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

Évaluation des exercices :

[E]= « élémentaire » : application directe des définitions et des résultats du cours.
[S]= « standard » : exercice « classique », souvent rencontré et souvent utilisé.

Feuille d'exercices 10

[E] **Exercice 1 -** Soient K un corps, L une extension algébrique de K.

1 - Montrer que toute clôture algébrique de L est une clôture algébrique de K.

2 - En déduire que si Ω est une clôture algébrique de K, il existe un K-plongement de L dans Ω.

3 - Soit U une extension algébriquement close de K, et soit $U_0 \subset U$ la fermeture algébrique de K dans U. Rappeler pourquoi U_0 est une clôture algébrique de K. En déduire que $\mathrm{Hom}_K(L, U) = \mathrm{Hom}_K(L, U_0)$.

Exercice 2 - Soit $K = \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, et soit $L = K(j) \subset \mathbb{C}$ (avec $j = e^{2i\pi/3}$).

1 - Trouver tous les ($\mathbb{Q}$-)plongements de K dans $\mathbb{C}$ et tous les ($\mathbb{Q}$-)automorphismes de K. Montrer que K n'est pas une extension galoisienne de $\mathbb{Q}$.

2 - Combien y a-t-il de $\mathbb{Q}$-plongements de L dans $\mathbb{C}$? Montrer qu'un tel plongement est déterminé par les images de $\sqrt[3]{2}$ (3 possibilités) et de j (2 possibilités) et que les 6 combinaisons sont possibles et définissent des automorphismes de L.

3 - Montrer que l'extension $L/\mathbb{Q}$ est galoisienne.

4 - Soit G le groupe de Galois de L sur $\mathbb{Q}$. À l'aide de l'action de G sur les trois racines de $X^3 - 2$, définir un morphisme de groupes $\varphi : G \to S_3$. Montrer que φ est injectif, puis que c'est un isomorphisme.

Exercice 3 - Soit $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. On rappelle (feuille **9**, ex. **5**) que $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ et que $[K : \mathbb{Q}] = 4$.

1 - Montrer que K est une extension galoisienne de $\mathbb{Q}$.

2 - Soit $\sigma \in G := \mathrm{Gal}(K/\mathbb{Q})$ défini par $\sigma(\sqrt{2}) = -\sqrt{2}$ et $\sigma(\sqrt{3}) = \sqrt{3}$; soit $\tau \in G$ défini par $\tau(\sqrt{2}) = \sqrt{2}$ et $\tau(\sqrt{3}) = -\sqrt{3}$. Calculer $\sigma\,\tau$, puis écrire la table de G et montrer que $G \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Exercice 4 - Soit K un corps de caractéristique $p > 0$. Soit $a \in K$ tel que le polynôme $P := X^p - X - a$ n'ait pas de racine dans K, et soit $L = K[X]/(P)$. Montrer que L est une extension galoisienne de K, de groupe de Galois isomorphe à $\mathbb{Z}/p\mathbb{Z}$. (Utiliser l'exercice **9** de la feuille **9**).

Quelques extensions galoisiennes (ou non) de $\mathbb{Q}$

Exercice 5 - Dans l'exercice **2**, expliciter la correspondance de Galois. Même question pour l'exercice **3**.

Exercice 6 - Désignons par α l'élément $\sqrt{2 + \sqrt{2}}$ de $\mathbb{C}$.

1 - Calculer $[\mathbb{Q}(\alpha) : \mathbb{Q}]$, puis déterminer le polynôme minimal P de α sur $\mathbb{Q}$.

2 - Montrer que l'extension $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ est galoisienne. (On pourra remarquer que c'est une extension de décomposition du polynôme P.)

3 - Déterminer le groupe de Galois de $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}$ (en précisant son action sur les racines de P). À quel groupe plus classique est-il isomorphe ?

4 - Donner la liste des sous-corps de $\mathbb{Q}(\alpha)$.

Exercice 7 - (extrait de l'examen terminal du 19/12/2008) Soit p un nombre premier. On note α le nombre réel $p^{1/4}$, et l'on désigne par K le corps de décomposition sur $\mathbb{Q}$, dans $\mathbb{C}$, du polynôme $X^4 - p$.

1 - Montrer que $K = \mathbb{Q}(i, \alpha)$, et déterminer le degré de K sur $\mathbb{Q}$.

2 - L'extension $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ est-elle galoisienne ?

3 - Le groupe de Galois de K sur $\mathbb{Q}$ est-il abélien ?

Exercice 8 - (généralisation de l'exercice **3**) Soient p_1, ..., p_n des nombres premiers distincts deux à deux. On désigne par K le corps $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$. On note α le nombre $\sqrt{p_1} + \cdots + \sqrt{p_n}$.

1 - Montrer que K est une extension galoisienne de $\mathbb{Q}$. On posera dans la suite $G := \mathrm{Gal}(K/\mathbb{Q})$.

2 - Pour $0 \leq k \leq n$, on pose $K_k = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k})$ (avec la convention $K_0 = \mathbb{Q}$). Montrer, par récurrence sur k, la propriété suivante : pour tout $s \in \mathbb{N}^*$ et pour tout s-uplet $(i_1, \ldots, i_s)$ tels que $k < i_1 < \cdots < i_s \leq n$, on a $\sqrt{p_{i_1} p_{i_2} \ldots p_{i_s}} \notin K_k$.

3 - En déduire que $[K : \mathbb{Q}] = 2^n$ et donner une $\mathbb{Q}$-base de K.

4 - Montrer que pour tout $k \in \{1, \ldots, n\}$, il existe $\sigma_k \in G$ tel que $\sigma_k(\sqrt{p_k}) = -\sqrt{p_k}$ et $\sigma_k(\sqrt{p_l}) = \sqrt{p_l}$ pour tout $l \in \{1, \ldots, n\} \backslash \{k\}$. En déduire que pour tout $(\varepsilon_1, \ldots, \varepsilon_n) \in \{1, -1\}^n$, le nombre $\varepsilon_1 \sqrt{p_1} + \cdots + \varepsilon_n \sqrt{p_n}$ est racine du polynôme minimal de α sur $\mathbb{Q}$.

5 - Montrer que $K = \mathbb{Q}(\alpha)$. (On raisonnera sur le degré du polynôme minimal de α sur $\mathbb{Q}$.)

6 - Montrer que G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$.

7 - Montrer que tout sous-corps de K est une extension galoisienne de $\mathbb{Q}$.

Corps finis

Exercice 9 -

1 - Montrer que $X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$ (on pourra montrer que c'est le polynôme minimal du nombre complexe $\zeta = e^{i\pi/4}$).

2 - Montrer que $X^4 + 1$ est réductible dans $\mathbb{F}_2[X]$.

3 - Soit p un nombre premier impair. En remarquant que l'ordre de $\mathbb{F}_{p^2}^\times$ est un multiple de 8, montrer que le polynôme $X^4 + 1$ possède une racine dans $\mathbb{F}_{p^2}$. En déduire que $X^4 + 1$ est réductible dans $\mathbb{F}_p[X]$.

Exercice 10 - Soit Ω un corps de caractéristique $\neq 2$.

1 - Soit $x \in \Omega$. Montrer que les conditions suivantes sont équivalentes :

(i) $x^4 = -1$;

(ii) x est un élément d'ordre 8 du groupe $\Omega^\times$.

Dans la suite on note α une racine de $P := X^4 + 1$ dans Ω, et l'on pose $\beta = \alpha + \alpha^{-1}$.

2 - Calculer β^2.

3 - Montrer que l'ensemble des racines de P est $R := \{\alpha, \alpha^{-1}, -\alpha, -\alpha^{-1}\}$ (avec les relations $\alpha^{-1} = \alpha^7$, $-\alpha^{-1} = \alpha^3$, $-\alpha = \alpha^5$).

4 - Soient a et b deux entiers. À quelle condition a-t-on $\alpha^a = \alpha^b$?

Dans la suite on fixe un nombre premier $p \neq 2$, et on prend pour Ω une clôture algébrique de $\mathbb{F}_p$. On note $\varphi : x \mapsto x^p$ l'automorphisme de Frobenius de Ω.

5 - En fonction de la classe de p modulo 8, décrire l'action de φ sur l'ensemble R.

6 - En remarquant que l'orbite de α sous φ a au plus deux éléments, retrouver le fait que α est de degré ≤ 2 sur $\mathbb{F}_p$ (exercice **9**, question **3**).

7 - Déduire de la question **5** les deux équivalences :

(i) $\alpha \in \mathbb{F}_p \Leftrightarrow p \equiv 1 \pmod 8$;

(ii) $\beta \in \mathbb{F}_p \Leftrightarrow p \equiv \pm 1 \pmod 8$.

(On peut aussi montrer directement (i) en considérant le groupe $\mathbb{F}_p^\times$).

8 - Déduire des questions précédentes l'équivalence :

$$2 \text{ est un carré dans } \mathbb{F}_p \quad \Leftrightarrow \quad p \equiv \pm 1 \pmod 8.$$

Exercice 11 - Soit K un corps fini de cardinal q, et soit $n \in \mathbb{N}^*$. Le but de l'exercice est de montrer que le polynôme $(X^{q^n} - X) \in K[X]$ est le produit de tous les polynômes irréductibles unitaires de $K[X]$ dont le degré divise n. On notera L un corps de décomposition de ce polynôme.

1 - Soit P un facteur irréductible de $(X^{q^n} - X)$ dans $K[X]$. Montrer que le degré de P divise n. (Raisonner sur le degré du corps de rupture de P.)

2 - Réciproquement, soit P un polynôme irréductible de degré d, avec $d|n$. Montrer que P divise $(X^{q^n} - X)$. (On pourra montrer que toute racine de P est racine de $(X^{q^n} - X)$, et utiliser le fait que K est un corps parfait.)

3 - Conclure, en remarquant que le polynôme $(X^{q^n} - X)$ n'a pas de racines multiples dans L.