left(\sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}\right) = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} f(a_{(i_1,\dots,i_n)})b_1^{i_1}\dots b_n^{i_n}$$

vérifie les propriétés requises. En effet :

- ✦ Il est clair que $g(\sigma(a)) = g(a) = f(a)$ pour tout $a \in A$ (prendre $(i_1,\dots,i_n) = (0,\dots,0)$).
- ✦ Il est clair que $g(X_k) = b_k$ pour tout $k \in [\![1\,;n]\!]$ (prendre $(i_1,\dots,i_n) = (0,\dots,0,1,0,\dots,0)$ avec le 1 en $k^{\text{ième}}$ position).
- ✦ Il reste à vérifier que $g$ est bien un morphisme d'anneaux.
  - ✧ $g(1) = f(1) = 1$.
  - ✧ Posons $P = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}$ et $Q = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a'_{(i_1,\dots,i_n)}.X_1^{i_1}\dots X_n^{i_n}$. Alors

$$\begin{aligned} g(P+Q) &= g\left(\sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} (a_{(i_1,\dots,i_n)} + a'_{(i_1,\dots,i_n)}).X_1^{i_1}\dots X_n^{i_n}\right) = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} f(a_{(i_1,\dots,i_n)} + a'_{(i_1,\dots,i_n)}).b_1^{i_1}\dots b_n^{i_n} \\ &= \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} (f(a_{(i_1,\dots,i_n)}) + f(a'_{(i_1,\dots,i_n)})).b_1^{i_1}\dots b_n^{i_n} \\ &= \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} f(a_{(i_1,\dots,i_n)}).b_1^{i_1}\dots b_n^{i_n} + \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} f(a'_{(i_1,\dots,i_n)}).b_1^{i_1}\dots b_n^{i_n} = g(P) + g(Q). \end{aligned}$$

  - ✧ ➢ Soient $P = a.X_1^{i_1}\dots X_n^{i_n}$ et $P = a'.X_1^{j_1}\dots X_n^{j_n}$ des termes monomiaux. Alors

$$g(PQ) = g(aa'.X_1^{i_1+j_1}\dots X_n^{i_n+j_n}) = f(aa'.b_1^{i_1+j_1}\dots b_n^{i_n+j_n}) = f(a).b_1^{i_1}\dots b_n^{i_n}\cdot f(a').b_1^{j_1}\dots b_n^{j_n} = g(P)g(Q).$$

    ➢ Soient $P$ et $Q$ quelconques dans $A[X_1,\dots,X_n]$. Alors $P = \sum_{k=1}^n T_k$ et $Q = \sum_{\ell=1}^m S_\ell$ où les $T_k$ et les $S_\ell$ sont des termes monomiaux. En utilisant ce que nous avons déjà démontré, on a

$$\begin{aligned} g(PQ) &= g(\sum_{k=1}^n\sum_{\ell=1}^m T_kS_\ell) = \sum_{k=1}^n\sum_{\ell=1}^m g(T_kS_\ell) = \sum_{k=1}^n\sum_{\ell=1}^m g(T_k)g(S_\ell) \\ &= \left(\sum_{k=1}^n g(T_k)\right)\left(\sum_{\ell=1}^m g(S_\ell)\right) = g\left(\sum_{k=1}^n T_k\right)g\left(\sum_{\ell=1}^m S_\ell\right) = g(P)g(Q). \qquad \checkmark \end{aligned}$$

***Exemple.*** Soit $A$ un anneau et soit $I$ un idéal de $A$. Le morphisme d'anneaux $f : A \to (A/I)[X]$ obtenu par composition de la projection canonique $\pi : A \to A/I$ et de l'inclusion $A/I \to (A/I)[X]$ induit donc grâce au théorème **5** un morphisme d'anneaux $\varphi_I : A[X] \to (A/I)[X]$ qui prolonge $f$ et tel que $\varphi_I(X) = X$ (c'est-à-dire que $\varphi_I(\sum_{i=0}^n a_iX^i) = \sum_{i=0}^n \pi(a_i)X^i$). Il est clair que $\varphi_I$ est surjectif.

De même, si $f : A \to (A/I)[X_1,\dots,X_n]$ est la composée de la projection canonique $\pi : A \to A/I$ et de l'inclusion $A/I \to (A/I)[X_1,\dots,X_n]$ , il existe un morphisme d'anneaux surjectif $\varphi_I : A[X_1,\dots,X_n] \to (A/I)[X_1,\dots,X_n]$ qui prolonge $f$ et tel que $\varphi_I(X_i) = X_i$ pour tout $i$ (c'est-à-dire que $\varphi_I(\sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{(i_1,\dots,i_n)}X_1^{i_1}\cdots X_n^{i_n}) = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} \pi(a_{(i_1,\dots,i_n)})X_1^{i_1}\cdots X_n^{i_n}$).

**Cas particulier.** Soit $p \in \mathbb{N}$ un nombre premier et soit $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ la projection canonique. On pose $\pi(n) = \overline{n}$. Le morphisme $\varphi_{(p)} : \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$ consiste à réduire les coefficients des polynôme modulo $p$ : $\varphi_{(p)}(\sum_{k=0}^n a_kX^k) = \sum_{k=0}^n \overline{a}_kX^k$. On appelle $\varphi_{(p)}$ le morphisme de réduction modulo $p$.

**Corollaire 6.** Soit $\sigma \in \mathfrak{S}_n$. On a un isomorphisme d'anneaux $A[X_1,\dots,X_n] \cong A[X_{\sigma(1)},\dots,X_{\sigma(n)}]$.
En particulier, on en déduit que pour tout $i \in [\![1\,;n]\!]$, on peut identifier les anneaux $A[X_1,\dots,X_n]$ et $A[X_1,\dots,X_{i-1},X_{i+1},\dots,X_n][X_i]$.

*Démonstration.* On applique la propriété universelle des anneaux de polynômes avec $B = A[X_{\sigma(1)},\dots,X_{\sigma(n)}]$ et $b_i = X_{\sigma(i)}$ pour obtenir un morphisme d'anneaux $\varphi : A[X_1,\dots,X_n] \to A[X_{\sigma(1)},\dots,X_{\sigma(n)}]$ qui fixe les éléments de $A$ et envoie chaque $X_i$ sur $X_{\sigma(i)}$.

On applique à nouveau la propriété universelle des anneaux de polynômes avec $B = A[X_1, \dots, X_n]$ et $b_i = X_i$ (avec au départ l'anneau $A[X_{\sigma(1)}, \dots, X_{\sigma(n)}]$) pour obtenir un morphisme d'anneaux $\psi : A[X_{\sigma(1)}, \dots, X_{\sigma(n)}] \to A[X_1, \dots, X_n]$ qui fixe les éléments de $A$ et envoie chaque $X_{\sigma(i)}$ sur $X_i$.
Alors $\psi \circ \varphi$ est un endomorphisme d'anneaux de $A[X_1, \dots, X_n]$ qui fixe les éléments de $A$ et les $X_i$; or $\mathrm{id}_{A[X_1,\dots,X_n]}$ est également un tel endomorphisme, donc par unicité on a $\psi \circ \varphi = \mathrm{id}_{A[X_1,\dots,X_n]}$.
De même, $\varphi \circ \psi = \mathrm{id}_{A[X_{\sigma(1)},\dots,X_{\sigma(n)}]}$ donc $\varphi$ et $\psi$ sont des isomorphismes réciproques. ✓

**Définition 7.** ✦ *Le **degré partiel** du monôme $X_1^{i_1} \cdots X_n^{i_n}$ (ou du terme monomial $a_{(i_1,\dots,i_n)} X_1^{i_1} \cdots X_n^{i_n}$ avec $a_{(i_1,\dots,i_n)} \neq 0$) en l'indéterminée $X_k$ est $i_k$. Il s'agit du degré de ce monôme vu dans l'anneau $A[X_1, \dots, X_{k-1}, X_{k+1}, \dots, X_n][X_k]$, c'est-à-dire un polynôme en l'indéterminée $X_k$ et à coefficients dans $A[X_1, \dots, X_{k-1}, X_{k+1}, \dots, X_n]$.*

✦ *Le **degré partiel** du polynôme $P$ en l'indéterminée $X_k$ est le maximum des degrés partiels en $X_k$ des termes monomiaux non nuls qui constituent $P$ :*

$$\deg_{X_k} P := \max\Big\{ i_k ; a_{(i_1,\dots,i_n)} \neq 0 \Big\}.$$

*C'est le degré de $P$ vu comme polynôme dans $A[X_1, \dots, X_{k-1}, X_{k+1}, \dots, X_n][X_k]$.*

## II Fonctions polynomiales.

Dans toute cette section, $A$ est un anneau (commutatif unitaire).
Si $n \in \mathbb{N}^*$, on note $\mathcal{F}(A^n, A)$ l'ensemble des applications de $A^n$ dans $A$. Il est bien connu que $\mathcal{F}(A^n, A)$ est un anneau commutatif, pour les opérations suivantes : si $f$ et $g$ sont dans $\mathcal{F}(A^n, A)$,

$$\begin{aligned} (f+g)(x) &= f(x) + g(x) \quad \text{pour tout } x \in A^n \\ (fg)(x) &= f(x)g(x) \quad \text{pour tout } x \in A^n. \end{aligned}$$

L'élément neutre (resp. unité) est l'application constante égale à 0 (resp. 1).

**Définition 8.** *Soit $P = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{(i_1,\dots,i_n)} . X_1^{i_1} \dots X_n^{i_n} \in A[X_1, \dots, X_n]$, où $a_{(i_1,\dots,i_n)} \in A$, pour tout $(i_1, \dots, i_n) \in \mathbb{N}^n$. On associe à $P$ la fonction $\widetilde{P} \in \mathcal{F}(A^n, A)$ définie par*

$$\begin{array}{rccc} \widetilde{P} & : & A^n & \longrightarrow & A \\ & & (\alpha_1, \dots, \alpha_n) & \mapsto & \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{(i_1,\dots,i_n)} \alpha_1^{i_1} \dots \alpha_n^{i_n} \end{array} .$$

*Cette fonction s'appelle la **fonction polynomiale** associée à $P$. Par abus de notation, pour $(\alpha_1, \dots, \alpha_n) \in A^n$, on écrira souvent $P(\alpha_1, \dots, \alpha_n)$ au lieu de $\widetilde{P}(\alpha_1, \dots, \alpha_n)$.*

**Proposition 9.** Soit $n \in \mathbb{N}^*$. L'application $A[X_1, \dots, X_n] \longrightarrow \mathcal{F}(A^n, A)$, $P \mapsto \widetilde{P}$ est un morphisme d'anneaux. Son image est notée $\mathcal{F}_{\mathrm{pol}}(A^n, A)$ et elle est appelée l'**anneau des fonctions polynomiales** sur $A^n$.

*Démonstration.* C'est une simple vérification.
On peut également, pour éviter des calculs techniques, utiliser la propriété universelle des anneaux de polynômes (théorème 5). Pour tout $i \in [\![1 ; n]\!]$, soit $\pi_i \in \mathcal{F}(A^n, A)$ l'application définie par $\pi_i(\alpha_1, \dots, \alpha_n) = \alpha_i$ (la projection sur la $i^{\mathrm{me}}$ composante). Soit $f : A \to \mathcal{F}(A^n, A)$ l'application qui à $x \in A$ associe l'application constante égale à $x$ ; c'est un morphisme d'anneaux. Alors il existe un unique morphisme d'anneaux $A[X_1, \dots, X_n] \to \mathcal{F}(A^n, A)$ qui prolonge $f$ et qui associe $\pi_i$ à $X_i$. On constate qu'il s'agit bien de l'application $P \mapsto \widetilde{P}$. ✓

Soit $n \in \mathbb{N}^*$. La proposition 9 montre que l'on dispose d'un morphisme d'anneaux surjectif

$$\begin{array}{rccc} \varphi_n & : & A[X_1, \dots, X_n] & \longrightarrow & \mathcal{F}_{\mathrm{pol}}(A^n, A) \\ & & P & \mapsto & \widetilde{P} \end{array} .$$

***Remarque.*** Soit $A$ un anneau intègre. On sait que $\varphi_1 : A[X] \to \mathcal{F}_{\text{pol}}(A, A)$ est injectif si, et seulement si, $A$ est infini.

En effet, si $A$ est fini, posons $A = \{t_1, \dots, t_s\}$. Alors le polynôme $P = \prod_{i=1}^{s}(X - t_i)$ n'est pas nul (il est de degré $s$) mais la fonction polynomiale $\widetilde{P} : A \to A$ est nulle.

D'autre part, si $A$ est infini, puisqu'il est intègre tout polynôme non nul de $A[X]$ a un nombre fini de racines, donc la fonction polynomiale associée ne peut pas être nulle.

Ce résultat est encore vrai pour les polynômes en plusieurs indéterminées.

**Théorème 10.** Soit $A$ un anneau intègre et soit $n \in \mathbb{N}^*$. Le morphisme $\varphi_n$ d'anneaux est un isomorphisme si, et seulement si, $A$ est infini.

*Démonstration.* ✦ Supposons que $A$ est infini. Il suffit de démontrer que, pour tout $n \in \mathbb{N}^*$, $\varphi_n$ est injectif (puisqu'il est surjectif par construction). On raisonne par récurrence sur $n$. Le cas $n = 1$ est connu. On suppose le résultat acquis jusqu'à l'ordre $s$, $s \in \mathbb{N}^*$. Soit $P \in A[X_1, \dots, X_{s+1}]$ ; il existe une famille $\{P_i\}_{i\in\mathbb{N}}$ d'éléments de $A[X_1, \dots, X_s]$ telle que $P = \sum_{i\in\mathbb{N}} P_i X_{s+1}^i$. Si l'on suppose que $P$ n'est pas nul, alors il existe $i_0 \in \mathbb{N}$ tel que $P_{i_0} \neq 0$. Par hypothèse de récurrence, on en déduit l'existence de $(a_1, \dots, a_s) \in A^s$ tel que $\widetilde{P}_{i_0}(a_1, \dots, a_s) \neq 0$. Soit enfin $\psi\colon A[X_1, \dots, X_{s+1}] \longrightarrow A[X_{s+1}]$ le morphisme d'anneaux tel que $\psi_{|A} = \mathrm{id}_A$, $\psi(X_i) = a_i$ pour $1 \leqslant i \leqslant s$ et $\psi(X_{s+1}) = X_{s+1}$. Alors le polynôme $\psi(P) = \sum_{i\in\mathbb{N}} \widetilde{P}_i(a) X_{s+1}^i$ de $A[X_{s+1}]$ n'est pas nul puisque $\widetilde{P}_{i_0}(a) \neq 0$. Il existe donc $a \in A$ tel que $\widetilde{\psi(P)}(a) \neq 0$. On en déduit aussitôt que $\widetilde{P}$ ne s'annule pas en $(a_1, \dots, a_s, a)$, donc la fonction polynomiale associée à $P$ n'est pas nulle.

✦ Supposons que $A$ est fini. On sait qu'il existe un polynôme $P \in A[X_1]$ dont la fonction polynômiale associée $\widetilde{P} : A \to A$ est nulle. Posons $P = \sum_{i=0}^{d} a_i X_1^i$.
On dispose d'un morphisme d'anneaux injectif $\sigma : A[X_1] \to A[X_1, \dots, X_n]$ qui envoie $X_1$ sur $X_1$ et fixe les éléments de $A$. Il est clair que $\sigma(P) \neq 0$. Mais on a

$$\widetilde{\sigma(P)}(\alpha_1, \dots, \alpha_n) = \sum_{i=0}^{d} a_i \alpha_1^i = \widetilde{P}(\alpha_1) = 0$$

donc la fonction polynomiale associée au polynôme non nul $\sigma(P)$ est nulle. Ainsi, $\varphi_n$ n'est pas injective. ✓

## III Arithmétique dans les anneaux de polynômes

### III.1. Théorèmes de transfert.

On a vu dans le corollaire 4 que la propriété d'être intègre se transfère de l'anneau $A$ à l'anneau $A[X_1, \dots, X_n]$. On peut remarquer que, comme l'indique le corollaire 1.32, la propriété d'un anneau d'être principal ne se transfère pas de l'anneau $A$ à l'anneau $A[X]$. Il résulte aussi du corollaire 1.32 que la propriété d'un anneau d'être euclidien ne se transfère pas de l'anneau $A$ à l'anneau $A[X]$.

Dans cette section, on étudie le transfert de la propriété d'être factoriel de l'anneau $A$ à l'anneau $A[X_1, \dots, X_n]$. Pour ce faire, il faut introduire la notion de contenu d'un polynôme.

**Définition 11.** *On suppose que $A$ est un anneau factoriel.*

**(1)** *Si $P \in A[X] \setminus \{0\}$, un élément de $A$ est appelé un **contenu** de $P$ si c'est un pgcd des coefficients de $P$.*

**(2)** *Un polynôme $P \in A[X] \setminus \{0\}$ est dit **primitif** si $1$ est un pgcd de ses coefficients.*

*On notera $c \sim c(P)$ si $c$ est un contenu de $P$.*

***Remarque.*** Le fait que $A$ soit un anneau factoriel assure l'existence de pgcd dans $A$ et donc la notion de contenu a bien un sens pour les polynômes à coefficients dans $A$.

***Exemple.*** Les polynômes $2X^2 + 3X + 4$ et $X^3 + X + 1$ de $\mathbb{Z}[X]$ sont primitifs, le polynôme $2X^2 + 6X + 4$ admet 2 comme contenu. Notons que $2X^2 + 6X + 4 = 2 \cdot (X^2 + 3X + 2)$ avec $X^2 + 3X + 2$ primitif.

**Lemme 12.** Soit $A$ un anneau factoriel. Soit $P \in A[X] \setminus \{0\}$. Alors $p \in A$ est un contenu de $P$ si et seulement s'il existe $P_1 \in A[X]$ primitif tel que $P = pP_1$.

*Démonstration.* ($\Rightarrow$) Notons $P = \sum_{i=0}^{n} a_i X^i$. Soit $p$ un contenu de $P$. Alors pour tout $i$ il existe $a'_i \in A$ tel que $a_i = pa'_i$ et 1 est un pgcd des $a'_i$ d'après le lemme **1.23**. On a alors $P = pP_1$ avec $P_1 = \sum_{i=0}^{n} a'_i X^i \in A[X]$ primitif.

($\Leftarrow$) Supposons que $P = pP_1$ avec $P_1$ primitif. Posons $P_1 = \sum_{i=0}^{n} a_i X^i$. Alors $P = \sum_{i=0}^{n} pa_i X^i$ et $p = p \cdot 1$ est un pgcd des coefficients $pa_i$ d'après le lemme **1.23** et donc $p$ est un contenu de $P$. ✓

**Lemme 13** (Lemme de Gauss)**.** On suppose $A$ factoriel. Soient $P$ et $Q$ des polynômes non nuls de $A[X]$.

**(1)** Si $P$ et $Q$ sont primitifs, alors $PQ$ est primitif.

**(2)** Si $p$ et $q$ sont des contenus de $P$ et $Q$ respectivement, alors $pq$ est un contenu de $PQ$.

*Démonstration.* **(1)** On raisonne par l'absurde. Supposons que 1 n'est pas pgcd des coefficients de $PQ$. Alors, puisque $A$ est factoriel, il existe un pgcd des coefficients de $PQ$. Soit $\pi \in A$ un diviseur irréductible de ce pgcd ; il divise donc tous les coefficients de $PQ$. Soient $d, e$ les degrés respectifs de $P$ et $Q$ ; comme $P$ et $Q$ sont primitifs, il existe au moins un coefficient de $P$ et un coefficient de $Q$ qui ne sont pas divisibles par $\pi$. Posons $P = \sum_{i=0}^{d} a_i X^i$, $Q = \sum_{j=0}^{e} b_j X^j$, $i_0 = \inf\{i,\ 0 \leqslant i \leqslant d \text{ tq } \pi \nmid a_i\}$ et $j_0 = \inf\{j,\ 0 \leqslant j \leqslant e \text{ tq } \pi \nmid b_j\}$. Le coefficient d'indice $i_0 + j_0$ de $PQ$ est

$$\sum_{i+j=i_0+j_0} a_i b_j = a_{i_0} b_{j_0} + \sum_{\substack{i+j=i_0+j_0 \\ i<i_0 \text{ ou } j<j_0}} a_i b_j.$$

Mais alors, par définition de $\pi$, $\pi$ divise le membre de gauche et le second terme du membre de droite dans l'équation ci-dessus, donc $\pi | a_{i_0} b_{j_0}$. Comme $A$ est factoriel et $\pi$ irréductible, il s'ensuit (condition d'Euclide) que $\pi$ divise $a_{i_0}$ ou $b_{j_0}$, ce qui constitue une contradiction. Ainsi 1 est pgcd des coefficients de $PQ$.

**(2)** On utilise le lemme **12**. Il existe des polynômes primitifs $P', Q' \in A[X]$ tels que $P = pP'$ et $Q = qQ'$. Alors $PQ = pqP'Q'$ avec $P'Q'$ primitif d'après **(1)**, donc $pq$ est un contenu de $PQ$ d'après le lemme **12**. ✓

***Remarque.*** Soit $A$ un anneau factoriel. Alors $A$ est intègre, donc son corps des fractions $K$ existe et $A$ peut être identifié à un sous-anneau de $K$. On a alors une injection $A \to K \to K[X]$ qui est un morphisme d'anneaux. On en déduit donc grâce à la propriété universelle des anneaux de polynômes un morphisme d'anneaux $A[X] \to K[X]$ qui prolonge cette injection $A \hookrightarrow K[X]$ et qui à $X$ associe $X$. Il est facile de voir que ce morphisme est injectif, et donc que $A[X]$ peut être identifié à un sous-anneau de $K[X]$.

**Lemme 14.** Soit $A$ un anneau factoriel et soit $K$ son corps des fractions. Soit $P \in A[X]$. On suppose qu'il existe $Q, R$ dans $K[X]$ tels que $P = QR$. Alors il existe $Q', R'$ dans $A[X]$ et $\alpha, \beta$ dans $K \setminus \{0\}$ tels que $P = Q'R'$, $Q' = \alpha Q$, et $R' = \beta R$.

*Démonstration.* En réduisant tous les coefficients de $Q$ et $R$ aux mêmes dénominateurs, on voit qu'il existe $q, r \in A$ et $Q_0, R_0 \in A[X]$ tels que $qQ = Q_0$ et $rR = R_0$. On a alors $Q_0 R_0 = qrP$.
Soient $c$ un contenu de $Q_0$ et $d$ un contenu de $R_0$. On peut donc écrire $Q_0 = cQ_1$ et $R_0 = dR_1$ avec $Q_1$ et $R_1$ dans $A[X]$ primitifs d'après le lemme **12**. On a donc $qrP = cdQ_1R_1$ avec $Q_1R_1$ primitif (lemme de Gauss), donc à l'aide du lemme **12** on en déduit que $cd$ est un contenu de $qrP$ et donc que $qr$ divise $cd$ : il existe $\lambda \in A$ tel que $cd = \lambda qr$ d'où $P = \lambda Q_1 R_1$. Finalement on pose $\alpha = \lambda c^{-1} q \in K$, $\beta = d^{-1} r \in K$, $Q' = \alpha Q$ et $R' = \beta R$. ✓

**Théorème 15.** Soit $A$ un anneau factoriel et soit $K$ son corps des fractions.
Les éléments irréductibles de $A[X]$ sont

- les éléments irréductibles de $A$ et
- les polynômes non constants et primitifs de $A[X]$ qui sont irréductibles dans $K[X]$.

*Démonstration.* On rappelle que $A[X]^\times = A^\times$ ($A$ est intègre).

**(1)** Soit $a \in A$. Démontrons que $a$ est irréductible dans $A[X]$ si et seulement s'il est irréductible dans $A$.

- ✦ Si $a$ est irréductible dans $A$, il n'est ni nul ni inversible dans $A$ et donc il n'est ni nul ni inversible dans $A[X]$. De plus, si $a = PQ$ avec $P, Q$ dans $A[X]$, alors $P$ et $Q$ sont de degré 0 donc ils sont dans $A$ et par conséquent $P$ ou $Q$ est un élément inversible de $A$ donc de $A[X]$.
- ✦ Réciproquement, si $a$ est irréductible dans $A[X]$, il n'est ni nul ni inversible dans $A[X]$ et donc il n'est ni nul ni inversible dans $A$ et si $a = bc$ avec $b, c$ dans $A$, alors $b$ ou $c$ est inversible dans $A[X]$ et donc dans $A$.

**(2)** Soit $P$ dans $A[X]$ de degré supérieur ou égal à 1. Alors $P$ n'est ni nul ni inversible dans $A[X]$.

- ✦ Supposons que $P$ est primitif et irréductible dans $K[X]$. Si $P = QR$ avec $Q, R$ dans $A[X]$, l'irréductibilité de $P$ dans $K[X]$ assure que $Q$, par exemple, est un élément inversible de $K[X]$. Donc, $Q = a$ avec $a \in A \setminus \{0\}$. L'égalité $P = aR$ assure que si $d$ est un contenu de $P$, alors $a|d$. Mais $P$ est primitif, donc $a = Q$ est inversible. Ainsi, $P$ est irréductible dans $A[X]$.
- ✦ Réciproquement, supposons que $P$ est irréductible dans $A[X]$. Si $d$ est un contenu de $P$, alors $P = dP'$ avec $P' \in A[X]$ primitif et de degré $\geqslant 1$ donc non inversible. Par conséquent, $d$ est inversible dans $A[X]$ donc dans $A$ et donc $P$ est primitif.

  Démontrons que $P$ est irréductible dans $K[X]$. Il n'est pas inversible dans $K[X]$ (de degré $\geqslant 1$). Si $P = QR$ dans $K[X]$, grâce au lemme **14** on peut supposer que $Q$ et $R$ sont dans $A[X]$. Or $P$ est irréductible dans $A[X]$ donc par exemple $Q$ est inversible dans $A[X]$ et donc $Q$ est inversible dans $K[X]$. ✓

***Remarque.*** Soit $A$ un anneau factoriel et soit $K$ son corps des fractions. Soit $P \in A[X]$ de contenu $c \in A$ et tel que $P = QR$ dans $K[X]$. Alors il existe des polynômes $\widetilde{Q}$ et $\widetilde{R}$ dans $A[X]$ qui sont primitifs, tels que $\widetilde{Q} \sim Q$ et $\widetilde{R} \sim R$ dans $K[X]$ et qui vérifient $P = c\widetilde{Q}\widetilde{R}$.

En effet, il suffit de combiner le lemme **12**, le lemme de Gauss et le lemme **14**.

En particulier, si $P \in A[X]$ est primitif et tel que $P = QR$ dans $K[X]$, alors il existe des polynômes $\widetilde{Q}$ et $\widetilde{R}$ dans $A[X]$ qui sont primitifs, tels que $\widetilde{Q} \sim Q$ et $\widetilde{R} \sim R$ dans $K[X]$ et qui vérifient $P = \widetilde{Q}\widetilde{R}$.

**Théorème 16** (Théorème de Gauss)**.** Si $A$ est factoriel, alors $A[X]$ est factoriel.

*Démonstration.* Notons $K = \operatorname{Frac} A$.

- ✦ On sait déjà que $A[X]$ est intègre puisque $A$ est intègre.
- ✦ On commence par démontrer que l'anneau $A[X]$ satisfait la condition (E). Soit $P \in A[X]$, non nul et non inversible dans $A[X]$.
  - ✧ Si $P$ est de degré 0, il s'écrit comme produit d'éléments irréductibles de $A$ (et donc de $A[X]$ d'après le théorème **15**) et c'est terminé.
  - ✧ Supposons donc que $P$ est de degré $\geqslant 1$. En particulier, $P$ n'est ni nul ni inversible dans $K[X]$. Notons $c$ un contenu de $P$.

    Comme $K[X]$ est principal ($K$ est un corps) et donc factoriel, il existe $r \in \mathbb{N}^*$ et $P_1, \dots, P_r$ des polynômes irréductibles de $K[X]$ tels que $P = P_1 \dots P_r$. D'après la remarque précédente, il existe pour tout $i \in [\![1\,;r]\!]$ des polynômes primitifs $P_i' \in A[X]$ tels que $P_i' \sim P_i$ dans $K[X]$ vérifiant $P = cP_1' \cdots P_r'$. Puisque $A$ est factoriel, on peut écrire $c = q_1 \dots q_s$ où les $q_j$ sont des éléments irréductibles de $A$. On a alors $P = q_1 \dots q_s P_1' \dots P_r'$ et d'après le théorème précédent, les $q_j$ sont irréductibles dans $A[X]$ et les $P_i'$ aussi puisqu'ils ne sont pas constants, ils sont primitifs et ils sont irréductibles dans $K[X]$ (associés aux $P_i$).
- ✦ Pour démontrer que $A[X]$ est factoriel, c'est-à-dire que la condition (U) est vérifiée, il suffit grâce au théorème **1.24** de démontrer que $A[X]$ satisfait la condition de primalité, c'est-à-dire de démontrer qu'un élément irréductible de $A[X]$ engendre un idéal premier de $A[X]$. Soit $P$ un polynôme irréductible de $A[X]$.
  - ✧ Si $P = a \in A$, alors $a$ est un élément irréductible de $A$. On a un morphisme surjectif d'anneaux $A[X] \to (A/(a))[X]$ (*cf.* exemple page 19), et il est facile de voir qu'il induit un isomorphisme $A[X]/(aA[X]) \cong (A/(a))[X]$ par le premier théorème d'isomorphisme. Or $A$ est factoriel et $a$ est irréductible dans $A$, donc $A/(a)$ est intègre, donc $A[X]/(aA[X]) \cong (A/(a))[X]$ est intègre, et donc $aA[X]$ est un idéal premier de $A[X]$.

✧ Si maintenant $\deg P \geqslant 1$, alors $P$ est primitif et irréductible dans $K[X]$ d'après le théorème **15**. Comme $P$ est irréductible dans l'anneau factoriel $K[X]$, l'idéal $PK[X]$ est premier dans $K[X]$. Il suffit donc de démontrer que $PA[X] = PK[X] \cap A[X]$ pour conclure que $PA[X]$ est premier dans $A[X]$. Il est clair que $PA[X] \subset PK[X] \cap A[X]$. Démontrons l'autre inclusion : soit $PQ \in PK[X] \cap A[X]$, avec $Q \in K[X]$ et $PQ \in A[X]$. Nous allons démontrer que $Q \in A[X]$. En réduisant les coefficients de $Q$ au même dénominateur, on peut écrire $dQ = Q'$ avec $d \in A$ et $Q' \in A[X]$. Notons $c$ un contenu de $Q'$. Puisque $P$ est primitif, $c$ est un contenu de $PQ'$. Or $PQ' = dPQ$ avec $PQ \in A[X]$, donc $d$ divise $c$. Posons $c = da$ avec $a \in A$. On sait qu'il existe un polynôme primitif $Q_1 \in A[X]$ tel que $Q' = cQ_1 = daQ_1$. On en déduit que $PQ = aPQ_1$ et donc que $Q = aQ_1 \in A[X]$. ✓

**Théorème 17.** Si $A$ est factoriel et $n \in \mathbb{N}^*$, alors $A[X_1, \ldots, X_n]$ est factoriel.

*Démonstration.* Par récurrence sur $n$ à l'aide du théorème **16**. ✓

***Remarque.*** On vérifie facilement que si $A$ est un anneau tel que $A[X_1, \ldots, X_n]$ est factoriel, alors $A$ est factoriel.

Cependant, en général, un sous-anneau ou un anneau quotient d'un anneau factoriel n'est pas factoriel. Par exemple, $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel (cf. TD) mais c'est un sous-anneau de $\mathbb{C}$ qui est factoriel et il est isomorphe au quotient $\mathbb{Z}[X]/(X^2+3)$ de $\mathbb{Z}[X]$ qui est factoriel.

## III.2. Tests d'irréductibilité.

**Rappel.** Un élément $a \in A$ est une racine d'un polynôme $f$ de $A[X]$ si et seulement si le polynôme $X - a$ divise $f$ dans $A[X]$.

Il en découle que si $A$ est intègre, le nombre de racines de $f$ dans $A$ est au plus $\deg(f)$.

**Proposition 18.** Soit $A$ un anneau.

**(1)** Soit $a \in A$ et soit $f \in A[X]$. Alors $f$ est irréductible dans $A[X]$ si, et seulement si, $f(X-a)$ est irréductible.

**(2)** On suppose que $A$ est intègre. Alors pour tout $a \in A$ le polynôme $X - a$ est irréductible.

**(3)** On suppose que $A$ est intègre. Si $f \in A[X]$ est irréductible et si $\deg(f) \geqslant 2$, alors $f$ n'a pas de racine dans $A$.

**(4)** Soit $K$ un corps. Soit $f \in K[X]$ un polynôme de degré 2 ou 3. Alors $f$ est irréductible si, et seulement si, $f$ n'a pas de racine dans $K$.

*Démonstration.* **(1)** Si $f(X-a) = P(X)Q(X)$ avec $P$ et $Q$ non inversibles, alors $f(X) = P(X+a)Q(X+a)$, et $P(X+a)$ et $Q(X+a)$ ne sont pas inversibles (en effet, s'il existe $R$ tel que $P(X+a)R(X) = 1$ donc $P(X)R(X-a) = 1$ et donc $P$ est inversible, ce qui est une contradiction).

**(2)** On rappelle que $A[X]^\times = A^\times$ lorsque $A$ est intègre. Notons que $X - a$ n'est pas nul et n'est pas inversible. Si $X - a = PQ$ alors $P$ et $Q$ ne sont pas nuls et donc $\deg P \geqslant 0$, $\deg Q \geqslant 0$ et $\deg P + \deg Q = \deg(X-a) = 1$ (puisque $A$ est intègre), et finalement on doit avoir $\deg P = 0$ ou $\deg Q = 0$ c'est-à-dire que $P$ ou $Q$ est constant, par exemple $P$. Si on pose $P = b$ et $Q = cX + d$, on a alors $ac = 1$ (en identifiant) et donc $P = a$ est inversible dans $A$ donc dans $A[X]$.

Finalement, $X - a$ est irréductible.

**(3)** Si $f$ a une racine $a$ dans $A$, alors $X - a$ divise $f$ donc $f = (X-a)P$ et on a $\deg P = \deg f - 1 \geqslant 1$ (car $A$ est intègre). Puisque $A$ est intègre, les polynômes non constants ne sont pas inversibles donc $f$ n'est pas irréductible.

**(4)** Puisque $K$ est intègre et que $\deg f \geqslant 2$, on a déjà vu que si $f$ est irréductible alors $f$ n'a pas de racine dans $A$.

Réciproquement, supposons que $f$ est réductible. Alors il existe $P$ et $Q$ non constants tels que $f = PQ$. On a $\deg P + \deg Q \in \{2; 3\}$ et $\deg P \geqslant 1$, $\deg Q \geqslant 1$, donc $\deg P = 1$ ou $\deg Q = 1$. Or un polynôme de degré 1 à coefficients dans un corps $K$ a nécessairement une racine, donc $f$ aussi. ✓

***Remarque.*** Notons que si $A$ n'est pas intègre, les éléments inversibles de $A[X]$ ne sont pas tous de degré 0. Par exemple, dans $\mathbb{Z}/4\mathbb{Z}[X]$ on a $(2X+1)^2 = 1$ donc $2X+1$ est inversible mais n'est pas constant. Il faut donc faire attention dans la démonstration de l'affirmation **(1)**.

***Remarque.*** Les affirmations **(2)** et **(3)** sont fausses si $A$ n'est pas intègre.
Exercice : rechercher des contre-exemples.

- *Pour* **(2)** *: dans* $\mathbb{Z}/6\mathbb{Z}[X]$ *on a* $X-1=(2X+1)(3X-1)$ *avec* $2X+1$ *et* $3X-1$ *non inversibles. En effet, si* $(2X+1)P=1$ *avec* $P=\sum_{i=0}^{d}a_iX^i$ *et* $a_d\neq 0$*, alors* $a_0=1$*,* $2a_d=0$ *et* $a_{i+1}=4a_i$ *pour tout* $i$ *avec* $0\leqslant i\leqslant d-1$*, d'où* $a_i=4$ *pour tout* $i\in[\![1\,;d]\!]$*, mais alors* $0=2a_d=2\cdot 4=2$ *(ou* $0=2a_0=2$ *si* $d=0$*), une contradiction ; pour* $3X-1$ *on peut raisonner de la même façon.*
  *Autre contre-exemple : notons* $e=(1,0)\in\mathbb{Z}^2$*; dans* $\mathbb{Z}^2[X]$*, on a* $X=(eX+(1-e))((1-e)X+e)$ *avec* $eX+(1-e)$ *et* $(1-e)X+e$ *non inversibles car leurs coefficients constants* $e$ *et* $1-e$ *ne sont pas inversibles.*
- *Pour* **(3)**, $2X^2+X\in\mathbb{Z}/4\mathbb{Z}[X]$ *est de degré* 2*, il admet* 0 *comme racine, mais il est irréductible. En effet,* $2X^2+X=(2X+1)X$ *avec* $2X+1$ *inversible (cf. remarque précédente), donc il suffit de démontrer que* $X$ *est irréductible. Supposons donc que* $X=PQ$ *avec* $P=\sum_{i=0}^{d}a_iX^i$ *et* $Q=\sum_{i=0}^{e}b_iX^i$*. Alors* $a_0b_0=0$ *et* $a_0b_1+a_1b_0=1$*. Dans* $\mathbb{Z}/4\mathbb{Z}$*,* $a_0b_0=0$ *implique* $a_0=0$ *ou* $b_0=0$ *ou* $(a_0,b_0)=(2,2)$*, mais si* $a_0=2=b_0$ *alors* $2(b_1+a_1)=1$ *et donc* 2 *est inversible, une contradiction. Donc* $a_0$ *ou* $b_0$ *est nul, par exemple* $a_0$*. Ecrivons* $P=XP_1$*. On a donc* $X(P_1Q-1)=0$*. Mais si* $XR=0$*, on vérifie facilement que* $R=0$ *donc* $P_1Q=1$ *et donc* $Q$ *est inversible.*

***Remarque.*** L'affirmation **(4)** est fausse si on remplace $K$ par un anneau (même intègre). Exercice : rechercher des contre-exemples.

*Dans* $\mathbb{Z}[X]$*, le polynôme* $2(X^2+1)$ *est de degré* 2 *et sans racine mais il n'est pas irréductible (*2 *et* $X^2+1$ *ne sont pas inversibles).*

**Proposition 19** (Test des racines entières)**.** Soit $A$ un anneau factoriel et soit $K$ son corps des fractions. Soit $P=\sum_{i=0}^{n}a_iX^i\in A[X]$ avec $a_n\neq 0$, $n\geqslant 1$, et soit $\alpha=\frac{p}{q}\in K$ une racine de $P$ dans $K$ avec $p$ et $q$ deux éléments premiers entre eux de $A$. Alors $q$ divise $a_n$ et $p$ divise $a_0$.

*Démonstration.* cf. TD. ✓

Soit $I$ un idéal de l'anneau $A$. On note $\varphi_I : A[X]\to(A/I)[X]$ le morphisme d'anneaux de l'exemple page 19.

**Proposition 20** (Critère de réduction)**.** Soient $A$ un anneau factoriel et $I$ un idéal premier de $A$. Soit $P=\sum_{i=0}^{n}a_iX^i\in A[X]$ avec $a_n\notin I$, $n\geqslant 1$; si $\varphi_I(P)$ est irréductible dans $(A/I)[X]$ ou dans $(\mathrm{Frac}(A/I))[X]$, alors $P$ est irréductible dans $(\mathrm{Frac}\,A)[X]$.

*Démonstration.* Notons $K=\mathrm{Frac}\,A$. On peut remarquer que $I$ est premier donc $A/I$ est intègre, il a donc bien un corps des fractions.
Supposons que $P=QR$ avec $Q,R$ dans $K[X]$. Grâce au lemme **14**, on peut supposer que $Q$ et $R$ sont dans $A[X]$. Posons $Q=\sum_{i=0}^{q}b_iX^i$ et $R=\sum_{i=0}^{r}c_iX^i$ avec $a_n=b_qc_r\notin I$. On a $\varphi_I(P)=\varphi_I(Q)\varphi_I(R)$. Puisque $\varphi_I(P)$ est irréductible dans $(A/I)[X]$ ou dans $(\mathrm{Frac}(A/I))[X]$, par exemple $\varphi_I(Q)$ est inversible dans $(A/I)[X]$ ou dans $(\mathrm{Frac}(A/I))[X]$, donc dans les deux cas c'est un élément non nul de $\mathrm{Frac}(A/I)$. Donc $\deg\varphi_I(Q)=0$. Mais $0\neq\overline{a}_n=\overline{b}_q\overline{c}_r$, donc $\overline{b}_q\neq 0$, et donc $\deg\varphi_I(Q)=q$. Donc $\deg Q=q=0$ et $Q$ est une constante non nulle de $K$, donc inversible dans $K$ et donc dans $K[X]$. Donc $P$ est irréductible dans $K[X]$. ✓

**Proposition 21** (Critère d'Eisenstein)**.** Supposons $A$ factoriel et considérons $P=\sum_{i=0}^{n}a_iX^i\in A[X]$ avec $n=\deg P\geqslant 1$. S'il existe un élément irréductible $p$ de $A$ tel que $p\nmid a_n$, $p|a_i$ pour $0\leqslant i\leqslant n-1$ et $p^2\nmid a_0$, alors $P$ est irréductible dans $(\mathrm{Frac}\,A)[X]$.

*Démonstration.* Notons $K=\mathrm{Frac}\,A$. Puisque $\deg P\geqslant 1$, $P$ n'est pas inversible dans $K[X]$. Supposons que $P$ ne soit pas irréductible dans $K[X]$. Alors, il existe $Q,R$ dans $K[X]$ tels que $P=QR$ et $0<q=\deg Q<\deg P$ et $0<r=\deg R<\deg P$. D'après le lemme **14**, on peut supposer que $Q,R$ sont dans $A[X]$. Posons $Q=\sum_{j=0}^{q}b_jX^j$ et $R=\sum_{k=0}^{r}c_kX^k$. Comme $p$ ne divise pas $a_n$, $p$ ne divise ni $b_q$ ni $c_r$. Comme $p$ divise $a_0$ et $p^2$ ne divise pas $a_0$, l'égalité $a_0=b_0c_0$ assure que $p$ divise $b_0$ ou $c_0$ (car $A$ satisfait la condition d'Euclide) mais pas les deux. Quitte à échanger $Q$ et $R$, on peut supposer que $p$ divise $c_0$ et pas $b_0$. Soit donc $\ell=\inf\{1\leqslant i\leqslant r \text{ tel que } p\nmid c_i\}$ ; comme $r<n$, l'égalité $a_\ell=b_0c_\ell+\cdots+b_\ell c_0$ montre que $b_0c_\ell$ est divisible par $p$ et donc que $c_\ell$ est divisible par $p$. Ceci constitue une contradiction. ✓

# CHAPITRE 3

# *Polynômes symétriques*

Ce chapitre n'a pas été traité en 2016-2017.

## I L'ANNEAU DES POLYNÔMES SYMÉTRIQUES

Soit $A$ un anneau quelconque (commutatif et unitaire).

***Notation.*** Soit $n \in \mathbb{N}^*$, soit $f \in A[X_1, \dots, X_n]$ un polynôme et soit $\gamma \in \mathfrak{S}_n$. On note ${}^{\gamma}f$ le polynôme $f(X_{\gamma(1)}, \dots, X_{\gamma(n)})$.

**Définition 1.** *Un polynôme $f \in A[X_1, \dots, X_n]$ est dit **symétrique** si pour tout $\gamma \in \mathfrak{S}_n$ on a ${}^{\gamma}f = f$.*

***Exemples.*** ✦ $X^2 + Y^2 + Z^2$ est un polynôme symétrique de $\mathbb{Z}[X, Y, Z]$ (mais pas de $\mathbb{Z}[X, Y, Z, T]$).
✦ $X_1X_2 + X_2X_3 + X_3X_1$ est un polynôme symétrique de $\mathbb{Z}[X_1, X_2, X_3]$.
✦ $X^3Y + Y^3Z + Z^3X$ n'est pas un polynôme symétrique de $\mathbb{Z}[X, Y, Z]$.

***Remarque.*** Si $f$ est un polynôme symétrique, alors le degré partiel de $f$ par rapport à chacune de ses variables est le même, et on l'appelle **degré partiel** de $f$.

**Lemme 2.** Soit $\varphi : A[X_1, \dots, X_n] \to A[X_1, \dots, X_{n-1}]$ l'unique morphisme d'anneaux qui fixe les éléments de $A$ ainsi que $X_1, \dots, X_{n-1}$ et qui vérifie $\varphi(X_n) = 0$, obtenu grâce à la propriété universelle des anneaux de polynômes. On a $\varphi(P) = P(X_1, \dots, X_{n-1}, 0)$.
Soit $f \in A[X_1, \dots, X_n]$ un polynôme symétrique. Alors $\varphi(f)$ est un polynôme symétrique de $A[X_1, \dots, X_{n-1}]$.

*Démonstration.* Soit $\gamma \in \mathfrak{S}_{n-1}$ et soit $\gamma' \in \mathfrak{S}_n$ la permutation définie par $\gamma'_{|[\![1;n-1]\!]} = \gamma$ et $\gamma'(n) = n$.
Alors ${}^{\gamma}\varphi(f) = \varphi({}^{\gamma'}f) = \varphi(f)$, ce que l'on voulait. ✓

**Lemme 3.** Soit $\gamma \in \mathfrak{S}_n$. Soit $\psi_\gamma : A[X_1, \dots, X_n] \to A[X_1, \dots, X_n]$ l'application définie par $\psi_\gamma(P) = {}^{\gamma}P$. Alors $\psi_\gamma$ est un automorphisme d'anneaux qui fixe les éléments de $A$.

*Démonstration.* Notons que $\psi_\gamma$ est l'unique morphisme d'anneaux qui fixe les éléments de $A$ et qui vérifie $\psi_\gamma(X_i) = X_{\gamma(i)}$ pour tout $i$. Il admet comme réciproque $\psi_{\gamma^{-1}}$, qui est l'unique morphisme d'anneaux qui fixe les éléments de $A$ et qui vérifie $\psi_\gamma(X_i) = X_{\gamma^{-1}(i)}$ pour tout $i$. En effet, $\psi_\gamma \circ \psi_{\gamma^{-1}}$ et $\mathrm{id}_{A[X_1,\dots,X_n]}$ sont deux morphismes d'anneaux qui prolongent $A \hookrightarrow A[X_1, \dots, X_n]$ et qui fixent tous les $X_i$, donc par l'unicité dans la propriété universelle 2.5 ils sont égaux. De même, $\psi_{\gamma^{-1}} \circ \psi_\gamma = \mathrm{id}_{A[X_1,\dots,X_n]}$, donc $\psi_\gamma$ est bien un automorphisme d'anneaux. ✓

**Conséquence 4.** L'ensemble des polynômes symétriques est un sous-anneau de $A[X_1,\dots,X_n]$.

En effet, on a ${}^\gamma(f-g) = {}^\gamma f - {}^\gamma g$, ${}^\gamma(fg) = ({}^\gamma f)({}^\gamma g)$ et ${}^\gamma 1 = 1$ puisque $\psi_\gamma$ est un morphisme d'anneaux. En particulier, la somme et le produit de polynômes symétriques sont des polynômes symétriques.

***Remarque.*** On vérifie facilement que l'application $\psi : \mathfrak{S}_n \to \mathrm{Aut}(A[X_1,\dots,X_n])$ qui à $\gamma$ associe $\psi_\gamma$ est un morphisme de groupes, c'est-à-dire que pour tout $(\gamma,\tau) \in \mathfrak{S}_n^2$ on a $\psi(\gamma\tau) = \psi(\gamma)\psi(\tau)$ ou autrement dit

$$\forall(\gamma,\tau)\in\mathfrak{S}_n^2,\ \forall f \in A[X_1,\dots,X_n],\ {}^\gamma({}^\tau f) = {}^{\gamma\tau} f.$$

On a donc une action du groupe $\mathfrak{S}_n$ sur $A[X_1,\dots,X_n]$.

## II Polynômes symétriques élémentaires

**Définition 5.** *Soit $k \in [\![1\,;n]\!]$. Le polynôme $\sigma_k = \sum_{\substack{H\subset[\![1;n]\!]\\|H|=k}} \left(\prod_{i\in H} X_i\right)$ de $A[X_1,\dots,X_n]$ est un polynôme symétrique, appelé **$k$-ième polynôme symétrique élémentaire**. On pose $\sigma_0 = 1$.*

***Remarque.*** On a $\deg\sigma_k = k$ (où deg désigne le degré total).

On peut écrire $\sigma_k = \sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n} X_{i_1}X_{i_2}\cdots X_{i_k}$.

***Notation.*** Lorsqu'il peut y avoir ambiguïté, on écrira $\sigma_{n,k}$ pour le $k$-ième polynôme symétrique élémentaire en $X_1,\dots,X_n$ (on précise le nombre d'indéterminées dans la notation).

***Exemples.*** ✦ $\sigma_1 = X_1 + \cdots + X_n$.

✦ $\sigma_2 = X_1X_2 + X_1X_3 + \cdots + X_1X_n + X_2X_3 + \cdots + X_{n-1}X_n$.

✦ $\sigma_n = X_1X_2\cdots X_n$.

**Lemme 6.** Les polynômes symétriques élémentaires sont symétriques.

*Démonstration.* Soit $\gamma \in \mathfrak{S}_n$. Alors

$${}^\gamma\sigma_k = \sum_{\substack{H\subset[\![1;n]\!]\\|H|=k}} \left(\prod_{i\in H} X_{\gamma(i)}\right) \overset{j=\gamma(i)}{=} \sum_{\substack{H\subset[\![1;n]\!]\\|H|=k}} \left(\prod_{j\in\gamma^{-1}(H)} X_j\right) \overset{H'=\gamma^{-1}(H)}{=} \sum_{\substack{H'\subset[\![1;n]\!]\\|H'|=k}} \left(\prod_{j\in H'} X_j\right) = \sigma_k. \qquad \checkmark$$

**Lemme 7.** ✦ Soit $\varphi : A[X_1,\dots,X_{n+1}] \to A[X_1,\dots,X_{n+1}]$ le morphisme du lemme 2, défini par $\varphi(P) = P(X_1,\dots,X_n,0)$. Alors $\varphi(\sigma_{n+1,k}) = \sigma_{n,k}$ pour tout $k \in [\![1\,;n]\!]$, autrement dit, $\sigma_{n,k} = \sigma_{n+1,k}(X_1,\dots,X_n,0)$.

✦ On a $\sigma_{n+1,0} = 1$, $\sigma_{n+1,n+1} = \sigma_{n,n}X_{n+1}$ et $\sigma_{n+1,k} = \sigma_{n,k} + \sigma_{n,k-1}X_{n+1}$ pour tout $k \in [\![0\,;n]\!]$.

*Démonstration.* La première partie est évidente (ou se déduit de la deuxième). Pour la deuxième, on a

$$\begin{aligned}
\sigma_{n,k} + \sigma_{n,k-1}X_{n+1} &= \sum_{\substack{H\subset[\![1;n]\!]\\|H|=k}} \left(\prod_{i\in H} X_i\right) + \sum_{\substack{H'\subset[\![1;n]\!]\\|H'|=k-1}} \left(\prod_{i\in H'} X_i\right) X_{n+1} \\
&= \sum_{\substack{H\subset[\![1;n+1]\!]\\|H|=k \text{ et } n+1\notin H}} \left(\prod_{i\in H} X_i\right) + \sum_{\substack{H\subset[\![1;n+1]\!]\\|H|=k \text{ et } n+1\in H}} \left(\prod_{i\in H} X_i\right) \\
&= \sum_{\substack{H\subset[\![1;n+1]\!]\\|H|=k}} \left(\prod_{i\in H} X_i\right) = \sigma_{n+1,k}. \qquad \checkmark
\end{aligned}$$

**Lemme 8.** Soit $P \in A[X_1, \dots, X_n]$ un polynôme symétrique et supposons que $X_i$ divise $P$ pour un $i \in [\![1\,;n]\!]$. Alors $\sigma_n$ divise $P$.

*Démonstration.* Quitte à permuter les indéterminées, on peut supposer que $i = n$. On raisonne par récurrence sur $n$.

✦ Si $n = 1$, c'est clair car $\sigma_{1,1} = X_1$.

✦ Supposons le résultat vrai au rang $n-1$ pour un entier $n > 1$. Posons

$$P = P_0 + P_1 X_n + P_2 X_n^2 + \cdots + P_d X_n^d$$

avec $P_i \in A[X_1, \dots, X_{n-1}]$ pour tout $i$. Puisque $P(X_1, \dots, X_{n-1}, 0) = 0$ par hypothèse, on a $P_0 = 0$.
Vérifions que les $P_i$ sont des polynômes symétriques de $A[X_1, \dots, X_{n-1}]$. Soit donc $\gamma \in \mathfrak{S}_{n-1}$ et soit $\gamma' \in \mathfrak{S}_n$ égal à $\gamma$ sur $[\![1\,;n-1]\!]$ et tel que $\gamma'(n) = n$. On a alors

$$P = {}^{\gamma'}P = \sum_{i=1}^{d} {}^{\gamma'}P_i ({}^{\gamma'}X_n)^i = \sum_{i=1}^{d} {}^{\gamma}P_i X_n^i$$

donc en identifiant, ${}^{\gamma}P_i = P_i$ pour tout $i$. Donc $P_i$ est symétrique.
Soit maintenant $\tau = (n-1, n) \in \mathfrak{S}_n$. Alors $P = {}^{\tau}P = P(X_1, \dots, X_{n-2}, X_n, X_{n-1})$. On applique le morphisme $\varphi$ du lemme 2 (ie. $X_n \mapsto 0$). On obtient donc

$$0 = \varphi(P) = P(X_1, \dots, X_{n-2}, 0, X_{n-1}) = \sum_{i=1}^{d} P_i(X_1, \dots, X_{n-2}, 0) X_{n-1}^i.$$

On en déduit par identification que pour tout $i$, $1 \leqslant i \leqslant d$, on a $P_i(X_1, \dots, X_{n-2}, 0)$. Par hypothèse de récurrence, on sait que $\sigma_{n-1,n-1} = X_1 \cdots X_{n-1}$ divise $P_i$ pour tout $i$, posons $P_i = Q_i X_1 \cdots X_{n-1}$. Alors $P = \sum_{i=1}^{d} P_i X_n^i = \sum_{i=1}^{d} Q_i X_1 \cdots X_{n-1} X_n^i$ est un multiple de $X_1 \cdots X_n = \sigma_{n,n}$. ✓

***Remarque.*** Pour tout polynôme $P \in A[X_1, \dots, X_n]$, on a $\deg(P\sigma_n) = \deg P + n$ (où deg désigne le degré total). En particulier, si $P\sigma_n = 0$ alors $P = 0$.
En effet, posons $P = \sum_{\underline{i} \in \mathbb{N}^n} a_{\underline{i}} X_1^{i_1} \cdots X_n^{i_n}$ et $\deg P = \max\{\sum_{k=1}^{n} i_k ;\ a_{\underline{i}} \neq 0\}$. On a alors $P\sigma_n = \sum_{\underline{i} \in \mathbb{N}^n} a_{\underline{i}} X_1^{i_1+1} \cdots X_n^{i_n+1}$ donc $\deg(P\sigma_n) = \max\{\sum_{k=1}^{n}(i_k+1) ;\ a_{\underline{i}} \neq 0\} = \max\{(\sum_{k=1}^{n} i_k) + n ;\ a_{\underline{i}} \neq 0\} = \deg P + n$.

**Proposition 9.** Soit $P$ un polynôme tel que $P(\sigma_1, \dots, \sigma_n) = 0$. Alors $P = 0$.

*Démonstration.* On raisonne par récurrence sur $n$.

✦ Si $n = 1$, le résultat est clair ($\sigma_1 = X_1$).

✦ Soit $n \geqslant 2$ et supposons le résultat vrai au rang $n-1$. Soit $\mathcal{S}$ l'ensemble des polynômes $f \in A[X_1, \dots, X_n]$ non nuls tels que $f(\sigma_{n,1}, \dots, \sigma_{n,n}) = 0$. On veut démontrer que $\mathcal{S} = \varnothing$. Supposons par l'absurde que $\mathcal{S} \neq \varnothing$.
L'ensemble $\{\deg f ;\ f \in \mathcal{S}\}$ est une partie non vide de $\mathbb{N}$ donc admet un minimum $d_0$. Soit $P \in \mathcal{S}$ de degré $d_0$. Posons $P = \sum_{i=0}^{d} P_i X_n^i$ avec $P_i \in A[X_1, \dots, X_{n-1}]$.
Si $P_0 = 0$ alors $P = X_n Q$ pour un $Q \in A[X_1, \dots, X_n]$. Notons que $Q \neq 0$. On a dans ce cas $0 = P(\sigma_{n,1}, \dots, \sigma_{n,n}) = \sigma_{n,n} Q(\sigma_{n,1}, \dots, \sigma_{n,n}) = X_1 \cdots X_n Q(\sigma_{n,1}, \dots, \sigma_{n,n})$. On en déduit que $Q(\sigma_{n,1}, \dots, \sigma_{n,n}) = 0$ d'après la remarque précédente. Mais $\deg Q < d_0$ et $Q \in \mathcal{S}$ (puisque $Q \neq 0$), donc on a obtenu une contradiction.
Par conséquent, $P_0 \neq 0$, et donc $P(X_1, \dots, X_{n-1}, 0) = P_0(X_1, \dots, X_{n-1}) \neq 0$. Par hypothèse de récurrence, on en déduit que $P_0(\sigma_{n-1,1}, \dots, \sigma_{n-1,n-1}) \neq 0$. Mais on a

$$\begin{aligned} P_0(\sigma_{n-1,1}, \dots, \sigma_{n-1,n-1}) &= P(\sigma_{n-1,1}, \dots, \sigma_{n-1,n-1}, 0) \\ &= P(\sigma_{n,1}(X_1, \dots, X_{n-1}, 0), \dots, \sigma_{n,n-1}(X_1, \dots, X_{n-1}, 0), \sigma_{n,n}(X_1, \dots, X_{n-1}, 0)) = 0 \end{aligned}$$

en utilisant le lemme 7. On a donc bien une contradiction. ✓

**Définition 10.** *Le **poids** d'un monôme $X_1^{i_1}\cdots X_n^{i_n}$ est l'entier $i_1+2i_2+3i_3+\cdots+ni_n$.*

*Le **poids** d'un polynôme est le maximum des poids des monômes qui le constituent : si $P = \sum_{\underline{i}\in\mathbb{N}^n} a_{\underline{i}} X_1^{i_1}\cdots X_n^{i_n}$, le poids de $P$ est $\max\left\{\text{poids}(X_1^{i_1}\cdots X_n^{i_n})\,;\, a_{\underline{i}}\neq 0\right\} = \max\left\{i_1+2i_2+3i_3+\cdots+ni_n\,;\, a_{\underline{i}}\neq 0\right\}$.*

***Exemple.*** Le polynôme $P = X_1 + X_1X_2^2 + X_1X_3$ est de poids $\max(1,5,4) = 5$.

***Remarque.*** Le degré de $P(\sigma_1,\dots,\sigma_n)$ est inférieur ou égal au poids de $P$.

Vérifions d'abord cela dans le cas où $P = X_1^{\alpha_1}\cdots X_n^{\alpha_n}$ est un monôme. On a $\deg P(\sigma_1,\dots,\sigma_n) = \alpha_1\deg\sigma_1+\cdots+\alpha_n\deg\sigma_n = \sum_{i=1}^n \alpha_i i$ qui est bien le poids de $P$ (on a égalité car tous les polynômes $\sigma_k$ sont unitaires.

Soit maintenant $P = \sum_{j=1}^r M_j$ un polynôme non nul où les $M_j$ sont des monômes. Par définition, $\text{poids}(P) = \max\{\text{poids}(M_j);\ 1\leqslant j\leqslant r\}$. On a alors

$$\deg P(\sigma_1,\dots,\sigma_n) \leqslant \max\{\deg M_j(\sigma_1,\dots,\sigma_n);\ 1\leqslant j\leqslant r\} = \max\{\text{poids}(M_j);\ 1\leqslant j\leqslant r\} = \text{poids}(P).$$

**Théorème 11.** Soit $A$ un anneau. Soit $P\in A[X_1,\dots,X_n]$ un polynôme symétrique. Alors il existe un unique polynôme $T\in A[Y_1,\dots,Y_n]$ tel que $T(\sigma_1,\dots,\sigma_n) = P$. Ce polynôme est de poids $d = \deg(P)$.

***Exemple.*** ✦ Si $P = X_1^2+X_2^2\in\mathbb{Z}[X_1,X_2]$, on a $P = (X_1+X_2)^2 - 2X_1X_2 = \sigma_1^2-2\sigma_2$. Le polynôme $T$ est donc $T = Y_1^2-2Y_2$.

✦ Si $P = X_1^3X_2+X_1X_2^3\in\mathbb{Z}[X_1,X_2]$, on a $P = X_1X_2(X_1^2+X_2^2) = \sigma_2(\sigma_1^2-2\sigma_2)$ et $T = Y_1^2Y_2-2Y_2^2$.

*Démonstration.* L'unicité découle de la proposition 9. Démontrons l'existence.

On raisonne par récurrence sur $n$ (le nombre d'indéterminées).

✦ Si $n=1$, le résultat est évident, car $\sigma_{1,1} = X_1$.

✦ Soit $n>1$ et supposons que le résultat est vrai pour les polynômes symétriques de $A[X_1,\dots,X_{n-1}]$. Soit $P\in A[X_1,\dots,X_n]$ un polynôme symétrique de degré total $d\in\mathbb{N}$. On fait maintenant un raisonnement par récurrence sur $d$.

✧ Si $d=0$, c'est évident ($P$ est constant).

✧ Soit $d>0$ et supposons le résultat vrai pour les polynômes symétriques de $A[X_1,\dots,X_n]$ de degré total inférieur ou égal à $(d-1)$.

Soit $\varphi$ le morphisme du lemme 2. Puisque le polynôme $\varphi(P)$ est un polynôme symétrique de $A[X_1,\dots,X_{n-1}]$, par hypothèse de récurrence (sur $n$), il existe un unique polynôme $V\in A[Y_1,\dots,Y_{n-1}]$ de poids inférieur ou égal à $d$ tel que $\varphi(P) = V(\sigma_{n-1,1},\dots,\sigma_{n-1,n-1})$.

Posons $P' = V(\sigma_{n,1},\dots,\sigma_{n,n-1})$. Notons que $\deg P'\leqslant\text{poids}(V)\leqslant d$. Alors $P'$ est un polynôme symétrique de $A[X_1,\dots,X_n]$ et on a $\varphi(P-P') = 0$ donc $X_n$ divise $P-P'$ dans $A[X_1,\dots,X_n]$. On en déduit grâce au lemme 8 que $\sigma_{n,n}$ divise $P-P'$.

Posons $P-P' = Q\sigma_{n,n}$. Alors $Q$ est symétrique ; en effet, si $\gamma\in\mathfrak{S}_n$, alors $({}^\gamma Q)\sigma_{n,n} = {}^\gamma(Q\sigma_{n,n}) = {}^\gamma(P-P') = P-P' = Q\sigma_{n,n}$ et on en déduit que ${}^\gamma Q = Q$ (cf. remarque p. 29). De plus, $\deg Q = \deg(Q\sigma_{n,n})-n = \deg(P-P')-n\leqslant d-n<d$ donc, par hypothèse de récurrence, on peut écrire $Q = W(\sigma_{n,1},\dots,\sigma_{n,n})$ pour un unique polynôme $W\in A[Y_1,\dots,Y_n]$ de poids $\deg Q$.

Posons enfin $T = V+WY_n$. On a $T(\sigma_{n,1}\dots,\sigma_{n,n}) = V(\sigma_{n,1}\dots,\sigma_{n,n}) + W(\sigma_{n,1}\dots,\sigma_{n,n})\sigma_{n,n} = P' + Q\sigma_{n,n} = P$. On a donc démontré l'existence.

On a de plus $\text{poids}(T)\leqslant\max(\text{poids}(V), n+\text{poids}(W))\leqslant d$ et si $\text{poids}(T)<d$ alors $d = \deg P = \deg T(\sigma_{n,1},\dots,\sigma_{n,n})\leqslant\text{poids}(T)<d$, une contradiction. On en déduit donc que $\text{poids}(T) = d = \deg P$. ✓

**Définition 12.** *Un polynôme $f\in A[X_1,\dots,X_n]$ est dit **homogène** si tous ses monômes sont de même degré. Ce degré commun est nécessairement le degré total de $f$, on l'appelle **degré** du polynôme homogène $f$.*

***Remarque.*** ✦ Tout polynôme $f$ s'écrit de manière unique comme somme de polynômes homogènes, que l'on appelle **composantes homogènes** de $f$.

✦ Si $f$ est un polynôme symétrique, alors ses composantes homogènes sont symétriques.
En effet, posons $f = \sum_{i=1}^{r} f_i$ avec $f_i$ homogènes de degrés deux à deux distincts. Soit $\gamma \in \mathfrak{S}_n$. Alors $\sum_{i=1}^{r} f_i = f = {}^{\gamma}f = \sum_{i=1}^{r} {}^{\gamma}f_i$ donc pour tout $i$ on a ${}^{\gamma}f_i = f_i$.

✦ Pour tout $k$, le polynôme $\sigma_k$ est homogène de degré $k$ et de degré partiel 1.

***Remarque.*** Dans la pratique, afin de simplifier les calculs, avant d'appliquer la méthode de la démonstration pour trouver $T$, on écrit $P$ comme somme de polynômes homogènes et on applique la méthode à chaque composante homogène.

On suit alors la procédure suivant pour un $P$ homogène :

(i) On calcule $\varphi(P)$ et on trouve $V \in A[Y_1, \dots, Y_{n-1}]$ tel que $\varphi(P) = V(\sigma_{n-1,1}, \dots, \sigma_{n-1,n-1})$ en suivant la procédure récursive (on recommence jusqu'à n'avoir qu'une indéterminée ou avoir une expression en les polynômes symétriques élémentaires).

(ii) On détermine $Q \in A[X_1, \dots, X_n]$ symétrique tel que $P - V(\sigma_{n,1}, \dots, \sigma_{n,n-1}) = Q\sigma_{n,n}$.

(iii) On trouve $W \in A[Y_1, \dots, Y_n]$ tel que $Q = W(\sigma_{n,1}, \dots, \sigma_{n,n})$ par la procédure récursive.

(iv) On pose $T = V + WY_n$.

***Exemple.*** **(1)** $P = XYZ + X^2Y + X^2Z + Y^2Z + XY^2 + XZ^2 + YZ^2$. Soit $\varphi_Z : A[X, Y, Z] \to A[X, Y]$ le morphisme d'anneaux donné par $\varphi_Z(P) = P(X, Y, 0)$.

✦ On a $\varphi_Z(P) = X^2Y + XY^2 = XY(X + Y) = \sigma_{2,2}\sigma_{2,1}$ (autrement dit, $V = XY$).

✦ On considère $P - V(\sigma_{3,1}\sigma_{3,2}) = P - (X + Y + Z)(XY + XZ + YZ) = -2XYZ = -2\sigma_{3,3}$ (autrement dit, $Q = -2$).

✦ On pose $T = V + QZ$ et on a bien $P = T(\sigma_{3,1}, \sigma_{3,2}, \sigma_{3,3}) = \sigma_{3,1}\sigma_{3,2} - 2\sigma_{3,3}$.

**(2)** $P = X_1^3 + X_2^3 + X_3^3$. On note $\varphi_3 \colon A[X_1, X_2, X_3] \to A[X_1, X_2]$ et $\varphi_2 \colon A[X_1, X_2] \to A[X_1]$ les morphismes d'anneaux du lemme 2.

✦ On a $\varphi_3(P) = X_1^3 + X_2^3$.

✧ On a $\varphi_2(\varphi_3(P)) = X_1^3 = \sigma_{1,1}^3$.

✧ $\varphi_3(P) - \sigma_{2,1}^3 = (X_1^3 + X_2^3) - (X_1 + X_2)^3 = -3X_1^2X_2 - 3X_1X_2^2 = -3(X_1 + X_2)\sigma_{2,2} = -3\sigma_{2,1}\sigma_{2,2}$ donc $\varphi_3(P) = \sigma_{2,1}^3 - 3\sigma_{2,1}\sigma_{2,2}$.

✧ $P - (\sigma_{3,1}^3 - 3\sigma_{3,1}\sigma_{3,2}) = 3X_1X_2X_3 = 3\sigma_{3,3}$ (d'où $Q = 3$).

✦ Donc $P = \sigma_{3,1}^3 - 3\sigma_{3,1}\sigma_{3,2} + 3\sigma_{3,3} = T(\sigma_{3,1}, \sigma_{3,2}, \sigma_{3,3})$ avec $T = X_1^3 - 3X_1X_2 + 3X_3$.

Notons que le poids de $T$ est bien $3 = \deg P$.

On peut résumer nos résultats.

**Théorème 13.** L'endomorphisme d'anneaux de $A[X_1, \dots, X_n]$ qui à $P$ associe $P(\sigma_1, \dots, \sigma_n)$ obtenu grâce à la propriété universelle est injectif et a pour image le sous-anneau des polynômes symétriques.

## IV Coefficients et racines de polynômes

### IV.1. Racines dans un sur-corps

Nous aurons besoin du résultat suivant, dont vous verrez des versions plus précises si vous suivez l'option Théorie des corps au S2.

**Proposition 14.** Soit $K$ un corps et soit $P \in K[X]$ un polynôme non constant. Alors

**(1)** Il existe un corps $L$ dont $K$ est un sous-corps et tel que $P$ a une racine dans $L$.

**(2)** Il existe un corps $L$ dont $K$ est un sous-corps et tel que $P$ est scindé dans $L[X]$, c'est-à-dire qu'il peut s'écrire comme un produit de polynômes de degré 1 de $L[X]$.

*Démonstration.* **(1)** Supposons dans un premier temps que $P$ est irréductible dans $K[X]$. Puisque $K[X]$ est un anneau principal, l'idéal $(P)$ est maximal, donc $L := K[X]/(P)$ est un corps. De plus, $K$ s'identifie à un sous-corps de $L$ par le biais du morphisme d'anneaux $K \hookrightarrow K[X] \twoheadrightarrow L$ composé de l'injection naturelle et de la projection canonique sur le quotient ; ce morphisme est nécessairement injectif car il n'est pas nul ($P$ n'est pas constant) et son noyau est un idéal du corps $K$. Enfin, notons $x$ la classe de $X$ dans $L$. Alors $P(x) = \overline{P(X)} = 0$ donc $x$ est une racine de $P$ dans $L$.

Si maintenant $P$ n'est pas irréductible dans $K[X]$, soit $Q$ un facteur irréductible de $P$. Il existe alors un corps $L$ dont $K$ est un sous-corps dans lequel $Q$ a une racine $\alpha$. Puisque $\alpha$ est aussi une racine de $P$, on a le résultat.

**(2)** On raisonne par récurrence sur le degré $d > 0$ de $P$. Si $d = 1$, il suffit de prendre $L = K$.

Soit donc $d > 1$ et supposons que le résultat est vrai pour les polynômes à coefficients dans un corps quelconque et de degré au plus $d-1$. D'après la première partie, il existe un corps $K'$ dont $K$ est un sous-corps et dans lequel $P$ a une racine $\alpha$. Ainsi, dans $K'[X]$ on a $P = (X-\alpha)Q$. Or $Q \in K'[X]$ est de degré $d-1$ donc il existe un corps $L$ dont $K'$ est un sous-corps et tel que $Q$ est scindé dans $L[X]$. Mais alors $K$ est un sous-corps de $L$ et $P = (X-\alpha)Q$ est scindé dans $L[X]$. Donc le résultat est vrai pour les polynômes de degre $d$. ✓

## IV.2. Relation coefficients-racines

**Théorème 15.** Dans l'anneau $A[X_1, \dots, X_n, T]$ on a

$$\prod_{i=1}^{n}(T - X_i) = \sum_{k=0}^{n}(-1)^{n-k}\sigma_{n-k}T^k.$$

*Démonstration.* On raisonne par récurrence sur $n$.

- ✦ Pour $n = 1$, on a $P = (T - X_1) = T + (-1)^1\sigma_{1,1}$.
- ✦ Supposons le résultat vrai au rang $n$. Soit $P = (T - X_1)\cdots(T - X_n)(T - X_{n+1})$. Par hypothèse de récurrence, on a

$$\begin{aligned}
P &= \left(\prod_{i=1}^{n}(T - X_i)\right)(T - X_{n+1}) = \left(\sum_{k=0}^{n}(-1)^{n-k}\sigma_{n,n-k}T^k\right)(T - X_{n+1}) \\
&= \sum_{k=0}^{n}(-1)^{n-k}\sigma_{n,n-k}T^{k+1} - \sum_{k=0}^{n}(-1)^{n-k}\sigma_{n,n-k}X_{n+1}T^k \\
&= \sum_{k=1}^{n+1}(-1)^{n+1-k}\sigma_{n,n+1-k}T^k + \sum_{k=0}^{n}(-1)^{n+1-k}\sigma_{n,n-k}X_{n+1}T^k \\
&= \sigma_{n,0}T^{n+1} + \sum_{k=1}^{n}(-1)^{n+1-k}(\sigma_{n,n+1-k} + \sigma_{n,n-k}X_{n+1})T^k + (-1)^{n+1}\sigma_{n,n}X_{n+1} \\
&= \sum_{k=0}^{n+1}(-1)^{n+1-k}\sigma_{n+1,n+1-k}T^k
\end{aligned}$$

en utilisant le lemme 7 pour la dernière ligne. ✓

**Corollaire 16** (Relations coefficients/racines)**.** Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ un polynôme avec $a_n \in A^\times$, et soient $\beta_1, \dots, \beta_n$ les racines de $P$, dans $A$ ou dans un corps $K$ contenant $A$ (dans le cas où $A$ est intègre). Alors, pour tout $k \in \{0, 1, \dots, n\}$, on a $\sigma_k(\beta_1, \dots, \beta_n) = (-1)^k a_{n-k}a_n^{-1}$. En particulier, $\sigma_k(\beta_1, \dots, \beta_n) \in A$.

*Démonstration.* On a $a_n^{-1}P = (X - \beta_1)\cdots(X - \beta_n) = X^n - \widetilde{\sigma}_1 X^{n-1} + \widetilde{\sigma}_2 X^{n-2} + \cdots + (-1)^n\widetilde{\sigma}_n$ d'après le théorème, où $\widetilde{\sigma}_k = \sigma_k(\beta_1, \dots, \beta_n)$. Le résultat s'en déduit par identification. ✓

***Remarque.*** Pour $n = 2$, on retrouve le résultat très classique $(X - \beta_1)(X - \beta_2) = X^2 - \sigma_1 X + \sigma_2$ où $\sigma_1$ est la somme des racines et $\sigma_2$ est leur produit.

***Exemple.*** Soit $P = X^4 + 12X - 5$. Déterminons ses racines dans $\mathbb{C}$, sachant que la somme de deux d'entre elles est égale à 2.

Notons $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ les racines de $P$ dans $\mathbb{C}$, avec par exemple $\alpha_1 + \alpha_2 = 2$. On a alors

$$\begin{cases} 0 = \sigma_1 = 2 + \alpha_3 + \alpha_4 \\ 0 = \sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4 \\ -12 = \sigma_3 = \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4 \\ -5 = \sigma_4 = \alpha_1\alpha_2\alpha_3\alpha_4 \end{cases}$$

où $\sigma_k$ désigne le $k^{\text{ième}}$ polynôme symétrique élémentaire en les $\alpha_i$.

Posons $p = \alpha_1\alpha_2$, $s = \alpha_1 + \alpha_2 = 2$, $q = \alpha_3\alpha_4$ et $t = \alpha_3 + \alpha_4$. On a alors

$$\begin{cases} s = 2 \\ s + t = 0 \\ p + \alpha_1 t + \alpha_2 t + q = 0 \\ pt + sq = -12 \\ pq = -5 \end{cases} \iff \begin{cases} s = 2 \\ t = -2 \\ p + st + q = 0 \\ 2(q - p) = -12 \\ pq = -5 \end{cases} \iff \begin{cases} s = 2 \\ t = -2 \\ p + q = 4 \\ p - q = 6 \\ pq = -5 \end{cases} \iff \begin{cases} s = 2 \\ t = -2 \\ p = 5 \\ q = -1 \end{cases}$$

Or $\alpha_1$ et $\alpha_2$ sont les deux racines de $X^2 - sX + p = X^2 - 2X + 5$ et $\alpha_3$ et $\alpha_4$ sont les deux racines de $X^2 - tX + q = X^2 + 2X - 1$.

On en déduit finalement que les racines de $P$ sont $1 \pm 2i$ et $-1 \pm \sqrt{2}$.

## IV.3. Application : Théorème de d'Alembert-Gauss

Nous allons utiliser les polynômes symétriques pour démontrer le théorème de d'Alembert-Gauss.

**Théorème 17** (Théorème de d'Alembert-Gauss)**.** Soit $P \in \mathbb{C}[X]$ un polynôme non constant. Alors $P$ a une racine dans $\mathbb{C}$.

*Démonstration.* Remarquons que $\overline{P}P \in \mathbb{R}[X]$ (où $\overline{P}$ désigne le conjugué de $P$). De plus, si $P$ a une racine dans $\mathbb{C}$ alors $\overline{P}P$ aussi et si $\overline{P}P$ a une racine dans $\mathbb{C}$, alors soit $P$ a une racine dans $\mathbb{C}$ soit $\overline{P}$ a une racine $\alpha \in \mathbb{C}$ mais alors $\overline{\alpha} \in \mathbb{C}$ est une racine de $P$. Ainsi, $P$ a une racine complexe si, et seulement si, $\overline{P}P$ a une racine complexe et on peut donc supposer que $P \in \mathbb{R}[X]$. De plus, quitte à multiplier par l'inverse du coefficient dominant, on peut supposer que $P$ est unitaire.

Posons $\deg P = d = 2^n q$ avec $q$ impair. On va raisonner par récurrence sur $n \in \mathbb{N}$.

- ✦ Si $n = 0$, alors $P$ est de degré impair et il a une racine réelle d'après le théorème des valeurs intermédiaires.
- ✦ Supposons que $n \geqslant 1$ et que le résultat est vrai pour les polynômes de degré $2^{n-1}q'$ avec $q'$ impair.

  Il existe un corps $L$ dont $\mathbb{C}$ est un sous-corps dans lequel $P$ est scindé : $P = (X - \alpha_1)\cdots(X - \alpha_d)$ avec $\alpha_i \in L$. On doit démontrer que l'un au moins des $\alpha_i$ est dans $\mathbb{C}$.

  Notons $\sigma_1, \ldots, \sigma_d$ les polynômes symétriques élémentaires en $X_1, \ldots, X_d$ et posons $\widetilde{\sigma}_k = \sigma_k(\alpha_1, \ldots, \alpha_d)$. D'après le corollaire **16**, pour tout $k$ on a $\widetilde{\sigma}_k \in \mathbb{R}$.

  Pour tout $(i, j) \in \mathbb{N}^2$ avec $1 \leqslant i, j \leqslant d$ et tout $c \in \mathbb{R}$, on pose $\beta_{ij}^{(c)} = \alpha_i + \alpha_j + c\alpha_i\alpha_j$ ; nous allons démontrer que pour tout $c$, l'un des $\beta_{ij}^{(c)}$ est dans $\mathbb{C}$. Pour cela, on considère les polynômes

  $$\widetilde{Q}_c = \prod_{1 \leqslant i,j \leqslant d} (X - \beta_{ij}^{(c)}) \in L[X],\ c \in \mathbb{R}.$$

  On a $\widetilde{Q}_c = Q_c(\alpha_1, \ldots, \alpha_d)$ où $Q_c = \prod_{1 \leqslant i,j \leqslant d}(X - X_i - X_j - cX_iX_j) \in \mathbb{R}[X][X_1, \ldots, X_d]$. Le polynôme $Q_c$ est un polynôme symétrique en $X_1, \ldots, X_d$, donc d'après le théorème **11**, il existe un polynôme $T \in \mathbb{R}[X][X_1, \ldots, X_d]$ tel que $Q_c = T(\sigma_1, \ldots, \sigma_d)$. On en déduit que $\widetilde{Q}_c = T(\widetilde{\sigma}_1, \ldots, \widetilde{\sigma}_d) \in \mathbb{R}[X]$ puisque les $\widetilde{\sigma}_k$ sont réels.

  De plus, $\deg Q_c = \sum_{i=1}^{n}(d - i + 1) = \frac{d(d+1)}{2} = 2^{n-1}q'$ avec $q' = q(d+1)$ impair. Donc d'après l'hypothèse de récurrence $Q_c$ a une racine $\gamma_c$ dans $\mathbb{C}$.

  Par conséquent, pour tout $c \in \mathbb{R}$, il existe $(i(c), j(c)) \in [\![1\,;d]\!]^2$ tel que $\gamma_c = \beta_{i(c)j(c)}^{(c)} = \alpha_{i(c)} + \alpha_{j(c)} + c\alpha_{i(c)}\alpha_{j(c)} \in \mathbb{C}$.

Puisque $\mathbb{R}$ est infini et que les indices $(i(c), j(c))$ parcourent un ensemble fini, il existe des nombres réels $c_1 \neq c_2$ tels que $(i(c_1), j(c_1)) = (i(c_2), j(c_2))$. Notons $r = i(c_1) = i(c_2)$ et $s = j(c_1) = j(c_2)$. Alors $\gamma_{c_1} = \alpha_r + \alpha_s + c_1\alpha_r\alpha_s \in \mathbb{C}$ et $\gamma_{c_2} = \alpha_r + \alpha_s + c_2\alpha_r\alpha_s \in \mathbb{C}$. Posons $u = \alpha_r + \alpha_s$ et $v = \alpha_r\alpha_s$. Alors $(c_1 - c_2)v = \gamma_{c_1} - \gamma_{c_2} \in \mathbb{C}$ donc $v \in \mathbb{C}$ et $u = \gamma_{c_1} - c_1 v \in \mathbb{C}$. De plus, $\alpha_r$ et $\alpha_s$ sont les racines de $X^2 - uX + v \in \mathbb{C}[X]$, et l'on sait que ces racines sont complexes.
On a donc démontré que les racines $\alpha_r$ et $\alpha_s$ de $P$ sont dans $\mathbb{C}$, donc $P$ a bien une racine complexe. ✓

## V Exemple : le discriminant

Soit $K$ un corps. Soit $(t_1, \dots, t_n) \in K^n$. Soit $P = (X - t_1)(X - t_2)\cdots(X - t_n) \in K[X]$.

**Définition 18.** *On appelle **discriminant** de $P$ le produit* $\mathrm{Disc}(P) = \prod_{i<j}(t_i - t_j)^2$.

$\mathrm{Disc}(P)$ est un polynôme symétrique en $t_1, \dots, t_n$ car tout $\gamma \in \mathfrak{S}_n$ agit sur $\prod_{i<j}(t_i - t_j)$ en multipliant par $\pm 1$. C'est donc un polynôme en les $\sigma_i$, où on note $\sigma_i = \sigma_i(t_1, \dots, t_n)$.

***Exemples.*** ✦ Pour $\deg P = 2$, si $P = X^2 + bX + c$ alors $\mathrm{Disc}(P) = (t_1 - t_2)^2 = (t_1 + t_2)^2 - 4t_1t_2 = \sigma_1^2 - 4\sigma_2 = b^2 - 4c$.
En effet, le lien coefficients-racines nous permet de dire que $\sigma_1 = -b$ et $\sigma_2 = c$.
✦ Pour $\deg P = 3$ et $P = X^3 + aX + b$, on a $\mathrm{Disc}(P) = -4a^3 - 27b^2$.

*Démonstration.* On peut raisonner comme pour les polynômes de degré 2. On peut aussi raisonner de façon plus théorique.
On a $\sigma_1 = 0$, $\sigma_2 = a$ et $\sigma_3 = -b$. Le polynôme $\mathrm{Disc}(P) \in K[t_1, t_2, t_3]$ est homogène de degré 6, donc il existe un polynôme $T \in K[Y_1, Y_2, Y_3]$ de poids 6 tel que $P = T(\sigma_1, \sigma_2, \sigma_3)$. Puisque $\sigma_1 = 0$, on cherche $T \in K[Y_2, Y_3]$.
Un monôme $Y_2^m Y_3^n$ est de poids $2m + 3n$, donc il est de poids 6 si et seulement si $(m, n) \in \{(0, 2), (3, 0)\}$. Ainsi, $T = \lambda Y_2^3 + \mu Y_3^2$. Ainsi, $\mathrm{Disc}(P) = T(\sigma_1, \sigma_2, \sigma_3) = \lambda\sigma_2^3 + \mu\sigma_3^2 = \lambda a^3 + \mu b^2$.
Ceci est vrai pour tout polynôme $P$, c'est-à-dire que $\lambda$ et $\mu$ ne dépendent pas de $a$ et $b$. On va donc spécialiser à des polynômes particuliers.

- ✦ Soit $P = X^3 - X = X(X - 1)(X + 1)$. On a alors $\mathrm{Disc}(P) = ((0 - (-1))(0 - 1)(-1 - (-1)))^2 = 4$ donc, puisqu'ici $a = -1$ et $b = 0$ on a $-\lambda = 4$ d'où $\lambda = -4$.
- ✦ Soit $P = X^3 - 1 = (X - 1)(X - j)(X - j^2)$. On a alors $\mathrm{Disc}(P) = \left((1 - j)(1 - j^2)(j - j^2)\right)^2 = -27$ donc, puisqu'ici $a = 0$ et $b = -1$ on a $\mu = -27$.

Finalement, $\mathrm{Disc}(P) = -4a^3 - 27b^2$. ✓

**Exercice 19.** Faire le cas $\deg P = 3$ en général. *[Indication : Si $P = X^3 + aX^2 + bX + c$, faire le changement d'indéterminée $Y = X + \frac{a}{3}$.]*

**Proposition 20.** Si $P$ est scindé dans $K[X]$, alors $P$ n'a que des racines simples si, et seulement si, $\mathrm{Disc}(P) \neq 0$.

*Démonstration.* Evident. ✓

Fin du cours en 2015-2016.

## VI Complément : résultant de deux polynômes

Le résultant, qui est un polynôme associé à un couple de polynômes, permet de généraliser la notion de discriminant et fournit des méthodes de calcul plus efficaces. Il permet aussi de définir le discriminant d'un polynôme qui n'est pas scindé.
Soit $K$ un corps. Notons $K_n[X]$ l'espace vectoriel des polynômes de degré au plus $n$. Par convention on pose $K_{-1}[X] = \{0\}$.

**Définition 21.** *Soit $(P,Q) \in K[X]^2$ avec $p = \deg P \geqslant 1$ et $q = \deg Q \geqslant 1$. Soit $\varphi : K_{q-1}[X] \times K_{p-1}[X] \to K_{p+q-1}[X]$ l'application linéaire définie par $\varphi(U,V) = UP + VQ$.*
*On appelle **résultant de $P$ et $Q$** et on note $\mathrm{Res}(P,Q) \in K$ le déterminant de $\varphi$.*

***Remarque.*** On munit $K_{q-1}[X] \times K_{p-1}[X]$ de la base $\mathcal{E} = \{(X^{q-1},0),\dots,(X,0),(1,0),(0,X^{p-1}),\dots,(0,X),(0,1)\}$ et $K_{p+q-1}[X]$ de la base $\mathcal{F} = \{X^{p+q-1},\dots,X,1\}$. Posons $P = \sum_{i=0}^{p} a_i X^i$ et $Q = \sum_{i=0}^{q} b_i X^i$ avec $a_p b_q \neq 0$. Notons $C_P$ la matrice colonne à $(p+1)$ lignes $C_P = \begin{pmatrix} a_p \\ a_{p-1} \\ \vdots \\ a_0 \end{pmatrix}$ et, de la même façon, soit $C_Q$ la matrice colonne à $(q+1)$ lignes $C_Q = \begin{pmatrix} b_q \\ b_{q-1} \\ \vdots \\ b_0 \end{pmatrix}$. Soient $A$ et $B$ les matrices de taille respectivement $q \times (p+q)$ et $p \times (p+q)$ suivantes

$$A = \begin{pmatrix} C_P & 0 & \cdots & 0_{q-1} \\ & C_P & & \\ & & \ddots & \\ 0_{q-1} & 0_{q-2} & \cdots & C_P \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} C_Q & 0 & \cdots & 0_{p-1} \\ & C_Q & & \\ & & \ddots & \\ 0_{p-1} & 0_{p-2} & \cdots & C_Q \end{pmatrix}.$$

Alors $\mathrm{Res}(P,Q)$ est le déterminant de la matrice par blocs $\begin{pmatrix} A & B \end{pmatrix}$.

En effet, la colonne ${}^t(0_i, {}^tC_P, 0_{q-1-i})$ pour $0 \leqslant i \leqslant q-1$ est la matrice de $X^{q-1-i}P$ dans la base $\mathcal{F}$ et de même pour les autres colonnes.

Pour la même raison, on peut aussi remarquer que $\mathrm{Res}(P,Q)$ est le déterminant dans la base $\mathcal{F}$ du système de vecteurs $(X^{q-1}P, X^{q-2}P, \dots, XP, P, X^{p-1}Q, X^{p-2}Q, \dots, XQ, Q)$.

***Exemple.*** Par exemple si $P = a_3X^3 + a_2X^2 + a_1X + a_0$ et $Q = b_2X^2 + b_1X^1 + b_0$ on a

$$\mathrm{Res}(P,Q) = \begin{vmatrix} a_3 & 0 & b_2 & 0 & 0 \\ a_2 & a_3 & b_1 & b_2 & 0 \\ a_1 & a_2 & b_0 & b_1 & b_2 \\ a_0 & a_1 & 0 & b_0 & b_1 \\ 0 & a_0 & 0 & 0 & b_0 \end{vmatrix}.$$

**Définition 22.** *Soit $P$ un polynôme de degré $p \geqslant 1$ et soit $a$ une constante.*
*On appelle **résultant** de $P$ et $a$ et on note $\mathrm{Res}(P,a)$ le déterminant de l'application linéaire $\varphi : K_{p-1}[X] \to K_{p-1}[X]$ définie par $\varphi(U) = aU$. Autrement dit, $\mathrm{Res}(P,a) = a^p$.*
*On appelle **résultant** de $a$ et $P$ et on note $\mathrm{Res}(a,P)$ le déterminant de l'application linéaire $\varphi : K_{p-1}[X] \to K_{p-1}[X]$ définie par $\varphi(U) = aU$. Autrement dit, $\mathrm{Res}(a,P) = a^p$.*

***Remarque.*** Avec la convention $K_{-1}[X] = \{0\}$, cette définition coïncide avec la définition précédente pour les polynômes non constants.

**Proposition 23.** Soient $P$ et $Q$ deux polynômes non nuls dont l'un au moins n'est pas constant. On note $p = \deg P$ et $q = \deg Q$. Alors

**(1)** $\mathrm{Res}(P,Q) = (-1)^{pq}\,\mathrm{Res}(Q,P)$.

**(2)** $\mathrm{Res}(\lambda P, \mu Q) = \lambda^q \mu^p\,\mathrm{Res}(P,Q)$.

*Démonstration.* Si $P$ ou $Q$ est constant, le résultat est évident. Supposons donc que $P$ et $Q$ ne sont pas constants.

**(1)** Rappelons que si on applique une permutation $\gamma \in \mathfrak{S}_n$ aux colonnes (ou lignes) d'une matrice $M$ de taille $n \times n$ pour obtenir la matrice $N$, alors $\det(N) = \varepsilon(\gamma)\det(M)$ où $\varepsilon$ désigne la signature.
Soit $\gamma = \begin{pmatrix} p+q & p+q-1 & \cdots & 3 & 2 & 1 \end{pmatrix} \in \mathfrak{S}_{p+q}$ la permutation circulaire. Notons que $\varepsilon(\gamma) = p+q-1$ car $\gamma = \begin{pmatrix} p+q-1 & p+q-2 \end{pmatrix}\begin{pmatrix} p+q-2 & p+q-3 \end{pmatrix}\cdots\begin{pmatrix} 3 & 2 \end{pmatrix}\begin{pmatrix} 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & p+q \end{pmatrix}$ est un

produit de $p+q-1$ transpositions. Si on permute les colonnes de $\begin{pmatrix} A & B \end{pmatrix}$ avec $\gamma$, cela revient à décaler chaque colonne d'un cran vers la gauche et la première colonne devient la dernière.

Pour passer de la matrice $\begin{pmatrix} A & B \end{pmatrix}$ à la matrice $\begin{pmatrix} B & A \end{pmatrix}$, on doit donc appliquer la permutation $\gamma^q$ aux colonnes. Puisque $\varepsilon$ est un morphisme de groupes, $\varepsilon(\gamma^q) = q\varepsilon(\gamma) = q(p+q-1) = pq + q^2 - q$ qui a même parité que $pq$. On en déduit que $\mathrm{Res}(P,Q) = (-1)^{pq}\,\mathrm{Res}(Q,P)$.

**(2)** Cela découle de la multilinéarité du déterminant (chacune des $q$ colonnes $C_P$ de $A$ est multipliée par $\lambda$ et chacune des $p$ colonnes $C_Q$ de $B$ est multipliée par $\mu$). ✓

**Proposition 24.** Soient $P$ et $Q$ deux polynômes non nuls dont l'un au moins n'est pas constant. On note $p = \deg P$ et $q = \deg Q$. Les assertions suivantes sont équivalentes.

(i) $P$ et $Q$ ont un facteur commun non-constant.

(ii) $\mathrm{Res}(P,Q) = 0$.

(iii) Il existe $U \in K_{q-1}[X]$ et $V \in K_{p-1}[X]$ tels que $UP + VQ = 0$.

*Démonstration.* Si $P$ ou $Q$ est constant, il est facile de vérifier qu'aucune des trois assertions n'est vraie. Supposons donc que $P$ et $Q$ ne sont pas constants.

- ✦ (i)⇒(ii). Soit $R$ un diviseur commun de $P$ et $Q$. Alors pour tout $(U,V)$ le polynôme $R$ divise $\varphi(U,V) = UP + VQ$. En particulier, $\varphi$ n'est pas surjective et donc $\mathrm{Res}(P,Q) = \det\varphi = 0$.
- ✦ (ii)⇒(iii). Puisque $\det\varphi = \mathrm{Res}(P,Q) = 0$, l'application linéaire $\varphi$ n'est pas injective. Soit $(U,V) \in \mathrm{Ker}\,\varphi$. Alors $UP + VQ = \varphi(U,V) = 0$.
- ✦ (iii)⇒(ii). Supposons que (iii) est vérifiée et que $P$ et $Q$ soient premiers entre eux. Alors $P$ divise $VQ = -UP$ donc par la condition de Gauss ($K[X]$ est factoriel) le polynôme $P$ divise $U$. Mais ceci contredit le fait que $p = \deg P > \deg U$. ✓

Dans la suite, on fixe un polynôme $P$ de degré $p \geqslant 1$ et de coefficient dominant $a_p$. On note $E = K[X]/(P)$.

**Lemme 25.** Notons $x$ la classe de $X$ dans $E$. Alors $E$ est un $K$-espace vectoriel de dimension $p$ et de base $\mathcal{B} = \left\{x^{p-1}, x^{p-2}, \dots, x, 1\right\}$.

*Démonstration.* Pour vérifier que $E$ est bien un $K$-espace vectoriel, il suffit de vérifier que $(P) = \{PQ; Q \in K[X]\}$ est un sous-espace vectoriel de $K[X]$ (exercice). Nous allons vérifier que $\mathcal{B}$ est une base de $E$.

Soit $u \in E$. Alors il existe $Q \in K[X]$ tel que $u = \overline{Q} = Q(x)$. La division euclidienne de $Q$ par $P$ donne $Q = AP + R$ avec $\deg R < p$. On a alors $u = Q(x) = A(x)P(x) + R(x) = R(x) \in \mathrm{vect}\{\mathcal{B}\}$. Donc $\mathcal{B}$ est une famille génératrice.

Supposons maintenant que $\sum_{i=0}^{p-1} \lambda_i x^i = 0$ avec $(\lambda_0, \dots, \lambda_{p-1}) \in K^p$. Posons $Q = \sum_{i=0}^{p-1} \lambda_i X^i$. Alors $Q(x) = 0$ donc $Q \in (P)$ et donc $P$ divise $Q$. Mais $\deg Q < p = \deg P$ donc $Q = 0$ et donc $\lambda_i = 0$ pour tout $i$. Donc $\mathcal{B}$ est libre et c'est bien une base de $E$. ✓

**Lemme 26.** Soit $Q \in K[X] \setminus \{0\}$. L'application $\theta_Q : E \to E$ qui à un vecteur $u$ associe $Q(x)u$ est une application linéaire.

De plus, si pour $i \in [\![0\,;p-1]\!]$ on note $R_i$ le reste de la division euclidienne de $X^iQ$ par $P$, alors la matrice de $\theta_Q$ dans $\mathcal{B}$ est la matrice du système de vecteurs $\left\{R_{p-1}, \dots, R_0\right\}$ dans la base $\mathcal{F}$ de $K_{p+q-1}[X]$.

*Démonstration.* Il est facile de vérifier que $\theta_Q$ est une application linéaire.

De plus, on a $\theta_Q(x^i) = Q(x)x^i = R_i(x)$ comme dans la démonstration du lemme précédent. Donc la $j^{\text{me}}$ colonne de la matrice de $\theta_Q$ est obtenue en écrivant les coefficients de $R_j(x)$ dans la base $\mathcal{B}$. Puisque $\deg R_j < p$, ceci revient à écrire les coefficients de $R_j$ dans la base $\left\{X^{p-1}, \dots, X, 1\right\}$ de $K_{p-1}[X]$ ou dans la base $\mathcal{F}$ de $K_{p+q-1}[X]$. ✓

**Lemme 27.** Soit $Q \in K[X] \setminus \{0\}$ et soit $q = \deg Q$. Alors $\mathrm{Res}(P,Q) = a_p^q \det(\theta_Q)$.

*Démonstration.* Si $q = 0$ alors $Q = b_0 \in K$ et on a $\det(\theta_Q) = b_0^p = \mathrm{Res}(P, b_0)$. Supposons donc que $q > 0$. On rappelle que $\mathrm{Res}(P, Q)$ est le déterminant dans la base $\mathcal{F}$ du système de vecteurs $(X^{q-1}P, X^{q-2}P, \dots, XP, P, X^{p-1}Q, X^{p-2}Q, \dots, XQ, Q)$. Avec les notations des lemmes précédents, puisque $P$ est un des vecteurs de la famille et que $X^iQ = A_iP + R_i$ pour des polynômes $A_i$, il s'agit du déterminant dans la base $\mathcal{F}$ du système de vecteurs $(X^{q-1}P, X^{q-2}P, \dots, XP, P, R_{p-1}, \dots, R_0)$. La matrice dans la base $\mathcal{F}$ de ce système de vecteurs s'écrit $\begin{pmatrix} T & 0 \\ N & M \end{pmatrix}$ où $M$ est la matrice $p \times p$ de $\{R_{p-1}, \dots, R_0\}$ dans $\mathcal{F}$ et donc de $\theta_Q$ dans $\mathcal{B}$, et où la matrice $T$ est triangulaire inférieure $q \times q$ de termes diagonaux tous égaux à $a_p$. Ainsi, $\mathrm{Res}(P, Q) = \begin{vmatrix} T & 0 \\ N & M \end{vmatrix} = a_p^q \det(M) = a_p^q \det(\theta_Q)$. ✓

**Proposition 28.** Soit $\alpha \in K$ et soient $P, Q, R$ des polynômes de $K[X]$. Alors

(i) $\mathrm{Res}(X - \alpha, Q) = Q(\alpha)$,

(ii) $\mathrm{Res}(P, QR) = \mathrm{Res}(P, Q)\,\mathrm{Res}(P, R)$ et $\mathrm{Res}(PR, Q) = \mathrm{Res}(P, Q)\,\mathrm{Res}(R, Q)$,

(iii) Si $R$ est le reste de la division euclidienne de $Q$ par $P$ et si $\deg R = r \geqslant 0$ alors $\mathrm{Res}(P, Q) = a_p^{q-r}\,\mathrm{Res}(P, R)$.

*Démonstration.* (i) Ici $p = 1$, $a_p = 1$ et $R_0 = Q(\alpha)$ donc $\theta_Q = Q(\alpha)\,\mathrm{id}_K$ et finalement $\mathrm{Res}(X - \alpha, Q) = \det(Q(\alpha)) = Q(\alpha)$.
*Une autre démonstration ne faisant pas intervenir les lemmes précédents mais seulement les propriétés du déterminant.*
*Posons* $Q = \sum_{i=0}^{q} b_i X^i$. *Alors* $\mathrm{Res}(X - \alpha, Q)$ *est le déterminant* $(q+1) \times (q+1)$ *suivant :*

$$\begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & b_q \\ -\alpha & 1 & 0 & \cdots & 0 & b_{q-1} \\ \vdots & & & \cdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & b_1 \\ 0 & 0 & 0 & \cdots & -\alpha & b_0 \end{vmatrix}.$$

*On effectue l'opération suivante sur les lignes :*

$$L_{q+1} \longleftarrow L_{q+1} + \alpha L_q + \alpha^2 L_{q-1} + \cdots + \alpha^q L_1 = \sum_{i=0}^{q} \alpha^i L_{q+1-i}.$$

*On a alors*

$$\mathrm{Res}(P, Q) = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & b_q \\ -\alpha & 1 & 0 & \cdots & 0 & b_{q-1} \\ \vdots & & & \cdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & b_1 \\ 0 & 0 & 0 & \cdots & 0 & Q(\alpha) \end{vmatrix} = Q(\alpha) \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ -\alpha & 1 & 0 & \cdots & 0 \\ \vdots & & & \cdots & \\ 0 & 0 & 0 & \cdots & 1 \end{vmatrix} = Q(\alpha)$$

*en développant suivant la dernière ligne pour obtenir le déterminant d'une matrice triangulaire avec des* 1 *sur la diagonale.*

(ii) Notons $r = \deg R$. D'après le lemme précédent, on a $\mathrm{Res}(P, QR) = a_p^{q+r} \det(\theta_{QR})$. Mais il est facile de vérifier que $\theta_{QR} = \theta_R \circ \theta_Q$ donc

$$\mathrm{Res}(P, QR) = a_p^{q+r} \det(\theta_{QR}) = a_p^q a_p^r \det(\theta_R) \det(\theta_Q) = \mathrm{Res}(P, Q)\,\mathrm{Res}(P, R)$$

en utilisant à nouveau le lemme précédent.
La deuxième partie découle de la première et de la proposition 23.

(iii) Dans $E$ on a $Q(x) = R(x)$ et on en déduit que $\theta_Q = \theta_R$. Le résultat découle alors du lemme précédent. ✓

**Théorème 29.** Si $P$ est scindé sur $K$ de racines $\alpha_1, \dots, \alpha_p$, alors

$$\mathrm{Res}(P, Q) = a_p^q Q(\alpha_1) \cdots Q(\alpha_p).$$

Si de plus $Q$ est scindé sur $K$ de racines $\beta_1, \dots, \beta_q$, alors

$$\mathrm{Res}(P, Q) = a_p^q b_q^p \prod_{i=1}^{p} \prod_{j=1}^{q} (\alpha_i - \beta_j).$$

*Démonstration.* On a $P = a_p(X-\alpha_1)\cdots(X-\alpha_p)$ donc d'après la proposition 23 on a $\operatorname{Res}(P,Q) = a_p^q \operatorname{Res}((X-\alpha_1)\cdots(X-\alpha_p),Q)$. On peut donc dans la suite supposer que $a_p = 1$.
Démontrons la première formule par récurrence sur $p$. On a déjà démontré dans la proposition précédente que le résultat est vrai pour $p = 1$. Supposons donc le résultat vrai pour les polynômes scindés de degré au plus $p-1$. Soit $P$ un polynôme scindé unitaire de racines $\alpha_1,\dots,\alpha_p$, il s'écrit $P = R(X-\alpha_p)$ avec $R = (X-\alpha_1)\cdots(X-\alpha_{p-1})$ scindé de degré $p-1$. On a donc d'après la proposition précédente $\operatorname{Res}(P,Q) = \operatorname{Res}(R(X-\alpha_p),Q) = \operatorname{Res}(R,Q)\operatorname{Res}(X-\alpha_n,Q) = \big(Q(\alpha_1)\cdots Q(\alpha_{p-1})\big)Q(\alpha_p)$ en utilisant l'hypothèse de récurrence.
Donc la première formule est vraie.
Si de plus $Q = b_q\prod_{j=1}^q(X-\beta_j)$ alors $\operatorname{Res}(P,Q) = a_p^q\prod i = 1^p Q(\alpha_i) = a_p^q b_q^p\prod_{i=1}^p\prod_{j=1}^q(\alpha_i-\beta_j)$. ✓

On peut généraliser la définition de discriminant comme suit.

**Définition 30.** *Soit $P\in K[X]$. On définit le **discriminant** de $P$ par*

$$\operatorname{Disc}(P) = (-1)^{p(p-1)/2}a_p^{-1}\operatorname{Res}(P,P').$$

***Remarque.*** Si $P$ est scindé de racines $\alpha_1,\dots,\alpha_p$, alors

$$\operatorname{Disc}(P) = (-1)^{p(p-1)/2}a_p^{2p-2}\prod_{i\neq j}(\alpha_i-\alpha_j) = a_p^{2p-2}\prod_{i<j}(\alpha_i-\alpha_j)^2.$$

On constate que pour $a_p = 1$ on retrouve la définition précédente du discriminant.

**Corollaire 31.** Les polynômes $P$ et $P'$ sont premiers entre eux si, et seulement si, $\operatorname{Disc}(P)\neq 0$.
En particulier, si $P$ est scindé dans $K$, alors $P$ n'a que des racines simples si, et seulement si, $\operatorname{Disc}(P)\neq 0$.