(Exercice 3 fiche 4)

Partie B

$i \Rightarrow ii$: la famille $\sqrt{a_I}$, $I \subset \{1,...,n\}$,est génératrice et contient $2^n = [K : \mathbb{Q}]$ éléments, c'est donc une base.

$ii \Rightarrow iii$: solution : il y a au plus 2^n automorphismes de K. Ils sont tous de la forme $\widetilde{\phi}$ pour une certaine application $\phi : \{1,....,n\} \to \{-1,1\}$. Il y a exactement 2^n telles applications.

Or, $|\mathrm{Aut}_{\mathbb{Q}}(K)| = [K : \mathbb{Q}] = 2^n$. Donc tous les morphismes $\widetilde{\phi}$ existent.

$iii \Rightarrow iv$: Soit ϕ tel que $\phi(1) = ... = \phi(i) = 1$ et $\phi(i+1) = -1$. Alors $\widetilde{\phi}(\sqrt{a_{i+1}}) = -\sqrt{a_{i+1}}$ et $\widetilde{\phi}$ est l'identité sur $\mathbb{Q}[\sqrt{a_1},...,\sqrt{a_i}]$. Donc $\sqrt{a_{i+1}} \notin \mathbb{Q}[\sqrt{a_1},...,\sqrt{a_i}]$.

$iv \Rightarrow i$: $[K : \mathbb{Q}] = \prod_{i=1}^{n} [\mathbb{Q}(\sqrt{a_1},....,\sqrt{a_{i-1}})[\sqrt{a_i}] : \mathbb{Q}(\sqrt{a_1},....,\sqrt{a_{i-1}})] = 2^n$.

(Exercice 3 fiche 4 parties C,D)

Partie B.

1.

MONTRONS QUE $\mathbb{Q}(\sqrt{a_1},...,\sqrt{a_n}) = \sum_I \mathbb{Q}\sqrt{a_I}$.

Il suffit de montrer qu'un monôme $\sqrt{a_1}^{\alpha_1}....\sqrt{a_n}^{\alpha_n}$

où les $\alpha_i \in \mathbb{N}$ est une combinaison linéaire des $\sqrt{a_I}$.

C'est évident car si α_i est pair, $\sqrt{a_i}^{\alpha_i} \in \mathbb{Q}$ si a_i est impair c'est dans $\mathbb{Q}\sqrt{a_i}$.

Partie C.

D'après la partie B, les $a_I = \sqrt{\prod_{i \epsilon I} p_i}$, $I \subset \{1,...,j\}$, forment une base du $\mathbb{Q}-$espace vectoriel $K_j = \mathbb{Q}\left(\sqrt{p_1},...,\sqrt{p_j}\right)$.

Donc si $\sqrt{p_{j+1}} \epsilon K_j$, on peut trouver des rationnels t_I, $I \subset \{1,...,j\}$ tels que :

$\sqrt{p_{j+1}} = \sum_I t_I a_I$. Mais alors $\sigma\left(\sqrt{p_{j+1}}\right) = \sum_I t_I \sigma(a_I) = \pm \sqrt{p_{j+1}}$ pour tout automorphisme σde K_j.

Or, d'après la partie B, il existe σ_i automorphisme de K_j tel que $\sigma_i(\sqrt{p_k}) = \sqrt{p_k}$ si $k \notin I$, $-\sqrt{p_i}$ si $k = i$.

Alors $\sigma_i\left(\sqrt{p_{j+1}}\right) = \sum_{I:i\in I} -t_I a_I + \sum_{I:i\notin I} t_I a_I$.

Obtenir une contradiction s'il y a au moins deux coefficients t_I non nuls .

en effet si $I_1 \neq I_2$ sont tels que t_{I_1}et $t_{I_2} \neq 0$, alors on peut choisir un $i \epsilon I_1$ tel que $i \notin I_2$ (ou bien un $i \in I_2$ tel que $i \notin I_1$).

Alors $\sigma_i\left(\sqrt{p_{j+1}}\right) = ... - t_{I_1} a_{I_1 - ....} + ... + t_{I_2} a_{I_2} + ... \neq \pm \left(\sum_I t_I a_I\right)$ ...

D'où la contradiction. Donc $\sqrt{p_{j+1}} = q\sqrt{p_{k_1}....p_{k_i}}$ pour un certain $q \in \mathbb{Q}$ et un certain $I = \{k_{1,...,}k_i\} \subset \{1,....,j\}$.

Partie C.

D'après la partie B, les $a_I = \sqrt{\prod_{i \epsilon I} p_i}$, $I \subset \{1,...,j\}$, forment une base du $\mathbb{Q}-$espace vectoriel $K_j = \mathbb{Q}\left(\sqrt{p_1},...,\sqrt{p_j}\right)$.

Donc si $\sqrt{p_{j+1}} \epsilon K_j$, on peut trouver des rationnels t_I, $I \subset \{1,...,j\}$ tels que :

$\sqrt{p_{j+1}} = \sum_I t_I a_I$. Mais alors $\sigma\left(\sqrt{p_{j+1}}\right) = \sum_I t_I \sigma(a_I) = \pm \sqrt{p_{j+1}}$ pour tout automorphisme σde K_j.

Or, d'après la partie B, il existe σ_i automorphisme de K_j tel que $\sigma_i(\sqrt{p_k}) = \sqrt{p_k}$ si $k \notin I$, $-\sqrt{p_i}$ si $k = i$.

Alors $\sigma_i\left(\sqrt{p_{j+1}}\right) = \sum_{I:i\in I} -t_I a_I + \sum_{I:i\notin I} t_I a_I$.

Obtenir une contradiction s'il y a au moins deux coefficients t_I non nuls .

en effet si $I_1 \neq I_2$ sont tels que t_{I_1}et $t_{I_2} \neq 0$, alors on peut choisir un $i \epsilon I_1$ tel que $i \notin I_2$ (ou bien un $i \in I_2$ tel que $i \notin I_1$).

Alors $\sigma_i\big(\sqrt{p_{j+1}}\big) = ... - t_{I_1} a_{I_1 - ....} + ... + t_{I_2} a_{I_2} + ... \neq \pm \left(\sum_I t_I a_I\right)$ ...

D'où la contradiction. Donc $\sqrt{p_{j+1}} = q\sqrt{p_{k_1}....p_{k_i}}$ pour un certain $q \in \mathbb{Q}$ et un certain $I = \{k_{1,...,}k_i\} \subset \{1, ..., j\}$.

Mais ceci est absurde : on aurait $p_{j+1} = q^2 p_{k_1}....p_{k_i}$ impossible car les p_k sont 2à2 distincts

...

partie D.

Indication. Le nombre de plongements de $\mathbb{Q}(u)$ dans $\mathbb{C}$ $=[\mathbb{Q}(u): \mathbb{Q}]$.

Soient $\sigma, \sigma' \in \mathrm{Gal}(K/\mathbb{Q})$. Si $\sigma(u) = \sigma'(u)$, alors $\sigma(k_1\sqrt{p_1} + ... + k_n\sqrt{p_n}) = \sigma'(k_1\sqrt{p_1} + ... + k_n\sqrt{p_n})$
$\Leftrightarrow k_1\sigma(\sqrt{p_1}) + ... k_n\sigma(\sqrt{p_n}) = k_1\sigma'(\sqrt{p_1}) + ... k_n\sigma'(\sqrt{p_n})$.

Or $\sigma\Big(\sqrt{p}_i\Big) = \pm\sqrt{p_i} = \pm\sigma'(\sqrt{p_i})$. Comme les $\sqrt{p_i}$ sont $\mathbb{Q}-$linéairement indépendants, si les k_i sont non nuls, alors $\sigma(\sqrt{p_i}) = \sigma'(\sqrt{p_i})$pour tout i et $\sigma = \sigma'$.

Donc $[\mathbb{Q}(u): \mathbb{Q}] \geqslant |\mathrm{Gal}(K/\mathbb{Q})| = [K: \mathbb{Q}] => [\mathbb{Q}(u): \mathbb{Q}] = [K: \mathbb{Q}] \Rightarrow \mathbb{Q}(u) = K$.

Pour le 2. raisonner
par récurrence sur n.

On peut supposer qu'aucun a_i n'est un carré d'entiers. Montrer qu'il existe $\sigma : K \to \mathbb{C}$ tel que $\sigma(x) \neq x$. où $K = \mathbb{Q}(\sqrt{a_1}, ..., \sqrt{a_n})$ et

$x = k_1\sqrt{a_1} + ... + k_n\sqrt{a_n}$.
Notons p_i les nombres premiers qui apparaissent dans la décomposition des a_i avec un exposant impair. Supposons par exemple que $a_1 = n_1^2 p_1 q$ où n_1 et $q \in \mathbb{N}$. Il existe $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ tel que $\sigma(\sqrt{p_1}) = -\sqrt{p_1}$ et $\sigma(\sqrt{p_i}) = \sqrt{p_i}$ si $i \neq 1$. Alors $\sigma(\sqrt{a_1}) = -a_1$.

Donc $\sigma(x) = -k_1\sqrt{a_1} + ... + k_n\,\sigma(\sqrt{a_n})$. Or $\sigma(\sqrt{a_i}) = \pm\sqrt{a_i}$ Donc $\sigma(x) = -k_1\sqrt{a_1} \underbrace{+.... + k_n\,\sigma(\sqrt{a_n})}_{\leqslant k_2\sqrt{a_2} + ... + k_n\sqrt{a_n}} < k_1\sqrt{a_1} + k_2\sqrt{a_2} + ... + k_n\sqrt{a_n}$

$< x$. Donc $\sigma(x) \neq x$ et $x \notin \mathbb{Q}$.

3.

$K = \mathbb{Q}[10,\, 42] = \mathbb{Q} + \mathbb{Q}\sqrt{10} + \mathbb{Q}\sqrt{42} + \mathbb{Q}\sqrt{420} = \mathbb{Q} + \mathbb{Q}\sqrt{10} + \mathbb{Q}\sqrt{42} + \mathbb{Q}\sqrt{105}$. Et 1, $\sqrt{10}$,$\sqrt{42}$, $\sqrt{105}$ forment une base de K comme $\mathbb{Q}-$espace vectoriel.

Supposons par l'absurde que $\sqrt{15} \epsilon \mathbb{Q}[10, 42]$. Alors il existe $a, b, c, d \epsilon \mathbb{Q}$ tels que $\sqrt{15} = a + b\sqrt{10} + c\sqrt{42} + d\sqrt{105}$. Soit $\sigma \epsilon \mathrm{Gal}(K/\mathbb{Q})$ tel que $\sigma\big(\sqrt{2}\big) = \sqrt{2}$, $s\big(\sqrt{3}\big) = \sqrt{3}$, $\sigma\big(\sqrt{5}\big) = \sqrt{5}$, $s\big(\sqrt{7}\big) = -\sqrt{7}$, alors $\sigma\big(\sqrt{15}\big) = \sqrt{15} = a + b\sqrt{10} - c\sqrt{42} - d\sqrt{105}$. Donc $c = d = 0$. Mais $\sqrt{15} = a + b\sqrt{10} \Rightarrow 15 = a^2 + 10b^2 + 2\mathrm{ab}\sqrt{10} \Rightarrow \mathrm{ab} = 0$ car $\boldsymbol{\sqrt{10} \notin \mathbb{Q}}$**. Si $\boldsymbol{a = 0}$, alors $\boldsymbol{\sqrt{15} = b\sqrt{10} \Rightarrow 3.5 = b^2.2.5}$ absurde. Si $\boldsymbol{b = 0}$, alors $\boldsymbol{\sqrt{15} \epsilon \mathbb{Q}}$ absurde aussi.**

Conclusion $\sqrt{15} \notin \mathbb{Q}[10, 42]$. q.e.d