

EXAMEN DE MATHÉMATIQUES

MERCREDI 6 JANVIER 2010

L'épreuve dure 3 heures. Les exercices **A**, **B**, **C** et **D** peuvent être traités indépendamment. Les résumés du cours de C. Blanchet et une page recto-verso de notes manuscrites sont seuls autorisés.

Une réponse ne vaut que si elle est démontrée par un argument explicite et juste. Le barème est donné à titre indicatif.

A– (4 points) Soit M le sous-module de $\mathbb{Z}^3$ engendré par $u = \begin{pmatrix} 8 \\ 7 \\ 12 \end{pmatrix}$, $v = \begin{pmatrix} 18 \\ 16 \\ 26 \end{pmatrix}$ et $w = \begin{pmatrix} 30 \\ 26 \\ 40 \end{pmatrix}$.

- (a) Calculer le déterminant de (u, v, w) .
(b) Est-ce que M est un sous-module libre ? Quel est son rang ?
(c) Est-ce que le quotient $G = \mathbb{Z}^3/M$ est un module de torsion ? Est-ce un groupe abélien fini ?
- Déterminer les facteurs invariants de G .
- Est-ce que G est isomorphe au groupe produit $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3$?

B– (6 points) Soit K le corps $\mathbb{Q}(\sqrt{2})$.

- Quel est le degré de l'extension $(K : \mathbb{Q})$?
Montrer que le groupe $\text{Gal}(K : \mathbb{Q})$ est engendré par un élément σ d'ordre 2 qu'on précisera.
- Pour $z \in K$, on définit $N(z) = z \sigma(z)$.
 - Montrer que pour tout $z \in K$, on a $N(z) \in \mathbb{Q}$.
 - Montrer que si $z \in K$ est un carré, alors $N(z)$ est un carré dans $\mathbb{Q}$.
 - Est-ce que $4 + 2\sqrt{2}$ est un carré dans K ?Soit L le corps $K(\alpha)$, avec $\alpha = \sqrt{4 + 2\sqrt{2}}$. On note $\beta = \sqrt{4 - 2\sqrt{2}}$.
- Quel est le degré de l'extension $(L : \mathbb{Q})$?
 - Quel est le polynôme minimal de α sur $\mathbb{Q}$?
 - Montrer que L contient β . (On pourra calculer $\alpha\beta$.)
 - Est-ce que l'extension $(L : \mathbb{Q})$ est normale ? galoisienne ?
- Montrer que L est égal à $\mathbb{Q}(\alpha)$.
 - Montrer qu'il existe un unique élément $h \in \text{Gal}(L : \mathbb{Q})$ tel que $h(\alpha) = \beta$.
 - Calculer $h(\alpha^2)$, $h(\sqrt{2})$ et $h(\beta)$. Quel est l'ordre de h ?
 - Déterminer les sous-corps de L .

C– (6 points) Soit $\mathbb{F} = \mathbb{F}_{27}$ le corps à 27 éléments.

1. Déterminer la structure des groupes abéliens $(\mathbb{F}, +)$ et $(\mathbb{F}^*, \times)$.
2. Quel est le groupe de Galois de $\mathbb{F}$? Quels sont les sous-corps de $\mathbb{F}$?
3. Soit $\mathbb{K}$ le corps de décomposition du polynôme $P = X^{13} - 1$ sur le corps à 3 éléments $\mathbb{F}_3$ et α une racine de P distincte de 1 dans $\mathbb{K}$.
 - (a) Est-ce que l'extension $(\mathbb{K} : \mathbb{F}_3)$ est séparable? galoisienne?
 - (b) Montrer que α engendre le groupe des racines 13-ièmes de 1 dans $\mathbb{K}$, puis que $\mathbb{K} = \mathbb{F}_3(\alpha)$.
 - (c) Quel est l'ordre de l'automorphisme de Frobenius de $\mathbb{K}$? Déterminer $[\mathbb{K} : \mathbb{F}_3]$. Quel est le cardinal de $\mathbb{K}$?
 - (d) Quel est le degré du polynôme minimal de α ?
4. Est-ce que le polynôme cyclotomique $\phi_{13} \in \mathbb{Z}[X]$ reste irréductible sur $\mathbb{F}_3$?
5. Combien y a-t-il de polynômes irréductibles de degré 3 sur $\mathbb{F}_3$?

D– (4 points + questions hors barème) Soit p un nombre premier impair.

1. (a) Montrer que pour tout $x \in \mathbb{F}_p^*$, on a $x^{\frac{p-1}{2}} = \pm 1$.
(b) Montrer que $x \in \mathbb{F}_p^*$ est un carré dans $\mathbb{F}_p$ si et seulement si $x^{\frac{p-1}{2}} = 1$.

Pour k entier premier avec p , on pose $L(k, p) = 1$ si $x = \bar{k}$ est un carré dans $\mathbb{F}_p$ et $L(k, p) = -1$ sinon.

Soit r un nombre premier impair différent de p .

2. Montrer que le discriminant du polynôme $Q = X^r - 1$ est $D = (-1)^{\frac{r-1}{2}} r^r$.
3. Montrer que $L(D, p) = (-1)^{\frac{(p-1)(r-1)}{4}} L(r, p)$.

Les questions qui suivent sont hors barème.

On note σ la permutation des racines de Q induite par l'automorphisme de Frobenius du corps de décomposition de Q sur $\mathbb{F}_p$.

4. Montrer que la permutation σ est composée de $\frac{r-1}{m}$ cycles disjoints d'ordre m .
5. Montrer que la signature de σ est égale à $L(p, r)$.
6. Démontrer la *loi de réciprocité quadratique de Gauss* :

$$L(p, r) = (-1)^{\frac{(p-1)(r-1)}{4}} L(r, p) .$$