E.N.S. Ulm, L3, 2000–2003
Univ. Paris-Sud, M1, 2004–2007
Stéphane Fischler

T.D. numéro 14
Algèbre

Exercice 1 Dans cet exercice, on étudie l'extension $K = \mathbb{Q}(\sqrt[3]{2}, j)$ de $\mathbb{Q}$ (on note j la racine cubique de l'unité de partie imaginaire strictement positive).

1. Démontrer que $K/\mathbb{Q}$ est une extension de degré 6.
2. Démontrer que K est le corps de décomposition sur $\mathbb{Q}$ du polynôme $X^3 - 2$. En déduire que $K/\mathbb{Q}$ est normale, et que son groupe de Galois est isomorphe à $\mathfrak{S}_3$.
3. Démontrer que les éléments de G sont donnés par $j \mapsto j^\varepsilon$ et $\sqrt[3]{2} \mapsto j^\eta \sqrt[3]{2}$ pour $(\varepsilon, \eta) \in \{1, 2\} \times \{0, 1, 2\}$.
4. A-t-on $K = \mathbb{Q}(\sqrt[3]{2} + j)$?

On pose $G = \mathrm{Gal}(K/\mathbb{Q})$. On fixe l'isomorphisme de la question précédente en notant respectivement 1, 2 et 3 les nombres $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$.

4. Pour chacune des six permutations $\tau \in \mathfrak{S}_3$, expliciter l'élément de G qui correspond à τ.
5. Donner la liste des sous-groupes de $\mathfrak{S}_3$. Lesquels sont distingués dans $\mathfrak{S}_3$?
6. Donner la liste des extensions intermédiaires entre $\mathbb{Q}$ et K. Lesquelles sont normales sur $\mathbb{Q}$?
7. Utiliser la question précédente pour répondre directement à la question 4.

Exercice 2 Étudier l'extension $\mathbb{F}_{2^{12}}/\mathbb{F}_2$: calculer son groupe de Galois, dessiner le treillis de ses sous-groupes et celui des extensions intermédiaires.

Exercice 3 Dans cet exercice, on étudie l'extension $K = \mathbb{Q}(\sqrt[4]{2}, i)$ de $\mathbb{Q}$.

1. Démontrer que $K/\mathbb{Q}$ est une extension de degré 8, et en donner une base (comme espace vectoriel).
2. Démontrer que K est le corps de décomposition sur $\mathbb{Q}$ du polynôme $X^4 + 2$. En déduire que $K/\mathbb{Q}$ est normale.

On pose $G = \mathrm{Gal}(K/\mathbb{Q})$. On rappelle que $\mathcal{D}_4$ est le groupe diédral d'ordre 8, formé par les isométries du plan qui fixent un carré.

3. Démontrer que tout sous-groupe de $\mathfrak{S}_4$ d'ordre 8 est isomorphe à $\mathcal{D}_4$. (Indication : on pourra utiliser un théorème de Sylow)
4. En déduire que G est isomorphe à $\mathcal{D}_4$.

5. Démontrer qu'il existe un unique élément ϱ de G tel que $\varrho(\sqrt[4]{2}) = i\sqrt[4]{2}$ et $\varrho(i) = i$. Démontrer qu'il existe un unique élément σ de G tel que $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$ et $\sigma(i) = -i$.

6. Démontrer que ϱ est d'ordre 4, et σ d'ordre 2.

Pour fixer les idées, on se place dans un plan orienté et on note $ABCD$ un carré, $r \in \mathcal{D}_4$ la rotation d'angle $\pi/2$ et $s \in \mathcal{D}_4$ la symétrie orthogonale par rapport à la diagonale (AC).

7. Démontrer qu'il existe un unique isomorphisme de G dans $\mathcal{D}_4$ qui envoie ϱ sur r et σ sur s.

8. Donner la liste des sous-groupes de $\mathcal{D}_4$. Lesquels sont distingués dans $\mathcal{D}_4$? (Indication : dessiner un treillis pour représenter les inclusions entre sous-groupes ; au total, il y a dix sous-groupes de $\mathcal{D}_4$)

9. Donner la liste des extensions intermédiaires entre $\mathbb{Q}$ et K. Lesquelles sont normales sur $\mathbb{Q}$?

Exercice 4 Soient $n \geq 1$ un entier, et E un ensemble formé par exactement n nombres premiers (deux à deux distincts). Démontrer que l'extension de $\mathbb{Q}$ engendrée par les $\sqrt{p}$, pour $p \in E$, est normale, de degré 2^n, et que son groupe de Galois est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$. En déduire que les nombres $\sqrt{p}$, pour p premier, sont linéairement indépendants sur $\mathbb{Q}$.

Exercice 5 Transmission de messages par Minitel Notons $P \in \mathbb{F}_2[X]$ le polynôme $X^7 + X^3 + 1$, dont on admet qu'il est irréductible. On considère le corps $K = \mathbb{F}_2[X]/(P)$, qui est de cardinal 128. Dans cet exercice, on construit un code qui a été utilisé pour le Minitel (d'après un article de P. Arnoux, *Pour la Science*, mars 1988). Le problème est de compléter un message à transmettre en y adjoignant des "bits de contrôle" pour que celui qui reçoit le message soit capable de détecter la présence d'erreurs, voire de les corriger, si elles ne sont pas trop nombreuses.

Notons x la classe de X dans K. On représente le message à transmettre par une suite binaire de longueur 120, notée $a = (a_k)_{0 \leq k \leq 119}$ (avec $a_k \in \mathbb{F}_2$). Le message qu'on va transmettre est noté $\varphi(a) = (a_k)_{0 \leq k \leq 126} \in \mathbb{F}_2^{127}$; il est donné par la formule

$$x^7 \sum_{k=0}^{119} a_k x^k = \sum_{\ell=0}^{6} a_{120+\ell}\, x^\ell \text{ dans } K$$

1. Démontrer que l'application φ est bien définie.

2. Démontrer que x engendre le groupe K^*.

3. On suppose que le message a été transmis avec au plus une erreur. Démontrer que celui qui reçoit la transmission peut savoir si une erreur a été commise ou pas, et qu'il peut (le cas échéant) la corriger.

4. Démontrer que si $a \neq a'$ alors $\varphi(a)$ et $\varphi(a')$ diffèrent par au moins trois coordonnées.

5. On suppose que le message a été transmis avec exactement deux erreurs. Démontrer le récepteur sait qu'au moins une erreur a été commise, mais qu'il est incapable (en général) de la corriger.

6. On suppose que le message a été transmis avec au moins trois erreurs. Donner un exemple où le récepteur reçoit un message faux en pensant qu'aucune erreur n'a été commise.