Université Aix-Marseille 2019–2020

Master 1 – Mathématiques & Applications
Algèbre & Géométrie

DEVOIR SURVEILLÉ 2

Notation. Pour toute puissance d'un nombre premier q, on notera $\mathbb{F}_q$ le corps à q éléments.

Exercice 1.

1. Montrer que les corps $\mathbb{R}$ et $\mathbb{C}$ ne sont pas isomorphes.
2. Montrer que les corps $\mathbb{Q}(\sqrt{3})$ et $\mathbb{Q}(\sqrt{7})$ ne sont pas isomorphes.

Exercice 2.

1. Soit $\mathbb{K}$ un corps commutatif. Le but de cette question est de montrer que tout sous-groupe multiplicatif fini de $\mathbb{K}^*$ est cyclique. On considère donc $H \subset \mathbb{K}^*$ sous-groupe fini.
   (a) Montrer que, pour tout $n \in \mathbb{N}^*$, le polynôme $X^n - 1$ possède au plus n racines dans $\mathbb{K}$.
   (b) Soit p un diviseur premier de $|H|$ et $\alpha \in \mathbb{N}^*$ la puissance maximale telle que p^α divise $|H|$.
      i. Montrer qu'un élément de H dont l'ordre n'est pas divisible par p^α est racine de $X^{\frac{|H|}{p}} - 1$.
      ii. Montrer qu'il existe au moins un élément de H dont l'ordre est divisible par p^α.
      iii. Montrer qu'il existe au moins un élément de H d'ordre exactement p^α.
   (c) Montrer qu'il existe au moins un élément de H d'ordre $|H|$ et conclure.
2. Soit q une puissance d'un nombre premier. Montrer que pour tout diviseur d de $q-1$, il existe au moins un élément du groupe $\mathbb{F}_q^*$ d'ordre d.

Exercice 3.
Soit p un nombre premier impair. et $P := X^4 + 1 \in \mathbb{F}_{p^2}[X]$.

1. (a) Montrer que $\alpha \in \mathbb{F}_{p^2}$ est racine de P si et seulement si α est d'ordre huit dans le groupe $\mathbb{F}_{p^2}^*$.
   (b) Montrer que si $\alpha \in \mathbb{F}_{p^2}$ est racine de P, alors $-\alpha$, α^{-1} et $-\alpha^{-1}$ le sont aussi.
   (c) Montrer que P est scindé.
2. Montrer que les racines de $X^p - X \in \mathbb{F}_{p^2}[X]$ forment un sous-corps isomorphe à $\mathbb{F}_p$ (et que l'on notera d'ailleurs $\mathbb{F}_p$ par la suite).
3. Soit $\alpha \in \mathbb{F}_{p^2}$ racine de P.
   (a) Montrer que $(\alpha + \alpha^{-1})^2 = 2$.
   (b) i. Montrer que, pour tout $k \in \mathbb{Z}$, α^k ne dépend que du reste de la division euclidienne de k par 8.
      ii. Montrer que $(\alpha + \alpha^{-1})^p = \varepsilon(\alpha + \alpha^{-1})$ avec $\varepsilon = 1$ si $p \equiv \pm 1 \mod 8$ et $\varepsilon = -1$ sinon.
   (c) Montrer que $\alpha + \alpha^{-1} \in \mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \mod 8$.
4. Montrer que 2 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \mod 8$.
5. Donner deux exemples explicites illustrant chacun des cas possibles.

Exercice 4.
Soit p un nombre premier et $n \in \mathbb{N}^*$. Montrez que $\mathrm{GL}_n(\mathbb{F}_p)$ possède $p^{\frac{n(n-1)}{2}} \prod_{i=1}^{n}(p^i - 1)$ éléments.