Calculez $D(X)$, PGCD des polynômes de $\mathbb{R}[X]$ suivants :

$$P(X) = X^5 + X^4 + 1$$
$$Q(X) = X^4 + X^3 - X^2 - 2X - 2$$

Trouvez deux polynômes U et V tels que :

$$P(X)U(X) + Q(X)V(X) = D(X)$$

(Paris VII – Jussieu – DEUG 1ère année – Septembre 2000)

Analyse

On utilise classiquement l'algorithme d'Euclide pour obtenir un PGCD de P et Q.
Dans ce qui suit, nous utilisons la notation : $P \wedge Q$ pour désigner un PGCD des polynômes P et Q.

Résolution

On commence donc par effectuer la division euclidienne de P par Q.

On a :

$$X^5 + X^4 + 1 = X\left(X^4 + X^3 - X^2 - 2X - 2\right) + \underbrace{\left(X^3 + 2X^2 + 2X + 1\right)}_{R_1}.$$

On a alors : $P \wedge Q = Q \wedge R_1$. On effectue la division euclidienne de Q par R_1 :

$$\begin{aligned}
X^4 + X^3 - X^2 - 2X - 2 &= X\left(X^3 + 2X^2 + 2X + 1\right) + \left(-X^3 - 3X^2 - 3X - 2\right) \\
&= X\left(X^3 + 2X^2 + 2X + 1\right) - \left(X^3 + 2X^2 + 2X + 1\right) + \left(-X^2 - X - 1\right) \\
&= (X - 1)\underbrace{\left(X^3 + 2X^2 + 2X + 1\right)}_{R_1} + \underbrace{\left(-X^2 - X - 1\right)}_{R_2}
\end{aligned}$$

On a alors : $Q \wedge R_1 = R_1 \wedge R_2$. On effectue la division euclidienne de R_1 par $-R_2$ (rappelons qu'avec l'algorithme d'Euclide, on peut multiplier tout reste obtenu par un scalaire non nul).

On a :

$$\begin{aligned} X^3 + 2X^2 + 2X + 1 &= X\left(X^2 + X + 1\right) + \left(X^2 + X + 1\right) \\ &= \left(X + 1\right)\left(X^2 + X + 1\right) \end{aligned}$$

$-R_2$ divise R_1 et est le dernier reste non nul obtenu.

Il vient donc : $P \wedge Q = R_2$. C'est à dire :

$$D\left(X\right) = X^2 + X + 1$$

Pour la suite, il est intéressant d'écrire les divisions des polynômes *P* et *Q* par *D* :

$$\begin{aligned} P\left(X\right) &= X^5 + X^4 + 1 = \left(X^3 - X + 1\right)\left(X^2 + X + 1\right) \\ Q\left(X\right) &= X^4 + X^3 - X^2 - 2X - 2 = \left(X^2 - 2\right)\left(X^2 + X + 1\right) \end{aligned}$$

D étant un PGCD de *P* et *Q*, les polynômes $P^*\left(X\right) = X^3 - X + 1$ et $Q^*\left(X\right) = X^2 - 2$ sont premiers entre eux.

Il existe donc (théorème de BEZOUT) un couple unique de polynômes *U* et *V* tels que :

$$\begin{cases} U\left(X\right)P^*\left(X\right) + V\left(X\right)Q^*\left(X\right) = 1 \\ \deg U < \deg Q^* \\ \deg V < \deg P^* \end{cases} \qquad \text{(S)}$$

En multipliant cette égalité par le polynôme D, on retrouve la question posée :

$$\begin{aligned} & U\left(X\right)P^*\left(X\right) + V\left(X\right)Q^*\left(X\right) = 1 \\ \Leftrightarrow\ & D\left(X\right)\left(U\left(X\right)P^*\left(X\right) + V\left(X\right)Q^*\left(X\right)\right) = D\left(X\right) \\ \Leftrightarrow\ & U\left(X\right)P\left(X\right) + V\left(X\right)Q\left(X\right) = D\left(X\right) \end{aligned}$$

Le système (S) se résout, par exemple, en posant :

$$\begin{aligned} U\left(X\right) &= aX + b && \text{(il faut } \deg U < \deg Q^*\text{)} \\ V\left(X\right) &= cX^2 + dX + e && \text{(il faut } \deg V < \deg P^*\text{)} \end{aligned}$$

On a alors :

$$\begin{aligned}
&U(X)P^*(X)+V(X)Q^*(X)=1\\
&\Leftrightarrow (aX+b)\left(X^3-X+1\right)+\left(cX^2+dX+e\right)\left(X^2-2\right)=1\\
&\Leftrightarrow (a+c)X^4+(b+d)X^3+(-a-2c+e)X^2+(a-b-2d)X+(b-2e)=1
\end{aligned}$$

$$\Leftrightarrow \begin{cases} a+c=0 \\ b+d=0 \\ -a-2c+e=0 \\ a-b-2d=0 \\ b-2e=1 \end{cases} \Leftrightarrow \begin{cases} c=-a \\ d=-b \\ -a+2a+\dfrac{1}{2}(b-1)=0 \\ a-b+2b=0 \\ e=\dfrac{1}{2}(b-1) \end{cases} \Leftrightarrow \begin{cases} c=-a \\ d=-b \\ e=\dfrac{1}{2}(b-1) \\ a+\dfrac{1}{2}b=\dfrac{1}{2} \\ a+b=0 \end{cases}$$

Les deux dernières lignes nous donnent facilement : $a=1$ et $b=-1$.
On en tire alors, avec les trois premières lignes : $c=-1$, $d=1$ et $e=-1$.

Finalement :

$$\begin{aligned}
U(X)&=X-1\\
V(X)&=-X^2+X-1
\end{aligned}$$

Résultat final

Le PGCD de $P(X)=X^5+X^4+1$ et $Q(X)=X^4+X^3-X^2-2X-2$ est :

$$D(X)=X^2+X+1$$

On a alors :

$$U(X)P(X)+V(X)Q(X)=D(X)$$

avec :

$$\begin{aligned}
U(X)&=X-1\\
V(X)&=-X^2+X-1
\end{aligned}$$