Leonid Monin
Léo Navarro Chafloque

Solutions – Semaine 12

Exercice 1.
Soit $f = x^3 + ax + 1 \in \mathbb{Q}[x]$ avec $a > 0$, $a \in \mathbb{Z}$.

1. Montrer que f est irréductible sur $\mathbb{Q}$.
2. Montrer que f a une racine réelle, mais pas trois.
3. Soit $K = \mathbb{Q}[x]/(f)$. Montrer que $K/\mathbb{Q}$ est une extension de degré 3 qui n'est pas Galoisienne.
4. Soit L le corps de décomposition de f sur $\mathbb{Q}$. Montrer que $\mathrm{Gal}(L/Q) \cong S_3$.

Solution.

1. As $\deg f = 3$ one just has to verify that f does not have a root over $\mathbb{Q}$. So, we need to show that if b and c are non-zero relatively prime integers, then
$$(b/c)^3 + (ab/c) + 1 \neq 0,$$
or equivalently
$$b^3 + abc^2 + c^3 \neq 0.$$
Suppose the contrary. Then c divides b^3 and b divides c^3. Using the relative prime assumption we obtain both b and c are plus-minus 1, so that a root has to be 1 or -1 but one sees as $a > 0$ that
$$1 + a + 1 \neq 0 \quad \text{and} \quad -1 - a + 1 \neq 0.$$
2. Since $f(x)$ tends to $-\infty$ as x goes to $-\infty$ and goes to $+\infty$ as x goes to $+\infty$, we deduce by the mean value theorem that f has at least one real root. Also, it is unique because the derivative is strictly positive so the function is stricly increasing.
3. Let α denote the unique real root. Then, $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ is a degree 3 extension and additionally $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Hence, the other two roots of f, say β and γ, cannot be contained in $\mathbb{Q}(\alpha)$. So, every element $g \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ can send α only to α. However, as α generated $\mathbb{Q}(\alpha)$ this means that $g = \mathrm{id}$.
4. Let α, β and γ be as in the previous point. Then both β and γ are roots of $h = \frac{f}{x-\alpha} \in \mathbb{Q}(\alpha)[x]$. As this polynomial has degree 2, and β and γ are not in $\mathbb{Q}[x]$, $h = m_{\beta,\mathbb{Q}(\alpha)} = m_{\gamma,\mathbb{Q}(\alpha)}$. So, $\mathbb{Q}(\alpha, \beta, \gamma)$ has degree 2 over $\mathbb{Q}(\alpha)$. So, by the multiplicativity of the degrees of field extensions, $L = \mathbb{Q}(\alpha, \beta, \gamma)$ has degree 6 over $\mathbb{Q}$. Let G be the Galois group of L over $\mathbb{Q}$. Then, G acts faithfully on α, β and γ, which yields an embedding $G \hookrightarrow S_3$. As both have 6 elements, this is in fact an isomorphism.

Exercice 2.
Décrivez le groupe $\mathrm{Gal}(K/\mathbb{Q})$ dans les cas suivants: $K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{7}), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\xi)$ où $\xi = e^{2i\pi/3}$.

Solution.

Pour toutes les extensions sauf $\mathbb{Q}(\sqrt[3]{2})$, on est dans un cas de forme $\mathbb{Q}(\alpha)$ avec le polynôme minimal de α de degré 2. Notons α' l'autre racine et $m(t) \in \mathbb{Q}[t]$ le polynôme minimal. On voit que $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$ en utilisant la formule du discriminant. Dès lors
$$\mathbb{Q}(\alpha) \xleftarrow{\mathrm{ev}_\alpha} \mathbb{Q}[t]/(m(t)) \xrightarrow{\mathrm{ev}_{\alpha'}} \mathbb{Q}(\alpha')$$

est un automorpshime non trivial, comme il envoie $\alpha \mapsto \alpha'$. Par le dernier point de la Proposition 4.6.5 on déduit que $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ est cyclique d'ordre 2.

En plongeant $\mathbb{Q}(\sqrt[3]{2})$ dans le corps de décomposition de x^3-2 on voit qu'un automorphisme doit envoyer $\sqrt[3]{2}$ sur une autre racine de x^3-2. Mais comme la seule racine de x^3-2 contenue dans $\mathbb{Q}(\sqrt[3]{2})$ est $\sqrt[3]{2}$ on conclut que $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ est réduit à l'identité.

Exercice 3.
Soit $\xi = e^{\frac{2\pi i}{3}}$. Considérons

$$\mathbb{Q}(\xi, \sqrt[3]{2}) \subseteq \mathbb{C},$$

un corps de décomposition de x^3-2.

On attire l'attention sur le point (3) de la Proposition 4.6.5. Que le groupe $\mathrm{Gal}(L/K)$ *agit transitivement sur les racines d'un polynôme minimal est un théorème* d'existence. *En effet étant donné des racines* α_1, α_2 *d'un polynôme minimal, la transitivité signifie qu'il existe* $\phi \in \mathrm{Gal}(L/K)$ *tel que* $\phi(\alpha_1) = \alpha_2$.

1. Montrez qu'il existe $\phi \in \mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q})$ tel que $\phi(\xi) = \xi$ et $\phi(\sqrt[3]{2}) = \xi\sqrt[3]{2}$. Quel est l'ordre de ϕ ?

2. Montrez qu'il existe $\psi \in \mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q})$ avec $\psi(\xi\sqrt[3]{2}) = \xi^2\sqrt[3]{2}$ et $\psi(\sqrt[3]{2}) = \sqrt[3]{2}$. Quel est l'ordre de ψ ?

3. En utilisant l'action de $\mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})$ sur les racines de x^3-2 et la Proposition 4.6.5 du cours, déduisez que $\mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2}) \cong S_3$.

4. Raisonnez similairement pour calculer les groupes de Galois des extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

Solution.

1. On considère l'extension

   $$\mathbb{Q}(\xi) \subset \mathbb{Q}(\xi, \sqrt[3]{2}).$$

   Comme $\mathbb{Q}(\xi, \sqrt[3]{2})$ est le corps de décomposition de $x^3-2 \in \mathbb{Q}(\xi)[x]$, on peut appliquer le point (3) de la Proposition 4.6.4 pour avoir l'existence d'un $\phi \in \mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q}(xi))$ tel que $\phi(\sqrt[3]{2}) = \xi\sqrt[3]{2}$.

   Explicitement, on peut construire cet automorphisme de la manière suivante.

   On étend l'identité sur $\mathbb{Q}(\xi)$ en utilisant les évaluations

   $$\mathbb{Q}(\xi, \sqrt[3]{2}) \xleftarrow{\mathrm{ev}_{\sqrt[3]{2}}} \mathbb{Q}(\xi)[t]/(t^3-2)) \xrightarrow{\mathrm{ev}_{\xi\sqrt[3]{2}}} \mathbb{Q}(\xi, \sqrt[3]{2})$$

   le polynôme t^3-2 étant irréductible dans $\mathbb{Q}(\xi)$ car il n'a pas de racines. En effet toute racine de ce polynôme est de degré 3 sur $\mathbb{Q}$ et ne peut donc être contenue dans $\mathbb{Q}(\xi)$ qui est une extension de degré 2.

2. Comme $\mathbb{Q}(\xi, \sqrt[3]{2})$ est le corps de décomposition de $x^2+x+1 \in \mathbb{Q}(\sqrt[3]{2})[x]$, on peut appliquer le point (3) de la Proposition 4.6.4 pour avoir l'existence d'un $\psi \in \mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2}))$ tel que $\psi(\xi) = \xi^2$ et $\psi(\xi\sqrt[3]{2}) = \xi^2\sqrt[3]{2}$.

   Solution commune aux points 1. et 2. On sait comme $\mathbb{Q}(\xi, \sqrt[3]{2})$ est un corps de décomposition d'un polynôme séparable, qu'elle est Galoisienne et donc que

   $$|\mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q})| = 6.$$

   Aussi, on sait que si $\phi \in \mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})$ alors forcément

   $$\phi(\xi) = \xi, \xi^2 \quad \phi(\sqrt[3]{2}) = \sqrt[3]{2}, \xi\sqrt[3]{2}, \xi^2\sqrt[3]{2}.$$

   Comme on dénombre 6 possibilités d'automorphismes, elles sont forcément toutes réalisées. Cela démontre les points 1. et 2. simultanément.

3. Par le point (2) de la Proposition mentionnée on a un morphisme injectif $\mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})/\mathbb{Q}) \to S_3$. Mais par le quatrième point, on sait que $\mathrm{Gal}(\mathbb{Q}(\xi, \sqrt[3]{2})$ a $[\mathbb{Q}(\xi, \sqrt[3]{2})\colon \mathbb{Q}] = 6$ éléments ce qui conclut.

4. Commençons par remarquer que les éléments de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$ doivent envoyer $\sqrt{i} \mapsto \pm\sqrt{i}$ pour $i = 2, 3, 5$. En effet par le point 1 de la Proposition 4.6.4 les racines de (t^2-2) et (t^2-3) et (t^2-5) sont respectivement permutées. Ainsi, on voit qu'on au plus 4 (respectivement 8) automorphismes entièrement déterminés par $\sqrt{2} \mapsto \pm\sqrt{2}$ et $\sqrt{3} \mapsto \pm\sqrt{3}$ et $(\sqrt{5} \mapsto \pm\sqrt{5})$.

   Mais par le quatrième point de la Proposition 4.6.4, on sait que la taille des groupes de Galois sont égaux au degré de ces extensions. En effet les extensions considérées sont respectivement les corps de décomposition des polynômes séparables

$$(t^2-2)(t^2-3) \quad \text{et} \quad (t^2-2)(t^2-3)(t^2-5).$$

   Dès lors on sait que $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ a 4 éléments et que $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$ a 8 éléments. En effet on peut calculer le degré de ces extensions en utilisant les extensions successives de degré 2

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}).$$

   Ainsi, on conclut que les 4 (respectivement 8) automorphismes sont donc entièrement déterminés par $\sqrt{2} \mapsto \pm\sqrt{2}$ et $\sqrt{3} \mapsto \pm\sqrt{3}$ et $(\sqrt{5} \mapsto \pm\sqrt{5})$. Notons τ_i pour l'automorphisme qui envoie $\sqrt{i} \mapsto -\sqrt{i}$ et fixe $\sqrt{j}$ si $j \neq i$ pour $i, j = 2, 3, 5$. Ces automorphismes génèrent les groupes de Galois considérés et commutent deux à deux. Ainsi on voit que ces groupes de Galois sont abéliens. Notons C_2 pour un groupe d'ordre 2; on conclut maintenant que les morphismes

$$C_2 \oplus C_2 \to \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \quad \text{et} \quad C_2 \oplus C_2 \oplus C_2 \to \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$$

   définis en utilisant la propriété universelle de la somme directe de groupe abéliens en envoyant les générateurs des copies de C_2 sur les τ_i sont des isomorphismes.

Exercice 4.
Soit K un corps et L un corps de décomposition généré par des éléments séparables. En utilisant la Proposition 4.6.5 du cours montrez que si $\alpha \in L$ alors si l'orbite de α par l'action $\mathrm{Gal}(L/K)$ est de taille $[L : K]$ on a $L = K(\alpha)$.

Calculez des éléments primitifs pour chacune des extensions apparaissant dans l'exercice 3 en utilisant ce principe.

Solution.

Montrons l'affirmation. Premièrement, si on suppose que l'orbite de α est de taille $[L\colon K]$ alors tous les éléments de l'orbite sont de racines de $m_\alpha(t)$ par le premier point de la Proposition 4.6.4. Ainsi le degré de $m_\alpha(t)$ est au moins $[L\colon K]$. Mais comme il est également au plus $[L\colon K]$, on conclut qu'il est de degré $[L\colon K]$. On conclut alors $K(\alpha) = L$ par égalité des degrés.

Maintenant on en déduit que

$$\xi + \sqrt[3]{2} \quad \text{et} \quad \sqrt{2} + \sqrt{3} \quad \text{et} \quad \sqrt{2} + \sqrt{3} + \sqrt{6}$$

sont des éléments primitifs des extensions de l'exercice 3.

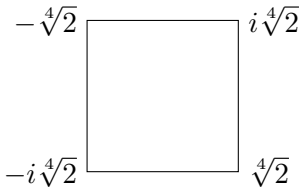
Exercice 5. 1. Montrez que $K = \mathbb{Q}(i, \sqrt[4]{2})$ est le corps de décomposition de $x^4 - 2 \in \mathbb{Q}[x]$.

2. Montrez qu'il existe $r, s \in \mathrm{Gal}(K/\mathbb{Q})$ tel que

   (a) $r(\sqrt[4]{2}) = i\sqrt[4]{2}$ et $r(i) = i$,

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

3. Déduire que si l'on nomme les sommets d'un carré selon les racines de x^4-2 comme ci-dessous



le groupe $\mathrm{Gal}(K,\mathbb{Q})$ est isomorphe au groupe D_8 des symétries du carré.

4. Donner un élément $\alpha \in K$ avec $\mathbb{Q}(\alpha) = K$.

Solution.

1. Les racines de x^4-2 sont $\pm\sqrt[4]{2}$ et $\pm i\sqrt[4]{2}$, et l'extension de $\mathbb{Q}$ générée par ces éléments est bel et bien K.

2. Montrons d'abord que $[K:\mathbb{Q}] = 8$. Comme x^4-2 est irréductible sur $\mathbb{Z}[x]$ par Eisenstein et primitif, il est aussi irréductible sur $\mathbb{Q}[x]$ par les lemmes de Gauss. Ainsi, $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}] = 4$. Comme $i \notin \mathbb{Q}(\sqrt[4]{2})$, on en déduit que le polynôme minimal de i sur $\mathbb{Q}(\sqrt[4]{2})$ est x^2+1, et donc $[\mathbb{Q}(i,\sqrt[4]{2}):\mathbb{Q}(\sqrt[4]{2})] = 2$. On en déduit donc que $[\mathbb{Q}(i,\sqrt[4]{2}):\mathbb{Q}] = 8$ par multiplicativité des degrés.

   Vu que $8 = [K:\mathbb{Q}] = [K:\mathbb{Q}(i)][\mathbb{Q}(i):\mathbb{Q}]$, on en déduit que $[K:\mathbb{Q}(i)] = 4$. Ainsi, x^4-2 est nécessairement le polynôme minimal de $\sqrt[4]{2}$ sur $\mathbb{Q}(i)$ (sinon cette extension serait de degré < 4). Par la proposition 4.6.5.(3), le groupe de Galois de $K/\mathbb{Q}(i)$ agit transitivement sur les racines de x^4-2, donc on obtient l'existence de r comme dans (a).

   Montrons maintenant l'existence de s. Notez que $r^2(\sqrt[4]{2}) = -\sqrt[4]{2}$ et $r^2(i) = i$. Ainsi, si l'on considère s comme la composée de r^2 et de la conjugaison complexe habituelle, alors $s(\sqrt[4]{2}) = -\sqrt[4]{2}$ et $s(i) = -i$.

3. Par le point précédent, cette extension est un corps de décomposition. Vu qu'elle est séparable ($\mathbb{Q}$ est parfait, car de caractéristique zéro), on en déduit par la Proposition 4.6.5 que $|\mathrm{Gal}(K/\mathbb{Q})| = 8$. Montrons que $\langle r,s\rangle = \mathrm{Gal}(K/\mathbb{Q})$. Vu que r est d'ordre 4 et que s n'est pas une puissance de r (tout ceci de vérifie à la main), on obtient que $\langle r,s\rangle$ contient au moins 5 éléments. Comme son ordre doit diviser 8, on en déduit que

$$\langle r,s\rangle = \mathrm{Gal}(K/\mathbb{Q}).$$

   Nous allons conclure de deux manières différentes:

   (a) Par la géométrie: notez que r et s agissent par isométries sur le carré de la donnée (r est une rotation d'un quart de tour dans le sens anti-horaire, et s est la symmétrie d'axe d'en bas à gauche vers en haut à droite). Cette action est nécessairement fidèle, car ces quatre sommets génèrent K sur $\mathbb{Q}$.

   Ainsi, $\langle r,s\rangle$ agit fidèlement par isométries sur ce carré. Comme le groupe d'isométries du carré est D_8 (donc d'ordre 8), on a une injection $\langle r,s\rangle \hookrightarrow D_8$ est un isomorphisme. Comme $\mathrm{Gal}(K/\mathbb{Q}) = \langle r,s\rangle$ est d'ordre 8, on conclut que $\mathrm{Gal}(K/\mathbb{Q}) \cong D_8$.

   (b) Par la théorie des groupes: on calcule à la main que $r^4 = id, s^2 = id$ et $(rs)^2 = id$. Comme D_8 a comme présentation $\langle \sigma,\tau | \sigma^4 = 1\ \tau^2 = 1\ (\sigma\tau)^2 = 1\rangle$, on obtient par définition l'existence d'un morphisme surjectif $D_8 \to \langle r,s,\rangle = \mathrm{Gal}(K/\mathbb{Q})$ envoyant σ sur r et τ sur s. Comme ces deux groupes sont d'ordre 8, on conclut que notre morphisme est un isomorphisme.

4. Comme on l'a vu au point précédent, on a que $\mathrm{Gal}(K/\mathbb{Q}) = \langle r, s\rangle = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$. Prenons $\alpha = \sqrt[4]{2}+i$. Vu qu'une $\mathbb{Q}$-base de K est donnée par $\{1, i, \sqrt[4]{2}, \sqrt{2}, (\sqrt[4]{2})^3, i\sqrt[4]{2}, i\sqrt{2}, i(\sqrt[4]{2})^3\}$, un calcul direct montre que cet élément n'est fixé par aucun $g \neq id$ de $\mathrm{Gal}(K/\mathbb{Q})$, donc c'est bien un élément primitif.