Examen 7 Juin 2004

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

Barême approximatif: sur 20

Quand n est un entier positif on désigne par ϕ_n le n-ième polynôme cyclotomique.

(1) **Exercice 1.** Soit n un entier ≥ 1. On désigne par μ la fonction de Möbius. Vérifier

$$\phi_n(X) = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)}.$$

(4) **Exercice 2.** On pose $\zeta = e^{i\pi/4}$ et $R = \mathbf{Q}(\zeta)$.
a) Décomposer le polynôme $X^8 - 1$ 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 $X^2 - 2$ 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 $R \cap \mathbf{R}$?
Indiquer trois corps distincts de degré 2 sur $\mathbf{Q}$ contenus dans $\mathbf{R}$.
c) Montrer que si a est un entier positif impair, le polynôme $X^a - 2$ est irréductible sur R.

(4) **Exercice 3.**
a) Quels sont les nombres premiers p pour lesquels le polynôme $X^4 - 4$ a une racine dans $\mathbf{F}_p$?
b) Quels sont les nombres premiers p pour lesquels le polynôme $X^4 - 4$ est complètement décomposé dans $\mathbf{F}_p$?
c) Quand p est un nombre premier pour lequel le polynôme $X^4 - 4$ a une racine dans $\mathbf{F}_p$ mais n'est pas complètement décomposé dans $\mathbf{F}_p$, le décomposer en facteurs irréductibles sur $\mathbf{F}_p$.
Quelles sont les deux plus petites valeurs de p qui conviennent? Comment s'écrit cette décomposition dans ces deux cas particuliers?

TSVP ../..

(5) **Exercice 4.** Soient n un entier positif, G le groupe $(\mathbf{Z}/n\mathbf{Z})^\times$, p un nombre premier qui ne divise pas n et H le sous groupe de G engendré par la classe de p modulo n. On désigne par $C_1, \ldots, C_r$ les classes de G modulo H. Soit K le corps de décomposition du polynôme ϕ_n sur $\mathbf{F}_p$ et $\zeta \in K$ une racine primitive n-ième de l'unité. On définit des polynômes $P_1, \ldots, P_r$ dans $K[X]$ par

$$P_j(X) = \prod_{a \in C_j} (X - \zeta^a) \qquad 1 \leq j \leq r.$$

Montrer que ces polynômes appartiennent à $\mathbf{F}_p[X]$, qu'ils sont irréductibles sur $\mathbf{F}_p$ et que l'on a

$$\phi_n(X) = P_1(X) \cdots P_r(X).$$

(6) **Exercice 5.** Soit n un entier ≥ 3. On désigne par

$$P = \prod_{\substack{1 \leq a \leq n \\ (a,n)=1}} a$$

le produit des nombres entiers inférieurs à n et premiers avec n. Vérifier que les propriétés suivantes sont équivalentes
(i) $n \in \{4,\ p^a,\ 2p^a$ avec p premier impair et $a \geq 1\}$.
(ii) Le groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique.
(iii) Le groupe des caractères de $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique.
(iv) Si un entier a vérifie $a^2 \equiv 1 \pmod{n}$, alors $a \equiv \pm 1 \pmod{n}$.
(v) $P \equiv -1 \pmod{n}$.
(vi) $P \not\equiv 1 \pmod{n}$.