

Plaquette 2 - Arithmétique des polynômes : restes, PGCD et Bézout

Polynômes et fractions rationnelles — Licence 1 (L1)

Corrections détaillées

Boîte à outils

Division euclidienne : pour $B \neq 0$, il existe un unique couple (Q, R) avec

$$A = BQ + R, \quad \deg R < \deg B$$

- **Reste par évaluation** : si B a des racines simples $b_1, \dots, b_k$, le reste R ($\deg R < k$) est déterminé par $R(b_i) = A(b_i)$. Pour une racine **double** b , on ajoute $R'(b) = A'(b)$.
- **PGCD** : dernier reste non nul de l'algorithme d'Euclide, **normalisé** (unitaire).
- **Bézout** : $A \wedge B = 1 \Leftrightarrow \exists U, V \in K[X], AU + BV = 1$.
- **Gauss** : $A \mid BC$ et $A \wedge B = 1 \Rightarrow A \mid C$; si $A \wedge B = 1$, $A \mid P$ et $B \mid P$, alors $AB \mid P$.
- Dans $\mathbb{C}[X]$: $A \wedge B = 1 \Leftrightarrow A$ et B n'ont **aucune racine commune**.
- **Irréductibles** : de degré 1 dans $\mathbb{C}[X]$; de degré 1, ou 2 sans racine réelle, dans $\mathbb{R}[X]$. Un polynôme de degré 2 ou 3 est irréductible sur K si et seulement s'il n'a **pas de racine** dans K .

$$\text{pgcd}(X^m - 1, X^n - 1) = X^{\text{pgcd}(m, n)} - 1$$

Correction de l'exercice 1 - PGCD et relation de Bézout

a) On factorise par groupements :

$$A = X^2(X + 1) + (X + 1) = (X + 1)(X^2 + 1), \quad B = X^2(X - 1) + (X - 1) = (X - 1)(X^2 + 1)$$

— $X^2 + 1$ n'a pas de racine réelle : il est **irréductible** dans $\mathbb{R}[X]$.

b) Le facteur commun est $D = X^2 + 1$ ($X + 1$ et $X - 1$ sont distincts).

— **Contrôle par Euclide** : $A = 1 \times B + (2X^2 + 2)$, puis $B = \left(\frac{X}{2} - \frac{1}{2}\right)(2X^2 + 2) + 0$. Dernier reste non nul : $2X^2 + 2$, normalisé en $X^2 + 1$ ✓

c) La première division donne directement $A - B = 2(X^2 + 1)$, donc

$$\frac{1}{2}A - \frac{1}{2}B = X^2 + 1$$

— $U = \frac{1}{2}, V = -\frac{1}{2}$.

d) $\frac{A}{D} = X + 1$ et $\frac{B}{D} = X - 1$. Relation de Bézout : $\frac{1}{2}(X + 1) - \frac{1}{2}(X - 1) = 1$. Ils sont **premiers entre eux**.

— **Règle générale** (comme dans $\mathbb{Z}$) : après division par le PGCD, les quotients sont toujours premiers entre eux.

Réponse. $A = (X + 1)(X^2 + 1)$, $B = (X - 1)(X^2 + 1)$; $D = X^2 + 1 = \frac{1}{2}A - \frac{1}{2}B$.

Correction de l'exercice 2 - PGCD de deux polynômes $X^n - 1$

a) Racines de $X^4 - 1$: $\{1, i, -1, -i\}$. Racines de $X^6 - 1$: $\{e^{ik\pi/3}\}$, soit $1, -1$ et $\pm \frac{1}{2} \pm \frac{\sqrt{3}}{2}i$.

— Racines communes : 1 et -1 ($\pm i$ ne sont pas racines sixièmes : $i^6 = -1$).

b) Toutes les racines sont simples ; le PGCD unitaire est le produit des $(X - \alpha)$ sur les racines communes :

$$\text{pgcd}(X^4 - 1, X^6 - 1) = (X - 1)(X + 1) = X^2 - 1$$

— Cohérent avec $\text{pgcd}(4, 6) = 2$.

c) Si $z^d = 1$, comme $d \mid m$ et $d \mid n$, $z^m = z^n = 1$. Réciproquement, Bézout dans $\mathbb{Z}$: $d = um + vn$, et si $z^m = z^n = 1$ (donc $z \neq 0$) :

— $z^d = (z^m)^u (z^n)^v = 1$ (exposants éventuellement négatifs).

d) $X^N - 1$ a N racines **distinctes** (les $e^{2ik\pi/N}$), donc toutes simples. Le PGCD est le produit des $X - z$ pour z racine commune, c'est-à-dire pour z racine d -ième de l'unité : c'est $X^d - 1$.

— **Parallèle** : c'est l'analogie exact de $\text{pgcd}(2^m - 1, 2^n - 1) = 2^d - 1$ vu en arithmétique des entiers.

Réponse. $\text{pgcd}(X^4 - 1, X^6 - 1) = X^2 - 1$; en général $X^{\text{pgcd}(m, n)} - 1$.

Correction de l'exercice 3 - Reste par deux racines simples

a) $B = (X - 1)(X - 2)$, de degré 2 : le reste est de degré ≤ 1 , $R = aX + b$.

b) $X^n = BQ + R$; en $X = 1$ et $X = 2$, B s'annule :

$$a + b = 1, \quad 2a + b = 2^n$$

— Par différence : $a = 2^n - 1$, puis $b = 1 - a = 2 - 2^n$.

— $R = (2^n - 1)X + 2 - 2^n$.

c) $n = 2$: $R = 3X - 2$ et $X^2 = 1 \times (X^2 - 3X + 2) + 3X - 2$ ✓

— $n = 3$: $R = 7X - 6$; $X^3 = (X + 3)(X^2 - 3X + 2) + 7X - 6$ (développer : $X^3 - 3X^2 + 2X + 3X^2 - 9X + 6 = X^3 - 7X + 6$ ✓).

d) $M^2 = \begin{pmatrix} 1 & 3 \\ 0 & 4 \end{pmatrix}$ et $3M - 2I_2 = \begin{pmatrix} 1 & 3 \\ 0 & 4 \end{pmatrix}$: $M^2 - 3M + 2I_2 = 0$ ✓

— On substitue M dans $X^n = BQ + R$: $M^n = B(M)Q(M) + R(M) = R(M)$ car $B(M) = 0$.

$$M^n = (2^n - 1)M + (2 - 2^n)I_2 = \begin{pmatrix} 1 & 2^n - 1 \\ 0 & 2^n \end{pmatrix}$$

— **Contrôle** $n = 5$: $\begin{pmatrix} 1 & 31 \\ 0 & 32 \end{pmatrix}$, identique au calcul direct de M^5 ✓

Réponse. $R = (2^n - 1)X + 2 - 2^n$; $M^n = \begin{pmatrix} 1 & 2^n - 1 \\ 0 & 2^n \end{pmatrix}$.

Correction de l'exercice 4 - Reste modulo $X^2 + 1$

a) $X^n = (X^2 + 1)Q + a_n X + b_n$; on évalue en i , racine de $X^2 + 1$:

$$i^n = a_n i + b_n$$

— a_n, b_n sont réels (division dans $\mathbb{R}[X]$) : ce sont la partie imaginaire et la partie réelle de i^n . (L'évaluation en $-i$ donne l'équation conjuguée, rien de plus.)

b) Les puissances de i sont $1, i, -1, -i$ selon $n \equiv 0, 1, 2, 3 \pmod{4}$:

— $n \equiv 0$: $R_n = 1$; $n \equiv 1$: $R_n = X$; $n \equiv 2$: $R_n = -1$; $n \equiv 3$: $R_n = -X$.

c) Le reste est linéaire en le dividende : reste de $P =$ somme des restes. $2026 \equiv 2$ et

$2027 \equiv 3 \pmod{4}$:

$$R = -1 + (-X) + 1 = -X$$

— **Contrôle** : $P(i) = i^{2026} + i^{2027} + 1 = -1 - i + 1 = -i$, et $R(i) = -i$ ✓

d) $X^2 + 1 \mid X^n + 1 \Leftrightarrow$ le reste $R_n + 1$ est nul $\Leftrightarrow R_n = -1 \Leftrightarrow n \equiv 2 \pmod{4}$.

— **Vérification** : $X^2 + 1 \mid X^2 + 1$ ✓ ; $X^6 + 1 = (X^2 + 1)(X^4 - X^2 + 1)$ ✓ ; mais $X^4 + 1$ n'est pas divisible par $X^2 + 1$ (reste 2).

Réponse. $R_n \in \{1, X, -1, -X\}$ selon $n \bmod 4$; reste de P : $-X$; $X^2 + 1 \mid X^n + 1 \Leftrightarrow n \equiv 2 \pmod{4}$.

Correction de l'exercice 5 - Reste par une racine double

a) En $X = 1$: $A(1) = 0 + R(1)$. En dérivant, $A' = 2(X - 1)Q + (X - 1)^2 Q' + R'$, qui en 1 donne $A'(1) = R'(1)$.

b) $R = aX + b$ avec $R(1) = 1^n = 1$ et $R'(1) = a = n \times 1^{n-1} = n$:

$$R = nX - (n - 1)$$

— **Contrôle** $n = 2$: $X^2 = (X - 1)^2 + 2X - 1$ ✓ ; $n = 5$: $R = 5X - 4$ (confirmé par la division).

c) Soit $P = nX^{n+1} - (n + 1)X^n + 1$: $P(1) = n - (n + 1) + 1 = 0$ et $P'(X) = n(n + 1)X^n - n(n + 1)X^{n-1}$, donc $P'(1) = 0$.

— 1 est racine au moins **double** : $(X - 1)^2 \mid P$.

d) $\sum_{k=0}^n x^k = \frac{x^{n+1} - 1}{x - 1}$. On dérive (quotient) :

$$\sum_{k=1}^n kx^{k-1} = \frac{(n+1)x^n(x-1) - (x^{n+1} - 1)}{(x-1)^2} = \frac{nx^{n+1} - (n+1)x^n + 1}{(x-1)^2}$$

— Le numérateur est exactement le P de c) : c) garantit que ce quotient est un **polynôme**, cohérent avec le membre de gauche.

— **Contrôle** $n = 2, x = 2$: $1 + 2 \times 2 = 5$; formule : $\frac{2 \times 8 - 3 \times 4 + 1}{1} = 5$ ✓

Réponse. Reste de X^n par $(X - 1)^2$: $nX - (n - 1)$; $\sum_{k=1}^n kx^{k-1} = \frac{nx^{n+1} - (n+1)x^n + 1}{(x-1)^2}$.

Correction de l'exercice 6 - Divisibilité par $X^2 + X + 1$

a) j et $j^2 = \bar{j}$ sont les racines de $X^2 + X + 1$ (racines cubiques de l'unité autres que 1), distinctes. $X^2 + X + 1 \mid P_n \Leftrightarrow P_n(j) = P_n(\bar{j}) = 0$. Comme P_n est à coefficients réels, $P_n(\bar{j}) = \overline{P_n(j)}$: il suffit que $P_n(j) = 0$.

b) $1 + j + j^2 = 0$ donne $1 + j = -j^2$. Donc

$$P_n(j) = (-j^2)^n - j^n - 1 = (-1)^n j^{2n} - j^n - 1$$

c) $j^3 = 1$: j^n ne dépend que de $n \bmod 3$, et $(-1)^n$ de $n \bmod 2$; on étudie donc $n \bmod 6$.

$n \bmod 6$	$(-1)^n$	j^n	j^{2n}	$P_n(j)$
0	1	1	1	$1 - 1 - 1 = -1$
1	-1	j	j^2	$-j^2 - j - 1 = 0$
2	1	j^2	j	$j - j^2 - 1 = 2j \neq 0$
3	-1	1	1	-3
4	1	j	j^2	$j^2 - j - 1 = 2j^2 \neq 0$
5	-1	j^2	j	$-j - j^2 - 1 = 0$

— (Pour $n \equiv 2$: $-j^2 - 1 = j$ puisque $1 + j + j^2 = 0$, donc $j - j^2 - 1 = 2j$; de même $j^2 - j - 1 = 2j^2$ pour $n \equiv 4$.)

— **Conclusion** : $X^2 + X + 1 \mid P_n \Leftrightarrow n \equiv 1 \text{ ou } 5 \pmod{6}$, c'est-à-dire n premier avec 6.

d) $P_5 = (X + 1)^5 - X^5 - 1 = 5X^4 + 10X^3 + 10X^2 + 5X = 5X(X^3 + 2X^2 + 2X + 1)$.

— $X^3 + 2X^2 + 2X + 1 = (X + 1)(X^2 + X + 1) \checkmark$ Donc $P_5 = 5X(X + 1)(X^2 + X + 1)$.

Réponse. $X^2 + X + 1 \mid (X + 1)^n - X^n - 1 \Leftrightarrow n \equiv \pm 1 \pmod{6}$; $P_5 = 5X(X + 1)(X^2 + X + 1)$.

Correction de l'exercice 7 - Lemme de Gauss et polynômes imposés

a) On cherche U, V avec $(X - 1)U + (X^2 + 1)V = 1$. La division $X^2 + 1 = (X - 1)(X + 1) + 2$ donne :

$$\frac{1}{2}(X^2 + 1) - \frac{1}{2}(X + 1)(X - 1) = 1$$

— $U = -\frac{X+1}{2}, V = \frac{1}{2}$: ils sont **premiers entre eux**. (Autre argument : aucune racine complexe commune, $1 \notin \{i, -i\}$.)

b) $P = (X - 1)S$; $X^2 + 1$ divise $(X - 1)S$ et est premier avec $X - 1$: par **Gauss**, $X^2 + 1 \mid S$. Donc $(X - 1)(X^2 + 1) \mid P$.

c) P réel ou complexe ? L'énoncé ne l'impose pas : cherchons dans $\mathbb{C}[X]$. $P(1) = P(i) = 0$ et $\deg P = 3$: $P = (X - 1)(X - i)(aX + b)$.

— $P(0) = (-1)(-i)b = ib = 2$, donc $b = -2i$, et $a \neq 0$ quelconque :
 $P = (X - 1)(X - i)(aX - 2i)$.

— **Dans** $\mathbb{R}[X]$: $P(i) = 0$ entraîne $P(-i) = 0$; par b), $P = c(X - 1)(X^2 + 1)$ et $P(0) = -c = 2$:
 $P = -2(X - 1)(X^2 + 1)$ (c'est le cas $a = -2$).

d) Dans $\mathbb{R}[X]$: $P = (X - 1)(X^2 + 1)(\alpha X + \beta)$ avec $P(0) = -\beta = 2$:

$$P = (X - 1)(X^2 + 1)(\alpha X - 2), \quad \alpha \in \mathbb{R}$$

— $\alpha = 0$ redonne le degré 3 ; $\alpha \neq 0$ donne un degré 4. **Contrôle** : $P(0) = (-1)(1)(-2) = 2$
 $\checkmark$

Réponse. $\frac{1}{2}(X^2 + 1) - \frac{1}{2}(X + 1)(X - 1) = 1$; dans $\mathbb{R}[X]$: $P = -2(X - 1)(X^2 + 1)$ en degré 3,
 $P = (X - 1)(X^2 + 1)(\alpha X - 2)$ en degré ≤ 4 .

Correction de l'exercice 8 - Irréductibilité

a) Si P (degré 2 ou 3) se factorise en produit de deux polynômes non constants, les degrés possibles sont $1 + 1$ ou $1 + 2$: l'un des facteurs est de **degré** 1, $a(X - r)$, et $r \in K$ est racine. Réciproquement, une racine r donne le facteur $X - r$.

b) $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$: **réductible** dans $\mathbb{R}[X]$.

— Dans $\mathbb{Q}[X]$: ses racines $\pm\sqrt{2}$ sont irrationnelles, donc il n'a pas de racine dans $\mathbb{Q}$: **irréductible** par a).

c) Une racine rationnelle irréductible $\frac{p}{q}$ vérifierait $p \mid -1$ et $q \mid 1$ (plaquette 1 de l'arithmétique) : candidats ± 1 .

$$P(1) = 1 - 1 - 1 = -1 \neq 0, \quad P(-1) = -1 + 1 - 1 = -1 \neq 0$$

— Aucune racine rationnelle et degré 3 : **irréductible** sur $\mathbb{Q}$.

d) $x^4 + 4 > 0$ pour tout réel : aucune racine réelle. Mais (identité de Sophie Germain) :

$$X^4 + 4 = (X^2 + 2X + 2)(X^2 - 2X + 2)$$

— Facteurs à coefficients **entiers** : réductible dans $\mathbb{Q}[X]$ et $\mathbb{R}[X]$.

— a) ne s'applique pas : en degré 4, on peut avoir deux facteurs de degré 2 **sans racine**.
« Pas de racine » n'implique « irréductible » qu'en degré 2 ou 3.

Réponse. $X^2 - 2$: irréductible sur $\mathbb{Q}$, pas sur $\mathbb{R}$; $X^3 - X - 1$ irréductible sur $\mathbb{Q}$;
 $X^4 + 4 = (X^2 + 2X + 2)(X^2 - 2X + 2)$.

Correction de l'exercice 9 - Diviseurs $X^2 + aX + b$ de $X^4 + 1$

a) $z^4 = -1 = e^{i\pi}$: $z = e^{i(2k+1)\pi/4}$, $k = 0, 1, 2, 3$, soit $\frac{\pm 1 \pm i}{\sqrt{2}}$.

b) $(X - e^{i\pi/4})(X - e^{-i\pi/4}) = X^2 - 2\cos\frac{\pi}{4}X + 1 = X^2 - \sqrt{2}X + 1$; de même avec $\frac{3\pi}{4}$:

$$X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$$

— **Vérification** : $(X^2 + 1)^2 - 2X^2 = X^4 + 1$ ✓

c) Un diviseur unitaire réel de degré 2 a pour racines deux racines de $X^4 + 1$ **stables par conjugaison** (sinon ses coefficients ne seraient pas réels) : il faut prendre une paire conjuguée.

— Deux possibilités : $(a, b) = (-\sqrt{2}, 1)$ ou $(\sqrt{2}, 1)$.

d) Dans $\mathbb{C}[X]$, tout choix de **deux racines distinctes** parmi quatre donne un diviseur unitaire : $\binom{4}{2} = 6$ diviseurs.

— Par exemple $(X - e^{i\pi/4})(X - e^{3i\pi/4}) = X^2 - i\sqrt{2}X - 1$ (somme des racines $i\sqrt{2}$, produit $e^{i\pi} = -1$), non réel.

Réponse. $X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$; $(a, b) = (\pm\sqrt{2}, 1)$; 6 diviseurs unitaires de degré 2 dans $\mathbb{C}[X]$.

Correction de l'exercice 10 - Reste par trois racines

a) $\deg B = 3$ donc $\deg R \leq 2$. En évaluant $X^n = BQ + R$ en 0, 1 et -1 (racines de B) :

$$R(0) = 0, \quad R(1) = 1, \quad R(-1) = (-1)^n$$

b) $R = aX^2 + bX$ (car $R(0) = 0$), avec $a + b = 1$ et $a - b = (-1)^n$.

— **n pair** : $a - b = 1$, d'où $a = 1$, $b = 0$: $R = X^2$.

— **n impair** : $a - b = -1$, d'où $a = 0$, $b = 1$: $R = X$.

— **Explication directe** : $X^3 \equiv X$ modulo B , donc $X^{2k} \equiv X^2$ et $X^{2k+1} \equiv X$ par récurrence.

c) Par linéarité du reste : $X^{100} \rightarrow X^2$, $X^{51} \rightarrow X$, $3 \rightarrow 3$. Reste : $X^2 + X + 3$.

— **Contrôle** en $X = -1 : 1 - 1 + 3 = 3$ et $R(-1) = 1 - 1 + 3 = 3 \checkmark$; en $X = 1 : 5 = 5 \checkmark$

d) $M^3 - M = 0$: on substitue M dans $X^n = BQ + R$, et $B(M) = 0$:

— $M^{100} = M^2$ et $M^{51} = M$.

— **Exemple** : une matrice de symétrie S ($S^2 = I$) vérifie $S^3 = S$; on retrouve $S^{100} = S^2 = I \checkmark$

Réponse. $R = X^2$ si n pair, $R = X$ si n impair ; reste $X^2 + X + 3$; $M^{100} = M^2$, $M^{51} = M$.

Correction de l'exercice 11 - Polynômes à coefficients entiers

a) $P = \sum c_k X^k$ avec $c_k \in \mathbb{Z}$. Alors $P(a) - P(b) = \sum c_k (a^k - b^k)$, et chaque terme est divisible par $a - b$:

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \dots + b^{k-1})$$

b) Il faudrait $3 - 1 = 2 \mid P(3) - P(1) = 3$: **impossible**.

— (En revanche $P = \frac{3X+1}{2}$ vérifie ces valeurs, mais n'est pas à coefficients entiers.)

c) Soit $n \in \mathbb{Z}$. Si n est pair, $n - 0$ est pair et divise $P(n) - P(0)$: $P(n) \equiv P(0) \pmod{2}$ est **impair**. Si n est impair, $n - 1$ est pair : $P(n) \equiv P(1) \pmod{2}$, impair.

— Dans les deux cas $P(n)$ est impair, donc non nul : pas de racine entière.

d) $P(0) = 1$ (impair) et $P(1) = 1 - 3 + 2 + 7 + 1 = 8$: pair ! Le critère c) ne s'applique pas directement.

— On raisonne autrement : une racine entière n diviserait le coefficient constant 1 (car $n \mid P(n) - P(0) = -1$ d'après a) avec $b = 0$) : $n = \pm 1$.

— $P(1) = 8 \neq 0$ et $P(-1) = -1 - 3 - 2 - 7 + 1 = -12 \neq 0$. **Aucune racine entière**.

— **Leçon** : un critère de parité peut échouer ; la divisibilité par $a - b$ reste l'outil de base.

Réponse. $a - b \mid P(a) - P(b)$; b) impossible ; c) $P(n)$ toujours impair ; d) seuls candidats ± 1 , qui ne sont pas racines.

Correction de l'exercice 12 - Construire C à partir de $\mathbb{R}[X]$

a) Par division euclidienne, tout P s'écrit $(X^2 + 1)Q + R$ avec $\deg R \leq 1$: $P \equiv R = a + bX$. L'unicité du reste donne l'unicité de (a, b) .

b) $(a + bX)(c + dX) = ac + (ad + bc)X + bdX^2$, et $X^2 \equiv -1$:

$$(a + bX)(c + dX) \equiv (ac - bd) + (ad + bc)X \pmod{X^2 + 1}$$

— C'est exactement la multiplication de $(a + bi)(c + di)$: la classe de X joue le rôle de i . On **construit** ainsi $\mathbb{C}$ comme $\mathbb{R}[X] / (X^2 + 1)$.

c) Bézout : $(1 + X)(1 - X) = 1 - X^2 = 2 - (X^2 + 1)$, donc

— $(1 + X)\frac{1-X}{2} \equiv 1 \pmod{X^2 + 1}$: l'inverse est $\frac{1-X}{2}$.

— **Contrôle** : $\frac{1}{1+i} = \frac{1-i}{2} \checkmark$

d) $X^2 - 1 = (X - 1)(X + 1)$ est **réductible** : modulo $X^2 - 1$, $(X - 1)(X + 1) \equiv 0$ alors qu'aucun facteur n'est congru à 0. Il y a des **diviseurs de zéro**, donc pas de corps.

— **Règle** : $K[X] / (P)$ est un corps si et seulement si P est irréductible — l'analogie de « $\mathbb{Z} / n\mathbb{Z}$ corps $\Leftrightarrow n$ premier ».

Réponse. $(a + bX)(c + dX) \equiv (ac - bd) + (ad + bc)X$; inverse de $1 + X$: $\frac{1-X}{2}$; $X^2 - 1$

réductible : diviseurs de zéro.

Correction de l'exercice 13 - Racines communes et PGCD

a) $B(-1) = -1 + 2 - 2 + 1 = 0$. On factorise par $X + 1$:

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

— (Développer : $X^3 + X^2 + X + X^2 + X + 1$ ✓)

b) $(X^2 + 1)(X^2 + X + 1) = X^4 + X^3 + X^2 + X^2 + X + 1 = X^4 + X^3 + 2X^2 + X + 1$ ✓

c) Les facteurs irréductibles de A sur $\mathbb{R}$ sont $X^2 + 1$ et $X^2 + X + 1$; ceux de B sont $X + 1$ et $X^2 + X + 1$.

— $\text{pgcd}(A, B) = X^2 + X + 1$; racines communes : j et $j^2 = \bar{j}$.

d) $A = (X - 1)B + R$ avec $R = A - (X - 1)B$. On calcule

$$(X - 1)B = X^4 + 2X^3 + 2X^2 + X - X^3 - 2X^2 - 2X - 1 = X^4 + X^3 - X - 1.$$

— $R = 2X^2 + 2X + 2 = 2(X^2 + X + 1)$.

— Puis $B = (X + 1)(X^2 + X + 1)$: le reste suivant est **nul**. Dernier reste non nul normalisé : $X^2 + X + 1$ ✓

Réponse. $B = (X + 1)(X^2 + X + 1)$; $\text{pgcd}(A, B) = X^2 + X + 1$, racines communes j, j^2 .

Correction de l'exercice 14 - Division par un polynôme paramétré

a) Le reste $R = \alpha X + \beta$ vérifie $R(j) = P(j)$ (et $R(\bar{j}) = P(\bar{j})$, conjugué car tout est réel). Avec $j^3 = 1, j^4 = j$ et $j^2 = -1 - j$:

$$P(j) = j + a(-1 - j) + b = (1 - a)j + (b - a)$$

— Donc $R = (1 - a)X + (b - a)$ (deux polynômes de degré ≤ 1 égaux en $j \notin \mathbb{R}$ ont mêmes coefficients).

b) $B \mid P \Leftrightarrow R = 0 \Leftrightarrow a = 1$ et $b = a = 1$.

c) $P = X^4 + X^2 + 1$ et $P = (X^2 + X + 1)(X^2 - X + 1)$.

— **Vérification** : $(X^2 + 1 + X)(X^2 + 1 - X) = (X^2 + 1)^2 - X^2 = X^4 + X^2 + 1$ ✓

d) C'est exactement l'identité utilisée dans la vérification : **différence de deux carrés**.

— **Méthode** : pour un reste modulo un diviseur à racines non réelles, on évalue en une racine complexe et on identifie ; une seule évaluation suffit (la conjuguée donne la même information).

Réponse. Reste $(1 - a)X + (b - a)$; $B \mid P \Leftrightarrow a = b = 1$;

$$X^4 + X^2 + 1 = (X^2 + X + 1)(X^2 - X + 1).$$

Correction de l'exercice 15 - Synthèse : Bézout pour deux polynômes premiers entre eux

a) Les racines complexes de A (1, double) et de B ($\pm i$) sont distinctes : pas de racine commune, donc $A \wedge B = 1$.

b) Euclide : $A = X^2 - 2X + 1 = 1 \times B + (-2X)$; puis $B = (-2X)\left(-\frac{X}{2}\right) + 1$.

— On remonte : la seconde division donne $1 = B - (-2X)\left(-\frac{X}{2}\right) = B + \frac{X}{2}(-2X)$, et la première $-2X = A - B$.

— Donc $1 = B + \frac{X}{2}(A - B) = \frac{X}{2}A + \left(1 - \frac{X}{2}\right)B$.

$$U = \frac{X}{2}, \quad V = 1 - \frac{X}{2}$$

— **Vérification** : $\frac{X}{2}(X^2 - 2X + 1) + \left(1 - \frac{X}{2}\right)(X^2 + 1) = \frac{X^3 - 2X^2 + X}{2} + X^2 + 1 - \frac{X^3 + X}{2} = 1$
✓

c) On divise $AU + BV = 1$ par AB :

$$F = \frac{1}{AB} = \frac{V}{A} + \frac{U}{B} = \frac{1 - \frac{X}{2}}{(X-1)^2} + \frac{X/2}{X^2 + 1}$$

— On décompose le premier terme : $1 - \frac{X}{2} = -\frac{1}{2}(X-1) + \frac{1}{2}$, donc

$$\frac{1 - X/2}{(X-1)^2} = -\frac{1}{2(X-1)} + \frac{1}{2(X-1)^2}.$$

— **Décomposition sur $\mathbb{R}$** : $F = -\frac{1}{2(X-1)} + \frac{1}{2(X-1)^2} + \frac{X}{2(X^2 + 1)}.$

d) En $X = 0$: $F(0) = 1$; décomposition : $\frac{1}{2} + \frac{1}{2} + 0 = 1$ ✓

— **Méthode** : une relation de Bézout entre les facteurs du dénominateur **sépare** la fraction en deux morceaux ; c'est la preuve de l'existence de la décomposition en éléments simples.

Réponse. $\frac{X}{2}(X-1)^2 + \left(1 - \frac{X}{2}\right)(X^2 + 1) = 1$; $F = -\frac{1}{2(X-1)} + \frac{1}{2(X-1)^2} + \frac{X}{2(X^2 + 1)}.$