Corrigé du devoir à la maison de février

*

Exercice 1 *Si K est un corps, le groupe des permutations paires $\mathfrak{A}_n$ agit sur le corps des fractions rationnelles $K(X_1,...,X_n)$ par permutations des variables.*

On note $j := \frac{-1+i\sqrt{3}}{2} \in \mathbb{C}$.

a) LE groupe $\mathfrak{A}_3$ est engendré par le $3-$cycle $c = (123)$ donc $\mathbb{C}(X_1,X_2,X_3)^{\mathfrak{A}_3} = \mathbb{C}(X_1,X_,2,X_3)^{\{1,c\}}$. On a $c.t_k = j^{2k}t_k$. Donc $y_1,y_2,y_3 \in \mathbb{C}(X_1,X_2,X_3)^{\mathfrak{A}_3}$.

b) On a $\mathbb{C}(X_1,X_2,X_3) = \mathbb{C}(t_1,t_2,t_3)$. De plus, $t_2 = t_1^2/y_1$, $t_3 = y_3$ donc $\mathbb{C}(X_1,X_2,X_3) = \mathbb{C}(t_1,t_2,t_3) = \mathbb{C}(y_1,y_2,y_3,t_1)$.

c) Comme $t_1^3 = y_1^2y_2$, t_1 est de degré $\leqslant 3$ sur $\mathbb{C}(y_1,y_2,y_3)$ donc : $[\mathbb{C}(X_1,X_2,X_3) : \mathbb{C}(y_1,y_2,y_3)] = [\mathbb{C}(y_1,y_2,y_3,t_1) : \mathbb{C}(y_1,y_2,y_3)] \leqslant 3$.

d) Donc $\mathbb{C}(y_1,y_2,y_3) \leqslant \mathbb{C}(X_1,X_2,X_3)^{\mathfrak{A}_3} \leqslant \mathbb{C}(X_1,X_2,X_3)$ et $[\mathbb{C}(X_1,X_2,X_3)^{\mathfrak{A}_3} : \mathbb{C}(y_1,y_2,y_3)] = [\mathbb{C}(X_1,X_2,X_3) : \mathbb{C}(y_1,y_2,y_3)]/[\mathbb{C}(X_1,X_2,X_3)^{\mathfrak{A}_3} : \mathbb{C}(X_1,X_2,X_3)] = [\mathbb{C}(X_1,X_2,X_3) : \mathbb{C}(y_1,y_2,y_3)]/3 \leqslant 1$. Donc $\mathbb{C}(y_1,y_2,y_3) = \mathbb{C}(X_1,X_2,X_3)^{\mathfrak{A}_3}$.

e) Comme $1+j+j^2 = 0$, on a :

$$y_1 = \frac{(X_1+jX_2+j^2X_3)^3}{(X_1+j^2X_2+jX_3)(X_1+jX_2+j^2X_3)}$$

$$= \frac{X_1^3+X_2^3+X_3^3+6X_1X_2X_3+3j(X_1^2X_2+X_2^2X_3+X_3^2X_1)+3j^2(X_1X_2^2+X_2X_3^2+X_3X_1^2)}{X_1^2+X_2^2+X_3^2-X_1X_2-X_2X_3-X_1X_3}$$

$$= j\underbrace{\frac{-X_1^3-X_2^3-X_3^3-6X_1X_2X_3+3(X_1^2X_2+X_2^2X_3+X_3^2X_1)}{X_1^2+X_2^2+X_3^2-X_1X_2-X_2X_3-X_1X_3}}_{=z_1}$$

$$+j^2\underbrace{\frac{-X_1^3-X_2^3-X_3^3-6X_1X_2X_3+3(X_1X_2^2+X_2X_3^2+X_3X_1^2)}{X_1^2+X_2^2+X_3^2-X_1X_2-X_2X_3-X_1X_3}}_{=z_2}.$$

Puisque $y_2 = \overline{y_1}$, on a

$$y_2 = j^2\frac{-X_1^3-X_2^3-X_3^3-6X_1X_2X_3+3(X_1^2X_2+X_2^2X_3+X_3^2X_1)}{X_1^2+X_2^2+X_3^2-X_1X_2-X_2X_3-X_1X_3}$$

$$+j\frac{-X_1^3-X_2^3-X_3^3-6X_1X_2X_3+3(X_1X_2^2+X_2X_3^2+X_3X_1^2)}{X_1^2+X_2^2+X_3^2-X_1X_2-X_2X_3-X_1X_3}.$$

f) On a $\mathbb{Q}(X_1,X_2,X_3) \geqslant \mathbb{Q}(X_1,X_2,X_3)^{\mathfrak{A}_3} \geqslant \mathbb{Q}(z_1,z_2,y_3)$.
Or, $[\mathbb{Q}(X_1,X_2,X_3) : \mathbb{Q}(X_1,X_2,X_3)^{\mathfrak{A}_3}] = 3$. D'un autre côté, on a : $\mathbb{Q}(j)(y_1,y_2,y_3) = \mathbb{Q}(j)(z_1,z_2,y_3)$. Donc :

$$[\mathbb{Q}(j)(X_1,X_2,X_3) : \mathbb{Q}(z_1,z_2,y_3)]$$

$$= [\mathbb{Q}(j)(X_1,X_2,X_3) : \mathbb{Q}(X_1,X_2,X_3)][\mathbb{Q}(X_1,X_2,X_3) : \mathbb{Q}(z_1,z_2,y_3)]$$

$$= 2[\mathbb{Q}(X_1,X_2,X_3) : \mathbb{Q}(z_1,z_2,y_3)]$$

car j est de degré 2 sur $\mathbb{Q}(X_1,X_2,X_3)$. D'où :

$$[\mathbb{Q}(X_1,X_2,X_3) : \mathbb{Q}(z_1,z_2,y_3)] = 1/2[\mathbb{Q}(j)(X_1,X_2,X_3) : \mathbb{Q}(z_1,z_2,y_3)]$$

$$= 1/2[\mathbb{Q}(j)(X_1, X_2, X_3) : \mathbb{Q}(j)(z_1, z_2, y_3)][\mathbb{Q}(j)(z_1, z_2, y_3) : \mathbb{Q}(z_1, z_2, y_3)]$$

$$= 1/2[\mathbb{Q}(j)(X_1, X_2, X_3) : \mathbb{Q}(j)(y_1, y_2, y_3)][\mathbb{Q}(j)(z_1, z_2, y_3) : \mathbb{Q}(z_1, z_2, y_3)]$$

$$\leqslant 1/2.3.2 = 3$$

car $\mathbb{Q}(j)(X_1, X_2, X_3) = \mathbb{Q}(j)(y_1, y_2, y_3, t_1)$ *et* $t_1^3 - y_1^2 y_2 = 0$. *Donc* $[\mathbb{Q}(X_1, X_2, X_3) : \mathbb{Q}(z_1, z_2, y_3)] \leqslant 3 \Rightarrow \mathbb{Q}(z_1, z_2, y_3) = \mathbb{Q}(X_1, X_2, X_3)^{\mathfrak{A}_3}$.

Exercice 2 a) Comme x_n est racine du polynôme $(T-x_1)...(T-x_n) \in L_n[T]$, x_n est de degré $\leqslant n$ sur L_n. De même, x_{n-1} est racine du polynôme $(T - x_1)...(T-x_{n-1}) = \frac{(T-x_1)...(T-x_n)}{T-x_n} \in L_n(x_n) = L_{n-1}$ (par exemple par unicité de la division euclidienne) donc x_{n-1} est de degré $\leqslant n-1$ sur L_{n-1}. Ainsi de suite, x_i est de degré $\leqslant i$ sur L_i. Donc

$$[L_0 : L_n] = \prod_{i=1}^{n} [L_{i-1} : L_i] = \prod_{i=1}^{n} \underbrace{[L_i(x_i) : L_i]}_{\leqslant i} \leqslant n! \ .$$

Or $[L_0 : L_n] = [\mathbb{Q}(X_1, ..., X_n) : \mathbb{Q}(X_1, ..., X_n)^{\mathfrak{S}_n}] = n!$. Donc pour tout i, $[L_{i-1} : L_i] = [L_i(x_i) : L_i] = i$ et $1, ..., x_i^{i-1}$ est une base de L_{i-1} comme L_i-espace vectoriel.

b) Comme $1, x_n, ..., x_n^{n-1}$ est une base de L_{n-1} comme L_n-espace vectoriel, comme $1, ..., x_{n-1}^{n-2}$ est une base de L_{n-1} comme $L_{n-2}-$espace vectoriel, les produits $x_n^{a_n} x_{n-1}^{a_{n-1}}$, $1 \leqslant a_{n-1} \leqslant n-2$, $1 \leqslant a_n \leqslant n-1$ forment une base de L_{n-2} comme L_n-espace vectoriel. De même, les les produits $x_n^{a_n} x_{n-1}^{a_{n-1}} x_{n-2}^{a_{n-2}}$, $1 \leqslant a_{n-2} \leqslant n-3$, $1 \leqslant a_{n-1} \leqslant n-2$, $1 \leqslant a_n \leqslant n-1$, forment une base de L_{n-3} comme L_n-espace vectoriel ... ainsi de suite, on en déduit que $\{x_1^{a_1}...x_n^{a_n} \ : \ \forall\, i,\ 0 \leqslant a_i \leqslant i-1\}$ est une base de $L_0 = \mathbb{Q}(x_1, ..., x_n)$ comme $L-$espace vectoriel.

c) Il suffit de montrer que $A' := A + Ax + ... + Ax^{d-1}$ est un sous-anneau de B. Pour cela il suffit de montrer que A' est stable par multiplication par x. C'est le cas car $Ax^d = A(-a_1 x^{d-1} - ... - a_d) \leqslant A + Ax + ... + Ax^{d-1} = A'$.

d) Soit $A := \mathbb{Q}[s_1, ..., s_n]$. D'après la question précédente, $A[x_n] = A + ... + Ax_n^{n-1}$.Car le polynôme $(T - x_1)...(T - x_n) \in A[T]$ est bien unitaire de degré n. De même le polynôme $(T - x_1)...(T - x_{n-1}) \in A[x_n][T]$ est bien unitaire de degré $n-1$. Donc $A[x_n][x_{n-1}] = A[x_n] + ... + A[x_n]x_{n-1}^{n-2} = \sum_{\substack{0 \leqslant i \leqslant n-2 \\ 0 \leqslant j \leqslant n-1}} A x_{n-1}^i x_n^j$. Ansi de suite ... on trouve finalement que $A[x_1, ..., x_n] = \mathbb{Q}[x_1, ..., x_n]$ est une combinaison $\mathbb{Q}[s_1, ..., s_n]-$linéaire des monômes $x_1^{a_1}...x_n^{a_n}$ où $\forall\, i,\ 0 \leqslant a_i \leqslant i-1$.

e) Soit $g \in \mathbb{Q}[x_1, ..., x_n]^{\mathfrak{S}_n}$. Alors d'une part $g = \sum_\alpha r_\alpha x^\alpha$ où α décrit les $n-$uplets $(a_1, ..., a_n)$ où $\forall\, i,\ 0 \leqslant a_i \leqslant i-1$ et où les $r_\alpha \in \mathbb{Q}[s_1, ..., s_n]$. Et d'autre part, les monômes $x_1^{a_1}...x_n^{a_n}$ où $\forall\, i,\ 0 \leqslant a_i \leqslant i-1$ forment une base de $\mathbb{Q}(x_1, ..., x_n)$ comme $\mathbb{Q}(s_1, ..., s_n)-$espace vectoriel. Comme $g \in \mathbb{Q}(s_1, ..., s_n)$, seul le coefficient devant 1 : $r_{(0,...,0)}$ est non nul et $g = r_{(0,...,0)} \in \mathbb{Q}[s_1, ..., s_n]$.

Exercice 3 a) Évident car $|\mathbb{F}_q^n| = q^n$.

b) En développant par rapport à la dernière colonne, on voit que $\Delta_n(T)$ est un polynôme de degré au plus q^n et dont le coefficient de degré q^n est : $\Delta_{n-1}(X_n)$.Il est clair que Δ_n s'annule en $\widehat{v}$ pour tout $v \in \mathbb{F}_q^n$. Donc $F_n(T)$ divise $\Delta_n(T)$ dans $\mathbb{F}_q[X_1, ..., X_n][T]$. Les degrés sont les mêmes donc $\Delta_n(T) = cF_n(T)$ où c est une constante. Cette constante est $\Delta_{n-1}(X_n)$ (en comparant les coefficients de degré q^n).

c) On a :

$$\Delta_1(T) = X_1T^q - X_1^qT = X_1^{q+1}\left(\left(\frac{T}{X_1}\right)^q - \frac{T}{X_1}\right)$$

$$= X_1^{q+1}\prod_{c\in\mathbb{F}_q}\left(\frac{T}{X_1} - c\right)$$

$$= X_1\prod_{c\in\mathbb{F}_q}(T - cX_1) = X_1F_1(T)\ .$$

En particulier $\Delta_1(T) \neq 0$ et par récurrence, $\Delta_n(T) \neq 0$ pour tout n.

d) On a $\Delta_n(T) = \Delta_{n-1}(X_n)F_n(T)$. En développant $\Delta_n(T)$ par rapport à la dernière colonne, on voit que $\Delta_n(T) = \sum_{i=0}^n d_{n,i}T^{q^i}$ pour certains coefficients $d_{n,i} \in \mathbb{F}_q[X_1, ..., X_n]$ homogènes de degré $\sum_{\substack{j=0\\ j\neq i}}^n q^j$. On a donc $F_n(T) = \sum_{i=0}^n c_{n,i}T^{q^i}$ pour certains coefficients $c_{n,i} \in \mathbb{F}_q[X_1, ..., X_n]$. On a $c_{n,i}\Delta_{n-1}(X_n) = d_{n,i}$ pour tout i. Comme $\Delta_{n-1}(X_n) \neq 0$ est homogène de degré $\sum_{j=0}^{n-1} q^j$, $c_{n,i}$ est homogène de degré $\sum_{\substack{j=0\\ j\neq i}}^n q^j - \sum_{j=0}^{n-1} q^j = q^n - q^i$.

e) Si $g \in G$, alors $g.F_n(T) = \prod_{v\in\mathbb{F}_q^n} g.(T - \widehat{v}) = \prod_{v\in\mathbb{F}_q^n}(T - \widehat{g(v)}) = F_n(T)$. En particulier tous les coefficients $c_{n,i}$ sont dans $\mathbb{F}_q(X_1, ..., X_n)^G$.

f) Posons $L := \mathbb{F}_q(c_{n,0}, ..., c_{n,n-1})$. Comme $\frac{F_n(T)}{T} \in L[T]$ est de degré $q^n - 1$ et annule X_n, X_n est de degré $\leqslant q^n - 1$ sur L. Comme X_{n-1} est annulé par $\frac{F_n(T)}{\prod_{c\in\mathbb{F}_q} T - cX_n} \in L(X_n)[T]$, qui est de degré $q^n - q$, X_{n-1} est de degré $\leqslant q^n - q$ sur $L(X_n)$. De même, comme X_{n-i} est annulé par

$$\frac{F_n(T)}{\prod_{c_n,...,c_{n-i+1}\in\mathbb{F}_q}(T - c_nX_n - ... - c_{n-i+1}X_{n-i+1})} \in L(X_n, ..., X_{n-i+1})[T]\,,$$

X_{n-i} est de degré $\leqslant q^n - q^i$ sur $L(X_n, ..., X_{n-i+1})$. On a donc :

$$[\mathbb{F}_q(X_1, ..., X_n) : \mathbb{F}_q(c_{n,0}, ..., c_{n,n-1})] = [L(X_1, ..., X_n) : L]$$

$$= \underbrace{[L(X_1, ..., X_n) : L(X_2, ..., X_n)]}_{\leqslant q^n - q^{n-1}} ... \underbrace{[L(X_n) : L]}_{\leqslant q^n - 1}$$

$$\leqslant (q^n - q^{n-1})...(q^n - 1) = |G|\ .$$

g) Or : $L \leqslant \mathbb{F}_q(X_1, ..., X_n)^G \leqslant \mathbb{F}_q(X_1, ..., X_n)$ et $[\mathbb{F}_q(X_1, ..., X_n) : \mathbb{F}_q(X_1, ..., X_n)^G] = |G|$. Donc forcément, $\mathbb{F}_q(c_{n,0}, ..., c_{n,n-1}) = L = \mathbb{F}_q(X_1, ..., X_n)^G$.

h) Posons $A := \mathbb{F}_q[c_{n,0}, ..., c_{n,n-1}]$. Pour tout i, X_{n-i} est racine de

$$\frac{F_n(T)}{\prod_{c_n,...,c_{n-i+1}\in\mathbb{F}_q}(T - c_nX_n - ... - c_{n-i+1}X_{n-i+1})} \in A[X_n, ..., X_{n-i+1}][T]$$

qui est unitaire de degré $q^n - q^i$. Comme dans l'exercice 2, on en déduit que $A[X_1, ..., X_n]$ est engendré, comme $A-$module par les monômes $X_n^{a_n}...X_1^{a_1}$ où pour tout i, $0 \leqslant a_i \leqslant q^n - q^{n-i+1}$. D'un autre côté, on déduit de la question précédente que pour tout i, $[L(X_n, ..., X_{n-i}) : L(X_n, ..., X_{n-i+1})] = q^n - q^i$. Donc les mnômes $X_n^{a_n}...X_1^{a_1}$, où pour tout i, $0 \leqslant a_i \leqslant q^n - q^{n-i+1}$, forment une base de $\mathbb{F}_q(X_1, ..., X_n)$ comme $L-$espace vectoriel. Il est clair que :

$$\mathbb{F}_q[X_1, ..., X_n]^G \geqslant \mathbb{F}_q[c_{n,0}, ..., c_{n,n-1}] \ .$$

Réciproquement, soit $P \in \mathbb{F}_q[X_1, ..., X_n]^G$. On a d'une part

$$P = \sum_{\substack{a_1,...,a_n \in \mathbb{N} \\ \forall\ i,\ 0 \leqslant a_i \leqslant q^n - q^{n-i+1}}} \lambda_a X_n^{a_n}...X_1^{a_1}$$

pour certains coefficients $\lambda_a \in A = \mathbb{F}_q[c_{n,0}, ..., c_{n,n-1}]$. Et d'autre part,

$$P = \sum_{\substack{a_1,...,a_n \in \mathbb{N} \\ \forall\ i,\ 0 \leqslant a_i \leqslant q^n - q^{n-i+1}}} \mu_a X_n^{a_n}...X_1^{a_1}$$

pour des coefficients uniques $\mu_a \in L = \mathbb{F}_q(c_{n,0}, ..., c_{n,n-1}) = \mathbb{F}_q(X_1, ..., X_n)^G$. Par unicité, comme $P \in \mathbb{F}_q[X_1, ..., X_n]^G \leqslant L$, on a :

$$\lambda_{(0,...,0)} = \mu_{(0,...,0)} = P$$

et tous les autres coefficients $\mu_a = \lambda_a = 0$, $a \neq (0, ..., 0)$.
En particulier, $P = \lambda_{(0,...,0)} \in A = \mathbb{F}_q[X_1, ..., X_n]^G$.

i) Si $\mathbb{F}_q = \mathbb{Z}/2\mathbb{Z}$, alors :

$$F_2(T) = T(T - X_1)(T - X_2)(T - X_1 - X_2)$$

$$= T^4 + T^2 \underbrace{(X_1^2 + X_2^2 + X_1X_2)}_{=c_{2,1}} + T \underbrace{(X_1^2X_2 + X_1X_2^2)}_{=c_{2,0}} \ .$$