Ex 13

Variante 1 : On pose $I = \{ h \in \mathbb{Q}[X] \mid h(\alpha) = 0 \}$

. I est un idéal. (facile)

. $\mathbb{Q}[X]$ est principal donc $\exists k \in I$ tq $I = \langle k \rangle$
$= \mathbb{Q}[X] \cdot k$

$f \in I$ donc $\exists q \in \mathbb{Q}[X]$ tq $f = q \times k$

Or f irréd. dans $\mathbb{Q}[X]$ donc k est cst ou k égale f à une cste près

or $1 \notin I$ donc $k = f$ (à une cste près)

Ainsi $I = \langle f \rangle$. Or $g \in I$ et donc $f \mid g$.

Variante 2 : Justifions que $\mathrm{pgcd}_{\mathbb{Q}[X]}(f,g) = \mathrm{pgcd}_{\mathbb{C}[X]}(f,g)$.

$f, g \in \mathbb{Q}[X] \subseteq \mathbb{C}[X]$

↳ La div. euclidienne dans $\mathbb{Q}[X]$ sera la même que dans $\mathbb{C}[X]$. L'algor. d'Euclide donnera les mêmes restes et donc le même pgcd.

On applique l'algo. d'Euclide à f et g : on obtient des restes $R_1, \dots, \underset{\neq 0}{R_q}, R_{q+1} = 0$

$R_q \in \mathbb{Q}[X]$.

$\langle f, g \rangle_{\mathbb{Q}[X]} = \langle R_q \rangle_{\mathbb{Q}[X]}$

$\deg(R_q) \geq 1$ car $f(\alpha) = g(\alpha) = 0$ ie $X - \alpha$ divise f et g dans $\mathbb{C}[X]$

f est multiple de R_q donc $R_q = 1$ ou $= f$ (à une cste près)

or $\deg(R_q) \geq 1$, $R_q = f$.

On conclut comme dans la variante 1

Ex 14

On écrit $m = qn + r$ ← $r < n$

$$(a+b)^q = \sum_{k=0}^{q} \binom{q}{k} a^k b^{q-k}$$
$$= a^q + q a^{q-1} b + \dots + b^q$$
$$= a^q + b \times (\dots)$$

$$X^m - 1 = X^{qn+r} - 1$$
$$= (X^n)^q \times X^r - 1$$
$$= ((X^n - 1) + 1)^q \times X^r - 1$$
$$= (1^q + (X^n - 1) \times Q) \times X^r - 1$$
$$= X^r \times Q \times (X^n - 1) + \underbrace{X^r - 1}_{\text{de deg} < \deg(X^n - 1)}$$

$X^r - 1$ = reste de la division de $X^m - 1$ par $X^n - 1$

Notons $r_1, \dots, r_p = d$, $r_{p+1} = 0$ les restes obtenus dans l'alg. d'Euclide appliqué à m et n.

On a alors : les restes dans l'alg. d'Euclide appliqué à $X^m - 1$ et $X^n - 1$ sont $X^{r_1} - 1, \dots, X^d - 1, 0$

Ainsi $\operatorname{pgcd}_{\mathbb{Q}[X]}(X^m - 1, X^n - 1) = X^d - 1$ où $d = \operatorname{pgcd}(m, n)$

Notons $D = \operatorname{pgcd}_{\mathbb{Z}[X]}(X^m - 1, X^n - 1)$

On a : $D \mid X^d - 1$ car $X^d - 1 \in \mathbb{Q}[X]\{f, g\}$ et $D \mid f$ et $\mid g$.

On a même $X^d - 1 \in \mathbb{Z}[X] \cdot \{f, g\}$ (les étapes des divisions se font dans $\mathbb{Z}[X]$)

De plus
$$X^n - 1 = X^{ad} - 1 = (X^d)^a - 1$$
$$= (X^d - 1 + 1)^a - 1 = 1 + A \times (X^d - 1) - 1$$
$$= A \times (X^d - 1)$$

D'où $X^n - 1 \in \langle X^d - 1 \rangle$ et idem pour $X^m - 1$

Finalement : $\mathbb{Z}[X](X^d - 1) = \mathbb{Z}[X]\{X^m - 1, X^n - 1\}$

D'où $X^d - 1 = \operatorname{pgcd}_{\mathbb{Z}[X]}(X^m - 1, X^n - 1)$

Ex 15

$f = X^5 + X^4 + 1 \qquad g = X^4 + X^2 + 1$

$$\begin{array}{l|l} X^5+X^4+1 & X^4+X^2+1 \\ \hline -X^5-X^3-X & X+1 \\ \overline{X^4+X^3+X+1} & \\ -X^4-X^2-1 & \\ \overline{\underbrace{X^3+X^2+X}_{R_1}} & \end{array}$$

Dans $\mathbb{Z}_2$, $1 = -1$

$$\begin{array}{l|l} X^4+X^2+1 & X^3+X^2+X \\ \hline -X^4-X^3-X^2 & X+1 \\ \overline{X^3+1} & \\ -X^3-X^2-X & \\ \overline{\underbrace{X^2+X+1}_{R_2}} & \end{array}$$

R_1 divisé par R_2

$X^3+X^2+X = X(X^2+X+1) + 0$

Dernier reste non nul, c'est

$R_2 = \text{pgcd}(f,g)$

$$\begin{array}{l|l} X^5+X^3+X+1 & X^4+1 \\ \hline -X^5-X & X \\ \overline{\underbrace{X^3+1}_{R_1}} & \end{array} \qquad (1)$$

$$(2) \qquad \begin{array}{l|l} X^4+1 & X^3+1 \\ \hline -X^4-X & X \\ \overline{\underbrace{X+1}_{R_2}} & \end{array}$$

$X^3+1 = Q \times (X+1) + 0$ Donc $R_2 = \text{pgcd}(f,g)$

$Q = X^2+X+1$

$X^4+1 = X(X^3+1) + R_2$ ← pgcd

$g = X \times R_1 + R_2$

$\quad = X \times (f - Xg) + R_2$

$R_2 = -Xf + (X^2+1)g$

Dans la division (1):

$f = Xg + R_1$

$R_1 = f - Xg$

Ex 16

$f = X^4 + 1 \qquad g = X^3 + X + 1 \qquad$ dans $\mathbb{Z}_3[X]$

$$
\begin{array}{r|l}
X^4 + 1 & X^3 + X + 1 \\ \hline
-X^4 - X^2 - X & X \\
\underbrace{2X^2 + 2X + 1}_{R_1} &
\end{array}
\qquad (1)
\qquad
\begin{array}{r|l}
X^3 + X + 1 & 2X^2 + 2X + 1 \\ \hline
-4X^3 - 4X^2 - 2X & 2X + 1 \\
2X^2 + 2X + 1 & \\
0 &
\end{array}
$$

$$\mathrm{pgcd}_{\mathbb{Z}_3(x)}(f, g) = R_1$$

Dans $\mathbb{Z}_5[X]$:

$$
\begin{array}{r|l}
X^4 + 1 & X^3 + X + 1 \\ \hline
-X^4 - X^2 - X & X \\
\underbrace{-X^2 - X + 1}_{R_1} &
\end{array}
\qquad (1)
\qquad
\begin{array}{r|l}
X^3 + X + 1 & -X^2 - X + 1 \\ \hline
-X^3 - X^2 + X & -X + 1 \\
-X^2 + 2X + 1 & \\
+X^2 + X - 1 & \\
\underbrace{3X}_{R_2} &
\end{array}
\qquad
\begin{array}{r|l}
-X^2 - X + 1 & 3X \\ \hline
+X^2 & -2X - 2 \\
-X + 1 & \\
+X & \\
\underbrace{1}_{R_3} &
\end{array}
$$

Dans $\mathbb{Z}_5$: L'inverse de 3 est 2 car $\overline{2} \times \overline{3} = \overline{6} = \overline{1}$

Ici $\mathrm{pgcd}_{\mathbb{Z}_5(x)}(f, g) = R_3 = 1$