Leonid Monin
Léo Navarro Chafloque

Solutions – Semaine 14

Exercice 1.
Soit K un corps, et soit $K \subseteq M = K(\alpha)$ et $K \subseteq N = K(\beta)$ des extensions galoisiennes de K.

1. Démontrez que $K \subseteq L = K(\alpha, \beta)$ est aussi galoisienne.

Supposons à partir de maintenant que $M \cap N = K$ en tant que sous-corps de L.

2. Démontrez que $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K)$ qui est la restriction sur chaque composante est un isomorphisme.

Solution.

1. On sait par le cours qu'une extension est Galoisienne si et seulement si c'est un corps de décomposition d'un polynôme séparable. Ainsi les polynômes $m_{\alpha,K}$ et $m_{\beta,K}$ sont séparables et se scindent sur $K(\alpha)$ et $K(\beta)$ respectivement. Ainsi, le polynôme $m_{\alpha,K}m_{\beta,K}$ est aussi séparable et se scinde sur $K(\alpha, \beta)$. Comme $K(\alpha, \beta)$ est généré par les racines de $m_{\alpha,K}m_{\beta,K}$ (il est généré par α et β), c'est bien un corps de décomposition de $m_{\alpha,K}m_{\beta,K}$. Par le même fait rappelé plus haut, $K(\alpha, \beta)$ est Galoisien sur K.

2. Comme M/K est Galoisienne, on sait que pour tout $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(M) = M$. Ainsi, σ se restricte en un élément $\sigma|_M \in \mathrm{Gal}(M/K)$, et on a donc un morphisme de groupes $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$. En faisant la même chose pour N, on en déduit un morphisme de groupes

$$\mathrm{Gal}(L/K) \xrightarrow{\quad\phi\quad} \mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K)$$

$$\sigma \longmapsto (\sigma|_M, \sigma|_N)$$

Ce morphisme est automatiquement injectif, car si $\sigma \in \mathrm{Gal}(L/K)$ se restreint à l'identité sur M et sur N, alors il fixe α et β. Come $L = K(\alpha, \beta)$, on doit avoir $\sigma = id$.

De plus, $|\mathrm{Gal}(L/K)| = [L : K]$ et

$$|\mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K)| = |\mathrm{Gal}(M/K) \cdot |\mathrm{Gal}(N/K)| = [M : K][N : K].$$

Supposons que l'on a prouvé que $[L : M] = [N : K]$. Alors

$$[M : K][N : K] = [M : K][L : M] = [L : K].$$

Ainsi, ϕ est un morphisme injectif entre groupes finis ayant le même cardinal. C'est donc automatiquement un isomorphisme, ce qui conclut la preuve.

Montrons maintenant que $[L : M] = [N : K]$ (c'est ici ou on utilisera que $M \cap N = K$!). Comme $L = M(\beta)$, il est équivalent de montrer que $\deg(m_{\beta,M}) = \deg(m_{\beta,K})$. Comme $m_{\beta,M}$ divise $m_{\beta,K}$, ce qu'il faut réellement montrer est que $m_{\beta,M} = m_{\beta,K}$.

Comme $m_{\beta,K}$ sur scinde sur N, on a que

$$m_{\beta,K}(t) = \prod_i (t - \beta_i) \in N[t],$$

où le produit se fait sur les racines de $m_{\beta,K}$. Ainsi, en voyant $m_{\beta,M}(t)$ comme un élément de $L[t]$, on a nécessairement que

$$m_{\beta,M}(t) = c\prod_j (t-\beta_j)$$

où $c \in L$ et les β_j sont certaines racines de $m_{\beta,K}$. Comme $m_{\beta,M}$ est unitaire, $c = 1$ et donc comme tous les β_j sont dans N, on en déduit que $m_{\beta,M}(t) \in N[t]$. Ainsi $m_{\beta,M}(t) \in M[t] \cap N[t] = K[t]$, et comme il s'annule en β, il est divisible par $m_{\alpha,K}(t)$. Cela conclut donc la preuve.

Exercice 2 (Correspondance de Galois)**.**
Calculez les groupes de Galois $\mathrm{Gal}(E/\mathbb{Q})$ puis exprimez tous les sous-corps intermédiaires avec leur sous-groupe correspondant ainsi que des éléments primitifs* et polynôme minimaux pour ceux-ci des extensions Galoisiennes E de $\mathbb{Q}$ donnés par

1. le corps de décomposition de $x^3 - 2$ dans $\mathbb{C}$,
2. le corps de décomposition de $x^4 - 2$ dans $\mathbb{C}$.

Utilisez ce que vous savez déjà grâce aux exercices de la série 12.

Solution.

1. On a déjà calculé que $E = \mathbb{Q}(\xi, \sqrt[3]{2})$ et que $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$. Notons r un élément d'ordre 3 et s un élément d'ordre 2 de sorte que $\langle r, s\rangle = \mathrm{Gal}(E/\mathbb{Q})$, avec

   (a) $r(\xi) = \xi$, $r(\sqrt[3]{2}) = \xi\sqrt[3]{2}$.
   (b) $s(\sqrt[3]{2}) = \sqrt[3]{2}$, $s(\xi) = \xi^2$.

   Les sous-groupes de $\mathrm{Gal}(E/\mathbb{Q})$ sont les suivants (regroupés par classe de conjugaison, avec leur ordre en titre de colonne)

   1 | 2 | 3 | 6

   $$\{e\} \longrightarrow < s >, < sr >, < sr^2 > \longrightarrow \mathrm{Gal}(E/\mathbb{Q}) \quad ; \quad \{e\} \longrightarrow < r > \longrightarrow \mathrm{Gal}(E/\mathbb{Q})$$

   Comme ξ est de degré 2, on voit que $\mathbb{Q}(\xi)$ est le sous-corps fixé par $< r >$. Comme $\sqrt[3]{2}$ est de degré 3, on voit que $\mathbb{Q}(\sqrt[3]{2})$ est le sous-corps fixé par $< s >$.

   Notons également que $sr = rsr^{-1}$ et que $sr^2 = r^2sr^{-2}$. Ainsi comme les conjugués correspondent à l'image par l'élément de l'extension on obtient que les sous-corps fixés par $< sr >$ et $< sr^2 >$ sont respectivement $\mathbb{Q}(\xi\sqrt[3]{2})$ et $\mathbb{Q}(\xi^2\sqrt[3]{2})$. On résume cela en imitant en miroir le tableau des sous-groupes ci-dessus, le nombre de la colonne correspondant maintenant au degré.

   6 | 3 | 2 | 1

   $$\mathbb{Q}(\xi, \sqrt[3]{2}) \longrightarrow \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\xi\sqrt[3]{2}), \mathbb{Q}(\xi^2\sqrt[3]{2}) \longrightarrow \mathbb{Q} \quad ; \quad \mathbb{Q}(\xi, \sqrt[3]{2}) \longrightarrow \mathbb{Q}(\xi) \longrightarrow \mathbb{Q}$$

*C'est à dire des générateurs sur $\mathbb{Q}$ de ces extensions intermédiaires.

En ce qui est des éléments primitifs, ils sont tous déjà donnés sauf $\xi + \sqrt[3]{2}$ pour l'extension E. Les polynômes minimaux de ξ et $\sqrt[3]{2}$ et leurs conjugués sont x^2+x+1 et x^3+2 respectivement. Quant à $\xi + \sqrt[3]{2}$ – on pourrait multiplier les $x - \alpha$ où α sont tous les conjugés de l'élément. C'est un peu fastidieux, alors on écrit la matrice de multiplication par cet élément dans la base de E suivante

$$1, \xi, \sqrt[3]{2}, \xi\sqrt[3]{3}, \sqrt[3]{4}, \xi\sqrt[3]{4}$$

c'est à dire (on utilise $\xi^2 = -1 - \xi$)

$$\begin{pmatrix} 0 & -1 & 0 & 0 & 2 & 0 \\ 1 & -1 & 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 1 & -1 \end{pmatrix}$$

puis on calcule le polynôme caractéristique de cette matrice pour conclure que le polynôme suivant

$$x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9$$

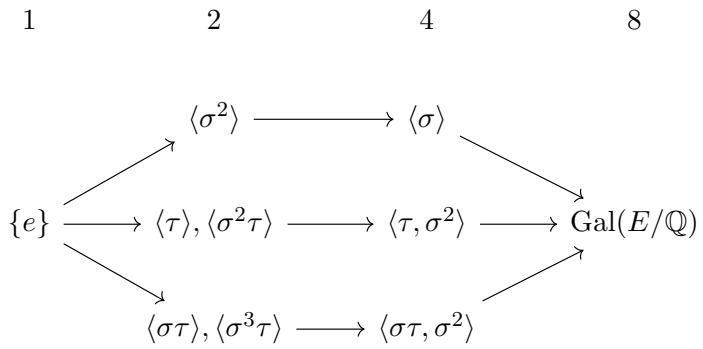
annule $\xi + \sqrt[3]{2}$ – comme il est de degré 6, c'est le polynôme minimal.

2. On a déjà calculé que $E = \mathbb{Q}(i, \sqrt[4]{2})$ et que $\mathrm{Gal}(E/\mathbb{Q}) \cong D_8$. Notons σ un élément d'ordre 4 et τ un élément d'ordre 2

   (a) $\sigma(i) = i$, $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$.

   (b) $\tau(i) = -i$, $\tau(\sqrt[4]{2}) = -\sqrt[4]{2}$.

   Notons que $\tau(-\sqrt[4]{2}) = \sqrt[4]{2}$ et $i\sqrt[4]{2}$ et $-i\sqrt[4]{2}$ sont fixés par τ. Notons aussi que $\sigma(\sqrt{2}) = -\sqrt{2}$. Les sous-groupes de $\mathrm{Gal}(E/\mathbb{Q})$ sont les suivants (regroupés par classe de conjugaison, avec leur ordre en titre de colonne)



   Notons que $\sqrt{2}$ est fixée par σ^2 et τ et que $i\sqrt{2}$ est fixée par σ^2 et $\sigma\tau$, et que i est fixée par σ, on a en comparant les degrés sur $\mathbb{Q}$ que

$$E^{<\sigma>} = \mathbb{Q}(i) \quad E^{\langle\tau,\sigma^2\rangle} = \mathbb{Q}(\sqrt{2}) \quad E^{\langle\sigma\tau,\sigma^2\rangle} = \mathbb{Q}(i\sqrt{2}).$$

   Comme $\mathbb{Q}(i, \sqrt{2})$ est une sous-Galois extension de de degré 4 on conclut qu'elle corresponds au seul sous-groupe normal d'ordre 2, c'est à dire

$$E^{<\sigma^2>} = \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i + \sqrt{2}).$$

Comme $i\sqrt[4]{2}$ est fixée par τ et qu'il a degré 4, et que $\sigma^2\tau = \sigma\tau\sigma^{-1}$, on obtient que

$$E^{<\tau>} = \mathbb{Q}(i\sqrt[4]{2}) \qquad E^{<\sigma^2\tau>} = E^{\sigma<\tau>\sigma^{-1}} = \sigma(E^{<\tau>}) = \mathbb{Q}(-\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}).$$

Notons que $\sqrt[4]{2}(1-i) = \sqrt[4]{2} - i\sqrt[4]{2}$ is est fixée par $\sigma\tau$ et de degré 4 car on peut calculer son orbite par le groupe de Galois explicitement et qu'elle est de taille 4, on obtient en comparant les degrés

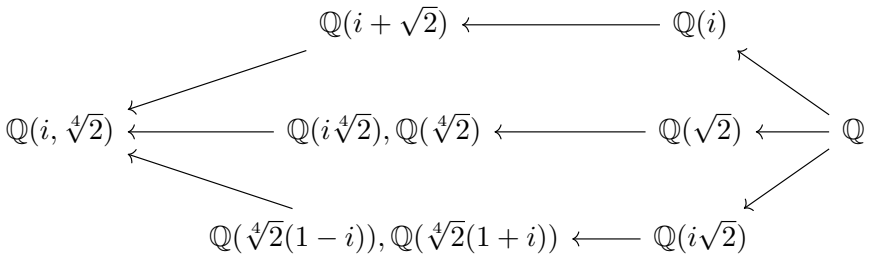
$$E^{<\sigma\tau>} = \mathbb{Q}(\sqrt[4]{2}(1-i)).$$

Maintenant en utilisant le même argument que ci-dessus on obtient finalement

$$E^{<\sigma^3\tau>} = \mathbb{Q}(\sqrt[4]{2}(1+i)).$$

On résume la correspondance obtenue en imitant en miroir le diagramme des sous-groupes ci-dessus.

8 4 2 1



En ce qui est des polynômes minimaux des éléments primitifs apparaissant ci-dessus,

(a) Les polynômes minimaux de $i, \sqrt{2}, i\sqrt{2}$ sont respectivement x^2+1, x^2-2 et x^2+2.

(b) Le polynôme minimal de $i+\sqrt{2}$ est

$$x^4 - 2x^2 + 9$$

En effet en multipliant on trouve que le polynôme minimal est

$(x-(i+\sqrt{2}))(x+(i+\sqrt{2}))(x-(i-\sqrt{2}))(x+(i-\sqrt{2})) = (x^2-(1+2i\sqrt{2}))(x^2-(1-2i\sqrt{2})) = x^4-2x^2+9.$

(c) Le polynôme minimal de $i\sqrt[4]{2}$ et $\sqrt[4]{2}$ est

$$x^4 - 2.$$

(d) Le polynôme minimal de $\sqrt[4]{2}(1-i)$ et $\sqrt[4]{2}(1+i)$ est

$$x^4 + 8.$$

En effet $(1-i)^4 = (1+i)^4 = -4$.

Pour conclure on calcule le polynôme minimal de l'élément primitif de $i+\sqrt[4]{2}$. Pour cela on calcule le produit des $x-\alpha$ où les α sont les conjugués de $i+\sqrt[4]{2}$. On regroupe deux par deux ceux ci $i+i^k\sqrt[4]{2}$ et $-i+i^k\sqrt[4]{2}$ pour $k=0,1,2,3$. On commence par multiplier les polynômes en regroupant par paire comme ci-dessus pour obtenir les quatres polynômes de degré 2

$$x^2 + 2\sqrt[4]{2}x + \sqrt{2}, \quad x^2 - 2\sqrt[4]{2}x + \sqrt{2}, \quad x^2 + 2i\sqrt[4]{2}x - \sqrt{2}, \quad x^2 - 2i\sqrt[4]{2}x - \sqrt{2}.$$

Puis un multipliant les deux premiers puis les deux suivants, on obtient respectivement

$$x^4 - 2\sqrt{2}x^2 + 2, \quad x^4 + 2\sqrt{2}x^2 + 2.$$

Et finalement en multipliant ces deux derniers polynômes,

$$x^8 - 4x^4 + 4.$$