北航中法工程师学院
Centrale Pékin

Algèbre 1

École Centrale de Pékin

Cours de mathématiques du cycle préparatoire

9 décembre 2021

Table des matières

Avant-propos

Vous trouverez au fil de ce cours différents symboles :

- Le symbole "  ", situé dans la marge, signifie que le point correspondant est un point délicat (il s'agit d'un *virage dangereux*).
- Le symbole "□" est un marqueur signifiant la fin d'une démonstration.
-  Ce cours peut comporter des fautes de frappe, des coquilles, voire des erreurs d'argumentation. Ainsi, il faut toujours être vigilant lorsque vous suivez et que vous travaillez ce cours. Vérifier que les exemples sont justes et que les preuves n'ont pas de fautes est un exercice très utile (et indispensable) en mathématiques pour comprendre les notions et comprendre leurs utilisations.

Vous trouverez aussi des notations mathématiques :

$\mathbb{N}$	l'ensemble des entiers naturels
$\mathbb{Z}$	l'ensemble des entiers relatifs
$a\mathbb{Z}$	l'ensemble des multiples de a
$\text{pgcd}(a,b)$	le plus grand diviseur commun d'entiers a et b
$\text{ppcm}(a,b)$	le plus petit multiple commun d'entiers a et b
$a \equiv b \bmod n$	a est congru à b modulo n (n divise $b-a$)
$\mathbb{K}$	un corps (en général $\mathbb{R}, \mathbb{C}$ ou $\mathbb{Q}$)
$\mathscr{M}_{n,p}(\mathbb{K})$	l'ensemble des matrices à n lignes et p colonnes à coefficients dans $\mathbb{K}$
$\mathscr{M}_n(\mathbb{K})$	l'ensemble des matrices carrées $n \times n$ à coefficients dans $\mathbb{K}$
$E_{i,j}$	les matrices de la base canonique de $\mathscr{M}_{n,p}(\mathbb{K})$
M^{-1}	l'inverse d'une matrice carrée M
${}^tM$	la transposée d'une matrice M
$\text{rg}(M)$	le rang d'une matrice M
$Tr(M)$	la trace d'une matrice carrée M
$\mathbb{K}[X]$	l'ensemble des polynômes à une indéterminée à coefficients dans $\mathbb{K}$
$\mathbb{K}_n[X]$	l'ensemble des polynômes à une indéterminée à coefficients dans $\mathbb{K}$, de degré au plus n
$\deg(P)$	le degré d'un polynôme P

Chapitre 1 Arithmétique dans $\mathbb{Z}$

Table des matières du chapitre

1.1 Divisibilité dans $\mathbb{Z}$

1.1.1 Définitions et premières propriétés

Définition 1
*Soient $a, b \in \mathbb{Z}$ des entiers. On dit que a **divise** b \整除\ s'il existe un entier $k \in \mathbb{Z}$ tel que $b = ka$. Cette relation est notée $a \mid b$.*

*On dit aussi que a est un **diviseur** de b, ou que b est **divisible** par a, ou que b est un **multiple** de a.*

Exemples 2

- *2 divise 6 mais 2 ne divise pas 7.*
- *Soit $a \in \mathbb{Z}$. Alors 1, -1, a et $-a$ divisent a.*
- *Pour tout $a \in \mathbb{Z}$ on a $a \mid 0$.*
- *Le seul multiple de 0 est 0 : Si $0 \mid a$ alors $a = 0$.*

Remarque 3 — *Soit $a \in \mathbb{Z}$. L'ensemble des multiples de a est l'ensemble*

$$a\mathbb{Z} = \{ak,\ k \in \mathbb{Z}\} = \{\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots\}.$$

Si $a = 0$, on a $a\mathbb{Z} = \{0\}$.
Sinon, on peut remarquer que $|a|$ est le plus petit entier strictement positif contenu dans $a\mathbb{Z}$, c'est-à-dire : $|a| = \inf(\{k \in a\mathbb{Z},\ k > 0\})$.

Proposition 4
Soient $a, b \in \mathbb{Z}$. L'entier a divise b si et seulement si l'ensemble des multiples de b est inclus dans l'ensemble des multiples de a :

$$a \mid b \quad \Leftrightarrow \quad b\mathbb{Z} \subset a\mathbb{Z}.$$

Preuve — Supposons que $a \mid b$. Soit $m \in b\mathbb{Z}$. Alors il existe $p \in \mathbb{Z}$ tel que $m = pb$. Comme $a \mid b$, il existe $k \in \mathbb{Z}$ tel que $b = ka$. Donc $m = pka \in a\mathbb{Z}$, d'où $b\mathbb{Z} \subset a\mathbb{Z}$.

Réciproquement, supposons que $b\mathbb{Z} \subset a\mathbb{Z}$. Comme $b = 1 \times b \in b\mathbb{Z}$ on a $b \in a\mathbb{Z}$. Donc, il existe $k \in \mathbb{Z}$ tel que $b = ka$. Ainsi, a divise b, ce qui donne le résultat. □

PROPOSITION 5
Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$. Si a divise b alors $|a| \leq |b|$.

Preuve — Supposons que a divise b. Alors il existe $k \in \mathbb{Z}$ tel que $b = ka$. Comme b est non nul, k l'est également. Le nombre k étant un entier, on a ainsi $|k| \geq 1$, d'où $|b| = |ka| \geq |a|$. □

PROPOSITION 6 (Propriétés de la relation de divisibilité)
Soient $a, b, c, d \in \mathbb{Z}$.

- *Si $a \mid b$ et $b \mid c$, alors $a \mid c$.*
- *On a les équivalences :*

$$a \mid b \text{ et } b \mid a \quad \Leftrightarrow \quad a\mathbb{Z} = b\mathbb{Z} \quad \Leftrightarrow \quad |a| = |b| \quad \Leftrightarrow \quad a = b \text{ ou } a = -b.$$

- *Si $a \mid b$ et $c \mid d$, alors $ac \mid bd$.*
  En particulier, si $a \mid b$, alors $a^n \mid b^n$ pour tout $n \in \mathbb{N}$
- *Si $ab \mid c$ alors $a \mid c$ et $b \mid c$.*
- *Si $d \mid a$ et $d \mid b$, alors pour tous $u, v \in \mathbb{Z}$ on a $d \mid (au + bv)$.*

Preuve —

- On a $k_1, k_2 \in \mathbb{Z}$ tels que $b = k_1 a$ et $c = k_2 b$. Donc $c = k_1 k_2 a$ avec $k_1 k_2 \in \mathbb{Z}$, donc a divise c.
- Si $a \mid b$ et $b \mid a$, la Proposition 4 nous donne $a\mathbb{Z} \subset b\mathbb{Z}$ et $b\mathbb{Z} \subset a\mathbb{Z}$, donc $a\mathbb{Z} = b\mathbb{Z}$.
  Supposons que $a\mathbb{Z} = b\mathbb{Z}$. Si $a = 0$ ou $b = 0$ on a alors $a\mathbb{Z} = b\mathbb{Z} = \{0\}$, donc $a = b = 0$, d'où $|a| = |b|$. Si $a \neq 0$ et $b \neq 0$, la Proposition 5 nous donne $|a| \leq |b|$ et $|b| \leq |a|$, donc $|a| = |b|$.
  Supposons que $|a| = |b|$. On a alors $a = \pm|b|$, donc $a = \pm b$, c'est-à-dire $a = b$ ou $a = -b$.
  Supposons que $a = b$ ou $a = -b$. On a alors $a \mid b$ et $b \mid a$. Cela démontre l'équivalence entre toutes ces conditions.
- Supposons que $a \mid b$ et $c \mid d$. Alors il existe $k_1 \in \mathbb{Z}$ tel que $b = ak_1$ et il existe $k_2 \in \mathbb{Z}$ tel que $d = ck_2$. Donc $bd = ack_1k_2$ et $k_1k_2 \in \mathbb{Z}$. Donc $ac \mid bd$.
- Si $ab \mid c$, alors il existe $k \in \mathbb{Z}$ tel que $c = kab = a(kb) = b(ka)$. On a donc $a \mid c$ et $b \mid c$.
- Soient $u, v \in \mathbb{Z}$. Supposons que $d \mid a$ et $d \mid b$. Alors il existe $k_1, k_2 \in \mathbb{Z}$ tels que $a = k_1 d$ et $b = k_2 d$. On a ainsi $au + bv = d(uk_1 + vk_2)$ avec $uk_1 + vk_2 \in \mathbb{Z}$, donc $d \mid (au + bv)$.

□

REMARQUE 7 — *La réciproque de l'avant-dernière proposition est fausse : $4 \mid 12$ et $6 \mid 12$ mais $4 \times 6 = 24$ ne divise pas 12.*

EXEMPLE 8 — *Déterminons les entiers naturels n tels que $2n + 3$ divise $3n + 7$.*

Soit $n \in \mathbb{N}$. Supposons que $2 + 3n \mid 3n + 7$. Comme $2n + 3 \mid 2n + 3$, on a ainsi

$$2 + 3n \mid 2(3n + 7) - 3(2n + 3) = 5.$$

Les diviseurs de 5 sont $1, -1, 5$ et -5. Vu que $n \in \mathbb{N}$, on a $2n + 3 > 0$. On obtient donc $2n + 3 = 1$ ou $2n + 3 = 5$, soit $n = -1$ ou $n = 1$. Comme n est positif, on en déduit que $n = 1$.

Réciproquement, si $n = 1$ alors $2n + 3 = 5$ et $3n + 7 = 10$, et donc $2n + 3 \mid 3n + 7$.

Il existe donc un unique entier naturel, $n = 1$, tel que $2n + 3$ divise $3n + 7$.

EXERCICE 9 — *Déterminer les entiers $n \in \mathbb{Z}$ tels que $n + 3 \mid n^2$.*

1.1.2 Division euclidienne

On rappelle que la **partie entière** (ou plancher) d'un nombre réel x, notée $\lfloor x \rfloor$ ou E, est le plus grand entier n tel que $n \leq x$, c'est-à-dire : $\lfloor x \rfloor = \sup(\{n \in \mathbb{Z} \text{ tel que } n \leq x\})$.

THÉORÈME 10 (Division euclidienne d'entiers)
Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors existe un unique couple d'entiers $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ tel que

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

*L'entier q est appelé le **quotient** \商\ et l'entier r est appelé le **reste** \余数\ de la division euclidienne de a par b \整数的带余除法（或欧几里德除法）\.*

Preuve —

- Existence : Posons $q = \left\lfloor \frac{a}{b} \right\rfloor$ et $r = a - qb$. Alors $(q, r) \in \mathbb{Z} \times \mathbb{N}$ et $a = bq + r$. Comme $q = \left\lfloor \frac{a}{b} \right\rfloor$, on a $q \leq \frac{a}{b} < q + 1$. Comme b est strictement positif, on obtient ainsi $bq \leq a < bq + b$. Donc, on a $0 \leq r = a - bq < b$. Ainsi, le couple (q, r) convient.
- Unicité : Soient (q_1, r_1) et (q_2, r_2) deux couples vérifiant l'énoncé. Alors on a $a = bq_1 + r_1$ et $a = bq_2 + r_2$. Cela donne $bq_1 + r_1 = bq_2 + r_2$, d'où $b(q_1 - q_2) = r_2 - r_1$.
  Comme r_1 et r_2 sont positifs, on a $|r_2 - r_1| \leq \max(r_1, r_2) < b$. Ainsi, on a $b|q_1 - q_2| < b$, donc $|q_1 - q_2| < 1$. Comme $q_1 - q_2 \in \mathbb{Z}$ on obtient $q_1 - q_2 = 0$, soit $q_1 = q2$, et donc $r_1 = r_2$, ce qui prouve l'unicité.

□

REMARQUE 11 — *On a montré en particulier que $q = \left\lfloor \frac{a}{b} \right\rfloor$*

EXEMPLES 12

- *On a $22 = 3 \times 6 + 4$ et $0 \leq 4 < 6$, donc le quotient de la division euclidienne de 22 par 6 est 3 et le reste est 4.*
  Les expressions $22 = 2 \times 6 + 10$ ou $22 = 4 \times 6 - 2$ ne vérifient pas la condition imposée sur le reste r.
- *On a $-12 = -3 \times 5 + 3$ et $0 \leq 3 < 5$, donc le quotient de la division euclidienne de -12 par 5 est -3 et le reste est 3.*
  L'expressions $-12 = -2 \times 5 - 2$ ne vérifie pas la condition imposée sur le reste r.

PROPOSITION 13
Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Alors b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

Preuve —

- Supposons que b divise a. Alors il existe $k \in \mathbb{Z}$ tel que $a = kb$. On a donc $a = kb + 0$, et par unicité de la division euclidienne le reste de la division euclidienne de a par b vaut 0.
- Réciproquement, supposons que le reste de la division euclidienne de a par b soit nul. Alors il existe $q \in \mathbb{Z}$ tel que $a = qb + 0 = qb$. Donc b divise a.

□

1.1.3 Relation de congruence modulo un entier

DÉFINITION 14
*Soient a, b et $n \in \mathbb{Z}$. On dit que a **est congru à** b **modulo** n si n divise $b - a$, ou encore, s'il existe $k \in \mathbb{Z}$ tel que $b = a + kn$. On note alors $a \equiv b \bmod n$.*

EXEMPLE 15 — *On a :* $11 \equiv 1 \bmod 5$, $-1 \equiv 2 \bmod 3$, $0 \equiv 100 \bmod 2$.

REMARQUE 16 — *Soient $a, n \in \mathbb{Z}$. On a $n \mid a \Leftrightarrow a \equiv 0 \bmod n$.*

PROPOSITION 17
Soient $a, b, c, n \in \mathbb{Z}$ On a :

- $a \equiv a \bmod n$ *(la congruence est symétrique) ;*

- *Si $a \equiv b \bmod n$, alors $b \equiv a \bmod n$ (la congruence est réflexive) ;*
- *Si $a \equiv b \bmod n$ et $b \equiv c \bmod n$, alors $a \equiv c \bmod n$ (la congruence est transitive).*

Preuve —

- On a $a - a = 0$ et n divise 0.

- Si $a \equiv b \bmod n$ alors n divise $b - a$. Donc n divise $a - b = (-1)(b - a)$, donc $b \equiv a \bmod n$.
- Il existe des entiers $k_1, k_2 \in \mathbb{Z}$ tels que $b = a + k_1 n$ et $c = b + k_2 n$. On a donc $c = a + (k_1 + k_2)n$, donc $a \equiv c \bmod n$.

□

PROPOSITION 18 (Opérations sur les congruences)
Soient $a, b, c, d, m, n \in \mathbb{Z}$. On a :

1. *$a \equiv b \bmod n$ si et seulement si $a + c \equiv b + c \bmod n$.*
2. *Si $a \equiv b \bmod n$ et $c \equiv d \bmod n$ alors $a + c \equiv b + d \bmod n$.*
   La congruence modulo n est compatible avec la somme d'entiers.
3. *Si $a \equiv b \bmod n$ alors $ac \equiv bc \bmod n$.*
4. *Si $a \equiv b \bmod n$ et $c \equiv d \bmod n$ alors $ac \equiv bd \bmod n$.*
   La congruence modulo n est compatible avec la multiplication d'entiers.
   En particulier, si $a \equiv b \bmod n$ alors pour tout $k \in \mathbb{N}$, $a^k \equiv b^k \bmod n$.
5. *Si m est non nul, alors on a $a \equiv b \bmod n$ si et seulement si $ma \equiv mb \bmod mn$.*

Preuve —

1. On a $a \equiv b \bmod n$ si et seulement si n divise $b - a = (b + c) - (a + c)$, soit si et seulement si $a + c \equiv b + c \bmod n$.
2. Supposons $a \equiv b \bmod n$ et $c \equiv d \bmod n$. D'après le point précédent on a $a + c \equiv b + c \bmod n$ et $b + c \equiv b + d \bmod n$. Donc, par transitivité de la congruence modulo n, on a $a + c \equiv b + d \bmod n$.
3. Supposons $a \equiv b \bmod n$. Alors n divise $b - a$, donc n divise $c(b - a) = bc - ac$. Donc $ac \equiv bc \bmod n$.
4. Supposons $a \equiv b \bmod n$ et $c \equiv d \bmod n$. D'après le point précédent on a $ac \equiv bc \bmod n$ et $bc \equiv bd \bmod n$. Donc, par transitivité de la congruence modulo n, on a $ac \equiv bd \bmod n$.
5. Supposons que $a \equiv b \bmod n$. Alors il existe $k \in \mathbb{Z}$ tel que $b = a + kn$. Donc $mb = ma + k(mn)$ et $ma \equiv mb \bmod mn$. Réciproquement, supposons que $ma \equiv mb \bmod mn$. Alors il existe $k \in \mathbb{Z}$ tel que $mb = ma + kmn$. Comme m est non nul, la division par m donnc $b = a + kn$, donc $a \equiv b \bmod n$.

□

EXEMPLES 19

- *$2^{518} + 8^{211}$ est divisible par 3.*
  ***Preuve** — On a $2 \equiv -1 \bmod 3$. Donc $2^{518} \equiv (-1)^{518} \equiv 1 \bmod 3$. De même, $8 \equiv -1 \bmod 3$ donc $8^{211} \equiv (-1)^{211} \equiv -1 \bmod 3$. Ainsi,*
  $$2^{518} + 8^{211} \equiv 1 - 1 \equiv 0 \bmod 3.$$
  Donc 3 divise $2^{518} + 8^{211}$. □
- *Déterminer les entiers n tels que $3n + 5 \equiv 4 \bmod 7$.*
  Soit $n \in \mathbb{Z}$. Alors on a :
  $$3n + 5 \equiv 4 \bmod 7 \Leftrightarrow 3n \equiv -1 \bmod 7 \Rightarrow 5 \times 3n \equiv (-1 \times 5) \bmod 7 \Leftrightarrow n \equiv 2 \bmod 7.$$
  On vérifie alors réciproquement que tous les entiers de l'ensemble $\{2 + 7k \mid k \in \mathbb{Z}\} = 2 + 7\mathbb{Z}$ sont des solutions de $3n + 5 \equiv 4 \bmod 7$.
  Une autre façon de prouver la réciproque est la suivante :
  $$n \equiv 2 \bmod 7 \Leftrightarrow 15n \equiv -5 \bmod 7 \Rightarrow 45n \equiv -15 \bmod 7 \Leftrightarrow 3n \equiv -1 \bmod 7 \Leftrightarrow 3n + 5 \equiv 4 \bmod 7.$$
  Donc $3n + 5 \equiv 4 \bmod 7 \Leftrightarrow n = 2 + 7k$, $k \in \mathbb{Z}$.
- *Pour tout entier $n \in \mathbb{Z}$ impair, 8 divise $n^2 - 1$.*
  ***Preuve** — En effet, soit n un entier impair. Il existe donc $k \in \mathbb{Z}$ tel que $n = 2k+1$. Alors $n^2 - 1 = 4k^2 + 4k = 4k(k+1)$. Or k et $k+1$ étant deux entiers successifs, l'un d'entre eux est pair et donc $k(k+1)$ est pair. Donc $k(k+1) \equiv 0 \bmod 2$. Donc $4k(k+1) \equiv 0 \bmod 8$. Donc $n^2 - 1 \equiv 0 \bmod 8$. D'où le résultat.* □

1.2 PGCD, PPCM

1.2.1 Plus grand diviseur commun

Définition 20
Soient $a_1, \ldots, a_n$ des éléments de $\mathbb{Z}$. On appelle ***diviseur commun*** \公约数组成的集合\ *de $a_1, \ldots, a_n$ tout élément $d \in \mathbb{Z}$ tel que $d \mid a_i$ pour tout $i \in \{1, \ldots, n\}$.*

Exemples 21

- *6 est un diviseur commun de 12 et 18.*
- *3 est un diviseur commun de 9, 12 et 21.*

Lemme 22
Soient a et b deux éléments de $\mathbb{Z}$. L'ensemble $a\mathbb{Z} + b\mathbb{Z} = \{ak_1 + bk_2 \mid (k_1, k_2) \in \mathbb{Z}^2\}$ vérifie les propriétés suivantes :

- *$0 \in a\mathbb{Z} + b\mathbb{Z}$;*
- *Pour $x \in a\mathbb{Z} + b\mathbb{Z}$, on a $-x \in a\mathbb{Z} + b\mathbb{Z}$;*
- *Pour $x, y \in a\mathbb{Z} + b\mathbb{Z}$, on a $x + y \in a\mathbb{Z} + b\mathbb{Z}$.*

L'ensemble $a\mathbb{Z} + b\mathbb{Z}$ est ainsi un sous-groupe de $(\mathbb{Z}, +)$ (voir chapitre Structures algébriques).

Preuve — D'après sa définition, $a\mathbb{Z} + b\mathbb{Z}$ est un sous-ensemble de $\mathbb{Z}$.

- On a $0 = 0 \times a + 0 \times b$, donc $0 \in a\mathbb{Z} + b\mathbb{Z}$.
- Soit $x \in a\mathbb{Z} + b\mathbb{Z}$. Il existe k_1,k_2 dans $\mathbb{Z}$ tels que $x = ak_1 + bk_2$.
  On a alors $-x = -ak_1 - bk_2 = a(-k_1) + b(-k_2)$, donc $-x \in a\mathbb{Z} + b\mathbb{Z}$.
- Soit $(x, y) \in (a\mathbb{Z} + b\mathbb{Z})^2$. Il existe k_1,k_2,k_3,k_4 dans $\mathbb{Z}$ tels que $x = ak_1 + bk_2$ et $y = ak_3 + bk_4$.
  On a alors $x + y = ak_1 + bk_2 + (ak_3 + bk_4) = a(k_1 + k_3) + b(k_2 + k_4)$, donc $x + y \in a\mathbb{Z} + b\mathbb{Z}$.

□

Proposition 23
Soient $a, b \in \mathbb{Z}$. Alors il existe un unique entier naturel $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Preuve — • Si $a = 0$ et $b = 0$, on a $a\mathbb{Z} + b\mathbb{Z} = \{0\} + \{0\} = \{0\}$. Pour $d = 0$ on a ainsi $d\mathbb{Z} = 0\mathbb{Z} = \{0\} = a\mathbb{Z} + b\mathbb{Z}$. Pour tout autre entier $c \neq 0$, l'ensemble $c\mathbb{Z}$ contient une infinité d'éléments. Ainsi $d = 0$ est l'unique entier vérifiant $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

• Supposons maintenant que $a \neq 0$ ou $b \neq 0$.

Existence : L'ensemble $a\mathbb{Z} + b\mathbb{Z}$ contient $|a| = \pm a + 0.b$ et $|b| = 0.a + \pm b$, donc il contient au moins un entier strictement positif. L'ensemble $(a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N}^* = \{n \in a\mathbb{Z} + b\mathbb{Z}, n > 0\}$ est donc une sous-partie de $\mathbb{N}$ qui est non-vide. Cet ensemble admet donc un plus petit élément, que l'on note d. Montrons par double inclusion que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

◃ Comme $d \in a\mathbb{Z} + b\mathbb{Z}$, il existe $u, v \in \mathbb{Z}$ tels que $d = au + bv$. Pour tout $k \in \mathbb{Z}$, on a donc $kd = a(ku) + b(kv) \in a\mathbb{Z} + b\mathbb{Z}$. Donc, $d\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$.

▹ Pour l'inclusion réciproque, prenons $c \in a\mathbb{Z} + b\mathbb{Z}$. On effectue la division euclidienne de c par d : $c = dq + r$, avec $0 \leq r < d$. Alors $r = c - dq$ appartient à $a\mathbb{Z} + b\mathbb{Z}$ d'après la proposition précédente. On doit alors avoir $r = 0$ par minimalité de d.

Ainsi, on a $c = dq + 0$, donc c est un multiple de d, donc $c \in d\mathbb{Z}$. Cela donne $a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$, et donc $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Unicité : Supposons avoir $d, d' \in \mathbb{N}$ tels que $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} = d'\mathbb{Z}$. On a donc $d\mathbb{Z} = d'\mathbb{Z}$. La Proposition 6 nous donne alors $d = d'$, ce qui conclut la preuve. □

Définition 24
Soient $a, b \in \mathbb{Z}$. L'unique entier $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ est appelé le ***plus grand diviseur commun*** \最大公约数\ *de a et b (en abrégé* pgcd*). On le note $d = \text{pgcd}(a, b)$ ou encore $d = a \wedge b$.*

Remarque 25 — *Si $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, alors tout élément de $a\mathbb{Z} + b\mathbb{Z}$ est un multiple de d. Comme $a\mathbb{Z} + b\mathbb{Z}$ contient $a = 1.a + 0.b$ et $b = 0.a + 1.b$, on remarque en particulier que a et b dont des multiples de d, c'est-à-dire que d est un diviseur commun à a et à b.*

PROPOSITION 26
Soient $a, b \in \mathbb{Z}$. Alors $d = \text{pgcd}(a, b)$ si et seulement si :

1. *$d \mid a$ et $d \mid b$,*
   Autrement dit, d est un diviseur commun à a et b.
2. *Pour tout $d' \in \mathbb{Z}$ tel que $d' \mid a$ et $d' \mid b$, on a $d' \mid d$.*
   Autrement dit, tout diviseur commun de a et b divise d.

Preuve —

• Supposons que $d = \text{pgcd}(a, b)$. On a $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Le premier point vient de la remarque précédente.

Soit $d' \in \mathbb{Z}$ tel que $d' \mid a$ et $d' \mid b$. La Proposition 4 donne $a\mathbb{Z} \subset d'\mathbb{Z}$ et $b\mathbb{Z} \subset d'\mathbb{Z}$ donc $a\mathbb{Z} + b\mathbb{Z} \subset d'\mathbb{Z}$. Donc $d\mathbb{Z} \subset d'\mathbb{Z}$, et $d' \mid d$. D'où le second point.

• Réciproquement, supposons 1) et 2). Montrons par double inclusion que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

▷ Comme $d \mid a$ et $d \mid b$, la Proposition 4 donne $a\mathbb{Z} \subset d\mathbb{Z}$ et $b\mathbb{Z} \subset d\mathbb{Z}$, donc $a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$.

◁ Soit $d' = pgcd(a, b)$. Alors on a $d' \mid a$ et $d' \mid b$. L'hypothèse 2 donne $d' \mid d$, donc $d\mathbb{Z} \subset d'\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.

Finalement, on a montré que $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, ce qui conclut. □

REMARQUE 27 — *Le pgcd de a et b est donc bien le plus grand diviseur commun pour la relation $\leq$ sur $\mathbb{N}$.*

REMARQUE 28 — *Pour une famille d'entiers $a_1,\ldots,a_n \in \mathbb{Z}$ on peut démontrer par récurrence qu'il existe un unique $d \in \mathbb{N}$ tel que $a_1\mathbb{Z} + \ldots + a_n\mathbb{Z} = d\mathbb{Z}$, et définir ainsi le pgcd de la famille $a_1, \ldots, a_n$.*

On peut alors démontrer de même que ce pgcd est un diviseur commun de a_1, …, a_n qui est un multiple de tout autre diviseur commun.

EXEMPLES 29— *On a :* $\text{pgcd}(12, 18) = 6$, $\text{pgcd}(10, 12, 18) = 2$, $\text{pgcd}(2, 3) = 1$, $\text{pgcd}(8, 6) = 2$.

PROPOSITION 30
Soient $a, b, c, k \in \mathbb{Z}$. On a :

- $\text{pgcd}(a, b) = \text{pgcd}(|a|, |b|)$,
- $\text{pgcd}(a, 0) = |a|$,
- $\text{pgcd}(a, 1) = 1$,
- $\text{pgcd}(a, b) = \text{pgcd}(b, a)$,
- $\text{pgcd}(a, \text{pgcd}(b, c)) = \text{pgcd}(\text{pgcd}(a, b), c)$,
- $\text{pgcd}(ka, kb) = |k|\text{pgcd}(a, b)$.

Preuve — Ces propriétés découlent immédiatement de la définition du pgcd comme l'unique entier positif d tel que $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. En effet, on a :

1. $a\mathbb{Z} + b\mathbb{Z} = |a|\mathbb{Z} + |b|\mathbb{Z}$,
2. $a\mathbb{Z} + 0\mathbb{Z} = a\mathbb{Z}$,
3. $a\mathbb{Z} + \mathbb{Z} = \mathbb{Z}$,
4. $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + a\mathbb{Z}$,
5. $a\mathbb{Z}+(b\mathbb{Z}+c\mathbb{Z}) = (a\mathbb{Z}+b\mathbb{Z})+c\mathbb{Z}$,
6. $ak\mathbb{Z} + bk\mathbb{Z} = |k|(a\mathbb{Z} + b\mathbb{Z})$.

□

PROPOSITION 31
Soient $a, b \in \mathbb{Z}$, et $d = \text{pgcd}(a, b)$.
Alors il existe deux entiers $u_0, v_0 \in \mathbb{Z}$ tels que

$$au_0 + bv_0 = d.$$

Preuve — Par définition on a $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. Donc $d \in a\mathbb{Z} + b\mathbb{Z}$. Il existe donc $(u_0, v_0) \in \mathbb{Z}^2$ tel que $d = au_0 + bv_0$. □

EXEMPLE 32 — *On a* $\text{pgcd}(4, 6) = 2$ *et* $4 \times (-1) + 6 \times 1 = 2$. *On a aussi* $4 \times 2 + 6 \times (-1) = 2$.

On peut donc remarquer que les entiers u et v ne sont pas uniques.

1.2.2 Calcul du PGCD avec l'algorithme d'Euclide

Le pgcd de deux entiers se calcule facilement de manière algorithmique. Ce calcul est basé sur le résultat suivant.

LEMME 33
Soient $a\mathbb{Z}$, $b \in \mathbb{N}^*$. Notons r le reste de la division euclidienne de a par b. Alors on a :

$$\text{pgcd}(a, b) = \text{pgcd}(b, r).$$

Preuve — Par division euclidienne, il existe $q \in \mathbb{Z}$ tel que $a = bq + r$. On vérifie alors que $a\mathbb{Z} + b\mathbb{Z} = r\mathbb{Z} + b\mathbb{Z}$. Par définition du pgcd, on a donc $\text{pgcd}(a, b) = \text{pgcd}(b, r)$. □

L'algorithme d'Euclide permet de calculer le pgcd de deux entiers, il est basé sur des divisions euclidiennes successives.

PRINCIPE DE L'ALGORITHME D'EUCLIDE

Soient a et b deux entiers tels que $0 \leq b \leq a$.

Si $b = 0$ alors $\text{pgcd}(a, b) = a$ et c'est terminé. On suppose donc b non nul.

- Étape 1 : *On effectue la division euclidienne de a par b : $a = bq_0 + r_0$ avec $0 \leq r_0 < b$.*
  D'après le lemme, $\text{pgcd}(a, b) = \text{pgcd}(b, r_0)$.
  Si $r_0 = 0$ alors $\text{pgcd}(a, b) = b$ et c'est terminé.
  Sinon, on passe à l'étape suivante.
- Étape 2 : *On effectue la division euclidienne de b par r_0 : $b = r_0q_1 + r_1$ avec $0 \leq r_1 < r_0$.*
  D'après le lemme, $\text{pgcd}(a, b) = \text{pgcd}(b, r_0) = \text{pgcd}(r_0, r_1)$.
  Si $r_1 = 0$ alors $\text{pgcd}(r_0, r_1) = r_0$ et donc $\text{pgcd}(a, b) = r_0$ et c'est terminé.
  Sinon, on passe à l'étape suivante.
- Étape 3 : *On effectue la division euclidienne de r_0 par r_1 : $r_0 = r_1q_2 + r_2$ avec $0 \leq r_2 < r_1$.*
  D'après le lemme, $\text{pgcd}(a, b) = \text{pgcd}(r_0, r_1) = \text{pgcd}(r_1, r_2)$.
  Si $r_2 = 0$ alors $\text{pgcd}(r_1, r_2) = r_1$ et donc $\text{pgcd}(a, b) = r_1$ et c'est terminé.
  Sinon on passe à l'étape suite, etc.
- ...

La suite des restes obtenus est une suite strictement décroissante d'entiers positifs, il existe donc un entier $n_0 \in \mathbb{N}$ tel que $r_{n_0} = 0$. D'après le lemme précédent, on a : $\text{pgcd}(a, b) = \text{pgcd}(b, r_0) = \ldots = \text{pgcd}(r_{n_0-1}, r_{n_0}) = r_{n_0-1}$.

REMARQUE 34 — *On peut toujours se ramener au cas où $0 \leq b \leq a$ en utilisant le fait que $\text{pgcd}(a, b) = \text{pgcd}(b, a)$ et que $\text{pgcd}(a, b) = \text{pgcd}(|a|, |b|)$.*

EXEMPLE 35 — *Calculons le pgcd de 721 et 658 à l'aide de l'algorithme d'Euclide.*

1. *Division euclidienne de 721 par 658 : $721 = 658 \times 1 + 63$. Le reste vaut 63.*
2. *Division euclidienne de 658 par 63 : $658 = 63 \times 10 + 28$. Le reste vaut 28.*
3. *Division euclidienne de 63 par 28 : $63 = 28 \times 2 + 7$. Le reste vaut 7.*
4. *Division euclidienne de 28 par 7 : $28 = 7 \times 4 + 0$. Le reste est nul !*

Le dernier reste non nul dans la suite des divisions euclidienne est donc 7. Ainsi, $\text{pgcd}(721, 658) = 7$.

1.2.3 Plus petit multiple commun

DÉFINITION 36
*Soient $a_1, \ldots, a_n \in \mathbb{Z}$. On appelle **multiple commun** de $a_1, \ldots, a_n$ tout élément m de $\mathbb{Z}$ tel que m est un multiple de a_i (ou encore, $a_i \mid m$) pour tout $i \in \{1, \ldots, n\}$.*

Exemples 37

- 12 *est un multiple commun de* 4 *et* 6.
- 36 *est un multiple commun de* 2, 3 *et* 9.
- 105 *est un multiple commun de* 3, 5 *et* 7.

Proposition 38
Soient $a, b \in \mathbb{Z}$. Alors il existe un unique entier positif $m \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

Preuve — • Si $a = 0$ et $b = 0$, on a $a\mathbb{Z} \cap b\mathbb{Z} = \{0\} \cap \{0\} = \{0\}$. Pour $m = 0$ on a ainsi $m\mathbb{Z} = 0\mathbb{Z} = \{0\} = a\mathbb{Z} \cap b\mathbb{Z}$. Pour tout autre entier $c \neq 0$, l'ensemble $c\mathbb{Z}$ contient une infinité d'éléments. Ainsi $m = 0$ est l'unique entier vérifiant $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

• Supposons maintenant que $a \neq 0$ ou $b \neq 0$.

Existence : L'entier positif $|ab|$ est dans $a\mathbb{Z}$ et dans $b\mathbb{Z}$, donc $|ab| \in a\mathbb{Z} \cap b\mathbb{Z}$. Cet ensemble contient donc au moins un entier strictement positif. L'ensemble $(a\mathbb{Z} \cap b\mathbb{Z}) \cap \mathbb{N}^* = \{n \in a\mathbb{Z} \cap b\mathbb{Z},\ n > 0\}$ est donc une sous-partie de $\mathbb{N}$ qui est non-vide. Cet ensemble admet donc un plus petit élément, que l'on note m. Montrons par double inclusion que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

◁ Comme $m \in a\mathbb{Z} \cap b\mathbb{Z}$, il existe $u, v \in \mathbb{Z}$ tels que $m = au$ et $m = bv$. Pour tout $k \in \mathbb{Z}$, on a donc $km = a(ku) \in a\mathbb{Z}$ et $km = b(kv) \in b\mathbb{Z}$. Donc, $m\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$.

▷ Pour l'inclusion réciproque, prenons $c \in a\mathbb{Z} \cap b\mathbb{Z}$. On effectue la division euclidienne de c par m : $c = mq + r$, avec $0 \leq r < m$. Si l'on avait $r > 0$, alors $r = c - mq$ appartiendrait à $a\mathbb{Z}$ et à $b\mathbb{Z}$, donc à $a\mathbb{Z} \cap b\mathbb{Z}$. Mais comme $0 < r < m$, cela contredirait le fait que m est le plus petit entier strictement positif contenu dans $a\mathbb{Z} \cap b\mathbb{Z}$.

Ainsi, on a $c = mq + 0$, donc c est un multiple de m, donc $c \in m\mathbb{Z}$. Cela donne $a\mathbb{Z} \cap b\mathbb{Z} \subset m\mathbb{Z}$, et donc $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

Unicité : Supposons avoir $m, m' \in \mathbb{N}$ tels que $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z} = m'\mathbb{Z}$. On a donc $m\mathbb{Z} = m'\mathbb{Z}$. La Proposition 6 nous donne alors $m = m'$, ce qui conclut la preuve. □

Définition 39
Soient a, b des éléments de $\mathbb{Z}$. L'unique entier naturel $m \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ est appelé le ***plus petit multiple commun*** \最小公倍数\ *de a et de b (en abrégé* ppcm*).*
On le note $m = \mathrm{ppcm}(a, b)$ ou encore $m = a \vee b$.

Proposition 40
Soient $a, b \in \mathbb{Z}$ et $m \in \mathbb{N}$. On a $m = \mathrm{ppcm}(a, b)$ si et seulement si :

1. *$a \mid m$ et $b \mid m$,*
   Autrement dit, m est un multiple commun de a et de b.
2. *Pour tout $m' \in \mathbb{Z}$ tel que $a \mid m'$ et $b \mid m'$, on a $m \mid m'$.*
   Autrement dit, tout multiple commun de a et de b est un multiple de m.

Preuve —

• Supposons que $m = \mathrm{ppcm}(a, b)$, c'est-à-dire $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Comme $m \in m\mathbb{Z} \subset a\mathbb{Z}$, on a $a \mid m$. On obtient de même $b \mid m$. D'où le premier point.

Soit $m' \in \mathbb{Z}$ tel que $a \mid m'$ et $b \mid m'$. Alors $m' \in a\mathbb{Z}$ et $m' \in b\mathbb{Z}$, donc $m' \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Donc $m \mid m'$.

• Réciproquement, supposons 1) et 2). Montrons par double inclusion que $mZ = a\mathbb{Z} \cap b\mathbb{Z}$.

▷ Le premier point donne $m \in a\mathbb{Z}$ et $m \in b\mathbb{Z}$, donc $m \in a\mathbb{Z} \cap b\mathbb{Z}$. Ainsi, on a $m\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$.

◁ Soit $m' = \mathrm{ppcm}(a, b)$. On a alors $a \mid m'$ et $b \mid m'$. Le point 2) nous donne $m \mid m'$. Ainsi, on a $m'\mathbb{Z} \subset m\mathbb{Z}$, soit $a\mathbb{Z} \cap b\mathbb{Z} = m'\mathbb{Z} subset m\mathbb{Z}$.

Finalement, on obtient $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, ce qui conclut la preuve. □

Remarque 41 — *Le ppcm de a et b est donc bien le plus petit multiple commun pour la relation $\leq$ sur $\mathbb{N}$.*

Remarque 42 — *Pour une famille d'entiers $a_1, \ldots, a_n \in \mathbb{Z}$ on peut démontrer par récurrence qu'il existe un unique $m \in \mathbb{N}$ tel que $a_1\mathbb{Z} \cap \ldots \cap a_n\mathbb{Z} = m\mathbb{Z}$, et définir ainsi le ppcm de la famille $a_1, \ldots, a_n$.*

On peut alors démontrer de même que ce ppcm est un multiple commun de a_1, …, a_n qui est un diviseur de tout autre multiple commun.

Exemple 43 — $\mathrm{ppcm}(3, 6) = 6$, $\mathrm{ppcm}(4, 6) = 12$, $\mathrm{ppcm}(2, 3) = 6$.

PROPOSITION 44
Soient $a, b, k \in \mathbb{Z}$. On a :

1. $\text{ppcm}(a,b) = \text{ppcm}(|a|,|b|)$,
2. $\text{ppcm}(a,0) = 0$,
3. $\text{ppcm}(1,a) = |a|$,
4. $\text{ppcm}(a,b) = \text{ppcm}(b,a)$,
5. $\text{ppcm}(a,\text{ppcm}(b,c)) = \text{ppcm}(\text{ppcm}(a,b),c)$,
6. $\text{ppcm}(ka,kb) = |k|\text{ppcm}(a,b)$.

Preuve — Ces propriétés découlent de la définition du ppcm. □

Preuve — Ces propriétés découlent immédiatement de la définition du ppcm comme l'unique entier positif m tel que $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$. En effet, on a :

1. $a\mathbb{Z} \cap b\mathbb{Z} = |a|\mathbb{Z} \cap |b|\mathbb{Z}$,
2. $a\mathbb{Z} \cap 0\mathbb{Z} = 0\mathbb{Z}$,
3. $a\mathbb{Z} \cap \mathbb{Z} = a\mathbb{Z}$,
4. $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z} = b\mathbb{Z} \cap a\mathbb{Z}$,
5. $a\mathbb{Z} \cap (b\mathbb{Z} \cap c\mathbb{Z}) = (a\mathbb{Z} \cap b\mathbb{Z}) \cap c\mathbb{Z}$,
6. $ak\mathbb{Z} \cap bk\mathbb{Z} = |k|(a\mathbb{Z} \cap b\mathbb{Z})$.

□

1.3 Théorème de Bézout et théorème de Gauss

1.3.1 Nombres entiers premiers entre eux

DÉFINITION 45
Soient $a, b \in \mathbb{Z}$. On dit que a et b sont ***premiers entre eux*** \互素\ *si* $\text{pgcd}(a,b) = 1$.

EXEMPLE 46 — *2 et 3 sont premiers entre eux. 9 et 16 sont premiers entre eux. 6 et 4 ne sont pas premiers entre eux.*

Si a ne divise pas b et b ne divise pas a, on ne peut pas dire que a et b sont premiers entre eux !
Par exemple, 6 ne divise pas 15 et 15 ne divise pas 6 mais $\text{pgcd}(6,15) = 3$, donc 6 et 15 ne sont pas premiers entre eux.

DÉFINITION 47
Soient $a_1,\ldots,a_n \in \mathbb{Z}$. On dit que $a_1,\ldots,a_n$ sont ***premiers entre eux deux à deux*** *si* $\text{pgcd}(a_i,a_j) = 1$ *pour tous i, j dans $\{1,\ldots,n\}$ avec $i \neq j$.*

1.3.2 Théorème de Bézout et théorème de Gauss

THÉORÈME 48 (Théorème de Bézout)
Soient $a, b \in \mathbb{Z}$. Les entiers a et b sont premiers entre eux si et seulement s'il existe deux entiers $u, v \in Z$ tels que

$$au + bv = 1.$$

Preuve — Supposons que a et b sont premiers entre eux. Alors on a $\text{pgcd}(a,b) = 1$. Cela veut dire que $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$. Ainsi, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Réciproquement, supposons qu'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. On a alors $1 \in a\mathbb{Z} + b\mathbb{Z}$, donc $1\mathbb{Z} = \mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$. Comme $a\mathbb{Z} + b\mathbb{Z} \subset \mathbb{Z}$, on en déduit que $a\mathbb{Z} + b\mathbb{Z} = 1\mathbb{Z}$. Donc $\text{pgcd}(a,b) = 1$, et a et b sont premiers entre eux. □

EXEMPLE 49 — *n et $n+1$ sont premiers entre eux car $(n+1) \times 1 + n \times (-1) = 1$.*

L'algorithme d'Euclide étendu permet d'obtenir les coefficients u et v, appelés **coefficients de Bézout**. Alors que l'algorithme d'Euclide s'intéresse uniquement aux restes de divisions euclidiennes successives, l'algorithme d'Euclide étendu considère également les quotients de ces divisions euclidiennes.

PRINCIPE : À l'aide de l'algorithme d'Euclide, on construit de proche en proche des éléments u_k et v_k de $\mathbb{Z}$ tels que l'ont ait à chaque étape :

$$r_k = au_k + bv_k,$$

où les r_k sont les restes des divisions euclidiennes successives de l'algorithme d'Euclide.

EXEMPLE 50 — *Expliquons sur un exemple, avec $a = 1795$ et $b = 343$.*

$$\begin{array}{rcccccccc|l}
343 & = & 0 & \times 1795 & + & 1 & \times 343 & & \\
80 & = & 1 & \times 1795 & + & (-5) & \times 343 & & 1795 - 5 \times 343 = 80 \\
23 & = & 0 + (-4).1 & \times 1795 & + & 1 + (-4)(-5) & \times 343 & & 343 - 4 \times 80 = 23 \\
23 & = & -4 & \times 1795 & + & 21 & \times 343 & & \\
11 & = & 1 + (-3)(-4) & \times 1795 & + & (-5) + (-3)(21) & \times 343 & & 80 - 3 \times 23 = 11 \\
11 & = & 13 & \times 1795 & + & (-68) & \times 343 & & \\
1 & = & (-4) + (-2)(13) & \times 1795 & + & 21 + (-2)(-68) & \times 343 & & 23 - 2 \times 11 = 1 \\
1 & = & -30 & \times 1795 & + & 157 & \times 343 & &
\end{array}$$

L'algorithme d'Euclide (à droite) nous dit que $\text{pgcd}(1795, 343) = 1$. *Et on a obtenu en même temps (à gauche) que* $1 = 1795 \times u + 343 \times v$ *avec* $u = -30$ *et* $v = 157$.

THÉORÈME 51 (Théorème de Gauss)
Soient $a, b, c \in \mathbb{Z}$ des éléments de $\mathbb{Z}$.
Si a et b sont premiers entre eux et si $a \mid bc$, alors $a \mid c$.

Preuve — On suppose que a et b sont premiers entre eux et que $a \mid bc$. D'après le théorème de Bézout, il existe des entiers $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Comme $a \mid bc$, il existe $k \in \mathbb{Z}$ tel que $bc = ak$. On a donc $c = auc + bvc = auc + avk = a(uc + vk)$. Donc $a \mid c$. □

Quand a et b ne sont pas premiers entre eux, si $a \mid bc$ et même si a ne divise pas b, on ne peut pas dire que $a \mid c$!
Par exemple, 8 divise 4×6 mais 8 ne divise ni 4 ni 6.

EXEMPLE 52 — *Si $4 \mid 3n$ alors $4 \mid n$, car 4 et 3 sont premiers entre eux.*

Conséquences de ces théorèmes

PROPOSITION 53
Soient $a, b, c \in \mathbb{Z}$.
Si a et b premiers entre eux et si $a \mid c$ et $b \mid c$, alors $ab \mid c$.

Preuve — Supposons que $a \mid c$ et $b \mid c$ avec $\text{pgcd}(a, b) = 1$. Le théorème de Bézout nous dit qu'il existe alors des entiers $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. On a donc $c = auc + bvc$. Comme $a \mid c$, on a on a $ab \mid bc$. Comme $b \mid c$, on a on a $ab \mid ac$. Donc, ab divise $acu + bcv = c$. □

COROLLAIRE 54
Soient $a_1, \ldots, a_n, c \in \mathbb{Z}$.
Si les a_i sont premiers entre eux deux à deux et si $a_i \mid c$ pour tout $1 \leq i \leq n$, alors $a_1 \times a_2 \times \ldots a_n \mid c$.

Preuve — Cette généralisation de la proposition précédente se démontre par récurrence sur n. □

Si a et b ne sont pas premiers entre eux, on ne peut rien dire ! Par exemple $4 \mid 4$ et $2 \mid 4$ mais $4 \times 2 = 8$ ne divise pas 4.

EXEMPLE 55 — *Si $4 \mid n$ et $3 \mid n$ alors $12 \mid n$ car 4 et 3 sont premiers entre eux.*

PROPOSITION 56
Soient $a, b, c \in \mathbb{Z}$.
Si a est premier avec b et si a est premier avec c, alors a est premier avec bc.

Preuve — Supposons a premier avec b et avec c. D'après le théorème de Bézout, il existe $u_1, u_2, v_1, v_2 \in \mathbb{Z}$ tels que $1 = au_1 + bv_1$ et $1 = au_2 + cv_2$. Par multiplication, on obtient :

$$1 = a(au_1u_2 + u_1cv_2 + bv_1u_2) + bc(v_1v_2).$$

Ainsi, d'après le théorème de Bézout, a et bc sont premiers entre eux. □

COROLLAIRE 57
Soient $a, b_1, \ldots, b_n \in \mathbb{Z}$. Si a est premier avec b_i pour tout $i \in \{1, \ldots, n\}$, alors a est premier avec $b_1 \times b_2 \times \ldots \times b_n$.

Preuve — Cette généralisation de la proposition précédente se démontre par récurrence sur n. □

PROPOSITION 58
Soient $a, b \in \mathbb{Z}$. Si a est premier avec b alors a^m est premier avec b^n pour tous $m, n \in \mathbb{N}$.

Preuve — Soient $m, n \in \mathbb{N}$. Si $m = 0$ ou $n = 0$ on a $a^m = 1$ ou $b^n = 1$, et dans ce cas le résultat est vrai.

Supposons $m, n \neq 0$. Comme a est premier avec b, le corollaire précédent nous dit que a est premier avec b^n. Comme b^n est premier avec a, le corollaire précédent nous dit que b^n est premier avec a^m. □

EXEMPLE 59 — *Soit $n \in \mathbb{N}^*$. Comme n est premier avec $n - 1$ et avec $n + 1$, n est premier avec $(n - 1)(n + 1) = n^2 - 1$.*

PROPOSITION 60
Soient $a, b \in \mathbb{Z}$. Posons $d = \mathrm{pgcd}(a, b)$. Alors il existe des éléments a' et b' de $\mathbb{Z}$ tels que

$$a = da',\ b = db', \quad \text{et} \quad \mathrm{pgcd}(a', b') = 1.$$

Preuve — Si $(a, b) = (0, 0)$, alors $a' = b' = 1$ conviennent.

Supposons que $(a, b) \neq (0, 0)$. Comme $d = \mathrm{pgcd}(a, b)$, on sait que $d \mid a$ et $d \mid b$. Les nombres $a' = \frac{a}{\mathrm{pgcd}(a,b)}, b' = \frac{b}{\mathrm{pgcd}(a,b)}$ sont donc des entiers, tels que $a = da'$ et $b = db'$. On a alors $d = \mathrm{pgcd}(a, b) = \mathrm{pgcd}(da', db') = d\,\mathrm{pgcd}(a', b')$. Donc, comme d est non nul, on a $\mathrm{pgcd}(a', b') = 1$. □

PROPOSITION 61
Soit $r \in \mathbb{Q}$ un nombre rationnel. Alors il existe un unique couple d'entiers $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \dfrac{p}{q}$, avec p et q premiers entre eux.
*L'écriture d'un rationnel sous cette forme est appelée **forme irréductible**.*

Preuve —
• Existence : Comme $r \in \mathbb{Q}$, il existe $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \dfrac{a}{b}$. Posons $d = \mathrm{pgcd}(a, b)$. D'après la proposition précédente, il existe $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ tels que $a = pd$, $b = qd$ et $\mathrm{pgcd}(p, q) = 1$. On a donc $r = \dfrac{a}{b} = \dfrac{pd}{qd} = \dfrac{p}{q}$, avec p et q premiers entre eux.

• Unicité : Soient $(p_1, q_1) \in \mathbb{Z} \times \mathbb{N}^*$ et $(p_2, q_2) \in \mathbb{Z} \times \mathbb{N}^*$ tels que $r = \dfrac{p_1}{q_1} = \dfrac{p_2}{q_2}$ et $\mathrm{pgcd}(p_1, q_1) = \mathrm{pgcd}(p_2, q_2) = 1$.

On a alors $p_1q_2 = p_2q_1$, donc $q_2 \mid p_2q_1$. Comme q_2 et p_2 sont premiers entre eux, le théorème de Gauss nous di que $q_2 \mid q_1$. Par symétrie des rôles de q_1 et q_2, on en déduit que $q_1 \mid q_2$. Ainsi on a $|q_1| = |q_2|$, et par positivité de q_1 et q_2 on obtient $q_1 = q_2$. Comme $p_1q_2 = p_2q_1$, on obtient également $p_1 = p_2$, ce qui conclut la preuve. □

1.4 NOMBRES PREMIERS

1.4.1 L'ensemble des nombres premiers

Définition 62
Soit $p \in \mathbb{N}$. On dit que p est un nombre ***premier*** *\素数\ si p est différent de 1 et si ses seuls diviseurs positifs sont 1 et p.*
On note $\mathcal{P}$ l'ensemble des nombres premiers.

Exemple 63 — *2, 3, 5, 7, 11, 13, 17, 23, ..., sont les plus petits nombres premiers.*

Théorème 64
Tout nombre entier $n \geq 2$ a au moins un diviseur premier.

Preuve — Soit $n \geq 2$. L'ensemble des diviseurs de n qui sont positifs et différents de 1 est une partie non vide de $\mathbb{N} \setminus \{0, 1\}$. Il admet donc un minimum p.

Si p n'était pas premier, alors il admettrait lui-même un diviseur q tel que $2 \leq q < p$. Comme $q \mid p$ et $p \mid n$, on aurait $q \mid n$ q. Cela est une contradiction avec la minimalité de p.

Ainsi, p est un nombre premier, et p divise n. □

Proposition 65
Tout nombre entier $n \geq 2$ qui n'est pas premier a au moins un diviseur premier p tel que $2 \leq p \leq \sqrt{n}$.

Preuve — Soit n un entier supérieur ou égal à 2 et non premier. En reprenant la démonstration précédente, le minimum p de l'ensemble des diviseurs supérieurs ou égaux à 2 de n est un nombre premier. Comme p divise n, il existe $q \in \mathbb{N}$ tel que $n = pq$. q est alors un diviseur de n, donc $p \leq q$ par minimalité de p. On a donc $p^2 \leq pq = n$, d'où $p \leq \sqrt{n}$. □

Remarque 66 — *Le résultat précédent fournit une méthode pour déterminer si un nombre n est premier ou non :*
on effectue successivement la division euclidienne de n par tous les entiers inférieurs à $\sqrt{n}$, et si l'une des divisions donne un reste nul alors n n'est pas premier. Sinon, n est premier.

On peut améliorer cette méthode et dresser la liste des nombres premiers $p \leq n$ de manière algorithmique en utilisant le crible d'Eratosthène.
Pour cela, on écrit tous les nombres compris entre 2 à n, puis on procède comme suit :

1. *Le plus petit nombre est 2 qui est premier, et tous les multiples stricts de 2 ne sont pas premiers, on élimine alors tous ces multiples,*
2. *Le premier nombre restant est 3, qui est donc premier, et tous les multiples stricts de 3 ne sont pas premiers, on élimine alors tous ces multiples,*
3. *Le premier nombre restant est 5, qui est donc premier, et tous les multiples stricts de 5 ne sont pas premiers, on élimine alors tous ces multiples,*
4. *On poursuit ainsi jusqu'à tomber sur un nombre supérieur à $\sqrt{n}$.*

Les entiers non élimés sont alors exactement les nombres premiers inférieurs à n, puisque les entiers non premiers inférieurs à n possèdent un diviseur premier inférieur à $\sqrt{n}$ et ont donc été éliminés.

Proposition 67
Soient p un nombre premier et $a \in \mathbb{Z}$.
Alors soit p divise a, soit p et a sont premiers entre eux.

Preuve — Comme le pgcd de p et a divise p et que p est premier, on a $\text{pgcd}(p, a) = 1$ ou $\text{pgcd}(p, a) = p$. Supposons que p ne divise pas a. On a alors $\text{pgcd}(p, a) \neq p$ car $\text{pgcd}(a, p) \mid a$, donc $\text{pgcd}(p, a) = 1$ et a et p sont premiers entre eux. □

 Ce résultat, comme un certain nombre en arithmétique, n'est vrai que si p est un nombre premier. Par exemple, 6 ne divise pas 15 et 6 et 15 ne sont pas premiers entre eux.

1.4.2 Théorème d'Euclide et petit théorème de Fermat

PROPOSITION 68
Soient $p, q \in \mathbb{N}$ deux nombres premiers distincts. Alors p et q sont premiers entre eux.

Preuve — Soient p, q deux nombres premiers. Supposons que p et q ne sont pas premiers entre eux. La proposition précédente nous dit alors que p divise q et que q divise p. On obtient donc que $p = q$. Par contraposition, on obtient le résultat. □

THÉORÈME 69 (Théorème d'Euclide)
Soient p un nombre premier et $a, b \in \mathbb{Z}$.
Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Preuve — Supposons que $p \mid ab$.

• Si p divise a, c'est bon.

• Sinon, p ne divise pas a. Comme p est premier, p et a sont alors premiers entre eux. Le théorème de Gauss nous dit alors que p divise b, ce qui conclut la preuve. □

PROPOSITION 70
Soient p un nombre premier et $a_1, \ldots, a_n \in \mathbb{Z}$.
Si p divise le produit $a_1 \times \ldots \times a_n = \Pi_{i=1}^{n} a_i$, alors p divise l'un des a_i.

Preuve — Cette généralisation du théorème précédent se démontre par récurrence sur n. □

EXEMPLE 71 — *Soit $(a, b) \in \mathbb{Z}^2$. Si $2 \mid ab$, alors $2 \mid a$ ou $2 \mid b$, car 2 est un nombre premier.*

THÉORÈME 72 (Petit théorème de Fermat)
Soit p est un nombre premier et $a \in \mathbb{Z}$. On a :

$$a^p \equiv a \bmod p.$$

Si p ne divise pas a, alors :

$$a^{p-1} \equiv 1 \bmod p.$$

Preuve — Démontrons dans un premier lieu le résultat pour $a \geq 0$. Nous allons procéder par récurrence sur a.
• Initialisation : Pour $a = 0$ on a $0^p \equiv 0 \bmod p$.
• Hérédité : Supposons que $a^p \equiv a \bmod p$ pour un $a \geq 0$. La formule du binôme nous donne : $(a+1)^p = \sum_{k=0}^{p} a^k \binom{k}{p}$. On rappelle que $\binom{k}{p}$ est égal à $\binom{k}{p} = \frac{p!}{k!(p-k)!}$, où $n! = 1 \times 2 \times \ldots \times n$, et que ce nombre est un entier.
Soit $1 \leq k \leq p-1$. Comme p est premier, p ne divise donc pas $k!$ ni $(p-k)!$, alors que p divise $p!$. Ainsi, le théorème d'Euclide appliqué à $(k!(p-k)!)\binom{k}{p} = p!$ nous dit que p divise $\binom{k}{p}$. On obtient donc :

$$(a+1)^p = \sum_{k=0}^{p} a^k \binom{k}{p} \equiv 1 + 0 + \ldots + 0 + a^p \bmod p \equiv a + 1 \bmod p,$$

ce qui prouve que le résultat est vrai pour $a + 1$.

Le résultat est ainsi vrai pour tout $a \geq 0$.

Soit maintenant $a \neq 0$. Si $p = 2$, on a $(-1)^2 = 1 \equiv -1 \bmod 2$. Si $p \neq 2$ alors p est impair et $(-1)^p = -1 \equiv -1 \bmod p$. Ainsi, on obtient :

$$a^p = (-|a|)^p \equiv (-1)^p |a| \bmod p.$$

Maintenant, lorsque p ne divise pas a, alors a est premier avec p. D'après le théorème de Bézout il existe $u, v \in \mathbb{Z}$ tels que $au + bp = 1$. Cela donne :

$$ua^p \equiv a^{p-1} \bmod p \equiv ua \bmod p \equiv 1 \bmod p.$$

□

REMARQUE 73 — *Le petit théorème de Fermat est très utile pour calculer/simplifier les puissances d'un nombre entier a modulo p. Nous reverrons ce théorème, qui est très important, en étudiant les groupes (voir chapitre Structures algébriques).*

EXEMPLE 74 — *Calculer* $2021^{2021} \bmod 13$ *(déterminer le reste de* 2021^{2021} *dans la division euclidienne par* 13*).*
Le nombre 13 *est premier. D'après le petit théorème de Fermat, on a donc* $2021^{12} \equiv 1 \bmod 13$.

La division euclidienne de 2021 *par* 12 *donne :* $2021 = 12 \times 168 + 5$.

D'autre part, on a $2021 \equiv 6 \bmod 13$. *On a donc :*

$$2021^{2021} \equiv 6^{12\times 168+5} \bmod 13 \equiv (6^{12})^{168} \times 6^5 \bmod 13 \equiv 6^5 \bmod 13.$$

Cela permet de terminer le calcul :

$$6^2 = 36 \equiv -3 \bmod 13, \quad 6^4 = (6^2)^2 \equiv 9 \bmod 13, \quad 6^5 \equiv 9 \times 6 \bmod 13 \equiv 2 \bmod 13.$$

Donc, $2021^{2021} \equiv 2 \bmod 13$.

PROPOSITION 75
L'ensemble $\mathcal{P}$ *est infini : il existe une infinité de nombres premiers.*

Preuve — Supposons par l'absurde qu'il existe un nombre fini N de nombres premiers, notés p_1,p_2,...,p_N.

On pose alors $p = p_1 \times p_2 \times \ldots \times p_N + 1$. Pour tout $1 \leq j \leq N$, $\Pi_{i=1}^N p_i$ est un multiple de p_j. Ainsi, pour tout $1 \leq j \leq N$, p_j ne divise pas p. En effet, sinon p_j diviserait $p - \Pi_{i=1}^N p_i = 1$, ce qui est impossible puisque $p_j > 1$.

On remarque que p est un nombre entier supérieur ou égal à 2. Il admet donc un diviseur premier. Par hypothèse, ce diviseur est forcément de la forme p_{i_0} pour un $i_0 \in \{1, \ldots, N\}$. Cela implique que $p_{i_0} \mid p$, ce qui est absurde.

Ainsi, le nombre de nombres premiers est infini, ce qui conclut la preuve. □

1.4.3 Décomposition en produit de facteurs premiers

THÉORÈME 76 (Théorème fondamental de l'arithmétique)
Soit $n \in \mathbb{N}$ *un entier naturel, avec* $n \geq 2$.
Alors n se décompose, de manière unique à l'ordre près des termes, en produit de facteurs premiers :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_N^{\alpha_N},$$

où les p_i *sont des nombres premiers deux à deux distincts et les* α_i *sont des entiers naturels non nuls.*

Preuve —

- *Existence :* Démontrons ce résultat par récurrence sur n. Pour tout $n \geq 2$, on note (H_n) la propriété : « n se décompose en produit de facteurs premiers. »
  • *Initialisation :* $n = 2$ est un nombre premier, donc n s'écrit comme le produit de nombres premiers. Donc (H_2) est vraie.
  • *Hérédité :* Soit $n \geq 3$. Supposons (H_k) vraie pour tout $2 \leq k \leq n-1$.
  Si n est premier, alors n se décompose en produit de facteurs premiers.
  Sinon, il existe des entiers naturels a, b, avec $a, b > 1$, tels que $n = ab$. On a ainsi $a < n$ et $b < n$, donc l'hypothèse de récurrence s'applique à a et à b, qui se décomposent en un produit de facteurs premiers. Comme n est le produit de a et b, il est un produit de facteurs premiers, donc (H_n) est vraie.
- *Unicité :* Supposons que n se décompose en deux produits :
  $$n = p_1^{\alpha_1} \times \ldots \times p_N^{\alpha_N} \quad \text{et} \quad n = q_1^{\beta_1} \times \ldots \times q_R^{\beta_R},$$
  où les p_i et q_j sont des nombres premiers, avec les p_i distincts deux à deux, les q_j également, et où les α_i, β_j sont des entiers naturels non nuls.
  Pour tout $i \in \{1, \ldots, N\}$ on a $p_i \mid n$, donc p_i divise l'un des q_j. Comme p_i et q_j sont des nombres premiers, on a $p_i = q_j$. Donc, $\{p_1, \ldots, p_N\} \subset \{q_1, \ldots, q_R\}$.
  Par symétrie des rôles, on en déduit que $\{q_1, \ldots, q_R\} \subset \{p_1, \ldots, p_N\}$. Ces deux ensembles sont donc égaux et on a $N = R$. Quitte à permuter les indices, on peut supposer que $p_i = q_i$ pour tout $i \in \{1, \ldots, N\}$.
  Soit $\leq i \leq N$. On a $p_i^{\alpha_i} \mid n$, avec $n = q_1^{\beta_1} \times \ldots q_N^{\beta_N} = q_i^{\beta_i} \times k$. Comme $q_i = p_i$, on a $\text{pgcd}(p_i^{\alpha_i}, k) = 1$. Ainsi, le théorème de Gauss nous dit que $p_i^{\alpha_i} \mid p_i^{\beta_i}$. Donc $\alpha_i \leq \beta_i$. Par symétrie des rôles, on a de même $\beta_i \leq \alpha_i$, donc finalement $\alpha_i = \beta_i$.
  Cette décomposition en produit de facteurs premiers est donc unique à l'ordre près.

□

DÉFINITION 77
Soient $n \geq 2$ *un entier naturel et p un nombre premier.*
On définit $\nu_p(n)$ *l'exposant de p dans la décomposition de n en facteurs premiers (* *avec* $\nu_p(n) = 0$ *si p ne divise pas n). L'entier* $\nu_p(n)$ *est appelé la* ***valuation p-adique*** *de n.*

Remarque 78 — *On a* $\nu_p(n) = \max\{k \in \mathbb{N} \mid p^k \text{ divise } n\}$.
On peut aussi écrire l'entier n *comme :*

$$n = \Pi_{p\in\mathcal{P},\, p\leq n} p^{\nu_p(n)}.$$

Méthode 79 — *Pour décomposer un nombre entier* $n \geq 2$*, on peut procéder de la façon suivante :*

1. *On cherche la plus grande puissance* $\alpha_1 \geq 0$ *de* 2 *divisant* n*, on obtient* $n = 2^{\alpha_1} n_1$ *où* $n_1 \in \mathbb{N}$ *et* n_1 *n'est plus divisible par* 2*. Si* $n_1 = 1$*, on a terminé, sinon on passe à l'étape suivante.*
2. *On cherche la plus grande puissance* $\alpha_2 \geq 0$ *de* 3 *divisant* n_1*, on obtient alors* $n = 2^{\alpha_1} \times 3^{\alpha_2} n_2$ *où* $n_2 \in \mathbb{N}$ *et* n_2 *n'est plus divisible par* 3 *(ni* 2 *par la première étape). Si* $n_2 = 1$*, on a terminé, sinon on passe à l'étape suivante.*
3. *On cherche la plus grande puissance* $\alpha_3 \geq 0$ *de* 5 *divisant* n_2*, etc.*

Exemple 80 — $360 = 2^3 \times 3^2 \times 5$, $147 = 3 \times 7^2$, $1575 = 3^2 \times 5^2 \times 7$.

Proposition 81
Soit un entier $n \geq 2$*. Soit* $n = p_1^{\alpha_1} \times \ldots \times p_N^{\alpha_N}$ *la décomposition de* n *en facteurs premiers, avec* p_i *des nombres premiers distincts deux à deux et* α_i *des entiers naturels non nuls.*

Alors les diviseurs positifs de n *sont exactement les entiers de la forme* $p_1^{\beta_1} \ldots p_N^{\beta_N}$ *avec* $0 \leq \beta_i \leq \alpha_i$ *pour tout* $1 \leq i \leq N$*.*

L'entier n *possède ainsi* $\Pi_{i=1}^N (\alpha_i + 1)$ *diviseurs.*

Preuve — Soit m un diviseur de n. Alors tous les facteurs premiers de m sont des diviseurs de n. Ainsi, m est de la forme $m = p_1^{\beta_1} \ldots p_N^{\beta_N}$.

Comme $m \mid n$ on a $p_i^{\beta_i} \mid n$ pour tout $1 \leq i \leq N$, donc $\beta_i \leq \alpha_i$ d'après la preuve du théorème.

Réciproquement, tout entier m de la forme $m = p_1^{\beta_1} \ldots p_N^{\beta_N}$ avec $\beta_i \leq \alpha_i$ $\forall 1 \leq i \leq N$ est un diviseur de n.

Par unicité de la décomposition en facteurs premiers (à l'ordre près des termes), le nombre de diviseurs de n est égal au nombre de choix possibles des N entiers $(\beta_1, \ldots, \beta_N)$. Comme on a $\beta_i \in \{0, \ldots, \alpha_i\}$, on a $\alpha_i + 1$ choix pour β_i, ce qui donne $\Pi_{i=1}^N (\alpha_i + 1)$ diviseurs de n. □

Exemple 82 — *Les diviseurs positifs de* $45 = 3^2 \times 5$ *sont les suivants :* $3^0 \times 5^0 = 1$, $3^0 \times 5 = 5$, $3 \times 5^0 = 3$, $3 \times 5 = 15$, $3^2 \times 5^0 = 9$, $3^2 \times 5 = 45$.

On dispose du résultat suivant pour calculer le pgcd et le ppcm de deux entiers à partir de leur décomposition en produit de nombres premiers.

Proposition 83
Soient $a, b \in \mathbb{N}$ *supérieurs ou égaux à* 2*. On suppose que* $a = p_1^{\alpha_1} \times \ldots \times p_N^{\alpha_N}$ *et* $b = p_1^{\beta_1} \times \ldots \times p_N^{\beta_N}$*, où les* p_i *sont des nombres premiers distincts deux à deux et les* α_i, β_i *sont des entiers naturels (éventuellement nuls). Alors on a :*

- $\text{pgcd}(a, b) = p_1^{\min(\alpha_1, \beta_1)} \times \ldots \times p_N^{\min(\alpha_N, \beta_N)}$,
- $\text{ppcm}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \times \ldots \times p_N^{\max(\alpha_N, \beta_N)}$.

Preuve — On montre que $p_1^{\min(\alpha_1, \beta_1)} \times \ldots \times p_N^{\min(\alpha_N, \beta_N)}$ est un diviseur commun de a et b, et le plus grand de leurs diviseurs communs.

On montre que $p_1^{\max(\alpha_1, \beta_1)} \times \ldots \times p_N^{\max(\alpha_N, \beta_N)}$ est un multiple commun de a et b, et le plus petit de leurs multiples communs.

Les Propositions 26 et 40 nous disent alors que ces quantités sont $\text{pgcd}(a, b)$ et $\text{ppcm}(a, b)$. □

Exemples 84

- $\text{pgcd}(147, 1575) = 3 \times 7 = 21$,
- $\text{ppcm}(147, 1575) = 3^2 \times 5^2 \times 7^2 = 11025$.

On établit alors la relation suivante qui lie pgcd et ppcm.

PROPOSITION 85
Soient $a, b \in \mathbb{Z}$. Alors on a

$$\text{pgcd}(a,b) \times \text{ppcm}(a,b) = |a| \times |b|.$$

En particulier, si a et b sont premiers entre eux, on a $\text{ppcm}(a,b) = |a| \times |b|$.

Preuve — On peut supposer a et b positifs. Si $a = 0$ ou $b = 0$ on a $\text{ppcm}(a,b) = 0$, et le résultat est vrai. Si $a = 1$ ou $b = 1$ on a $\text{pgcd}(a,b) = 1$, et le résultat est vrai.

Supposons que $a \geq 2$ et $b \geq 2$. Soient $p_1, \ldots, p_N$ les nombres premiers divisant a ou b. D'après le théorème fondamental de l'arithmétique, on a alors $a = p_1^{\alpha_1} \times \ldots \times p_N^{\alpha_N}$ et $b = p_1^{\beta_1} \times \ldots \times p_N^{\beta_N}$, où les α_i, β_i sont des entiers naturels (éventuellement nuls).

La proposition précédents nous fournit alors les valeurs de $\text{pgcd}(a,b)$ et $\text{ppcm}(a,b)$ en fonction des p_i, α_i et β_i. On a alors :

$$\begin{array}{ll} \text{pgcd}(a,b) \times \text{ppcm}(a,b) & = p_1^{\min(\alpha_1,\beta_1)+\max(\alpha_1,\beta_1)} \times \ldots \times p_N^{\min(\alpha_N,\beta_N)+\max(\alpha_N,\beta_N)} \\ & = p_1^{\alpha_1+\beta_1} \times \ldots \times p_N^{\alpha_N+\beta_N} = ab \end{array},$$

ce qui conclut. □

EXEMPLE 86 — *Les multiples communs à 12 et 18 sont les multiples de 36.*
En effet, $\text{ppcm}(12,18) = \dfrac{12 \times 18}{\text{pgcd}(12,18)} = \dfrac{12 \times 18}{6} = 36.$

PROPOSITION 87
Soient $a, b \in \mathbb{Z}$. Alors a et b sont premiers entre eux si et seulement s'ils n'ont pas de facteurs premiers en commun dans leur décomposition en produit de facteurs premiers.

Preuve — Si a et b sont premiers entre eux, alors leur seul diviseur commun positif est 1 et ils n'ont donc pas de facteur premier en commun.

Réciproquement, supposons que a et b n'ont pas de facteurs premiers en commun. Notons $d = \text{pgcd}(a,b)$. Si l'on avait $d \geq 2$, alors d admettrait un diviseur premier p. Comme d divise a et b, p diviserait également a et b et il serait donc un facteur premier commun à a et à b, ce qui est impossible. On a donc $d = 1$, donc a et b sont premiers entre eux. □

EXEMPLE 88 — $825 = 3 \times 5^2 \times 11$ *et* $56 = 2^3 \times 7$ *sont premiers entre eux.*

Chapitre 2 Matrices

Table des matières du chapitre

Dans ce chapitre, après avoir défini les matrices et les opérations sur ces matrices :

- on les utilise pour représenter un système linéaire et pour le résoudre ;
- on étudie les structures de l'ensemble des matrices (structure d'espace vectoriel et d'anneau, sous-ensembles particuliers).

2.1 Définitions

Dans tout ce chapitre, l'ensemble $\mathbb{K}$ désignera $\mathbb{R}$ ou $\mathbb{C}$ ou $\mathbb{Q}$. Ces ensembles sont des corps, et cette notion sera traitée en Algèbre 2, chapitre Structures algébriques. [1]

Définition 1
Soit $\mathbb{K}$ un corps. Soient n et p deux entiers naturels non nuls.
Soit A un tableau, avec n lignes, p colonnes, dont les nombres sont dans $\mathbb{K}$. C'est-à-dire :

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,j} & \dots & a_{1,p} \\ a_{2,1} & a_{2,2} & \dots & a_{2,j} & \dots & a_{2,p} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i,1} & a_{i,2} & \dots & a_{i,j} & \dots & a_{i,p} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,j} & \dots & a_{n,p} \end{pmatrix}.$$

*Les nombres $a_{1,1}, \dots, a_{n,p}$ sont appelés **coefficients** de A.*
*On dit alors que A est une **matrice** à n lignes et p colonnes à coefficients dans $\mathbb{K}$, ou matrice $n \times p$ \数域$\mathbb{K}$上n行p列（或$n \times p$）的矩阵\.*
On note $\mathscr{M}_{n,p}(\mathbb{K})$ l'ensemble des matrices $n \times p$.

Pour A une matrice à n lignes et p colonnes, A est définie par ses $n \times p$ coefficients. On écrit aussi cette matrice comme :

$$A = (a_{i,j})_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]} \quad \text{ou} \quad A = (a_{i,j})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant p}.$$

Les entiers i, j sont appelés **indices** des coefficients de la matrice A.
Le premier indice d'un coefficient est le numéro de sa ligne, et le second indice est le numéro de sa colonne.

1. Un corps est un ensemble $\mathbb{K}$ muni d'une opération d'addition $+$ et d'une opération de multiplication $\times$. Ces opérations vérifient des propriétés comme $a+b=b+a$, $a.b=b.a$, $a(b+c)=ab+bc$,... Il faut aussi que tout élément non-nul possède un inverse pour la multiplication $\times$. C'est pour cela que $\mathbb{Z}$ n'est pas un corps, mais $\mathbb{Q}$ oui. Les exemples essentiels de corps sont $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Exemple 2 — $A = \begin{pmatrix} 1 & 2 & 3 \\ -1 & 10 & 5 \end{pmatrix}$ *est une matrice à 2 lignes et 3 colonnes, donc* $A \in \mathscr{M}_{2,3}(\mathbb{Q})$.
$B = \begin{pmatrix} \frac{1}{5} \\ 10 \\ \sqrt{2} \end{pmatrix}$ *est une matrice à 3 lignes et 1 colonne, donc* $B \in \mathscr{M}_{3,1}(\mathbb{R})$. $C = \begin{pmatrix} 1+i & \exp(\frac{i\Pi}{6}) \\ -1 & \sqrt{5} \end{pmatrix}$ *est une matrice à 2 lignes et 2 colonnes, donc* $C \in \mathscr{M}_{2,2}(\mathbb{C})$. *Pour* $C = (c_{i,j})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant p}$, *on a* $c_{1,1} = 1+i$, $c_{1,2} = \exp(\frac{i\Pi}{6})$, $c_{2,1} = -1$, $c_{2,2} = \sqrt{5}$.

Définition 3
Soient $\mathbb{K}$ *un corps et* $n, p \in \mathbb{N}^*$. *Soit* A *une matrice à* n *lignes et* p *colonnes à coefficients dans* $\mathbb{K}$.

- *On dit que la matrice* A *est* ***nulle*** *si tous les coefficients* $a_{i,j}$ *sont nuls.*
  On la note alors $A = 0_{\mathscr{M}_{n,p}(\mathbb{K})}$ *ou* $0_{n,p}$ *ou* 0 *;*
- *Si* $p = 1$, *on dit alors que* A *est une* ***matrice ligne****. Si* $q = 1$, *on dit alors que* A *est une* ***matrice colonne****. L'usage est de lire une matrice en suivant ses colonnes ;*
- *Si* $n = p$, *on dit alors que* $A = (a_{i,j})_{1 \leqslant i,j \leqslant n}$ *est une* ***matrice carrée*** \方阵\.
  On note $\mathscr{M}_n(\mathbb{K})$ *l'ensemble* $\mathscr{M}_{n,n}(\mathbb{K})$ *des matrices de taille* $n \times n$.

2.2 L'espace vectoriel $\mathscr{M}_{n,p}(\mathbb{K})$

Définition 4
Soit $\mathbb{K}$ *un corps. Soient* $n, p \in \mathbb{N}^*$.
Pour chaque $(i,j) \in [\![1,n]\!] \times [\![1,p]\!]$, *on définit* $E_{i,j}$ *la matrice de* $\mathscr{M}_{n,p}(\mathbb{K})$ *dont tous les coefficients sont nuls, sauf le coefficient d'indice* (i,j) *qui vaut 1. C'est-à-dire :*

$$E_{ij} = \begin{pmatrix} a_{1,1}=0 & \dots & a_{1,j}=0 & \dots & a_{1,p}=0 \\ \vdots & & \vdots & & \vdots \\ a_{i,1}=0 & \dots & a_{i,j}=1 & \dots & a_{i,p}=0 \\ \vdots & & \vdots & & \vdots \\ a_{n,1}=0 & \dots & a_{n,j}=0 & \dots & a_{n,p}=0 \end{pmatrix} = (\delta_{i,k}\delta j, l)_{k,l}.$$

Exemple 5 — *Dans* $\mathscr{M}_2(\mathbb{K})$, *on a* $E_{1,2} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $E_{2,2} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $E_{2,1} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

Définition 6 (Multiplication par un scalaire, Somme de matrices)
Soit $\mathbb{K}$ *un corps. Soient* $n, p \in \mathbb{N}^*$. *On définit les opérations suivantes :*

1. *Le* ***produit d'un scalaire*** $\lambda \in \mathbb{K}$ ***et d'une matrice*** $A = (a_{i,j})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant p} \in \mathscr{M}_{n,p}(\mathbb{K})$ *est la matrice notée* $\lambda \cdot A$ *ou* λA *obtenue en multipliant tous les coefficients par* λ *:*

$$\lambda \cdot A = (\lambda a_{i,j})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant p} \in \mathscr{M}_{n,p}(\mathbb{K}).$$

2. *La* ***somme de deux matrices*** $A = (a_{i,j}) \in \mathscr{M}_{n,p}(\mathbb{K})$ *et* $B = (b_{i,j}) \in \mathscr{M}_{n,p}(\mathbb{K})$ *est la matrice*

$$A + B = (a_{i,j} + b_{i,j}) \in \mathscr{M}_{n,p}(\mathbb{K}).$$

Exemple 7 — $2.\begin{pmatrix} 1 & 0 \\ 5 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 10 & 5 \end{pmatrix}$.
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix}$
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 3 \end{pmatrix}$ *n'a pas de sens.*

PROPOSITION 8
L'ensemble $(\mathscr{M}_{n,p}(\mathbb{K}),+,.)$ des matrices $n\times p$, muni des opérations d'addition et de mutliplication par un scalaire, est un $\mathbb{K}-$espace vectoriel.
Il est de dimension $n\cdot p$. La famille $(E_{i,j})_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]}$ est une base de $\mathscr{M}_{n,p}(\mathbb{K})$.
On l'appelle ***la base canonique de*** $\mathscr{M}_{n,p}(\mathbb{K})$ \矩阵空间的标准基\.

Preuve — L'ensemble $(\mathscr{M}_{n,p}(\mathbb{K}),+,.)$ des applications de $[\![1,n]\!]\times[\![1,p]\!]$ dans $\mathbb{K}$ vérifie les axiomes de structure d'un espace vectoriel (voir Géométrie 1).
De plus, toute matrice $A=(a_{i,j})_{1\leqslant i\leqslant n,1\leqslant j\leqslant p}$ s'écrit comme :

$$A=\sum_{(i,j)\in[\![1,n]\!]\times[\![1,p]\!]} a_{i,j}\,E_{i,j}$$

Cette écriture étant unique, toute matrice de $\mathscr{M}_{n,p}(\mathbb{K})$ est une unique combinaison linéaire des $n\cdot p$ matrices $E_{i,j}$. Ainsi, les np matrices $E_{i,j}$ forment une base de $\mathscr{M}_{n,p}(\mathbb{K})$, et cet espace vectoriel est donc de dimension np (voir Géométrie 1). □

DÉFINITION 9
Soient $\mathbb{K}$ un corps et $n\in\mathbb{N}^*$. On dit qu'une matrice carrée $A\in\mathscr{M}_n(\mathbb{K})$ est

- ***triangulaire supérieure*** \上三角矩阵\ *si $\forall(i,j)$ avec $i>j$, on a $a_{i,j}=0$. C'est-à-dire si A est de la forme :*

$$\begin{pmatrix} * & \cdots & & * \\ 0 & & & \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & * \end{pmatrix}$$

  où chaque $*$ est un scalaire de $\mathbb{K}$ quelconque.
  On note $\mathscr{T}_n(\mathbb{K})$ l'ensemble des matrices $n\times n$ triangulaires supérieures.
  (De même, A est une matrice ***triangulaire inférieure*** \下三角矩阵\ *si $\forall i<j$ on a $a_{i,j}=0$.)*
- ***diagonale*** \对角阵\ *si $\forall(i,j)$ avec $i\neq j$ on a $a_{i,j}=0$, c'est-à-dire si A est de la forme :*

$$\begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}.$$

  Cette matrice se note $\mathrm{Diag}\,(\lambda_1,\lambda_2,\ldots,\lambda_n)$.
  On note $\mathscr{D}_n(\mathbb{K})$ l'ensemble des matrices diagonales de taille $n\times n$.

EXEMPLE 10 — $\begin{pmatrix} 0 & 1 & 5 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 & 5 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ *sont des matrices triangulaires supérieures.*
$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ *est une matrice diagonale.*
La matrice nulle $0_{\mathscr{M}_n(\mathbb{K})}$ est une matrice diagonale.
Les matrices diagonales sont des matrices triangulaires supérieures et des matrices triangulaires inférieures.

REMARQUE 11 — *L'ensemble $\mathscr{T}_n(\mathbb{K})$ est un sous-espace vectoriel de $\mathscr{M}_n(\mathbb{K})$. La famille $(E_{i,j})_{1\leqslant i\leqslant j\leqslant n}$ est une famille génératrice de cet espace vectoriel. Ainsi, on a* $\dim\mathscr{T}_n(\mathbb{K})=\dfrac{n(n+1)}{2}$.
L'ensemble $\mathscr{D}_n(\mathbb{K})$ est un sous-espace vectoriel de $\mathscr{M}_n(\mathbb{K})$. La famille $(E_{i,i})_{1\leqslant i\leqslant n}$ est une famille génératrice de cet espace vectoriel. Ainsi, on a $\dim\mathscr{D}_n(\mathbb{K})=n$.

2.3 PRODUIT DE DEUX MATRICES

Produit de matrices, propriétés

Définition 12
Soient $\mathbb{K}$ un corps et $p, q, r \in \mathbb{N}^*$. On définit le ***produit*** *de deux matrices*

$$A = (a_{i,j})_{(i,j)\in[\![1,p]\!]\times[\![1,q]\!]} \in \mathscr{M}_{p,q}(\mathbb{K}) \quad \text{et} \quad B = (b_{j,k})_{(j,k)\in[\![1,q]\!]\times[\![1,r]\!]} \in \mathscr{M}_{q,r}(\mathbb{K}),$$

noté $A \times B$ ou AB, comme la matrice

$$C = (c_{i,k})_{(i,k)\in[\![1,p]\!]\times[\![1,r]\!]} \in \mathscr{M}_{p,r}(\mathbb{K}) \text{ avec } c_{i,k} = \sum_{j=1}^{q} a_{i,j}\, b_{j,k}.$$

Remarque 13 —

1. *Le produit AB n'a de sens que si le nombre de colonnes de la matrice A soit égal au nombre de lignes de la matrice B.*
2. *Pour $n \in \mathbb{N}^*$, si A et B appartiennent à $\mathscr{M}_n(\mathbb{K})$, alors le produit $A \times B$ est bien défini et est aussi un élément de $\mathscr{M}_n(\mathbb{K})$.*
3. *Dans le calcul de $c_{i,k}$ interviennent les coefficients de la $i^{ème}$ ligne de B et les coefficients de la $k^{ème}$ colonne de A :*

$$\begin{pmatrix} a_{1,1} & \dots & a_{1,j} & \dots & a_{1,q} \\ \vdots & & & & \vdots \\ a_{i,1} & \dots & a_{i,j} & \dots & a_{i,q} \\ \vdots & & & & \vdots \\ a_{p,1} & \dots & a_{p,j} & \dots & a_{p,q} \end{pmatrix} \rightarrow \begin{pmatrix} c_{1,1} & \dots & & \dots & c_{1,r} \\ \vdots & & & & \vdots \\ & & \boxed{c_{i,k}} & & \\ \vdots & & & & \vdots \\ c_{p,1} & \dots & & \dots & c_{p,r} \end{pmatrix} \quad \begin{matrix} \\ \\ \\ \\ \\ \end{matrix} \begin{pmatrix} b_{1,1} & \dots & b_{1,k} & \dots & b_{1,r} \\ \vdots & & \vdots & & \vdots \\ b_{j,1} & & b_{j,k} & & b_{j,r} \\ \vdots & & \vdots & & \vdots \\ b_{q,1} & \dots & b_{q,k} & \dots & b_{q,r} \end{pmatrix} \downarrow$$

Exemples 14

1. $\begin{pmatrix} 2 & -1 & 3 \\ -2 & 2 & -1 \end{pmatrix} \begin{pmatrix} -1 & 2 & 1 \\ 4 & -2 & 3 \\ -2 & 1 & -1 \end{pmatrix} = \begin{pmatrix} -12 & 9 & -4 \\ 12 & -9 & 5 \end{pmatrix}.$
2. $\begin{pmatrix} -1 & 2 & 1 \\ 4 & -2 & 3 \\ -2 & 1 & -1 \end{pmatrix} \begin{pmatrix} 2 & -1 & 3 \\ -2 & 2 & -1 \end{pmatrix}$ *n'a pas de sens.*
3. *Le produit d'une matrice carrée et d'une matrice colonne est une matrice colonne. Par exemple :*

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 14 \\ 0 \\ 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ -3 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Cet exemple permet de remarquer que le produit de deux matrices non-nulles peut être une matrice nulle. Ainsi :

$$AX = 0 \not\Longrightarrow A = 0 \quad ou \quad X = 0.$$

Proposition 15
Soient $\mathbb{K}$ un corps et $p, q \in \mathbb{N}^*$. Soient A et B dans $\mathscr{M}_{p,q}(\mathbb{K})$. On a :

(i) Si $AX = BX$ pour toute matrice colonne $X \in \mathscr{M}_{q,1}(\mathbb{K})$, alors $A = B$;

(ii) En particulier, si l'on a $AX = 0$ pour tout $X \in \mathscr{M}_{q,1}(\mathbb{K})$, alors la matrice A est la matrice nulle.

Preuve —

(i) Soit X_j la matrice colonne dont tous les coefficients sont nuls sauf le j-ième qui vaut 1. Le produit $A\,X_j$ est alors la j-ième colonne de la matrice A. De nême, $B\,X_j$ est la j-ième colonne de B.
Comme pour chaque $j \in [\![1, q]\!]$ on a $A\,X_j = B\,X_j$, les matrices A et B ont ainsi les mêmes colonnes. Donc $A = B$.

(ii) On est dans le cas particulier où la matrice B est nulle. Le point (i) donne alors $A = B = 0$.

□

REMARQUE 16 —

1. *Le produit d'une matrice ligne et d'une matrice colonne de même longueur est une matrice* 1×1 *qu'on identifie à un scalaire. Par exemple :*

$$\begin{pmatrix}1 & 2 & 3\end{pmatrix}\begin{pmatrix}1\\2\\3\end{pmatrix} = (14) = 14.$$

2. *Le produit d'une matrice colonne et d'une matrice ligne de même longueur est une matrice carrée. Par exemple :*

$$\begin{pmatrix}1\\2\\3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\2 & 4 & 6\\3 & 6 & 9\end{pmatrix}.$$

EXERCICE 17 —

1. *Calculer les deux produits*

$$\begin{pmatrix}\lambda_1 & 0 & 0\\0 & \lambda_2 & 0\\0 & 0 & \lambda_3\end{pmatrix}\begin{pmatrix}a & d & g\\b & e & h\\c & f & i\end{pmatrix} \quad et \quad \begin{pmatrix}a & d & g\\b & e & h\\c & f & i\end{pmatrix}\begin{pmatrix}\lambda_1 & 0 & 0\\0 & \lambda_2 & 0\\0 & 0 & \lambda_3\end{pmatrix}.$$

2. *Montrer que :*

$$E_{i,j}\,E_{k,l} = \delta_{j,k}\,E_{i,l}$$

où $\delta_{j,k}$ *est le* ***symbole de Kronecker*** \克罗内克符号\ *qui vaut* 1 *si* $j = k$ *et* 0 *sinon.*

PROPOSITION 18
Soient $\mathbb{K}$ *un corps,* $n \geq 1$, *et* $1 \leq i, j \leq n$. *On a :*

$$E_{i,j}\,E_{k,l} = \delta_{j,k}\,E_{i,l}.$$

Les matrices $E_{i,j}$ formant la base canonique de l'espace vectoriel $\mathscr{M}_n(\mathbb{K})$, connaître le produit de deux de ces matrices est parfois très utile.

PROPOSITION 19 (Propriétés du produit matriciel)
Soient $\mathbb{K}$ *un corps et* $p, q, r, s \in \mathbb{N}^*$. *Soient* $A, A' \in \mathscr{M}_{p,q}(\mathbb{K})$, $B, B' \in \mathscr{M}_{q,r}(\mathbb{K})$, $C \in \mathscr{M}_{r,s}(\mathbb{K})$, *et* $\lambda \in \mathbb{K}$. *On a :*

1. $A\,(\lambda\,B) = \lambda\,(A\,B)$.
Le produit matriciel et la multiplication par un scalaire commutent.
2. $A\,(B + B') = (A\,B) + (A\,B')$ *et* $(A + A')\,B = (A\,B) + (A'\,B)$.
Le produit matriciel est distributif à gauche et à droite par rapport à l'addition de matrices.
3. $A\,(B\,C) = (A\,B)\,C$.
*On dit que le produit matriciel a la propriété d'****associativité*** \结合律\. *Le résultat d'une chaîne de produits matriciels ne dépend pas de l'ordre dans lequel on effectue les produits.*

Preuve — Soient $A = (a_{i,j})_{(i,j)\in[\![1,p]\!]\times[\![1,q]\!]}$, $B = (b_{i,j})_{(i,j)\in[\![1,q]\!]\times[\![1,r]\!]}$, $B' = (b'_{i,j})_{(i,j)\in[\![1,q]\!]\times[\![1,r]\!]}$ et $C = (c_{i,j})_{(i,j)\in[\![1,r]\!]\times[\![1,s]\!]}$ quatre matrices. Soit $\lambda \in \mathbb{K}$. On a alors les égalités :

1.
$$\begin{array}{rcl} A(\lambda B) & = & (\sum_{k=1}^{n} a_{i,k}\lambda b_{k,j})_{(i,j)\in[\![1,p]\!]\times[\![1,r]\!]} \\ & = & (\lambda\sum_{k=1}^{n} a_{i,k} b_{k,j})_{(i,j)\in[\![1,p]\!]\times[\![1,r]\!]} \\ & = & \lambda(AB). \end{array} .$$

2.
$$\begin{array}{rcl} A(B+B') & = & (\sum_{k=1}^{n} a_{i,k}(b_{k,j}+b'_{k,j}))_{(i,j)\in[\![1,p]\!]\times[\![1,r]\!]} \\ & = & (\sum_{k=1}^{n} a_{i,k} b_{k,j} + \sum_{k=1}^{n} a_{i,k} b'_{k,j})_{(i,j)\in[\![1,p]\!]\times[\![1,r]\!]} \\ & = & AB + AB'. \end{array} .$$

L'autre égalité se démontre de la même manière.

3.
$$\begin{array}{rcl} (AB)C & = & (\sum_{l=1}^{r}(\sum_{k=1}^{q} a_{i,k} b_{k,l}) c_{l,j})_{(i,j)\in[\![1,p]\!]\times[\![1,s]\!]} \\ & = & (\sum_{k=1}^{q} a_{i,k}(\sum_{l=1}^{r} b_{k,l} c_{l,j}))_{(i,j)\in[\![1,p]\!]\times[\![1,s]\!]} \\ & = & A(BC) \end{array} .$$

□

L'anneau $\mathscr{M}_n(\mathbb{K})$

Définition 20
Soient $\mathbb{K}$ un corps et $n \in \mathbb{N}^*$. On définit la ***la matrice identité*** \通常称为单位阵\ *$n \times n$, notée I_n, comme la matrice :*

$$I_n = \mathrm{Diag}\,(1, 1, \ldots, 1) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Définition 21
Soient $\mathbb{K}$ un corps et $n \in \mathbb{N}^*$. Soit $A \in \mathscr{M}_n(\mathbb{K})$. Pour $k \in \mathbb{N}$ on définit la ***puissance k-ième*** *de A, notée A^k, par :*

$$\begin{array}{rcl} A^0 & = & I_n \\ A^k & = & A \times A \times \ldots \times A \ (k \text{ fois}), \text{ si } k > 0 \end{array}$$

Cette définition a bien un sens car il a été montré à la Prop. 19 que le produit matriciel est associatif ($A(BC) = (AB)C =_{def} ABC$).

Exercice 22 — *Montrer que, pour toute matrice colonne $X \in \mathscr{M}_{n,1}(\mathbb{K})$ et toute matrice carrée $A \in \mathscr{M}_n(\mathbb{K})$, on a :*

$$I_n\, X = X \qquad et \qquad I_n\, A = A\, I_n = A.$$

Montrer que, pour tous $k, l \in \mathbb{N}$, on a $A^k \times A^l = A^{k+l}$.

Proposition 23
Soient $\mathbb{K}$ un corps et $n \in \mathbb{N}^*$. L'ensemble $(\mathscr{M}_n(\mathbb{K}), +, \times)$ des matrices carrées $n \times n$ muni de l'addition de matrices et de la multiplication matricielle est un anneau. C'est-à-dire :

- *L'ensemble $(\mathscr{M}_n(\mathbb{K}), +)$ des matrices carrées $n \times n$ muni de l'addition de matrices est un groupe, commutatif ($A + B = B + A$), dont l'élément neutre est la matrice nulle 0_n.*
- *La multiplication matricielle est associative ($A(BC) = (AB)C$).*
- *La multiplication matricielle est distributive à droite et à gauche par rapport à l'addition ($A(B+B') = AB + AB'$ et $(A + A')B = AB + A'B$), et a un élément neutre qui est la matrice identité I_n ($AI_n = I_nA = A$).*

De plus, cet anneau n'est pas intègre :

$$AB = 0 \not\Longrightarrow \quad A = 0 \text{ ou } B = 0,$$

C'est-à-dire qu'il existe des matrices A, B non-nulles telles que $AB = 0$.
Et cet anneau n'est pas commutatif :

$$AB \text{ n'est pas toujours égal à } BA.$$

C'est-à-dire qu'il existe des matrices A, B telles que $AB \neq BA$.

Preuve —Les notions de groupe et d'anneau seront détaillées dans le cours Algèbre 2. Commençons par montrer que $(\mathscr{M}_n(\mathbb{K}), +\times)$ est un anneau :

- L'ensemble $(\mathscr{M}_n(\mathbb{K}), +)$ est un groupe commutatif dont l'élément neutre est la matrice nulle (voir cours Algèbre 2) ;
- D'après la proposition 19, la multiplication matricielle $\times$ est une loi de composition interne associative ;
- D'après la proposition 19, la multiplication matricielle $\times$ est distributive à gauche et à droite par rapport à la loi d'addition matricielle $+$. La matrice identité I_n est un élément neutre pour $\times$ car $I_n A = A I_n = A$ pour tout $A \in \mathscr{M}_n(\mathbb{K})$ (voir 22).

Cet anneau n'est pas intègre car $E_{1,2}E_{1,1} = 0$ (voir 17), et n'est pas commutatif car

$$E_{1,2}E_{1,1} = 0 \neq E_{1,2} = E_{1,1}E_{1,2}.$$

□

Remarque 24 (Difficultés dans les anneaux non commutatifs) — *Pour A et B deux matrices de $\mathscr{M}_n(\mathbb{K})$, on ne peut en général pas appliquer les formules du binôme pour développer $(A+B)^2$, $(A+B)^m$ ou pour factoriser $A^2 - B^2$,$A^m - B^m$.*
On a par exemple $(A+B)^2 = (A+B)(A+B) = A^2 + AB + BA + B^2$, mais on ne peut pas simplifier plus cette expression car A et B ne commutent pas forcément (on ne sait rien entre AB et BA).
Lorsque les matrices A et B commutent on peut appliquer les formules de développement ou de factorisation, ce qui en fait un cas très particulier.

Exemple 25 (Difficultés dans les anneaux non intègres) —
Prenons $a \in [0,1]$ et $b = \sqrt{1-a^2}$. Posons $A = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}$. On a alors :

$$A^2 = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}\begin{pmatrix} a & b \\ b & -a \end{pmatrix} = \begin{pmatrix} a^2+b^2 & ab-ba \\ ab-ba & b^2+a^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

Ainsi, dans $\mathscr{M}_2(\mathbb{K})$ (pour $\mathbb{K} = \mathbb{Q}$,$\mathbb{R}$ ou $\mathbb{C}$), il existe une infinité de matrices A telles que $A^2 = I_2$.
Cela bien que l'équation $x^2 = 1$ ne possède que deux solutions dans $\mathbb{Q}$,$\mathbb{R}$ ou $\mathbb{C}$.
Cela est lié au fait que l'anneau $\mathscr{M}_2(\mathbb{K})$ n'est pas intègre. En effet on a :

$$\begin{aligned} A^2 = I_2 &\iff A^2 - I_2 = 0 \iff A^2 - I_2^2 = 0 \\ &\iff (A - I_2)(A + I_2) = 0, \text{ car } A \text{ et } I_2 \text{ commutent,} \end{aligned}$$

mais on ne peut pas avancer plus loin car les résultats que l'on voudrait utiliser ne sont pas vrais en général dans $\mathscr{M}_2(\mathbb{K})$.

2.4 Matrices inversibles

Définition 26
*Soient $\mathbb{K}$ un corps et $n \in \mathbb{N}^*$. Une matrice $A \in \mathscr{M}_n(\mathbb{K})$ est **inversible** \可逆的\ s'il existe une matrice B vérifiant :*

$$AB = BA = I_n.$$

Cela revient à dire que A possède un inverse pour la loi de multiplication matricielle sur $\mathscr{M}_n(\mathbb{K})$.
*L'ensemble des matrices inversibles de $\mathscr{M}_n(\mathbb{K})$ se note $\mathrm{GL}_n(\mathbb{K})$. On l'appelle le **groupe linéaire de** $\mathscr{M}_n(\mathbb{K})$ \域$\mathbb{K}$上的n阶一般线性群\.*

EXEMPLE 27 — *Pour $\lambda_1, \cdots, \lambda_n \in \mathbb{K}$ non-nuls, la matrice diagonale $A = \mathrm{Diag}(\lambda_1, \lambda_2, \cdots, \lambda_n)$ est inversible.*
En effet, pour $B = \mathrm{Diag}\left(\frac{1}{\lambda_1}, \frac{1}{\lambda_2}, \cdots, \frac{1}{\lambda_n}\right)$, on a

$$A\,B = B\,A = \mathrm{Diag}(1, 1, \cdots, 1) = I_n$$

En particulier, la matrice identité I_n est elle-même inversible.
Par contre, la matrice nulle 0 n'est pas inversible car pour tout matrice B on a $0.B = 0 \neq I_n$.

PROPOSITION 28
Soient $\mathbb{K}$ un corps et $n \in \mathbb{N}^*$. Soient $A, B \in \mathscr{M}_n(\mathbb{K})$ inversibles. Alors :

- ***L' inverse** de A est unique. On le note A^{-1} \矩阵A的逆或A的逆矩阵\ ;*
- *La matrice AB est inversible, et*
$$(AB)^{-1} = B^{-1}A^{-1}\ ;$$
(*Le passage à l'inverse renverse le produit matriciel.*)
- *La matrice A^{-1} est inversible, et $(A^{-1})^{-1} = A$;*

L'ensemble $(\mathrm{GL}_n(\mathbb{K}), \times)$ muni de la loi de multiplication matricielle est un groupe.

Preuve —
- Soient $C, D \in \mathscr{M}_n(\mathbb{K})$ tels que $AC = CA = I_n = AD = DA$.
On a alors $CAD = C(AD) = C\,I_n = C$ et $CAD = (CA)D = I_n\,D = D$, donc $C = D$.
- On a :
$$(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}I_nB = B^{-1}B = I_n$$
$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n.$$
Donc $(AB)^{-1} = B^{-1}A^{-1}$.
- On a : $AA^{-1} = A^{-1}A = I_n$, donc A^{-1} est inversible d'inverse A.

Les propriétés qui ont été montrées assurent que $(\mathrm{GL}_n(\mathbb{K}), \circ)$ est un groupe. Cette notion sera développée dans le cours Algèbre 2. □

REMARQUE 29 — *Calculer un produit de matrices (ex : A^2) s'effectue facilement avec des additions et des multiplications de nombres (n^2 fois (n produits et n produits)). Cela est facile à coder algorithmiquement. Par contre, calculer l'inverse d'une matrice A est moins évident. Avec la définition 26, on peut déterminer A^{-1} en résolvant le système de n^2 équations $(\mathcal{S})$: $BA = I_n$, où les n^2 inconnues sont les $(b_{i,j})_{i,j}$. Cela qui semble plus difficile et plus long. Il faut aussi savoir si une matrice A donnée est inversible ou non. Nous verrons des résultats et méthodes pour déterminer, parfois rapidement, si une matrice A est inversible et pour calculer A^{-1}.*

REMARQUE 30 — *Une matrice A est inversible si et seulement s'il existe B telle que $BA = AB = I_n$.*
Pour montrer qu'une matrice A est inversible, il y a ainsi deux égalités à vérifier ($AB = I_n$ et $BA = I_n$).
Si l'on trouve une matrice B telle que $AB = I_n$, on ne peut donc pas dire que A est inversible d'inverse B. Nous verrons par la suite que cette égalité est en réalité suffisante.

PROPOSITION 31
Soient $\mathbb{K}$ un corps et $n \in \mathbb{N}^*$. Soit $A \in \mathscr{M}_n(\mathbb{K})$. S'il existe $B \in \mathscr{M}_n(\mathbb{K})$ non-nulle telle que $AB = 0$, alors la matrice A n'est pas inversible.

Preuve — Si A était inversible, on aurait

$$A^{-1}(AB) = A^{-1}.0 = 0 \text{ et } A^{-1}(AB) = (A^{-1}A)B = I_n.B = B,$$

donc $B = 0$, ce qui est impossible car B est non-nulle. Donc A n'est pas inversible. □

COROLLAIRE 32
Soient $\mathbb{K}$ un corps et $n \in \mathbb{N}^*$. Soient $\lambda_1, \cdots, \lambda_n \in \mathbb{K}$. La matrice diagonale $A = \text{Diag}(\lambda_1, \cdots, \lambda_n)$ est inversible si et seulement si $\lambda_i \neq 0$, $\forall 1 \leq i \leq n$.

Preuve — Si tous les λ_i sont non-nuls, on a montré que A est inversible d'inverse $A^{-1} = \text{Diag}\left(\frac{1}{\lambda_1}, \frac{1}{\lambda_2}, \cdots, \frac{1}{\lambda_n}\right)$.
Supposons qu'il existe un indice j tel que $\lambda_j = 0$. Posons $B = \text{Diag}(\gamma_1 \cdots, \gamma_n)$ avec $\gamma_i = 0$ si $i \neq j$ et $\gamma_j = 1$. On a alors

$$A\,B = \text{Diag}(\lambda_1\gamma_1, \cdots, \lambda_n\gamma_n) = \text{Diag}(0, 0, \cdots, 0) = 0,$$

donc la matrice A n'est pas inversible d'après la proposition précédente. □

PROPOSITION 33
Soient $\mathbb{K}$ un corps et $n \in \mathbb{N}^*$. Soit $A \in \mathscr{M}_n(\mathbb{K})$ une matrice dont une ligne est nulle ou une colonne est nulle.
Alors A n'est pas inversible.

Preuve — Soit $1 \leq k \leq n$. On pose $A = (a_{i,j})_{i,j}$. Supposons que la k-ème ligne de A est nulle.
On pose $M = E_{k,k} \times A$. Comme toutes les lignes de $E_{k,k}$ sont nulles sauf la k-ème, alors M est une matrice dont toutes les lignes sont nulles sauf la k-ème.

De plus, par définition du produit matriciel, la k-ème ligne de M est égale à la k-ème ligne de A. Donc M est égale à la matrice nulle, c'est-à-dire : $E_{k,k} \times A = 0$.

D'après la Proposition 31, la matrice A n'est donc pas inversible.

On obtient le même résultat si la k-ème colonne de A est nulle en regardant $A \times E_{k,k}$. □

Matrices de taille 2×2 inversibles

EXERCICE 34 — *Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.*
Résoudre le système linéaire $(\mathcal{S})$ $BA = I_n$,
d'inconnue $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$.
Dans les cas où $(\mathcal{S})$ admet une solution B, calculer AB. Que trouve-t-on ?

PROPOSITION 35
Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathscr{M}_2(\mathbb{K})$.
La matrice A est inversible si et seulement si $ad - bc \neq 0$.
Si $ad - bc \neq 0$, on a :

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Preuve — Posons $B = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. On calcule :

$$AB = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} = (ad - bc)I_2$$

$$BA = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} da - bc & 0 \\ 0 & da - bc \end{pmatrix} = (ad - bc)I_2.$$

Donc, si $ad - bc \neq 0$, en posant $C = \frac{1}{ad-bc}B$, on a $AC = CA = I_2$. Donc A est inversible d'inverse C.
Supposons maintenant que $ad - bc = 0$. On a alors $AB = 0$. Si $A = 0$ alors A n'est pas inversible.
Si $A \neq 0$ alors l'un des coefficients a, b, c ou d est non-nul, donc la matrice B est elle aussi non-nulle. Comme on a $AB = 0$, la Proposition 31 nous dit alors que A n'est pas inversible. □

2.5 Système linéaire, matrice d'un système linéaire

Système linéaire

Soient n et p deux entiers naturels non nuls et $\mathbb{K}$ un corps. Un **système linéaire** \线性方程组\ de n équations à p inconnues s'écrit

$$(\mathscr{S}) \ : \ \left\{ \begin{array}{ccccccccccccc} a_{1,1}\,x_1 & + & a_{1,2}\,x_2 & + & \ldots & + & a_{1,j}\,x_j & + & \ldots & + & a_{1,p}\,x_p & = & b_1 \\ \vdots & & \vdots & + & \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ a_{i,1}\,x_1 & + & a_{i,2}\,x_2 & + & \ldots & + & a_{i,j}\,x_j & + & \ldots & + & a_{i,p}\,x_p & = & b_i \\ \vdots & & \vdots & + & \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ a_{n,1}\,x_1 & + & a_{n,2}\,x_2 & + & \ldots & + & a_{n,j}\,x_j & + & \ldots & + & a_{n,p}\,x_p & = & b_n \end{array} \right.$$

- Les p inconnues sont x_1, x_2,..., x_p. On appelle **une solution du système** \线性方程组的解\ toute p-liste $(x_1, x_2, \ldots, x_p) \in \mathbb{K}^p$ vérifiant les n équations de $(\mathscr{S})$.
- Les np scalaires $a_{i,j} \in \mathbb{K}$ sont les **coefficients** du système.
- La $n-$liste $(b_1, b_2, \ldots, b_n) \in \mathbb{K}^n$ est le **second membre** du système.
- Si $b_1 = b_2 = \cdots = b_n = 0$, alors on dit que le système est **homogène** \齐次线性方程组\, ou que le système est **sans second membre**.

La matrice $A = (a_{i,j})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}}$ s'appelle la **matrice du système linéaire** \系数矩阵\. Elle contient les coefficients du système linéaire. Comme le système linéaire s'écrit aussi :

$$(\mathscr{S}) \ : \ \sum_{j=1}^{p} a_{i,j}\,x_j = b_i \,, \forall i \in [\![1, n]\!]$$

on peut utiliser la matrice A pour réécrire le système linéaire sous la forme :

$$(\mathscr{S}) \ : \ A\,X = B$$

où

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_p \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

sont les matrices colonnes des inconnues et du second membre.

Nous allons présenter une méthode pour résoudre n'importe quel système linéaire $AX = Y$.
Nous commencerons par résoudre des systèmes linéaires simples (les systèmes échelonnés), puis nous verrons une méthode pour se ramener à un système linéaire échelonné (la méthode du Pivot).

Matrices échelonnées

Définition 36
Soient $\mathbb{K}$ un corps et $n, p \in \mathbb{N}^*$. Soit $A \in \mathscr{M}_{n,p}(\mathbb{K})$, avec $A = (a_{i,j})_{i,j}$.
Soit $1 \leq i \leq n$. Si la i-ème ligne de A est non-nulle, on définit $\alpha_i = \inf(\{1 \leq k \leq p \text{ tels que } a_{i,k} \neq 0\})$.

Pour L_i la i-ème ligne de A, si L_i est non-nulle on a : $L_i = (0, 0, \ldots, 0, a_{i,\alpha_i}, *, *)$.

Si la k-ème ligne de A est nulle, on pose alors $\alpha_i = p + i$.

*On dit alors que la matrice A est **échelonnée** si l'on a :*

$$\alpha_1 < \alpha_2 < \ldots < \alpha_n.$$

EXEMPLE 37 — $A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$ *est échelonnée.* $B = \begin{pmatrix} 0 & 2 & 3 \\ 1 & 0 & 2 \\ 0 & 2 & 0 \end{pmatrix}$ *n'est pas échelonnée.*

$C = \begin{pmatrix} 1 & 2 & 3 & 1 \\ 0 & 2 & 2 & -1 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ *n'est pas échelonnée.* $D = \begin{pmatrix} 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$, *on a* $\alpha_1 = 3$, $\alpha_2 = 4$, $\alpha_3 = 7$, $\alpha_4 = 8$ *est échelonnée.*

Pour $E = 0_{\mathscr{M}_{n,p}(\mathbb{K})}$ *on a* $\alpha_1 = p+1$,$\alpha_2 = p+2$,$\ldots$, $\alpha_n = p+n$. *La matrice nulle est échelonnée.*

Pour $F \in \mathscr{M}_n(\mathbb{K})$ *une matrice diagonale dont les coefficients diagonaux sont non-nuls,* F *est échelonnée.*

REMARQUE 38 — *On dit que le système linéaire* $(\mathcal{S})$ *:* $AX = Y$, *où* $X, Y \in \mathscr{M}_{p,1}(\mathbb{K})$ *et* $A \in \mathscr{M}_{n,p}(\mathbb{K})$ *est échelonné si la matrice* A *est échelonnée.*

REMARQUE 39 — *Soit* $A \in \mathscr{M}_n(\mathbb{K})$ *une matrice échelonnée. Comme on a*

$$1 \leq \alpha_1 < \alpha_2 < \ldots < \alpha_n,$$

on remarque en particulier que A *est une matrice triangulaire supérieure.*

Les matrices carrées échelonnées sont un cas particulier de matrices triangulaires supérieures.

Résolution d'un système échelonné

PROPOSITION 40 (Résolution d'un système linéaire échelonné)
Soient $\mathbb{K}$ *un corps,* $n, p \in \mathbb{N}^*$. *Soit* $A \in \mathscr{M}_{n,p}(\mathbb{K})$ *une matrice échelonnée. Soient* $(y_1, \ldots, y_p) \in \mathbb{K}^p$.
Alors, on peut toujours résoudre le système $(\mathcal{S})$ *:* $AX = Y$.

REMARQUE 41 — *On détermine les solutions* $(x_1, \ldots, x_p)$ *du système échelonné* $(\mathcal{S})$ *:* $AX = Y$ *en remontant ligne par ligne :*

Soit r *le numéro de la dernière ligne non-nulle de* A.
Comme A *est échelonnée, les lignes* $r+1, \ldots, n$ *sont nulles, et les lignes* $1, \ldots, r$ *sont non-nulles.*

• *Toutes les lignes nulles de la matrice* A *donnent des équations de la forme :* $0 = y_j$, *pour* $r+1 \leq j \leq n$.
- Si l'un de ces y_j *est non-nul, alors le système* $(\mathcal{S})$ *n'a pas de solutions, et la résolution est terminée.*
- Si tous les y_j *sont nuls pour* $r+1 \leq j \leq n$, *alors ces équations sont de la forme :* $0 = 0$.
On retire ces équations du système (équations toujours vraies), et on continue la résolution.

• *Pour tout* $1 \leq i \leq r$, *on a* $a_{i,\alpha_i} \neq 0$.
Pour chaque ligne L_i, *on exprime* x_{α_i} *en fonction de* b_i, *et* $x_{\alpha_i+1}, \ldots, x_p$.

• *Ligne* r *: Le coefficient* x_{α_r} *est alors déterminé.*

• *Ligne* $r-1$ *: On remplace* x_{α_r} *par l'expression à la ligne* r. *Le coefficient* $x_{\alpha_{r-1}}$ *est alors déterminé.*

• *Ligne* $r-2$ *: On remplace* $x_{\alpha_r}, x_{\alpha_{r-1}}$ *par leurs expressions. Le coefficient* $x_{\alpha_{r-2}}$ *est alors déterminé.*

• $\ldots$

• *Ligne* 1 *: On remplace* $x_{\alpha_r}, \ldots, x_{\alpha_2}$ *par leurs expressions. Le coefficient* x_{α_1} *est alors déterminé.*

On obtient alors les valeurs de $x_{\alpha_1}, \ldots, x_{\alpha_r}$ *en fonction de* $y_1, \ldots, y_r$ *ainsi que des* x_j *pour* $j \neq \alpha_1, \ldots, \alpha_r$.

EXEMPLE 42 — *Résolution dans* $\mathbb{R}$ *du système linéaire :*

$$(\mathcal{S}) : \begin{cases} x_1 + x_2 + 2x_3 = 3 \\ 0 + 2x_2 + 2x_3 = 4 \\ 0 + 0 - x_3 = 3 \\ 0 + 0 + 0 = 0 \end{cases}$$

La matrice A associée à ce système linéaire est échelonnée. Elle possède une ligne nulle.

On a ainsi :

$$(\mathcal{S}) \Longleftrightarrow \left\{ \begin{array}{rl} x_1 & = 3 - x_2 - 2x_3 \\ x_2 & = 2 - x_3 \\ x_3 & = -3 \\ 0 & = 0 \end{array} \right. \Longleftrightarrow \left\{ \begin{array}{rl} x_1 & = 3 - 5 - 2(-3) = 4 \\ x_2 & = 5 \\ x_3 & = -3 \end{array} \right.$$

L'ensemble des solutions de $(\mathcal{S})$ est donc $\{(4, 5, 3)\}$. Ce système linéaire possède une unique solution.

EXEMPLE 43 — *Résolution dans $\mathbb{R}$ du système linéaire d'équations :*

$$(\mathcal{S}) : \left\{ \begin{array}{rcrcrcrcl} x_1 & + & 3x_2 & - & 2x_3 & + & 5x_4 & = & -1 \\ 0 & + & 2x_2 & + & 2x_3 & - & 2x_4 & = & 4 \end{array} \right.$$

On remarque que la matrice A associée à ce système linéaire est échelonnée. On a :

$$(\mathcal{S}) \Leftrightarrow \left\{ \begin{array}{rl} x_1 & = -1 - 3x_2 + 2x_3 - 5x_4 \\ x_2 & = 2 - x_3 + x_4 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rl} x_1 & = -1 - 3(2 - x_3 + x_4) + 2x_3 - 5x_4 = -7 + 5x_3 - 8x_4 \\ x_2 & = 2 - x_3 + x_4 \end{array} \right.$$

L'ensemble des solutions de $(\mathcal{S})$ est donc :

$$\begin{aligned} S &= \{(-7 + 5x_3 - 8x_4, 2 - x_3 + x_4, x_3, x_4),\ x_3, x_4 \in \mathbb{R}\} \\ &= \{(-7, 2, 0, 0) + (5x_3, -x_3, x_3, 0) + (-8x_4, x_4, 0, x_4),\ x_3, x_4 \in \mathbb{R}\} \\ &= (-7, 2, 0, 0) + Vect((5, -1, 1, 0), (-8, 1, 0, 1)). \end{aligned}$$

Ce système linéaire possède une infinité de solutions.

EXEMPLE 44 — *Résoudre dans, selon $(y_1, y_2, y_3, y_4) \in \mathbb{R}^4$, le système linéaire d'équations :*

$$(\mathcal{S}) : \left\{ \begin{array}{rcrcrcrcl} x_1 & + & 2x_2 & + & x_3 & - & x_4 & = & y_1 \\ 0 & - & x_2 & + & x_3 & + & 0 & = & y_2 \\ 0 & + & 0 & + & 2x_3 & + & 6x_4 & = & y_3 \\ 0 & + & 0 & + & 0 & + & 0 & = & y_4 \end{array} \right.$$

On remarque que la matrice A associée à ce système linéaire est échelonnée.
• *La quatrième ligne du système est $0 = y_4$.*
- *Si $y_4 \neq 0$, ce système n'a pas de solutions ($S = \emptyset$).*

- *Si $y_4 = 0$, on poursuit la résolution. On a :*

$$(\mathcal{S}) \Longleftrightarrow \left\{ \begin{array}{rl} x_1 & = y_1 - 2x_2 - x_3 + x_4 \\ x_2 & = -y_2 + x_3 \\ x_3 & = \frac{1}{2}y_3 - 3x_4 \\ 0 & = 0 \end{array} \right. \Longleftrightarrow \left\{ \begin{array}{rl} x_1 & = y_1 - 2x_2 - x_3 + x_4 \\ x_2 & = -y_2 + \frac{1}{2}y_3 - 3x_4 \\ x_3 & = \frac{1}{2}y_3 - 3x_4 \end{array} \right.$$

$$(\mathcal{S}) \Longleftrightarrow \left\{ \begin{array}{rl} x_1 & = y_1 - 2(-y_2 + \frac{1}{2}y_3 - 3x_4) - (\frac{1}{2}y_3 - 3x_4) + x_4 = y_1 + 2y_2 - \frac{3}{2}y_3 + 10x_4 \\ x_2 & = -y_2 + \frac{1}{2}y_3 - 3x_4 \\ x_3 & = \frac{1}{2}y_3 - 3x_4 \end{array} \right.$$

L'ensemble des solutions de $(\mathcal{S})$ est donc :

$$\begin{aligned} S &= \{(y_1 + 2y_2 - \frac{3}{2}y_3 + 10x_4, -y_2 + \frac{1}{2}y_3 - 3x_4, \frac{1}{2}y_3 - 3x_4, x_4),\ x_4 \in \mathbb{R}\} \\ &= (y_1 + 2y_2 - \frac{3}{2}y_3, -y_2 + \frac{1}{2}y_3, \frac{1}{2}y_3, 0) + Vect((10, -3, -3, 1)). \end{aligned}$$

En conclusion, si $y_4 \neq 0$ ce système linéaire n'admet pas de solutions. Si $y_4 = 0$, alors ce système linéaire possède une infinité de solutions, décrites au-dessus.

2.6 Méthode du Pivot

La méthode du Pivot permet de transformer toute matrice en une matrice échelonnée, en la multipliant par des matrices inversibles.

Matrices élémentaires

Définition 45
Soient $\mathbb{K}$ un corps, $n \in \mathbb{N}^*$. Soient $1 \leq i, j \leq n$, $i \neq j$ et $\lambda \in \mathbb{K}$.
*On définit les matrices suivantes, appelées **matrices élémentaires** :*

- $E(i,j,\lambda) = I_n + \lambda.E_{i,j}$;
- $M(i,\lambda) = I_n - E_{i,i} + \lambda.E_{i,i}$;
- $S(i,j) = I_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$.

Exemple 46 — *Dans $\mathscr{M}_3(\mathbb{K})$, on a :*
$E(1,3,\lambda) = \begin{pmatrix} 1 & 0 & \lambda \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $M(2,\lambda) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & 1 \end{pmatrix}$, *et* $S(1,3) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$.

La matrice $E(i,j,\lambda)$ est la matrice identité pour laquelle on a ajouté λ en (i,j).

La matrice $M(i,\lambda)$ est une matrice diagonale, qui vaut λ en (i,i), et 1 sur le reste la diagonale.

La matrice $S(i,j)$ est la matrice identité pour laquelle on a déplacé les coefficients (i,i) et (j,j) (en (i,j) et (j,i)).

Proposition 47
Soient $\mathbb{K}$ un corps, $n,p \in \mathbb{N}^*$. Soient $1 \leq i, j \leq n$, $i \neq j$ et $\lambda \in \mathbb{K}$. Soit $A \in \mathscr{M}_{n,p}(\mathbb{K})$. Alors :

- *$E(i,j,\lambda)$ est inversible.*
  L'opération $A \mapsto E(i,j,\lambda)A$ revient à effectuer : Ligne i devient (Ligne i+λ.Ligne j).
  On note $L_i \leftarrow L_i + \lambda.L_j$ cette opération.
- *$M(i,\lambda)$ est inversible si $\lambda \neq 0$.*
  L'opération $A \mapsto M(i,\lambda)A$ revient à effectuer : Ligne i devient λ.Ligne i.
  On note $L_i \leftarrow \lambda.L_i$ cette opération.
- *$S(i,j)$ est inversible.*
  L'opération $A \mapsto S(i,j)A$ revient à effectuer : Ligne i devient Ligne j, et Ligne j devient Ligne i.
  On note $L_i \leftrightarrow L_j$ cette opération.

Preuve — On rappelle que $E_{i,j} \times E_{k,l} = \delta_{j,k}\, E_{i,l}$.

- Le calcul donne : $E(i,j,\lambda) \times E(i,j,-\lambda) = (I_n + \lambda.E_{i,j})(I_n - \lambda.E_{i,j}) = I_n - \lambda^2 E_{i,j}^2 = I_n$.
  En prenant $\gamma = -\lambda$, on a aussi : $E(i,j,-\lambda) \times E(i,j,\lambda) = I_n$.
  La forme de la matrice $E(i,j,\lambda)$ et la définition du produit matriciel impliquent que l'opération $A \mapsto E(i,j,\lambda)A$ revient à ajouter à la Ligne i de A la quantité λ.(Ligne j).
- Soit $\lambda \neq 0$. Le calcul donne : $M(i,\lambda) \times M(i,\frac{1}{\lambda}) = I_n = M(i,\frac{1}{\lambda}) \times M(i,\lambda)$.
  La forme de la matrice $M(i,\lambda)$ et la définition du produit matriciel impliquent que l'opération $A \mapsto M(i,\lambda)A$ revient à multiplier la Ligne i de A par λ.
- Le calcul donne : $S(i,j) \times S(i,j) = I_n$.
  La forme de la matrice $S(i,j)$ et la définition du produit matriciel impliquent que l'opération $A \mapsto S(i,j)A$ revient à échanger la Ligne i et la Ligne j.

□

Théorème 48
Soient $\mathbb{K}$ un corps, $n,p \in \mathbb{N}^*$. Soit $A \in \mathscr{M}_{n,p}(\mathbb{K})$.
Alors il existe $B \in \mathscr{M}_{n,p}(\mathbb{K})$ une matrice échelonnée, et $M_1, \ldots, M_r$ des matrices élémentaires de $\mathscr{M}_n(\mathbb{K})$ telles que :

$$M_1 \times \ldots \times M_r \times A = B.$$

Autrement dit, il est possible de transformer la matrice A en une matrice échelonnée B en un nombre fini d'opérations élémentaires.

REMARQUE 49 — *Soient $X, Y \in \mathscr{M}_{p,1}(\mathbb{K})$ des vecteurs colonne. Comme les matrices élémentaires sont inversibles, on a :*

$$AX = Y \iff (M_1 \dots M_r A)X = M_1 \dots M_r Y \iff BX = Y'.$$

En possédant une méthode pour trouver de telles matrices élémentaires $M_1, \dots, M_r$, on peut alors résoudre tout système linéaire $AX = Y$ en se ramenant à un système linéaire échelonné $BX = Y'$.

Méthode du Pivot

REMARQUE 50 (Méthode du Pivot) — *Soit $A \in \mathscr{M}_{n,p}(\mathbb{K})$.*
On échelonne la matrice A en utilisant les opérations élémentaires.
On procède colonne par colonne, de la gauche vers la droite.
On rappelle que pour $1 \leq i \leq n$, l'entier α_i désigne la position du coefficient non-nul de la ligne L_i le plus à gauche (et $\alpha_i = n + i$ si la ligne L_i est nulle).

- *Pour L_i et L_j deux lignes telles que $\alpha_i < \alpha_j$ mais $i > j$, l'opération $L_i \leftrightarrow L_j$ permute les lignes L_i et L_j :*

$$\begin{cases} L_j : (0, 0, \dots, 0, 0, \dots, 0, a_{i,\alpha_i}, *, \dots, *) \\ L_i : (0, 0, \dots, 0, a_{i,\alpha_j}, *, \dots, *, *, \dots, *) \end{cases} \xrightarrow[L_i \leftrightarrow L_j]{} \begin{cases} L_j : (0, 0, \dots, 0, a_{i,\alpha_j}, *, \dots, *, *, \dots, *) \\ L_i : (0, 0, \dots, 0, 0, \dots, 0, a_{i,\alpha_i}, *, \dots, *) \end{cases}$$

- *Pour a_{i,α_i} le coefficient non-nul le plus à gauche de L_i, l'opération $L_i \leftarrow \frac{1}{a_{i,\alpha_i}} L_i$ change ce coefficient en un 1 (utile pour certains calculs).*

$$L_i : (0, 0, \dots, 0, a_{i,\alpha_i}, *, \dots, *) \xrightarrow[L_i \leftarrow \frac{1}{a_{i,\alpha_i}} L_i]{} L_i : (0, 0, \dots, 0, 1, *, \dots, *).$$

- *Pour L_i et L_j deux lignes telles que $\alpha_i = \alpha_j$, avec $j < i$, l'opération $L_i \leftarrow L_i + \frac{-a_{i,\alpha_i}}{a_{j,\alpha_j}} L_j$ annule le coefficient a_{i,α_i} et préserve les 0 situés avant :*

$$\begin{cases} L_j : (0, 0, \dots, 0, a_{j,\alpha_j}, *, \dots, *) \\ L_i : (0, 0, \dots, 0, a_{i,\alpha_j}, *, \dots, *) \end{cases} \xrightarrow[L_i \leftarrow L_i + \frac{-a_{i,\alpha_i}}{a_{j,\alpha_j}} L_j]{} \begin{cases} L_j : (0, 0, \dots, 0, a_{j,\alpha_j}, *, \dots, *) \\ L_i : (0, 0, \dots, 0, 0, *, \dots, *) \end{cases}$$

Voyons cela sur des exemples (échelonnage de matrice, résolution d'un système linéaire).

EXEMPLE 51 — *Appliquer la méthode du Pivot sur* $A = \begin{pmatrix} 1 & 2 & 0 & 3 \\ -1 & 1 & 1 & 0 \\ 2 & 1 & 7 & 1 \end{pmatrix}$.

On a : $\begin{pmatrix} 1 & 2 & 0 & 3 \\ -1 & 1 & 1 & 0 \\ 2 & 1 & 7 & 1 \end{pmatrix} \xrightarrow[L_3 \leftarrow L_3 - 2L_1]{L_2 \leftarrow L_2 + L_1} \begin{pmatrix} 1 & 2 & 0 & 3 \\ 0 & 3 & 1 & 3 \\ 0 & -3 & 7 & -5 \end{pmatrix} \xrightarrow[L_3 \leftarrow L_3 + 3L_2]{L_2 \leftarrow \frac{1}{3} L_2} \begin{pmatrix} 1 & 2 & 0 & 3 \\ 0 & 1 & \frac{1}{3} & 1 \\ 0 & 0 & 8 & -2 \end{pmatrix}$.
On a bien obtenu une matrice échelonnée.
Pour B cette matrice échelonnée, les opérations effectuées donnent :

$$E(3, 2, 3)M(2, \frac{1}{3})E(3, 1, -2)E(1, 2, 1)A = B.$$

EXEMPLE 52 — *Appliquer la méthode du Pivot sur* $A = \begin{pmatrix} 0 & 2 & 1 \\ 2 & 2 & 1 \\ 1 & 4 & 3 \end{pmatrix}$.

On a : $\begin{pmatrix} 0 & 2 & 1 \\ 2 & 2 & 1 \\ 1 & 4 & 3 \end{pmatrix} \xrightarrow[L_1 \leftrightarrow L_3]{} \begin{pmatrix} 1 & 4 & 3 \\ 2 & 2 & 1 \\ 0 & 2 & 1 \end{pmatrix} \xrightarrow[L_2 \leftarrow L_2 - 2L_1]{} \begin{pmatrix} 1 & 4 & 3 \\ 0 & -6 & -5 \\ 0 & 2 & 1 \end{pmatrix}$.

$$\begin{pmatrix}1 & 4 & 3\\ 0 & -6 & -5\\ 0 & 2 & 1\end{pmatrix} \quad \begin{matrix}\longrightarrow\\ L_2 \leftarrow \frac{1}{-6}L_2\\ L_3 \leftarrow L_3 - 2L_2\end{matrix} \quad \begin{pmatrix}1 & 4 & 3\\ 0 & 1 & \frac{5}{6}\\ 0 & 0 & \frac{-2}{3}\end{pmatrix}.$$

On a bien obtenu une matrice échelonnée. Pour B cette matrice échelonnée, les opérations effectuées donnent : $E(3,2,-2)M(2,\frac{-1}{6})E(2,1,-2)S(1,3)A = B$.

Si l'on avait effectué $L_1 \leftrightarrow L_2$ dans l'exemple précédent, on aurait obtenu une matrice échelonnée différente. Cela ne dérange pas.

Exemple 53 (Résolution d'un système linéaire avec la méthode du Pivot) —
Résoudre le système linéaire : $(\mathcal{S}) : \begin{cases} x_1 + 4x_2 - 5x_3 = 1\\ 2x_1 - 2x_2 + x_3 = 0\\ 3x_1 - x_2 - x_3 = 1\end{cases}$.

On utilise la méthode du Pivot :

$$\begin{matrix}\\ (\mathcal{S})\\ \\ \end{matrix} \begin{matrix}\iff\\ L_2 \leftarrow L_2 - 2L_1\\ L_3 \leftarrow L_3 - 3L_1\end{matrix} \begin{cases} x_1 + 4x_2 - 5x_3 = 1\\ 0 - 10x_2 + 11x_3 = -2\\ 0 - 9x_2 + 14x_3 = -2\end{cases}$$

$$\begin{matrix}\\ (\mathcal{S})\\ \\ \end{matrix} \begin{matrix}\iff\\ L_2 \leftarrow \frac{1}{-10}L_2\\ L_3 \leftarrow L_3 + 9L_2\end{matrix} \begin{cases} x_1 + 4x_2 - 5x_3 = 1\\ 0 + x_2 + \frac{-11}{10}x_3 = \frac{1}{5}\\ 0 + 0 + (14 + \frac{-99}{10})x_3 = -2 + \frac{9}{5}\end{cases} \quad (\textit{système échelonné})$$

$$(\mathcal{S}) \iff \begin{cases} x_1 + 4x_2 - 5x_3 = 1\\ 0 + x_2 + \frac{-11}{10}x_3 = \frac{1}{5}\\ 0 + 0 + \frac{41}{10}x_3 = \frac{-1}{5}\end{cases} \iff \begin{cases} x_1 = 1 - 4x_2 + 5x_3\\ x_2 = \frac{1}{5} + \frac{11}{10}x_3\\ x_3 = \frac{-10}{5.41} = \frac{-2}{41}\end{cases}$$

$$(\mathcal{S}) \iff \begin{cases} x_1 = 1 - 4x_2 + 5x_3\\ x_2 = \frac{1}{5} + \frac{11}{10}\frac{-2}{41} = \frac{60}{410} = \frac{6}{41}\\ x_3 = \frac{-2}{41}\end{cases} \iff \begin{cases} x_1 = 1 - 4\frac{6}{41} + 5\frac{-2}{41} = \frac{7}{41}\\ x_2 = \frac{6}{41}\\ x_3 = \frac{-2}{41}\end{cases}$$

L'ensemble des solutions de $(\mathcal{S})$ est $\{(\frac{7}{41}, \frac{6}{41}, \frac{-2}{41})\}$.

Calcul de l'inverse d'une matrice avec la méthode du Pivot

Pour $A \in \mathscr{M}_n(\mathbb{K})$ une matrice carrée, la méthode du Pivot peut être utilisée pour déterminer si A est inversible ou non, et pour calculer A^{-1}.

Proposition 54
Soient $\mathbb{K}$ un corps, $n \in \mathbb{N}^*$. Soit $A \in \mathscr{M}_n(\mathbb{K})$.
Si, en appliquant la méthode du Pivot à A, on obtient à une étape une matrice dont une ligne est nulle, alors A n'est pas inversible.
Si, en appliquant la méthode du Pivot à A, on obtient une matrice échelonnée sans ligne nulle, alors A est inversible.

Preuve — La méthode du Pivot revient à multiplier A à gauche par des matrices inversibles $M_1, \dots, M_r$. Comme $(M_1 \dots M_r)$ est inversible, la matrice A est inversible si et seulement si $(M_1 \dots M_r)A$ est inversible. Et la Proposition 33 nous dit qu'une matrice possédant une ligne nulle n'est pas inversible.
Enfin, soit B une matrice carrée qui est échelonnée et sans ligne nulle. Alors on doit avoir $\alpha_i = i$ pour tout $1 \leq i \leq n$. Ainsi, B est une matrice triangulaire supérieure dont les coefficients diagonaux sont non-nuls. Une telle matrice est inversible. □

Exemple 55 — *La matrice* $A = \begin{pmatrix}1 & 2 & 1\\ -4 & 3 & 2\\ -3 & 5 & 3\end{pmatrix}$ *est-elle inversible ?*

On applique la méthode du Pivot à A :

$$\begin{pmatrix}1&2&1\\-4&3&2\\-3&5&3\end{pmatrix} \begin{array}{c}\longrightarrow\\ L_2\leftarrow L_2+4L_1\\ L_3\leftarrow L_3+3L_1\end{array} \begin{pmatrix}1&2&1\\0&11&6\\0&11&6\end{pmatrix} \begin{array}{c}\longrightarrow\\ L_3\leftarrow L_3-L_2\end{array} \begin{pmatrix}1&2&1\\0&11&6\\0&0&0\end{pmatrix}$$

On a obtenu une matrice avec la ligne nulle pendant la méthode du Pivot. Donc A n'est pas inversible.

Remarque 56 — *Soit $A\in\mathscr{M}_n(\mathbb{K})$. S'il existe des matrices élémentaires $M_1,\dots,M_r$ telles que $M_1\dots M_rA=I_n$, alors on a $A=(M_1\dots M_r)^{-1}$. Donc A est inversible et $M_1\dots M_r=A^{-1}$.*

Proposition 57
Soient $\mathbb{K}$ un corps, $n\in\mathbb{N}^*$. Soit $A\in\mathscr{M}_n(\mathbb{K})$.
On pose $B=(A\mid I_n)\in\mathscr{M}_{n,2n}(\mathbb{K})$, la matrice obtenue en "collant" les matrices A et I_n. C'est-à-dire :

$$B=\begin{pmatrix}a_{1,1}&\dots&a_{1,n}&1&0&\dots&0\\a_{2,1}&\dots&a_{2,n}&0&1&\dots&0\\\vdots&&\vdots&\vdots&&\ddots&\vdots\\a_{n,1}&\dots&a_{n,n}&0&0&\dots&1\end{pmatrix}.$$

Si, en appliquant la méthode du Pivot à B, on obtient une matrice de la forme $(I_n\mid M)$, alors on a $M=A^{-1}$.

Preuve — Appliquer la méthode du Pivot à la matrice B de taille $n\times 2n$ revient à multiplier B à gauche par des matrices élémentaires $M_1,\dots,M_r$ de taille $n\times n$.
Or, les propriétés de la multiplication matricielle nous donnent :

$$M_r\dots M_1\cdot B=M_r\dots M_1\cdot(A\mid I_n)=((M_r\dots M_1)\cdot A\mid M_r\dots M_1).$$

Donc, si $M_r\dots M_1\cdot B=(I_n\mid M)$, on a $(M_r\dots M_1)\cdot A=I_n$ et $M=Mr\dots M_1$.

Comme la matrice $M_r\dots M_1$ est inversible, on en déduit que $A=(M_r\dots M_1)^{-1}$. Donc, A est inversible et $A^{-1}=(M_r\dots M_1)=M$. □

Exemple 58 — *Montrer que la matrice $A=\begin{pmatrix}1&2&1\\-4&3&2\\1&5&3\end{pmatrix}$ est inversible, et calculer son inverse.*

On applique la méthode du Pivot à la matrice $B=(A\mid I_3)$:

$$\begin{pmatrix}1&2&1&1&0&0\\-4&3&2&0&1&0\\1&5&3&0&0&1\end{pmatrix} \begin{array}{c}\longrightarrow\\ L_2\leftarrow L_2+4L_1\\ L_3\leftarrow L_3-L_1\end{array} \begin{pmatrix}1&2&1&1&0&0\\0&11&6&4&1&0\\0&3&2&-1&0&1\end{pmatrix}$$

$$\begin{array}{c}\longrightarrow\\ L_2\leftarrow \frac{1}{11}L_2\\ L_3\leftarrow L_3-3L_2\end{array} \begin{pmatrix}1&2&1&1&0&0\\0&1&\frac{6}{11}&\frac{4}{11}&\frac{1}{11}&0\\0&0&\frac{4}{11}&\frac{-23}{11}&\frac{-3}{11}&1\end{pmatrix} \begin{array}{c}\longrightarrow\\ L_3\leftarrow \frac{11}{4}L_3\\ L_2\leftarrow L_2-\frac{6}{11}L_2\\ L_1\leftarrow L_1-L_3\end{array} \begin{pmatrix}1&2&0&\frac{27}{4}&\frac{3}{4}&\frac{-11}{4}\\0&1&0&\frac{4}{11}+\frac{23.6}{4.11}&\frac{1}{11}+\frac{3.6}{4.11}&\frac{-6}{4}\\0&0&1&\frac{-23}{4}&\frac{-3}{4}&\frac{11}{4}\end{pmatrix}$$

$$=\begin{pmatrix}1&2&0&\frac{27}{4}&\frac{3}{4}&\frac{-11}{4}\\0&1&0&\frac{7}{2}&\frac{1}{2}&\frac{-3}{2}\\0&0&1&\frac{-23}{4}&\frac{-3}{4}&\frac{11}{4}\end{pmatrix} \begin{array}{c}\longrightarrow\\ L_1\leftarrow L_1-2L_2\end{array} \begin{pmatrix}1&0&0&\frac{-1}{4}&\frac{-1}{4}&\frac{1}{4}\\0&1&0&\frac{7}{2}&\frac{1}{2}&\frac{-3}{2}\\0&0&1&\frac{-23}{4}&\frac{-3}{4}&\frac{11}{4}\end{pmatrix}$$

On a obtenu une matrice de la forme $(I_3\mid M)$. Donc A est inversible et $A^{-1}=M$, avec :

$$A^{-1}=\frac{1}{4}\begin{pmatrix}-1&-1&1\\14&2&-6\\-23&-3&11\end{pmatrix}.$$

PROPOSITION 59
Soient $\mathbb{K}$ un corps, $n \in \mathbb{N}^*$. Soit $A \in \mathscr{M}_n(\mathbb{K})$. Soit $1 \leq j \leq n$. On suppose qu'il existe $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ tels que la ligne L_j de A soit combinaison linéaire des lignes $L_1, \ldots, L_n$ (sauf L_j) :

$$L_j = \sum_{i=0,\, i\neq j}^{n} \lambda_i L_i.$$

Alors la matrice A n'est pas inversible.

Preuve — Supposons avoir $L_j = \sum_{i=0,\, i\neq j}^{n} \lambda_i L_i$. On applique à A la suite d'opérations élémentaires : $L_j \leftarrow L_j - \lambda_i L_i$, pour $1 \leq i \leq n$, $i \neq j$. Ces opérations ne changent que la ligne L_j.
Après ces $n-1$ opérations, la ligne L_j est devenue : $L_j = \sum_{i=0,\, i\neq j}^{n} \lambda_i L_i - (\sum_{i=0,\, i\neq j}^{n} \lambda_i L_i) = 0$.

La matrice obtenue est donc une matrice avec une ligne nulle. Cette matrice n'est pas inversible d'après la Proposition 33.
Donc, la matrice A n'est pas inversible. □

EXEMPLE 60 — *Soit $n \in \mathbb{N}^*$. On pose $A = (a_{i,j})_{i,j} \in \mathscr{M}_n(\mathbb{R})$ avec $a_{i,i} = -(n-1)$ et $a_{i,j} = 1$ si $i \neq j$.*

On remarque que la somme des lignes de A vaut :

$$L_1 + \ldots + L_n = (n-1-(n-1),\, n-1-(n-1),\, \ldots,\, n-1-(n-1)) = (0,\, 0,\, \ldots,\, 0).$$

On a donc $L_n = -L_1 - L_2 - \ldots - L_{n-1}$.
La proposition précédente nous dit alors que A n'est pas inversible.

2.7 TRANSPOSÉE D'UNE MATRICE

DÉFINITION 61
Soient $\mathbb{K}$ un corps et $p, q \in \mathbb{N}^*$. Soit $A \in \mathscr{M}_{p,q}(\mathbb{K})$.
*On définit la **transposée** \转置\ de A, notée ${}^tA$, par $b_{i,j} = a_{j,i}$, $\forall 1 \leq i \leq p, 1 \leq j \leq q$.*

EXEMPLE 62 — *Pour $A = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$, on a ${}^tA = \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}$.*

Pour $B = \begin{pmatrix} a_1 & a_2 & \ldots & a_p \\ 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \end{pmatrix} \in \mathscr{M}_{3,p}(\mathbb{K})$, on a ${}^tB = \begin{pmatrix} a_1 & 0 & 0 \\ a_2 & 0 & 0 \\ \vdots & & \vdots \\ a_p & 0 & 0 \end{pmatrix} \in \mathscr{M}_{p,3}(\mathbb{K})$.

REMARQUES 63
1. *Transposer une matrice transforme ses lignes en colonnes (et ses colonnes en lignes).*
2. *La transposée d'une matrice ligne est une matrice colonne.*
   La transposée d'une matrice carrée est une matrice carrée.
   La transposée d'une matrice triangulaire supérieure est une matrice triangulaire inférieure.
3. *Soit $A \in \mathscr{M}_n(\mathbb{K})$ une matrice carrée. Alors les matrices carrées A et ${}^tA$:*
   (a) *ont la même diagonale ;*
   (b) *sont les symétriques l'une de l'autre par rapport à la diagonale.*

PROPOSITION 64
Pour $A, B \in \mathscr{M}_{p,q}(\mathbb{K})$ et $\lambda \in \mathbb{K}$ un scalaire, on a :

$${}^t({}^tA) = A \qquad et \qquad {}^t(\lambda A) = \lambda\, {}^tA \qquad et \qquad {}^t(A+B) = {}^tA + {}^tB.$$

PROPOSITION 65
Soient $\mathbb{K}$ un corps et $p,q,r \in \mathbb{N}^*$. Soient $A \in \mathscr{M}_{p,q}(\mathbb{K})$ et $B \in \mathscr{M}_{q,r}(\mathbb{K})$. On a :

$$^t(A\,B) = {}^tB\,{}^tA.$$

La transposition renverse l'ordre du produit matriciel.

Preuve — Soient $A = (a_{i,j})_{(i,j)}$ et $B = (b_{j,k})_{(j,k)}$.

La matrice $C = A\,B$ possède p lignes et r colonnes, donc $C' = {}^t(A\,B)$ possède r lignes et p colonnes. On a :

$$c'_{k,i} = c_{i,k} = \sum_{j=1}^{q} a_{i,j}\,b_{j,k}.$$

Comme $A' = {}^tA \in \mathscr{M}_{q,p}(\mathbb{K})$ et $B' = {}^tB \in \mathscr{M}_{r,q}(\mathbb{K})$, le produit $D = {}^tB\,{}^tA$ existe et possède lui aussi r lignes et p colonnes. La relation :

$$d_{k,i} = \sum_{j=1}^{q} b'_{k,j}\,a'_{j,i} = \sum_{j=1}^{q} b_{j,k}\,a_{i,j} = c'_{k,i}$$

prouve que les matrices ${}^tB{}^tA$ et ${}^t(A\,B)$ ont tous leurs coefficients égaux, donc qu'elles sont égales. □

EXERCICE 66 — *1. Soit A une matrice inversible.*
Montrer que sa transposée est inversible et que ${}^t\left(A^{-1}\right) = ({}^tA)^{-1}$.
2. Soit B une matrice dont la colonne C_j est combinaison linéaire des C_i, $1 \leq i \leq n$, $i \neq j$: $C_j = \sum_{i=0,\,i\neq j}^{n} \lambda_i C_i$.
Montrer que B n'est pas inversible.

DÉFINITION 67
Soient $\mathbb{K}$ un corps et $n \in \mathbb{N}^*$. Soit $A \in \mathscr{M}_n(\mathbb{K})$. On dit que la matrice A est ***symétrique*** \对称矩阵\ *si ${}^tA = A$. On note $\mathscr{S}_n(\mathbb{K})$ l'ensemble des matrices $n \times n$ symétriques.*
On dit que la matrice A est ***antisymétrique*** \反对称矩阵\ *si ${}^tA = -A$. On note $\mathscr{A}_n(\mathbb{K})$ l'ensemble des matrices $n \times n$ antisymétriques.*

PROPOSITION 68
Soient $\mathbb{K}$ un corps et $n \in \mathbb{N}^*$. Alors :

(i) Toute matrice $M \in \mathscr{M}_n(\mathbb{K})$ s'écrit d'une unique façon comme la somme d'une matrice symétrique et d'une matrice antisymétrique.

(ii) Les ensembles $\mathscr{S}_n(\mathbb{K})$ et $\mathscr{A}_n(\mathbb{K})$ sont des sous-espaces vectoriels de $\mathscr{M}_n(\mathbb{K})$ qui sont supplémentaires dans $\mathscr{M}_n(\mathbb{K})$ (voir Géométrie 1) :

$$\mathscr{S}_n(\mathbb{K}) \oplus \mathscr{A}_n(\mathbb{K}) = \mathscr{M}_n(\mathbb{K}).$$

Preuve — (i) Soit $M \in \mathscr{M}_n(\mathbb{K})$. On peut alors écrire :

$$M = S + A, \qquad \text{avec} \qquad S = \frac{M + {}^tM}{2} \quad \text{et} \quad A = \frac{M - {}^tM}{2}.$$

D'après la Proposition 64, S est symétrique et A est antisymétrique.

Montrons que cette écriture est unique. Supposons que $M = S + A = S' + A'$.

Alors on a $S - S' = A' - A$ avec $S - S'$ symétrique et $A' - A$ antisymétrique.

Pour $N = S - S'$, N est à la fois symétrique et antisymétrique, donc $N = {}^tN = -N$. Cela donne $2N = 0$, donc N est nulle. Ainsi, on a $S = S'$ et $A = A'$.

(ii) Montrons que $\mathscr{S}_n(\mathbb{K})$ et $\mathscr{A}_n(\mathbb{K})$ sont des sous-espaces vectoriels de $\mathscr{M}(n)\mathbb{K}$.

La matrice nulle est symétrique. L'ensemble $\mathscr{S}_n(\mathbb{K})$ est donc non vide.

Pour A,B deux matrices symétriques, et λ,μ deux scalaires, on a ${}^t(\lambda A+\mu B) = \lambda {}^tA+\mu {}^tB = \lambda A+\mu B$. Donc la matrice $\lambda A+\mu B$ est symétrique. Ainsi, $\mathscr{S}_n(\mathbb{K})$ est bien un sous-espace vectoriel de $\mathscr{M}_n(\mathbb{K})$.

On montre la même chose pour $\mathscr{A}_n(\mathbb{K})$.

De plus, la preuve de (i) a montré que $\mathscr{S}_n(\mathbb{K}) \cap \mathscr{A}_n(\mathbb{K}) = \{0\}$. Ces sous-espaces vectoriels sont donc supplémentaires dans $\mathscr{M}_n(\mathbb{K})$. □

EXERCICE 69 — *Montrer que* $\dim \mathscr{S}_n(\mathbb{K}) = \dfrac{n(n+1)}{2}$ *et* $\dim \mathscr{A}_n(\mathbb{K}) = \dfrac{n(n-1)}{2}$.

2.8 Matrice d'une famille de vecteurs, rang d'une matrice

DÉFINITION 70
Soit E un $\mathbb{K}$-ev de dimension finie. Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E. Soient $x_1, \dots, x_p$ des vecteurs de E.
Pour $1 \leq j \neq p$, soit $x_j = \sum_{i=1}^{n} a_{i,j} e_i$ la décomposition du vecteur x_j dans la base E.
On définit la matrice $Mat_{\mathcal{B}}(x_1, \dots, x_p) = (a_{i,j})_{i,j} \in \mathscr{M}_{n,p}(\mathbb{K})$.
Cette matrice est appelée ***la matrice de la famille*** $(x_1, \dots, x_p)$ ***dans la base*** $\mathcal{B}$.

REMARQUE 71 — *La j-ème colonne C_j de la matrice $Mat_{\mathcal{B}}(x_1, \dots, x_p)$ contient les coefficients de la décomposition du vecteur x_j dans la base $\mathcal{B}$.*

EXEMPLE 72 — *Pour $E = \mathbb{K}^2$, $\mathcal{B} = ((1,-1),(0,1))$, et $x_1 = (1,0), x_2 = (1,1), x_3 = (2,1)$, on a :*

$$Mat_{\mathcal{B}}(x_1, x_2, x_3) = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix}.$$

REMARQUE 73 — *Soit $A \in \mathscr{M}_{n,p}(\mathbb{K})$. Notons $C_1, \dots, C_p$ les colonnes de A, vues comme vecteurs colonne de $\mathbb{K}^n$.*
Alors, la matrice A est exactement la matrice de la famille de vecteurs $(C_1, \dots, C_p)$ dans la base banonique de $\mathbb{K}^n$.

DÉFINITION 74
Soient $\mathbb{K}$ un corps et $n, p \geq 1$. Soit $A \in \mathscr{M}_{n,p}(\mathbb{K})$. Soient $C_1, \dots, C_p$ les colonnes de A, vues comme vecteurs colonnes de $\mathbb{K}^n$.
On définit le ***rang de*** *A, noté $rang(A)$ ou $rg(A)$, comme le rang de la famille de vecteurs $(C_1, \dots, C_p)$:*

$$rang(A) = rang(C_1, \dots, C_p).$$

REMARQUE 75 — *On a ainsi $rang(A) \leq \max(n, p)$, puisque cela correspond au rang d'une famille de p vecteurs dans un e.v. de dimension n.*

EXEMPLE 76 —
- *On a $rg(I_n) = n$*
- *On a $rg(0) = 0$*
- *Soient $a_1, \dots, a_p \in \mathbb{K}$. On pose :*

$$A = \begin{pmatrix} a_1 & \dots & a_p \\ 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix} \in \mathscr{M}_{n,p}(\mathbb{K}).$$

Alors $rang(A) = 0$ si tous les a_i sont nuls, et $rang(A) = 1$ sinon.

PROPOSITION 77
Soit E un $\mathbb{K}$-ev de dimension n. Soit $\mathcal{B}$ une base de E. Soient $x_1, \dots, x_p$ des vecteurs de E. Alors, on a :

$$rg(Mat_{\mathcal{B}}(x_1, \dots, x_p)) = rg(x_1, \dots, x_p).$$

Autrement dit, le rang de la famille $x_1, \dots, x_p$ est égal au rang de sa matrice associée dans la base $\mathcal{B}$.

Preuve — Posons $A = \mathrm{Mat}_{\mathcal{B}}(x_1, \dots, x_p) = (a_{i,j})_{i,j}$ et $\mathcal{B} = (e_1, \dots, e_n)$. On a donc :

$$x_j = \sum_{i=1}^{n} a_{i,j} e_i, \, \forall 1 \leq j \leq p.$$

Notons $C_1, \dots, C_p$ les colonnes de A, vues comme vecteurs colonne de $\mathbb{K}^n$, et $\mathcal{B}' = (f_1, \dots, f_n)$ la base canonique de $\mathbb{K}^n$..
Soient $\lambda_1, \dots, \lambda_p \in \mathbb{K}$. Montrons que l'on a

$$\sum_{k=1}^{p} \lambda_k x_k = 0 \iff \sum_{k=1}^{p} \lambda_k C_k = 0.$$

On a :

$$\begin{array}{rcl} & 0 & = \sum_{k=1}^{p} \lambda_k x_k \\ \iff & 0 & = \sum_{k=1}^{p} \lambda_k (\sum_{i=1}^{n} a_{i,k} e_i) \\ \iff & 0 & = \sum_{i=1}^{n} \left(\sum_{k=1}^{p} \lambda_k a_{i,k}\right) e_i. \end{array}$$

Comme la famille $(e_1, \dots, e_n)$ est une base de E, cela est équivalent à :

$$\sum_{k=1}^{p} \lambda_k a_{i,k} = 0, \, \forall 1 \leq i \leq n.$$

Comme la famille $(f_1, \dots, f_n)$ est une base de $\mathbb{K}^n$, cela est équivalent à :

$$\begin{array}{rcl} & 0 & = \sum_{i=1}^{n} \left(\sum_{k=1}^{p} \lambda_k a_{i,k}\right) f_i \\ \iff & 0 & = \sum_{k=1}^{p} \lambda_k (\sum_{i=1}^{n} a_{i,k} f_i) = \sum_{k=1}^{p} \lambda_k C_k, \end{array}$$

ce qui prouve l'équivalence.

Soit $r = \mathrm{rg}(x_1, \dots, x_p)$. D'après les propriétés du rang, il exite une sous-famille de $(x_1, \dots, x_p)$ à r éléments qui est libre. Quitte à réordonner les vecteurs, on suppose que la famille $(x_1, \dots, x_r)$ est libre.
Alors la famille $(C_1, \dots, C_r)$ est elle aussi libre. En effet,

$$b_1 C_1 + \dots + b_r C_r = 0 \text{ est équivalent à } b_1 x_1 + \dots + b_r x_r = 0,$$

ce qui est équivalent à $b_1 = b_2 = \dots = b_r = 0$ par liberté de $(x_1, \dots, x_r)$.
Comme $\mathrm{rg}(x_1, \dots, x_p) = r$, cela veut aussi dire que les vecteurs $x_{r+1}, \dots, x_p$ sont combinaison linéaire de $x_1, \dots, x_r$.
D'après le raisonnement précédent, le vecteur x_k est combinaison linéaire de $x_1, \dots, x_r$ si et seulement si le vecteur C_k est combinaison linéaire de $C_1, \dots, C_r$.
On en déduit donc que $\mathrm{rg}(\mathrm{Mat}_{\mathcal{B}}(x_1, \dots, x_p)) = r$, ce qui conclut. □

REMARQUE 78 — *Ainsi, on peut déterminer le rang d'une famille de vecteurs en calculant celui de sa matrice associée dans une base $\mathcal{B}$ bien choisie.*
Réciproquement, on peut calculer le rang d'une matrice A en montrant qu'elle est la matrice associée à une famille de vecteurs, dans une certaine base, et dont on connaît déjà le rang.

COROLLAIRE 79
Soit E un $\mathbb{K}$-ev de dimension finie. Soient $\mathcal{B}, \mathcal{B}'$ deux bases de E. Soient $x_1, \dots, x_p$ des vecteurs de E. Alors, on a :

$$rg(Mat_{\mathcal{B}}(x_1, \dots, x_p)) = rg(Mat_{\mathcal{B}'}(x_1, \dots, x_p)).$$

Autrement dit le rang de la matrice associée à la famille de vecteurs $(x_1, \dots, x_p)$ ne dépend pas de la base choisie.

Preuve — Découle de la proposition précédente. □

PROPOSITION 80
Soient $\mathbb{K}$ un corps et $n, p \geq 1$. Soit $A \in \mathscr{M}_{n,p}(\mathbb{K})$ une matrice échelonnée.
Alors, rang(A) est égal au nombre de lignes non-nulles de A.

Preuve — Soit $(e_1, \dots, e_n)$ la base canonique de $\mathbb{K}^n$.
Soit m le nombre de lignes non-nulles de A. Comme A est échelonnée, toutes ses colonnes sont donc des éléments de $\text{Vect}(e_1, \dots, e_m) = K^m \times \{0\}^{n-m}$, sous-ev de dimension m.
De plus, la famille $C_{\alpha_1}, \dots, C_{\alpha_m}$ est une famille de vecteurs colonne échelonnée dans la base $(e_1, \dots, e_m)$. Cette famille est donc libre.
On obtient donc que $\text{rg}(C_1, \dots, C_p) = m$, ce qui conclut. □

EXEMPLE 81 — *Soit* $A = \begin{pmatrix} -1 & 2 & 0 & 3 \\ 0 & 0 & 2 & 5 \\ 0 & 0 & 0 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix}$. *Alors, on a* $rang(A) = 3$.
Les vecteurs colonne C_1, C_3, C_4 *de* A *forment une famille échelonnée dans le sous-ev* $\text{Vect}\, e_1, e_2, e_3$.

PROPOSITION 82
Soient $\mathbb{K}$ *un corps et* $n, p \geq 1$. *Soit* $A \in \mathscr{M}_{n,p}(\mathbb{K})$. *Soit* $M \in \mathscr{M}_n(\mathbb{K})$ *une matrice inversible. Alors, on a :*

$$rang(MA) = rang(A).$$

Autrement dit, multiplier la matrice A *à gauche par une matrice inversible ne change pas son rang.*

Preuve — Soient $C_1, \dots, C_p$ les colonnes de A, vues comme vecteurs colonnes de $\mathbb{K}^n$. Soit $(e_1, \dots, e_n)$ la base canonique de $\mathbb{K}^n$. Soient $C'_1, \dots, C'_p$ les colonnes de MA.
Soient $\lambda_1 \dots, \lambda_p \in \mathbb{K}$. Montrons l'équivalence :

$$\lambda_1 C_1 + \dots + \lambda_r C_r = 0 \iff \lambda_1 C'_1 + \dots \lambda_r C'_r = 0.$$

La multiplication à gauche par M donne :

$$C'_j = MC_j, \forall 1 \leq j \leq p.$$

Donc,

$$\lambda_1 C_1 + \dots + \lambda_r C_r = 0 \implies 0 = M \times 0 = \lambda_1 MC_1 + \dots + \lambda_r MC_r = \lambda_1 C'_1 + \dots \lambda_r C'_r.$$

Comme M est inversible on a $A = M^{-1}MA$, d'où :

$$C_j = M^{-1}C'_j, \forall 1 \leq j \leq p.$$

Donc,

$$\lambda_1 C'_1 + \dots + \lambda_r C'_r = 0 \implies 0 = M^{-1} \times 0 = \lambda_1 M^{-1} C'_1 + \dots + \lambda_r M^{-1} C'_r = \lambda_1 C_1 + \dots \lambda_r C_r.$$

On peut alors montrer que $\text{rg}(C_1, \dots, C_p) = \text{rg}(C'_1, \dots, C'_p)$ en reprenant la preuve de la Proposition 77 □

COROLLAIRE 83 (Calcul du rang par la méthode du Pivot)
Soient $\mathbb{K}$ *un corps et* $n \geq 1$. *Soit* $A \in \mathscr{M}_n(\mathbb{K})$.
Soient $M_1, \dots, M_r$ *des matrices élémentaires et* B *une matrice échelonnée telles que* $M_r \dots M_1 A = B$.
Alors, le rang de A *est égal au nombre de lignes non-nulles de* B.

Preuve — Les matrices élémentaires sont inversibles, donc on a $\text{rg}(A) = \text{rg}(B)$, et B est une matrice échelonnée. □

En appliquant la méthode du Pivot à la matrice A pour se ramener à une matrice échelonnée, on obtient ainsi un calcul du rang de A.

PROPOSITION 84
Soient $\mathbb{K}$ *un corps et* $n \geq 1$. *Soit* $A \in \mathscr{M}_n(\mathbb{K})$.
Si $rang(A) < n$, *alors il existe* $B \in \mathscr{M}_n(\mathbb{K})$ *non-nulle telle que* $AB = 0$, *et* A *n'est pas inversible.*

Preuve — Si $\text{rang}(A) < n$, alors la famille des colonnes $(C_1, \dots, C_n)$ de A est liée : il existe une colonne de A qui est combinaison linéaire des autres.
Ainsi, il existe $1 \leq i \leq n$ et $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ tels que :

$$C_i = \sum_{j \neq i} \lambda_j C_j.$$

Posons $M = I_n + \sum_{j \neq i} -\lambda_j E_{j,i}$. L'opération $A \mapsto AM$ ne change pas les lignes $C_1, \dots, C_{i-1}, C_{i+1}, \dots, C_n$, et transforme C_i en $C_i - \sum_{j \neq i} \lambda_j C_j = 0$.
Ainsi, la matrice AM possède une colonne nulle. D'après la preuve de la Proposition 33, il existe une matrice B non-nulle telle que $AMB = 0$. Ainsi, la matrice AM n'est pas inversible.
Or, la matrice M est inversible, d'inverse $M' = I_n + \sum_{j \neq i} \lambda_j E_{j,i}$. (les opérations $C_i \mapsto C_i - \sum_{j \neq i} \lambda_j C_j$ et $C_i \mapsto C_i + \sum_{j \neq i} \lambda_j C_j$ sont inverses l'une de l'autre)

On en déduit que $B' = MB$ est une matrice qui est non-nulle. Comme on a $AB' = 0$, on en conclut donc que la matrice A n'est pas inversible. □

THÉORÈME 85
Soient $\mathbb{K}$ un corps et $n \geq 1$. Soit $A \in \mathscr{M}_n(\mathbb{K})$.
Alors A est inversible si et seulement si rang$(A) = n$.

Preuve — Par contraposée de la proposition précédente, si A est inversible alors on a $\text{rang}(A) = n$.

Réciproquement, supposons que $\text{rang}(A) = n$. Soient $C_1, \ldots, C_n$ les colonnes de A. Alors la famille de vecteurs colonne $(C_1, \ldots, C_n)$ est une base de $\mathbb{K}^n$. En particulier, les vecteurs de la base canonique $(e_1, \ldots, e_n)$ de $\mathbb{K}^n$ sont des combinaisons linéaires de $(C_1, \ldots, C_n)$:

$$e_i = \sum_{j=1}^{n} b_{i,j} C_j, \forall 1 \leq i \leq n.$$

On pose $B = (b_{i,j})_{i,j}$. La relation précédente donne :

$$A \times B = I_n.$$

Montrons que l'on a de même $BA = I_n$.
Comme $\text{rang}(A) = n$, on doit aussi avoir $\text{rang}({}^tA) = n$.
En effet, en supposant par l'absurde avoir $\text{rang}({}^tA) < n$, la Proposition précédente nous donnerait l'existence d'une matrice carrée C non-nulle telle que ${}^tAC = 0$. On aurait alors ${}^tCA = 0$, ce qui donnerait :

$$0 = {}^tCAB = {}^tC,$$

Cela contredit le fait que C est non-nulle.
Ainsi, on a $\text{rang}({}^tA) = n$.
Donc, il existe une matrice M telle que ${}^tAM = I_n$. Cela équivaut à ${}^tMA = I_n$. On obtient :

$${}^tM = {}^tMAB = B, \text{ donc } {}^tM = B.$$

On a ainsi $BA = AB = I_n$, donc la matrice A est inversible. □

PROPOSITION 86
Soient $\mathbb{K}$ un corps et $n \geq 1$. Soient $A \in \mathscr{M}_n(\mathbb{K})$. Alors :

- *Il existe $B \in \mathscr{M}_n(\mathbb{K})$ telle que $AB = I_n$ (ou $BA = I_n$) si et seulement si A est inversible, si et seulement si rg$(A) = n$.*
- *Il existe $C \in \mathscr{M}_n(\mathbb{K})$ non-nulle telle que $AC = 0$ (ou $CA = 0$) si et seulement si A n'est inversible, si et seulement si rg$(A) < n$.*

Preuve — Notons $C_1, \ldots, C_n$ les colonnes de A, vues comme vecteurs colonne de $\mathbb{K}^n$. Notons $(e_1, \ldots, e_n)$ la base canonique de $\mathbb{K}^n$.

- Pour $B = (b_{i,j})_{i,j}$, la relation $AB = I_n$ donne :

  $$\sum_{j=1}^{n} b_{i,j} C_j = e_i, \forall 1 \leq i \leq n.$$

  Les vecteurs de la base canonique sont donc des combinaisons linéaire de $C_1, \ldots, C_n$. On a donc que $\text{rg}(C_1, \ldots, C_n) = n$.
  Donc $\text{rg}(A) = n$ et A est inversible.
  Si l'on a $BA = I_n$, alors ${}^tA{}^tB = I_n$. On en déduit que ${}^tA$ est inversible, et donc que A est inversible.
- S'il existe C non-nulle telle que $AC = 0$ ou $CA = 0$, on sait que A n'est pas inversible, ce qui est équivalent à $\text{rg}(A) < n$ d'après le théorème précédent.
  Si A n'est pas inversible, alors on a $\text{rg}(A) < n$, donc il existe une matrice C non-nulle telle que $AC = 0$ d'après la Proposition 84.

□

REMARQUE 87 — *Le rang d'une matrice, que l'on peut calculer comme le rang d'une famille de vecteurs ou bien avec la méthode du Pivot, est donc une quantité qui permet de dire si une matrice A est inversible ou non.*
La dernière proposition simplifie grandement les conditions permettant de montrer qu'une matrice A est inversible ou non.
Ces résultats sont très utiles pour étudier les matrices.

2.9 Trace d'une matrice

Définition 88
Soient $\mathbb{K}$ un corps et $n \in \mathbb{N}^*$. Soit $A = (a_{i,j})_{(i,j)} \in \mathscr{M}_n(\mathbb{K})$. On définit la ***trace*** *de A, notée $\mathrm{Tr}(A)$ ou $\mathrm{tr}(A)$, comme la somme des éléments de la diagonale de A :*

$$\mathrm{Tr}(A) = a_{1,1} + \cdots + a_{n,n} = \sum_{i=1}^{n} a_{i,i} \in \mathbb{K}.$$

Remarque 89 — *La trace d'une matrice n'est définie que pour les matrices carrées.*

Proposition 90
Soient $A, B \in \mathscr{M}_n(\mathbb{K})$. On a :

$$\mathrm{Tr}(AB) = \mathrm{Tr}(BA).$$

Preuve — Pour $A = (a_{i,j})_{(i,j)}$ et $B = (b_{i,j})_{(i,j)}$, on a :

$$\begin{array}{rcl} \mathrm{Tr}(AB) & = & \mathrm{Tr}\left((\sum_{k=1}^{n} a_{i,k}b_{k,j})_{(i,j)}\right) \\ & = & \sum_{i=1}^{n}(\sum_{k=1}^{n} a_{i,k}b_{k,i}) \\ & = & \sum_{k=1}^{n}(\sum_{i=1}^{n} b_{k,i}a_{i,k}) \\ & = & \mathrm{Tr}\left((\sum_{i=1}^{n} b_{k,i}a_{i,j})_{(k,j)}\right) \\ & = & \mathrm{Tr}(BA). \end{array}$$

□

Remarque 91 — *Soient A et B deux matrices carrées. La trace de AB n'est en général pas égale à la trace de A multipliée par la trace de B. Par exemple :*

$$\mathrm{Tr}(I_2 I_2) = \mathrm{Tr}(I_2) = 2 \neq 4 = \mathrm{Tr}(I_2)\mathrm{Tr}(I_2).$$

Exercice 92 — *Soit $A \in \mathscr{M}_n(\mathbb{K})$.*

1. *On prend $\mathbb{K} = \mathbb{R}$. Montrer alors que $\mathrm{Tr}({}^tAA)$ est un nombre positif. Montrer que $\mathrm{Tr}({}^tAA)$ est nul si et seulement si A est la matrice nulle.*
2. *Montrer qu'il existe une matrice non nulle A dans $\mathscr{M}_2(\mathbb{C})$ telle que $\mathrm{Tr}({}^tAA)$ est nul.*

Exercice 93 —
Montrer que l'ensemble des matrices dont la trace est nulle est un sous-espace vectoriel de $\mathscr{M}_n(\mathbb{K})$. Déterminer une base de ce sous-espace vectoriel. Quelle est la dimension de ce sous-espace vectoriel ?

Chapitre 3 Polynômes à une indéterminée

Table des matières du chapitre

Un polynôme \多项式\ s'écrit de la forme

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$$

où les a_i s'appellent les coefficients de P \多项式P的系数\ et X où est l'indéterminée.
Le premier problème est de définir correctement ce que l'on veut dire par "l'indéterminée X", de choisir à quel ensemble appartiennent les coefficients a_i, et d'avoir les outils nécessaires pour manipuler les polynômes efficacement.
On retrouvera les polynômes tant en analyse (par ex. les développements limités) qu'en algèbre (par ex. polynôme caractéristique d'une application linéaire). Une bonne maîtrise des produits, divisions et factorisations de polynômes ainsi que de la caractérisation des racines est indispensable.

3.1 Polynômes, opérations sur les polynômes

3.1.1 Polynômes à une indéterminée

Dans tout ce chapitre, l'ensemble $\mathbb{K}$ désignera $\mathbb{R}$ ou $\mathbb{C}$ ou $\mathbb{Q}$. Ces ensembles sont des corps, et cette notion sera traitée en Algèbre 2, chapitre Structures algébriques. [1]

1. Un corps est un ensemble $\mathbb{K}$ muni d'une opération d'addition $+$ et d'une opération de multiplication $\times$. Ces opérations vérifient des propriétés comme $a+b=b+a$, $a.b=b.a$, $a(b+c)=ab+bc$,... Il faut aussi que tout élément non-nul possède un inverse pour la multiplication $\times$. C'est pour cela que $\mathbb{Z}$ n'est pas un corps, mais $\mathbb{Q}$ oui. Les exemples essentiels de corps sont $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Définition 1
Soit $\mathbb{K}$ un corps. On appelle ***polynôme à une indéterminée*** *à coefficients dans $\mathbb{K}$ toute suite d'éléments $(a_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ qui est nulle à partir d'un certain rang :*

$$\exists d \in \mathbb{N},\ \text{tel que } (a_n)_{n\in\mathbb{N}} = (a_0, a_1, \ldots, a_d, 0, \ldots, 0, \ldots).$$

L'ensemble des polynômes est noté $\mathbb{K}[X]$.

Définition 2
Soit $\mathbb{K}$ un corps. On définit sur $\mathbb{K}[X]$ deux lois internes $(+, \times)$ et une loi externe $(.)$:

1. *L'addition, $+$, est définie par :*

$$(a_0, \ldots, a_d, 0, \ldots) + (b_0, \ldots, b_{d'}, 0, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots, a_k + b_k, \ldots) = (a_n + b_n)_{n\in\mathbb{N}}.$$

   Une telle suite est bien dans $\mathbb{K}[X]$ car $c_k = 0$ pour $k > sup(d, d')$.
   La suite nulle, notée $0_{\mathbb{K}[X]} = (0, \ldots, 0, \ldots)$ ou 0, est l'élément neutre pour l'addition $+$.
2. *La multiplication, $\times$, est définie par :*

$$(a_0, \ldots, a_d, 0, \ldots) \times (b_0, \ldots, b_{d'}, 0, \ldots) = (c_n)_{n\in\mathbb{N}},\ \text{avec } c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

   Une telle suite est bien dans $\mathbb{K}[X]$ car $c_k = 0$ pour $k > m + n$.
   On note $1_{\mathbb{K}[X]} = (1, 0, \ldots, 0, \ldots)$, ou 1, l'élément neutre pour la multiplication $\times$.
3. *La multiplication par un scalaire de $\mathbb{K}$, ., définie par :*

$$\begin{array}{rcl} \mathbb{K} \times \mathbb{K}[X] & \to & \mathbb{K}[X] \\ (\lambda, (a_0, a_1, \ldots, a_d, 0 \ldots)) & \mapsto & \lambda.(a_n)_{n\in\mathbb{N}} = (\lambda.a_0, \lambda a_1, \ldots, \lambda.a_d, 0, \ldots). \end{array}$$

Proposition 3
Soit $\mathbb{K}$ un corps. Soient $P, Q, R \in \mathbb{K}[X]$. Soit $\lambda \in \mathbb{K}$. On a :

1. *$P + (Q + R) = (P + Q) + R$ ($+$ est associative) ;*
2. *$P + Q = Q + P$ ($+$ est commutative) ;*
3. *$P + 0 = 0 + P = P$ (0 est le neutre de $+$) ;*
4. *$\lambda.(P + Q) = \lambda.P + \lambda.Q$ ($.$ est distributive sur $+$) ;*
5. *$P \times (Q \times R) = (P \times Q) \times R$ ($\times$ est associatve) ;*
6. *$(P \times Q) = (Q \times P)$ ($\times$ est commutative) ;*
7. *$(P \times 1) = (1 \times P) = P$ (1 est le neutre de $\times$) ;*
8. *$P \times (Q + R) = P \times Q + P \times R = (Q + R) \times P$ ($\times$ est distributive sur $+$) ;*
9. *$P \times (\lambda.Q) = \lambda.P \times Q$ ($\times$ et $.$ commutent).*

L'ensemble $(\mathbb{K}[X], +, .)$ est donc un $\mathbb{K}$-espace vectoriel.

Preuve — Soient $P = (a_n)_{n\geq 0}$, $Q = (b_n)_{n\geq 0}$, $R = (c_n)_{n\geq 0}$.

1. On a : $(a_n)_{n\geq 0} + ((b_n)_{n\geq 0} + (c_n)_{n\geq 0}) = (a_n + b_n + c_n)_{n\geq 0} = ((a_n)_{n\geq 0} + (b_n)_{n\geq 0}) + (c_n)_{n\geq 0}$.
2. On a : $(a_n)_{n\geq 0} + (b_n)_{n\geq 0} = (a_n + b_n)_{n\geq 0} = (b_n)_{n\geq 0} + (a_n)_{n\geq 0}$.
3. On a : $P + 0 = (a_n + 0)_{n\geq 0} = (a_n)_{n\geq 0} = P$, et de la même façon $0 + P = P$.
4. On a : $\lambda.(P + Q) = (\lambda(a_n + b_n))_{n\geq 0} = (\lambda a_n + \lambda b_n))_{n\geq 0} = \lambda.P + \lambda.Q$.
5. Pour $(P \times Q) \times R = ((a_n)_{n\geq 0} \times ((b_n)_{n\geq 0}) \times (c_n)_{n\geq 0} = (d_n)_{n\geq 0}$, on a $d_n = \sum_{l=0}^{n}(\sum_{k=0}^{l} a_k b_{l-k})c_{n-l})$. Le coefficient d_n se réécrit :

$$\begin{aligned} d_n &= \sum_{l=0}^{n}(\sum_{k=0}^{l} a_k b_{l-k})c_{n-l}) = \sum_{m=0}^{n} a_m(\sum_{r=m}^{n} b_{r-m}c_{n-r}) \\ &= \sum_{m=0}^{n} a_m(\sum_{s=0}^{n-m} b_s c_{n-m-s}) \end{aligned}$$

   On obtient donc que

$$(P \times Q) \times R = ((a_n)_{n\geq 0} \times (b_n)_{n\geq 0}) \times (c_n)_{n\geq 0} = (a_n)_{n\geq 0} \times ((b_n)_{n\geq 0} \times (c_n)_{n\geq 0}) = P \times (Q \times R).$$

6. Pour $P \times Q = (a_n)_{n\geq 0} \times (b_n)_{n\geq 0} = (e_n)_{n\geq 0}$, on a $e_n = \sum_{k=0}^{n} a_k b_{n-k}$ pour tout $n \geq 0$. Le coefficient e_n se réécrit : $e_n = \sum_{l=0}^{n} a_{n-l} b_l$, ce qui implique que
$$P \times Q = (a_n)_{n\geq 0} \times (b_n)_{n\geq 0} = (b_n)_{n\geq 0} \times (a_n)_{n\geq 0} = Q \times P.$$
7. En prenant $(b_n)_{n\geq 0} = 1_{\mathbb{K}[X]}$, le calcul donne :
$$(a_n)_{n\geq 0} \times 1_{\mathbb{K}[X]} = 1_{\mathbb{K}[X]} \times (a_n)_{n\geq 0} = (a_n)_{n\geq 0}.$$
8. Pour $P \times (Q + R) = (a_n)_{n\geq 0} \times ((b_n)_{n\geq 0} + (c_n)_{n\geq 0}) = (f_n)_{n\geq 0}$, on a $f_n = \sum_{k=0}^{n} a_k (b_{n-k} + c_{n-k})$ pour tout $n \geq 0$. Le coefficient f_n se réécrit : $f_n = \sum_{k=0}^{n} a_k b_{n-k} + \sum_{k=0}^{n} a_k c_{n-k}$, ce qui implique que
$$(a_n)_{n\geq 0} \times ((b_n)_{n\geq 0} + (c_n)_{n\geq 0}) = (a_n)_{n\geq 0} \times (b_n)_{n\geq 0} + (a_n)_{n\geq 0} \times (c_n)_{n\geq 0}.$$
9. Avec les propriétés précédentes, on a :
$$P \times (\lambda.Q) = P \times (\lambda.1_{\mathbb{K}[X]} \times Q) = (P \times (\lambda.1_{\mathbb{K}[X]})) \times Q = (\lambda.1_{\mathbb{K}[X]}) \times P \times Q = \lambda.(P \times Q).$$

□

Proposition 4
Soit $\mathbb{K}[X]$ un corps. Soient $P, Q \in \mathbb{K}[X]$.
On a $P \times Q = 0$ si et seulement si $P = 0$ ou $Q = 0$.

Preuve — Soient $P = (a_n)_{n\geq 0}$ et $Q = (b_n)_{n\geq 0}$ dans $\mathbb{K}[X]$.
Si la suite $(a_n)_{n\geq 0}$ ou la suite $(b_n)_{n\geq 0}$ est la suite nulle, alors $(a_n)_{n\geq 0} \times (b_n)_{n\geq 0}$ est la suite nulle, par définition de $\times$ (si $P = 0$ ou $Q = 0$, alors $P \times Q = 0$).
Supposons que les suites $P = (a_n)_{n\geq 0}$ et $Q = (b_n)_{n\geq 0}$ sont non-nulles. Soient k, k' les plus grands entiers tels que $a_k, b_{k'} \neq 0$.
Pour $P \times Q = (a_n)_{n\geq 0} \times (b_n)_{n\geq 0} = (d_n)_{n\geq 0}$, on a alors $d_{k+k'} = a_k b_{k'}$. Comme $d_{k+k'} \neq 0$, on a donc $(a_n)_{n\geq 0} \times (b_n)_{n\geq 0} \neq 0$ (si $P \neq 0$ ou $Q \neq 0$, alors $P \times Q \neq 0$), ce qui termine la preuve. □

Écriture d'un polynôme

Définition 5
*Soit $\mathbb{K}$ un corps. On définit **l'indéterminée** de $\mathbb{K}[X]$ comme la suite $X = (0, 1, 0, \ldots, 0, \ldots)$.*

Proposition 6
Dans $\mathbb{K}[X]$, on pose $X^0 = 1$. Pour tout $k \in \mathbb{N}$, on a alors :
$$X^k = \underbrace{X \times \ldots \times X}_{k \text{ fois}} = (\underbrace{0, \ldots, 0}_{k}, 1, 0, \ldots, 0, \ldots).$$
Tout polynôme $P \in \mathbb{K}[X]$ non nul s'écrit de manière unique de la forme :
$$P = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0,$$
avec $a_0, \ldots, a_n \in \mathbb{K}$ et $a_n \neq 0$.

Remarque 7 — *L'indéterminée X est un élément très important pour travailler dans $\mathbb{K}[X]$.*
On écrit souvent $P(X)$ à la place de P. Cette écriture est parfois très utile (par exemple pour différencier un polynôme $P(X)$ de sa fonction polynômiale associée $x \mapsto P(x)$).
Un polynôme quelconque de $\mathbb{K}[X]$ est ainsi de la forme $P(X) = \sum_{k=0}^{n} a_k X^k$, pour un $n \geq 0$ et des $a_0, \ldots, a_n \in \mathbb{K}$.

Corollaire 8
Soit $P(X) = \sum_{k=0}^{n} a_i X^i \in \mathbb{K}[X]$ un polynôme. Alors $P(X)$ est le polynôme nul si et seulement si l'on a $a_k = 0$ pour tout $k \in \{0, \ldots, n\}$.

Remarque 9 — *La somme de polynômes sous la nouvelle écriture ne pose pas de problèmes. Pour le produit, on a :*
$$\left(\sum_{k=0}^{n} a_k X^k\right) \times \left(\sum_{k=0}^{m} b_k X^k\right) = \sum_{k=0}^{m+n} c_k X^k, \text{ avec } c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

EXEMPLE 10 — *Pour multiplier rapidement deux polynômes, on utilise la distributivité du produit sur la somme et on regroupe les termes de même degré :*

$$(X+1)(X^3+X+2) = X^4(1.1) + X^3(1.1) + X^2(1.1) + X(1.1+1.2) + (1.2) = X^4 + X^3 + X^2 + 3X + 2,$$
$$X^2+X+1)(X^2-4X+3) = X^4(1.1) + X^3(1.(-4)+1.1) + X^2(1.1+1.(-4)+1.3) + X(1.3+1.(-4)) + (1.3) \quad = X$$

REMARQUE 11 — *De la même façon, on peut aussi définir $\mathbb{Z}[X]$ l'ensemble des polynômes à une indéterminée à coefficients dans $\mathbb{Z}$. Cet ensemble n'est pas nouveau, car $\mathbb{Z}[X]$ est aussi le sous-ensemble de $\mathbb{Q}[X]$ des polynômes dont tous les coefficients sont entiers.*

Les ensembles de polynômes à coefficients dans $\mathbb{Z}$ (et plus généralement dans un anneau A, voir cours Algèbre 2) seront utiles plus tard (polynômes de matrices, polynômes d'endomorphismes,...), mais il faut d'abord étudier les polynômes à coefficients dans un corps. Ce chapitre étudie $\mathbb{K}[X]$.

3.1.2 Degré d'un polynôme

DÉFINITION 12
Soit $P(X) = \sum_{k=0}^{n} a_k X^k$ un polynôme non nul. On appelle degré \次数\ de P, noté $\deg(P)$, le plus grand entier k tel que $a_k \neq 0$.
Pour $d = \deg P$, le terme $a_d X^d$ est appelé terme dominant du polynôme P, a_d le coefficient dominant \最高次项系数\ de P.
a_0 est appelé le coefficient constant de P.
*On dit que P est un polynôme **unitaire** \首一多项式\ si son coefficient dominant vaut 1.*
Enfin, le degré du polynôme nul est par convention $\deg(0) = -\infty$.

EXEMPLES 13 *Le polynôme $2X^2+X+1$ n'est pas unitaire, mais X^7+X^3+2 l'est. On a $\deg(X^7+X^3+2) = 7$.*
Pour $\lambda \in \mathbb{K}^*$ on a $\deg(\lambda) = 0$, tandis que $\deg(0) = -\infty$.
Pour tout $n \geq 0$, on a $\deg(X^n) = n$.

PROPOSITION 14
Soient P,$Q \in \mathbb{K}[X]$. Il résulte des définitions de $+$ et $\times$ que

1. $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$;
   Si $\deg P \neq \deg Q$, alors $\deg P + Q = \max(\deg P, \deg Q)$.
2. $\deg(P \times Q) = \deg P + \deg Q$;
3. $\forall \lambda \in \mathbb{K}^*$, $\deg \lambda.P = \deg P$.

Preuve —

1. Si $P = 0$ alors $P + Q = Q$ et le résultat est évident. Il en est de même si $Q = 0$.

   Si $P \neq 0$ et $Q \neq 0$, alors, en posant $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{m} b_k X^k$ avec $n = \deg(P)$ et $m = \deg(Q)$, on a :

   $$P + Q = \sum_{k=0}^{\max(n,m)} (a_k + b_k) X^k.$$

   Ainsi, cela donne :

   $$\deg(P+Q) \leqslant \max(\deg(P), \deg(Q)).$$

2. Si $P = 0$ ou $Q = 0$, alors $P \times Q = 0$ et :

   $$\deg(PQ) = \deg(0) = -\infty = \deg(P) + \deg(Q).$$

   Sinon, on a $P = \sum_{k=0}^{n} a_k X^k$ avec $a_n \neq 0$ et $Q = \sum_{k=0}^{m} b_k X^k$ avec $b_m \neq 0$. Cela donne :

   $$PQ = \sum_{k \in \mathbb{N}} \Big(\sum_{i+j=k} a_i b_j \Big) X^k.$$

   Le coefficient de degré $n+m$ est $a_n b_m \neq 0$, et tous les coefficients de degré strictement supérieur à $n+m$ sont nuls. Donc, on a :

   $$\deg(PQ) = \deg(P) + \deg(Q).$$

□

Exemples 15

1. $\deg((X^3+X+3)+(X^2+2))=3$;
2. $\deg((X^3+X+3)+(-X^3+3X+7))=1$;
3. $\deg((X^3+X+2)(X^5+3X^4+2))=8$.

Le degré d'un polynôme permet de montrer à nouveau que : Pour $P,Q\in\mathbb{K}[X]$, on a $PQ(X)=0$ si et seulement si $P(X)=0$ ou $Q(X)=0$.

Remarque 16 — *L'écriture* $P(X)=\sum_{k=0}^{n}a_kX^k$ *avec* $a_0,\dots,a_n\in\mathbb{K}$ *nous dit seulement que* $\deg(P)\leq n$.

Il faut rajouter la condition $a_n\neq 0$ *pour avoir* $\deg(P)=n$.

Exemple 17 — *Quel est de degré du polynôme* $(X+1)^n-(X-1)^n$ *?*

Proposition 18
Soit $\mathbb{K}$ *un corps. On dit que* $P\in\mathbb{K}[X]$ *est inversible s'il existe* $Q\in\mathbb{K}[X]$ *tel que* $P(X)Q(X)=Q(X)P(X)=1$.
Les polynômes inversibles de $\mathbb{K}[X]$ *sont les polynômes constants et non-nuls.*

Preuve — Soit $P\in\mathbb{K}[X]$ inversible. On a alors $Q\in\mathbb{K}[X]$ tel que $P(X)Q(X)=1$. Cela donne $\deg(PQ)=\deg(P)+\deg(Q)=\deg(1)=0$. Comme P et Q sont non-nuls, leurs degrés sont des entiers positifs. On a ainsi $\deg(P)=\deg(Q)=0$, donc P et Q sont des polynômes constants non-nuls.

Réciproquement, pour $P(X)=\lambda$ avec $\lambda\neq 0$, P est inversible dans $\mathbb{K}[X]$. □

Définition 19
Soient $\mathbb{K}$ *un corps et* $n\in\mathbb{N}$. *On définit* $\mathbb{K}_n[X]$ *l'ensemble des polynômes sur* $\mathbb{K}$ *de degré inférieur ou égal à* n *:*

$$\mathbb{K}_n[X]=\{P\in\mathbb{K}[X],\ \deg(P)\leq n\}.$$

L'ensemble $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $(\mathbb{K}[X],+,.)$.

3.1.3 Fonctions polynomiales

Définition 20
Soit $P(X)\in\mathbb{K}[X]$, *avec* $P(X)=\sum_{k=0}^{n}a_kX^k$. *On appelle fonction polynomiale associée au polynôme* $P(X)$, *la fonction notée* P *ou* f_P *ou* $(x\mapsto P(x))$, *définie par :*

$$P:\begin{array}{ccc}\mathbb{K}&\to&\mathbb{K}\\ x&\mapsto&P(x):=\sum_{k=0}^{n}a_kx^k\end{array}.$$

Remarque 21 — *La fonction* $\psi: P(X)\in\mathbb{K}[X]\mapsto(x\mapsto P(x))\mathcal{F}(\mathbb{K},\mathbb{K})$ *vérifie les propriétés :*

- $\psi(P+Q)=\psi(P)+\psi(Q)$;
- $\psi(\lambda.P)=\lambda\psi(P)$;
- $\psi(P\times Q)=\psi(P)\times\psi(Q)$.

En particulier, ψ *est une application linéaire de* $\mathbb{K}[X]$ *vers* $\mathcal{F}(\mathbb{K},\mathbb{K})$.

On montrera par la suite que si le corps $\mathbb{K}$ *a une infinité d'éléments, alors l'application linéaire* ψ *est injective.*

Exemple 22 — *La fonction* $x\in\mathbb{R}\mapsto ax^2+bx+c$ *est entre autres la fonction polynômiale associée à* $aX^2+bX+c\in\mathbb{R}[X]$.

Composition de polynômes

DÉFINITION 23
Soient $P, Q \in \mathbb{K}[X]$, avec $P(X) = \sum_{k=0}^{n} a_k X^k$.
On définit la composée des polynômes P et Q, notée $P \circ Q$, par le polynôme :

$$P \circ Q(X) = P(Q(X)) := \sum_{k=0}^{\infty} a_k Q(X)^k.$$

REMARQUE 24 —

1. *Dans le cas particulier où $Q(X) = X$, on a $P(Q(X)) = P(X)$, c'est pourquoi on utilise aussi bien les notations P que $P(X)$ pour désigner ce polynôme.*
2. *L'opération de composition $\circ$ est distributive à droite sur les opérations $+,\times,.$:*

   $$(\lambda \cdot P + \mu \cdot Q)(R(X)) = \lambda \cdot P(R(X)) + \mu \cdot Q(R(X)) \quad et \quad (P \times Q)(R(X)) = P(R(X)) \times Q(R(X)).$$

   Mais, on fera attention au fait que l'opération de composition des polynômes n'est pas distributive à gauche avec $+,.,\times$. En effet, en général on a :

   $$P\circ(Q+R)(X) \neq P\circ Q(X)+P\circ R(X) \quad , \quad P\circ(\lambda X) \neq \lambda P(X) \quad et \quad P\circ(Q\times R)(X) \neq P\circ Q(X)\times P\circ R(X).$$

3. *Pour $f_P : \mathbb{K} \to \mathbb{K}$ et $f_Q : \mathbb{K} \to \mathbb{K}$ les fonctions polynomiales associées aux polynômes P et Q, alors on a $f_{P\circ Q} = f_P \circ f_Q$.*
   La composée de polynômes est construite pour s'assimiler à une composée de fonctions. C'est pourquoi elle ne se comporte pas très bien avec l'addition et les multiplications.

EXEMPLE 25 — *Pour $P(X) = X^2 + 2X + 3$, $\lambda = 2$, et $Q(X) = X + 1$, on a :*
$P \circ Q(X) = P(X + 1)(X + 1)^2 + 2(X + 1) + 3 = X^2 + 4X + 6$ *et* $P(\lambda X) = 4X^2 + 4X + 3$,
tandis que $P(X) + P(1) = X^2 + 2X + 9$ *et* $2P(X) = 2X^2 + 4X + 6$.

EXERCICE 26 — *Soient $P, Q \in \mathbb{K}[X]$. Déterminer $\deg(P \circ Q)$ en fonction de $\deg(P)$ et $\deg(Q)$.*

3.2 L'ESPACE VECTORIEL $\mathbb{K}[X]$

3.2.1 Familles échelonnées en degré

PROPOSITION 27
Soient $\mathbb{K}$ un corps et $n \in \mathbb{N}$. L'espace vectoriel $\big(\mathbb{K}[X], +, .\big)$ est un $\mathbb{K}$-espace vectoriel de dimension infinie.
La famille $\{1, X, \ldots, X^n, \ldots\} = \{X^k,\ k \geq 0\}$ est une base de cet espace vectoriel, appelée base canonique de $\mathbb{K}[X]$.
Le sous-espace vectoriel $\mathbb{K}_n[X]$ des polynômes de degré au plus n est un sous-espace vectoriel de $\mathbb{K}[X]$, de dimension $n + 1$.
La famille $\{1, X, \ldots, X^n\}$ est une base de cet espace, appelée base canonique de $\mathbb{K}_n[X]$.

Preuve — Montrons par l'absurde que $\mathbb{K}[X]$ est de dimension infinie : Supposons qu'il existe $\{P_1, \ldots, P_m\}$ une famille génératrice finie de $\mathbb{K}[X]$. On pose $d = \max_{i \in [\![1,n]\!]} \deg P_i$. Alors toute combinaison linéaire $\sum_{i=1}^{m} \lambda_i P_i$ est de degré au plus d. Ainsi, X^{d+1} ne peut pas s'écrire comme une combinaison linéaire des P_i. Ceci contredit le fait que cette famille soit génératrice. Par définition de $\mathbb{K}[X]$ et de X^k, la famille $\{1, X, X^2, \ldots\}$ est génératrice de $\mathbb{K}[X]$.

Soient $k_1 < k_2 < \ldots < k_r$ des entiers, et $a_1, \ldots, a_r \in \mathbb{K}$, tels que $P(X) = a_1 X^{k_1} + a_2 X^{k_2} + \ldots + a_r X^{k_r}$ soit le polynôme nul. D'après le Corollaire 8 , un polynôme est nul si et seulement si tous ses coefficients sont nuls. Comme les k_i sont tous distincts, on a donc $a_1 = a_2 = \ldots = a_r = 0$. La famille $\{X^k,\ k \in \mathbb{N}\}$ est donc libre. C'est donc une base de $\mathbb{K}[X]$.

La famille $\{1, X, \dots, X^n\}$ étant une sous-famille d'une famille libre, elle est libre. Cette famille est contenue dans $\mathbb{K}_n[X]$, et tout polynôme de $\mathbb{K}_n[X]$ s'écrit comme une combinaison linéaire de ses éléments. Cette famille est donc une base de $\mathbb{K}_n[X]$, qui est ainsi de dimension $\text{Card}(\{1, X, \dots, X^n\}) = n+1$. □

DÉFINITION 28
Soit $\{P_0, \dots, P_n\}$ une famille de polynômes de $\mathbb{K}[X]$. On dit que cette famille est échelonnée en degré si $\deg P_i = i$ pour tout $i \in [\![0, n]\!]$.

PROPOSITION 29
Soit $\{P_0, \dots, P_n\}$ une famille de polynômes de $\mathbb{K}[X]$ échelonnée en degré. Alors cette famille est une base de $\mathbb{K}_n[X]$.

Preuve — Comme $\dim \mathbb{K}_n[X]$ est de dimension $n+1$, il suffit de montrer que la famille $\{P_0, \dots, P_n\}$ est libre. On sait par hypothèse que $\deg P_0 = 0$, donc $P_0 \neq 0$. Pour tout $1 \leq i \leq n$, on a $\deg(P_i) = i > \max(\deg(P_0), \dots, \deg(P_{i-1}))$. Ainsi, $P_i \notin \text{Vect}(P_0, \dots, P_{i-1})$. Cette famille est donc libre, ce qui conclut la preuve. □

REMARQUE 30 — *Si vous pouvez montrer qu'une famille de $n+1$ polynômes est échelonnée en degré, vous aurez montré que c'est une base de $\mathbb{K}_n[X]$. La famille $(1, 1+X, 1+X+X^2, \dots, 1+X+\dots+X^n)$ est une base de $\mathbb{K}_n[X]$ car elle est échelonnée en degré.*
Plus généralement, une famille $\{P_1, \dots, P_n\}$ de polynômes qui sont de degrés tous distincts est libre. En réordonnant ces polynômes selon leur degré, on peut voir cet ensemble comme une sous-famille d'une famille échelonnée en degré.

Nous allons voir une famille de polynômes assez classique et très utile qui elle n'est pas écéhelonnée en degré, mais qui forme une base de $\mathbb{K}_n[X]$.

3.2.2 Polynômes interpolateurs de Lagrange

DÉFINITION 31
Soit $n \geq 1$. Soient $a_0, \dots, a_n \in \mathbb{K}$ des éléments deux à deux distincts.
*On définit la famille de polynômes $\{L_0, \dots, L_n\}$, appelés **polynômes interpolateurs de Lagrange**, par :*

$$L_i(X) == \frac{\prod_{k=0, k\neq i}^{n} (X - a_k)}{\prod_{k=0, k\neq i}^{n} (a_i - a_k)} = \frac{(X-a_0)\dots(X-a_{i-1})(X-a_{i+1})\dots(X-a_n)}{(a_i-a_0)\dots(a_i-a_{i-1})(a_i-a_{i+1})\dots(a_i-a_n)}, \ \forall i \in [\![0, n]\!].$$

PROPOSITION 32
Soit $n \geq 1$. Soient $a_0, \dots, a_n \in \mathbb{K}$ deux à deux distincts. On a alors :

1. *$L_i(a_j) = \delta_{i,j}$, $\forall i \in [\![0, n]\!]$. ($\delta_{i,j} = 1$ si $i = j$ et $\delta_{i,j} = 0$ si $i \neq j$)*
2. *La famille $\{L_0, \dots, L_n\}$ est une famille de polynômes de degré n qui forme une base de $\mathbb{K}_n[X]$.*
3. *Soit $P \in \mathbb{K}_n[X]$. Alors $P(X) = \sum_{i=0}^{n} P(a_i) L_i(X)$.*
4. *Soient b_0, ..., $b_n \in \mathbb{K}$.*
   Il existe un unique polynôme $Q \in \mathbb{K}_n[X]$ tel que $Q(a_i) = b_i$ pour tout $0 \leq i \leq n$. On a :

$$Q(X) = \sum_{i=0}^{n} b_i L_i(X).$$

Preuve —

1. On a $L_i(a_j) = \dfrac{(a_j-a_0)\dots(a_j-a_{i-1})(a_j-a_{i+1})\dots(a_j-a_n)}{(a_i-a_0)\dots(a_i-a_{i-1})(a_i-a_{i+1})\dots(a_i-a_n)} = \begin{cases} 1 \text{ si } i = j \\ 0 \text{ sinon car } (a_i - a_i) \text{ apparaît au numérateur.} \end{cases}$
2. Comme $\dim(\mathbb{K}_n[X]) = n+1$, il suffit de montrer que la famille $\{L_0, \dots, L_n\}$ est libre.

   $$\text{Si } \sum_{i=0}^{n} \lambda_i L_i = 0, \text{ alors } \sum_{i=0}^{n} \lambda_i L_i(a_j) = 0 \, \forall j \in [\![0, n]\!], \text{ donc } \lambda_j = 0 \, \forall j \in [\![0, n]\!].$$

   Cette famille est donc bien une base de $\mathbb{K}_n[X]$.

3. Soit $P(X) = \sum_{i=0}^{n} c_i L_i(X)$ la décomposition de P dans la base $\{L_0, \dots, L_n\}$. On a alors $P(a_j) = \sum_{i=0}^{n} c_i L_i(a_j) = c_j$, donc $c_j = P(a_j)$ pour tout $1 \leq j \leq n$. Cette écriture est unique car elle correspond à une décomposition dans une base.
4. Avec les notations de l'énoncé, le polynôme $Q(X) = \sum_{i=0}^{n} \alpha_i L_i(X)$ vérifie bien que $Q(a_j) = b_j$, et on a montré en 3) qu'il est alors unique.

EXEMPLE 33 (Matrice de Vandermonde) — *Soient a_0, ..., $a_n \in \mathbb{K}$ des éléments deux à deux distincts. On cherche à montrer que la matrice suivante, appelée matrice de Vandermonde, est inversible et à calculer son inverse.*

$$V(a_0, \dots, a_n) = \begin{pmatrix} 1 & a_0 & \dots & a_0^n \\ \vdots & \vdots & \dots & \vdots \\ 1 & a_{n-1} & \dots & a_{n-1}^n \\ 1 & a_n & \dots & a_n^n \end{pmatrix}.$$

Soient $y_0, \dots, y_n \in \mathbb{K}$. On cherche à résoudre :

$$V(a_0, \dots, a_n) \begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_0.1 + x_1 a_0 + \dots + x_n a_0^n \\ \vdots \\ x_0.1 + x_1 a_{n-1} + \dots + x_n a_{n-1}^n \\ x_0.1 + x_1 a_n + \dots + x_n a_n^n \end{pmatrix} = \begin{pmatrix} y_0 \\ \vdots \\ y_n \end{pmatrix}.$$

En posant $P(X) = x_0 + x_1 X + \dots + x_n X^n$, le polynôme P serait alors un polynôme de degré au plus n tel que $P(a_i) = y_i$ pour tout $i \in [\![0, n]\!]$. D'après ce qui précède, un tel polynôme existe et vaut :

$$P(X) = \sum_{i=0}^{n} y_i L_i(X) = x_0 + x_1 X + \dots + x_n X^n.$$

Ainsi, le système linéaire initial possède toujours une solution. Cela implique que la matrice $V(a_0, \dots, a_n)$ est inversible. Pour trouver la valeur de $(x_0, \dots, x_n)$ en fonction de $(y_0, \dots, y_n)$, il suffit de développer chaque polynôme interpolateur de Lagrange. Pour $L_j = \sum_{i=0}^{n} a_{i,j} X^i$, on a alors $x_i = \sum_{j=0}^{n} a_{i,j} y_j$. Ainsi, l'inverse de la matrice de Vandermonde est $V(a_0, \dots, a_n)^{-1} = (a_{i,j})_{0 \leq i,j \leq n}$.

□

REMARQUE 34 — *Nous venons de montrer qu'en prenant $n+1$ points deux à deux distincts, un polynôme de degré au plus n, était uniquement déterminé par sa valeur en ces $n+1$ points.*
Si $\mathbb{K}$ a une infinité d'éléments, alors il existe des familles de polynômes interpolateurs de Lagrange pour toute famille de points aussi grande que l'on veut.

Il existe cependant des corps $\mathbb{K}$ avec un nombre fini d'éléments (voir cours Algèbre 2). Sur un tel corps, on ne peut interpoler que pour $n+1 \leq Card(\mathbb{K})$ points distincts.

EXEMPLE 35 — *Trouver le polynôme $P \in \mathbb{R}[X]$ de degré au plus 2 tel que $P(0) = 1$, $P(1) = 2$ et $P(3) = 3$.*

3.3 Division euclidienne de polynômes

3.3.1 Notion de divisibilité

DÉFINITION 36
Soient A, $B \in \mathbb{K}[X]$ deux polynômes. On dit que A divise B, noté $A|B$, s'il existe un polynôme $C \in \mathbb{K}[X]$ tel que $B = AC$.

DÉFINITION 37
On dit que deux polynômes A et B sont associés s'il existe $\lambda \in \mathbb{K}^*$, tel que $A = \lambda B$.

EXEMPLE 38 — *Les polynômes $2X^3 + 1$ et $4X^3 + 2$ sont associés.*

REMARQUE 39 — *Deux polynômes $A, B \in \mathbb{K}[X]$ sont associés si et seulement si A divise B et B divise A.*

Comme les éléments inversibles de $\mathbb{K}[X]$ sont les polynômes constants non-nuls, travailler au polynôme associé près est égal à travailler à un polynôme inversible près.

Par exemple, tout polynôme A non-nul est associé à un polynôme unitaire (de coefficient dominant égal à 1).

Cette relation de divisibilité sur $\mathbb{K}[X]$ est similaire à celle sur $\mathbb{Z}$. Travailler "au polynôme associé près" dans $\mathbb{K}[X]$ est égal à travailler "au signe près" dans $\mathbb{Z}$.

3.3.2 Division euclidienne de polynômes

THÉORÈME 40 (Division euclidienne de polynômes)
Soient A et $B \in \mathbb{K}[X]$ avec $B \neq 0$. Il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que :

$$A = QB + R \qquad \text{avec} \qquad \deg R < \deg B.$$

Preuve — L'unicité se montre comme pour la division euclidienne d'entiers : on suppose qu'il existe deux couples possibles, et on montre qu'ils sont égaux.
Existence : Le cas $B = \lambda \in \mathbb{K}^*$ ($\deg B = 0$) est immédiat avec $(Q, R) = (\lambda^{-1}A, 0)$. Supposons B non constant.
On procède par récurrence sur $\deg(A)$. On remarque d'une part que si $\deg(A) < \deg(B)$, alors $(Q, R) = (0, A)$.
D'autre part, si $\deg A \geq \deg B$, en écrivant :

$$A = a_n X^n + \ldots + a_0, \ B = b_m X^m + \ldots + b_0, \text{ avec } a_n b_m \neq 0,$$

on remarque que le polynôme $A - \frac{a_n}{b_m} X^{n-m} B$ est de degré strictement inférieur àdeg(A), ce qui permet d'appliquer l'hypothèse de récurrence à ce dernier. □

REMARQUE 41 — *Soient $A, B \in \mathbb{K}[X]$ avec B non-nul. On a $B|A$ si et seulement si le reste de la division euclidienne de A par B est nul.*

EXEMPLE 42 (Algorithme de la division euclidienne \欧几里德算法 / 辗转相除法\) —
On effectue une division euclidienne de polynômes en faisant descendre le degré du polynôme à diviser. Voici en exemple la division euclidienne de $A = X^5 + 4X^4 + 2X^3 + X^2 - X - 1$ par $B = X^3 - 2X + 3$:

$$\begin{array}{rrrrrr|l} X^5 & +4X^4 & +2X^3 & +X^2 & -X & -1 & X^3 - 2X + 3 \\ \cline{7-7} & 4X^4 & +4\,X^3 & -2X^2 & -X & -1 & X^2 + 4X + 4 \\ & & 4X^3 & +6X^2 & -13X & -1 & \\ & & & 6X^2 & -5X & -13 & \end{array}$$

On trouve finalement $X^5 + 4X^4 + 2X^3 + X^2 - X + 1 = (X^3 - 2X + 3)(X^2 + 4X + 4) + (6X^2 - 5X - 13)$.

3.4 PGCD ET PPCM, THÉORÈMES DE BÉZOUT ET DE GAUSS

PROPOSITION-DÉFINITION 43
Soient A,$B \in \mathbb{K}[X]$.
Alors, il existe un unique polynôme $D \in \mathbb{K}[X]$, unitaire, tel que :

$$A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X].$$

*On appelle D le **plus grand diviseur commun** de A et B, et on le note* $\gcd(A, B)$ *ou $A \wedge B$.*

Preuve — Soient $A, B \in \mathbb{K}[X]$. On a $A\mathbb{K}[X] + B\mathbb{K}[X] = \{AU + BV, U, V \in \mathbb{K}[X]\}$.
Existence : Si $A(X) = B(X) = 0$ alors on a $A\mathbb{K}[X] + B\mathbb{K}[X] = \{0\} = 0\mathbb{K}[X]$, et $D(X) = 0$ convient.
Si $A \neq 0$ ou $B \neq 0$, alors $A\mathbb{K}[X] + B\mathbb{K}[X]$ contient des polynômes non-nuls. Soit D un polynôme non-nul de $A\mathbb{K}[X] + B\mathbb{K}[X]$ de plus petit degré. Si λ est son coefficient dominant, on remarque que $\lambda^{-1}D \in A\mathbb{K}[X] + B\mathbb{K}[X]$. On peut donc supposer que D est unitaire. Montrons que $A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$.
Comme $D \in A\mathbb{K}[X] + B\mathbb{K}[X]$, on a $U, V \in \mathbb{K}[X]$ tels que $D = Au + BV$. Pour $P \in D\mathbb{K}[X]$, on a $P = SD$ avec $S \in \mathbb{K}[X]$, donc $P = ASU + BSV \in A\mathbb{K}[X] + B\mathbb{K}[X]$.

Réciproquement, soit $Q \in A\mathbb{K}[X] + B\mathbb{K}[X]$. On effectue la division euclidienne de Q par D :

$$Q = SD + R, \text{ avec } \deg R < \deg D.$$

On a alors $R = QD - Q \in A\mathbb{K}[X] + B\mathbb{K}[X]$. Comme $\deg(R) < \deg(D)$, on a donc $R = 0$ par définition de P. Cela montre que $A\mathbb{K}[X] + B\mathbb{K}[X] \subset D\mathbb{K}[X]$.

Unicité : Supposons que $D_1\mathbb{K}[X] = D_2\mathbb{K}[X]$ avec D_1, D_2 unitaires. Alors il existe $U, V \in \mathbb{K}[X]$ tels que $D_2 = UD_2$ et $D_2 = VD_1$. On a donc D_1 divise D_2 et D_2 divise D_1. Ces polynômes sont donc associés : $D_1(X) = \lambda D_2(X)$ pour un $\lambda \in \mathbb{K}$, $\lambda \neq 0$. Comme P et Q sont unitaires, on a donc $P = Q$, ce qui démontre l'unicité voulue. □

PROPOSITION-DÉFINITION 44
Soient A,$B \in \mathbb{K}[X]$.
Alors, il existe un unique polynôme $M \in \mathbb{K}[X]$, unitaire, tel que :

$$A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X].$$

On appelle M le plus petit commun multiple de A et B, et on le note $\text{ppcm}(A, B)$ *ou* $A \vee B$.

Preuve — Cette preuve est identique à celle de l'existence et de l'unicité du ppcm de deux entiers.
Les idées de la preuve sont identiques à celle du $\text{pgcd}(A, B)$. □

DÉFINITION 45
Soient A,$B \in \mathbb{K}[X]$. On dit que A et B sont ***premiers entre eux*** *si* $\text{pgcd}(A, B) = 1$.

PROPOSITION 46 (Théorème de Bézout)
Soient A,$B \in \mathbb{K}[X]$.
Les polynômes A et B sont premiers entre eux si et seulement s'il existe $C, D \in \mathbb{K}[X]$ tels que $A(X)C(X) + B(X)D(X) = 1$.

Preuve — On a $\text{pgcd}(A, B) = 1$ si et seulement si $A\mathbb{K}[X] + B\mathbb{K}[X] = \mathbb{K}[X]$. Cela implique qu'il existe $C, D \in \mathbb{K}[X]$ tels que $1 = A(X)C(X) + B(X)D(X)$.

Réciproquement, si l'on a $1 = A(X)C(X)+B(X)D(X)$, alors $A\mathbb{K}[X]+B\mathbb{K}[X]$ contient $1.\mathbb{K}[X] = \mathbb{K}[X]$, d'où $A\mathbb{K}[X]+B\mathbb{K}[X] = \mathbb{K}[X]$. □

REMARQUE 47 — *On peut montrer façon identique au cas de $\mathbb{Z}$ que* $\text{pgcd}(A, B)$ *et* $\text{ppcm}(A, B)$ *sont bien le plus grand commun diviseur et plus petit commun multiple de A et de B, au sens de la division de polynômes.*

De même, avec la division euclidienne on peut déterminer $\text{pgcd}(A, B)$ *via l'algorithme d'Euclide, et l'on peut trouver $U, V \in \mathbb{K}[X]$ tels que $AU + BV = \text{pgcd}(A, B)$ via l'algorithme d'Euclide étendu.*

PROPOSITION 48
Soient $A, B \in \mathbb{K}[X]$. Alors $S = \text{pgcd}(A, B)$ si et seulement si :

1. *$S \mid A$ et $S \mid B$,*
2. *Pour tout $T \in \mathbb{K}[X]$ tel que $T \mid A$ et $T \mid B$, on a $T \mid S$.*

Autrement dit, S est le plus grand diviseur de A et de B.

PROPOSITION 49
Soient $A, B \in \mathbb{K}[X]$. Alors $S = \text{ppcm}(A, B)$ si et seulement si :

1. *$A \mid S$ et $B \mid S$,*
2. *Pour tout $T \in \mathbb{K}[X]$ tel que $A \mid T$ et $B \mid T$, on a $S \mid T$.*

Autrement dit, S est le plus petit multiple de A et de B.

EXEMPLE 50 (Algorithme d'Euclide) — *Calculons le pgcd de $X^4 - 5X^2 + X + 2$ et $X^2 - 3X + 1$ à l'aide de l'algorithme d'Euclide.*

1. *Division euclidienne de $X^4 - 5X^2 + X + 2$ par $X^2 - 3X + 1$:*
   $X^4 - 5X^2 + X + 2 = (X^2 - 3X + 1) \times (X^2 + 3X + 3) + 7X - 1$.
2. *Division euclidienne de $X^2 - 3X + 1$ par $7X - 1$:* $X^2 - 3X + 1 = 7X - 1 \times \frac{7X-20}{49} + \frac{29}{49}$.
3. *Division euclidienne de $7X - 1$ par $\frac{29}{49}$:* $7X - 1 = \frac{29}{49} \times \frac{49}{29}(7X - 1) + 0$. *Le reste est nul !*

Le dernier reste non nul dans la suite des divisions euclidienne est donc 1 *(à association près). Ainsi, on a* $\text{pgcd}(X^4 - 5X^2 + X + 2, X^2 - 3X + 1) = 1$.

Exemple 51 (Algorithme d'Euclide étendu) — *Appliquons l'algorithme d'Euclide étendu pour déterminer le pgcd et des coefficients de Bézout pour* $X^4 + X^3 - 2X + 4$ *et* $X^2 - X + 3$.

$$\begin{aligned}
X^4 + X^3 - 2X + 4 &= (X^2 - X + 3)(X^2 + 2X - 1) + (-9X + 7) \\
X^2 - X + 3 &= (-9X + 7) \times \tfrac{-9X+2}{81} + \tfrac{229}{81} \\
-9X + 7 &= \tfrac{229}{81} \times \tfrac{81(-9X+7)}{229} + 0 \\
&\textit{d'où} \\
X^2 - X + 3 &= 0 \times (X^4 + X^3 - 2X + 4) + 1 \times (X^2 - X + 3) \\
-9X + 7 &= 1 \times (X^4 + X^3 - 2X + 4) + (-X^2 - 2X + 1) \times (X^2 - X + 3) \\
\tfrac{229}{81} &= \tfrac{9X-2}{81} \times (X^4 + X^3 - 2X + 4) + \tfrac{-9X^3-16X^2+13X+79}{81} \times (X^2 - X + 3)
\end{aligned}$$

On a ainsi $\text{pgcd}(X^4 + X^3 - 2X + 4, X^2 - X + 3) = 1$, *et :*

$$1 = \frac{9X - 2}{229}(X^4 + X^3 - 2X + 4) + \frac{-9X^3 - 16X^2 + 13X + 79}{229}(X^2 - X + 3).$$

Proposition 52 (Théorème de Gauss)
Soient $A, B, C \in \mathbb{K}[X]$.
Si A *divise* BC *et* $\text{pgcd}(A, B) = 1$, *alors* $A|C$.

Preuve — la preuve est identique au cas des entiers. D'après e théorème de Bézout, il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$. Cela donne $AUC + BVC = C$. Comme $A|BC$, on a $A|(AUC + BCV) = C$. □

3.5 Polynômes irréductibles, décomposition en facteurs irréductibles

Définition 53
Soit $P \in \mathbb{K}[X]$. *On dit que* P *est un* ***polynôme irréductible sur*** $\mathbb{K}$ *si* $deg(P) \geq 1$ *et* P *n'est divible que par ses polynômes associés ou par les polynômes constants.*

Un polynôme irréductible sur $\mathbb{K}$ est donc un polynôme dont les diviseurs sont, à association près, 1 et lui-même. Tout comme un nombre premier est un entier dont les diviseurs sont, au signe près, 1 et lui-même.

Exemple 54 —

1. $X^2 + 1$ *irréductible sur* $\mathbb{R}$ *(écrire la division de* $X^2 + 1$ *par* $X + a$ *et aboutir à une contradiction), mais n'est pas irréductible sur* $\mathbb{C}$ $X^2 + 1 = (X + i)(X - i)$.
2. *Les polynômes de degré* 1, $P(X) = aX + b$, *sont toujours irréductibles (quelque soit le corps* $\mathbb{K}$*).*
3. $X^2 - 2$ *est un polynôme irréductible sur* $\mathbb{Q}$, *mais n'est pas irréductible sur* $\mathbb{R}$ *car* $X^2 - 2 = (X + \sqrt{2})(X - \sqrt{2})$.

Lemme 55 (Théorème d'Euclide)
Soient $A, B, P \in \mathbb{K}[X]$ *avec* P *irréductible.*
Si $P|AB$, *alors* $P|A$ *ou* $P|B$.

Preuve — Supposons que $P \mid AB$.

• Si P divise B, c'est bon.

• Sinon, P ne divise pas A. Comme P est irréductible et comme $\text{pgcd}(A, P)$ divise P on a alors $\text{pgcd}(A, P) = 1$, donc P et A sont premiers entre eux. Le théorème de Gauss nous dit alors que P divise B, ce qui conclut la preuve. □

THÉORÈME 56 (Décomposition en produit de facteurs irréductibles)
Soit $A \in \mathbb{K}[X]$ non-nul.
Alors A se décompose, de manière unique à l'ordre près des termes, en produit de facteurs irréductibles :

$$A(X) = a_n P_1(X)^{\alpha_1} \times P_2(X)^{\alpha_2} \dots P_N(X)^{\alpha_N},$$

où les P_i sont des polynômes irréductibles unitaires deux à deux distincts, les α_i sont des entiers non nuls, et a_n est le coefficient dominant de A.

Preuve — En divisant P par son coefficient dominant, on se ramène à un polynôme unitaire. La preuve (existence, puis unicité) est ensuite identique à celle de la décomposition des entiers en produit de facteurs premiers (voir chapitre Arithmétique). A la place de raisonner par récurrene sur la taille de n, on raisonnera sur le degré de P. en raisonnant sur les degrés. □

EXEMPLE 57 — *Dans $\mathbb{R}[X]$ et $\mathbb{Q}[X]$, le polynôme $X^3 - 1$ se décompose en $X^3 - 1 = (X-1)(X^2+X+1)$. Mais dans $\mathbb{C}[X]$, il se décompose en $X^3 - 1 = (X-1)(X-j)(X-j^2)$.*

PROPOSITION 58
Soit $P \in \mathbb{K}[X]$ de degré ≥ 1. Soit $P = a_n P_1^{\alpha_1} \times \ldots \times P_N^{\alpha_N}$ la décomposition de P en produit de polynômes irréuctibles, avec P_i des polynômes irréductibles unitaires distincts deux à deux et α_i des entiers naturels non nuls.

Alors les diviseurs unitaies de P sont exactement les polynômes de la forme $P_1^{\beta_1} \dots P_N^{\beta_N}$ avec $0 \leq \beta_i \leq \alpha_i$ pour tout $1 \leq i \leq N$.

Le polynôme P possède ainsi $\Pi_{i=1}^N(\alpha_i + 1)$ diviseurs unitaires.

Preuve — La preuve est identique à celle du résultat pour les entiers. (voir Arithmétique) □

EXEMPLE 59 — *Les diviseurs unitaires de $X^3 - 5X + 6 = (X-2)(X-3)$ sont les suivants : 1, $X-2$, $X-3$, $(X-2)(X-3)$.*

PROPOSITION 60
Soient $P, Q \in \mathbb{K}[X]$ de degré ≥ 1. On suppose que $P = a_n P_1^{\alpha_1} \times \ldots \times P_N^{\alpha_N}$ et $Q = b_m P_1^{\beta_1} \times \ldots \times P_N^{\beta_N}$, où les P_i sont des polynômes irréductibles unitaires distincts deux à deux et les α_i, β_i sont des entiers naturels (éventuellement nuls). Alors on a :

- $\text{pgcd}(P,Q) = P_1^{\min(\alpha_1,\beta_1)} \times \ldots \times P_N^{\min(\alpha_N,\beta_N)}$,
- $\text{ppcm}(P,Q) = P_1^{\max(\alpha_1,\beta_1)} \times \ldots \times P_N^{\max(\alpha_N,\beta_N)}$.

Preuve — La preuve est identique à celle du résultat pour les entiers. (voir Arithmétique) □

PROPOSITION 61
Soient $P, Q \in \mathbb{K}[X]$ unitaires. Alors on a

$$\text{pgcd}(P,Q) \times \text{ppcm}(P,Q) = P \times Q.$$

En particulier, si P et Q sont premiers entre eux, on a $\text{ppcm}(P,Q) = PQ$.

Preuve — La preuve est identique à celle pour les entiers. (voir Arithmétique) □

DÉFINITION 62
Soit $P \in \mathbb{K}[X]$ non-nul.
*On dit que P est **scindé** s'il admet autant de racines (comptées avec multiplicité) que son degré.*
Il est équivalent de dire que $P(X) = a_n \prod_{i=1}^r (X - z_i)^{\alpha_i}$, pour des $z_1, \ldots, z_r \in \mathbb{K}$.
*On dit que P est **scindé à racines simples** si le polynôme P est scindé et si toutes ses racines sont distinctes.*
Il est équivalent de dire que $P(X) = a_n \prod_{i=1}^n (X - z_i)$, pour des $z_1, \ldots, z_n \in \mathbb{K}$ distincts.

Exemple 63 — *Le polynôme $X^n - 1$ admet donc n racines dans $\mathbb{C}$. On a vu qu'il ne possède aucune racine double, ce qui montre qu'il existe exactement n racines n-ièmes de l'unité dans $\mathbb{C}$.*

Remarque 64 — *Nous verrons que les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1, et que les polynômes irréductibles de $\mathbb{R}[X]$ sont ceux 1 et ceux de degré 2 de discriminant strictement négatif (c'est-à-dire sans racines réelles). Cela est lié aux propriétés analytiques de $\mathbb{R}$ et de $\mathbb{C}$.*

3.6 Racines d'un polynôme

Définition 65
*Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. On dit que α est une **racine** du polynôme P si l'on a $P(\alpha) = 0$, où $P(\alpha)$ désigne l'image de α par la fonction polynômiale associée à P.*

Proposition 66
Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.
Alors, a est une racine de P si et seulement si $(X - a)|P(X)$.

Preuve — On écrit la division euclidienne de $P(X)$ par $(X-a)$: $P(X) = (X-a)Q(X)+R(X)$ avec $\deg(R) < \deg(X-A) = 1$. $R(X)$ est donc un polynôme constant : $R(X) = \lambda$. L'évaluation en a donne $P(a) = 0.Q(a) + R(a) = \lambda$. Ainsi, a est une racine de P si et seulement si $R(X) = 0$, si et seulement si $(X - a)$ divise $P(X)$. □

Définition 67
*Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$, et $k \geq 1$. On dit que a est une racine de **multiplicité** k de P si l'on a $(X-\alpha)^k|P$ et $(X - a)^{k+1} \not| P$.*
Une racine de multiplicité 1 est appelée racine simple de P.

Proposition 68
Soient $P \in \mathbb{K}[X]$ et $a_1, \ldots, a_r \in \mathbb{K}$, tels que $a_1, \ldots, a_r$ sont des racines de P de multiplicités respectives α_1, ...,α_r. Alors il existe $Q \in \mathbb{K}[X]$ tel que :

$$P = (X - a_1)^{\alpha_1} \ldots (X - a_r)^{\alpha_r} Q \qquad et \qquad Q(a_i) \neq 0, \forall 1 \leq i \leq r.$$

Preuve — Les polynômes $(X - a_i)$ sont irréductibles. On utilise alors le théorème de décomposition en facteurs irréductibles pour obtenir une telle décomposition. De plus, si $Q(a_i) = 0$ pour un $1 \leq i \leq r$, alors a_i est une racine de Q et donc une racine de multiplicité au moins $\alpha_i + 1$ de P. Donc aucun des a_i n'est racine de Q. □

Corollaire 69
Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ de degré $n \geq 0$.
Alors P possède au plus n racines, comptées avec leur multiplicité.

Preuve — Dans la proposition précédente, on a $\deg(P) = n = a_1 + \ldots + a_r + \deg(Q)$. D'où $a_1 + \ldots + a_r \leq n$. □

Proposition 70
Soit $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$ (plus généralement un corps avec un nombre infini d'éléments). Alors la fonction $\psi : P \in \mathbb{K}[X] \mapsto (x \mapsto P(x)) \in \mathcal{F}(\mathbb{K}, \mathbb{K})$ est injective.

Preuve — On a déjà vu que ψ est une application linéaire. $\mathrm{Ker}(\psi)$ est l'ensemble des polynômes qui admettent tous les éléments de $\mathbb{K}$ comme racine. Comme $\mathbb{K}$ a un nombre infini d'éléments, aucun polynôme non-nul ne peut posséder autant de racines d'après le corollaire précédent. On a donc $\mathrm{Ker}(\psi) = \{0\}$, donc ψ est injective. □

Remarque 71 — *Cette proposition prouve que deux fonctions polynomiales sont égales sur $\mathbb{K}$ si et seulement si leurs polynômes associés ont les mêmes coefficients.*
Ainsi, par exemple, $P : x \in \mathbb{R} \mapsto x^7 + 5x^4 + 1 \in \mathbb{R}$ n'est pas du tout la même fonction que $Q : x \in \mathbb{R} \mapsto x^7 + 5x^2 + 1 \in \mathbb{R}$.
De telles fonctions ne sont égales qu'en au plus 4 points (on a $P(x) = Q(x)$ ssi $(P - Q)(x) = 0$, et

$\deg(P-Q)=4$*).*

Si $\mathbb{K}$ est un corps avec un nombre fini d'éléments (nous en verrons en Algèbre 2), l'ensemble $\mathcal{F}(\mathbb{K},\mathbb{K})$ a $Card(\mathbb{K})^{Card(\mathbb{K})}$ fonctions, alors que $\mathbb{K}[X]$ possède une infinité de polynômes. La fonction $\varphi : P \mapsto (x \mapsto P(x))$ ne peut ainsi pas être injective.

3.7 Dérivation dans $\mathbb{K}[X]$

3.7.1 Dérivée d'un polynôme

Définition 72
Soit $P \in \mathbb{K}[X]$ avec $P = a_nX^n + \ldots + a_0$. On appelle ***polynôme dérivé*** *de P, noté P', le polynôme :*

$$P'(X) = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \ldots + a_1.$$

Remarque 73 — *On a $na_n = \underbrace{a_n + \ldots + a_n}_{n}$. Si $\mathbb{K}$ contient $\mathbb{Z}$, alors $na_n = n \times a_n$. Pour $n \geq 1$ et $a_n \neq 0$, ce coefficient est donc non nul, d'où $\deg(P') = n-1$.*
Dans ce chapitre, nous travaillons avec les corps $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, qui contiennent $\mathbb{Z}$. Mais nous verrons au cours Algèbre 2 d'autres corps qui ne contiennent pas $\mathbb{Z}$. (si le corps $\mathbb{K}$ ne contient pas $\mathbb{Z}$, il se peut que l'on ait $a_n \neq 0$ et $na_n = 0$)

Proposition 74
Soit $\mathbb{K}$ un corps tel que $\mathbb{K}$ contient $\mathbb{Z}$. Soit $P \in \mathbb{K}[X]$. On a $\deg(P') = \deg(P) - 1$ si $\deg(P) \geq 1$, et $P'(X) = 0$ sinon.

Proposition 75
Soit $\mathbb{K}$ un corps. La fonction $D : P \in \mathbb{K}[X] \mapsto P' \in \mathbb{K}[X]$ est une application linéaire.
Si $\mathbb{K}$ contient $\mathbb{Z}$, alors $\mathrm{Ker}(D) = \{\lambda,\ \lambda \in \mathbb{K}\}$ l'ensemble des polynômes constants.

Preuve — Soient $P, Q \in \mathbb{K}[X]$, $\lambda \in \mathbb{K}$. Par définition de $P \mapsto P'$ on a $(P + \lambda Q)' = P' + \lambda Q'$.
Lorsque $\mathbb{K}$ contient $\mathbb{Z}$, on a vu que les seuls polynôme dont le polynôme dérivé est nul sont les polynômes constants. □

Proposition 76 (Formules de dérivation)
Soient $P, Q \in \mathbb{K}[X]$, $\lambda \in \mathbb{K}$, $m \geq 1$. On a :

1. $(\lambda P)'(X) = \lambda P'(X)$;
2. $(P+Q)'(X) = P'(X) + Q'(X)$ *(dérivée d'une somme) ;*
3. $(PQ)'(X) = P'(X)Q(X) + P(X)Q'(X)$ *(dérivée d'un produit) ;*
4. $(P^m)'(X) = mP'(X)P(X)^{m-1}$ *(dérivée d'une puissance) ;*
5. $(P \circ Q)'(X) = Q'(X).(P' \circ Q)(X)$ *(dérivée d'une composée).*

Preuve — Les points 1) et 2) ont déjà été démontrés. 3) Soit $Q \in \mathbb{K}[X]$. Les fonctions $P \mapsto (PQ)'$ et $P \mapsto P'Q + PQ'$ sont des applications linéaires. On vérifie alors que ces applications liénaires coïncident sur une base de $\mathbb{K}[X]$.

On pose $Q(X) = a_0 + a_1X + \ldots + a_nX^n$. Soit $m \geq 0$. Pour $P(X) = X^m$, on a :

$$\begin{aligned}(PQ)'(X) &= (a_0X^m + \ldots + a_nX^{m+n})' = ma_0X^{m-1} + (m+1)a_1X^m \ldots + (m+n)a_nX^{m+n-1}\\ &= ma_0X^{m-1} + ma_1X^m + \ldots + ma_nX^{m+n-1} + 0 + a_1X^m + 2a_2X^{m+1} + \ldots + na_nX^{m+n-1}\\ &= (mX^{m-1})(a_0 + a_1X + \ldots + a_nX^n) + X^m(a_1 + 2a_2X + \ldots + na_nX^{n-1}) = P'(X)Q(X) + P(X)Q'(X).\end{aligned}$$

Comme la famille $\{X^m,\ m \geq 0\}$ est une base de $\mathbb{K}[X]$, par linéarité, cette égalité est donc vraie pour tout $P \in \mathbb{K}[X]$.
4) On démontre cette relation par récurrence sur $m \geq 1$ à l'aide de 3).

5) Soit $Q \in \mathbb{K}[X]$. Les fonctions $P \mapsto (P \circ Q)'$ et $P \mapsto Q' \times (P' \circ Q)$ sont des applications linéaires. On vérifie que ces applications linéaires coïncident sur une base de $\mathbb{K}[X]$.

On pose $Q(X) = a_0 + a_1X + \ldots + a_nX^n$. Soit $m \geq 0$. On pose $P(X) = X^m$. Si $m = 0$ on a $(P \circ Q)(X) = 1$, donc $(P \circ Q)' = 0$ et $Q' \times (P' \circ Q) = 0$.
Si $m \geq 1$, on a $(P \circ Q)'(X) = (Q^m)'(X) = mQ'(X)Q(X)^{m-1} = Q'(X) \times (P' \circ Q)(X)$. Comme $\{X^m,\ m \geq 0\}$ est une base de $\mathbb{K}[X]$, cela conclut la preuve. □

PROPOSITION 77
Soient $\mathbb{K} = \mathbb{R}$ et $P \in \mathbb{R}[X]$. Soient $f_P : x \mapsto P(x)$ et $f_{P'} : x \mapsto P'(x)$ les fonctions polynômiales associées à P et P'. Alors on a $f_{P'} = (f_P)'$.

REMARQUE 78 — *Dans le cadre des fonctions, la notion de dérivée a un sens sur $\mathbb{R}$. Ainsi, on peut identifier la dérivée d'un polynôme réel à la dérivée de sa fonction polynômiale associée. Pour tout corps $\mathbb{K}$, l'opération de dérivation des polynômes de $\mathbb{K}[X]$ est bien définie, mais pour un corps comme $\mathbb{C}$, dériver une fonction $f : \mathbb{C} \to \mathbb{C}$ n'a pas de sens pour le moment. Il ne faudra donc pas confondre en général polynôme dérivé (qui existe) et dérivée de la fonction polynômiale (qui n'existe pas forcément).*

3.7.2 Formule de Taylor

PROPOSITION 79
Soient $\alpha \in \mathbb{K}$, $n \geq 1$, $k \geq 0$. On pose $P(X) = (X - \alpha)^n$. En notant $P^{(k)}$ le polynôme dérivé k-ième de P, on a :

$$P^{(k)}(X) = \frac{n!}{(n-k)!}(X-\alpha)^{n-k} \text{ si } 0 \leq k \leq n, \text{ et } P^{(k)}(X) = 0 \text{ si } k > n.$$

On en déduit que $P^{(n)}(X) = n!$, et que $P^{(k)}(\alpha) = 0$ si $k \neq n$.

Preuve — On démontre le résultat par récurrence sur k. □

THÉORÈME 80 (Formule de Taylor pour les polynômes)
Soit $\mathbb{K}$ un corps contenant $\mathbb{Z}$. Soient $a \in \mathbb{K}$ et $P \in \mathbb{K}[X]$ de degré n. On a l'égalité suivante :

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k = P(a) + \frac{P'(a)}{1!}(X-a) + \ldots + \frac{P^{(n)}(a)}{n!}(X-a)^n.$$

Preuve — Soit $P \in \mathbb{K}[X]$ de degré n. On considère la fonction :

$$\varphi : \begin{array}{ccc} \mathbb{K}_n[X] & \to & \mathbb{K}_n[X] \\ Q & \mapsto & \displaystyle\sum_{k=0}^{n} Q^{(k)}(a)\frac{(X-a)^k}{k!} \end{array}$$

Les applications $Q \mapsto Q^{(k)}$ et $Q \mapsto Q(a)$ sont linéaires, donc φ est linéaire comme somme et composée d'apllication linéaires. Montrons que l'on a $\varphi(P) = P$. Comme φ et $Id_{\mathbb{K}_n[X]}$ sont linéaires, il suffit de montrer cela pour une base de $\mathbb{K}_n[X]$.
Pour $0 \leq i \leq n$, on pose $Q_i(X) = \dfrac{(X-a)^i}{i!}$. La famille $\{Q_0, Q_1, \ldots, Q_n\}$ est échelonnée en degré, c'est donc une base de $\mathbb{K}_n[X]$. De plus, on a $Q_i(a) = 1$ si $i = 0$ et $Q_i(a) = 0$ sinon.
On calcule :

$$Q_0'(X) = 0 \text{ et } Q_i'(X) = \left(\frac{(X-a)^i}{i!}\right)' = \frac{(X-a)^{i-1}}{(i-1)!} = Q_{i-1}(X), \ \forall i \in [\![1, n]\!].$$

On en déduit que $Q_i^{(k)}(X) = Q_{i-k}(X)$ si $0 \leq k \leq i$, et $Q_i^{(k)}(X) = 0$ si $k > i$. Ainsi, on a :

$$\begin{aligned} \varphi(Q_i)(X) &= \sum_{k=0}^{n} Q_i^{(k)}(\alpha)\frac{(X-a)^k}{k!} = \sum_{k=0}^{i} Q_{i-k}(\alpha)\frac{(X-a)^k}{k!} \\ &= 1 \times \frac{(X-a)^i}{i!} + 0 \text{ car } \ Q_i(a) = \delta_{i,0} \\ &= \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad Q_i \end{aligned}$$

On a donc $\varphi = Id_{\mathbb{K}_n[X]}$ par linéarité. Cela donne $\varphi(P) = P$, ce qui conclut. □

REMARQUE 81 — *Nous avons montré que $\{Q_0, Q_1, \ldots, Q_n\}$ est une base de $\mathbb{K}_n[X]$. Pour P un polynôme de degré au plus n, la formule de Taylor nous dit alors que les coordonnées de P dans cette base $(P(a), P'(a), \ldots, P^{(n)}(a))$.*

EXEMPLE 82 — *On a* $X^2 - 10X + 1 = 1 + \frac{10}{1}(X-10) + \frac{2}{2}(X-10)^2 = 1 + 10(X-10) + (X-10)^2$.
Appliquer la fomule de Taylor à

1. $X^3 + X^2 + X + 1$ *et* $\alpha = 1$;
2. $2X^4 + 2X + 1$ *et* $\alpha = -1$.

3.7.3 Caractérisation des racines multiples

PROPOSITION 83 (Caractérisation des racines simples)
Soient $\mathbb{K}$ *un corps,* $a \in \mathbb{K}$, *et* $P \in \mathbb{K}[X]$.
L'élément a *est une racine simple du polynôme* P *si et seulement si* $P(a) = 0$ *et* $P'(a) \neq 0$.

Preuve — Si P admet une racine b de multiplicité $k \geq 1$, on a alors $P(X) = (X-b)^k.Q(X)$, avec $Q(b) \neq 0$. En dérivant, on obtient : $P'(X) = (X-b)^k Q'(X) + k(X-b)^{k-1}Q(X)$.

Supposons que a est une racine simple de P. On a donc $P(a) = 0$ et $P'(X) = (X-a)Q'(X) + 1.Q(X)$. Cela donne $P'(a) = 0 + Q(a) \neq 0$.

Réciproquement, supposons que $P(a) = 0$ et $P'(a) \neq 0$. Alors a est une racine de P. Soit k la multiplicité de a. Si $k > 1$, alors le polynôme $(X-a)^{k-1}$ s'annule en a, et on obtient : $P'(a) = (a-a)Q'(a) + k(a-a)^{k-1}Q(a) = 0$. Comme on a $P'(a) \neq 0$, a est donc de multiplicité 1. □

PROPOSITION 84 (Caractérisation des racines multiples)
Soit $\mathbb{K}$ *un corps contenant* $\mathbb{Z}$. *Soient* $a \in \mathbb{K}$, $k \geq 1$, *et* $P \in \mathbb{K}[X]$.
Alors a *est une racine de* P *de multiplicité* k *si et seulement si* $P(a)$, $P'(a)$,...,$P^{(k-1)}(a) = 0$ *et* $P^{(k)}(a) \neq 0$.

Preuve — C'est une conséquence immédiate de la formule de Taylor. En écrivant

$$P = P(a) + \frac{P'(a)}{1!}(X-a) + \ldots + \frac{P^{(i)}}{n!}(X-a)^i + \ldots + \frac{P^{(n)}}{n!}(X-a)^n,$$

on peut remarquer que $P(X)$ est un multiple de $(X-a)^k$ mais pas de $(X-a)^{k+1}$ si et seulement si $P(a)$,$P'(a), \ldots, P^{(k-1)}(a) = 0$ et $P^{(k)}(a) \neq 0$. □

REMARQUE 85 — *Le critère de caractérisation des racines simples est vrai dans tout corps* $\mathbb{K}$, *tandis que celui des racines multiples n'est vrai que dans un corps* $\mathbb{K}$ *contenant* $\mathbb{Z}$.

EXEMPLE 86 — *Dans* $\mathbb{C}[X]$, *le polynôme* $P = X^n - 1$ *n'admet que des racines simples, puisque* $P' = nX^{n-1}$ *n'admet pas de racine commune avec* P.

PROPOSITION 87 (Caractérisation des facteurs multiples)
Soient $\mathbb{K}$ *un corps contenant* $\mathbb{Z}$ *et* $P \in \mathbb{K}[X]$. *Soit* $P(X) = a_n P_1(X)^{\alpha_1} \times P_2(X)^{\alpha_2} \ldots P_N(X)^{\alpha_N}$ *sa décomposition en produit de facteurs irréductibles, avec* P_i *irréductibles distincts.*
Alors, on a $\text{pgcd}(P, P') = P_1(X)^{\alpha_1 - 1} \times P_2(X)^{\alpha_2 - 1} \ldots P_N(X)^{\alpha_N - 1}$.
Ainsi, P *est à facteurs irréductibles simples* ($\alpha_1 = \ldots = \alpha_N = 1$) *si et seulement si* $\text{pgcd}(P, P') = 1$.

Preuve — Le polynôme $\text{pgcd}(P, P')$ est un diviseur de P'. Ses facteurs irréductibles, s'il en possède, sont donc parmi les facteurs irréductibles de P, $P_1, \ldots, P_N$.
Soit $1 \leq i \leq N$. On a $P = P_i^{\alpha_i}.Q$, avec $Q \in \mathbb{K}[X]$ tel que $\text{pgcd}(P_i, Q) = 1$. En dérivant cette relation, on obtient :

$$P' = P_i'.P_i^{\alpha_i - 1}.Q + P_i^{\alpha_i}.Q'.$$

Comme P_i est irréductible on a $\deg(P_i) \geq 1$. Comme $\mathbb{K}$ contient $\mathbb{Z}$ on a alors $P_i' \neq 0$. Le polynôme P_i' est alors premier avec P_i. Ainsi, P' est un multiple de $P_i^{\alpha_i - 1}$ mais pas de $P_i^{\alpha_i}$.

Avec les propriétés du pgcd, on en conclut que P_i est un facteur irréductible de $\text{pgcd}(P, P')$ de multiplicité $\alpha_i - 1$. Cela donne donc $\text{pgcd}(P, P') = P_1(X)^{\alpha_1 - 1} \ldots P_N(X)^{\alpha_N - 1}$. Enfin, on a $\text{pgcd}(P, P') = 1$ si et seulement si $\alpha_1 = \ldots = \alpha_n = 1$. □

EXEMPLE 88 — *Pour* $P(X) = X^4 + 3X^2 + 1 \in \mathbb{Q}[X]$, *on a* $P'(X) = 4X^3 + 6X$. *Le calcul donne* $\text{pgcd}(P, P') = 1$. *Ainsi,* P *est un polynôme à facteurs premiers dans* $\mathbb{Q}[X]$. *(idem pour* $\mathbb{R}$ *et* $\mathbb{C}$*)*

Pour $P \in \mathbb{Q}[X]$

REMARQUE 89 — *Pour $P \in \mathbb{K}[X]$ avec $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, en calculant P' puis $\text{pgcd}(P, P')$, ce qui se fait très bien avec l'algorithme d'Euclide, on obtient ainsi un diviseur de P. Si P a un facteur irréductible de multiplicité au moins 2, on a $\text{pgcd}(P, P') \neq 1$, donc ce diviseur est non-trivial.*

On peut ensuite effectuer la division euclidienne de P par $\text{pgcd}(P, P')$ pour obtenir le polynôme $Q = P_1 \dots P_N$.

3.7.4 Théorème de Rolle pour les polynômes réels

On rappelle les deux résultats d'analyse suivants, qui sont utiles pour étudier les polynômes à coefficients réels.

PROPOSITION 90 (Théorème des valeurs intermédiaires)
Soit $I = [a, b]$ un intervalle de $\mathbb{R}$. Soit $f : [a, b] \to \mathbb{R}$ une fonction continue sur $[a, b]$.
• Si $f(a) \neq f(b)$, pour tout $d \in]f(a), f(b)[$, il existe $c \in]a, b[$ tel que $f(c) = d$.
• Si $f(a) < 0$ et $f(b) > 0$ (ou $f(a) > 0$ et $f(b) < 0$), alors il existe $c \in]a, b[$ tel que $f(c) = 0$.

PROPOSITION 91 (Théorème de Rolle)
Soit $I = [a, b]$ un intervalle de $\mathbb{R}$. Soit $f : [a, b] \to \mathbb{R}$ une fonction continue sur $[a, b]$ et dérivable sur $]a, b[$.
Si $f(a) = f(b)$, alors il existe $c \in]a, b[$ tel que $f'(c) = 0$.

COROLLAIRE 92
Soit $P \in \mathbb{R}[X]$.
• Soient a, b deux racines de P distinctes.
Alors il existe $c \in]a, b[$ tel que $P'(c) = 0$ (c est une racine de P).
• Si P possède r racines distinctes $a_1 < a_2 < \dots < a_r$, alors le polynôme P' possède au moins $r - 1$ racines $b_1, \dots, b_{r-1}$ telles que $b_i \in]a_i, a_{i+1}[$.
P' possède donc au moins $r - 1$ racines distinctes qui ne sont pas des racines de P.

Preuve — On utilise le théorème de Rolle à P sur chaque intervalle $[a_i, a_{i+1}]$. □

REMARQUE 93 — *Soit $P \in \mathbb{R}[X]$ non-constant. On peut alors utiliser les résultats précédents pour avoir beaucoup d'informations sur P'.*
On factorise P dans $\mathbb{R}[X]$:
• $P(X) = a_n \Pi_{i=1}^{r} (X - a_i)^{\alpha_i} Q(X)$, avec $a_1 < a_2 < \dots < a_r$, $\alpha_i \in \mathbb{N}^*$, et Q un polynôme sans racines.
On sait que $\Pi_{i=1}^{r} (X - a_i)^{\alpha_i - 1}$ divise $P'(X)$, et qu'il existe $r - 1$ nombres réels $b_1 < \dots < b_{r-1}$ avec $b_i \in]a_i, a_{i+1}[$ qui sont des racines de P'.
• On a donc $P'(X) = \Pi_{i=1}^{r} (X - a_i)^{\alpha_i - 1} \Pi_{j=1}^{r-1} (X - b_j) R(X)$, avec $R \in \mathbb{R}[X]$ un polynôme.
Pour $\deg(P) = n \geq 1$ on a $\deg(P') = n - 1$. On a aussi $\deg(\Pi_{i=1}^{r} (X - a_i)^{\alpha_i - 1} \Pi_{j=1}^{r-1} (X - b_j)) = \sum_{i=1}^{r} (\alpha_i - 1) + \sum_{j=1}^{r-1} 1 = \sum_{i=1}^{r} \alpha_i - 1$.

REMARQUE 94 — *Pour $P \in \mathbb{R}[X]$, le théorème de Rolle permet de trouver des racines de P'.*
Il ne dit pas comment calculer la valeur des racines $b_1, \dots, b_{r-1}$, mais on a des informations sur le nombre de racines distinctes de P' et sur leur position.
Cela est très important dans l'étude des polynômes réels/complexes comme fonctions, pour savoir sur quels intervalles le polynôme prend des valeurs positives/négatives/nulles.

COROLLAIRE 95
Soit $P \in \mathbb{R}[X]$ un polynôme scindé et non-constant.
Alors P' est scindé.
De plus, si P est scindé à racines simples alors P' est scindé à racines simples.

Preuve — On écrit $P(X) = a_n \Pi_{i=1}^{r} (X - a_i)^{\alpha_i}$, avec $a_1 < a_2 < \dots < a_r$, $\alpha_i \in \mathbb{N}^*$.
D'après la remarque précédente, pour tout $1 \leq i \leq r - 1$ il existe $b_i \in]a_i, a_{i+1}[$ qui est une racine de P', et $\Pi_{i=1}^{r} (X - a_i)^{\alpha_i - 1}$ divise P'.
Le polynôme $\Pi_{i=1}^{r} (X - a_i)^{\alpha_i - 1} \Pi_{j=1}^{r-1} (X - b_j)$ est de degré $\deg(P) - r + (r - 1) = \deg(P) - 1 = \deg(P')$.

D'après les propriétés de la divisibilité, on a donc $P'(X) = b\Pi_{i=1}^{r}(X-a_i)^{\alpha_i-1}\Pi_{j=1}^{r-1}(X-b_j)$.
Le polynôme P' est donc bien scindé.
De plus, P' est scindé à racines simples si et seulement si les racines de P sont de multiplicité 1 ou 2. Cela termine la preuve. □

3.8 Polynômes irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$

Factorisation dans $\mathbb{C}[X]$

On admettra le théorème fondamental suivant :

Théorème 96 (Théorème de D'alembert-Gauss)
Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine.

Corollaire 97
Soit $P \in \mathbb{C}[X]$ de degré $n \geq 1$. Alors P se décompose en :

$$P = a_n \prod_{i=1}^{r}(X-z_i)^{\alpha_i},$$

où $\alpha_1, \ldots, \alpha_r$ sont des entiers non nuls et $z_1, \ldots, z_r$ sont des nombres complexes deux à deux distincts. Cette décomposition est unique à l'ordre des z_i près.

Preuve — On écrit la décomposition en facteurs premiers de P : $P = a_n P_1^{\alpha_1} \ldots P_l^{\alpha_l}$ où les P_l sont des polynômes irréductibles de $\mathbb{C}[X]$ et unitaires.

D'après le théorème de D'alembert-Gauss, si P_i est irréductible alors il a une racine z_i et donc est divisible par $X - z_i$. Comme P_i est unitaire et irréductible, on a donc $P_i(X) = (X - z_i)$, d'où le résultat. □

Remarque 98 — *On peut formuler le corollaire en disant que les polynômes irréductibles dans $\mathbb{C}$ sont exactement les polynômes de degré 1, ou encore en disant que tout polynôme $P \in \mathbb{C}[X]$ se décompose en un produit de polynômes de degré 1.*

Factorisation dans $\mathbb{R}[X]$

La situation dans $\mathbb{R}$ est relativement différente, comme nous allons le prouver.

Lemme 99
Soit $P \in \mathbb{R}[X]$. Soit $\alpha \in \mathbb{C} \setminus \mathbb{R}$ une racine complexe de P. Alors, $\bar{\alpha}$ est aussi une racine de P.

Preuve — On écrit $P = a_n X^n + \ldots + a_0$ avec $a_i \in \mathbb{R}$. Alors, on a :

$$P(\bar{\alpha}) = a_n\bar{\alpha}^n + \ldots + a_1\bar{\alpha} + a_0 = \overline{a_n\alpha^n + \ldots + a_1\alpha + a_0} = \overline{P(\alpha)} = 0.$$

Donc $\bar{\alpha}$ est bien une racine de P. □

Proposition 100
Les polynômes irréductibles de $\mathbb{R}[X]$ sont :

1. *Les polynômes de degré 1, $\lambda(X-\beta)$, avec $\lambda \neq 0$;*
2. *Les polynômes de degré 2, $aX^2 + bX + c$, avec $b^2 - 4ac < 0$.*

Preuve — Soit $P \in \mathbb{R}[X]$ un polynôme irréductible. On a :

1. Si P possède une racine réelle a, alors $X - a$ divise P. Comme P est irréductible, on a donc $P(X) = \lambda(X-a)$ avec $\lambda \neq 0$;
2. Sinon, le polynôme P possède une racine $\alpha \in \mathbb{C} \setminus \mathbb{R}$ d'après le théorème de D'Alembert-Gauss. Le polynôme $(X-\alpha)(X-\bar{\alpha}) = X^2 - (\alpha+\bar{\alpha})X + \alpha\bar{\alpha}$ est à coefficients réels. D'après la proposition précédente, ce polynôme divise P. On a donc $P = \lambda(X^2 - (\alpha+\bar{\alpha})X + \alpha\bar{\alpha})$, et le discriminant est bien sûr négatif.

□

Exemple 101 —

1. *Le polynôme X^3+1 n'est pas irréductile dans $\mathbb{R}[X]$ car -1 est une racine. Il se décompose en $X^3+1=(X+1)(X^2-X+1)$.*
2. *X^4+1 n'a pas de racines sur $\mathbb{R}$ mais n'est pas irréductible. Sa décomposition est :*
$$X^4+1=(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1).$$
3. *Tout polynôme réel P de degré impair admet au moins une racine réelle. (Pourquoi ?)*

Corollaire 102
Soit $P\in\mathbb{R}[X]$ de degré $n\geq 1$. Alors P se décompose en :
$$P=a_n\prod_{i=1}^{r}(X-c_i)^{\alpha_i}\times\prod_{j=1}^{m}(X^2+c_jX+d_j)^{\beta_j},$$
où $\alpha_1,\dots,\alpha_r,\beta_i,\dots,\beta_m$ sont des entiers non nuls, les b_i sont distincts, les (c_j,d_j) sont distincts, avec $c_j^2-4d_j<0$. Cette décomposition est unique à l'ordre l'ordre des b_i et des (c_j,d_j) près.

Remarque 103 — *La situation est infiniment plus délicate dans $\mathbb{Q}[X]$. Par exemple, pour $P(X)=X^4+1$, les racines complexes de P sont $\exp(\frac{i\pi}{4})$,$\exp(\frac{3i\pi}{4})$,$\exp(\frac{5i\pi}{4})$, et $\exp(\frac{7i\pi}{4})$.*
Ce polynôme est réductible dans $\mathbb{R}[X]$ car
$$X^4+1=X^4+2X^2+1-2X^2=(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1).$$
Les polynômes de droite sont de discriminant -1, et sont donc irréductibles.
Si P était réductible dans $\mathbb{Q}[X]$, on aurait $P=QR$, avec $Q,R\in\mathbb{Q}[X]$ non-constants. On aurait donc $P=QR$ dans $\mathbb{R}[X]$, donc $Q(X)=X^2\pm\sqrt{2}X+1$. Mais $\sqrt{2}$ est irrationnel, donc un tel polynôme n'est pas à coefficients rationnels. Ainsi, P est irréductible dans $\mathbb{Q}[X]$.

3.9 Relations entre coefficients et racines

3.9.1 Fonctions symétriques élémentaires

Définition 104
Soient $\mathbb{K}$ un corps et $n\in\mathbb{N}$, $n\geq 2$. Soit $1\leq p\leq n$. On définit la p-ième fonction symétrique à n variables comme :
$$\sigma_p:\begin{array}{ccc}\mathbb{K}^n & \to & \mathbb{K}\\ (\alpha_1,\dots,\alpha_n) & \mapsto & \sum_{i_1<i_2<\dots<i_p}\alpha_{i_1}\dots\alpha_{i_p}\end{array}.$$

Exemple 105 — *On retiendra surtout les cas suivants :*

1. *Si $p=1$, $\sigma_1(\alpha_1,\dots,\alpha_n)=\alpha_1+\dots+\alpha_n$.*
2. *Si $p=n$, $\sigma_n(\alpha_1,\dots,\alpha_n)=\alpha_1\dots\alpha_n$.*
3. *Si $n=2$, $\sigma_1(\alpha_1,\alpha_2)=\alpha_1+\alpha_2$ et $\sigma_2(\alpha_1,\alpha_2)=\alpha_1\alpha_2$.*
4. *Si $n=3$,*
   (a) *$\sigma_1(\alpha_1,\alpha_2,\alpha_3)=\alpha_1+\alpha_2+\alpha_3$;*
   (b) *$\sigma_2(\alpha_1,\alpha_2,\alpha_3)=\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3$;*
   (c) *$\sigma_3(\alpha_1,\alpha_2,\alpha_3)=\alpha_1\alpha_2\alpha_3$.*

Remarque 106 —

1. *Dans la définition, on somme donc les produits $\alpha_{i_1}\dots\alpha_{i_p}$, où les i_k sont p entiers deux à deux distincts à choisir dans $\{1,\dots,n\}$. Il y a donc $\binom{n}{p}$ termes dans la somme.*
2. *Les polynômes $\sigma_i(\alpha_1,\dots,\alpha_n)$ sont dits symétriques, car changer l'ordre des α_k ne change pas la valeur de $\sigma_i(\alpha_1,\dots,\alpha_n)$.*

3.9.2 Relations entre fonctions symétriques élémentaires et coefficients

EXEMPLE 107 — *On obtient facilement les relations suivantes :*

1. *Soit* $P = X^2 + aX + b = (X - \alpha_1)(X - \alpha_2)$. *Alors on a :* $\begin{cases} \sigma_1(\alpha_1, \alpha_2) = \alpha_1 + \alpha_2 = -a \\ \sigma_2(\alpha_1, \alpha_2) = \alpha_1\alpha_2 = b \end{cases}$
2. *Soit* $P = X^3 + a_2X^2 + a_1X + a_0 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$. *Alors on a :*
   (a) $\sigma_1(\alpha_1, \alpha_2, \alpha_3) = \alpha_1 + \alpha_2 + \alpha_3 = -a_2$;
   (b) $\sigma_2(\alpha_1, \alpha_2, \alpha_3) = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = a_1$;
   (c) $\sigma_3(\alpha_1, \alpha_2, \alpha_3) = \alpha_1\alpha_2\alpha_3 = -a_0$.

PROPOSITION 108
Soit $P \in \mathbb{K}[X]$ *un polynôme de degré* n *qui est scindé. Soient* $\alpha_1, \ldots, \alpha_n$ *les racines de* P *comptées avec multiplicité. Pour* $P(X) = a_nX^n + \ldots + a_0$ *et* $P(X) = a_n \prod_{i=1}^{n}(X - \alpha_i)$, *on a :*

$$\sigma_p(\alpha_1, \ldots, \alpha_n) = (-1)^p \frac{a_{n-p}}{a_n}, \ \forall p \in \{1, \ldots, n\}.$$
$$a_p = (-1)^{n-p} a_n \sigma_{n-p}(\alpha_1, \ldots, \alpha_n), \ \forall p \in \{1, \ldots, n\}.$$

Preuve — Il faut développer le produit $P = a_n \prod_{i=1}^{n}(X - \alpha_i)$ et identifier les coefficients pour obtenir ces relations. □

REMARQUE 109 (Détermination des racines d'un polynôme) — *Soit* $P \in \mathbb{K}[X]$.

• *Si* P *est de degré* 1, *on a* $P(X) = \lambda(X - \alpha)$ *et il n'y a rien à étudier.*

• *Si* P *est de degré* 2, *on a* $P(X) = aX^2 + bX + c$. *Le discriminant* $\Delta = b^2 - 4ac$ *permet de dire si* P *possède ou non des racines dans le corps* $\mathbb{K}$, *et de donner l'expression de ces racines en fonction de* a, b, c. *Ces expressions utilisent* $+, \times, -, \frac{1}{\cdot}$ *et* $\sqrt{\cdot}$.

• *Si* P *est de degré* 3, *il existe des formules appelées formules de Cardan qui permettent de dire si* P *possède ou non des racines dans le corps* $\mathbb{K}$, *et de donner l'expression de ces racines en fonction des coefficients* $a_0, \ldots, a_3$. *Ces expressions utilisent* $+, \times, -, \frac{1}{\cdot}$, $\sqrt{\cdot}$ *et* $\sqrt[3]{\cdot}$, *et sont un peu lourdes.*

• *Si* P *est de degré* 4, *il existe des formules appelées formules de Cardan qui permettent de dire si* P *possède ou non des racines dans le corps* $\mathbb{K}$, *et de donner l'expression de ces racines en fonction des coefficients* $a_0, \ldots, a_4$. *Ces expressions utilisent* $+, \times, -, \frac{1}{\cdot}$, $\sqrt{\cdot}$, $\sqrt[3]{\cdot}$ *et* $\sqrt[4]{\cdot}$, *et sont très lourdes.*

• *Si* P *est de degré* 5, *il n'existe aucune formule générale utilisant* $+, \times, -, \frac{1}{\cdot}$, *et* $\sqrt[n]{\cdot}$ $\forall n \geq 2$, *qui permet de dire si* P *possède des racines dans le corps* $\mathbb{K}$, *ni d'exprimer les racines de* P *en fonction des coefficients* $a_0, \ldots, a_5$.
Autrement dit, il existe des polynômes P *de degré* 5 *dans* $\mathbb{R}[X]$ *ou* $\mathbb{C}[X]$ *tels que leurs racines ne sont égales à aucune expression algébrique utilisant les opérations* $+, \times, -, \frac{1}{\cdot}$, *et* $\sqrt[n]{\cdot}$ $\forall n \geq 2$ *et les coefficients* $a_0, \ldots, a_5$. *Cela est par exemple le cas pour* $P(X) = X^5 - 6X + 3$.
On peut estimer les racines de ce polynôme dans $\mathbb{R}$ *ou* $\mathbb{C}$ *à l'aide d'algorithmes (trouver les lieux où* $P(x)$ *est aussi proche de* 0 *que l'on veut), mais cela est moins efficace que de calculer des valeurs approchées de sommes/produits/quotients de racines* n*-èmes de nombres rationnels.*

- *Ainsi, si l'on vous demande de déterminer les racines d'un polynôme* P *de degré* 3 *ou plus, vous aurez forcément des racines évidentes, des relations algébriques, ou des propriétés supplémentaires pour déterminer des racines de* P *et vous ramener à un polynôme de degré* 2 *ou* 1.

3.9.3 Exemples d'applications

Résolution de systèmes à deux inconnues

EXEMPLE 110 — *On veut résoudre le système* $\begin{cases} x+y &= -3 \\ xy &= 2 \end{cases}$

On remarque qu'un couple $(x,y)=(\alpha_1,\alpha_2)$ *est solution du système si et seulement si* α_1 *et* α_2 *sont racines du polynôme* X^2+3X+1 *(prendre* $\sigma_1(\alpha_1,\alpha_2)=3$ *et* $\sigma_2(\alpha_1,\alpha_2)=2$*). Or, les racines de ce polynômes sont* -1 *et* -2*, donc l'ensemble des couples solutions est* $\{(-1,-2),(-2,-1)\}$.

PROPOSITION 111
Soient $a,b\in\mathbb{K}$*. Les solutions du système* $\begin{cases} x+y &= a \\ xy &= b \end{cases}$ *sont exactement les couples* (α_1,α_2) *tels que* α_1 *et* α_2 *sont les deux racines, si elles existent, (éventuellement racines doubles) du polynôme* $X^2-aX+b=0$.

Preuve — En effet (α_1,α_2) est solution du système ssi

$$(X-\alpha_1)(X-\alpha_2)=X^2-(\alpha_1+\alpha_2)+\alpha_1\alpha_2=X^2-aX+b=0.$$

□

Résolution de systèmes à trois inconnues

On reprend les mêmes arguments que dans le paragraphe précédent pour montrer que

PROPOSITION 112
Soient $a,b,c\in\mathbb{K}$*. Les solutions du système* $\begin{cases} x+y+z &= a \\ xy+xz+yz &= b \\ xyz &= c \end{cases}$ *sont exactement les triplets* $(\alpha_1,\alpha_2,\alpha_3)$ *avec* α_1*,* α_2 *et* α_3 *les trois racines, si elles existent, (éventuellement racines multiples) du polynôme* $X^3-aX^2+bX-c=0$.

EXEMPLE 113 — *Les solutions du système* $\begin{cases} x+y+z &= 1 \\ xy+xz+yz &= -1 \\ xyz &= -1 \end{cases}$ *sont exactement les triplets* $(\alpha_1,\alpha_2,\alpha_3)$ *avec* α_1*,* α_2 *et* α_3 *les trois racines (éventuellement multiples) du polynôme* $X^3-X^2-X+1=(X-1)^2(X+1)=0$*, c'est-à-dire :* $(1,1,-1)$*,* $(1,-1,1)$ *et* $(-1,1,1)$.

On termine ce paragraphe avec une une variante du résultat précédent

EXEMPLE 114 — *On veut résoudre le système* $\begin{cases} x+y+z &= 2 \\ x^2+y^2+z^2 &= 14 \\ x^3+y^3+z^3 &= 20 \end{cases}$ *. Soit* (x,y,z) *une solution. Pour* $\sigma_1(x,y,z)=x+y+z$*,* $\sigma_2(x,y,z)=xy+xz+yz$ *et* $\sigma_3(x,y,z)=xyz$*, on sait que* x,y,z *sont alors les trois racines du polynôme* $P(X)=X^3-\sigma_1(x,y,z)X^2+\sigma_2(x,y,z)X-\sigma_3(x,y,z)$.
On va chercher à exprimer ces trois quantités en fonctions des trois autres quantités connues.

Tout d'abord, on a $\sigma_1(x,y,z)=x+y+z=2$*. Ensuite, l'élévation au carré donne :*

$$4=(\sigma_1(x,y,z))^2=x^2+y^2+z^2+2(xy+xz+yz)=x^2+y^2+z^2+2\sigma_2(x,y,z),$$

ce qui permet d'obtenir $\sigma_2(x,y,z)=\frac{4-14}{2}=-5$*. Enfin, l'élévation au cube donne :*

$$\begin{aligned}(x+y+z)^3&=x^3+y^3+z^3+3x^2y+3x^2z+3y^2x+3y^2z+3z^2x+3z^2y+6xyz\\&=-2(x^3+y^3+z^3)+3(x+y+z)(x^2+y^2+z^2)+6xyz,\end{aligned}$$

ce qui permet d'obtenir $\sigma_3(x,y,z)=\frac{8+2\times20-3\times2\times14}{6}=-6$.

Donc, un triplet (x,y,z) *est solution du système si et seulement si* x,y,z *sont les trois racines du polynôme* $P(X)=X^3-2X^2-5X+6$*. On remarque que* 1 *est une racine évidente, pour ensuite trouver que les deux autres racines de* P *sont* -2 *et* -3.
En conclusion, les solutions du sytème initial sont :

$$\{(1,-2,3),(1,3,-2),(-2,1,3),(-2,3,1),(3,1,-2),(3,-2,1)\}.$$

Proposition 115
Soient $a, b, c \in \mathbb{K}$. Pour l'équation

$$\begin{cases} x+y+z & = a \\ x^2+y^2+z^2 & = b \\ x^3+y^3+z^3 & = c \end{cases},$$

on a $\sigma_1(x,y,z) = a$, $\sigma_2(x,y,z) = \dfrac{a^2-b}{2}$, et $\sigma_3 = \frac{a^3+2c-3ab}{6}$.

Les triplets (x,y,z) solutions du système sont exactement les triplets $(\alpha_1, \alpha_2, \alpha_3)$ avec α_1, α_2 et α_3 les trois racines, si elles existent, (ou éventuellement multiples) du polynôme $P(X) = X^3 - aX^2 + \dfrac{a^2-b}{2}X - \frac{a^3+2c-3ab}{6} = 0$.