Examen 9 Septembre 2004

`Les calculatrices ne sont pas autorisées, les documents non plus.`

Barême approximatif: sur 20

Tous les résultats vus en cours ou en TD peuvent être utilisés. Il est conseillé de dire quel énoncé précis est appliqué mais de ne pas le redémontrer.

Quand n est un entier positif on désigne par ϕ_n le n-ième polynôme cyclotomique.
Quand p est un nombre premier et a un entier rationnel on note

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divise } a, \\ 1 & \text{si } a \text{ est un carré non nul modulo } p, \\ -1 & \text{sinon} \end{cases}$$

le symbole de Legendre.

(3) **Exercice 1.** Soit

$$n = \prod_p p^{v_p(n)}$$

la décomposition de l'entier n en facteur premiers. On note

$$\Omega(n) = \sum_p v_p(n).$$

Montrer que

$$\lim_{x\to\infty} \frac{1}{x \log\log x} \sum_{n\le x} \Omega(n) = 1.$$

(2) **Exercice 2.** Est il vrai ou faux que tout nombre entier suffisamment grand est somme de trois carrés de nombres entiers? Justifier votre réponse.

`TSVP ../..`

(3) **Exercice 3.** Soit p un nombre premier impair. On pose

$$n = \begin{cases} p & \text{si } p \equiv 1 \pmod 4, \\ 4p & \text{si } p \equiv -1 \pmod 4). \end{cases}$$

Soit $\zeta \in \mathbf{C}$ une racine primitive n-ième de l'unité. Montrer que le corps quadratique $\mathbf{Q}(\sqrt{p})$ est contenu dans le corps $\mathbf{Q}(\zeta)$.
`Indication.` On rappelle que la somme de Gauss

$$S = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) e^{2i\pi a/p}$$

satisfait $S^2 = (-1)^{(p-1)/2} p$.

(5) **Exercice 4.** On pose $\zeta = e^{i\pi/6}$ et $K = \mathbf{Q}(\zeta)$.
a) Décomposer le polynôme $X^{12}-1$ en facteurs irréductibles sur $\mathbf{Q}$. Pour chacun de ces facteurs, écrire les racines dans $\mathbf{C}$ sous forme de puissances de ζ. Quel est le corps de décomposition de ce polynôme sur $\mathbf{Q}$?
b) En déduire que le polynôme $X^2 - 3$ est irréductible sur $\mathbf{Q}(i)$. Quel est le corps de rupture de ce polynôme sur le corps $\mathbf{Q}(i)$?
Quel est le corps $K \cap \mathbf{R}$?
Indiquer trois corps distincts de degré 2 sur $\mathbf{Q}$ contenus dans K.
c) Montrer que si a est un entier positif impair, le polynôme $X^a - 3$ est irréductible sur K.

(2) **Exercice 5.** Quel est le nombre de facteurs irréductibles du polynôme ϕ_{728} sur $\mathbf{F}_3$?

(5) **Exercice 6.** Soient $\mathbf{F}_q$ un corps fini à q éléments de caractéristique p.
a) Soit K un corps contenant $\mathbf{F}_q$ et soit $\zeta \in K$ tel que $\zeta^{q-1} = -1$. Vérifier $\zeta^2 \in \mathbf{F}_q^\times$.
b) Combien y a-t-il de facteurs irréductibles dans la décomposition du polynôme $X^{2q-1} - X$ sur $\mathbf{F}_q$?
Quels sont leurs degrés?
Quel est le degré sur $\mathbf{F}_q$ d'un corps de décomposition de $X^{2q-1} - X$ sur $\mathbf{F}_q$?
`Indication.` *Distinguer le cas $p = 2$ du cas p impair.*

http://www.math.jussieu.fr/~miw/enseignement.html