Faculté des Sciences & Techniques de Limoges
MASTER 1^{re} année

mercredi 3 novembre 2010

ALGÈBRE
Examen partiel.

Étude du nombre agébrique $\sqrt{\sqrt{2}+1}$

Soient $\theta = \sqrt{\sqrt{2}+1}$ et $\theta' = i\sqrt{\sqrt{2}-1} \in \mathbb{C}$; on note $K = \mathbb{Q}(\theta)$, $L = \mathbb{Q}(\theta')$ et $N = \mathbb{Q}(\theta, \theta')$.

1) a) Montrer que $\sqrt{2} \in K \cap L$.
b) Calculer $[L : \mathbb{Q}(\sqrt{2})]$ et en déduire que $L \cap \mathbb{R} = \mathbb{Q}(\sqrt{2})$
c) Montrer que $\mathbb{Q}(\sqrt{2}) = K \cap L$.

2) Calculer $\theta\theta'$ et en déduire que $N = \mathbb{Q}(\theta, i)$.

3) a) Donner un polynôme unitaire, de degré 4, à coefficients entiers, dont θ est racine.
b) Quelles sont ses autres racines ?
c) En déduire qu'il est irréductible.

4) a) Montrer que la clôture galoisienne de l'extension $K/\mathbb{Q}$ est $N/\mathbb{Q}$. Qu'en est-il de $L/\mathbb{Q}$?
b) Donner une base de N sur $\mathbb{Q}$ contenant θ et i.

5) a) Montrer que $(\theta + \theta')^2$ est un nombre complexe $\in \mathbb{Q}(i)$ qu'on calculera.
b) En considérant la partie réelle du nombre complexe $\theta + \theta'$ montrer que $\theta + \theta' \notin \mathbb{Q}(i)$ et calculer $[\mathbb{Q}(\theta + \theta') : \mathbb{Q}]$.
c) Parmi les nombres algébriques suivants : θ, θ', $\theta - \theta'$, $\sqrt{2}$, y en a t-il qui appartiennent à $\mathbb{Q}(\theta + \theta')$?
d) En déduire que $N = \mathbb{Q}(\theta + \theta', \sqrt{2})$.

6) Soit $c : z \mapsto \bar{z}$ la conjugaison complexe de $\mathbb{C}$; est-ce un automorphisme de K?, de L?, de N? Quel est le sous-corps de N des invariants par c ?

7) À l'aide de la question 4)b), montrer qu'il existe un unique automorphisme de N qui applique θ sur θ' et θ' sur θ; quel est le corps de ses invariants ?

8) a) À l'aide de la question 4)b), montrer qu'il existe un unique automorphisme σ de N qui applique θ sur θ' et θ' sur $-\theta$; calculer $\sigma(i\sqrt{2})$; en déduire le corps des invariants de σ ?
b) Montrer que $\sigma^4 = id_N$, que $c \circ \sigma \circ c = \sigma^3$ et en déduire que $\mathrm{Gal}(N/\mathbb{Q}) = \{id_N, \sigma, \sigma^2, \sigma^3, c, c \circ \sigma, c \circ \sigma^2, c \circ \sigma^3\}$.

La correspondance de Galois entre les sous-groupes de Gal(N/Q) et les sous-corps de N sera traitée en T.D.

Corrigé *sans phrase ou presque* *(ce qui n'est pas forcément conseillé aux étudiants !)*

1) $\sqrt{2} = \theta^2 - 1 \in \mathbb{Q}(\theta) \Rightarrow \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\theta)(\subset \mathbb{R})$; $\sqrt{2} = 1 - \theta'^2 \in \mathbb{Q}(\theta') \Rightarrow \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\theta') \cap \mathbb{R}$ et $[\mathbb{Q}(\theta') : \mathbb{Q}(\theta') \cap \mathbb{R}] \leq [\mathbb{Q}(\theta') : \mathbb{Q}(\sqrt{2})] \leq 2$.
$\mathbb{Q}(\theta') \not\subset \mathbb{R} \Rightarrow [\mathbb{Q}(\theta') : \mathbb{Q}(\theta') \cap \mathbb{R})] \geq 2 \Rightarrow \mathbb{Q}(\theta') \cap \mathbb{R} = \mathbb{Q}(\sqrt{2})$.
$\mathbb{Q}(\theta) \cap \mathbb{Q}(\theta') \subset \mathbb{Q}(\theta') \cap \mathbb{R} = \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\theta) \cap \mathbb{Q}(\theta') \Rightarrow \mathbb{Q}(\theta) \cap \mathbb{Q}(\theta') = \mathbb{Q}(\sqrt{2})$.

2) $\theta' = \sqrt{1-\sqrt{2}} \Rightarrow \theta\theta' = \sqrt{(1+\sqrt{2})(1-\sqrt{2})} = \sqrt{-1} = \pm i$; $\arg(\theta\theta') = \arg(\theta) + \arg(\theta') = \dfrac{\pi}{2} \Rightarrow$

$\theta\theta' = i \Rightarrow i \in \mathbb{Q}(\theta,\theta')$ et $\theta' \in \mathbb{Q}(\theta,i)$ donc $\mathbb{Q}(\theta,\theta') = \mathbb{Q}(\theta,i)$.
3) $\sqrt{2} = \theta^2 - 1 \Rightarrow 2 = \theta^4 - 2\theta^2 + 1 \Rightarrow \theta$ est racine de $X^4 - 2X^2 - 1$;
$\sqrt{2} = 1 - \theta'^2 \Rightarrow 2 = 1 - 2\theta'^2 + \theta'^4 \Rightarrow \theta'$ est racine de $X^4 - 2X^2 - 1$;
les racines de $X^4 - 2X^2 - 1$ sont donc $\pm\theta, \pm\theta'$.
$[\mathbb{Q}(\theta') : \mathbb{Q}] = [\mathbb{Q}(\theta') : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$ donc $X^4 + 2X^2 - 1$ est le polynôme minimal de θ' sur $\mathbb{Q}$ et c'est aussi celui de θ.
4) Le corps $\mathbb{Q}(\theta,\theta')$ est une extension galoisienne de $\mathbb{Q}$ en tant que corps des racines de $X^4 - 2X^2 - 1$. Réciproquement, toute extension galoisienne de $\mathbb{Q}$ contenant θ contient aussi ses conjugués $\pm\theta, \pm\theta'$ sur $\mathbb{Q}$ et donc $\mathbb{Q}(\theta,\theta')$. Cela s'applique aussi à θ'.
$\mathbb{Q} \subset \mathbb{Q}(\theta) \subset \mathbb{Q}(\theta,i) = \mathbb{Q}(\theta,\theta') \Rightarrow [\mathbb{Q}(\theta,\theta') : \mathbb{Q}] = [\mathbb{Q}(\theta,i) : \mathbb{Q}(\theta)][\mathbb{Q}(\theta) : \mathbb{Q}] = 8$ d'après le théorème de multiplicativité des degrés et $(1, \theta, \theta^2, \theta^3, i, i\theta, i\theta^2, i\theta^3)$ est une base de $\mathbb{Q}(\theta,\theta')$ sur $\mathbb{Q}$.
5) $(\theta + \theta')^2 = \theta^2 + 2\theta\theta' + \theta'^2 = \sqrt{2} + 1 + 2i - (\sqrt{2} - 1) = 2 + 2i \in \mathbb{Q}(i)$.
$\mathcal{R}e(\theta + \theta') = \theta \notin \mathbb{Q}$; $2i = (\theta + \theta')^2 - 2 \Rightarrow -4 = ((\theta + \theta')^2 - 2)^2 = (\theta + \theta')^4 - 4(\theta + \theta')^2 + 4$; $\theta + \theta'$ est donc racine de $X^4 - 4X^2 + 8$ et $[\mathbb{Q}(\theta + \theta') : \mathbb{Q}] \leq 4$.
$i = \dfrac{(\theta + \theta)^2 - 2}{2} \in \mathbb{Q}(\theta + \theta') \Rightarrow \mathbb{Q}(i) \subset \mathbb{Q}(\theta + \theta') \Rightarrow [\mathbb{Q}'(\theta + \theta') : \mathbb{Q}] = [\mathbb{Q}(\theta + \theta') : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] \geq 4 \Rightarrow$
$[\mathbb{Q}'(\theta + \theta') : \mathbb{Q}] = 4$.
$\theta \notin \mathbb{Q}(\theta + \theta')$ sinon $\theta' = (\theta + \theta') - \theta$ appartiendrait à $\mathbb{Q}(\theta,\theta')$ et on aurait $\mathbb{Q}(\theta,\theta') = \mathbb{Q}(\theta + \theta')$ ce qui est incompatible avec les degrés; pareil pour θ' , puis pour $\theta - \theta'$ car $\theta = \dfrac{(\theta + \theta') + (\theta - \theta')}{2}$ et aussi pour $\sqrt{2}$ car $\sqrt{2} = \dfrac{\theta^2 - \theta'^2}{2} = \dfrac{(\theta + \theta')(\theta - \theta')}{2}$.
$[\mathbb{Q}(\theta + \theta', \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\theta + \theta', \sqrt{2}) : \mathbb{Q}(\theta + \theta')][\mathbb{Q}(\theta + \theta') : \mathbb{Q}] = 2.4 = 8$;
$[\mathbb{Q}(\theta,\theta') : \mathbb{Q}] = 8$; $\mathbb{Q}(\theta + \theta', \sqrt{2}) \subset \mathbb{Q}(\theta,\theta') \Rightarrow \mathbb{Q}(\theta + \theta', \sqrt{2}) = \mathbb{Q}(\theta + \theta')$.
6) $\mathbb{Q}(\theta) \subset \mathbb{R} \Rightarrow c_{|\mathbb{Q}(\theta)} = \mathrm{id}_{\mathbb{Q}(\theta)}$; $c(\theta') = -\theta' \in \mathbb{Q}(\theta') \Rightarrow c_{|\mathbb{Q}(\theta')} \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\theta')) \Rightarrow c_{|\mathbb{Q}(\theta,\theta')} \in \mathrm{Gal}(\mathbb{Q}(\theta,\theta'))$.
$\mathbb{Q}(\theta,\theta')^{\langle c \rangle} = \mathbb{Q}(\theta,\theta') \cap \mathbb{R} = \mathbb{Q}(\theta,i) \cap \mathbb{R} = \mathbb{Q}(\theta)$.
7) D'après 4)b), il existe un unique automorphisme du corps $\mathbb{Q}(\theta,\theta')$ qui applique θ sur θ' et i sur i; il applique $\theta' = \dfrac{i}{\theta}$ sur $\dfrac{i}{\theta'} = \theta$ et il est le seul à le faire; il applique $\theta + \theta'$ sur lui-même donc son corps des invariants contient $\mathbb{Q}(\theta + \theta')$ mais pas $\mathbb{Q}(\theta,\theta')$ et, comme $[\mathbb{Q}(\theta,\theta') : \mathbb{Q}(\theta + \theta')] = 2$, il n'y a pas de corps intermédiaire et le sous-corps de $\mathbb{Q}(\theta,\theta')$ constitué de ses invariants est $\mathbb{Q}(\theta + \theta')$.
8) D'après 4)b), il existe un unique automorphisme du corps $\mathbb{Q}(\theta,\theta')$ qui applique θ sur θ' et i sur $-i$; il applique θ' sur $-\theta$; appelons-le σ. Alors $\sigma(\sqrt{2}) = \sigma(\theta^2 - 1) = \theta'^2 - 1 = -\sqrt{2}$ donc $\sigma(i\sqrt{2}) = (-i)(-\sqrt{2}) = i\sqrt{2}$. Donc $\mathbb{Q}((i\sqrt{2})) \subset \mathbb{Q}(\theta,\theta')^{\langle\sigma\rangle}$. Comme $\sigma^2(\theta) = \sigma(\theta') = \sigma(\dfrac{i}{\theta}) = \dfrac{-i}{\theta'} = -\theta$, $\sigma^2 \neq \mathrm{id}_{\mathbb{Q}(\theta,\theta')}$, et le sous-groupe $\langle\sigma\rangle$ de $\mathrm{Gal}(\mathbb{Q}(\theta,\theta')/\mathbb{Q})$ engendré par σ est au moins d'ordre 4; donc, par la théorie de Galois, $\mathbb{Q}(\theta,\theta')^{\langle\sigma\rangle}$ est au plus de degré 2 et, comme il contient $\mathbb{Q}(i\sqrt{2})$ qui est de degré 2, c'est lui.
Les automorphismes $id_N, \sigma, \sigma^2, \sigma^3, c, c\circ\sigma, c\circ\sigma^2, c\circ\sigma^3$ de $\mathbb{Q}(\theta,\theta')$ appliquent (i,θ) respectivement sur (i,θ), $(-i,\theta')$, $(i,-\theta)$, $(-i,-\theta')$, $(-i,\theta)$, $(i,-\theta')$, $(-i,-\theta)$, (i,θ'). Ils sont donc deux à deux distincts et, par suite, constituent le groupe de Galois de $\mathbb{Q}(\theta,\theta')$ sur $\mathbb{Q}$; cela montre aussi que $c\circ\sigma\circ c = \sigma^3 = \sigma^{-1}$.