Aix–Marseille Université 2019-2020

Mathématiques –Master 1

DS 3

Exercice 1

Dans tout cet exercice, on pourra admettre que $\sqrt{6}$, $\sqrt{7}$ et $\sqrt{42}$ sont irrationnels. On considère le corps $\mathbb{K} := \mathbb{Q}(\sqrt{6}+\sqrt{7})$.

1. (a) Trouver un polynôme $P_{\mathbb{K}} \in \mathbb{Q}[X]$ de degré quatre, annulateur de $\sqrt{6}+\sqrt{7}$. En déduire le polynôme minimal de $\sqrt{6}+\sqrt{7}$ sur $\mathbb{Q}$.
2. (a) Quel est le degré de $\mathbb{K}$ vu comme extension de $\mathbb{Q}$?
   (b) Montrer que $\mathbb{K}$ est égal à $\mathbb{Q}(\sqrt{6},\sqrt{7})$.
3. On note $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})$ le groupe des $\mathbb{Q}$–automorphismes de $\mathbb{K}$.
   (a) Donner explicitement tous les éléments de $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})$.
   (b) A quel groupe classique $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})$ est-il isomorphe ?
   (c) Donner un exemple d'extension de corps $\mathbb{K}'$ de $\mathbb{Q}$ dont le groupe $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K}')$ des $\mathbb{Q}$–automorphismes est de même cardinal que $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})$ sans lui être isomorphe.
4. (a) Soit $\varphi \in \mathrm{Gal}_{\mathbb{Q}}(\mathbb{K})$. Pour tout $P := \sum_{i=0}^{n} a_i X^i \in \mathbb{K}[X]$, on note
$$\varphi(P) := \sum_{i=0}^{n} \varphi(a_i) X^i \in \mathbb{K}[X].$$
   Montrer que $\alpha \in \mathbb{K}$ est racine de P si et seulement si $\varphi(\alpha)$ est racine de $\varphi(P)$.
   (b) En déduire toutes les racines de $P_{\mathbb{K}}$ dans $\mathbb{R}$.

Exercice 2

1. Donner la décomposition en facteurs irréductibles de X^5-1 sur $\mathbb{C}$, sur $\mathbb{R}$ et sur $\mathbb{Q}$.
2. En déduire une expression algébrique pour $\cos(2\pi/5)$.
3. Peut-on construire un pentagone régulier à la règle et au compas ?

Exercice 3

Soit p un nombre premier et $n \in \mathbb{N}^*$. On note $\mathrm{Aut}(\mathbb{F}_{p^n})$ le groupe des automorphismes de corps de $\mathbb{F}_{p^n}$ et $\varphi_F \in \mathrm{Aut}(\mathbb{F}_{p^n})$ le morphisme de Frobenius défini par $\varphi_F(x) = x^p$ pour tout $x \in \mathbb{F}_{p^n}$. Enfin, pour tout $\varphi \in \mathrm{Aut}(\mathbb{F}_{p^n})$, on note $\mathrm{Stab}(\varphi) := \left\{x \in \mathbb{F}_{p^n} \mid \varphi(x) = x\right\}$.

1. Montrer que, pour tout $\varphi \in \mathrm{Aut}(\mathbb{F}_{p^n})$, $\mathrm{Stab}(\varphi)$ est un sous-corps de $\mathbb{F}_{p^n}$.
2. Déterminer l'ordre de φ_F en tant qu'élément de $\mathrm{Aut}(\mathbb{F}_{p^n})$.
3. Montrer que, pour tout $k \in \mathbb{N}^*$, $\mathrm{Stab}(\varphi_F^k)$ est isomorphe à $\mathbb{F}_{p^{\mathrm{pgcd}(k,n)}}$.
4. Montrer que si $\mathbb{K} \subset \mathbb{F}_{p^n}$ est un sous-corps de $\mathbb{F}_{p^n}$, alors $\mathbb{K} = \mathrm{Stab}(\varphi_F^k)$ avec $k \in \mathbb{N}^*$ divisant n.
5. Soit $\mathbb{K}_1$ et $\mathbb{K}_2$ deux sous-corps de $\mathbb{F}_{p^n}$. A quel corps $\mathbb{K}_1 \cap \mathbb{K}_2$ est-il isomorphe ?

Exercice 4

Soit p un nombre premier et $n \in \mathbb{N}^*$. On identifiera dans tout l'exercice $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ avec le sous-corps $\left\{ \underbrace{1_{\mathbb{F}_{p^n}} + \cdots + 1_{\mathbb{F}_{p^n}}}_{k \text{ fois}} \mid k \in [\![0, p-1]\!] \right\} \subset \mathbb{F}_{p^n}$.

On rappelle que, pour tout $k \in \mathbb{N}^*$, $\binom{p}{k}$ est divisible par p et que, corollairement, le morphisme de Frobenius $\varphi_F : \begin{array}{ccc} \mathbb{F}_{p^k} & \to & \mathbb{F}_{p^k} \\ x & \mapsto & x^p \end{array}$ est linéaire.

1. (a) Montrer que $\mathbb{F}_p = \left\{ x \in \mathbb{F}_{p^n} \mid x^p = x \right\}$.
   (b) Montrer que $\mathbb{F}_p[X] = \left\{ P \in \mathbb{F}_{p^n}[X] \mid \big(P(X)\big)^p = P(X^p) \right\}$.
2. Soit $P \in \mathbb{F}_p[X]$ et x_0 une racine de P dans $\mathbb{F}_{p^n}$. On pose

$$r_0 := \min\left\{ r \in \mathbb{N} \mid x_0^{p^r} = x_0 \right\} \quad \text{et} \quad \widetilde{P} := \prod_{i=0}^{r_0 - 1} \left(X - x_0^{p^i} \right) \in \mathbb{F}_{p^n}[X].$$

   (a) Montrer que r_0 est bien défini.
   (b) Montrer que $\widetilde{P} \in \mathbb{F}_p[X]$.
   (c) Montrer que pour tout $i \in \mathbb{N}$, $x_0^{p^i}$ est racine de P.
   (d) i. Soit $x \in \mathbb{F}_{p^n}$, montrer que si $x^k = 1$ avec $k \in \mathbb{N}^*$ premier avec $p^n - 1$, alors $x = 1$.
   ii. Montrer que pour tout $i_1 < i_2 \in [\![0, r_0 - 1]\!]$, $x_0^{p^{i_1}} \neq x_0^{p^{i_2}}$.
   (e) Montrer que $\widetilde{P}$ divise P dans $\mathbb{F}_p[X]$.
3. Montrer qu'un polynôme irréductible $P \in \mathbb{F}_p[X]$ admet une racine dans $\mathbb{F}_{p^n}$ si et seulement si il est scindé à racines simples dans $\mathbb{F}_{p^n}$.
4. Soit $P \in \mathbb{F}_p[X]$ irreductible de degré $d \in \mathbb{N}^*$ admettant une racine x_0 dans $\mathbb{F}_{p^n}$.
   (a) Montrer que P divise $X^{p^n} - X$ et que $d = \min\left\{ r \in \mathbb{N} \mid x_0^{p^r} = x_0 \right\}$.
   (b) Montrer que, pour tout $k \in \mathbb{N}$, $x_0^{p^{kd}} = x_0$.
   (c) En déduire que d divise n.
5. Montrer qu'un polynôme irréductible $P \in \mathbb{F}_p[X]$ de degré $d \in \mathbb{N}^*$ admet une racine dans $\mathbb{F}_{p^n}$ si et seulement si d divise n.