Algèbre générale (complément pour 5/2)

Les exercices notés d'un obèle † sont de « grands classiques ».

Exercice 1 Soit $a \in \mathbb{C}^*$ et $n \in \mathbb{N}$, $n \geqslant 2$. Déterminer une condition nécessaire et suffisante pour que les solutions de $\left(\dfrac{1+iz}{1-iz}\right)^n = a^n$ soient toutes réelles.

z est solution si et seulement s'il existe $\omega \in \mathbb{U}_n$ (ensemble des racines n^e de l'unité) tel que $\dfrac{1+iz}{1-iz} = a\omega$, soit en résolvant $z = \dfrac{a\omega - 1}{i(a\omega+1)}$.

z est réel si et seulement si $\overline{z} = z$, soit $\dfrac{1-\overline{a\omega}}{i(\overline{a\omega}+1)} = \dfrac{a\omega-1}{i(a\omega+1)}$. Sachant que $a\overline{a} = |a|^2$ et $\omega\overline{\omega} = 1$ on obtient en développant : $|a|^2 = 1$. Les solutions sont donc toutes réelles si et seulement si $|a| = 1$.

Remarque. Si on pose $a = e^{i\theta}$ et $\omega = e^{\frac{2i\pi}{n}}$ on obtient $z = \dfrac{e^{i(\theta+\frac{2k\pi}{n})}-1}{i(e^{i(\theta+\frac{2k\pi}{n})}+1)} = \tan\left(\dfrac{\theta}{2} + \dfrac{k\pi}{n}\right) \in \mathbb{R}$.

Exercice 2 †

Soit m et n dans $\mathbb{N}^*$. Déterminer un polynôme unitaire $P \in \mathbb{C}[X]$ de degré maximal tel que P divise $X^n - 1$ et $X^m - 1$.

Cherchons les racines communes à $X^n - 1$ et $X^m - 1$: ce sont les nombres complexes z pour lesquels il existe k et k' dans $\mathbb{Z}$ tels que $z = \exp\left(\dfrac{2ik\pi}{n}\right) = \exp\left(\dfrac{2ik'\pi}{m}\right)$.

On doit avoir $\dfrac{2k\pi}{n} \equiv \dfrac{2k'\pi}{m} \mod (2\pi) \iff mk \equiv nk' \mod (mn)$. Il existe donc $p \in \mathbb{Z}$ tel que $mk = nk' + pmn$.

Posons $d = \operatorname{pgcd}(m,n)$, $m = dm'$ et $n = dn'$. Alors $m'k = n'k' + dm'n' = n'(k' + dm')$.

n' divise $m'k$ et m' et n' sont premiers entre eux donc n' divise k : posons $k = n'u$.

On en déduit que $z = \exp\left(\dfrac{2iu\pi}{d}\right)$, donc z est une racine d'ordre d de l'unité.

Réciproquement, si z est racine d'ordre d de l'unité, on a $z^d = 1$ donc $z^n = (z^d)^{n'} = 1$ et $z^m = (z^d)^{m'} = 1$ donc z est racine de $X^n - 1$ et $X^m - 1$.

De ceci il résulte que $P = X^d - 1$.

Exercice 3 †

Déterminer les polynômes non constants $P \in \mathbb{C}[X]$ tels que P' divise P.

Puisque $\deg P' = \deg P - 1$ il existe $a \neq 0$ et $\lambda \in \mathbb{C}$ tels que $P(X) = a(X-\lambda)P'(X)$. Notons n l'ordre de multiplicité de λ vu comme racine de P.

On a $P(X) = (X-\lambda)^n Q(X)$ avec $Q(\lambda) \neq 0$, et

$$P'(X) = n(X-\lambda)^{n-1}Q(X) + (X-\lambda)^n Q'(X).$$

En reportant dans l'égalité on obtient : $Q(X) = anQ(X) + an(X-\lambda)Q'(X)$ et donc $Q(\lambda) = anQ(\lambda)$. Puisque $Q(\lambda) \neq 0$ on en déduit $a = 1/n$.

Mais alors $(X-\lambda)Q'(X) = 0$, ce qui impose $Q' = 0$. Le polynôme Q est donc constant, et en posant $Q = \alpha$ on obtient $P(X) = \alpha(X-\lambda)^n$.

Réciproquement, il est évident que les polynômes de la forme $\alpha(X-\lambda)^n$ avec $\alpha \neq 0$ et $n \geqslant 1$ sont solutions.

Exercice 4

a) Montrer l'existence et l'unicité d'une famille de polynômes $(B_n)_{n\geqslant 0}$ telle que pour tout $n \in \mathbb{N}$, $X^n = B_n(X) - B_n(X-1)$ et $B_n(0) = 0$.

b) Vérifier que pour tout $n \geqslant 1$, $B_n'(X) = B_n'(0) + nB_{n-1}(X)$.

a) Considérons l'application $\phi : \mathbb{R}[X] \to \mathbb{R}[X]$ définie par $\phi(P) = P(X) - P(X-1)$. ϕ est une application linéaire. Déterminons son noyau et son image.

Soit $P \in \operatorname{Ker}\phi$; on a $P(X) = P(X-1)$. Si P n'est pas constant, soit $\alpha \in \mathbb{C}$ une de ses racines. Alors pour tout $n \in \mathbb{N}$, $\alpha + n$ est racine de P (récurrence) donc P possède une infinité de racine, ce qui est absurde. On en déduit que $\operatorname{Ker}\phi = \mathbb{R}$.

Par la formule du binôme il est facile de constater que pour tout $n \in \mathbb{N}^*$, $\deg \phi(X^n) = n-1$. Ceci montre que $\operatorname{Im}\phi$ contient une famille échelonnée en degré et donc que $\operatorname{Im}\phi = \mathbb{R}[X]$.
Considérons maintenant le sous-espace vectoriel H des polynômes $P \in \mathbb{R}[X]$ vérifiant $P(0) = 0$ (autrement dit dont le coefficient constant est nul). Il s'agit d'un sous-espace vectoriel de $\mathbb{R}[X]$, supplémentaire de $\mathbb{R} = \operatorname{Ker}\phi$. D'après le théorème du rang la restriction de ϕ à H est un isomorphisme de H vers $\operatorname{Im}\phi = \mathbb{R}[X]$.
Il existe donc un unique polynôme B_n de H tel que $\phi(B_n) = X^n$.

b) Pour tout $n \geqslant 1$, $B'_n(X) - B'_n(X-1) = nX^{n-1}$ donc $\phi(B'_n) = n\phi(B_{n-1}) = \phi(nB_{n-1})$. Puisque $\operatorname{Ker}\phi = \mathbb{K}$ il existe $\lambda \in \mathbb{R}$ tel que $B'_n(X) = nB_{n-1} + \lambda$, et sachant que $B_{n-1}(0) = 0$ il vient $\lambda = B'_n(0)$.

Exercice 5 Soient $A, B, C \in \mathbb{C}[X]$ tels que $A + B = C$. On suppose que A, B et C n'ont aucune racine commune et que l'un de ces trois polynômes est de degré strictement positif. On pose $D = A'B - AB'$.

a) Soit z une racine de ABC de multiplicité n. Montrer que z est racine de D de multiplicité au moins égale à $n-1$.

On note μ le nombre de racines distinctes de ABC.

b) Montrer que $\mu \geqslant \deg A + \deg B + \deg C - \deg D$.

c) Montrer que $\mu > \max\big(\deg A, \deg B, \deg C\big)$.

a) Si z est racine de A alors z est racine d'ordre n de A (puisque A, B, C n'ont pas de racines communes) donc z est racine d'ordre $n-1$ de A. Les polynômes A et A′ sont factorisables par $(X-z)^{n-1}$ donc D aussi.
Le raisonnement est identique si z est racine de B.
Supposons enfin z racine de C. Alors z est racine d'ordre n de C donc pour tout $k \in [\![0, n]\!]$, $C^{(k)}(z) = 0$, soit $B^{(k)}(z) = -A^{(k)}(z)$. Par ailleurs, pour tout $p \in [\![0, n-1]\!]$,

$$D^{(p)} = \sum_{k=0}^{p} \binom{p}{k} A^{(k+1)}B^{(p-k)} - \sum_{k=0}^{p} \binom{p}{k} A^{(p-k)}B^{(k+1)} = \sum_{k=0}^{p} \binom{p}{k} \Big(A^{(k+1)}B^{(p-k)} - A^{(p-k)}B^{(k+1)}\Big)$$

Mais $A^{(k+1)}(z)B^{(p-k)}(z) - A^{(p-k)}(z)B^{(k+1)}(z) = -A^{(k+1)}(z)A^{(p-k)}(z) + A^{(p-k)}(z)A^{(k+1)}(z) = 0$ donc $D^{(p)}(z) = 0$. On en déduit que z est racine au moins d'ordre $n-1$ de D.

b) Posons $A = k_1 \prod_{i=1}^{\alpha_i} (X - a_i)^{n_i}$, $B = k_2 \prod_{i=1}^{\beta_i} (X - b_i)^{p_i}$ et $C = k_3 \prod_{i=1}^{\gamma_i} (X - c_i)^{q_i}$. La question précédente a montré que D est factorisable par $\prod_{i=1}^{\alpha_i} (X - a_i)^{n_i - 1} \times \prod_{i=1}^{\beta_i} (X - b_i)^{p_i - 1} \times \prod_{i=1}^{\gamma_i} (X - c_i)^{q_i - 1}$ donc

$$\deg D \geqslant \sum_{i=1}^{\alpha_i} (n_i - 1) + \sum_{i=1}^{\beta_i} (p_i - 1) + \sum_{i=1}^{\gamma_i} (q_i - 1) = \deg A - \alpha_i + \deg B - \beta_i + \deg C - \gamma_i$$

et ainsi $\deg A + \deg B + \deg C - \deg D \leqslant \alpha_i + \beta_i + \gamma_i \leqslant \mu$.

c) $\deg D \leqslant \deg A + \deg B - 1$ donc $\deg A + \deg B - \deg D \geqslant 1$. D'après la question précédente, $1 + \deg C \leqslant \mu$ donc $\mu > \deg C$.
Si $\deg A \neq \deg B$ on a $\deg C = \max(\deg A, \deg B)$ donc on a aussi $\mu > \deg A$ et $\mu > \deg B$ et on peut conclure.
Si $\deg A = \deg B = deg C$ la même conclusion s'en suit.
Il reste à examiner le cas où $\deg A = \deg B > \deg C$.
Dans ce cas, on écrit $D = A'(C - A) - A(C' - A') = A'C - AC'$ donc $\deg D \leqslant \deg A + \deg C - 1$, et d'après la question précédente, $\deg B \geqslant \mu - 1$. Ainsi, $\mu > \deg B = \deg A$ et on peut là encore conclure.

Exercice 6 †
Soit $n \in \mathbb{N}^*$, $a_0 \in \mathbb{R}_+^*$ et $a_1, \dots, a_{n-1} \in \mathbb{R}_+$. On pose $P = X^n - \sum_{k=0}^{n-1} a_k X^k$.

a) Montrer que P possède une unique racine dans $\mathbb{R}_+^*$, que l'on note ρ.

b) Soit z une racine complexe de P. Montrer que $|z| \leqslant \rho$.

c) Montrer que $\rho \leqslant \max(1, a_0 + a_1 + \cdots + a_{n-1})$.

d) Montrer que $\rho \leqslant 1 + \max_{0 \leqslant k \leqslant n-1} a_k$.

a) Soit $f : \mathbb{R}_+^* \to \mathbb{R}$ définie par $f(x) = 1 - \sum_{k=0}^{n-1} \frac{a_k}{x^{n-k}}$, de sorte que $P(x) = x^n f(x)$.
On a $f'(x) = \sum_{k=0}^{n-1} \frac{(n-k)a_k}{x^{n-k+1}} > 0$ donc f est strictement croissante sur $\mathbb{R}_+^*$.
On a $\lim_{0^+} f(x) = -\infty$ et $\lim_{+\infty} f(x) = 1$ donc d'après le théorème de la bijection continue f s'annule pour une unique valeur ρ de $\mathbb{R}_+^*$. Sachant que pour tout $x > 0$, $P(x) = x^n f(x)$, P possède une unique racine dans $\mathbb{R}_+^*$.

b) On a $P(z) = 0 \iff z^n = \sum_{k=0}^{n-1} a_k z^k$ donc $|z|^n \leqslant \sum_{k=0}^{n-1} a_k |z|^k$. Autrement dit, $P(|z|) \leqslant 0$.
On ne peut avoir $|z| = 0$ car $a_0 > 0$ donc $f(|z|) \leqslant 0$, et compte tenu des variations de f on en déduit que $|z| \leqslant \rho$.

c) On a $\rho^n = \sum_{k=0}^{n-1} a_k \rho^k$. Supposons $\rho \geqslant 1$. Alors pour tout $k \in [\![0, n-1]\!]$, $\rho^k \leqslant \rho^{n-1}$ donc $\rho^n \leqslant \sum_{k=0}^{n-1} a_k \rho^{n-1}$, soit $\rho \leqslant \sum_{k=0}^{n-1} a_k$. Dans tous les cas on a bien $\rho \leqslant \max(1, a_0 + a_1 + \cdots + a_{n-1})$.

d) Posons $m = \max_k a_k$. On a $\rho^n = \sum_{k=0}^{n-1} a_k \rho^k$ donc $\rho^n \leqslant m \sum_{k=0}^{n-1} \rho^k$. Si $\rho \neq 1$ alors $\rho^n \leqslant m \frac{\rho^n - 1}{\rho - 1}$, ce qui s'écrit encore $\rho^{n+1} \leqslant (m+1)\rho^n - m$. Sachant que $m \geqslant 0$ il vient $\rho^{n+1} \leqslant (m+1)\rho^n$, puis $\rho \leqslant m+1$.
Enfin, si $\rho = 1$ l'inégalité $\rho \leqslant m+1$ est évidente puisque $m \geqslant 0$.

Exercice 7

a) Soit $n \in \mathbb{N}$. Montrer l'existence d'un unique polynôme R_n tel que pour tout $x \in \mathbb{R}^*$ on ait $R_n\left(x + \frac{1}{x}\right) = x^n + \frac{1}{x^n}$.

b) Donner une expression de R_n (n'utilisant pas de relation de récurrence).

a) Raisonnons par récurrence sur n.

- Si $n = 0$ on a $R_0 = 2$; si $n = 1$ on a $R_1 = X$.
- Si $n \geqslant 2$, supposons acquise l'existence de R_{n-1} et R_{n-2}. De l'égalité : $x^n + \frac{1}{x^n} = \left(x + \frac{1}{x}\right)\left(x^{n-1} + \frac{1}{x^{n-1}}\right) - \left(x^{n-2} + \frac{1}{x^{n-2}}\right)$ on tire $R_n(X) = XR_{n-1}(X) - R_{n-2}(X)$, ce qui assure l'existence de R_n. Enfin, s'il existait un autre polynôme solution S_n on aurait pour tout $x \in \mathbb{R}^*$, $(R_n - S_n)\left(x + \frac{1}{x}\right) = 0$ et $R_n - S_n$ s'annulerait une infinité de fois, donc $S_n = R_n$. La récurrence se propage.

b) La suite (R_n) est donc définie par la donnée de $R_0 = 2$, $R_1 = X$ et $R_n(X) = XR_{n-1}(X) - R_{n-2}(X)$.
Considérons un réel x quelconque et la suite (u_n) définie par $u_0 = 2$, $u_1 = x$ et $u_n = xu_{n-1} - u_{n-2}$. Il s'agit d'une suite à récurrence linéaire double ; son équation caractéristique est $r^2 - xr + 1 = 0$.
Notons δ une racine (réelle ou complexe) de $x^2 - 4$. Supposons dans un premier temps $x \neq \pm 2$, de sorte qu'il existe α et β dans $\mathbb{C}$ tels que pour tout $n \in \mathbb{N}$, $u_n = \alpha\left(\frac{x+\delta}{2}\right)^n + \beta\left(\frac{x-\delta}{2}\right)^n$.

Pour $n = 0$ et $n = 1$ on obtient $\begin{cases} 2 = \alpha + \beta \\ x = \frac{x}{2}(\alpha+\beta) + \frac{\delta}{2}(\alpha - \beta) \end{cases} \iff \begin{cases} \alpha + \beta = 2 \\ \alpha - \beta = 0 \end{cases} \iff \alpha = \beta = 1$. Ainsi,

$$u_n = \left(\frac{x+\delta}{2}\right)^n + \left(\frac{x-\delta}{2}\right)^n = \frac{1}{2^n} \sum_{k=0}^{n} \binom{n}{k} x^{n-k} \delta^k \left(1 + (-1)^k\right) = \frac{1}{2^{n-1}} \sum_{0 \leqslant 2p \leqslant n} \binom{n}{2p} x^{n-2p} \delta^{2p}$$

Sachant que $\delta^2 = x^2 - 4$ nous avons prouvé que pour tout $x \in \mathbb{R} \setminus \{-2, 2\}$, $P(x) = \frac{1}{2^{n-1}} \sum_{p=0}^{\lfloor n/2 \rfloor} \binom{n}{2p} x^{n-2p} (x^2 - 4)^p$.

Deux polynômes qui coïncident sur $\mathbb{R} \setminus \{-2, 2\}$ sont égaux donc $R_n(X) = \frac{1}{2^{n-1}} \sum_{p=0}^{\lfloor n/2 \rfloor} \binom{n}{2p} X^{n-2p} (X^2 - 4)^p$.

Exercice 8 Soit $P \in \mathbb{R}[X]$ un polynôme réel tel que pour tout $x \in \mathbb{R}$, $P(x) \geqslant 0$. Montrer l'existence de deux polynômes réels A et B tels que $P = A^2 + B^2$.

Considérons la décomposition dans $\mathbb{C}$ du polynôme :

$$P(X) = \lambda \prod_i (X - a_i)^{n_i} \prod_j (X - \beta_j)^{m_j} (X - \overline{\beta}_j)^{m_j}$$

avec $a_i \in \mathbb{R}$ et $\beta_j \in \mathbb{C} \setminus \mathbb{R}$.
Au voisinage de $+\infty$ on a $P(x) \sim \lambda x^{\deg P}$ donc $\lambda > 0$.
Au voisinage de l'un des a_i on a $P(x) \sim c(x - a_i)^{n_i}$ où c est une constante non nulle donc n_i est un entier pair (et accessoirement c est positif).
Posons donc déjà $Q = \sqrt{\lambda} \prod_i (X - a_i)^{n_i/2} \in \mathbb{R}[X]$. Alors $P(X) = Q(X)^2 \prod_j (X - \beta_j)^{m_j} (X - \overline{\beta}_j)^{m_j}$.
Le polynôme $\prod_j (X - \beta_j)_j^m$ est à coefficients complexes ; en séparant les paries réelles et imaginaires on peut le mettre sous la forme $R(X) + iS(X)$ où R et S sont des polynômes à coefficients réels.
On a ainsi $P(X) = Q(X)^2 \big(R(X) + iS(X)\big)\big(R(X) - iS(X)\big) = A(X)^2 + B(X)^2$ en posant $A = QR$ et $B = QS$.