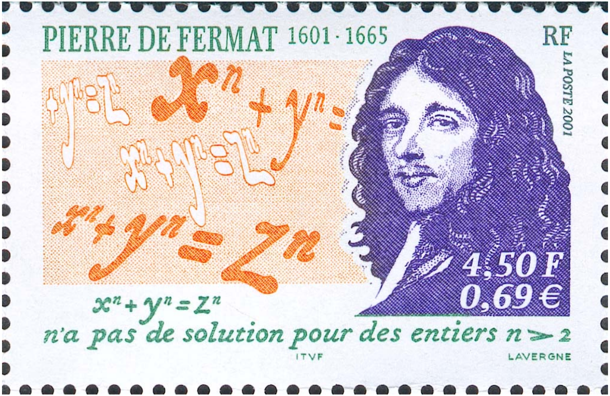


# Leçon 84 - L'anneau euclidien des polynômes

4 avril 2025

⇒ Décomposition en produits d'irréductibles

⇒ Idées plus générales

$\Rightarrow$ Décomposition en produits d'irréductibles

$\Rightarrow$ Idées plus générales

# Des polynômes « premiers »

Les polynômes irréductibles jouent ici le même rôle que les nombres premiers dans $\mathbb{Z}$.

# Des polynômes « premiers »

Les polynômes irréductibles jouent ici le même rôle que les nombres premiers dans $\mathbb{Z}$.

## Définition - Polynômes irréductibles

$P \in \mathbb{K}[X]$ est dit irréductible si

$$(P = AB, A, B \in \mathbb{K}[X]) \Rightarrow \deg A = 0 \text{ ou } \deg B = 0$$

# Des polynômes « premiers »

Les polynômes irréductibles jouent ici le même rôle que les nombres premiers dans $\mathbb{Z}$.

## Définition - Polynômes irréductibles

$P \in \mathbb{K}[X]$ est dit irréductible si

$$(P = AB, A, B \in \mathbb{K}[X]) \Rightarrow \deg A = 0 \text{ ou } \deg B = 0$$

## Proposition - Polynôme (de degré 1) irréductible

Quel que soit le corps $\mathbb{K}$ et $\alpha \in \mathbb{K}$, le polynôme $X - \alpha$ est irréductible sur $\mathbb{K}$.

# Des polynômes « premiers »

Les polynômes irréductibles jouent ici le même rôle que les nombres premiers dans $\mathbb{Z}$.

## Définition - Polynômes irréductibles

$P \in \mathbb{K}[X]$ est dit irréductible si

$$(P = AB, A, B \in \mathbb{K}[X]) \Rightarrow \deg A = 0 \text{ ou } \deg B = 0$$

## Proposition - Polynôme (de degré 1) irréductible

Quel que soit le corps $\mathbb{K}$ et $\alpha \in \mathbb{K}$, le polynôme $X - \alpha$ est irréductible sur $\mathbb{K}$.

**Démonstration**

# Lemmes

**Proposition - Polynômes irréductibles et polynômes premiers entre eux**

Un polynôme irréductible est premier avec tous les polynômes qu'il ne divise pas.
Un polynôme irréductible divise un produit si et seulement si il divise l'un des facteurs.

# Lemmes

**Proposition - Polynômes irréductibles et polynômes premiers entre eux**

Un polynôme irréductible est premier avec tous les polynômes qu'il ne divise pas.
Un polynôme irréductible divise un produit si et seulement si il divise l'un des facteurs.

**Démonstration**

# Théorème « d'Euclide »

**Théorème - Décomposition en produit de facteurs polynomiaux irréductibles**

Tout polynôme non constant de $\mathbb{K}[X]$ est le produit d'un scalaire (élément de $\mathbb{K}$) par un produit de polynômes irréductibles unitaires de $\mathbb{K}[X]$.
Cette décomposition est unique à l'ordre des facteurs près.

# Théorème « d'Euclide »





**Théorème - Décomposition en produit de facteurs polynomiaux irréductibles**

Tout polynôme non constant de $\mathbb{K}[X]$ est le produit d'un scalaire (élément de $\mathbb{K}$) par un produit de polynômes irréductibles unitaires de $\mathbb{K}[X]$.
Cette décomposition est unique à l'ordre des facteurs près.

**Démonstration**

# Critère de divisibilité

**Proposition - Critère de divisibilité par polynômes irréductibles**

Soient $A, B \in \mathbb{K}[X]$ non nuls. Si

$$A = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \dots P_k^{\alpha_k} \text{ et } B = \mu P_1^{\beta_1} P_2^{\beta_2} \dots P_k^{\beta_k}$$

où les $P_i$ sont irréductibles unitaires distincts deux à deux, $\alpha_i, \beta_i \in \mathbb{N}$ (éventuellement nuls), alors

$$A|B \Leftrightarrow \forall i \in [\![1,k]\!], \alpha_i \leqslant \beta_i$$
$$A \wedge B = \prod_{i=1}^k P_i^{\min(\alpha_i,\beta_i)}$$
$$A \vee B = \prod_{i=1}^k P_i^{\max(\alpha_i,\beta_i)}$$

# Critère de divisibilité

**Proposition - Critère de divisibilité par polynômes irréductibles**

Soient $A, B \in \mathbb{K}[X]$ non nuls. Si

$$A = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \dots P_k^{\alpha_k} \text{ et } B = \mu P_1^{\beta_1} P_2^{\beta_2} \dots P_k^{\beta_k}$$

où les $P_i$ sont irréductibles unitaires distincts deux à deux, $\alpha_i, \beta_i \in \mathbb{N}$ (éventuellement nuls), alors

$$A | B \Leftrightarrow \forall i \in [\![1, k]\!], \alpha_i \leqslant \beta_i$$
$$A \wedge B = \prod_{i=1}^{k} P_i^{\min(\alpha_i, \beta_i)}$$
$$A \vee B = \prod_{i=1}^{k} P_i^{\max(\alpha_i, \beta_i)}$$

**Démonstration**

⇒ Décomposition en produits d'irréductibles

⇒ Idées plus générales

# Polynômes irréductibles dans $\mathbb{C}[X]$

Rappel :

**Théorème - Théorème de d'Alembert-Gauss**

Soit $P \in \mathbb{C}[X]$, $\deg P \geqslant 1$. Alors $P$ possède au moins une racine dans $\mathbb{C}$.

# Polynômes irréductibles dans $\mathbb{C}[X]$

Rappel :

## Théorème - Théorème de d'Alembert-Gauss

Soit $P \in \mathbb{C}[X]$, $\deg P \geqslant 1$. Alors $P$ possède au moins une racine dans $\mathbb{C}$.

## Corollaire - Décomposition dans $\mathbb{C}$

Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré $1$.

# Polynômes irréductibles dans $\mathbb{C}[X]$

Rappel :

**Théorème - Théorème de d'Alembert-Gauss**

Soit $P \in \mathbb{C}[X]$, $\deg P \geqslant 1$. Alors $P$ possède au moins une racine dans $\mathbb{C}$.

**Corollaire - Décomposition dans $\mathbb{C}$**

Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré $1$.

**Démonstration**

# $\mathbb{C}$ algébriquement clos

**Théorème - $\mathbb{C}$ est algébriquement clos**

Tout polynôme non nul $P$ de $\mathbb{C}[X]$ se décompose de manière unique (à une permutation près) sous la forme
$P = \lambda \prod_{i=1}^{p} (X - x_i)^{m_i}$

où les $x_i \in \mathbb{C}$ sont distincts et $\displaystyle\sum_{i=1}^{p} m_i = \deg P$.

Tout polynôme non nul de $\mathbb{C}[X]$ est donc scindé sur $\mathbb{C}$.

# $\mathbb{C}$ algébriquement clos

## Théorème - $\mathbb{C}$ est algébriquement clos

Tout polynôme non nul $P$ de $\mathbb{C}[X]$ se décompose de manière unique (à une permutation près) sous la forme
$P = \lambda \prod_{i=1}^{p} (X - x_i)^{m_i}$

où les $x_i \in \mathbb{C}$ sont distincts et $\sum_{i=1}^{p} m_i = \deg P$.

Tout polynôme non nul de $\mathbb{C}[X]$ est donc scindé sur $\mathbb{C}$.

**Démonstration**

# $\mathbb{C}$ algébriquement clos

## Théorème - $\mathbb{C}$ est algébriquement clos

Tout polynôme non nul $P$ de $\mathbb{C}[X]$ se décompose de manière unique (à une permutation près) sous la forme
$P = \lambda \prod_{i=1}^{p} (X - x_i)^{m_i}$

où les $x_i \in \mathbb{C}$ sont distincts et $\sum_{i=1}^{p} m_i = \deg P$.

Tout polynôme non nul de $\mathbb{C}[X]$ est donc scindé sur $\mathbb{C}$.

**Démonstration**

## Savoir-faire. Décomposition en produit d'irréductibles de $\mathbb{C}[X]$

Sur $\mathbb{C}[X]$, les polynômes irréductibles sont de degré 1.
Donc décomposer un polynôme $P$ sur $\mathbb{C}[X]$ en produit d'irréductibles est équivalent à chercher toutes les racines de $P$ en tenant compte de leur multiplicité.
En règle générale, on choisit des facteurs unitaires, et on multiplie par $\lambda$, le coefficient dominant de $P$.

# Critère

En appliquant le critère de divisibilité par des irréductibles :

**Corollaire - Critère de divisibilité dans $\mathbb{C}$**

Soient $P, Q \in \mathbb{C}[X]$. Alors $P|Q$ dans $\mathbb{C}[X]$ si et seulement si les racines de $P$ sont des racines de $Q$ avec une multiplicité inférieure dans $P$.

# Critère

En appliquant le critère de divisibilité par des irréductibles :

**Corollaire - Critère de divisibilité dans $\mathbb{C}$**

Soient $P, Q \in \mathbb{C}[X]$. Alors $P|Q$ dans $\mathbb{C}[X]$ si et seulement si les racines de $P$ sont des racines de $Q$ avec une multiplicité inférieure dans $P$.

Exercice

Démontrer à nouveau que $P(X) - X$ divise $P(P(X)) - X$.
On commencera par faire l'étude dans $\mathbb{C}$, puis dans $\mathbb{K}$.

⇒ Décomposition en produits d'irréductibles

⇒ Idées plus générales

# Passage de $\mathbb{R}$ à $\mathbb{C}$ à $\mathbb{R}$

Comme $\mathbb{R}[X] \subset \mathbb{C}[X]$, on sait qu'un polynôme $P$ de $\mathbb{R}[X]$ tel que $\deg P \geqslant 1$ admet dans $\mathbb{C}$ $\deg P$ racines comptées avec leur multiplicité.

# Passage de $\mathbb{R}$ à $\mathbb{C}$ à $\mathbb{R}$

Comme $\mathbb{R}[X] \subset \mathbb{C}[X]$, on sait qu'un polynôme $P$ de $\mathbb{R}[X]$ tel que $\deg P \geqslant 1$ admet dans $\mathbb{C}$ $\deg P$ racines comptées avec leur multiplicité.

## Proposition - Conjugaison des racines

Si $z_0 \in \mathbb{C}$ est racine de multiplicité $m$ de $P \in \mathbb{R}[X]$,
alors il en est de même de $\overline{z_0}$.

# Passage de $\mathbb{R}$ à $\mathbb{C}$ à $\mathbb{R}$

Comme $\mathbb{R}[X] \subset \mathbb{C}[X]$, on sait qu'un polynôme $P$ de $\mathbb{R}[X]$ tel que $\deg P \geqslant 1$ admet dans $\mathbb{C}$ $\deg P$ racines comptées avec leur multiplicité.

**Proposition - Conjugaison des racines**

Si $z_0 \in \mathbb{C}$ est racine de multiplicité $m$ de $P \in \mathbb{R}[X]$,
alors il en est de même de $\overline{z_0}$.

**Démonstration**

# Irréductibles de $\mathbb{R}[X]$

**Proposition - Si $\deg P$ est impair**

Soit $P \in \mathbb{R}[X]$ tel que $\deg P$ soit impair. Alors $P$ a au moins une racine dans $\mathbb{R}$.

# Irréductibles de $\mathbb{R}[X]$

**Proposition - Si $\deg P$ est impair**

Soit $P \in \mathbb{R}[X]$ tel que $\deg P$ soit impair. Alors $P$ a au moins une racine dans $\mathbb{R}$.

**Démonstration**

# Irréductibles de $\mathbb{R}[X]$

**Proposition - Si $\deg P$ est impair**

Soit $P \in \mathbb{R}[X]$ tel que $\deg P$ soit impair. Alors $P$ a au moins une racine dans $\mathbb{R}$.

**Démonstration**

**Proposition - Description des irréductibles de $\mathbb{R}[X]$**

Les polynômes irréductibles dans $\mathbb{R}[X]$ sont

- les polynômes de degré $1$,
- les polynômes de degré $2$ à discriminant strictement négatif.

# Irréductibles de $\mathbb{R}[X]$

**Proposition - Si $\deg P$ est impair**

Soit $P \in \mathbb{R}[X]$ tel que $\deg P$ soit impair. Alors $P$ a au moins une racine dans $\mathbb{R}$.

**Démonstration**

**Proposition - Description des irréductibles de $\mathbb{R}[X]$**

Les polynômes irréductibles dans $\mathbb{R}[X]$ sont

- les polynômes de degré $1$,
- les polynômes de degré $2$ à discriminant strictement négatif.

**Démonstration**

# Factorisation

**Théorème - Factorisation dans $\mathbb{R}[X]$**

Tout polynôme non nul de $\mathbb{R}[X]$ se factorise de manière unique (à une permutation près) sous la forme

$$P = \lambda \prod_i (X - \alpha_i)^{m_i} \prod_j (X^2 + b_j X + c_j)^{p_j}$$

où les $\alpha_i, b_j, c_j$ sont des réels, $m_i, p_j$ des entiers tels que

$$\sum_i m_i + 2\sum_j p_j = \deg P, \qquad \text{et} \qquad b_j^2 - 4c_j < 0.$$

# Factorisation

**Théorème - Factorisation dans $\mathbb{R}[X]$**

Tout polynôme non nul de $\mathbb{R}[X]$ se factorise de manière unique (à une permutation près) sous la forme

$$P = \lambda \prod_i (X-\alpha_i)^{m_i} \prod_j (X^2+b_jX+c_j)^{p_j}$$

où les $\alpha_i, b_j, c_j$ sont des réels, $m_i, p_j$ des entiers tels que

$$\sum_i m_i + 2\sum_j p_j = \deg P, \qquad \text{et} \qquad b_j^2 - 4c_j < 0.$$

**Démonstration**

# Exercices

## Savoir-faire. Décomposition en produit d'irréductibles de $\mathbb{R}[X]$

On décompose $P$ sur $\mathbb{C}[X]$.
Si $\alpha$ est racine d'ordre $m$, alors $\overline{\alpha}$ également.
Le polynôme $(X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2)^m$ divise $P$ et est irréductible sur $\mathbb{R}[X]$.

# Exercices

## Savoir-faire. Décomposition en produit d'irréductibles de $\mathbb{R}[X]$

On décompose $P$ sur $\mathbb{C}[X]$.
Si $\alpha$ est racine d'ordre $m$, alors $\overline{\alpha}$ également.
Le polynôme $(X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2)^m$ divise $P$ et est irréductible sur $\mathbb{R}[X]$.

Exercice

Décomposer $2X^4 + 2$ dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.

# Exercices

### Savoir-faire. Décomposition en produit d'irréductibles de $\mathbb{R}[X]$

On décompose $P$ sur $\mathbb{C}[X]$.
Si $\alpha$ est racine d'ordre $m$, alors $\overline{\alpha}$ également.
Le polynôme $(X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2)^m$ divise $P$ et est irréductible sur $\mathbb{R}[X]$.

Exercice
Décomposer $2X^4 + 2$ dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.

Exercice
Décomposer dans $\mathbb{R}[X]$ le polynôme $X^{2n} - 1$.
Que vaut le produit des racines $2n$-ièmes de l'unité ?

# Exercices

## Savoir-faire. Décomposition en produit d'irréductibles de $\mathbb{R}[X]$

On décompose $P$ sur $\mathbb{C}[X]$.
Si $\alpha$ est racine d'ordre $m$, alors $\overline{\alpha}$ également.
Le polynôme $(X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2)^m$ divise $P$ et est irréductible sur $\mathbb{R}[X]$.

<u>Exercice</u>
Décomposer $2X^4 + 2$ dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.

<u>Exercice</u>
Décomposer dans $\mathbb{R}[X]$ le polynôme $X^{2n} - 1$.
Que vaut le produit des racines $2n$-ièmes de l'unité ?

<u>Exercice</u>
Soient $z_0, z_1, \dots z_{n-1}$ les racines $n$-ièmes de l'unité. Montrer que :

$$\prod_{k=0}^{n-1} (z_k^2 - 2z_k \cos\theta + 1) = 4\sin^2 \frac{n\theta}{2}$$

# Conclusion

**Objectifs**

⇒ Polynômes irréductibles

⇒ Quelques idées plus générales

# Conclusion

## Objectifs

### $\Rightarrow$ Polynômes irréductibles

- $P$ est irréductible si $AB = P \Longrightarrow A$ ou $B$ est inversible.

# Conclusion

## Objectifs

### ⇒ Polynômes irréductibles

- $P$ est irréductible si $AB = P \implies A$ ou $B$ est inversible.
- Les polynômes irréductibles jouent le même rôle que les nombres premiers :

# Conclusion

**Objectifs**

$\Rightarrow$ Polynômes irréductibles

- $P$ est irréductible si $AB = P \Longrightarrow A$ ou $B$ est inversible.
- Les polynômes irréductibles jouent le même rôle que les nombres premiers :
  - Unique décomposition en produit de facteurs irréductibles.

# Conclusion

## Objectifs

### ⇒ Polynômes irréductibles

- $P$ est irréductible si $AB = P \Longrightarrow A$ ou $B$ est inversible.
- Les polynômes irréductibles jouent le même rôle que les nombres premiers :
  - Unique décomposition en produit de facteurs irréductibles.
  - Critères de divisibilité, PGCD, PPCM

# Conclusion

## Objectifs

$\Rightarrow$ Polynômes irréductibles

- $P$ est irréductible si $AB = P \Longrightarrow A$ ou $B$ est inversible.
- Les polynômes irréductibles jouent le même rôle que les nombres premiers :
  - Unique décomposition en produit de facteurs irréductibles.
  - Critères de divisibilité, PGCD, PPCM
- Dans $\mathbb{C}[X]$ les irréductibles sont les $(X - a)$...

# Conclusion

## Objectifs

### ⇒ Polynômes irréductibles

- $P$ est irréductible si $AB = P \implies A$ ou $B$ est inversible.
- Les polynômes irréductibles jouent le même rôle que les nombres premiers :
  - Unique décomposition en produit de facteurs irréductibles.
  - Critères de divisibilité, PGCD, PPCM
- Dans $\mathbb{C}[X]$ les irréductibles sont les $(X-a)\dots$
- Dans $\mathbb{R}[X]$ les irréductibles sont les $(X-a)$ ou $X^2+aX+b$ avec $a^2-4b<0$

# Conclusion

**Objectifs**

⇒ Polynômes irréductibles

⇒ Quelques idées plus générales

# Conclusion

**Objectifs**

$\Rightarrow$ Polynômes irréductibles

$\Rightarrow$ Quelques idées plus générales

- On peut définir les congruences modulo un polynôme

# Conclusion

**Objectifs**

⇒ Polynômes irréductibles

⇒ Quelques idées plus générales

- On peut définir les congruences modulo un polynôme
- Si $A$ est un anneau euclidien (=muni d'une division euclidienne), Alors $A$ est principal (tout idéal est principal)

# Conclusion

**Objectifs**

⇒ Polynômes irréductibles

⇒ Quelques idées plus générales

- On peut définir les congruences modulo un polynôme
- Si $A$ est un anneau euclidien (=muni d'une division euclidienne), Alors $A$ est principal (tout idéal est principal)
- Dans ce cas, on définit $d = (a \wedge b)$ si $dA = aA + bA\ldots$

# Conclusion

**Objectifs**

⇒ Polynômes irréductibles

⇒ Quelques idées plus générales

**Pour la prochaine fois**

- Lecture du cours :
  chapitre 26 : Fractions rationnelles
- Exercices n° 694 & 696