Théorie de Galois - Interro 1

Vous pouvez traiter les exercices dans l'ordre qui vous convient. Prenez soin de bien justifier vos réponses et de bien présenter votre démarche; la qualité de la rédaction sera prise en compte dans la notation. Les calculatrices sont interdites. Le barème est donné à titre indicatif seulement. Des réponses partielles peuvent vous accorder une partie des points de la question en question. N'oubliez pas de numéroter vos pages.

1 Autour des extensions abéliennes (4 points)

Soit $f \in \mathbb{Q}[X]$ irréductible avec des racines réelles et non réelles dans $\mathbb{C}$. Soit $\mathbb{K}$ son corps de décomposition.

1. (2 points) Soit $\mathbb{M}/\mathbb{Q}$ une extension galoisienne finie. Si $\mathrm{Gal}(\mathbb{M}/\mathbb{Q})$ est abélien, montrer que tous les corps intermédiaires $\mathbb{L}$ sont tels que $\mathbb{L}/\mathbb{Q}$ est galoisienne. Montrer de plus que $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ est abélien.

   Solution: Par la correspondance galoisienne, pour le premier point, il s'agit en fait de montrer que tous les sous-groupes de $\mathrm{Gal}(\mathbb{M}/\mathbb{Q})$ sont normaux et c'est bien le cas car $\mathrm{Gal}(\mathbb{M}/\mathbb{Q})$ est abélien.

   Pour le second point, il suffit de remarquer que l'on a, par théorème

   $$\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{M}/\mathbb{Q})/\mathrm{Gal}(\mathbb{M}/\mathbb{L})$$

   de sorte que $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ est abélien comme quotient d'un groupe abélien.

2. (1 point) En déduire que $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ n'est pas abélien.

   Solution: Par la question précédente, il suffit de trouver un corps intermédiaire qui ne soit pas une extension galoisenne de $\mathbb{Q}$. Soit x une racine réelle de f. Le corps intermédiaire $\mathbb{Q}(x)$ convient: si $\mathbb{Q}(x)/\mathbb{Q}$ était galoisienne, alors tous les $\mathbb{Q}$-conjugués de x appartiendrait à $\mathbb{Q}(x)$, si bien qu'ils seraient réels.

3. (1 point) Le résultat tient-il toujours si l'on oublie l'hypothèse d'irréductibilité sur f ?

   Solution: Le polynôme $f = (X^2+1)(X-3)$ fournit un contre-exemple.

2 Vrai ou faux (4 points)

Répondre aux questions suivantes par vrai ou faux en justifisant ses réponses. On prendra garde au fait qu'il ne s'agit pas nécessairement de questions de cours trivialement évidentes.

1. (1 point) Soit $\mathbb{K}$ le corps de décomposition de $X^2 - 3 \in \mathbb{Q}[X]$. On a $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$.

   Solution: Faux car on a $|\mathrm{Gal}(\mathbb{K}/\mathbb{Q})| = [\mathbb{K} : \mathbb{Q}] = 2$ puisque $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ est une extension galoisienne finie de $\mathbb{Q}$: le corps $\mathbb{K}$ est un corps de décomposition donc $\mathbb{K}/\mathbb{Q}$ est normale et cette extension est séparable car $\mathbb{Q}$ est de caractéristique nulle.

2. (2 points) Soit $\mathbb{L}/\mathbb{K}$ une extension finie. Soit $x \in \mathbb{L}$. On suppose que l'on a

   $$\forall\ \sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{K}), \quad \sigma(x) = x.$$

   On a alors $x \in \mathbb{K}$.

   Solution: Faux, l'énoncé est dans le cours sous réserve que $\mathbb{L}/\mathbb{K}$ est galoisienne (il s'agit donc de trouver une extension non galoisienne pour trouver un contre-exemple). On sait que l'extension $\mathbb{Q}(7^{1/3})/\mathbb{Q}$ n'est pas galoisienne et on a $\left|\mathrm{Aut}(\mathbb{Q}(7^{1/3})/\mathbb{Q})\right| = 1$ car, par théorème, les automorphismes de $\mathbb{Q}(7^{1/3})/\mathbb{Q}$ sont en correspondance avec les $\mathbb{Q}$-conjugués de $7^{1/3}$ qui appartiennent à $\mathbb{Q}(7^{1/3})$, or le corps $\mathbb{Q}(7^{1/3})$ est réel et on sait que les $\mathbb{Q}$-conjugués de $7^{1/3}$ sont $7^{1/3}, j7^{1/3}, j^2 7^{1/3}$ (les deux derniers ne sont pas réels). Ainsi, on a bien l'hypothèse de l'énoncé vérifiée pour $x = 7^{1/3}$ et on a $x \notin \mathbb{Q}$.

3. (1 point) Soient $r \geqslant 1$, $x_1, \cdots, x_r \in \mathbb{C}$ des nombres algébriques sur $\mathbb{Q}$. Soit Ω l'ensemble des nombres algébriques sur $\mathbb{Q}$ appartenant à $\mathbb{C}$. Pour tout $i \in [\![1, r]\!]$, soit y_i un $\mathbb{Q}$-conjugué de x_i. Notons $\mathbb{K}$ le corps engendré par les x_i. Il existe un morphisme de corps $\sigma : \mathbb{K} \to \Omega$ vérifiant $\sigma(x_i) = y_i$ pour tout i.

   Solution: Posons $r = 2, x_1 = \sqrt{2}, x_2 = -\sqrt{2}$. Notons que x_1 et x_2 sont $\mathbb{Q}$-conjugués. Il n'existe pas de morphisme σ vérifiant $\sigma(x_1) = x_1$ et $\sigma(x_2) = x_1$.

3 Pensez indépendance (6.5 points)

1. Soient $\mathbb{L}_1/\mathbb{K}$ une extension galoisienne finie et soit $\mathbb{L}_2/\mathbb{K}$ une extension du même corps $\mathbb{K}$.

   (a) (1 point) Enoncer (sans prouver) les deux propriétés équivalentes définissant " $\mathbb{L}_1/\mathbb{K}$ et $\mathbb{L}_2/\mathbb{K}$ sont indépendantes" et vues en TD.

   (b) (1 point) On suppose que $[\mathbb{L}_1 : \mathbb{K}]$ et $[\mathbb{L}_2 : \mathbb{K}]$ sont premiers entre eux. Justifier que $\mathbb{L}_1$ et $\mathbb{L}_2$ sont des extensions linéairement indépendantes de $\mathbb{K}$.

   Solution: On propose deux solutions.

   <u>Première solution</u>

   Par théorème, il s'agit de montrer que l'on a $[\mathbb{L}_1 : \mathbb{K}][\mathbb{L}_2 : \mathbb{K}] = [\mathbb{L}_1\mathbb{L}_2 : \mathbb{K}]$. On a $[\mathbb{L}_1 : \mathbb{K}] \mid [\mathbb{L}_1\mathbb{L}_2 : \mathbb{K}]$ et $[\mathbb{L}_2 : \mathbb{K}] \mid [\mathbb{L}_1\mathbb{L}_2 : \mathbb{K}]$. Par le lemme de Gauss, on a donc $[\mathbb{L}_1 : \mathbb{K}][\mathbb{L}_2 : \mathbb{K}] \mid [\mathbb{L}_1\mathbb{L}_2 : \mathbb{K}]$. Or, on a $[\mathbb{L}_1\mathbb{L}_2 : \mathbb{K}] \leq [\mathbb{L}_1 : \mathbb{K}][\mathbb{L}_2 : \mathbb{K}]$, d'où l'égalité voulue.

Seconde solution

Il suffit de montrer que l'on a $\mathbb{L}_1 \cap \mathbb{L}_2 = \mathbb{K}$. Soit $x \in \mathbb{L}_1 \cap \mathbb{L}_2$. On a $[\mathbb{K}(x) : \mathbb{K}] \mid [\mathbb{L}_1 : \mathbb{K}]$ et $[\mathbb{K}(x) : \mathbb{K}] \mid [\mathbb{L}_1 = 2 : \mathbb{K}]$, d'où $[\mathbb{K}(x) : \mathbb{K}] = 1$ puis $x \in \mathbb{K}$.

2. Pour tout $n \in \mathbb{N}^*$, on note $\zeta_n = \exp(2i\pi/n)$ et $\mathbb{Q}_n = \mathbb{Q}(\zeta_n)$.

   (a) (2 points) Soient $m, n \in \mathbb{N}^*$ premiers entre eux. Justifier que l'on a

   $$\mathbb{Q}_{nm} = \mathbb{Q}_n \mathbb{Q}_m.$$

   On pourra justifier que l'on a $\langle \zeta_{nm} \rangle = \langle \zeta_n \rangle \langle \zeta_m \rangle$.

   Solution: Montrons d'abord l'indication.

   Première solution Par le théorème de Bézout, il existe u, v tels que $nu + mv = 1$. Ainsi, on a

   $$\zeta_{nm} = e^{\frac{2i\pi(nu+mv)}{nm}} = \zeta_m^u \zeta_n^v \in \langle \zeta_n \rangle \langle \zeta_m \rangle$$

   et on conclut à l'égalité des groupes par double inclusion.

   Seconde solution Le groupe produit $\langle \zeta_n \rangle \langle \zeta_m \rangle$ est d'ordre nm car le premier facteur est d'ordre n, le second d'ordre m et on a

   $$\langle \zeta_n \rangle \cap \langle \zeta_m \rangle = \{1\}$$

   car si x appartient à cette intersection, alors, par corollaire du théorème de Lagrange, l'élément x est d'ordre divisant n et m, d'où x d'ordre 1, c'est-à-dire $x = 1$.

   Ceci conclut la preuve de l'indication.

   On a trivialement $\mathbb{Q}_n \mathbb{Q}_m \subset \mathbb{Q}_{nm}$ et le sens réciproque découle du fait que l'on a $\zeta_{nm} \in \mathbb{Q}_n \mathbb{Q}_m$ par l'indication.

   (b) (1 point) Soient $m, n \in \mathbb{N}^*$ premiers entre eux. Montrer que l'on a $\mathbb{Q}_n \cap \mathbb{Q}_m = \mathbb{Q}$ (on pourra se servir la question précédente).

   Solution: Il s'agit de montrer que $\mathbb{Q}_n$ et $\mathbb{Q}_m$ sont indépendantes (puisqu'elles sont galoisiennes sur $\mathbb{Q}$) et ce que nous montrons maintenant. Par ce qui précède, on a

   $$[\mathbb{Q}_n \mathbb{Q}_m : \mathbb{Q}] = [\mathbb{Q}_{nm} : \mathbb{Q}] = \varphi(nm)$$

   et on a également

   $$[\mathbb{Q}_n : \mathbb{Q}][\mathbb{Q}_m : \mathbb{Q}] = \varphi(n)\varphi(m).$$

   De plus, les propriétés de fonction φ nous donnent $\varphi(nm) = \varphi(n)\varphi(m)$ (car $n \wedge m = 1$) et on conclut par théorème à ce que l'on a annoncé.

   (c) (1.5 points) Notons $n = \prod_{i=1}^{r} p_i^{e_i} = \prod_{i=1}^{r} q_i$ la décomposition en facteurs premiers de n. En déduire que le morphisme suivant est un isomorphisme (on admet que c'est bien un mor-

phisme)

$$\Phi : \left| \begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) & \longrightarrow & \prod_{i=1}^{r} \mathrm{Gal}(\mathbb{Q}_{q_i}/\mathbb{Q}) \\ \sigma & \longmapsto & (\sigma_{|\mathbb{Q}_{q_i}})_{i=1}^{r} \end{array} \right. .$$

Solution: On montre que ce morphisme est injectif et on conclura par cardinalité.

Soit $\sigma \in \mathrm{Ker}(\Phi)$. On a donc $\sigma_{|\mathbb{Q}_{q_i}} = \mathrm{id}_{\mathbb{Q}_{q_i}}$ pour tout i. Or, par ce qui précède, on a $\mathbb{Q}_n = \mathbb{Q}_{q_1} \cdots \mathbb{Q}_{q_r}$, d'où $\sigma = \mathrm{id}$. En effet, on a d'abord $\mathbb{Q}_n = \mathbb{Q}_{q_1}\mathbb{Q}_{n/q_1}$ par la question 2-a et en itérant on obtient ce que l'on a annoncé.

Ainsi, le morphisme Φ est injectif et puisque l'on a

$$\begin{aligned} |\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] &= \varphi(n) \\ &= \prod_{i=1}^{r} \varphi(q_i) \text{ car les } q_i \text{ sont premiers entre eux} \\ &= \prod_{i=1}^{r} [\mathbb{Q}(\zeta_{q_i}) : \mathbb{Q}] = \prod_{i=1}^{r} |\mathrm{Gal}(\mathbb{Q}(\zeta_{q_i})/\mathbb{Q})| \end{aligned}$$

on conclut par cardinalité que Φ est un isomorphisme.

4 Extensions multiquadratiques (8 points)

Soit $\mathbb{K}$ un corps de caractéristique différente de 2, soit $\mathbb{L}/\mathbb{K}$ une extension et soit $u_1, \ldots, u_r \in \mathbb{K}^*$ ayant des racines carrées $\sqrt{u_1}, \ldots, \sqrt{u_r} \in \mathbb{L}$. On note $\mathbb{K}^{*^2} = \{x^2 : x \in \mathbb{K}^*\}$.

1. (2 points) Montrer que l'extension $\mathbb{K}[\sqrt{u_1}, \ldots, \sqrt{u_r}]/\mathbb{K}$ est galoisienne finie.
2. (2 points) Montrer que l'on a

$$[\mathbb{K}[\sqrt{u_1}, \ldots, \sqrt{u_r}] : \mathbb{K}] = 2^r \Longrightarrow \left(\forall (\alpha_i)_i \in \mathbb{Z}^r, \quad \prod_{i=1}^{r} u_i^{\alpha_i} \in \mathbb{K}^{*^2} \implies \forall i \in [\![1, r]\!], 2 \mid \alpha_i \right).$$

On pourra raisonner par contraposée.

Solution: On suit l'indication. Supposons qu'il existe $\alpha_1, \ldots, \alpha_r \in \mathbb{Z}$ non tous pairs et tels que l'on a

$$\prod_{i=1}^{r} u_i^{\alpha_i} \in \mathbb{K}^{*^2}.$$

Quitte à réordonner les u_i, supposons que α_r est impair. On a alors

$$u_r = \prod_{i=1}^{r} u_i^{\alpha_i} \prod_{i=1}^{r-1} u_i^{-\alpha_i} u_r^{-\alpha_r+1}$$

d'où l'on tire

$$\sqrt{u_r} = \pm \sqrt{\prod_{i=1}^{r} u_i^{\alpha_i}} \prod_{i=1}^{r-1} \sqrt{u_i}^{-\alpha_i} u_r^{(-\alpha_r+1)/2} \in \mathbb{K}(\sqrt{u_1}, \ldots, \sqrt{u_{r-1}})$$

car $-\alpha_r + 1$ est pair, que l'on a $u_r \in \mathbb{K}$ et que le premier facteur est dans $\mathbb{K}$ car on a supposé

$$\prod_{i=1}^{r} u_i^{\alpha_i} \in \mathbb{K}^{*^2}.$$

Il s'en suit que l'on a, par le théorme de la base téléscopique

$$\begin{aligned}
[\mathbb{K}[\sqrt{u_1}, \dots, \sqrt{u_r}] : \mathbb{K}] &= [\mathbb{K}[\sqrt{u_1}, \dots, \sqrt{u_{r-1}}] : \mathbb{K}] \\
&= [\mathbb{K}(\sqrt{u_1}) : \mathbb{K}][\mathbb{K}(\sqrt{u_1})(\sqrt{u_2}, \dots, \sqrt{u_{r-1}}) : \mathbb{K}(\sqrt{u_1})] \\
&= 2[\mathbb{K}(\sqrt{u_1})(\sqrt{u_2}) : \mathbb{K}(\sqrt{u_1})][\mathbb{K}(\sqrt{u_1}, \sqrt{u_2})(\dots) : \mathbb{K}(\sqrt{u_1}, \sqrt{u_2})] \\
&= \dots \\
&= \leqslant 2^{r-1}.
\end{aligned}$$

car pour toute extension $\mathbb{L}/\mathbb{K}$, on a $\sqrt{u_i}$ de degré au plus $\deg_{\mathbb{K}}(\sqrt{u_i}) = 2$ sur $\mathbb{L}$.

3. Dans les deux questions suivantes - qui sont indépendantes - on pourra admettre que l'on a pour tout r' et tout $u_i' \in \mathbb{K}^*$

$$\left(\forall (\alpha_i)_i \in \mathbb{Z}^{r'}, \quad \prod_{i=1}^{r'} (u_i')^{\alpha_i} \in \mathbb{K}^{*^2} \implies \forall i \in [\![1, r']\!], 2 \mid \alpha_i \right) \implies [\mathbb{K}[\sqrt{u_1'}, \dots, \sqrt{u_r'}] : \mathbb{K}] = 2^{r'}.$$

   (a) (2 points) En supposant que l'on a $[\mathbb{K}[\sqrt{u_1}, \dots, \sqrt{u_r}] : \mathbb{K}] = 2^r$, montrer que l'on a

$$\mathrm{Gal}(\mathbb{K}[\sqrt{u_1}, \dots, \sqrt{u_r}]/\mathbb{K}) \simeq (\mathbb{Z}/2\mathbb{Z})^r$$

   On pourra utiliser une des différentes méthodes vues en TD ou montrer que les extensions $\mathbb{K}[\sqrt{u_r}]$ et $\mathbb{K}[\sqrt{u_1}, \dots, \sqrt{u_{r-1}}]$ sont indépendantes.

   Solution: Première solution

   On pose

$$\Phi : \left| \begin{array}{ccc} \mathrm{Gal}(\mathbb{K}[\sqrt{u_1}, \dots, \sqrt{u_r}]/\mathbb{K}) & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^r \\ \sigma & \longmapsto & (\beta_i)_{i=1}^r \end{array} \right.$$

   où β_i est défini par

$$\beta_i = \begin{cases} 0 & \text{si } \sigma(\sqrt{u_i}) = \sqrt{u_i} \\ 1 & \text{si } \sigma(\sqrt{u_i}) = -\sqrt{u_i}. \end{cases}$$

   Premièrement, l'application Φ est bien définie car on a $\sigma(\sqrt{u_i}) \in \{\pm\sqrt{u_i}\}$ puisque $X^2 - u_i$ est à coefficients dans $\mathbb{K}$ et annule $\sqrt{u_i}$. On vérifie que c'est un morphisme injectif comme on l'a déjà fait en TD et on conclut par cardinalité.

   Seconde solution

   On suit la première indication.

   On a par hypothèse $[\mathbb{K}(\sqrt{u_r})\mathbb{K}(\sqrt{u_1}, \dots, \sqrt{u_{r-1}}) : \mathbb{K}] = 2^r$. De plus, on a

$$[\mathbb{K}(\sqrt{u_1}, \dots, \sqrt{u_{r-1}}) : \mathbb{K}] = 2^{r-1}$$

par le résultat admis appliqué à $u_1, \ldots, u_{r-1}$ (ce résultat s'applique par la question 2 appliquée à $u_1, \ldots, u_r$).

Ainsi on a

$$[\mathbb{K}(\sqrt{u_r})\mathbb{K}(\sqrt{u_1}, \ldots, \sqrt{u_{r-1}}) : \mathbb{K}] = [\mathbb{K}(\sqrt{u_1}) : \mathbb{K}][\mathbb{K}(\sqrt{u_1}, \ldots, \sqrt{u_{r-1}}) : \mathbb{K}]$$

ce qui prouve bien que $\mathbb{K}(\sqrt{u_r})/\mathbb{K}$ et $\mathbb{K}(\sqrt{u_1}, \ldots, \sqrt{u_{r-1}})/\mathbb{K}$ sont indépendantes (car elles sont galoisiennes). Par théorème, on a donc

$$\mathrm{Gal}(\mathbb{K}(\sqrt{u_1}, \ldots, \sqrt{u_r})) \simeq \mathrm{Gal}(\mathbb{K}(\sqrt{u_r})/\mathbb{K}) \times \mathrm{Gal}(\mathbb{K}(\sqrt{u_1}, \ldots, \sqrt{u_{r-1}})/\mathbb{K})$$

le premier facteur est $\mathbb{Z}/2\mathbb{Z}$ et on traite le second en itérant.

(b) (1 point) Soient $p_1, \cdots, p_r$ des nombres premiers deux à deux distincts. On pose $u_i = \sqrt{p_i}$. Calculer $[\mathbb{Q}[\sqrt{u_1}, \ldots, \sqrt{u_r}] : \mathbb{Q}]$.

Solution: On montre que c'est 2^r en se servant de la réciproque de la question 2.

Soient $\alpha_1, \alpha_r \in \mathbb{Z}$ tels que

$$\prod_{i=1}^{r} p_i^{\alpha_i} \in \mathbb{Q}^{*^2}.$$

Il existe donc $a, b \in \mathbb{Z}$ tels que

$$\prod_{i=1}^{r} p_i^{\alpha_i} = \frac{a^2}{b^2}$$

d'où l'on tire $b^2 \prod_{i\in I}^{r} p_i^{\alpha_i} = a^2 \prod_{i\notin I}^{r} p_i^{\alpha_i}$ avec I l'ensemble des entiers i tels que $\alpha_i \geqslant 0$. En passant aux valuations, on a

$$v_{p_i}(p_i^{\alpha_i}) = \begin{cases} v_{p_i}(a^2) = 2v_{p_i}(a) & \text{si } i \in I \\ v_{p_i}(b^2) = 2v_{p_i}(b) & \text{sinon} \end{cases}$$

de sorte que $v_{p_i}(p_i^{\alpha_i}) = \alpha_i$ est pair.

4. (1 point) Montrer que l'on a

$$\left(\forall (\alpha_i)_i \in \mathbb{Z}^r, \quad \prod_{i=1}^{r} u_i^{\alpha_i} \in \mathbb{K}^{*^2} \implies \forall i \in [\![1, r]\!], 2 \mid \alpha_i\right) \implies [\mathbb{K}[\sqrt{u_1}, \ldots, \sqrt{u_r}] : \mathbb{K}] = 2^r.$$

On pourra s'intéresser à l'extension $\mathbb{K}(\sqrt{u_r})(\sqrt{u_1}, \ldots, \sqrt{u_{r-1}})/\mathbb{K}(\sqrt{u_r})$.

Solution: On montre par récurrence sur r que l'on a - pour toute extension $\mathbb{M}/\mathbb{L}$,(pour tout r,) tout $v_1, \ldots, v_r \in \mathbb{L}^*$ tels que $\sqrt{v_1}, \ldots, \sqrt{v_r} \in \mathbb{M}$ - l'implication suivante

$$\left(\forall (\alpha_i)_i \in \mathbb{Z}^r, \quad \prod_{i=1}^{r} v_i^{\alpha_i} \in \mathbb{L}^{*^2} \implies \forall i \in [\![1, r]\!], 2 \mid \alpha_i\right) \implies [\mathbb{L}[\sqrt{v_1}, \ldots, \sqrt{v_r}] : \mathbb{L}] = 2^r.$$

L'initialisation est facile.

Pour l'hérédité, on suppose le résultat acquis à $r-1$ et on le montre à r. Soient $\mathbb{M}/\mathbb{L}$ et $v_1, \ldots, v_r$ de tels objets. On suppose que l'on a

$$\forall (\alpha_i)_i \in \mathbb{Z}^r, \quad \prod_{i=1}^{r} v_i^{\alpha_i} \in \mathbb{L}^{*^2} \implies \forall i \in [\![1, r]\!], 2 \mid \alpha_i. \tag{1}$$

Par le théorème de la base téléscopique, on a

$$[\mathbb{L}[\sqrt{v_1}, \ldots, \sqrt{v_r}] : \mathbb{L}] = [\mathbb{L}(\sqrt{v_r})[\sqrt{v_1}, \ldots, \sqrt{v_{r-1}}] : \mathbb{L}(\sqrt{v_r})][\mathbb{L}[\sqrt{v_r}] : \mathbb{L}]$$

et on observe que le deuxième facteur vaut 2 sans quoi l'hypothèse faite (avec les α_i) tomberait à l'eau.

Montrons que le premier facteur vaut 2^{r-1} en faisant appel à l'hypothèse de récurrence pour l'extension $\mathbb{M}/\mathbb{L}(\sqrt{u_r})$ et les nombres $\sqrt{u_1}, \ldots, \sqrt{u_{r-1}}$. Pour pouvoir appliquer l'hypothèse de récurrence, on doit montrer que l'on a

$$\forall (\alpha_i)_i \in \mathbb{Z}^r, \quad \prod_{i=1}^{r-1} v_i^{\alpha_i} \in \mathbb{L}(\sqrt{v_r})^{*^2} \implies \forall i \in [\![1, r]\!], 2 \mid \alpha_i.$$

On se donne de tels α_i. On a alors $a, b \in \mathbb{L}$ tels que

$$\prod_{i=1}^{r-1} v_i^{\alpha_i} = (a + b\sqrt{v_r})^2 = a^2 + b^2 u_r + 2ab\sqrt{v_r}$$

de sorte que si $ab \neq 0$, alors on a $\sqrt{v_r} \in \mathbb{K}$ (ce qui est absurde d'après l'hypothèse (1)). Ainsi, il nous reste à distinguer les cas:

- si $b = 0$ alors il suffit de faire appel à l'hypothèse (1) pour conclure
- si $a = 0$ alors on a
$$\prod_{i=1}^{r-1} v_i^{\alpha_i} = b^2 v_r$$
c'est-à-dire
$$\prod_{i=1}^{r} v_i^{\alpha_i} = b^2$$
avec $\alpha_r = -1$ qui vient contredire l'hypothèse (1).

Bonus (1.5 puntos): Soit $\mathbb{K}$ le corps de décomposition de $X^4 - 12X^2 + 34 \in \mathbb{Q}[X]$. Est-il vrai que l'on a $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$?