HX3 2006/2007 - Fonctions polynômiales

1. Soit $P \in K[X]$. Montrer que $P \circ P - X$ est divisible par $P - X$.

2. Soit $P = a_n X^n + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$, $\lambda \in \mathbb{Z}$, $\mu \in \mathbb{Z}^*$ tel que $\text{pgcd}(\lambda, \mu) = 1$ et $P\left(\frac{\lambda}{\mu}\right) = 0$.

1) Montrer que μ divise a_n, λ divise a_0. En déduire que pour tout polynôme de $\mathbb{Q}[X]$, il est possible de déterminer l'ensemble de ses racines rationnelles.

2) Montrer que $\lambda - \mu$ divise $\sum_{k=0}^{n} a_k$ et $\lambda + \mu$ divise $\sum_{k=0}^{n} (-1)^k a_k$.

3) En déduire que $X^3 + X^2 + X + 2$ est irréductible dans $\mathbb{Q}[X]$.

3. Automorphismes de la K-algèbre $K[X]$:

1) Soit $(a, b) \in K^* \times K$. Montrer que $P \longmapsto P(aX + b)$ est un automorphisme de la K-algèbre $K[X]$.

2) Soit u un automorphisme de la K-algèbre $K[X]$. Vérifier l'existence de $(a, b) \in K^* \times K$ tel que $u(P) = P(aX + b)$.

4. Polynômes pairs et polynômes impairs : On dit que $P \in K[X]$ est pair (resp. impair) si $P(-X) = P(X)$ (resp. $P(-X) = -P(X)$). On écrit $P = \sum_{n \in \mathbb{N}} a_n X^n$. Vérifier l'équivalence des deux propositions :

(i) P pair (resp. impair);

(ii) Pour tout n impair (resp. pair) dans $\mathbb{N}$, $a_n = 0$.

On supposera la caractéristique différente de 2.

5. Soit $a \in \mathbb{C}$, $n \in \mathbb{N}$ impair. On suppose n non multiple de 3. Prouver que $X^2 + aX + a^2$ divise $(X + a)^n - X^n - a^n$.

6. Soient $\theta \in \mathbb{R}$, $n \in \mathbb{N}$. Déterminer dans $\mathbb{R}[X]$ le reste de la division euclidienne de $(\cos\theta + X \sin\theta)^n$ par $X^2 + 1$.

7. Soit $(m, n) \in \mathbb{N}^2$. Déterminer dans $\mathbb{R}[X]$ le quotient et le reste de la division euclidienne de $(X - 2)^m + (X - 1)^n - 1$ par $(X - 1)(X - 2)$.

8. Soient p et q dans $\mathbb{N}^*$ premiers entre eux. Montrer que $(X^p - 1)(X^q - 1)$ divise $(X - 1)(X^{pq} - 1)$ dans $\mathbb{C}[X]$. Qu'en est-il dans $\mathbb{R}[X]$ et $\mathbb{Q}[X]$?

9. Soit $(p, q) \in \mathbb{N}^2$. Calculer le reste de la division euclidienne de $X^p + X^q + 1$ par $X^2 + X + 1$.

10. 1) Donner une CNS sur $(p, q) \in \mathbb{C}^2$ pour que $P = X^2 + pX + q$ divise $P(X^2 + 1)$.

2) Donner une CNS sur $(p, q) \in \mathbb{R}^2$ pour que $X^2 + 2$ divise $X^4 + X^3 + pX^2 + qX + 2$.

11. Montrer que pour tout $n \in \mathbb{N}^*$, $(X - 1)^3$ divise $nX^{n+2} - (n + 2)X^{n+1} + (n + 2)X - n$.

12. Soit $n \in \mathbb{N}^*$. Déterminer le PGCD de $nX^{n+1} - (n + 1)X^n + 1$ et $X^n - nX + (n - 1)$.

13. Soit $P \in K[X]$.

1) Ecrire le reste de la division euclidienne de P par $(X - \alpha)^n$ comme combinaison linéaire de 1, $X - \alpha$,..., $(X - \alpha)^{n-1}$ (K est supposé de caractéristique nulle).

2) Soient α_1,..., α_n n éléments distincts de K. Ecrire le reste de la division euclidienne de P par $\prod_{i=1}^{n} (X - \alpha_i)$ comme combinaison linéaire des polynômes interpolateurs de Lagrange $(L_1, L_2, \ldots, L_n)$ relatifs à α_1,..., α_n.

14. Pour $n \geqslant 2$, on note $P_n = \sum_{k=0}^{n} \frac{X^k}{k!}$. P_n admet-il dans $\mathbb{C}$ des racines multiples?

15. Soit $n \in \mathbb{N}^*$.

1) Factoriser dans $\mathbb{C}[X]$ le polynôme $(X + 1)^n - (X - 1)^n$.

2) En déduire pour tout $p \in \mathbb{N}^*$

$$\prod_{k=1}^{p} \text{cotan}\,\frac{k\pi}{2p+1} = \frac{1}{\sqrt{2p+1}}$$

16. Soit $n \in \mathbb{N}^*$. Montrer que $\displaystyle\prod_{k=1}^{n-1}\left(X - e^{\frac{2ik\pi}{n}}\right) = \sum_{p=0}^{n-1} X^p$. En déduire

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

---

17. Soit $n \in \mathbb{N}^*$. Montrer que pour tout $k \in \{1, 2, \ldots, n-1\}$, $\tan^2 \frac{k\pi}{2n}$ est racine de $\displaystyle\sum_{p=0}^{n-1}(-1)^p C_{2n}^{2p+1} X^p$. En déduire que

$$\sum_{k=1}^{n-1} \tan^2 \frac{k\pi}{2n} = \frac{(n-1)(2n-1)}{3}$$

---

18. Décomposer en facteurs irréductibles dans $\mathbb{R}[X]$ les polynômes suivants :

$$X^6+1; \quad X^6+2X^4+2X^2+1; \quad X^4+2\cos\alpha X^2+1; \quad X^6-2\cos\alpha X^3+1 \quad (\alpha \in \mathbb{R})$$

---

19. Soit $P \in \mathbb{R}[X]$, $P \neq 0$ unitaire. Vérifier l'équivalence des quatre propositions :

(i) Pour tout $x \in \mathbb{R}$, $P(x) \geqslant 0$.

(ii) Toute racine réelle est d'ordre pair.

(iii) Il existe $(A, B) \in \mathbb{R}[X]^2$ tel que $P = A^2 + B^2$.

(iv) Il existe $C \in \mathbb{C}[X]$ tel que $P = \bar{C}C$.

---

20. On suppose K de caractéristique nulle. Soient $P \in K[X]$, $P \neq 0$, $n = \deg P$. Vérifier l'existence d'un unique $\alpha \in K$ tel que $P(X+\alpha)$ soit de la forme $\displaystyle\sum_{k=0}^{n} a_k X^k$ avec $a_{n-1} = 0$.

---

21. On suppose K de caractéristique nulle. Soit $Q \in K[X]$ non nul. On considère $Q = \lambda\prod_{i=1}^{n} P_i^{\alpha_i}$ la décomposition en facteurs irréductibles ($\lambda \in K^*$, P_i irréductible unitaire, $\alpha_i \in \mathbb{N}^*$, $P_i \neq P_j$ si $i \neq j$). Montrer que

$$\mathrm{pgcd}(Q, Q') = \prod_{i=1}^{n} P_i^{\alpha_i - 1}$$

Lorsque $K = \mathbb{C}$, préciser $\dfrac{P}{\mathrm{pgcd}(P, P')}$.

---

22. Soient λ_1, λ_2,..., λ_n n éléments distincts de K.

1) Montrer que

$$A = \begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \ldots & \lambda_1^{n-1} \\ 1 & \lambda_2 & \lambda_2^1 & \ldots & \lambda_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \lambda_n & \lambda_n^2 & \ldots & \lambda_n^{n-1} \end{pmatrix} = (\lambda_i^{j-1})_{1\leqslant i,j\leqslant n} \in \mathrm{GL}_{\ n}(K)$$

2) Calculer A^{-1} à l'aide des polynômes interpolateur de Lagrange.

3) Soit $P \in K[X]$, $\deg P = n-1$. Montrer que si la caractéristique de K est nulle, $(P(X+\lambda_1), P(X+\lambda_2), \ldots, P(X+\lambda_n))$ est une base du K-espace vectoriel $\{Q \in K[X],\ \deg Q < n\}$.

---

23. Soient $f : I \longrightarrow \mathbb{R}$ de classe $\mathcal{D}^n$, a_0, a_1,..., a_n $n+1$ points distincts de I.

1) On suppose que $f(a_0) = f(a_1) = \ldots = f(a_n) = 0$. Vérifier l'existence de $c \in I$ tel que $f^{(n)}(c) = 0$.

2) Vérifier l'existence de $c \in I$ tel que

$$\sum_{k=0}^{n} \frac{f(a_k)}{(a_k - a_0)\ldots\widehat{(a_k - a_k)}\ldots(a_k - a_n)} = \frac{f^{(n)}(c)}{n!}$$

24. Soit $P = X^n - X + 1$ ($n \geqslant 2$). Trouver le nombre de racines rationnelles, de racines réelles, de racines complexes de P.

25. Soit K un sous-corps de $\mathbb{C}$. Trouver tous les polynômes $P \in K[X]$ tel que $P'|P$.

26. Trouver les $P \in \mathbb{C}[X]$ tels que $(X+4)P(X) = XP(X+1)$.

27. Trouver les polynômes complexes dont l'image est contenue dans $\mathbb{R}$.

28. Soient α, β et γ les racines distinctes ou confondues de X^3+pX+q. Exprimer à l'aide de p et q : $\alpha^2+\beta^2+\gamma^2$, $\alpha^3+\beta^3+\gamma^3$, $\alpha^4+\beta^4+\gamma^4$, $\alpha^2\beta+\alpha\beta^2+\beta^2\gamma+\beta\gamma^2+\gamma^2\alpha+\gamma\alpha^2$, $\alpha^2\beta^2+\beta^2\gamma^2+\gamma^2\alpha^2$.

29. 1) Donner une CNS sur $(p,q) \in \mathbb{C}^2$ pour que z et z', deux des racines de X^3+pX+q vérifient $z^2+z'^2=1$.
2) Déterminer $\lambda \in \mathbb{C}$ pour que z et z', deux des racines de $X^3-5X+\lambda$ vérifient $z+z'=zz'$.
3) Déterminer $(a,b) \in \mathbb{C}^2$ pour que le polynôme $3X^3-6X^2+aX+b$ admette trois racines dans $\mathbb{C}$ de la forme α, $-\alpha$, 2α. Résoudre l'équation dans ce cas.

30. Soit $(s,p) \in \mathbb{C}^2$. Trouver une CNS sur (s,p) pour les deux racines de X^2-sX+p aient même argument.

31. Soient $(\alpha_1,\dots,\alpha_n) \in \mathbb{C}^n$, $P = \prod_{i=1}^{n}(X-\alpha_i) \in \mathbb{C}[X]$.
1) Montrer que, pour tout $z \in \mathbb{C}\backslash\{\alpha_1,\dots,\alpha_n\}$, on a

$$\frac{P'(z)}{P(z)} = \sum_{i=1}^{n} \frac{1}{z-\alpha_i}$$

2) Calculer $\sum_{i=1}^{5} \frac{1}{1-\alpha_i}$ lorsque α_1,..., α_5 sont les racines distinctes ou confondues de X^5+2X^4-X-1.
3) Montrer que si P est scindé sur $\mathbb{R}$, P' est aussi scindé sur $\mathbb{R}$.

32. On suppose connus les résultats de l'exercice précédent. Soit $P \in \mathbb{R}[X]$ un polynôme scindé sur $\mathbb{R}$.
1) Etablir que $(P')^2 - PP'' \geqslant 0$.
2) On écrit $P = \sum_{k=0}^{n} a_k X^k$. Montrer que si $1 \leqslant k \leqslant n-1$:

$$a_{k-1}a_{k+1} \leqslant a_k^2$$

33. Soit $P \in \mathbb{R}[X]$ de degré n admettant n racines réelles simples strictement supérieures à 1. On pose $Q = (1+X^2)PP' + X(P^2+P'^2)$. Montrer que Q a au moins $2n-1$ racines réelles distinctes.

34. On supposera la caractéristique de K nulle. Soit $\alpha \in K$. On définit

$$u : \begin{array}{ccc} K[X] & \longrightarrow & K[X] \\ P & \longmapsto & \alpha P(X+1) - P(X) \end{array}$$

1) Montrer que u est linéaire.
2) Quel est, pour tout $P \in K[X]$, le degré de $u(P)$ (discuter suivant que $\alpha = 1$ ou $\alpha \neq 1$).
3) En déduire $\operatorname{im} u$ et $\ker u$.
4) Soit $(P,Q) \in K[X]^2$ tel que $u(P) = Q$. Montrer que pour tout $N \in \mathbb{N}$, on a :

$$\sum_{n=0}^{N} \alpha^n Q(n) = \alpha^{N+1}P(N+1) - P(0)$$

5) Calculer

$$\sum_{n=0}^{N} n^2,\ \sum_{n=0}^{N} n^3,\ \sum_{n=0}^{N} 3^n n^2,\ \sum_{n=0}^{N} n\cos n\theta,\ \sum_{n=0}^{N} n\sin n\theta \ \ (\theta \in \mathbb{R})$$

35. Soit $P = \sum_{k\in\mathbb{N}} a_k X^k \in K[X]$, ω l'ordre de 1 comme racine de P. On définit l'endomorphisme

$$u : \begin{array}{ccc} K[X] & \longrightarrow & K[X] \\ Q & \longmapsto & Q(X+1) \end{array}$$

On note $v = P(u) \in \mathcal{L}(K[X])$.

1) Calculer $v(Q)$ pour $Q \in K[X]$.

2) Soit $Q \in K[X]$. Montrer que $\deg(v(q)) = \begin{cases} \deg Q - \omega \text{ si } \deg Q \geqslant \omega \\ -\infty \text{ si } \deg Q < \omega \end{cases}$ (cf exercice précédent)

3) En déduire $\operatorname{im} v$ et $\ker v$.

---

36. Soit $P = X^3 + pX + q \in \mathbb{C}[X]$. Montrer l'équivalence des propositions :

(i) P a une racine d'ordre au moins deux.

(ii) $\dfrac{q^2}{4} + \dfrac{p^3}{27} = 0$.

---

37. Soit $P = X^3 - X^2 - 2X + 1 \in \mathbb{R}[X]$. Montrer que P admet trois zéros réels dans $]-2,2[$. Soit θ un zéro de P. Montrer que θ est irrationnel et que $2-\theta^2$ est un autre zéro de P.

---

38. Soit $P \in \mathbb{Q}[X]$ un polynôme irréductible sur $\mathbb{Q}$. Montrer que P n'a pas de racine double dans $\mathbb{C}$.

---

39. Soit $P \in \mathbb{C}[X]$. Donner une CNS sur P pour que P induise une surjection de $\mathbb{Q}$ sur $\mathbb{Q}$.

---

40. Trouver tous les polynômes $P \in \mathbb{C}[X]$ tels que $P(X^2) = P(X)P(X+1)$.

---

41. Soit $P \in \mathbb{Z}[X]$ de degré $n \geqslant 1$. On note $d = \operatorname{pgcd}(P(0), P(1), \dots, P(n))$. En utilisant le polynôme $\Delta P = P(X+1) - P(X)$ prouver que d divise $P(k)$ pour tout $k \in \mathbb{Z}$.

---

42. 1) Résoudre dans $\mathbb{Z}/41\mathbb{Z}$: $x^3 - \overline{21}x^2 + \overline{29}x - \overline{9} = 0$

2) Résoudre dans $\mathbb{Z}/19\mathbb{Z}$: $x^3 = 1$.

---

43. **Carrés dans $\mathbb{Z}/p\mathbb{Z}$:** Soit $p \geqslant 3$ un nombre premier.

1) Montrer que pour tout $x \in \mathbb{Z}/p\mathbb{Z}^*$

$$x^{p-1} = 1$$

En déduire que pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, $x^p = x$ (petit théorème de Fermat).

2) Montrer qu'il y a dans $\mathbb{Z}/p\mathbb{Z}$ $\frac{p+1}{2}$ carrés. Préciser ces carrés lorsque $p = 13$.

3) Montrer que si $x \in (\mathbb{Z}/p\mathbb{Z})^*$:

$$x^{\frac{p-1}{2}} = \pm 1$$

En déduire que x est un carré non nul dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $x^{\frac{p-1}{2}} = 1$.

4) Montrer que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1 \pmod 4$.

---

44. **Théorème des deux carrés :** on suppose connus les résultats de l'exercice précédent. On note S l'ensemble des entiers de $\mathbb{N}^*$ somme de deux carrés entiers.

1) Prouver que S est stable par multiplication.

2) Soit $n \in S$. Montrer par récurrence sur n que si p est un nombre premier congru à 3 modulo 4, la valuation p-adique de n est paire.

3) Montrer que $2 \in S$.

4) Soit p un nombre premier congru à 1 modulo 4 et $n \in \mathbb{Z}$ tel que $n^2 \equiv -1 \pmod p$.

a. Montrer qu'il existe $(a,b) \in \mathbb{Z}^2$ tel que :

$$0 < b < \sqrt{p} \quad \text{et} \quad \left| b\frac{n}{p} - a \right| \leqslant \frac{1}{\sqrt{p}}$$

b. Montrer que $(bn - ap)^2 + b^2 = p$.

5) Conclure que S est exactement l'ensemble des entiers n tels que pour tout nombre premier p congru à 3 modulo 4, la valuation p-adique est paire.

---

45. **Polynôme minimal :** Soient A une K-algèbre, $a \in A$. On note

$$I_a = \{Q \in K[X],\ \ Q(a) = 0\} \quad \text{et} \quad K[a] = \operatorname{Vect}_{p\in\mathbb{N}}(a^p)$$

1) Montrer qu'il existe un unique $P \in K[X]$ unitaire tel que $I = PK[X]$ et que $K[a]$ est une sous-algèbre de A.
On suppose maintenant A de dimension finie.
2) Montrer que $P \neq 0$.
On note $\mu_a = P$: c'est le polynôme minimal de a (sur K).
3) Montrer que si $n = \deg \mu_a$, $(1, a, \dots, a^{n-1})$ est une base de $K[a]$.
4) Montrer l'équivalence des trois conditions suivantes :
(i) μ_a est un polynôme irréductible.
(ii) $K[a]$ est une algèbre intègre.
(iii) $K[a]$ est un corps.
On revient au cas général : A n'est plus supposée de dimension finie.
5) Soit $K = \mathbb{Q}$ et $A = \mathbb{C}$. On suppose $I_a \neq \{0\}$. On dit que a est *algébrique*. Montrer que μ_a est un polynôme irréductible sur $\mathbb{Q}$. Préciser $\mu_{\sqrt{2}+\sqrt{3}}$.
6) On suppose $A = \mathcal{M}_2(K)$. Soit $M \in A$, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Préciser μ_M.
7) Soit E un K-espace vectoriel de dimension finie. Préciser μ_u pour u homothétie, u affinité.

---

46. **Polynôme minimal ponctuel :** Soient E un K-espace vectoriel de dimension finie, $u \in \mathcal{L}(E)$, $x \in E$ et

$$I = \{Q \in K[X],\ \ (Q(u))(x) = 0\}$$

1) Vérifier l'existence d'un unique $\mu_{u,x} \in K[X]$ tel que $I = \mu_{u,x}K[X]$.
2) On suppose $\deg P = n$. Montrer que $(x, u(x), \dots, u^{n-1}(x))$ est une base de $\sum_{p\in\mathbb{N}} Ku^p(x) = \operatorname{Vect}_{p\in\mathbb{N}}(u^p(x))$ et que ce sous-espace est le plus petit sous-espace stable par u et contenant x.

---

47. **Polynômes cyclotomiques :** On pose $\Phi_1 = X - 1$ et pour $n \geqslant 2$, $\Phi_n = \displaystyle\prod_{\substack{1\leqslant k\leqslant n\\ \operatorname{pgcd}(k,n)=1}} \left(X - e^{\frac{2ik\pi}{n}}\right)$. On dira qu'un polynôme de $\mathbb{Z}[X]$ est primitif si le pgcd de ses coefficients est égal à 1.
1) Démontrer que $X^n - 1 = \displaystyle\prod_{\substack{1\leqslant d\leqslant n\\ d\mid n}} \Phi_d$.
On note φ l'indicatrice d'Euler : pour $n \geqslant 1$, $\varphi(n)$ est le nombre d'entiers $k \in [\![1, n]\!]$ premiers avec n.
2) Montrer que $n = \displaystyle\sum_{d\mid n} \varphi(d)$.
3) En déduire que $\Phi_n \in \mathbb{Z}[X]$.
4) Soit p un nombre premier.
a. Montrer que le produit de deux polynômes primitifs de $\mathbb{Z}[X]$ est primitif.
b. Exprimer $P = \Phi_p(X+1)$ puis montrer qu'il est irréductible dans $\mathbb{Q}[X]$
c. Conclure que Φ_p est irréductible.

---

48. 1) Montrer que $P_0 = X^3 + X + 1 \in \mathbb{C}[X]$ est à racines simples et ne possède aucune racine rationnelle.
Soit $\alpha \in \mathbb{C}$ une racine de P_0.
2) Démontrer que le plus petit sous-corps de $\mathbb{C}$ contenant α est

$$\mathbb{Q}[\alpha] = \{a + b\alpha + c\alpha^2, (a, b, c) \in \mathbb{Q}^3\}.$$

Montrer que tout élément de $\mathbb{Q}[\alpha]$ s'écrit de manière unique $a + b\alpha + c\alpha^2$ avec $(a, b, c) \in \mathbb{Q}^3$.
3) Soit $f, g : \mathbb{Q}[\alpha] \longrightarrow \mathbb{Q}[\alpha]$ deux morphismes de corps. On suppose $f(\alpha) = g(\alpha)$. Montrer que $f = g$.
4) Quels sont les automorphismes du corps $\mathbb{Q}[\alpha]$?

49. Groupe affine :

1) Soit $(a,b) \in K^* \times K$. Montrer que $aX+b$ est inversible dans le monoïde $(K[X], \circ)$.

2) Soit $P \in K[X]$. Vérifier l'équivalence des trois conditions suivantes :

(i) P inversible à gauche dans $(K[X], \circ)$;

(ii) P inversible à droite dans $(K[X], \circ)$;

(iii) Il existe $(a,b) \in K^* \times K$ tel que $P = aX+b$.

Conclure que $\{aX+b,\ (a,b) \in K^* \times K\}$ est un groupe pour $\circ$ appelé groupe affine.