Famille $\mathbb{Q}$-libre par la trace et un groupe de Galois en cadeau

Introduction

Ce développement est un banger vue pour la première fois sur la chaine YouTube de Philippe Caldero. La partie Galois est facultative.

I. Famille $\mathbb{Q}$-libre

Je vous propose d'apprendre ce développement par ce petit exercice (qui est fait pour des élèves de maths spé, c'est pas censé être trop dur) :

Exercice I.0.1. Famille $\mathbb{Q}$-libre par la trace Soit $\mathbb{L}$ un sous-corps de $\mathbb{C}$ (il contient $\mathbb{Q}$, c'est un $\mathbb{Q}$-espace vectoriel). Soit $\alpha \in \mathbb{L}$. On note m_α l'endomorphisme $\mathbb{Q}$-linéaire de $\mathbb{L}$ donné par $x \mapsto \alpha x$. Soit $p_1, \dots, p_n$ des nombres premiers distincts. On dit que $\alpha \in \mathbb{L}$ est algébrique s'il existe un polynôme non nul μ_α à coefficients dans $\mathbb{Q}$ qui annule α, on note μ_α un polynôme annulateur de degré minimal unitaire.

1. Soit $\alpha \in \mathbb{C}$. Montrer que si α est algébrique sur $\mathbb{Q}$, alors $\mathbb{Q}(\alpha)$ est un $\mathbb{Q}$-espace vectoriel de dimension finie dont on précisera la dimension en fonction de μ_α.
2. Montrer que si $d \in \mathbb{Z}$ n'est pas un carré, $\mathbb{Q}(\sqrt{d})$ est de dimension 2, en donner une base.
3. Montrer que χ_{m_α} est une puissance de μ_α.
4. Si $I \subset [\![1, n]\!]$, montrer que si $\alpha = \prod_{i \in I} \sqrt{p_i}$, alors $\mathrm{Tr}(m_\alpha) = 0$.
5. Montrer que la matrice $\left(\mathrm{Tr}\left(\prod_{i \in I} \sqrt{p_i} \prod_{j \in J} \sqrt{p_j}\right)\right)_{I,J \subset [\![1,n]\!]}$ est inversible.
6. En déduire que la famille $\left(\prod_{i \in I} \sqrt{p_i}\right)_I$ est $\mathbb{Q}$-libre et en déduire la dimension de $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$.

II. Un groupe de Galois vraiment facile

L'extension $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})/\mathbb{Q}$ est donc de degré 2^n. Si $p_1, \dots, p_n$ est une suite de nombres premiers tous différents, on va prouver que $G_n := \mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})/\mathbb{Q})$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}^n$ via l'isomorphisme : $\varphi_n : \left| \begin{array}{ccc} G_n & \longrightarrow & \mathbb{Z}/2\mathbb{Z}^n \\ \sigma & \longmapsto & (k_i)_i \end{array} \right.$ où $k_i = 0$ si $\sigma(\sqrt{p_i}) = \sqrt{p_i}$ et $k_i = 1$ si $\sigma(\sqrt{p_i}) = -\sqrt{p_i}$.

Par cardinalité, il n'y à qu'à prouver la surjectivité. Le groupe $\mathbb{Z}/2\mathbb{Z}^n$ est engendré par les $(\mathbb{1}_{i=j})_j$ pour chaque $i \in [\![1, n]\!]$. Soit $i \in [\![1, n]\!]$. L'extension

$$\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})/\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n} \text{ mais pas } \sqrt{p_i})$$

est de degré 2 (par le résultat du développement et le théorème de la base télescopique) et galoisienne donc son groupe de Galois est naturellement $\mathbb{Z}/2\mathbb{Z}$. Il existe donc un morphisme σ_i dans le groupe de cette extension tel que $\sigma_i(\sqrt{p_i}) = -\sqrt{p_i}$. Mais le groupe de cette extension est un sous-groupe de G_n, et $\sigma_i \in G_n$ est un antécédent de $(\mathbb{1}_{j \neq i})_j$. D'où le résultat.

Contactez-moi en cas de coquille s'il vous plaît ! prenom.nom@ens-lyon.fr