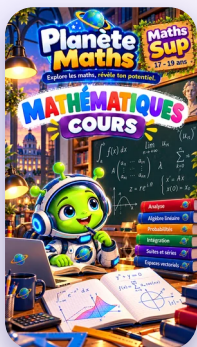


Arithmétique et polynômes : cours de maths Maths Sup à télécharger en PDF



Le livre de cours de maths Maths Sup

Tout le programme en un seul PDF de 103 pages, à imprimer ou à garder sur ta tablette.

[Voir le livre](#)

Deux mondes en apparence éloignés, les entiers et les polynômes, partagent la même charpente : une **division euclidienne**, un **PGCD**, une identité de **Bézout**, des briques irréductibles. Ce chapitre construit ces outils dans $\mathbb{Z}$, puis les transpose à $\mathbb{K}[X]$ (avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$) pour étudier racines, multiplicités et factorisations.

1. Division euclidienne dans $\mathbb{Z}$

P

Théorème (division euclidienne)

Pour tout entier a et tout entier $b \geq 1$, il existe un **unique** couple (q, r) d'entiers tel que

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

q est le quotient et r le reste.

L'unicité se démontre ainsi : si $bq + r = bq' + r'$, alors $b(q - q') = r' - r$; or $|r' - r| < b$ et c'est un multiple de b , donc $r' = r$ puis $q' = q$. Pour l'existence, on prend $q = \lfloor a/b \rfloor$.

E Exemple 1 : un dividende négatif

Division de -85 par 12 . On cherche le multiple de 12 situé juste en dessous de -85 : $12 \times (-8) = -96$. Donc $-85 = 12 \times (-8) + 11$, avec $0 \leq 11 < 12$. Le quotient est -8 et le reste 11 (jamais négatif).

I 2. PGCD et algorithme d'Euclide

D PGCD

Le plus grand commun diviseur de deux entiers non tous deux nuls, noté $a \wedge b$, est le plus grand entier qui divise à la fois a et b . Deux entiers sont **premiers entre eux** si $a \wedge b = 1$.

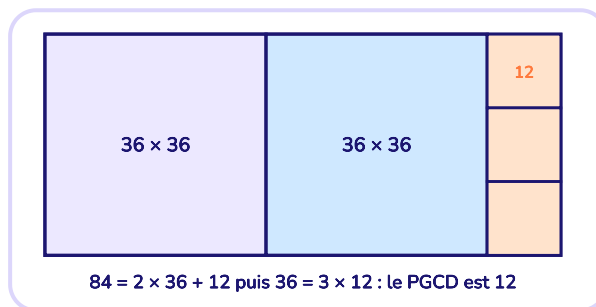
P Propriété clé

Si $a = bq + r$, alors $a \wedge b = b \wedge r$. En effet, les diviseurs communs de a et b sont exactement ceux de b et r .

M

Algorithme d'Euclide

1. Divise a par b : $a = bq_1 + r_1$.
2. Divise b par r_1 , puis r_1 par r_2 , etc.
3. Le **dernier reste non nul** est le PGCD, car la suite des restes décroît strictement dans les entiers positifs et finit par s'annuler.



E

Exemple 2 : PGCD de 1 001 et 357

$$1001 = 2 \times 357 + 287 ; 357 = 1 \times 287 + 70 ; 287 = 4 \times 70 + 7 ;$$

$$70 = 10 \times 7 + 0. \text{ Le dernier reste non nul est } 7, \text{ donc } 1001 \wedge 357 = 7.$$

3. Théorèmes de Bézout et de Gauss

P

Identité de Bézout

Pour tous entiers a, b non tous deux nuls, il existe des entiers u, v tels que $au + bv = a \wedge b$. En particulier, a et b sont premiers entre eux si et seulement s'il existe u, v avec $au + bv = 1$.

Les coefficients s'obtiennent en **remontant** l'algorithme d'Euclide. Avec l'exemple 2 :

$$7 = 287 - 4 \times 70 = 287 - 4(357 - 287) = 5 \times 287 - 4 \times 357, \text{ puis, comme}$$

$287 = 1001 - 2 \times 357$, on obtient $7 = 5 \times 1001 - 14 \times 357$.

P Théorème de Gauss

Si a divise bc et si $a \wedge b = 1$, alors a divise c .

Preuve : on écrit $au + bv = 1$; en multipliant par c , $c = acu + bcv$, et a divise les deux termes, donc $a \mid c$.

E Exemple 3 : une équation diophantienne

Réolvons $17x + 12y = 1$. On a $17 = 12 + 5$, $12 = 2 \times 5 + 2$, $5 = 2 \times 2 + 1$, d'où $1 = 5 \times 17 - 7 \times 12$. Le couple $(5, -7)$ est solution. Si (x, y) l'est aussi, $17(x - 5) = -12(y + 7)$; comme $17 \wedge 12 = 1$, Gauss donne $12 \mid x - 5$. Les solutions sont donc $x = 5 + 12k$, $y = -7 - 17k$ avec $k \in \mathbb{Z}$.

A Attention

Gauss exige $a \wedge b = 1$: $6 \mid 2 \times 3$ sans que 6 divise 2 ni 3 , car 6 n'est pas premier avec 2 .

4. Nombres premiers

D Nombre premier

Un entier $p \geq 2$ est premier si ses seuls diviseurs positifs sont 1 et p .

P**Propriétés**

- Il existe une infinité de nombres premiers (si $p_1, \dots, p_n$ étaient tous les premiers, $p_1 \cdots p_n + 1$ aurait un diviseur premier absent de la liste).
- Tout entier $n \geq 2$ s'écrit de façon **unique**, à l'ordre près, comme produit de nombres premiers.
- Un entier $n \geq 2$ non premier possède un diviseur premier $\leq \sqrt{n}$: pour tester la primalité, il suffit d'essayer les premiers jusqu'à $\sqrt{n}$.

E**Exemple 4 : 397 est-il premier ?**

Comme $\sqrt{397} < 20$, on teste **2, 3, 5, 7, 11, 13, 17, 19**. Les restes de la division de **397** par **7, 11, 13, 17, 19** valent **5, 1, 7, 6, 17** ; **397** est impair, sa somme de chiffres **19** n'est pas multiple de **3**, et il ne finit ni par **0** ni par **5**. Aucun ne divise : **397** est premier.

Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, le nombre de diviseurs positifs de n vaut $(\alpha_1 + 1) \cdots (\alpha_k + 1)$. Ainsi $7560 = 2^3 \times 3^3 \times 5 \times 7$ possède $4 \times 4 \times 2 \times 2 = 64$ diviseurs.

5. Polynômes et degré

Un polynôme à coefficients dans $\mathbb{K}$ s'écrit $P = a_n X^n + \cdots + a_1 X + a_0$. Si $a_n \neq 0$, l'entier n est le **degré** de P et a_n son coefficient dominant.

P**Degré d'une somme et d'un produit**

$\deg(P + Q) \leq \max(\deg P, \deg Q)$, avec égalité si les degrés sont différents ;
 $\deg(PQ) = \deg P + \deg Q$. Le produit de deux polynômes non nuls est donc non nul.

P**Division euclidienne dans $\mathbb{K}[X]$**

Pour A et $B \neq 0$, il existe un unique couple (Q, R) tel que $A = BQ + R$ avec $\deg R < \deg B$.

E**Exemple 5 : poser la division**

Divisons $A = X^4 + 2X^3 - X + 5$ par $B = X^2 + X - 1$. Le terme X^2 élimine X^4 :
 $A - X^2B = X^3 + X^2 - X + 5$. Le terme X élimine X^3 : on retranche
 $XB = X^3 + X^2 - X$ et il reste 5, de degré $0 < 2$. Donc
 $A = (X^2 + X - 1)(X^2 + X) + 5$: quotient $X^2 + X$, reste 5.

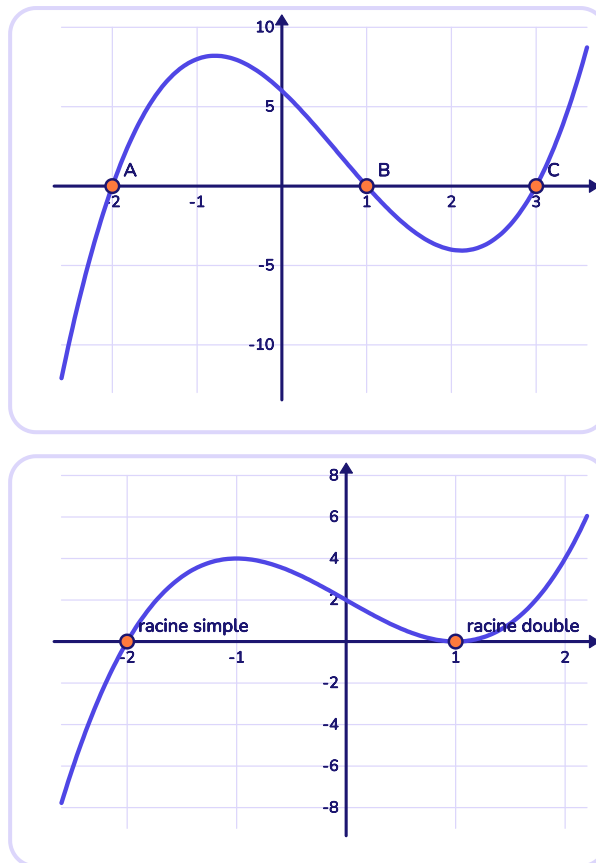
6. Racines et multiplicité**P****Racine et factorisation**

a est racine de P (c'est-à-dire $P(a) = 0$) si et seulement si $X - a$ divise P . Preuve : le reste de la division de P par $X - a$ est la constante $P(a)$.

D**Multiplicité**

a est racine de multiplicité $m \geq 1$ si $P = (X - a)^m Q$ avec $Q(a) \neq 0$. Sur $\mathbb{R}$ ou $\mathbb{C}$, c'est équivalent à $P(a) = P'(a) = \dots = P^{(m-1)}(a) = 0$ et $P^{(m)}(a) \neq 0$.

Un polynôme non nul de degré n possède au plus n racines, comptées avec leur multiplicité. Un polynôme de degré $\leq n$ qui s'annule en $n + 1$ points distincts est donc nul.



Sur la première courbe, trois racines simples : la courbe traverse l'axe. Sur la seconde, la racine double **1** correspond à un contact tangent sans traversée.

E Exemple 6 : multiplicité d'une racine

Soit $P = X^4 - 5X^3 + 6X^2 + 4X - 8$. On a $P(2) = 0$, $P'(2) = 0$, $P''(2) = 0$ mais $P^{(3)}(2) = 18 \neq 0$: **2** est racine triple, et $P = (X - 2)^3(X + 1)$.

I 7. Factorisation dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$

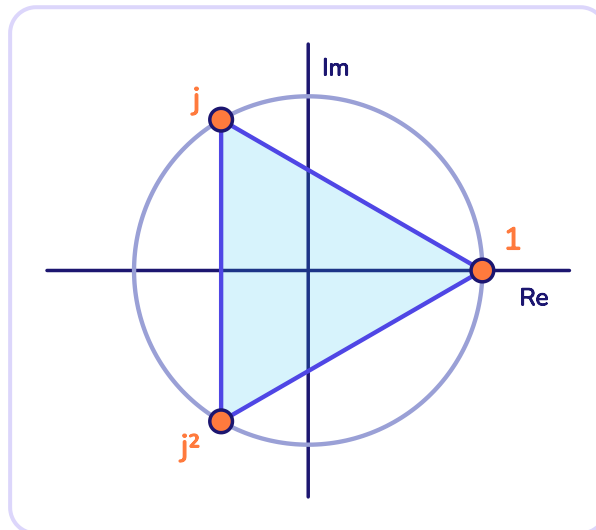
P Théorème de d'Alembert-Gauss

Tout polynôme non constant à coefficients complexes possède au moins une racine dans $\mathbb{C}$. Par conséquent, il est **scindé** : $P = a_n(X - z_1) \cdots (X - z_n)$, où les racines sont répétées selon leur multiplicité.

P

Facteurs irréductibles réels

Dans $\mathbb{R}[X]$, les polynômes irréductibles sont ceux de degré **1** et ceux de degré **2** de discriminant strictement négatif. Si P est réel et z racine non réelle, alors $\bar{z}$ est racine de même multiplicité : on regroupe $(X - z)(X - \bar{z}) = X^2 - 2\operatorname{Re}(z)X + |z|^2$.



E

Exemple 7 : factoriser $X^4 + 4$

$X^4 + 4 = (X^2 + 2)^2 - (2X)^2 = (X^2 - 2X + 2)(X^2 + 2X + 2)$, chaque facteur ayant un discriminant égal à -4 : c'est la factorisation dans $\mathbb{R}[X]$. Dans $\mathbb{C}[X]$, les racines sont $1 + i$, $1 - i$, $-1 + i$, $-1 - i$.

!

Astuce de Zyro

Chez moi, on dit qu'un polynôme réel de degré impair a toujours une racine réelle : les racines non réelles vont par paires conjuguées, donc il en reste forcément au moins une réelle, sans partenaire conjugué !

8. Relations coefficients-racines

P

Degré 2 et degré 3

Si $aX^2 + bX + c$ a pour racines x_1, x_2 : $x_1 + x_2 = -\frac{b}{a}$ et $x_1x_2 = \frac{c}{a}$.

Si $aX^3 + bX^2 + cX + d$ a pour racines x_1, x_2, x_3 : $\sigma_1 = x_1 + x_2 + x_3 = -\frac{b}{a}$,
 $\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3 = \frac{c}{a}$, $\sigma_3 = x_1x_2x_3 = -\frac{d}{a}$.

Ces relations viennent du développement de $a(X - x_1)(X - x_2)(X - x_3)$. Elles permettent de calculer des expressions symétriques des racines **sans les connaître**, par exemple

$$x_1^2 + x_2^2 + x_3^2 = \sigma_1^2 - 2\sigma_2.$$

E

Exemple 8 : vérification

$P = X^3 - 6X^2 + 11X - 6$ a pour racines **1, 2, 3**. On trouve $\sigma_1 = 6$,
 $\sigma_2 = 2 + 3 + 6 = 11$, $\sigma_3 = 6$, conformes aux coefficients $-(-6)$, **11** et $-(-6)$.

À retenir

- Division euclidienne : $a = bq + r$ avec $0 \leq r < b$ (entiers) ou $\deg R < \deg B$ (polynômes).
- Algorithme d'Euclide : le dernier reste non nul est le PGCD ; on remonte pour obtenir Bézout $au + bv = a \wedge b$.
- Gauss : $a \mid bc$ et $a \wedge b = 1$ impliquent $a \mid c$.
- Tout entier ≥ 2 se décompose de façon unique en nombres premiers ; on teste la primalité jusqu'à $\sqrt{n}$.
- a est racine de P si et seulement si $(X - a) \mid P$; la multiplicité se lit avec les dérivées successives.
- Dans $\mathbb{C}[X]$ tout polynôme est scindé ; dans $\mathbb{R}[X]$ les facteurs irréductibles sont de degré 1 ou 2.
- Relations coefficients-racines : $S = -b/a$, $P = c/a$ en degré 2, et les trois fonctions symétriques en degré 3.

Le livre de cours de maths Maths Sup

Tout le programme en un seul PDF de 103 pages, à imprimer ou à garder sur ta tablette.

Voir le livre

 **Zyro te conseille la suite**

 Exercices de maths

Arithmétique et polynômes : exercices de maths Maths Sup

 Contrôles de maths

Arithmétique et polynômes : contrôle de maths Maths Sup

 QCM de maths

Arithmétique et polynômes : QCM de maths Maths Sup

 Exercices de maths

Groupes, anneaux et corps : exercices de maths Maths Sup

 Exercices de maths

Espaces vectoriels et applications linéaires : exercices de maths Maths Sup

 Contrôles de maths

Groupes, anneaux et corps : contrôle de maths Maths Sup

Zyro vous emmène sur nos sites partenaires

Embarquez pour d'autres planètes du savoir et leurs applis.

Décollage