Contrôle Continu (26/10/21)

Durée : 2h
Documents, téléphones portables et appareils électroniques interdits
La redaction et la clarté de l'argumentation sera prise en compte dans la notation

---

Exercice 1 (Autour du cours)

Soient K un corps et $n \geq 2$ un entier. On suppose que K est de caractéristique différente de 2. On désigne par $\mathcal{S}_n$ le groupe symétrique de $\{1, 2, \ldots, n\}$.
Un polynôme $P \in K[X_1, \ldots, X_n]$ est *antisymétrique* si pour tout $\sigma \in \mathcal{S}_n$, $\sigma P = \varepsilon(\sigma)P$, où $\varepsilon(\sigma)$ est la signature de σ.

1) Vérifier que le polynôme de Vandermonde $V(X_1, \ldots, X_n) = \prod_{1 \leq i < j \leq n} (X_i - X_j)$ est antisymétrique.

Soit $\sigma \in \mathcal{S}_n$. $\sigma V = \prod (X_{\sigma(i)} - X_{\sigma(j)})$. Comme σ est bijective, σ induit une bijection sur l'ensemble des parties à deux éléments de $\{1, 2, \ldots n\}$. Ainsi, $\sigma V = (-1)^N V$ où N est le cardinal de l'ensemble $\{(i, j) \mid i < j \text{ et } \sigma(i) > \sigma(j)\}$, i.e. $(-1)^N = \epsilon(\sigma)$.

2) Montrer que tout polynôme antisymétrique P s'écrit sous la forme $P = V \cdot Q$, où $Q \in K[X_1, \ldots, X_n]^{\mathcal{S}_n}$ est un polynôme symétrique.

Soit P un polynôme antisymétrique. Pour toute transposition $\tau = (i, j) \in \mathcal{S}_n$ avec $i < j$, $\tau P = -P$. Donc, en considérant le morphisme d'évaluation

$$\varphi \colon K[X_1 \ldots, X_n] \cong K[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n][X_i] \longrightarrow K[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$$

qui envoie X_i sur X_j, on a $-\varphi(P) = \varphi(-P) = \varphi(\tau P) = \varphi(P)$ donc, comme K est de caractéristique différente de 2, $P \in Ker(\varphi) = (X_j - X_i)$. Donc $X_j - X_i$ divise P. Comme tous ces polynômes sont irréductibles et distincts deux à deux, ils sont premiers entre eux deux à deux et leur produit divise P, i.e. V divise P. Donc il existe $Q \in K[X_1, \ldots, X_n]$ tel que $P = VQ$. Enfin, si $\sigma \in S_n$, on a

$$(-1)^{\epsilon(\sigma)} VQ = (-1)^{\epsilon(\sigma)} P = \sigma P = (\sigma V)(\sigma Q) = ((-1)^{\epsilon(\sigma)} V)(\sigma Q).$$

Donc, par intégrité, $Q = \sigma Q$ et Q est symétrique.

3) Notons $K[X_1, \ldots, X_n]^{\mathcal{A}_n}$ la sous-algèbre de $K[X_1, \ldots, X_n]$, invariante sous l'action du groupe alterné $\mathcal{A}_n \subset \mathcal{S}_n$.

a) Montrer que $P \in K[X_1, \ldots, X_n]^{\mathcal{A}_n}$ s'écrit de manière unique sous la forme $P = A + B \cdot V$ où $A, B \in K[X_1, \ldots, X_n]^{\mathcal{S}_n}$ sont des polynômes symétriques.
Indication : montrer que l'orbite de P sous $\mathcal{S}_n$ ne prend qu'au plus deux valeurs P et $Q = \tau P$, où $\tau = (1\ 2)$ est une transposition, puis écrire $P = \frac{1}{2}(P + Q) + \frac{1}{2}(P - Q)$.

Soit $P \in P \in K[X_1, \ldots, X_n]^{\mathcal{A}_n}$ et soit $\sigma \in S_n$. Si $\sigma \in \mathcal{A}_n$, $\sigma P = P$ sinon, $(1, 2)\sigma \in A_n$ et $\sigma P = (1, 2)(1, 2)\sigma P = (1, 2)P$. Ainsi, on a $P + (1, 2)P$ symétrique et $P - (1, 2)P$ antisymétrique. Donc $P = \frac{1}{2}(P + (1, 2)P) + \frac{1}{2}(P - (1, 2)P)$ est la somme d'un polynôme symétrique et d'un polynôme antisymétrique. La question 2 permet alors de conclure sur l'existence de la décomposition. Montrons qu'elle est unique. Soit $A_1, B_1, A_2, B_2 \in K[X_1, \ldots, X_n]^{\mathcal{S}_n}$ tels que $A_1 + VB_1 = A_2 + VB_2$. On a alors $A_1 - A_2 = V(B_2 - B_1)$. Comme V est antisymétrique et A_1, A_2, B_1, B_2 symétriques, on a $A_1 - A_2$ symétrique et antisymétrique. Ainsi, comme le seul polynôme symétrique et antisymétrique est le polynôme nul, on a $A_1 = A_2$ qui implique $B_1 = B_2$. D'où l'unicité de la décomposition.

b) Soit $\varphi : K[\Sigma_1, \ldots, \Sigma_n][T] \longrightarrow K[X_1, \ldots, X_n]^{\mathcal{A}_n}$ le morphisme qui envoie Σ_i (vue comme indéterminée) sur le polynôme symétrique $\Sigma_i(X_1, \ldots, X_n)$, et T sur V. Montrer que φ est bien défini et surjectif.

On a $V \in K[X_1, \ldots, X_n]^{\mathcal{A}_n}$ et, pour tout $k \in \{1, 2, \ldots, n\}$, le polynôme symétrique élémentaire $\Sigma_k \in K[X_1, \ldots, X_n]^{\mathcal{S}_n} \subseteq K[X_1, \ldots, X_n]^{\mathcal{A}_n}$, Ainsi, par propriété universelle de l'anneau de polynôme $K[\Sigma_1, \ldots, \Sigma_n][T]$ le morphisme φ existe et est bien défini. Enfin montrons que φ est surjective. Soit

$P \in K[X_1,\dots,X_n]^{\mathcal{A}_n}$. Par 3.a), il existe $A, B \in K[X_1,\dots,X_n]^{\mathcal{S}_n}$ tels que $P = A + BV$. Par le théorème de structure des polynômes symétrique, il existe $A_0, B_0 \in K[\Sigma_1,\dots,\Sigma_n]$ tels que $\varphi(A_0) = A$ et $\varphi(B_0) = B$. En particulier on a $\varphi(A_0 + B_0 Y) = P$. D'où φ est surjective.

c) Montrer que φ induit un isomorphisme de $K[\Sigma_1,\dots,\Sigma_n][T]/(T^2-V^2)$ sur $K[X_1,\dots,X_n]^{\mathcal{A}_n}$.

Il suffit de montrer que le noyau de φ est $(T^2 - V^2)$. On a $T^2 - V^2 \in \ker\varphi$ et ce polynôme est irréductible sur $K[\Sigma_1,\dots,\Sigma_n]$ car il n'a pas de racine (sinon V serait un polynôme symétrique). Donc, comme φ n'est pas trivial, on a $\ker\varphi = (T^2 - V^2)$.

Exercice 2 (Sommes permutées)

Soient K un corps infini, $n \geq 2$ un entier, et $a_1, a_2, \dots, a_n \in K$ des éléments deux à deux distincts. Montrer qu'il existe un n-uplet $(x_1, x_2, \dots, x_n) \in K^n$ tel que les $n!$ sommes $\sum_{i=1}^{n} a_i x_{\sigma(i)}$, avec σ parcourant $\mathcal{S}_n$, sont deux à eux distinctes. Si $\tau \in \mathcal{S}_n$, on pourra considérer le polynôme

$$\prod_{\substack{\sigma\in\mathcal{S}_n\\ \sigma\neq\tau}} \left(\sum_{i=1}^{n}(a_{\sigma(i)} - a_{\tau(i)})X_i\right) \in K[X_1, X_2, \dots, X_n].$$

Notons, pour $\tau \in \mathcal{S}_n$, P_τ le polynôme de l'indication et supposons que le résultat est faux. Soit $(x_1,\dots,x_n) \in K$, il existe $\sigma, \tau \in \mathcal{S}_n$ tels que $\sigma \neq \tau$ et $\sum_{i=1}^n a_i x_{\sigma(i)} = \sum_{i=1}^n a_i x_{\tau(i)}$. Donc

$$0 = \sum_{i=1}^{n} a_i x_{\sigma(i)} - \sum_{i=1}^{n} a_i x_{\tau(i)} = \sum_{i=1}^{n} a_{\sigma^{-1}(i)} x_i - \sum_{i=1}^{n} a_{\tau^{-1}(i)} x_i = \sum_{i=1}^{n} (a_{\sigma^{-1}(i)} - a_{\tau^{-1}(i)}) x_i.$$

Donc l'un des facteurs de $P_{\tau^{-1}}$ s'annule en $(x_1, x_2, \dots, x_n)$. Ainsi, pour tout $(x_1, x_2, \dots, x_n) \in K^n$, il existe $\tau \in \mathcal{S}_n$ tel que P_τ s'annule en $(x_1, x_2, \dots, x_n)$. Donc, la fonction polynomial sur K associée au polynôme $P = \prod_{\tau\in\mathcal{S}_n} P_\tau$ est nulle. Comme K est infini, cela implique que P est nul. Mais, comme les a_i sont distincts deux à deux, pour tout $\sigma, \tau \in \mathcal{S}_n$, il existe $i \in \{1, 2, \dots, n\}$ tel que$\sigma(i) \neq \tau(i)$ et donc $a_{\sigma(i)} \neq a_{\tau(i)}$. Ainsi, comme on travail sur un corps (donc intègre), P n'est pas nul comme facteur de polynômes non nuls. D'où une contradiction.

Exercice 3 (Série génératrice de Fibonacci)

Soit $(u_n)_{n\in\mathbb{N}}$ la suite de réels définie par $u_0 = 0$, $u_1 = 1$, et pour tout $n \geq 2$, $u_n = u_{n-1} + u_{n-2}$. Soit $S = \sum_{n\in\mathbb{N}} u_n X^n \in \mathbb{Q}[[X]]$.

1) Montrer que $S = \dfrac{X}{1 - X - X^2}$.

On a

$$\begin{aligned}(1 - X - X^2)\sum_{n\in\mathbb{N}} u_n X^n &= \sum_{n\in\mathbb{N}} u_n X^n - \sum_{n\in\mathbb{N}} u_n X^{n+1} - \sum_{n\in\mathbb{N}} u_n X^{n+2}\\ &= \sum_{n\in\mathbb{N}} u_n X^n - \sum_{n\geq 1} u_{n-1} X^n - \sum_{n\geq 2} u_{n-2} X^n\\ &= u_0 + (u_0 + u_1)X + \sum_{n\geq 2} \underbrace{(u_n - u_{n-1} - u_{n-2})}_{0} X^n\\ &= X.\end{aligned}$$

D'où $(1 - X - X^2)S = X$ et, comme $1 - X - X^2$ est inversible dans $\mathbb{Q}[[X]]$ (ou bien n'a pas 0 comme racine), $S = \dfrac{X}{X^2 - X - 1}$.

2) En déduire, pour tout $n \in \mathbb{N}$, une expression de u_n en fonction de n.

On a $1 - X - X^2 = -(a - X)(b - X)$ avec $a = \dfrac{-1-\sqrt{5}}{2}$ et $b = \dfrac{-1+\sqrt{5}}{2}$. En décomposant en éléments simples la fraction rationnelle, on obtient

$$\begin{aligned} S = \frac{1}{a-b}\left(\frac{a}{a-X} - \frac{b}{b-X}\right) &= \frac{1}{a-b}\left(\frac{1}{1-(X/a)} - \frac{1}{1-(X/b)}\right) \\ &= \frac{1}{a-b}\left(\sum_{n\geq 0}\left(\frac{X}{a}\right)^n - \sum_{n\geq 0}\left(\frac{X}{b}\right)^n\right) \\ &= \frac{1}{a-b}\sum_{n\geq 0}(a^{-n} - b^{-n})X^n. \end{aligned}$$

Donc, pour tout $n \in \mathbb{N}$,

$$\begin{aligned} u_n = \frac{1}{a-b}(a^{-n} - b^{-n}) &= \frac{1}{\sqrt{5}}\left(\left(\frac{2}{-1+\sqrt{5}}\right)^n - \left(\frac{2}{-1-\sqrt{5}}\right)^n\right) \\ &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right). \end{aligned}$$

Exercice 4 (Un théorème de Kronecker)

Soit $P_1 \in \mathbb{Z}[X]$ un polynôme unitaire dont les racines $z_1, \ldots, z_n \in \mathbb{C}$ (comptées avec multiplicité) vérifient $0 < |z_i| \leq 1$. On se propose de montrer que les z_i sont des racines de l'unité.

1) Soit Ω_n l'ensemble des polynômes unitaires de $\mathbb{Z}[X]$ de degré n dont les racines dans $\mathbb{C}$ sont de module inférieur ou égal à 1.

a) Montrez que si $P = \sum_{k=0}^{n} a_k X^k \in \Omega_n$, alors pour tout $0 \leq k \leq n$, $|a_k| \leq \binom{n}{k}$.

Soit $P \in \omega_n$ et soit $x_1, x_2, \ldots, x_n$ ses racines complexes comptées avec multiplicités. Comme P est unitaire, $a_n = 1 = \binom{n}{n}$. De plus, si $0 \leq k \leq n-1$, on a $a_k = \Sigma_{n-k}(x_1, x_2, \ldots, x_n)$ où les Σ_i sont les polynômes symétriques élémentaires de $\mathbb{Z}[X_1, X_2, \ldots, X_n]$. On a donc, en notant $\mathcal{P}_k(n)$ est l'ensemble des parties à k éléments de $\{1, 2, \ldots, n\}$,

$$|a_k| = \left|\sum_{A\in\mathcal{P}_k(n)}\prod_{i\in A} x_i\right| \leq \sum_{A\in\mathcal{P}_k(n)}\prod_{i\in A}|x_i| \leq \sum_{A\in\mathcal{P}_k(n)} 1 = \binom{n}{k}.$$

b) En déduire que Ω_n est fini.

Par la question précédente, on a $\Omega_n \subseteq \left\{\sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X] \;\middle|\; |a_k| \leq \binom{n}{k} \text{ pour tout } k\right\}$. Ce dernier ensemble est en bijection avec $\prod_{k=0}^{n}\left\{-\binom{n}{k}, -\binom{n}{k}+1, \ldots, \binom{n}{k}-1, \binom{n}{k}\right\}$ qui est fini. Donc Ω_n est fini.

2) Soit $k \geq 1$. On définit $P_k = (X - z_1^k)(X - z_2^k)\cdots(X - z_n^k)$.

a) Montrer que $P_k \in \mathbb{Z}[X]$.

Notons $P_k = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} + X^n$ (P_k est unitaire par définition). Fixons $r \in \{0, 1, \ldots n-1\}$ et montrons que $a_r \in \mathbb{Z}$. Par la relation coefficients-racines, $a_r = (-1)^{n-r}\Sigma_{n-r}(z_1^k, z_2^k, \ldots, z_n^k)$. En particulier, il existe $Q \in \mathbb{Z}[X_1, X_2, \ldots, X_n]^{\mathcal{S}_n}$ tel que $a_r = Q(z_1, z_2, \ldots, z_r)$. En utilisant le théorème de structure des les polynômes symétriques, il existe $Q_0 \in \mathbb{Z}[X_1, X_2, \ldots, X_n]$ tel que $Q = Q_0(\Sigma_1, \ldots, \Sigma_n)$. Ainsi, $a_r = Q_0\left(\Sigma_1(z_1, z_2, \ldots, z_n), \Sigma_2(z_1, z_2, \ldots, z_n)\ldots, \Sigma_n(z_1, z_2, \ldots, z_n)\right)$. Or, pour tout $i \in \{1, 2, \ldots, n\}$, $\Sigma_i(z_1, z_2, \ldots, z_k) \in \mathbb{Z}$ car ce sont, au signe près, les coefficient de $P_0 \in \mathbb{Z}[X]$. Ainsi, $a_k \in \mathbb{Z}$. Enfin, comme tous les coefficients de P_k sont dans $\mathbb{Z}$, c'est un polynôme de $\mathbb{Z}[X]$.

b) En déduire que $P_k \in \Omega_n$.

Pour tout $i \in \{1, 2, \ldots, n\}$, on a $|z_i^k| = |z_i|^k \leq 1$. Donc comme P est unitaire et de degré n, c'est un élément de Ω_n.

3) Soit $Z_n = \{z \in \mathbb{C} \mid \exists P \in \Omega_n \text{ tel que } P(z) = 0\}$.

a) Montrer que Z_n est fini.

Soit $P \in \Omega_n$. P est un polynôme à coefficients dans $\mathbb{Z}$ et donc dans $\mathbb{C}$. Comme $\mathbb{C}$ est un corps (donc intègre), le nombre de racine de P dans $\mathbb{C}$ est inférieur ou égal au degré de P. Ainsi, comme Ω_n est fini par la question 1.b,

$$Z_n = \bigcup_{P \in \Omega_n} \{\text{racines de } P \text{ dans } \mathbb{C}\}$$

est un ensemble fini comme union finie d'ensembles finis.

b) En déduire que pour tout $k \in \{1, 2, \ldots, n\}$, il existe $r, s \in \mathbb{N}$ distincts tels que $z_k^r = z_k^s$.

Soit $k \in \{1, 2, \ldots, n\}$. Par la question 2.b, $P_r \in \Omega_n$ pour tout $r \geq 0$. Ainsi $z_k^r \in Z_n$ pour tout $r \geq 0$. Cependant, par la question précédente, Z_n est fini, donc, par le principe des tirroirs, il existe $r, s \in \mathbb{N}$ distincts tels que $z_k^r = z_k^s$.

4) Conclure.

Soit $k \in \{1, 2, \ldots, n\}$. Par hypothèse, on a $z_k \neq 0$. De plus, par la question précédente, l existe $r, s \in \mathbb{N}$ distincts tels que $z_k^r = z_k^s$. En particulier $z_k^{r-s} = 1$ et z_k est une racine de l'unité.