

Annexe 1 - Algorithme de la division euclidienne de deux polynômes

★ **Exemple 1:** Division de $A=2X^5-3X^4+2X^2-1$ par $B=X^2-X+1$.

$$\begin{array}{r|l}
 2X^5-3X^4+2X^2-1 & X^2-X+1 \\
 -(2X^5-2X^4+2X^3) & \\
 \hline
 -X^4-2X^3+2X^2-1 & 2X^3-X^2-3X \\
 -(-X^4+X^3-X^2) & \\
 \hline
 -3X^3+3X^2-1 & \\
 -(-3X^3+3X^2-3X) & \\
 \hline
 3X-1 &
 \end{array}$$

Ainsi on $A = B.(2X^3-X^2-3X)+(3X-1)=B.Q+R$ avec $1=\deg(R)<\deg(B)=2$

Le résultat est $\boxed{Q = 2X^3-X^2-3X \text{ et } R = 3X-1}$

★ **Exemple 2:** Division de $A=2X^5-3X^4+2X^2-1$ par $B=X^7-1$.

On a ici $\deg(A) < \deg(B)$, donc,

$A = B.0_{\mathbb{K}[X]} + A = B.Q + R$ avec $\deg(R) = \deg(A) < \deg(B)$

Le résultat est $\boxed{Q = 0_{\mathbb{K}[X]} \text{ et } R = A = 2X^5-3X^4+2X^2-1}$

★ **Algorithme de la division euclidienne de A par B**

```

Q ← 0
R ← A
d ← deg(B)          d ≥ 0 car B ≠ 0
b ← coefficient dominant de B      b ≠ 0 car B ≠ 0
i ← 0              i compte le nombre d'étapes nécessaires
pour obtenir Q et R

Tant que deg(R) ≥ d, faire
  a ← coefficient dominant de R
  n ← deg(R)
  M ← a/b Xn-d
  Q ← Q + M
  R ← R - M.B
  i ← i+1

Fin de Tant que.
Afficher Q et R
  
```

★ **Preuve de cet algorithme**

- Le variant de boucle est $\deg(R)$. Les valeurs prises par cette variable forment une suite d'entiers naturels strictement décroissante. Donc il existe N tel que après N boucle $\deg(R) < d$
- L'invariant de boucle est $A = BQ + R$
- En sortie de boucle on a $A = BQ + R$ et $\deg(R) < \deg(B)$.