Université de Rouen
L2 Mathématiques - Informatiques
Année 2005-2006

Algèbre
Examen du 31 janvier 2006, durée 3h

L'USAGE DE LA CALCULATRICE N'EST PAS AUTORISÉ. L'USAGE DE TOUT DOCUMENT EST INTERDIT.

Une rédaction claire et concise sera appréciée. Toute affirmation devra être justifiée. Dans l'exercice 4 une question non résolue n'empêche pas de faire les suivantes, dans ce cas indiquez clairement que vous admettez le(s) résultat(s) de la question non faite.

Exercice 1. Trouver la décomposition en produit de cycles à supports disjoints, la signature, l'ordre des permutations suivantes de $\mathcal{S}_{10}$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 7 & 1 & 4 & 2 & 6 & 9 & 8 & 5 & 10 \end{pmatrix}$$
$$\tau = (10, 3, 4, 1) \circ (8, 7) \circ (4, 7) \circ (5, 6) \circ (2, 6) \circ (2, 9).$$

Donner une décomposition en produit de transpositions des permutations σ et τ. Calculer σ^{2006} et τ^{2006}.

Exercice 2. Soit le polynôme $P = X^8 + 2X^6 + 3X^4 + 2X^2 + 1$ et soit $j = \exp(2ik\pi/3)$ (j est une racine troisième de l'unité).

(a) calculer $1 + j + j^2$.

(b) Montrer que j est racine du polynôme P. Déterminer son ordre de multliplicité.

(c) Quelle conséquence peut-on tirer de la parité de P ?

(d) Quelle conséquence peut-on tirer du fait que les coefficients de P sont réels ?

(e) Décomposer P en produit de facteurs irréductibles dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.

Exercice 3. Décomposer en éléments simples dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$ la fraction rationnelle

$$\frac{X^3 + 4}{(X^2 - 1)(X^2 + 1)}.$$

On donnera toutes les étapes et explications des calculs.

Exercice 4.

Notations. Pour tout entier naturel non nul n, on pose $U_n = \{z \in \mathbb{C}\,;\, z^n = 1\} = \{\exp(2ik\pi/n)\,;\, k = 1, \dots, n\}$. La fonction d'Euler $\phi : \mathbb{N}^* \longmapsto \mathbb{N}^*$ est définie par $\phi(1) = 1$ et si $n > 1$, $\phi(n)$ est égal au nombres d'éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$.

Pour éviter de surcharger les notations, les éléments de l'ensemble $\mathbb{Z}/n\mathbb{Z}$ seront notés $a \bmod n$. Il faut donc comprendre que si a est un élément de $\mathbb{Z}$ alors $a \bmod n$ désigne la classe déquivalence de a pour la relation d'équivalence $x \equiv y \mod n$ si et seulement si $x - y \in n\mathbb{Z}$. Ainsi sans ambiguïté on pourra noter $2 \bmod 3$, $k \bmod p$, etc sans prendre une nouvelle notation pour les classes d'équivalence des différentes relations d'équivalence du type "mod n".

(a) Soient n et m deux entiers premiers entre eux. Le but cette question est de démontrer que $\phi(nm) = \phi(n)\phi(m)$.

-i- Soit ψ l'application définie par

$$\mathbb{Z} \mapsto \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$
$$a \mapsto \big(a \mod n, a \mod m\big).$$

Montrer que ψ est un morphisme d'anneau ($(\mathbb{Z}, +, \cdot)$ est l'anneau usuel des entiers relatifs tandis que $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +, \cdot)$ est muni de la structure usuelle d'anneau produit). Montrer que le noyau de ψ est l'idéal $nm\mathbb{Z}$.

-ii- Soient b et c deux entiers. On cherche à résoudre le système modulaire

(1) $$\begin{cases} a \equiv b \mod n \\ a \equiv c \mod m \end{cases}$$

Rappeler le théorème de Bezout pour le couple (n, m). En déduire qu'il existe p dans $\mathbb{N}$ tel que $pn \equiv 1 \mod m$. Montrer que l'entier $a = b + (c - b)pn$ est une solution de (1). En déduire que l'application ψ est surjective.

-iii- En déduire que l'application Ψ

$$\begin{aligned} \mathbb{Z}/nm\mathbb{Z} &\mapsto \big(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}\big) \\ a \mod nm &\mapsto \big(a \mod n, a \mod m\big) \end{aligned}$$

réalise un isomorphisme d'anneau.

-iv- A l'aide de la question précédente montrer que $x \bmod nm$ est inversible dans $\mathbb{Z}/nm\mathbb{Z}$ si et seulement si $x \bmod n$ et $x \bmod m$ sont inversibles respectivement dans $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$. En déduire que $\phi(nm) = \phi(n)\phi(m)$. Calculer $\phi(2)$, $\phi(3)$, $\phi(5)$, $\phi(15)$.

(b) Soit $n \in \mathbb{N}^*$. Montrer que dans $\mathbb{C}[X]$ on a $X^n - 1 = \displaystyle\prod_{k=1}^{n} \big(X - \exp(2ik\pi/n)\big)$.

(c) Soient d et n deux entiers naturels non nuls. Montrer que si $d|n$ (d divise n) alors $U_d \subset U_n$ et $X^d - 1 | X^n - 1$ dans $\mathbb{C}[X]$. Montrer que

$$\frac{X^n - 1}{X - 1} = X^{n-1} + X^{n-2} + \cdots + X + 1.$$

En déduire une formule analogue pour $\frac{X^n-1}{X^d-1}$ pour $d|n$.

(d) Soit n un entier naturel non nul. On rappelle que $U_n = \{z \in \mathbb{C}\,;\, z^n = 1\} = \{\exp(2ik\pi/n)\,;\, k = 1, \dots, n\}$ contient n éléments et que $(U_n, \cdot)$ est un groupe pour la multiplication usuelle dans $\mathbb{C}$. On pose

$$V_n = \{z \in U_n \,|\, z \text{ d'ordre } n \text{ dans le groupe multiplicatif } (U_n, \cdot)\},$$

autrement dit $z \in V_n$ si et seulement si ($z \in U_n$ et l'ordre de z dans le groupe $(U_n, \cdot)$ vaut n). On pose $\xi_n(X) = \displaystyle\prod_{z \in V_n} (X - z)$. Montrer que $\exp(2ik\pi/n) \in V_n$ si et seulement si $\mathrm{pgcd}(k, n) = 1$. En déduire $\xi_p(X)$ pour p premier.

(e) Montrer que $k \bmod n$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\mathrm{pgcd}(k, n) = 1$.

(f) Montrer que $\phi(n) = \deg(\xi_n(X))$. [indication : on pourra exprimer le degré de $\xi_n(X)$ en fonction du cardinal de l'ensemble V_n et utiliser les questions (d) et (e)]

(g) Montrer que U_n est réunion disjointe des V_d tels que $d|n$. En déduire que $X^n - 1 = \displaystyle\prod_{d|n} \xi_d(X)$ et que $n = \displaystyle\sum_{d|n} \phi(d)$.

(h) Calculer $\xi_1(X)$ et $\xi_2(X)$. À l'aide de la question (g) montrer que $X^4 - 1 = \xi_1(X)\xi_2(X)\xi_4(X)$. En déduire $\xi_4(X)$.