

Chapitre 18

Arithmétique

Objectifs

Dans \mathbb{Z} et $\mathbb{K}[X]$ qui sont des anneaux euclidiens :

- Définir la notion de congruence.
- Recherche des diviseurs communs : algorithme d'Euclide.
- Notion d'éléments premiers entre eux : théorème de Bezout et ses conséquences.
- Notion de Pgcd et de Ppcm.
- Notion d'éléments premiers (ou irréductibles), décomposition en facteurs premiers.

Sommaire

| | |
|--|----|
| I) Divisibilité | 2 |
| 1) Rappels | 2 |
| 2) Diviseurs communs | 2 |
| II) Éléments premiers entre eux | 3 |
| 1) Théorème de Bezout | 3 |
| 2) Conséquences | 4 |
| III) Le plus grand diviseur commun | 4 |
| 1) Définition | 4 |
| 2) Propriétés | 5 |
| IV) Le plus petit multiple commun | 6 |
| 1) Définition | 6 |
| 2) Propriétés | 7 |
| V) Éléments irréductibles, décomposition | 7 |
| 1) Définition | 7 |
| 2) Décomposition en facteurs irréductibles | 8 |
| 3) Applications | 9 |
| VI) Exercices | 10 |

Dans ce chapitre, l'anneau $(\mathcal{A}, +, \times)$ désigne $(\mathbb{Z}, +, \times)$ ou $(\mathbb{K}[X], +, \times)$. Pour $a \in \mathcal{A}$, on note $|a|$: la valeur absolue de a si $\mathcal{A} = \mathbb{Z}$ et $|a| = \deg(a)$ si $\mathcal{A} = \mathbb{K}[X]$. Pour $a \in \mathcal{A}$ non nul, on note \tilde{a} : la valeur absolue de a si $\mathcal{A} = \mathbb{Z}$ et le polynôme a normalisé si $\mathcal{A} = \mathbb{K}[X]$.

Notation : Soit $a \in \mathcal{A}$, on note $a.\mathcal{A}$ l'ensemble des multiples de a : $a.\mathcal{A} = \{ka \mid k \in \mathcal{A}\}$.

On vérifie facilement les propriétés suivantes :

- $b \in a.\mathcal{A} \iff a \mid b$ (a divise b).
- $\forall \lambda \in U(\mathcal{A}), (\lambda a).\mathcal{A} = a.\mathcal{A}$, et donc $a.\mathcal{A} = \tilde{a}.\mathcal{A}$ si $a \neq 0$.
- $(a.\mathcal{A}, +)$ est un groupe commutatif et $\forall b \in \mathcal{A}, \forall u \in a.\mathcal{A}, bu \in a.\mathcal{A}$. On dit que $a.\mathcal{A}$ est un idéal de \mathcal{A} .

Exercice : Montrer que $a.\mathcal{A} + b.\mathcal{A}$ et $(a.\mathcal{A}) \cap (b.\mathcal{A})$ sont également des idéaux de \mathcal{A} .

I) Divisibilité

1) Rappels

- Division euclidienne dans \mathcal{A} :

Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$, alors il existe $q, r \in \mathbb{Z}$ **uniques** tels que $a = bq + r$ avec $0 \leq r < |b|$.

Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$, alors il existe $Q, R \in \mathbb{K}[X]$ **uniques** tels que $A = BQ + R$ avec $\deg(R) < \deg(B)$.

- Soient $a, b \in \mathcal{A}$, on dit que b divise a lorsqu'il existe $k \in \mathcal{A}$ tel que $a = bk$, lorsque $b \neq 0$ ceci revient à dire que le reste de la division de a par b est nul. Notation : $b \mid a$.
- Quelques propriétés :
 - $b \mid a \iff a \in b\mathcal{A}$.
 - Si $a \neq 0$, alors $b \mid a \implies |b| \leq |a|$.
 - $(a \mid b \text{ et } b \mid a) \iff a\mathcal{A} = b\mathcal{A} \iff a = \lambda b$ avec λ inversible dans \mathcal{A} [on dit que a et b sont associés].
 - Si $b \mid a$ et $b \mid c$ alors $\forall u, v \in \mathcal{A}, b \mid au + cv$.
 - Si $nb \mid na$ et si $n \neq 0$, alors $b \mid a$.



DÉFINITION 18.1 (congruences)

Soient $a, b, n \in \mathcal{A}$, on dit que a est congru à b modulo n lorsque $n \mid a - b$. Notation : $a \equiv b \pmod{n}$.



THÉORÈME 18.1

- La relation de congruence modulo n est une relation d'équivalence.
- Soient $a, b, c, d, n \in \mathcal{A}$, si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors :

$$ac \equiv bd \pmod{n} \text{ et } a + c \equiv b + d \pmod{n}.$$

On dit que la relation de congruence est compatible avec les opérations.

Preuve: Laissée en exercice. □

Exemple: Dans \mathbb{Z} , si $n = a_0 + 10a_1 + \dots + 10^p a_p$ (écriture décimale) alors $n \equiv a_0 + \dots + a_p \pmod{3}$ car $10^k \equiv 1 \pmod{3}$.

2) Diviseurs communs



DÉFINITION 18.2 (diviseurs communs)

Pour $a \in \mathcal{A}$, on note D_a l'ensemble des diviseurs de a . Si $a, b \in \mathcal{A}$, on note $D_{a,b}$ l'ensemble des diviseurs communs à a et b , on a donc $D_{a,b} = D_a \cap D_b$, cet ensemble contient toujours les inversibles de \mathcal{A} .

Remarques:

- Pour tout élément $a \in \mathcal{A}$, $U(\mathcal{A}) \subset D_a$.
- Dans \mathbb{Z} : si $a \neq 0$, alors D_a est un ensemble fini, plus précisément $D_b \subset \llbracket -|a|..|a| \rrbracket$. Par contre dans $\mathbb{K}[X]$ l'ensemble D_a est infini mais l'ensemble des degrés des éléments de D_a est fini.
- $D_0 = \mathcal{A}$, Si λ est inversible alors $D_\lambda = U(\mathcal{A})$.
- Si a et b sont non nuls : $D_a = D_{\bar{a}}$ (on en déduit que $D_{a,b} = D_{\bar{a},\bar{b}}$).



THÉORÈME 18.2

Soient $a, b, q, r \in \mathcal{A}$, si $a = bq + r$, alors $D_{a,b} = D_{b,r}$.

Preuve: Si $d \in D_{a,b}$, alors $d \mid a$ et $d \mid b$ donc $d \mid a - bq$ i.e. $d \mid r$, donc $d \in D_{b,r}$.

Réciproquement, si $d \in D_{b,r}$, alors $d \mid b$ et $d \mid r$ donc $d \mid bq + r$ i.e. $d \mid a$, d'où $d \in D_{a,b}$. □

Application: Le théorème ci-dessus fournit un algorithme pour la recherche des diviseurs communs à a et b basé sur la division euclidienne : c'est l'**algorithme d'Euclide**¹, voici son principe :

On remarque que si $b = 0$ alors $D_{a,b} = D_a$. On peut supposer désormais que $b \neq 0$ et on cherche à calculer $D = D_{a,b}$:

Étape 1 : on effectue la division euclidienne de a par b : $a = bq_1 + r_1$ avec $0 \leq r_1 < b$ si $\mathcal{A} = \mathbb{Z}$, ou $\deg(r_1) < \deg(b)$ si $\mathcal{A} = \mathbb{K}[X]$. On a $D = D_{b,r_1}$, donc si $r_1 = 0$ alors $D = D_b$, sinon on passe à l'étape 2 :

1. EUCLIDE (300 av. J.C. – 275 av. J.C. environ) : on ne sait pratiquement rien de sa vie, il était vraisemblablement grec. Son œuvre est colossale et son ouvrage fondamental « Les éléments » regroupe toutes les connaissances de l'époque, il faudra près de vingt siècles pour dépasser son œuvre.

Étape 2 : on effectue la division euclidienne de b par r_1 : $b = r_1 q_2 + r_2$ avec $0 \leq r_2 < r_1$ si $\mathcal{A} = \mathbb{Z}$, ou $\deg(r_2) < \deg(r_1)$ si $\mathcal{A} = \mathbb{K}[X]$. On a donc $D = D_{r_1, r_2}$, donc si $r_2 = 0$ alors $D = D_{r_1}$, sinon on passe à l'étape 3 :

Étape 3 : on effectue la division euclidienne de r_1 par r_2 : $r_1 = r_2 q_3 + r_3$ avec $0 \leq r_3 < r_2$ si $\mathcal{A} = \mathbb{Z}$, ou $\deg(r_3) < \deg(r_2)$ si $\mathcal{A} = \mathbb{K}[X]$. On a donc $D = D_{r_2, r_3}$, donc si $r_3 = 0$ alors $D = D_{r_2}$, sinon on passe à l'étape 4...

- Si $\mathcal{A} = \mathbb{Z}$: la suite des restes obtenus est une suite strictement décroissante d'entiers positifs, elle est donc nécessairement finie, i.e. il existe un entier $n \geq 1$ tel que $r_n = 0$, l'ensemble cherché est donc $D = D_{r_{n-1}}$ (avec la convention $r_0 = b$).
- Si $\mathcal{A} = \mathbb{K}[X]$: la suite des degrés des restes obtenus est une suite strictement décroissante d'entiers positifs, elle est donc nécessairement finie, i.e. il existe un entier $n \geq 1$ tel que $R_n = 0$, l'ensemble cherché est donc $D = D_{R_{n-1}}$ (avec la convention $R_0 = b$).

$D_{a,b}$ est l'ensemble des diviseurs du dernier reste non nul.

Exemple: Cherchons les diviseurs communs à $a = 336$ et $b = 210$

- on effectue la division de a par b : $336 = 1 \times 210 + 126$, donc $D_{a,b} = D_{210,126}$.
- on effectue la division de 210 par 126 : $210 = 1 \times 126 + 84$, donc $D_{a,b} = D_{210,126} = D_{126,84}$.
- on effectue la division de 126 par 84 : $126 = 1 \times 84 + 42$, donc $D_{a,b} = D_{84,42}$.
- on effectue la division de 84 par 42 : $84 = 2 \times 42 + 0$, donc $D_{a,b} = D_{42,0} = D_{42}$, c'est à dire :

$$D_{336,210} = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42\}.$$

II) Éléments premiers entre eux

1) Théorème de Bezout



DÉFINITION 18.3

Soient $a, b \in \mathcal{A}$, on dit que a et b sont premiers entre eux (ou a est premier avec b) lorsque les seuls diviseurs communs sont les inversibles de \mathcal{A} , i.e. $D_{a,b} = U(\mathcal{A})$.

Dire que a est premier avec b revient à dire que le dernier reste non nul dans l'algorithme d'Euclide est un inversible de \mathcal{A} .

Remarques:

- Dans \mathbb{Z} : a est premier avec b ssi le seul diviseur commun **positif** est 1.
- Dans $\mathbb{K}[X]$: a est premier avec b ssi le seul diviseur commun **unitaire** est 1.
- Si a est premier avec b , alors au moins un des deux est non nul (sinon l'ensemble des diviseurs communs est \mathcal{A}).
- a est premier avec a ssi a est un inversible.



THÉORÈME 18.3 (théorème de Bezout²)

Soient $a, b \in \mathcal{A}$, alors a et b sont premiers entre eux ssi il existe $u, v \in \mathcal{A}$ tels que $au + bv = 1$. Les entiers u et v sont appelés coefficients de Bezout (non uniques en général).

Preuve: Supposons que u et v existent et soit d un diviseur commun à a et b , alors $d \mid a$ et $d \mid b$, donc $d \mid au + bv$ i.e. $d \mid 1$, donc $d \in U(\mathcal{A})$ ce qui prouve que a et b sont premiers entre eux.

Réciproquement : si a est premier avec b . En appliquant l'algorithme d'Euclide on vérifie qu'à chaque étape le reste r_k peut se mettre sous la forme $r_k = a.u_k + b.v_k$ avec u_k et v_k dans \mathcal{A} (récurrence), comme le dernier reste non nul est inversible dans \mathcal{A} , il existe bien u et v dans \mathcal{A} tels que $1 = au + bv$ (de plus on sait les calculer !). \square

Exemple: $\forall n \in \mathcal{A}, n$ et $n+1$ sont premiers entre eux, puisque $n+1 - n = 1$.

2. BEZOUT Étienne(1730 – 1783) : mathématicien français, l'un des précurseurs de la géométrie algébrique.

2) Conséquences



THÉORÈME 18.4



Si a est premier avec b et si a est premier avec c , alors a est premier avec le produit bc . On en déduit que si a est premier avec c_1, \dots, c_n , alors a est premier avec le produit $c_1 \times \dots \times c_n$.

Preuve: Il existe $u, v \in \mathcal{A}$ tels que $au + bv = 1$, il existe $p, q \in \mathcal{A}$ tels que $ap + cq = 1$. On effectue le produit de ces deux relations, ce qui donne $a(ucq + uap + pbv) + bc(vq) = 1$, d'après le théorème de Bezout, a et bc sont premiers entre eux. Une simple récurrence sur n permet de démontrer la généralisation. \square



THÉORÈME 18.5



Si a est premier avec c , si $a \mid b$ et si $c \mid b$, alors $ac \mid b$.

Preuve: Il existe $u, v \in \mathcal{A}$ tels que $au + cv = 1$, on multiplie par b , ce qui donne : $bau + bcv = b$, or $c \mid b$ donc $ac \mid bau$, et $a \mid b$ donc $ac \mid bcv$, ce qui entraîne $ac \mid bau + bcv$ i.e. $ac \mid b$.

Remarquons que ce théorème est faux lorsque a et c ne sont pas premiers entre eux, par exemple : $2 \mid 12$ et $4 \mid 12$ mais $2 \times 4 = 8 \nmid 12$. \square



THÉORÈME 18.6 (théorème de Gauss)



Si $a \mid bc$ et si a est premier avec c , alors $a \mid b$.

Preuve: Il existe $u, v \in \mathcal{A}$ tels que $au + cv = 1$, on multiplie par b , ce qui donne $bau + bvc = b$, or $a \mid bc$ donc $a \mid bau + bcv$, i.e. $a \mid b$. \square

Exercice: Résoudre dans \mathbb{Z} l'équation $5x + 3y = 2$.

Réponse: 5 et 3 sont premiers entre eux : $5(2) + 3(-3) = 1$, d'où $5(4) + 3(-6) = 2$, donc $(x_0 = 4, y_0 = -6)$ est une solution particulière. L'équation équivaut alors à $5(x - x_0) = 3(y_0 - y)$, d'après le théorème de Gauss, on a $3 \mid x - x_0$ et $5 \mid y_0 - y$, i.e. $x = x_0 + 3k$ et $y = y_0 - 5k'$, en reportant dans la relation on voit que $k = k'$ et donc les solutions sont les couples : $(x_0 + 3k, y_0 - 5k)$ avec $k \in \mathbb{Z}$.

III) Le plus grand diviseur commun

1) Définition


Soient $a, b \in \mathbb{Z}$ non tous deux nuls (i.e. $a \neq 0$ ou $b \neq 0$), on sait que $D_{a,b} = D_r$ où r est le dernier reste non nul dans l'algorithme d'Euclide, on voit que les diviseurs communs à a et b ont une valeur absolue inférieure ou égale à celle de r et donc r est le plus grand diviseur commun.

Soient $A, B \in \mathbb{K}[X]$ non tous deux nuls, on sait que $D_{A,B} = D_{\tilde{R}}$ où R est le dernier reste non nul dans l'algorithme d'Euclide. On voit que les diviseurs communs à A et B ont un degré inférieur ou égal à celui de R et donc \tilde{R} est un diviseur commun unitaire de degré maximal. Soit D un autre diviseur commun unitaire de degré maximal (i.e. $\deg(D) = \deg(R)$), alors $D \mid \tilde{R}$ mais l'égalité des degrés entraîne $D = \lambda \tilde{R}$, comme ces polynômes sont unitaires on a $\lambda = 1$ et donc $D = \tilde{R}$.



DÉFINITION 18.4

Soient $a, b \in \mathcal{A}$ non tous deux nuls, on appelle pgcd de a et de b le plus « grand diviseur commun » [normalisé]. Notation : $\text{pgcd}(a, b)$ ou $a \wedge b$, c'est le dernier reste non nul **normalisé** dans l'algorithme d'Euclide.

 Il en découle que deux éléments a et b de \mathcal{A} , non tous deux nuls, sont premiers entre eux ssi $\text{pgcd}(a, b) = 1$.



THÉORÈME 18.7



Soient $a, b \in \mathcal{A}$ non tous deux nuls, et $d = \text{pgcd}(a, b)$, alors d est l'unique élément normalisé dans \mathcal{A} tel que $a\mathcal{A} + b\mathcal{A} = d\mathcal{A}$.

Preuve: Unicité : si $d\mathcal{A} = d'\mathcal{A}$ alors d et d' sont associés, mais comme ils sont normalisés, on a $d = d'$.

Égalité : dans l'algorithme d'Euclide étendu, il existe u et v dans \mathcal{A} tel que $au + bv = d$, ce qui entraîne que $d\mathcal{A} \subset a\mathcal{A} + b\mathcal{A}$. Si $r \in a\mathcal{A} + b\mathcal{A}$, alors d est diviseur de r donc $a\mathcal{A} + b\mathcal{A} \subset d\mathcal{A}$, d'où l'égalité. \square



THÉORÈME 18.8 (Calcul pratique d'un pgcd)

$\color{red}{\blacklozenge}$ Si $a, b \in \mathcal{A}$ sont non tous deux nuls alors $\forall q \in \mathcal{A}, \text{pgcd}(a, b) = \text{pgcd}(a - bq, b)$.

Preuve: Soit $r = a - bq$, on a $a = bq + r$ et on sait alors que $D_{a,b} = D_{b,r}$, le résultat en découle. \square

L'algorithme d'Euclide s'écrit ainsi :

```

Procédure pgcd(a0, b0)
Variables
a, b, r: éléments de  $\mathcal{A}$ 
Début
  a  $\leftarrow$  a0
  b  $\leftarrow$  b0
  r  $\leftarrow$  b
  Tant que r est non nul faire
    r  $\leftarrow$  le reste de la division de a par b
    a  $\leftarrow$  b
    b  $\leftarrow$  r
  Fin du Tant que
  Renvoyer la valeur de a (qui contient le dernier reste non nul)
Fin.
```

Exemple: Soit à calculer $d = \text{pgcd}(3282, 1281)$:

- $3282 = 2 \times 1281 + 720$, donc $d = \text{pgcd}(1281, 720)$,
- $1281 = 1 \times 720 + 561$, donc $d = \text{pgcd}(720, 561)$,
- $720 = 1 \times 561 + 159$, donc $d = \text{pgcd}(561, 159)$,
- $561 = 3 \times 159 + 84$, donc $d = \text{pgcd}(159, 84)$,
- $159 = 1 \times 84 + 75$, donc $d = \text{pgcd}(84, 75)$,
- $84 = 1 \times 75 + 9$, donc $d = \text{pgcd}(75, 9)$,
- $75 = 8 \times 9 + 3$, donc $d = \text{pgcd}(9, 3)$,
- $9 = 3 \times 3 + 0$, donc $d = 3$.

2) Propriétés



THÉORÈME 18.9 (caractérisations du pgcd)

$\color{red}{\text{---}}$ Soient $a, b \in \mathcal{A}$ non tous deux nuls, et soit $d \in \mathcal{A}$ [non nul et normalisé]. On a alors :

$$d = \text{pgcd}(a, b) \iff \exists u, v \in \mathcal{A} \text{ premiers entre eux tels que } a = du \text{ et } b = dv.$$

Preuve: Si $d = \text{pgcd}(a, b)$ alors il existe $u, v \in \mathcal{A}$ tels que $a = du$ et $b = dv$, soit $k = u \wedge v$, alors kd divise a et b , donc $|kd| \leq |d|$ ce qui entraîne $k = 1$.

Si $a = du, b = dv$ avec $u \wedge v = 1$: alors d est un diviseur commun à a et b , d'après le théorème de Bezout, il existe $\alpha, \beta \in \mathcal{A}$ tels que $au + \beta v = 1$, d'où $d = \alpha a + \beta b$, on voit donc que tout diviseur commun à a et b est diviseur de d , donc $D_{a,b} = D_d$ i.e. d est le plus grand diviseur commun [d est normalisé], i.e. $d = a \wedge b$. \square



THÉORÈME 18.10 (quelques propriétés du pgcd)

$\color{red}{\text{---}}$ Soient $a, b \in \mathcal{A}$ non tous deux nuls :

- a) $\forall n \in \mathcal{A}, \text{ si } n \mid a \text{ et } n \mid b, \text{ alors } n \mid \text{pgcd}(a, b).$
- b) $\forall \lambda \in U(\mathcal{A}), \text{pgcd}(\lambda a, b) = \text{pgcd}(a, \lambda b) = \text{pgcd}(a, b).$
- c) $\forall k \in \mathcal{A} \setminus \{0\}, \text{pgcd}(ka, kb) = \tilde{k} \text{pgcd}(a, b).$

$$d) \forall n \in \mathbb{N}, \text{pgcd}(a^n, b^n) = \text{pgcd}(a, b)^n.$$

$$e) \text{ Si } a \text{ et } c \text{ sont premiers entre eux, alors } \text{pgcd}(a, bc) = \text{pgcd}(a, b).$$

Preuve: Pour le premier point : Soit $d = \text{pgcd}(a, b)$, alors $D_{a,b} = D_d$ donc tout diviseur commun à a et b est un diviseur de d .

Pour le deuxième point : $D_{\lambda a} = D_a$.

Pour le troisième point : soit $d = \text{pgcd}(a, b)$, alors il existe $u, v \in \mathbb{Z}$ premiers entre eux tels que $a = du$ et $b = dv$, d'où $ka = kdu$ et $kb = kdv$, donc $kd = \text{pgcd}(ka, kb)$.

Pour le quatrième point : en reprenant les notations ci-dessus, $a^n = d^n u^n$ et $b^n = d^n v^n$, or u et v sont premiers entre eux, donc u^n et v^n aussi (conséquence du théorème de Bezout), par conséquent $d^n = \text{pgcd}(a^n, b^n)$.

Pour le cinquième point : on reprend les notations ci-dessus, $a = du$ et $bc = dcv$ mais $u \mid a$ et a est premier avec c , donc u est premier avec c , d'où u est premier avec cv , et donc $d = \text{pgcd}(a, bc)$. \square

IV) Le plus petit multiple commun

1) Définition



THÉORÈME 18.11

Si a et b sont non nuls, il existe un unique élément m normalisé dans \mathcal{A} tel que $(a.\mathcal{A}) \cap (b.\mathcal{A}) = m.\mathcal{A}$.

Preuve: Le résultat est connu dans \mathbb{Z} car $(a.\mathcal{A}) \cap (b.\mathcal{A})$ est un sous-groupe de $(\mathbb{Z}, +)$.

Dans $\mathbb{K}[X]$: l'ensemble $C = \{\deg(u) \mid u \in (a.\mathcal{A}) \cap (b.\mathcal{A}), u \text{ non nul}\}$ est une partie non vide de \mathbb{N} (qui contient $\deg(ab)$), cet ensemble admet donc un plus petit élément. Autrement dit, parmi les multiples communs à a et b , non nuls, il y en a [au moins] un qui est **minimal** en degré. Soit m un multiple commun **minimal** et normalisé, soit m' un autre multiple commun, on effectue la division euclidienne de m' par m : $m' = mq + r$ avec $\deg(r) < \deg(m)$, or cette égalité entraîne que r est aussi un multiple commun à a et b , donc il est forcément nul, ce qui donne $m' = mq$, on en déduit que $(a.\mathcal{A}) \cap (b.\mathcal{A}) = m.\mathcal{A}$. L'unicité se montre comme pour le pgcd. \square

Il découle de ce théorème que c est un multiple commun à a et b si et seulement si $c \in (a.\mathcal{A}) \cap (b.\mathcal{A})$, ce qui équivaut à $c \in m.\mathcal{A}$, c'est à dire $m \mid c$. Ceci entraîne en particulier dans \mathbb{Z} : $m \leq |c|$, ou bien dans $\mathbb{K}[X]$: $\deg(m) \leq \deg(c)$.



DÉFINITION 18.5

Soit $a, b \in \mathcal{A}$, non nuls, et soit $m \in \mathcal{A}$ non nul et **normalisé**, on dit que m est le **ppcm** de a et b lorsque $(a.\mathcal{A}) \cap (b.\mathcal{A}) = m.\mathcal{A}$. Notation : $m = \text{ppcm}(a, b)$ ou encore $m = a \vee b$.



THÉORÈME 18.12 (caractérisation du ppcm)

Soient $a, b \in \mathcal{A}$, non nuls, et soit $m \in \mathcal{A}$ non nul et normalisé alors :

$$m = \text{ppcm}(a, b) \iff \exists u, v \in \mathcal{A} \text{ premiers entre eux tels que } m = au = bv.$$

Preuve: On suppose $a, b \in \mathcal{A}$, non nuls.

Si $m = \text{ppcm}(a, b)$: alors $a \mid m$ et $b \mid m$. Donc il existe $u, v \in \mathcal{A}$ tels que $m = au = bv$, soit $d = \text{pgcd}(u, v)$ alors il existe $\alpha, \beta \in \mathcal{A}$ premiers entre eux tels que $u = d\alpha$ et $v = d\beta$, d'où $m = ada = bd\beta$, mais alors $m' = a\alpha = b\beta$ est un multiple commun à a et b donc $|m'| \leq |m|$ ce qui entraîne $d = 1$.

Si $\exists u, v \in \mathcal{A}$ premiers entre eux tels que $m = au = bv$, alors $a \mid m$ et $b \mid m$, il existe α, β tels que $u\alpha + v\beta = 1$, soit m' un multiple commun, alors $m' = m'u\alpha + m'v\beta$, on en déduit que $m \mid m'$ et donc $|m| \leq |m'|$, ce qui prouve que $m = \text{ppcm}(a, b)$. \square

2) Propriétés



THÉORÈME 18.13

Soient $a, b \in \mathcal{A}$, non nuls :

$$a) \forall n \in \mathcal{A}, \text{ si } a \mid n \text{ et } b \mid n \text{ alors } \text{ppcm}(a, b) \mid n.$$

$$b) \text{ Si } a \text{ et } b \text{ sont premiers entre eux, alors } \text{ppcm}(a, b) = \widetilde{ab}.$$

$$c) \forall k \in \mathcal{A}, \text{ non nul, } \text{ppcm}(ka, kb) = \tilde{k} \text{ppcm}(a, b).$$

- d) $\text{ppcm}(a, b) \times \text{pgcd}(a, b) = \widetilde{ab}$.
 e) $\forall n \in \mathbb{N}, \text{ppcm}(a^n, b^n) = \text{ppcm}(a, b)^n$.

Preuve: Pour le premier point : découle de la démonstration du théorème précédent.

Pour le deuxième point : a et b sont premiers entre eux, alors $ab = ba$ par conséquent $\text{ppcm}(a, b) = ab$ d'après le théorème précédent.

Pour le troisième point : soit $m = \text{ppcm}(a, b)$, alors $m = au = bv$ avec u et v premiers entre eux, d'où $km = kau = kbv$ et donc $km = \text{ppcm}(ka, kb)$.

Pour le quatrième point : soit $m = \text{ppcm}(a, b)$ et $d = \text{pgcd}(a, b)$, il existe u et v premiers entre eux tels que $a = dv$ et $b = du$, or $au = bv$ donc $m = au = bv$ par conséquent $md = adu = ab$.

Pour le cinquième point : soit $m = \text{ppcm}(a, b)$ on a $m = au = bv$ avec u et v premiers entre eux, donc $m^n = a^n u^n = b^n v^n$ avec u^n et v^n premiers entre eux, donc $m^n = \text{ppcm}(a^n, b^n)$. \square

V) Éléments irréductibles, décomposition

1) Définition



DÉFINITION 18.6

Un élément p de \mathcal{A} est dit **irréductible** lorsque cet élément est non inversible et tel que ses diviseurs normalisés sont 1 et \tilde{p} . L'ensemble des éléments irréductibles normalisés de \mathcal{A} est noté $\mathcal{I}_{\mathcal{A}}$. Un élément irréductible normalisé de \mathbb{Z} est aussi appelé **nombre premier**.

Exemples:

- 2, 3, 5, 7, 11, 13, 17, 19, 23, ... sont des nombres premiers.
- Les nombres de *Fermat*³ : $F_n = 2^{2^n} + 1$ sont premiers pour $n = 0, 1, 2, 3, 4$ mais pas pour $n = 5$.
- Les nombres de *Mersennes*⁴ : $M_p = 2^p - 1$ où $p \in P$, sont premiers pour $p = 2, 3, 5, 7, 127, \dots$ mais pas pour $p = 11$.
- Tout polynôme de degré 1 est irréductible, donc $\forall \lambda \in \mathbb{K}, X + \lambda \in \mathcal{I}$.
- Tout polynôme de degré 2 **sans racine dans \mathbb{K}** est irréductible dans $\mathbb{K}[X]$. Cependant cette propriété ne se généralise pas au delà du degré 2, par exemple : $X^4 + 1$ est sans racine dans \mathbb{R} , mais ce polynôme est réductible car $X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$.
- La notion de polynôme irréductible dépend du corps \mathbb{K} , par exemple, $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$, mais pas dans $\mathbb{C}[X]$. De même, le polynôme $X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$, mais pas dans $\mathbb{R}[X]$.



THÉORÈME 18.14

Dans $\mathbb{C}[X]$, les polynômes irréductibles unitaires sont les polynômes unitaires de degré 1, c'est à dire :

$$\mathcal{I}_{\mathbb{C}[X]} = \{X + a \mid a \in \mathbb{C}\}.$$

Dans $\mathbb{R}[X]$, les polynômes irréductibles sont les polynômes unitaires de degré 1, plus les polynômes unitaires de degré 2 **sans racines réelles**. C'est à dire :

$$\mathcal{I}_{\mathbb{R}[X]} = \{X + a \mid a \in \mathbb{R}\} \cup \{X^2 + pX + q \mid p, q \in \mathbb{R}, p^2 - 4q < 0\}.$$

Preuve: Pour $\mathbb{C}[X]$ cela découle du théorème de D'Alembert.

Dans $\mathbb{R}[X]$: les polynômes annoncés sont bien irréductibles unitaires. Soit $P \in \mathcal{I}_{\mathcal{A}}$, avec $\deg(P) \geq 2$ alors P admet des racines complexes, et celles-ci sont non réelles (P est irréductible de degré supérieur à 1), soit α l'une d'elles, alors $\bar{\alpha}$ est également racine de P (et distincte de α), donc dans $\mathbb{C}[X]$ le polynôme P est divisible par $(X - \alpha)(X - \bar{\alpha}) = X^2 + pX + q \in \mathbb{R}[X]$ avec $p^2 - 4q < 0$. Mais alors P est divisible dans $\mathbb{R}[X]$ par $X^2 + pX + q$ (unicité du quotient et du reste), or $P \in \mathcal{I}_{\mathcal{A}}$, donc nécessairement $P = X^2 + pX + q$. \square

Propriétés élémentaires :

- a) Si p est irréductible, alors $\forall n \in \mathcal{A}$, si $n \notin M_p$ alors $\text{pgcd}(p, n) = 1$.

Preuve: Soit $d = \text{pgcd}(p, n)$, alors $d \mid p$ donc $d = 1$ ou $d = \tilde{p}$, mais \tilde{p} ne divise pas n , donc $d \neq \tilde{p}$, i.e. $d = 1$. \square

3. *FERMAT Pierre De* (1601 – 1665) : mathématicien amateur (éclairé !) l'un des plus féconds de son époque mais qui faisait peu de démonstrations et publiait peu.

4. *MERSENNE Marin* (1588 – 1648) : moine français qui entretenait une correspondance suivie avec les mathématiciens de son époque.

b) Si $n \in \mathcal{A}$ est non inversible, alors n possède au moins un diviseur irréductible.

Preuve: Soit $B = \{|d| \mid d \mid n \text{ et } d \notin U(\mathcal{A})\}$, alors B est une partie de \mathbb{N} non vide ($|n| \in B$), soit p un diviseur de n avec $|p| \in B$ **minimal**, si $d \mid p$ avec d normalisé et $d \notin U(\mathcal{A})$, alors $d \mid n$ et donc $|d| \in B$, d'où $|d| \geq |p|$, or $d \mid p$, donc $|d| \leq |p|$ et finalement $|d| = |p|$, d'où $d = \tilde{p}$ et donc p est irréductible. \square

c) L'ensemble $\mathcal{I}_{\mathcal{A}}$ est infini.

Preuve: Si $\mathcal{I}_{\mathcal{A}}$ est fini, alors $\mathcal{I}_{\mathcal{A}} = \{p_1, \dots, p_n\}$, posons $N = 1 + p_1 \times \dots \times p_n$, alors N est non inversible, donc N admet au moins un diviseur irréductible normalisé q , comme $q \in \mathcal{I}_{\mathcal{A}}$, on a $q \mid p_1 \times \dots \times p_n$, et comme $q \mid N$, on a $q \mid 1$ ce qui est absurde, donc $\mathcal{I}_{\mathcal{A}}$ est infini. \square

d) Si $p \in \mathcal{I}_{\mathcal{A}}$ et si $p \mid nm$, alors $p \mid n$ ou $p \mid m$.

Preuve: Supposons que p ne divise pas n , alors $n \notin M_p$ donc $\text{pgcd}(p, n) = 1$ et par conséquent $p \mid m$ (d'après le théorème de Gauss). \square

e) Dans \mathbb{Z} : si p est premier, alors $\forall k \in \llbracket 1..p-1 \rrbracket, p \mid \binom{p}{k}$.

Preuve: On a $k \binom{p}{k} = p \binom{p-1}{k-1}$ qui est donc divisible par p , mais comme $k \in \llbracket 1..p-1 \rrbracket$, p est premier avec k , par conséquent, d'après le théorème de Gauss, $p \mid \binom{p}{k}$. \square

Compléments : Soit $(p_n)_{n \geq 1}$ la suite strictement croissante des nombres premiers, la répartition de ces nombres encore aujourd'hui mal connue, cependant on a les quelques résultats suivants :

- Tout segment de la forme $\llbracket n..2n \rrbracket$ contient au moins un nombre premier (théorème de *Bertrand*).
- Si $a, b \in \mathbb{N}^*$ sont premier entre eux, alors il existe une infinité de nombre premiers de la forme $an + b$ (théorème de *Dirichlet*).
- $p_n \sim_{+\infty} n \ln(n)$ (théorème de *Hadamard*).

2) Décomposition en facteurs irréductibles



THÉORÈME 18.15 (décomposition en produit de facteurs premiers)

Tout élément $n \in \mathcal{A}$ non inversible, est un produit d'éléments irréductibles. Plus précisément, il existe $r \geq 1$, il existe $p_1, \dots, p_r \in \mathcal{I}_{\mathcal{A}}$, il existe des entiers $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$, il existe $\lambda \in U(\mathcal{A})$ tels que :

$$n = \lambda \times p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r}.$$

Preuve: On a $n = \lambda \times \tilde{n}$ avec λ inversible. On se ramène ainsi au cas où n est normalisé.

Dans \mathbb{Z} : par récurrence sur n : pour $n = 2$ il n'y a rien à montrer car 2 est premier. Supposons le théorème démontré jusqu'au rang $n \geq 2$, alors $n+1$ admet au moins un diviseur premier p , donc $n+1 = pk$, si $k = 1$ alors $n+1$ est premier, sinon k est un produit de facteurs premiers (HR), donc $n+1$ aussi.

Dans $\mathbb{K}[X]$: par récurrence sur $\deg(n)$: pour $\deg(n) = 1$ il n'y a rien à montrer. Supposons le théorème démontré jusqu'au rang k , si $\deg(n) = k+1$ alors n admet au moins un diviseur irréductible unitaire p , donc $n = pq$, si $q = 1$ alors n est irréductible, sinon q est un produit de facteurs irréductibles (HR), donc n aussi. \square



THÉORÈME 18.16 (unicité de la décomposition)

Si $n \in \mathcal{A}$ s'écrit sous la forme :

$$n = \lambda \times p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r} = \mu \times q_1^{\beta_1} \times \dots \times q_s^{\beta_s},$$

avec $p_1, \dots, p_r \in \mathcal{I}_{\mathcal{A}}, \alpha_1, \dots, \alpha_r \in \mathbb{N}^*, q_1, \dots, q_s \in \mathcal{I}_{\mathcal{A}}, \beta_1, \dots, \beta_s \in \mathbb{N}^*$, et $\lambda, \mu \in U(\mathcal{A})$ alors $r = s$, $\lambda = \mu$ et il existe une permutation σ de $\llbracket 1..r \rrbracket$ telle que pour $i \in \llbracket 1..r \rrbracket, p_i = q_{\sigma(i)}, \alpha_i = \beta_{\sigma(i)}$. La décomposition est unique [à l'ordre près].

Preuve: Si $p_1 \notin \{q_1, \dots, q_s\}$, alors p_1 est premier avec q_1, \dots, q_s , donc p_1 est premier avec $q_1^{\beta_1} \times \dots \times q_s^{\beta_s}$, i.e. p_1 est premier avec n , ce qui est absurde puisque $p_1 \mid n$, donc $p_1 \in \{q_1, \dots, q_s\}$. Finalement on a $\{p_1, \dots, p_r\} \subset \{q_1, \dots, q_s\}$ et par symétrie on a l'égalité des deux ensembles, donc $r = s$. Quitte à permuter les indices que la famille (q_i) , on peut supposer que $p_1 = q_1, \dots, p_r = q_r$.

Le théorème de Gauss entraîne que $p_k^{\alpha_k} \mid p_k^{\beta_k}$, donc $\alpha_k \leq \beta_k$, par symétrie on a $\beta_k \leq \alpha_k$, et donc $\alpha_k = \beta_k$, ce qui termine la preuve. \square

3) Applications

- Si $n \in \mathcal{A} \setminus U(\mathcal{A})$, alors la décomposition de n en produit de facteurs irréductibles permet de trouver tous les diviseurs de n .

En effet : Si $n = \lambda \times p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$, soit d est un diviseur normalisé de n , si p est un diviseur irréductible de d , alors p est un diviseur irréductible de n , donc $p \in \{p_1, \dots, p_r\}$, donc d s'écrit sous la forme :

$$d = p_1^{\beta_1} \times \dots \times p_r^{\beta_r} \text{ avec } 0 \leq \beta_k \leq \alpha_k$$

- Si $n, m \in \mathcal{A} \setminus U(\mathcal{A})$, alors à partir de leur décomposition en produit de facteurs irréductibles, on peut calculer $\text{pgcd}(n, m)$ et $\text{ppcm}(n, m)$.

En effet : Si $n = \lambda \times p_1^{\alpha_1} \times \dots \times p_r^{\alpha_r}$ et $m = \mu \times q_1^{\beta_1} \times \dots \times q_s^{\beta_s}$, alors les diviseurs irréductibles communs à n et m doivent appartenir à $\{p_1, \dots, p_r\} \cap \{q_1, \dots, q_s\}$, d'où la discussion :

- $\{p_1, \dots, p_r\} \cap \{q_1, \dots, q_s\} = \emptyset$, alors n et m sont premiers entre eux. i.e. $\text{pgcd}(n, m) = 1$ et donc $\text{ppcm}(n, m) = nm$.
- $\{p_1, \dots, p_r\} \cap \{q_1, \dots, q_s\} = \{v_1, \dots, v_t\}$, alors quitte à changer la numérotation, on peut supposer que $p_1 = q_1 = v_1, \dots, p_t = q_t = v_t$ sont les diviseurs irréductibles communs à n et m . Mais alors tout diviseur [normalisé] commun à n et m doit s'écrire sous la forme $v_1^{k_1} \times \dots \times v_t^{k_t}$ avec $k_i \leq \min(\alpha_i, \beta_i)$ pour $i \in \llbracket 1..t \rrbracket$, le plus grand diviseur commun est donc :

$$\text{pgcd}(n, m) = v_1^{k_1} \times \dots \times v_t^{k_t} \text{ avec } k_i = \min(\alpha_i, \beta_i) \text{ pour } i \in \llbracket 1..t \rrbracket.$$

En faisant le rapport $\frac{nm}{\text{pgcd}(n, m)}$ on obtient $\text{ppcm}(n, m)$, ce qui donne :

$$\text{ppcm}(n, m) = v_1^{k_1} \times \dots \times v_t^{k_t} \times p_{t+1}^{\alpha_{t+1}} \times \dots \times p_r^{\alpha_r} \times q_{t+1}^{\beta_{t+1}} \times \dots \times q_s^{\beta_s} \\ \text{avec } k_i = \max(\alpha_i, \beta_i) \text{ pour } i \in \llbracket 1..t \rrbracket.$$

Exemples:

- $336 = 2^4 \times 3 \times 7$ et $420 = 2^2 \times 3 \times 5 \times 7$, donc $\text{pgcd}(336, 420) = 2^2 \times 3 \times 7 = 84$, et $\text{ppcm}(336, 420) = 2^4 \times 3 \times 5 \times 7$.
- Dans $\mathbb{C}[X] : z \in \mathbb{C}$ est racine commune de P et Q si et seulement si z est racine de $\text{pgcd}(P, Q)$.

Exercice: Dans $\mathbb{C}[X]$ on a, pour $n, m \in \mathbb{N}^*$: $\text{pgcd}(X^n - 1, X^m - 1) = X^d - 1$ où $d = \text{pgcd}(n, m)$.

Réponse: Il existe $u, v \in \mathbb{Z}$ tels que $nu + mv = d$, on en déduit que $z^n = z^m = 1$ si et seulement si $z^d = 1$, les racines du pgcd sont donc les racines d -ièmes de l'unité, ce qui donne le résultat.

VI) Exercices

★Exercice 18.1

- a) Soit $n \in \mathbb{N}$, calculer :

$$i) \text{pgcd}(5^{n+1} + 6^{n+1}, 5^n + 6^n) \quad ii) \text{pgcd}(2n + 1, 9n + 4) \quad iii) \text{pgcd}(5n - 9, 2n - 6).$$

- b) Soient $a, b, c, d \in \mathbb{N}^*$ avec $a \wedge b = c \wedge d = 1$. Montrer que $\text{pgcd}(ac, bd) = \text{pgcd}(a, d) \times \text{pgcd}(c, b)$.

★Exercice 18.2

- a) Décomposer 2709 et 294 en produit de facteurs premiers, en déduire que $2709 \mid 2^{294} - 1$.
 b) Montrer que $\forall n \in \mathbb{N}, n^2 \mid (n+1)^n - 1, (2^n - 1)^2 \mid 2^{n(2^n - 1)} - 1$, et $n+1 \mid C_{2n}^n$.
 c) Soient $n, m, d \in \mathbb{N}^*$ tels que $n^d \mid m^d$, montrer que $n \mid m$.
 d) Soient $n, m, d, p \in \mathbb{N}^*$ avec $n \wedge m = 1$, montrer que si $nm = d^p$, alors il existe $u, v \in \mathbb{N}^*$ tels que $n = u^p$ et $m = v^p$.
 e) Soient $n, m \in \mathbb{N}^*$ premiers entre eux, soit d un diviseur positif de nm , montrer que d s'écrit de manière unique sous la forme $d = d_1 d_2$ avec d_1 diviseur positif de n et d_2 diviseur positif de m .

★Exercice 18.3

Soit p un nombre premier.

- Montrer que $\forall n \in \mathbb{N}, p \mid (n+1)^p - n^p - 1$. En déduire que $p \mid n^p - n$.
- Soit $n \in \mathbb{Z}$ tel que $n \notin p\mathbb{Z}$, montrer que $p \mid n^{p-1} - 1$.

★Exercice 18.4

En observant les carrés d'entiers modulo 11, résoudre dans \mathbb{Z} l'équation $x^2 + y^2 = 11z^2$.

★Exercice 18.5

En observant les carrés d'entiers modulo 23, montrer si n et m sont deux entiers dans \mathbb{N}^* tels que $m < n\sqrt{23}$, alors $n\sqrt{23} - m \geq \frac{2}{m}$.

★Exercice 18.6

Résoudre dans \mathbb{N}^2 le système $\begin{cases} x + y = 56 \\ \text{ppcm}(x, y) = 105 \end{cases}$.

★Exercice 18.7

Soit $n \in \mathbb{N}$.

- Déterminer n tel que $13 \mid n^2 + 20n + 74$.
- En déduire que $n^2 + 20n + 74$ n'est jamais divisible par 169.

★Exercice 18.8

Soient $a, b, c \in \mathbb{Z}$ avec a, b non tous deux nuls, on cherche à résoudre $ax + by = c$.

- Donner une condition nécessaire et suffisante pour qu'il y ait des solutions.
- Lorsque la condition est remplie, montrer que si on connaît une solution, alors toutes les autres solutions s'en déduisent. Résoudre $323x - 391y = 612$.

★Exercice 18.9

Soit $n \in \mathbb{N}$, quel est le chiffre des unités du nombre $N = 1 + 7 + \dots + 7^n$?

★Exercice 18.10

Soit $f : \mathbb{N}^* \times \mathbb{N}^* \rightarrow \mathbb{N}^*$ une application telle que : $\begin{cases} \forall a \in \mathbb{N}^*, f(a, a) = a \\ \forall a, b \in \mathbb{N}^*, f(a, b) = f(b, a) \\ \forall a, b \in \mathbb{N}^*, f(a, b) = f(a, a + b) \end{cases}$. Déterminer f .

★Exercice 18.11

Soient a, n deux entiers strictement positifs et premiers entre eux. On note r_1, \dots, r_p les entiers de l'intervalle $\llbracket 1..n \rrbracket$ qui sont premiers avec n .

- Montrer que l'application $f : \{r_1, \dots, r_p\} \rightarrow \{r_1, \dots, r_p\}$ définie par : $f(r_i)$ est le reste de la division de ar_i par n , est une bijection.
- En déduire $\prod_{k=1}^p ar_i \equiv \prod_{k=1}^p r_i \pmod{n}$, puis que $a^p \equiv 1 \pmod{n}$ [théorème d'Euler].

★Exercice 18.12

Un éleveur possède un troupeau de n moutons, s'il le partage équitablement entre 3 de ses enfants, il en restera x ($x \in \llbracket 0..2 \rrbracket$), s'il le partage entre 4 de ses enfants alors il en restera y ($y \in \llbracket 0..3 \rrbracket$), et s'il le partage entre ses 5 enfants, alors il en restera z ($z \in \llbracket 0..4 \rrbracket$). Combien de moutons peut-il y avoir dans son troupeau ?

★Exercice 18.13

Pour $n \geq 1$, on note $\varphi(n)$ le nombre d'entiers $k \in \llbracket 0..n-1 \rrbracket$ qui sont premiers avec n .

- Calculer $\varphi(n)$ pour $n = 2, 3, 4, 12$. Si p est premier, montrer que $\varphi(p^n) = p^{n-1}(p-1)$.
- On pose $A = \{\frac{k}{n} / 1 \leq k \leq n\}$, soit d un diviseur positif de n , si on met chaque élément de A sous forme irréductible, combien y aura-t-il de fractions avec un dénominateur égal à d ? En déduire que :

$$n = \sum_{d \mid n} \varphi(d).$$

★Exercice 18.14

Soit $P \in \mathbb{Q}[X]$ à coefficients entiers, soit $n \in \mathbb{Z}$, on pose $m = P(n)$.

- Montrer que $\forall k \in \mathbb{Z}, P(n + km) \equiv 0 \pmod{m}$.
- En déduire qu'il n'existe pas de polynôme P non constant à coefficients entiers, tel que $\forall n \in \mathbb{Z}, P(n)$ est un nombre premier.

★Exercice 18.15

Soient $nm \in \mathbb{N}^*$ avec $m \leq n$, montrer que : $X^{2^m} + X^{2^{m-1}} + 1 \mid X^{2^n} + X^{2^{n-1}} + 1$.

★Exercice 18.16

Montrer que dans $\mathbb{C}[X]$ deux polynômes non constants sont premiers entre eux ssi ils n'ont pas de racine commune. Montrer que l'équivalence est fausse dans $\mathbb{R}[X]$.

★Exercice 18.17

Résoudre dans \mathbb{R} le système :
$$\begin{cases} x^4 + x^3 - 4x^2 - 5x - 5 = 0 \\ x^5 - 5x^3 + 3x^2 - 15 = 0 \end{cases}.$$

★Exercice 18.18

Soient $P, Q \in \mathbb{K}[X]$, avec $P \neq Q$, on pose pour $n \in \mathbb{N}$, $T_n = \frac{P^n - Q^n}{P - Q}$.

- Montrer que $T_n \in \mathbb{K}[X]$.
- Montrer que si $\text{pgcd}(P, Q) = 1$, alors $\text{pgcd}(P - Q, T_n) = 1$.

★Exercice 18.19

- Montrer que le polynôme $P = X^4 - X^2 + 1$ est irréductible dans $\mathbb{Q}[X]$.
- Même question avec $P = X^4 + X^3 + X^2 + X + 1$.

★Exercice 18.20

Soit $P \in \mathbb{C}[X]$, calculer $\text{pgcd}(P, P')$. En déduire une condition simple sur les nombres p et q pour que le polynôme $P = X^3 + pX + q$ ait une racine multiple.

★Exercice 18.21

Soient $n, m \in \mathbb{N}^*$ et $d = \text{pgcd}(n, m)$. Avec l'algorithme d'Euclide, montrer que $\text{pgcd}(X^n - 1, X^m - 1) = X^d - 1$.