Théorie des nombres

Michel Waldschmidt

code UE : MMAT4020 code Scolar : MM020

Examen Partiel 23 Février 2011

Seul le polycopié est autorisé

Exercice 1. Soient K un corps de caractéristique p premier et soit G un sous–groupe fini d'ordre n de $K^\times$. Montrer que p ne divise pas n.

Exercice 2. On considère le polynôme $P := X^4 - 8 \in \mathbf{Q}[X]$ et une racine $\alpha := \sqrt[4]{8} \in \mathbf{R}$.

1. On pose $\beta := \alpha + \alpha^2$. Montrer que $\mathbf{Q}(\alpha) = \mathbf{Q}(\beta)$ (on pourra par exemple calculer $\beta(\beta - 2\alpha^2)$).
2. Calculer le degré de $\mathbf{Q}(\alpha)$ sur $\mathbf{Q}$.
3. Décrire un corps de décomposition L de P sur $\mathbf{Q}$.
4. Calculer le degré de l'extension $L/\mathbf{Q}$.

Exercice 3. On considère les groupes additifs $\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$ et les groupes multiplicatifs $\mathbf{R}_+^\times \subset \mathbf{R}^\times$ et $\boldsymbol{\mu} \subset \mathbf{U} \subset \mathbf{C}^\times$, où $\boldsymbol{\mu}$ est le groupe des racines de l'unité (c'est le sous–groupe de torsion de $\mathbf{C}^\times$) et $\mathbf{U}$ le groupe des nombres complexes de module 1.
Établir des isomorphismes de groupes

$$\mathbf{R} \longrightarrow \mathbf{R}_+^\times, \quad \mathbf{C}/\mathbf{Z} \longrightarrow \mathbf{C}^\times, \quad \mathbf{R}/\mathbf{Z} \longrightarrow \mathbf{U}, \quad \mathbf{Q}/\mathbf{Z} \longrightarrow \boldsymbol{\mu}, \quad \mathbf{R}_+^\times \times \mathbf{R}/\mathbf{Z} \longrightarrow \mathbf{C}^\times.$$

Exercice 4. Soit F un corps fini à q éléments. Préciser, selon les valeurs de q, le nombre de facteurs irréductibles du polynôme cyclotomique Φ_7 sur F et leurs degrés.
Donner la factorisation explicite de Φ_7 sur chacun des corps $\mathbf{F}_2$, $\mathbf{F}_3$, $\mathbf{F}_5$, $\mathbf{F}_7$, $\mathbf{F}_8$.

Exercice 5. Soient F un corps fini, $\mathbf{F}_p$ le sous–corps premier de F et $q = p^s$ le nombre d'éléments de F avec $s = [F : \mathbf{F}_p]$.
a) On suppose que $q - 1$ est un nombre premier. Quel est
• le nombre de $\alpha \in F^\times$ tels que $F = \mathbf{F}_p(\alpha)$?
• le nombre de $\alpha \in F^\times$ tels que α engendre le groupe cyclique $F^\times$?
b) Soit n un entier tel que l'ordre de p modulo n soit égal à s. Montrer qu'il existe un élément α d'ordre n dans le groupe multiplicatif $F^\times$ tel que $\mathbf{F}_p(\alpha) = F$.
c) En déduire que les conditions suivantes sont équivalentes :
(i) Tout élément $\alpha \in F^\times$ vérifiant $F = \mathbf{F}_p(\alpha)$ est un générateur du groupe cyclique $F^\times$.
(ii) $q - 1$ est premier.