

Feuille n° 2  
corrigés

**Exercice 8 feuille 2**

C'est en fait le théorème chinois des restes. On cherche  $P$  tel que

$$\begin{cases} P \equiv (X^3 + X + 1) \pmod{(X^4 - 2X^3 - 2X^2 + 10X - 7)} \\ P \equiv (2X^2 - 3) \pmod{(X^4 - 2X^3 - 3X^2 + 13X - 10)} \end{cases}$$

→ On cherche tout d'abord le pgcd de  $A = X^4 - 2X^3 - 2X^2 + 10X - 7$  et de  $B = X^4 - 2X^3 - 3X^2 + 13X - 10$ . L'algorithme d'Euclide donne

|     |     |                |         |         |     |
|-----|-----|----------------|---------|---------|-----|
| $A$ | $B$ | $X^2 - 3X + 3$ | $X - 1$ | $1$     | $0$ |
|     | $1$ | $X^2 + X - 3$  | $X - 2$ | $X - 1$ |     |

→ En "remontant" cet algorithme, on trouve

$$1 = A \times (X^3 - X^2 - 5X + 7) + B \times (-X^3 + X^2 + 4X - 5)$$

→ Comme dans la démonstration du théorème chinois des restes, le polynôme

$$P = (2X^2 - 3) \times A \times (X^3 - X^2 - 5X + 7) + (X^3 + X + 1) \times B \times (-X^3 + X^2 + 4X - 5)$$

convient.

Après calculs on trouve que  $P = -2X^7 + 7X^6 + 8X^5 - 64X^4 + 61X^3 + 115X^2 - 249X + 127$ .

→ C'est bien le polynôme de plus petit degré qui convient car les solutions sont modulo  $A \times B$  qui est un polynôme de degré 8.

**Exercice 14 feuille 2**

Soit  $D = P \wedge Q$ ; alors  $D$  divise  $P$ , et comme  $P$  est irréductible, c'est que  $D$  est une unité de  $\mathbb{k}[X]$ , ou bien que  $D$  est associé à  $P$ .

→ Si  $D$  est une unité de  $\mathbb{k}[X]$ , alors  $D = 1$  (le pgcd est unitaire), et par suite  $P$  et  $Q$  sont premiers entre eux.

→ Si  $D$  est associé à  $P$ , alors  $D = \lambda P$  où  $\lambda$  est l'inverse du coefficient dominant de  $P$ . Dans ce cas,  $P$  divise  $Q$ .

**Exercice 16 feuille 2**

1°  $\forall a \in A, (a^5)^3 = a^{15} = 1$ , donc  $a^5$  est une racine cubique de l'unité.

Par suite tous les  $a^5$  sont des racines de  $X^2 + X + 1 = 0$ . En effet,  $a^5 \neq 1$  car sinon  $a$  ne serait pas une racine **primitive** quinzisième de l'unité.

D'où  $(a^5)^2 + (a^5) + 1 = 0 \forall a \in A$ , ie tout  $a$  de  $A$  est racine de  $X^{10} + X^5 + 1$ .

On en déduit que  $P \mid (X^{10} + X^5 + 1)$ .

2°  $j^{10} + j^5 + 1 = j + j^2 + 1 = 0$ , donc  $j$ , et  $\bar{j}$ , sont racines de  $X^{10} + X^5 + 1$ .

Par suite  $X^2 + X + 1$  divise  $X^{10} + X^5 + 1$ .

3° La décomposition de  $X^2 + X + 1$  en produit de facteurs irréductibles de  $\mathbb{C}[X]$  est

$$X^2 + X + 1 = (X - j)(X - \bar{j}).$$

Or ni  $j$ , ni  $\bar{j}$  ne sont des racines de  $P$ , car ni  $j$ , ni  $\bar{j}$  ne sont des racines **primitives** quinzzièmes de l'unité.

Donc  $\text{pgcd}(P, X^2 + X + 1) = 1$ .

4° **Rappel** :  $a \mid c, b \mid c$  et  $a \wedge b = 1$ , entraîne que  $ab \mid c$ .

Ici, on a :  $P$  divise  $(X^{10} + X^5 + 1)$ ,  $(X^2 + X + 1)$  divise  $(X^{10} + X^5 + 1)$ , et

$\text{pgcd}(P, X^2 + X + 1) = 1$ , d'où

$$(X^2 + X + 1) \times P \text{ divise } (X^{10} + X^5 + 1)$$

De plus, le degré de  $P$  est le nombre de racines primitives quinièmes de l'unité.

Il y en a  $\phi(15) = \phi(3) \times \phi(5) = (3-1) \times (5-1) = 8$ .

Ainsi  $\deg((X^2 + X + 1) \times P) = 10 = \deg(X^{10} + X^5 + 1)$ . De plus  $P$  étant unitaire,  $(X^2 + X + 1) \times P$  est unitaire tout comme  $X^{10} + X^5 + 1$ , ce qui permet d'en déduire que

$$X^{10} + X^5 + 1 = (X^2 + X + 1) \times P$$

Le quotient de la division euclidienne de  $X^{10} + X^5 + 1$  par  $(X^2 + X + 1)$  nous donne

$$P = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1$$

### Exercice 17 feuille 2

1°  $X$  et  $1 - X$  sont des facteurs irréductibles de  $\mathbb{R}[X]$  premiers entre eux. On en déduit donc que

$\forall n \in \mathbb{N}^*$ ,  $X^n$  et  $(1 - X)^n$  sont premiers entre eux, d'où l'existence de deux polynômes  $P_0$  et  $Q_0$  de  $\mathbb{R}[X]$  tels que  $X^n P_0 + (1 - X)^n Q_0 = 1$  d'après le théorème de Bezout.

L'ensemble des couples  $(P, Q) \in \mathbb{R}[X]^2$  tels que  $X^n P + (1 - X)^n Q = 1$  (équation diophantienne) est donné par

$$P = P_0 - (1 - X)^n B \quad Q = Q_0 + X^n B, \quad B \in \mathbb{R}[X].$$

2° Effectuons la division euclidienne de  $P_0$  par  $(1 - X)^n$ .

Il existe un unique couple  $(A_0, R_0)$  de  $\mathbb{R}[X]^2$  tel que  $P_0 = (1 - X)^n A_0 + R_0$ , avec  $\deg R_0 < n$ .

Parmi tous les  $P$  de la forme  $P_0 - (1 - X)^n B$ , seul  $P_0 - (1 - X)^n A_0$  est de degré  $\leq n - 1$  (pour  $B = A_0$ ).

On a alors  $Q_0 + X^n A_0$  de degré  $\leq n - 1$  puisque  $P_n = P_0 - (1 - X)^n A_0$  et  $Q_n = Q_0 + X^n A_0$  sont solutions de (\*).

D'où l'existence et l'unicité d'un couple  $(P_n, Q_n)$  de polynômes de  $\mathbb{R}[X]$  de degrés  $\leq n - 1$  qui soient solution de (\*).

3° On a  $X^n P_n(X) + (1 - X)^n Q_n(X) = 1$ . Effectuons le changement de variable  $x \leftrightarrow 1 - x$ .

On obtient  $(1 - x)^n P_n(1 - x) + x^n Q_n(1 - x) = 1 \Leftrightarrow x^n Q_n(1 - x) + (1 - x)^n P_n(1 - x) = 1$ .

On travaille dans  $\mathbb{R}[X]$ , ie on peut identifier un polynôme et sa fonction polynômiale.

On a donc trouvé deux polynômes  $S$  et  $T$  définis par  $S = Q_n(1 - X)$  et  $T = P_n(1 - X)$ , de degrés  $\leq n - 1$ , tels que

$$X^n S + (1 - X)^n T = 1.$$

Or, par unicité d'un couple  $(P_n, Q_n)$  de polynômes de  $\mathbb{R}[X]$  de degrés  $\leq n - 1$  qui soient solution de (\*), on en déduit que  $S = P_n$ , et que  $T = Q_n$ , ie que  $Q_n(1 - X) = P_n(X)$ , et que  $P_n(1 - X) = Q_n(X)$ .

4° En dérivant (\*), on trouve  $nX^{n-1}P + X^n P' - n(1 - X)^{n-1}Q + (1 - X)^n Q' = 0$  pour tous  $P$  et  $Q$  solutions de (\*), donc en particulier pour  $P_n$  et  $Q_n$ .

On a ainsi  $X^{n-1} [nP_n + X P_n'] + (1 - X)^{n-1} [-nQ_n + (1 - X)Q_n'] = 0$

$\Leftrightarrow X^{n-1} [nP_n + X P_n'] = (1 - X)^{n-1} [nQ_n - (1 - X)Q_n']$ .

Or  $X^{n-1}$  et  $(1 - X)^{n-1}$  sont premiers entre eux, d'où, par le théorème de Gauss, on en déduit que  $X^{n-1}$  divise  $(1 - X)Q_n' - nQ_n$ .