Université de Rouen
L2 Mathématiques - Informatiques
Année 2007-2008

Algèbre
Examen du 21 janvier 2008, durée 3h

L'usage des calculatrices, téléphones et/ou ordinateurs portables, baladeurs numériques, assistants personnels est interdit. L'usage de tout document n'est pas autorisé.

Une rédaction claire et concise sera appréciée. Toute affirmation devra être justifiée.

Exercice 1. On considère ici $\mathcal{S}_{10}$, l'ensemble des permutations de $A = \{1, 2, 3, \ldots, 10\}$.

(a) Pour tout $m \in \mathbb{Z}$, on pose $g_m : \mathbb{Z} \mapsto \mathbb{Z}$ définie par $g_m(i) = mi - 10\mathrm{E}(\frac{mi}{10}) + 1$, où $E(x)$ désigne la partie entière de x ($x \in \mathbb{R}$). Lesquelles des applications g_1, g_3 et g_6 sont éléments de $\mathcal{S}_{10}$? Déterminer alors leur ordre et leur signature.

(b) Soient c_1 et c_2 les deux cycles définis par $c_1 = (1\,3\,5\,7\,9)$ et $c_2 = (2\,7\,4\,3\,5)$ (avec la convention donnée en cours de l'écriture d'un cycle). On pose $\sigma = c_1 \circ c_2$. Donner la décomposition en cycles disjoints de σ, son ordre et sa signature. Calculer σ^{2008}.

Exercice 2. Montrer que l'ensemble $H = \left\{\frac{1+2p}{1+2q}\,;\, p, q \in \mathbb{Z}\right\}$ est un sous-groupe de $(\mathbb{Q}^*, \cdot)$ (l'ensemble des rationnels non nuls muni de la multiplication usuelle).

Exercice 3. Petit théorème de Fermat.
On définit pour $n \in \mathbb{N}^*$ et $k \in \mathbb{N}$ le coefficient binomial

$$\mathrm{C}_n^k = \binom{n}{k} = \begin{cases} \dfrac{n!}{k! \times (n-k)!} & \text{si } 0 \le k \le n, \\ 0 & \text{si } k \ge n+1. \end{cases}$$

(a) Démontrer que pour tout $1 \le k \le n$ on a $\mathrm{C}_n^k = \mathrm{C}_{n-1}^{k-1} + \mathrm{C}_{n-1}^k$. En déduire que, pour tout $n \ge 1$ et tout $k \ge 0$, la quantité C_n^k est un entier. *[on pourra faire une récurrence sur n.]*

(b) Démontrer que pour tout $1 \le k \le n$ on a $k \times \mathrm{C}_n^k = n \times \mathrm{C}_{n-1}^{k-1}$.

(c) Soient a et b deux réels. Démontrer, par récurrence, la formule du binôme, à savoir : $\forall n \in \mathbb{N}^*$

$$(a+b)^n = \sum_{k=0}^{n} \mathrm{C}_n^k\, a^k b^{n-k}.$$

On suppose désormais que $n \ge 2$ est un entier premier.

(d) En utilisant la question (b) montrer que si $1 \le k \le n-1$ alors n divise C_n^k.

(e) Montrer que si $a \in \mathbb{N}^*$ est tel que $a^n \equiv a\,[n]$ alors $(a+1)^n \equiv a+1\,[n]$.
[indication : on pourra utiliser les questions (c) et (d)].

(f) Montrer le petit théorème de Fermat : si a est un entier quelconque et n un nombre premier, alors $a^n - a$ est un multiple de n.

(g) Utiliser le petit théorème de Fermat pour démontrer que si n est un nombre premier et si a et n sont premiers entre eux alors $a^{n-1} \equiv 1\,[n]$.

(h) Trouver un exemple d'entiers a et m tels que $1 \le a \le m-1$ et $a^{m-1} \not\equiv 1\,[m]$.

Exercice 4. Soit n un entier supérieur (ou égal) à 2 et Q un polynôme de degré 2.

(a) Montrer que pour tout $P \in \mathbb{R}_n[X]$ le polynôme $2P'Q - nPQ'$ appartient à $\mathbb{R}_n[X]$. On note par la suite φ l'application de $\mathbb{R}_n[X]$ dans $\mathbb{R}_n[X]$ qui à P associe $\varphi(P) = 2P'Q - nPQ'$.

(b) On suppose dans cette question que $n = 2$ et que $Q = X^2 + uX + v$ (u et v dans $\mathbb{R}$). Le but est de déterminer $\ker(\varphi) = \{P \in \mathbb{R}_2[X]\,;\, \varphi(P) = 0\}$ en fonction de Q.

-i- Montrer que Q et Q' sont premiers entre eux si et seulement si $u^2 - 4v \neq 0$.

-ii- Soit $P \in \ker(\varphi)$ avec $P \neq 0$. Montrer que si Q et Q' sont premiers entre eux alors Q divise P. En déduire $\ker(\varphi)$ quand Q et Q' sont premiers entre eux.

Tournez la page S.V.P.

-iii- Soit $P \in \ker(\varphi)$ avec $P \neq 0$. Montrer que si Q possède une racine double α alors $P(\alpha) = 0$. En déduire que nécessairement $P = \lambda(X-\alpha)^2$, $\lambda \in \mathbb{R}$.

-iv- Déterminer $\ker(\varphi)$ en fonction de Q.

(c) On suppose dans cette question que Q est un polynôme de degré 2 qui n'admet pas de racine double. Aucune hypothèse n'est faite sur n : n est un entier naturel plus grand que 2 ($n \geq 2$). Le but est de déterminer $\ker(\varphi)$.

-i- Que peut-on dire du PGCD de Q et de Q' ? *[Justifier votre réponse]*

-ii- Soit $P \in \ker(\varphi)$. Montrer que si P est non nul alors Q divise P.

-iii- Soit $P \in \ker(\varphi)$ avec $P \neq 0$. Montrer que P s'écrit $P = RQ^k$ avec $k \geq 1$ et R un polynôme tels que Q ne divise pas R. Montrer que $2R'Q = (n-2k)RQ'$. En déduire que n est nécessairement pair ainsi que le degré de R.

-iv- Si n est pair déterminer $\ker(\varphi)$ en fonction de Q.

-v- Si n est impair déterminer $\ker(\varphi)$.

Question bonus. Déterminer $\ker(\varphi)$ dans le cas $n \geq 2$ quelconque et Q admettant une racine double.