Plaquette 2 – Arithmétique de K[X] : division, PGCD, racines

Polynômes — Prépa MP / MPI (2e année)

Corrections détaillées

Boîte à outils

Division et arithmétique.

— Division euclidienne : $A = BQ + R$, $\deg R < \deg B$, unicité.

— $D = A \wedge B$ unitaire, $AU + BV = D$ (Bézout) ; $A \mid BC$ et $A \wedge B = 1 \Rightarrow A \mid C$ (Gauss).

— Irréductibles : sur $\mathbb{C}$, les $X - a$; sur $\mathbb{R}$, les $X - a$ et les $X^2 + pX + q$ avec $p^2 - 4q < 0$.

Racines.

— a racine d'ordre $m \Leftrightarrow (X-a)^m \mid P$ et $(X-a)^{m+1} \nmid P$
$\Leftrightarrow P(a) = \ldots = P^{(m-1)}(a) = 0 \neq P^{(m)}(a)$.

— P a une racine multiple $\Leftrightarrow P \wedge P' \neq 1$.

— Pour $P = a_n \prod (X - x_i)$ et σ_k les fonctions symétriques élémentaires des racines :

$$\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$$

— **Lagrange** : il existe un unique P de degré $\leq n$ prenant des valeurs données en $n+1$ points distincts.

Correction de l'exercice 1 – Division euclidienne et reste par évaluation

a) On abaisse le degré terme à terme : $X^5 = X^3(X^2+1) - X^3$, donc $A = X^3B + X^3 - X + 1$; puis $X^3 = X(X^2+1) - X$, donc $X^3 - X + 1 = XB - 2X + 1$. Ainsi

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

— Quotient $X^3 + X$, reste $1 - 2X$ (de degré $1 < 2$).

b) Le reste s'écrit $R = aX + b$ avec a, b réels. En évaluant en i, racine de B :
$A(i) = i^5 + 2i^3 - i + 1 = i - 2i - i + 1 = 1 - 2i$, et $R(i) = ai + b$. Par identification des parties réelle et imaginaire, $b = 1$ et $a = -2$: $R = 1 - 2X$.

Réponse. $A = (X^2+1)(X^3+X) + 1 - 2X$.

Correction de l'exercice 2 – Algorithme d'Euclide

a) Première division : $A = (X-2)B + R_1$ avec $R_1 = 2X^3 + X^2 - 2X - 1$.

— Deuxième division : $B = \left(\frac{X}{2} + \frac{1}{4}\right) R_1 + R_2$ avec $R_2 = \frac{3}{4}(X^2 - 1)$.

— Troisième division : $R_1 = (2X+1)(X^2-1)$, reste nul.

— Le dernier reste non nul, rendu unitaire, est le PGCD :

$$A \wedge B = X^2 - 1$$

b) $A = X^4(X-1) - (X-1) = (X-1)(X^4-1) = (X-1)^2(X+1)(X^2+1)$ et
$B = X^3(X+1) - (X+1) = (X+1)(X^3-1) = (X+1)(X-1)(X^2+X+1)$. Facteurs communs avec le plus petit exposant : $(X-1)(X+1) = X^2 - 1$ ✓.

Réponse. $A \wedge B = X^2 - 1$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Correction de l'exercice 3 – Reste de X^n par $(X-1)^2$

Le reste est de degré ≤ 1 : $X^n = (X-1)^2 Q + aX + b$.

— En évaluant en 1 : $1 = a + b$.

— En dérivant : $nX^{n-1} = 2(X-1)Q + (X-1)^2 Q' + a$, puis en évaluant en 1 (racine **double**, donc annule aussi la dérivée du premier terme) : $n = a$.

— Donc $b = 1 - n$ et

$$X^n \equiv nX + 1 - n \pmod{(X-1)^2}$$

— Vérification pour $n = 2$: $X^2 = (X-1)^2 + 2X - 1$ ✓.

— Application matricielle : si $(A-I)^2 = 0$, alors $A^n = nA + (1-n)I$.

Réponse. $R = nX + 1 - n$.

Correction de l'exercice 4 – Reste par $X^2 + X + 1$

a) j et $\bar{j}$ sont les racines de $X^2 + X + 1$ (car $X^3 - 1 = (X-1)(X^2+X+1)$ et $j^3 = 1$, $j \neq 1$). Et $X^3 - 1 = (X-1)(X^2+X+1)$ montre $X^3 \equiv 1$.

b) Pour $n = 3q + r$: $X^n = (X^3)^q X^r \equiv X^r$. Donc le reste vaut 1 si $n \equiv 0$, X si $n \equiv 1$, et $X^2 \equiv -X - 1$ si $n \equiv 2 \pmod 3$.

c) Divisibilité $\Leftrightarrow$ j et $\bar{j}$ racines (racines simples), $\Leftrightarrow j^{2n} + j^n + 1 = 0$ (l'autre condition s'en déduit par conjugaison).

— Si $3 \mid n$: $1 + 1 + 1 = 3 \neq 0$.

— Sinon $j^n \in \{j, j^2\}$ et j^{2n} est l'autre, d'où $1 + j + j^2 = 0$.

$$X^2 + X + 1 \mid X^{2n} + X^n + 1 \Leftrightarrow 3 \nmid n$$

Réponse. Restes 1, X, $-X-1$ selon le reste de n modulo 3 ; divisibilité si et seulement si $3 \nmid n$.

Correction de l'exercice 5 – Racine double et paramètre

a) Une racine multiple x annule P et $P' = 3X^2 - 3$, donc $x = \pm 1$.

— $P(1) = a - 2 = 0 \Leftrightarrow a = 2$: $X^3 - 3X + 2 = (X-1)^2(X+2)$.

— $P(-1) = a + 2 = 0 \Leftrightarrow a = -2$: $X^3 - 3X - 2 = (X+1)^2(X-2)$.

b) Soit $Q = nX^{n+1} - (n+1)X^n + 1$. Alors $Q(1) = n - (n+1) + 1 = 0$ et

$$Q' = n(n+1)X^n - n(n+1)X^{n-1}, \qquad Q'(1) = 0$$

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

Réponse. $a = 2$: $(X-1)^2(X+2)$; $a = -2$: $(X+1)^2(X-2)$; $Q(1) = Q'(1) = 0$.

Correction de l'exercice 6 – Factorisation de X^6 - 1

a) Ce sont les $\omega_k = \mathrm{e}^{ik\pi/3}$, $k = 0, \ldots, 5$: $1, -1, \mathrm{e}^{\pm i\pi/3}, \mathrm{e}^{\pm 2i\pi/3}$.

b) Dans $\mathbb{C}[X]$: $X^6 - 1 = \prod_{k=0}^{5} (X - \omega_k)$. Dans $\mathbb{R}[X]$, on regroupe les racines conjuguées : $(X - \mathrm{e}^{i\theta})(X - \mathrm{e}^{-i\theta}) = X^2 - 2\cos\theta\, X + 1$. Avec $\theta = \frac{\pi}{3}$ et $\frac{2\pi}{3}$:

$$X^6 - 1 = (X-1)(X+1)(X^2 - X + 1)(X^2 + X + 1)$$

c) Les racines sont $\mathrm{e}^{\pm i\pi/4}$, $\mathrm{e}^{\pm 3i\pi/4}$. En regroupant : $X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

On le retrouve aussi par $X^4+1=(X^2+1)^2-2X^2$, différence de deux carrés. (Aucune racine réelle, et pourtant X^4+1 n'est pas irréductible sur $\mathbb{R}$.)

Réponse. $X^6-1=(X-1)(X+1)(X^2-X+1)(X^2+X+1)$;
$X^4+1=(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$.

Correction de l'exercice 7 – Relations coefficients-racines

a) $P=X^3+0X^2-2X+1$: $\sigma_1=0$, $\sigma_2=-2$, $\sigma_3=-1$.

b) $a^2+b^2+c^2=\sigma_1^2-2\sigma_2=0+4=4$. Et $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}=\frac{bc+ca+ab}{abc}=\frac{\sigma_2}{\sigma_3}=2$.

c) Chaque racine vérifie $x^3=2x-1$; en sommant :

$$a^3+b^3+c^3=2\sigma_1-3=-3$$

— Vérification : $P=(X-1)(X^2+X-1)$; les racines φ, ψ du second facteur vérifient $\varphi+\psi=-1$ et $\varphi\psi=-1$, donc $\varphi^2+\psi^2=1+2=3$, et avec la racine 1 on retrouve $1+3=4$ ✓.

Réponse. $\sigma_1=0$, $\sigma_2=-2$, $\sigma_3=-1$; $\sum a^2=4$, $\sum\frac{1}{a}=2$, $\sum a^3=-3$.

Correction de l'exercice 8 – Relation de Bézout explicite

a) Un diviseur commun non constant aurait pour racine (complexe) une racine commune ; or -1 n'annule pas X^2+1. Premiers entre eux.

b) Division : $X^2+1=(X+1)(X-1)+2$. Donc $2=(X^2+1)-(X+1)(X-1)$ et

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

— $U=\frac{1}{2}$, $V=\frac{1-X}{2}$.

c) On évalue en A : $\frac{1}{2}(A^2+I)+\frac{I-A}{2}(A+I)=I$, avec $A^2+I=0$. Donc $(A+I)$ est inversible et $(A+I)^{-1}=\frac{I-A}{2}$. Vérification : $(A+I)(I-A)=I-A^2=2I$ ✓.

Réponse. $U=\frac{1}{2}$, $V=\frac{1-X}{2}$; $(A+I)^{-1}=\frac{1}{2}(I-A)$.

Correction de l'exercice 9 – Partie sans facteur carré

a) $P'=4X^3-6X^2+2=2(2X^3-3X^2+1)$, et 1 est racine : $2X^3-3X^2+1=(X-1)^2(2X+1)$. Comme $P(1)=0$ et $P\left(-\frac{1}{2}\right)=\frac{1}{16}+\frac{1}{4}-1-1\neq 0$, on obtient par divisions successives

$$P\wedge P'=(X-1)^2$$

b) 1 est racine de P de multiplicité 3 (ordre de multiplicité dans $P\wedge P'$ plus un). Le quotient $\frac{P}{(X-1)^3}=X+1$: $P=(X-1)^3(X+1)$.

c) Si $P=c\prod(X-a_i)^{m_i}$, alors a_i est racine de P' d'ordre exactement m_i-1, donc $P\wedge P'=\prod(X-a_i)^{m_i-1}$ et $\frac{P}{P\wedge P'}=c\prod(X-a_i)$: mêmes racines, toutes simples.

Réponse. $P\wedge P'=(X-1)^2$; $P=(X-1)^3(X+1)$.

Correction de l'exercice 10 – Interpolation de Lagrange

a) $L_0=\frac{(X-1)(X-2)}{2}$, $L_1=-X(X-2)$, $L_2=\frac{X(X-1)}{2}$. Donc

$$P=L_0+3L_1+7L_2=\frac{X^2-3X+2}{2}-3X^2+6X+\frac{7X^2-7X}{2}=X^2+X+1$$

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— Vérification : $P(0)=1$, $P(1)=3$, $P(2)=7$ ✓.

b) $Q-P$ s'annule en 0, 1, 2 : $Q=P+X(X-1)(X-2)R$ avec $R\in\mathbb{R}[X]$ quelconque.

c) $L_0+L_1+L_2$ et 1 sont de degré ≤ 2 et coïncident en trois points (valeur 1) : égaux par unicité. Même argument pour X, qui prend les valeurs $0,1,2$.

Réponse. $P=X^2+X+1$; $Q=P+X(X-1)(X-2)R$.

Correction de l'exercice 11 – Polynômes de Tchebychev

a) $T_2=2X^2-1$, $T_3=2X(2X^2-1)-X=4X^3-3X$. Par récurrence double, avec $\cos((n+1)\theta)+\cos((n-1)\theta)=2\cos\theta\cos(n\theta)$:

$$T_{n+1}(\cos\theta)=2\cos\theta\cos(n\theta)-\cos((n-1)\theta)=\cos((n+1)\theta)$$

b) Par récurrence, T_n est de degré n et de coefficient dominant 2^{n-1} (multiplié par 2 à chaque étape à partir de T_1).

c) $\cos(n\theta)=0$ pour $\theta_k=\frac{(2k+1)\pi}{2n}$, $k=0,\dots,n-1$; les $x_k=\cos\theta_k$ sont n réels **distincts** de $]-1,1[$ ($\cos$ est injectif sur $[0,\pi]$). Ce sont donc toutes les racines :

— $T_n=2^{n-1}\prod_{k=0}^{n-1}\left(X-\cos\frac{(2k+1)\pi}{2n}\right)$.

Réponse. $T_3=4X^3-3X$; $\deg T_n=n$, coefficient dominant 2^{n-1} ; racines $\cos\frac{(2k+1)\pi}{2n}$.

Correction de l'exercice 12 – Polynômes positifs sur R

a) Si a est racine d'ordre m impair, $P=(X-a)^mQ$ avec $Q(a)\neq 0$; P change de signe en a (Q est de signe constant au voisinage de a). Contradiction.

b) $P=c\prod(X-a_j)^{2m_j}\prod((X-z_k)(X-\overline{z}_k))^{n_k}$, avec $c>0$ (signe en $+\infty$) ou $P=0$. On pose $A=\prod(X-a_j)^{m_j}\prod(X-z_k)^{n_k}$; alors $\overline{A}=\prod(X-a_j)^{m_j}\prod(X-\overline{z}_k)^{n_k}$ et $P=c A\overline{A}$.

c) $A\overline{A}=(B+iC)(B-iC)=B^2+C^2$, donc

$$P=(\sqrt{c}B)^2+(\sqrt{c}C)^2$$

d) $X^4+1=(X^2-1)^2+2X^2=(X^2-1)^2+\left(\sqrt{2}X\right)^2$.

Réponse. Multiplicités paires ; $P=cA\overline{A}=B^2+C^2$; $X^4+1=(X^2-1)^2+(\sqrt{2}X)^2$.

Correction de l'exercice 13 – Si P est scindé sur R, P' aussi

a) Une racine d'ordre m de P est racine d'ordre $m-1$ de P' (si $m=1$, ce n'est pas une racine de P').

b) $P(a_i)=P(a_{i+1})=0$ et P est dérivable : Rolle fournit $b_i\in]a_i,a_{i+1}[$ avec $P'(b_i)=0$. Ces b_i sont distincts des a_j.

c) On obtient au moins

$$\sum_{i=1}^{r}(m_i-1)+(r-1)=n-r+r-1=n-1$$

— racines de P' comptées avec multiplicité, et $\deg P'=n-1$: ce sont toutes ses racines, P' est scindé sur $\mathbb{R}$.

— Exemple : $P=X^3-X$ a pour racines $-1,0,1$; $P'=3X^2-1$ a pour racines $\pm\frac{1}{\sqrt{3}}$, une dans chaque intervalle.

Réponse. $n-r$ racines aux a_i et $r-1$ par Rolle : $n-1=\deg P'$ racines réelles.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Correction de l'exercice 14 – L'équation P(X²) = P(X)P(X + 1)

a) $P(a^2) = P(a)P(a+1) = 0$. La suite $a, a^2, a^4, \dots$ est formée de racines ; P en a un nombre fini, donc les a^{2^k} ne sont pas tous distincts, ce qui impose $a = 0$ ou $|a| = 1$ (sinon les modules $|a|^{2^k}$ sont distincts).

b) $P((a-1)^2) = P(a-1)P(a) = 0$. Par a) appliqué à $(a-1)^2$: $(a-1)^2 = 0$ ou $|a-1| = 1$.

c) Une racine $a \neq 0, 1$ vérifie $|a| = |a-1| = 1$, d'où $a = \mathrm{e}^{\pm i\pi/3}$. Mais alors $a^2 = \mathrm{e}^{\pm 2i\pi/3}$ est racine et $|a^2 - 1| = \sqrt{3} \neq 1$: contradiction. Donc $P = cX^p(X-1)^q$. Coefficients dominants : $c = c^2$, donc $c = 1$. Et

$$P(X^2) = X^{2p}(X-1)^q(X+1)^q, \qquad P(X)P(X+1) = X^{p+q}(X-1)^q(X+1)^p$$

— d'où $p = q$: $P = (X^2 - X)^p$, $p \in \mathbb{N}$.

Réponse. $P = (X^2 - X)^p$, $p \in \mathbb{N}$.

Correction de l'exercice 15 – Synthèse : racines de l'unité et produit de sinus

a) Les ω^k sont n racines distinctes de $X^n - 1$, unitaire de degré n : d'où la factorisation. On divise par $X - 1$: $\dfrac{X^n - 1}{X - 1} = 1 + X + \dots + X^{n-1}$.

b) On évalue en 1 : $\prod_{k=1}^{n-1}(1 - \omega^k) = 1 + 1 + \dots + 1 = n$.

c) $1 - \mathrm{e}^{i\theta} = \mathrm{e}^{i\theta/2}\left(\mathrm{e}^{-i\theta/2} - \mathrm{e}^{i\theta/2}\right) = -2i\,\mathrm{e}^{i\theta/2}\sin\dfrac{\theta}{2}$, de module $2\sin\dfrac{\theta}{2}$. En prenant le module dans b), avec $\theta = \dfrac{2k\pi}{n}$ et $\sin\dfrac{k\pi}{n} > 0$:

$$\prod_{k=1}^{n-1} 2\sin\frac{k\pi}{n} = n \quad\Longrightarrow\quad \prod_{k=1}^{n-1}\sin\frac{k\pi}{n} = \frac{n}{2^{n-1}}$$

d) $n = 3$: $\sin\dfrac{\pi}{3}\sin\dfrac{2\pi}{3} = \dfrac{3}{4} = \dfrac{3}{2^2}$ ✓. $n = 4$: $\dfrac{\sqrt{2}}{2} \times 1 \times \dfrac{\sqrt{2}}{2} = \dfrac{1}{2} = \dfrac{4}{2^3}$ ✓.

Réponse. $\prod(1 - \omega^k) = n$; $\prod_{k=1}^{n-1}\sin\dfrac{k\pi}{n} = \dfrac{n}{2^{n-1}}$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).