Corrigé du devoir à la maison

Exo 1

a) Notons $e_1 := {}^t(1,0)$ et $e_2 := {}^t(0,1)$ la base canonique de k^2.

Si $g \in \mathrm{GL}_2(k)$ laisse fixes les droites $ke_1, ke_2, k(e_1+e_2)$, alors il existe $\lambda \in k^\times$ tel que $g = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$. On note Z le sous-groupe formé par ces matrices.

b) Le sous-groupe G de $\mathrm{GL}_2(k)/Z$ engendré par les matrices

$$\sigma := \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \tau := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

modulo Z opère sur l'ensemble des droites de k^2 qui passent par 0 et permutent les droites $l_1 := ke_1$, $l_2 := ke_2$,$l_3 := ke_3$.

On a donc un morphisme de groupes $G \to S_3$. Ce morphisme est injectif d'après la question a). Or par ce morphisme, σ correspond à la transposition (23) car $\sigma(l_2) = l_3, \sigma(l_3) = l_2, \sigma(l_1) = l_1$ et τ à la transposition (12). Or ces transpositions engendrent S_3 Donc G est isomorphe à S_3.

c) Notons $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ la classe d'une matrice modulo Z.

Si $A := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(k)/Z$, on note H_A l'endomorphisme de corps : $k(t) \to k(t)$, $f(t) \mapsto f\left(\frac{at+b}{ct+d}\right)$ (on voit facilement que H_A ne dépend que de la classe de A modulo Z).

On a $H_A \circ H_B = H_{BA}$ et $H_{I_2} = \mathrm{Id}$. En particulier, H_A est un automorphisme du corps $k(t)$ (d'inverse $H_{A^{-1}}$).

On a donc un morphisme de groupes :

$$\mathrm{GL}_2(k)/Z \to \mathrm{Aut}_k(k(t)) \quad A \mapsto H_{A^{-1}} \ .$$

Ce morphisme est injectif car $H_A(t) = t \Leftrightarrow a = d$ et $b = c = 0$.

De plus H_σ et H_τ sont les automorphismes qui envoient t sur $1-t$ et t sur t^{-1} (respectivement). Donc le groupe engendré par les matrices σ et τ modulo Z est isomorphe au sous-groupe H des automorphismes de $k(t)$ engendré par $f(t) \mapsto f(1-t)$ et $f(t) \mapsto f(t^{-1})$.

Donc l'extension $k(t)^H \subseteq k(t)$ est galoisienne de groupe de Galois isomorphe à S_3 d'après le théorème d'Artin. C'est une extension de degré 6. De plus, $k\left(\frac{(t^2-t+1)^3}{t^2(t-1)^2}\right) \subseteq k(t)^H$. Or, le polynôme

$$X^2(X-1)^2\left(\frac{(t^2-t+1)^3}{t^2(t-1)^2}\right) - (X^2-X+1)^3 \in k\left(\frac{(t^2-t+1)^3}{t^2(t-1)^2}\right)[X]$$

est de degré 6 et annule t. Donc :

$$[k(t) : k\left(\frac{(t^2-t+1)^3}{t^2(t-1)^2}\right)] \leq 6$$

et :

$$k(t)^H = k\left(\frac{(t^2-t+1)^3}{t^2(t-1)^2}\right) \ .$$

Plus généralement, on peut montrer que si $p(t), q(t)$ sont des polynômes premiers entre eux dans $k[t]$, alors le polynôme $q(X)\frac{p}{q} - p(X) \in k\left(\frac{p}{q}\right)[X]$ est le polynôme minimal de t sur $k\left(\frac{p}{q}\right)$ et que son degré est $\max\{\deg p, \deg q\}$.

*

Exo 2

a) Soit $K := \mathbb{C}(\sigma_1, .., \sigma_n)$.

Le polynôme $P(T) = (T - X_1)...(T - X_n) = T^n - \sigma_1 T^{n-1} + ... + (-1)^n \sigma_n$ est dans $K[T]$.

Comme le polynôme $\frac{P(T)}{(T-X_1)...(T-X_{i-1})} \in K(X_1, ..., X_{i-1})[T]$ annule X_i, $[K(X_1, ..., X_i) : K(X_1, ..., X_{i-1})] \leq n - i + 1$.

Donc $K(X_1, ..., X_n) = \mathbb{C}(X_1, ..., X_n)$ est de degré $\leq n!$ sur K.

Or, $K \subseteq \mathbb{C}(X_1, ..., X_n)^{S_n} \subseteq \mathbb{C}(X_1, ..., X_n)$ et $[\mathbb{C}(X_1, ..., X_n) : \mathbb{C}(X_1, ..., X_n)^{S_n}] = |S_n| = n!$.

Donc $K = \mathbb{C}(X_1, ..., X_n)^{S_n}$.

b) Soit $\Delta := \prod_{1 \leq i < j \leq n} (X_i - X_j)$.

Si $\sigma \in S_n$, $\sigma.\Delta = \epsilon(\sigma)\Delta$.

Donc $\mathbb{C}(\sigma_1, ..., \sigma_n, \Delta) \subseteq \mathbb{C}(X_1, ..., X_n)^{A_n}$ et $\Delta \notin \mathbb{C}(X_1, ..., X_n)^{S_n} = \mathbb{C}(\sigma_1, ..., \sigma_n)$.

Donc $[\mathbb{C}(X_1, ..., X_n) : \mathbb{C}(\sigma_1, ..., \sigma_n, \Delta)] \leq n!/2$.

Or, $[\mathbb{C}(X_1, ..., X_n) : \mathbb{C}(X_1, ..., X_n)^{A_n}] = |A_n| = n!/2$; donc :

$$\mathbb{C}(X_1, ..., X_n)^{A_n} = \mathbb{C}(\sigma_1, ..., \sigma_n, \Delta) \ .$$

c) Soient : $Y_1 = X_1 + jX_2 + j^2 X_3$, $Y_2 := X_1 + j^2 X_2 + jX_3$ et $Y_3 = X_1 + X_2 + X_3$.

Soit σ le 3−cycle (123). Comme $\sigma.Y_1 = j^2 Y_1$ et $\sigma.Y_2 = jY_2$, on a : $\mathbb{C}(Y_1^2/Y_2, Y_2^2/Y_1, Y_3) \subseteq \mathbb{C}(X_1, X_2, X_3)^{A_3}$.

Or, $\mathbb{C}(X_1, X_2, X_3) = \mathbb{C}(Y_1, Y_2, Y_3)$ car :

$$\begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix} = \begin{pmatrix} 1 & j & j^2 \\ 1 & j^2 & j \\ 1 & 1 & 1 \end{pmatrix}^{-1} \begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \end{pmatrix} \ .$$

Comme $Y_1^3 = (Y_1^2/Y_2)^2 Y_2^2/Y_1$, Y_1 est de degré ≤ 3 sur $\mathbb{C}(Y_1^2/Y_2, Y_2^2/Y_1, Y_3)$.

Donc $\mathbb{C}(Y_1, Y_2, Y_3) = \mathbb{C}(X_1, X_2, X_3) = \mathbb{C}(Y_1^2/Y_2, Y_2^2/Y_1, Y_3)(Y_1)$ est de degré ≤ 3 sur $\mathbb{C}(Y_1^2/Y_2, Y_2^2/Y_1, Y_3)$.

Comme $[\mathbb{C}(X_1, X_2, X_3) : \mathbb{C}(X_1, X_2, X_3)^{A_3}] = 3$, on a forcément :

$$\mathbb{C}(X_1, X_2, X_3)^{A_3} = \mathbb{C}(Y_1^2/Y_2, Y_2^2/Y_1, Y_3) \ .$$