Fiche IV, exercice 3 :

Soit $K := \mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, \sqrt[5]{5})$. Comme $\sqrt[5]{5}$ est de degré au plus 5 sur $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$, comme $\sqrt[3]{3}$ est de degré au plus 3 sur $\mathbb{Q}(\sqrt{2})$, comme $\sqrt{2}$ est de degré 2 sur $\mathbb{Q}$, K est de degré au plus $2 \times 3 \times 5$ sur $\mathbb{Q}$. Or, K contient $\sqrt{2}$ qui est de degré 2 sur $\mathbb{Q}$, $\sqrt[3]{3}$ qui est de degré 3 sur $\mathbb{Q}$ et $\sqrt[5]{5}$ qui est de degré 5 sur $\mathbb{Q}$. Donc le degré de K sur $\mathbb{Q}$ est un multiple de 2, de 3 et de 5 *i.e.* un multiple de $2 \times 3 \times 5$. Conclusion : $[K : \mathbb{Q}] = 30$.

Un plongement σ de K dans $\mathbb{C}$ est entièrement déterminé par

$$\sigma(\sqrt{2}), \sigma(\sqrt[3]{3}), \sigma(\sqrt[5]{5}) \ .$$

Or,

$$\sigma(\sqrt{2}) = \pm\sqrt{2} \ , \ \sigma(\sqrt[3]{3}) = j^l \sqrt[3]{3} \ , \ \sigma(\sqrt[5]{5}) = \zeta^m \sqrt[5]{5}$$

où $j = e^{2i\pi/3}, \zeta = e^{2i\pi/5}$ et $l \in \mathbb{Z}/3\mathbb{Z}, m \in \mathbb{Z}/5\mathbb{Z}$.

Cela fait au plus $2 \times 3 \times 5 = 30$ plongements. Or, il y a exactement $[K : \mathbb{Q}] = 30$ plongements de $\mathbb{Q}$ dans $\mathbb{C}$ donc toutes les possibilités sont réalisées : les plongements de K dans $\mathbb{C}$ sont les $\sigma_{k,l,m}$, $k \in \mathbb{Z}/2\mathbb{Z}, l \in \mathbb{Z}/3\mathbb{Z}, m \in \mathbb{Z}/5\mathbb{Z}$ où $\sigma_{k,l,m}$ est le plongement de K dans $\mathbb{C}$ qui envoie $\sqrt{2}$ sur $(-1)^k\sqrt{2}$, $\sqrt[3]{3}$ sur $j^l\sqrt[3]{3}$ et $\sqrt[5]{5}$ sur $\zeta^m\sqrt[5]{5}$.

Soit $x := \sqrt{2} + \sqrt[3]{3} + \sqrt[5]{5}$. Montrons que $K = \mathbb{Q}(x)$. Il suffit de montrer que x est de degré ≥ 30 sur $\mathbb{Q}$, il suffit donc de montrer qu'il existe au moins 30 plongements de $\mathbb{Q}(x)$ dans $\mathbb{C}$. Or, les $\sigma_{k,l,m}(x)$ sont deux à deux distincts.

En effet, on a :

$$\sigma_{k,l,m}(x) = \sigma_{k',l',m'}(x)$$
$$\Leftrightarrow (-1)^k\sqrt{2} + j^l\sqrt[3]{3} + \zeta^m\sqrt[5]{5} = (-1)^{k'}\sqrt{2} + j^{l'}\sqrt[3]{3} + \zeta^{m'}\sqrt[5]{5}$$

en particulier, si $m \neq m' \bmod 5$, alors $\sqrt[5]{5} \in \mathbb{Q}(\sqrt{2}, j, \sqrt[3]{3}, \zeta)$ et 5 divise $[\mathbb{Q}(\sqrt{2}, j, \sqrt[3]{3}, \zeta) : \mathbb{Q}]$.

Or, $\sqrt{2}, j$ sont de degrés 2 sur $\mathbb{Q}$, $\sqrt[3]{3}$ est de degré 3 sur $\mathbb{Q}$ et ζ de degré 4 sur $\mathbb{Q}$ (annulé par le polynôme irréductible $X^4 + X^3 + X^2 + X + 1$). Donc

$$[\mathbb{Q}(\sqrt{2}, j, \sqrt[3]{3}, \zeta) : \mathbb{Q}] =$$
$$\underbrace{[\mathbb{Q}(\sqrt{2}, j, \sqrt[3]{3}, \zeta) : \mathbb{Q}(\sqrt{2}, j, \sqrt[3]{3})]}_{\leq 4} \underbrace{[\mathbb{Q}(\sqrt{2}, j, \sqrt[3]{3}) : \mathbb{Q}(\sqrt{2}, j)]}_{\leq 3} \underbrace{[\mathbb{Q}(\sqrt{2}, j) : \mathbb{Q}]}_{\leq 4}$$

qui ne peut pas être un multiple de 5. Donc $m = m' \bmod 5$. De même, on voit que $l = l' \bmod 3$ et $k = k' \bmod 2$.

Fiche V, exo 1 : On a :

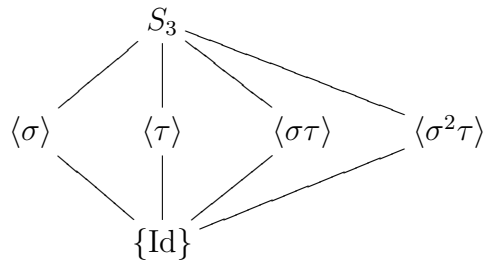
$$X^3 - 2 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$$

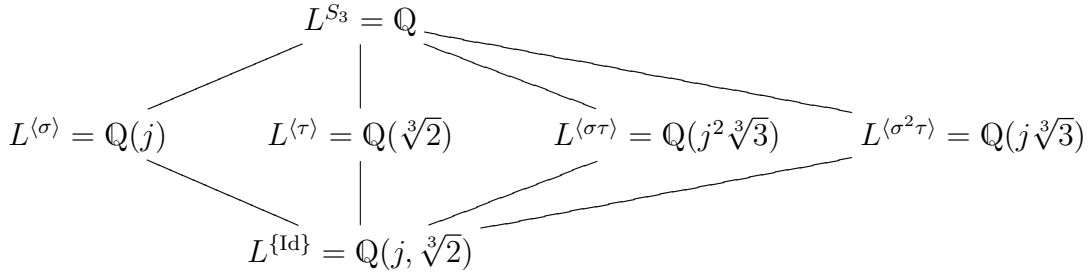
où $\alpha_k := j^{k-1}\sqrt[3]{2}$. Le corps de décomposition de X^3-2 est : $K := \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(j, \sqrt[3]{2})$ qui est de degré 6 sur $\mathbb{Q}$ car $\sqrt[3]{2}$ est de degré 3 sur $\mathbb{Q}$ et j de degré 2 sur $\mathbb{Q}(\sqrt[3]{2})$.

Soit G le groupe de Galois de X^3-2 sur $\mathbb{Q}$. comme G permute les racines $\alpha_1, \alpha_2, \alpha_3$, on peut l'identifier à un sous-groupe de S_3.

Soit τ la restriction de la conjugaison complexe à K et $\sigma \in \mathrm{Gal}(K/\mathbb{Q}(j))$ qui envoie $\sqrt[3]{2}$ sur $j\sqrt[3]{2}$. Alors τ correspond à la transposition (23) et σ au 3−cycle (123). Ces deux permutations engendrent S_3 donc $G = S_3$.

Voici le diagramme des sous-groupes de $G = S_3$ et le diagramme correspondants des sous-corps de $K = \mathbb{Q}(j, \sqrt[3]{2})$:





Les « traits » relient deux groupes (respectivement deux corps) qui n'ont pas de sous-groupes (respectivement pas de sous-corps) intermédiaires.

Pour la suite rappelons le théorème d'Artin (que nous démontrerons au prochain td) :

Théorème 0.0.1 *Soit K un corps. Soit G un sous-groupe fini du groupe des automorphismes du corps K. Alors l'extension $K^G \subseteq K$ est finie de degré l'ordre de G. On dit qu'une telle extension est galoisienne de groupe de Galois G (c'est une définition).*

exo 2 : Soit p un nombre premier et $q = p^r$ une puissance de p. On considère l'extension de degré n de corps finis : $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$. Soit $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ $x \mapsto x^q$. Comme $\mathbb{F}_q$ est de caractéristique p, F est bien un morphisme de corps donc injectif donc surjectif (car au départ et à l'arrivée, on a le même

cardinal). De plus $x^q = x$ pour tout $x \in \mathbb{F}_q$. Le groupe engendré par F est cyclique d'ordre n et il est clair que $\mathbb{F}_{q^n}^{\langle F \rangle} = \{x \in \mathbb{F}_{q^n} \ : \ x^q = x\} = \mathbb{F}_q$.

Donc $\mathbb{F}_{q^n}/\mathbb{F}_q$ est galoisienne cyclique.

exo 7 : On note u_k le point de coordonnées $(\cos(2k\pi/n), \sin(2k\pi/n))$ sur le cercle unité (ce sont les sommets d'un polygone régulier à n côtés). Par exemple si $n = 4$ on obtient le carré de somets $(\pm 1, 0), (0, \pm 1)$.

On note D_{2n} le sous-groupe de $\mathrm{GL}_2(\mathbb{R})$ formé des matrices qui laissent stable l'ensemble $\{u_0, ..., u_{n-1}\}$. Le groupe D_{2n} est d'ordre $2n$ engendré par la rotation d'angle $2\pi/n$:

$$R := \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}$$

et la symétrie :

$$S := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \ .$$

On appelle D_{2n} le groupe diédral d'ordre $2n$.

Remarque si G est un groupe engendré par deux éléments r, r tels que :

$$r^n = 1, s^2 = 1, (rs)^2$$

alors l'application $R \mapsto r, S \mapsto s$ se prolonge (de manière unique) en un morphisme de groupes $D_{2n} \to G$.

En particulier, les automorphismes $t \mapsto \zeta t, t \mapsto t^{-1}$ du corps $\mathbb{C}(t)$ engendrent un groupe G isomorphe à D_{2n}.

Donc l'extension $\mathbb{C}(t)^G \subseteq \mathbb{C}(t)$ est galoisienne de groupe de Galois $G \simeq D_{2n}$ et de degré $2n$.

Or, $\mathbb{C}(t^n + t^{-n}) \subseteq \mathbb{C}(t)^G$. De plus :

$$[\mathbb{C}(t) : \mathbb{C}(t^n + t^{-n})] = [\mathbb{C}(t) : \mathbb{C}(t^n)][\mathbb{C}(t^n) : \mathbb{C}(t^n + t^{-n})]$$

$$\leq n \times 2 = 2n$$

car $X^n - t^n \in \mathbb{C}(t^n)[X]$ annule t et $(X - t^n)(X - t^{-n}) \in \mathbb{C}(t^n + t^{-n})[X]$ annule t^n.

Donc $\mathbb{C}(t)^G = \mathbb{C}(t^n + t^{-n})$.

exo 8 :

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 :

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

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 $\max\{\deg p, \deg q\}$.