Université de Rennes 1 - UFR Mathématiques - Année 2011-2012
Master 1 de mathématiques - Algèbre générale de base

Feuille d'exercices 10 : indications de solutions

Exercice 1 - 2 : si Ω' est une clôture algébrique de L, il existe un K-isomorphisme $\varphi : \Omega' \to \Omega$ d'après la question **1** et l'« unicité » de la clôture algébrique. La restriction de φ à L est le K-plongement cherché.

Exercice 3 - 1 : $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, -\sqrt{2}, -\sqrt{3})$ donc est le corps de décomposition de $(X^2 - 2)(X^2 - 3)$ dans $\mathbb{C}$. **2** : l'existence de σ peut se voir en remarquant que $K = \mathbb{Q}(\sqrt{3})(\sqrt{2})$ est une extension quadratique de $\mathbb{Q}(\sqrt{3})$, qui admet un unique $\mathbb{Q}(\sqrt{3})$-automorphisme envoyant $\sqrt{2}$ sur $-\sqrt{2}$. L'automorphisme $\sigma\tau$ envoie $\sqrt{2}$ sur $-\sqrt{2}$ et $\sqrt{3}$ sur $-\sqrt{3}$, et est égal à $\tau\sigma$. On a $G = \{1, \sigma, \tau, \sigma\tau\}$, avec $\sigma^2 = \tau^2 = (\sigma\tau)^2 = \mathrm{Id}$, d'où la table du groupe.

On a un isomorphisme naturel $G \to \{-1, +1\}^2$ envoyant $\gamma \in G$ sur le couple $\left(\frac{\gamma(\sqrt{2})}{\sqrt{2}}, \frac{\gamma(\sqrt{3})}{\sqrt{3}}\right)$.

Sous forme matricielle, le plus simple est d'utiliser la $\mathbb{Q}$-base $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ de K (lemme des bases télescopiques !). Dans cette base, les matrices de σ, τ et $\sigma\tau$ sont respectivement $\mathrm{diag}(1, -1, 1, -1)$, $\mathrm{diag}(1, 1, -1, -1)$ et $\mathrm{diag}(1, -1, -1, 1)$.

Exercice 4 - On sait déjà que P est irréductible (feuille 9, ex. **9**, question **4**), donc L est bien une extension de K ; de plus P est scindé sur L (*ibid.*, question **3**) donc L est un corps de décomposition de P. Comme P est séparable ($P' = 1$), L est bien galoisien sur K. L'ensemble des racines de P est $\omega + \mathbb{F}_p$ où ω est la classe de X ; on a un isomorphisme de groupes $(\mathbb{Z}/p\mathbb{Z}, +) \xrightarrow{\sim} \mathrm{Gal}(L/K)$ envoyant $a \in \mathbb{Z}/p\mathbb{Z}$ sur l'automorphisme induit par $Q(X) \mapsto Q(X + a)$ (qui est l'unique K-automorphisme de L envoyant ω sur $\omega + a$; plus généralement il envoie chaque racine α de P sur $\alpha + a$). L'isomorphisme inverse s'écrit :

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \xrightarrow{\sim} & (\mathbb{Z}/p\mathbb{Z}, +) \\ \gamma & \longmapsto & \gamma(\omega) - \omega. \end{array}$$

Exercice 5 - Pour l'exercice **2** : on pose $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = j\alpha_1$, $\alpha_3 = j^2\alpha_1$, et l'on identifie G au groupe des permutations de $R := \{\alpha_1, \alpha_2, \alpha_3\}$. Notons σ le cycle $\alpha_1 \mapsto \alpha_1 \mapsto \alpha_2 \mapsto \alpha_3 \mapsto \alpha_1$, et τ_i ($i = 1, 2, 3$) la transposition fixant α_i et échangeant les deux autres. En dehors des sous-groupes triviaux G et $\{e\}$ (correspondant aux sous-corps $\mathbb{Q}$ et L de L), les sous-groupes de G sont :

- le groupe alterné $\{e, \sigma, \sigma^2\}$, qui correspond au corps $\mathbb{Q}(j)$ (c'est la seule possibilité pour des raisons de degré, et d'ailleurs on a bien $\sigma(j) = \frac{\sigma(j\alpha_1)}{\sigma(\alpha_1)} = \frac{\alpha_3}{\alpha_2} = j$) ;
- les groupes $\{e, \tau_i\}$ ($i = 1, 2, 3$) correspondant respectivement aux sous-corps $\mathbb{Q}(\alpha_i)$.

Pour l'exercice **3** : les sous-groupes non triviaux de G sont $\{e, \sigma\}$, $\{e, \tau\}$ et $\{e, \sigma\tau\}$, correspondant respectivement aux sous-corps $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{6})$.

Exercice 6 - 1 : on remarque que $\sqrt{2} = \alpha^2 - 2 \in \mathbb{Q}[\alpha]$, et que $\alpha \notin \mathbb{Q}[\sqrt{2}]$ (calcul élémentaire, ou bien remarquer que $\mathrm{N}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(2 + \sqrt{2}) = 2$ qui n'est pas un carré dans $\mathbb{Q}$), donc $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Le polynôme minimal est $P = (X^2 - 2)^2 - 2 = X^4 - 4X^2 + 2$ (on peut aussi calculer

P d'abord et utiliser le critère d'Eisenstein pour voir qu'il est irréductible et donc que α est de degré 4).

2 : montrons que $\mathbb{Q}(\alpha)$ est le corps de décomposition de P dans $\mathbb{C}$: cela suffit parce que $\mathbb{Q}$ est de caractéristique nulle (donc toute extension est séparable), ou encore parce que P est séparable. Il suffit de montrer que les racines de P sont $\pm\sqrt{2\pm\sqrt{2}}$ (qui appartiennent à $\mathbb{Q}(\alpha)$). Pour cela, le plus simple est d'utiliser $P = (X^2-2)^2 - 2$; on peut aussi dire que comme P est irréductible, toute racine de P est image de α par un $\mathbb{Q}$-plongement de $\mathbb{Q}(\alpha)$; or un tel plongement envoie $\sqrt{2}$ sur $\pm\sqrt{2}$, donc α^2 sur $2\pm\sqrt{2}$, donc la racine est bien parmi ces 4 nombres, d'où le résultat puisqu'il y a 4 racines.

3 : on sait que le groupe de Galois G est d'ordre 4, et donc isomorphe soit à $\mathbb{Z}/4\mathbb{Z}$, soit à $(\mathbb{Z}/2\mathbb{Z})^2$. Un élément σ de G est déterminé par $\sigma(\alpha)$, qui est l'une des 4 racines de P. Considérons l'élément γ vérifiant $\gamma(\alpha) = \beta := \sqrt{2-\sqrt{2}}$. La relation $\gamma(\alpha^2) = \beta^2$) implique immédiatement $\gamma(\sqrt{2}) = -\sqrt{2}$. Comme $\alpha\beta = \sqrt{2}$, on en déduit que $\gamma(\beta) = \frac{-\sqrt{2}}{\gamma(\alpha)} = \frac{-\sqrt{2}}{\beta} = -\alpha$. Ainsi γ permute circulairement $\alpha, \beta, -\alpha, -\beta$: il est d'ordre 4 et engendre G, qui est donc isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

4 : le seul sous-groupe non banal de G est $H := \{e, \gamma^2\}$; on connaît un sous-corps de degré 2 de $\mathbb{Q}(\alpha)$, à savoir $\mathbb{Q}(\sqrt{2})$ qui est donc le seul sous-corps non banal de $\mathbb{Q}(\alpha)$ et correspond à H.

Exercice 7 - **1** : $[K : \mathbb{Q}] = 8$. **2** : le polynôme $X^4 - p \in \mathbb{Q}[X]$ a une racine dans $\mathbb{Q}(\alpha)$ et n'est pas décomposé dans $\mathbb{Q}(\alpha)[X]$. Donc $\mathbb{Q}(\alpha)$ n'est pas galoisien sur $\mathbb{Q}$. **3** : il résulte de la question **2** que le sous-groupe $\mathrm{Gal}(K/\mathbb{Q}(\alpha))$ de $\mathrm{Gal}(K/\mathbb{Q})$ n'est pas distingué, de sorte que $\mathrm{Gal}(K/\mathbb{Q})$ ne peut pas être abélien.

Exercice 10 - **2** : $\beta^2 = 2$. **4** : puisque α est d'ordre 8 dans $\Omega^\times$, on a $\alpha^a = \alpha^b$ si et seulement si $a \equiv b \pmod 8$.

5 :

$p \bmod 8$	action de φ
1	action triviale
-1	double transposition $\alpha \leftrightarrow \alpha^{-1}$, $-\alpha \leftrightarrow -\alpha^{-1}$
3	double transposition $\alpha \leftrightarrow -\alpha^{-1}$, $-\alpha \leftrightarrow \alpha^{-1}$
-3	double transposition $\alpha \leftrightarrow -\alpha$, $\alpha^{-1} \leftrightarrow -\alpha^{-1}$

6 : observer que pour tout $z \in \Omega$, l'orbite de z sous φ est l'ensemble des conjugués de z sur $\mathbb{F}_p$, c'est-à-dire des racines du polynôme minimal de z sur $\mathbb{F}_p$: en effet, le groupe de Galois du corps de décomposition de ce polynôme est engendré par φ. Le cardinal de cette orbite est donc le degré de z sur $\mathbb{F}_p$.

7 : un élément de Ω est dans $\mathbb{F}_p$ si et seulement si il est invariant par φ.

Exercice 11 - **1** : utiliser le fait (vu en cours) que L est une extension de degré n de K. **2** : si α est racine de P, alors $K(\alpha)$ est un corps à q^d éléments, donc $\alpha^{q^d} = \alpha$, ce qui entraîne que $\alpha^{q^n} = \alpha$. Le fait que K soit parfait entraîne que les racines de P sont simples.