

**10.01M**

SESSION 2010

---

**Filière MP**

**MATHÉMATIQUES MPI 1**

---

Épreuve commune aux ENS de Paris, Lyon et Cachan

---

Durée : 6 heures

---

*L'usage de calculatrice est interdit*

## NOTATIONS :

Dans tout le problème on considérera des groupes abéliens qui seront notés tantôt additivement, tantôt multiplicativement. Le but du problème est notamment de démontrer un théorème de structure pour certains groupes abéliens, dits *p-primaires* (voir partie III), qui vérifient de plus une certaine condition de finitude. Cet objectif est atteint dans la question VI.2.b.

Si  $(A, +)$  est un groupe abélien (noté additivement), on note  $0$  son élément neutre et  $-x$  le symétrique d'un élément  $x$  de  $A$ . On pose aussi, pour tout  $n \in \mathbf{N}^*$  et tout  $x \in A$ ,  $nx = x + \dots + x$  ( $n$  termes); on convient également que  $0x = 0$  et que  $nx = (-n)(-x)$  si  $n$  est un entier négatif. Pour  $n \in \mathbf{N}^*$ , on note  $A[n]$  le sous-groupe de  $A$  constitué des éléments  $x$  qui vérifient  $nx = 0$ , et  $nA$  le sous-groupe de  $A$  constitué des éléments  $x$  de  $A$  qui s'écrivent  $x = ny$  avec  $y \in A$  : en d'autres termes  $A[n]$  et  $nA$  sont respectivement le noyau et l'image du morphisme de groupes  $x \mapsto nx$  de  $A$  dans  $A$ .

Si  $G_1, \dots, G_r$  sont des groupes abéliens (notés additivement), le produit cartésien  $G_1 \times \dots \times G_r$  est muni de la structure de *groupe produit* définie par  $(x_1, \dots, x_r) + (y_1, \dots, y_r) = (x_1 + y_1, \dots, x_r + y_r)$ . En particulier, on note  $G^r$  le groupe produit  $G \times \dots \times G$  ( $r$  facteurs), avec la convention que  $G^r$  est le groupe trivial si  $r = 0$ .

On note  $S^1 = \{z \in \mathbf{C}, |z| = 1\}$  le groupe multiplicatif des nombres complexes de module 1, que l'on considère comme une partie du  $\mathbf{C}$ -espace vectoriel normé  $\mathbf{C}$ . Pour tout nombre premier  $p$ , on note  $U_p$  l'ensemble des éléments  $z$  de  $\mathbf{C}$  tels qu'il existe  $n \in \mathbf{N}^*$  vérifiant  $z^{p^n} = 1$ .

## QUELQUES RÉSULTATS ADMIS :

On pourra utiliser sans démonstration les résultats suivants :

**A.** *Soient  $A$  et  $G$  deux groupes abéliens. On suppose que pour tout sous-groupe  $B$  de  $A$  avec  $B \neq A$  et tout morphisme de groupes  $f : B \rightarrow G$ , il existe un sous-groupe  $B'$  de  $A$  contenant strictement  $B$  et un morphisme  $f' : B' \rightarrow G$  dont la restriction à  $B$  est  $f$ .*

Alors pour tout sous-groupe  $C$  de  $A$  et tout morphisme de groupes  $g : C \rightarrow G$ , il existe un morphisme de groupes  $h : A \rightarrow G$  dont la restriction à  $C$  est  $g$ .

**B.** Soit  $E$  un  $\mathbf{C}$ -espace vectoriel de dimension finie et soit  $(u_i)_{i \in I}$  une famille d'endomorphismes diagonalisables de  $E$  telle que  $u_i \circ u_j = u_j \circ u_i$  pour tous  $i, j$  de  $I$ . Alors il existe une base de  $E$  dans laquelle la matrice de tous les  $u_i$  est diagonale.

**C.** Soit  $f : G \rightarrow H$  un morphisme de groupes dont le noyau  $\ker f$  et l'image  $\text{Im } f$  sont tous deux finis; alors  $G$  est fini et son cardinal est le produit du cardinal de  $\ker f$  et du cardinal de  $\text{Im } f$ .

Si  $G$  est un groupe fini, le cardinal de tout sous-groupe de  $G$  divise celui de  $G$ .

Les parties **I** et **II** sont indépendantes, ainsi que les parties **IV** et **V**.

## I

**I.1** Soit  $f : S^1 \rightarrow S^1$  un morphisme de groupes multiplicatifs. On suppose que  $f$  est continu. Pour tout  $t$  de  $\mathbf{R}$ , on pose  $g(t) = f(e^{it})$ .

- a) Montrer que  $g$  est un morphisme de groupes de  $(\mathbf{R}, +)$  dans  $(S^1, \times)$ .
- b) En considérant la fonction  $F(x) = \int_x^{a+x} g(t)dt$  (pour  $a$  réel fixé), montrer que  $g : \mathbf{R} \rightarrow \mathbf{C}$  est une application dérivable (on pourra effectuer un changement de variable dans l'intégrale).
- c) Montrer que pour tout  $a$  de  $\mathbf{R}$ , on a  $g'(a) = g(a)g'(0)$ .
- d) Montrer qu'il existe  $\lambda \in \mathbf{R}$  tel que  $g(t) = e^{i\lambda t}$  pour tout  $t$  de  $\mathbf{R}$ .
- e) En déduire qu'il existe  $k \in \mathbf{Z}$  tel que  $f(z) = z^k$  pour tout  $z \in S^1$ .

Dans toute la suite de cette partie I, on fixe un nombre premier  $p$ .

**I.2.** a) Montrer que  $U_p$  est un sous-groupe infini de  $(S^1, \times)$ .

b) Montrer que  $U_p$  est une partie dense de  $S^1$ .

**I.3.** Soit  $f : U_p \rightarrow U_p$  un morphisme de groupes multiplicatifs. On suppose que  $z \mapsto f(z)$  est une application continue en  $z = 1$ .

a) Montrer que  $f$  est une application uniformément continue.

b) Soit  $(x_n)$  une suite d'éléments de  $U_p$  qui converge vers un élément  $x$  de  $S^1$ . Montrer que la suite  $(f(x_n))$  converge dans  $S^1$  (on pourra montrer que cette suite est de Cauchy).

c) Montrer qu'il existe une unique application continue  $\bar{f} : S^1 \rightarrow S^1$  tel que  $\bar{f}(x) = f(x)$  pour tout  $x$  de  $U_p$ . Que peut-on en déduire pour  $f$  ?

## II

On dit qu'un groupe abélien  $(A, +)$  est *divisible* si pour tout  $n \in \mathbf{N}^*$ , le morphisme de groupes  $x \mapsto nx$  est une surjection de  $A$  dans  $A$ .

**1.** Soit  $(A, +)$  un groupe abélien. Soient  $B$  un sous-groupe de  $A$  et  $a$  un élément de  $A$ . On note  $B_a$  le sous-groupe de  $A$  constitué des éléments  $x$  qui s'écrivent  $x = b + ka$  avec  $b \in B$  et  $k \in \mathbf{Z}$  (on ne demande pas de vérifier que  $B_a$  est bien un sous-groupe de  $A$ ).

Soit  $D$  un groupe abélien; on considère un morphisme de groupes  $f : B \rightarrow D$ .

a) On suppose qu'il n'existe pas d'entier  $m > 0$  tel que  $ma \in B$ . Montrer que tout élément  $x$  de  $B_a$  s'écrit de manière unique  $x = b + ka$  avec  $b \in B$  et  $k \in \mathbf{Z}$ . En déduire qu'il existe un morphisme de groupes  $g : B_a \rightarrow D$  tel que  $g(x) = f(x)$  pour tout  $x$  de  $B$ .

b) On suppose maintenant qu'il existe un entier  $m > 0$  tel que  $ma \in B$ . On choisit un tel  $m$  minimal et on pose  $b_0 = ma$ . On fait enfin l'hypothèse supplémentaire qu'il existe  $d \in D$  tel que  $f(b_0) = md$ . Montrer qu'on peut définir un morphisme de groupes  $g$  de  $B_a$  dans  $D$  par la formule  $g(b + ka) = f(b) + kd$  pour tout  $k \in \mathbf{Z}$  et tout  $b \in B$  (on pourra commencer par montrer que l'ensemble des  $n \in \mathbf{Z}$  tels que  $na \in B$  est un sous-groupe de  $\mathbf{Z}$  dont  $m$  est un générateur).

Vérifier alors que  $g(x) = f(x)$  pour tout  $x$  de  $B$ .

c) Montrer que si  $D$  est divisible, alors il existe un morphisme de groupes  $h : A \rightarrow D$  tel que  $h(x) = f(x)$  pour tout  $x$  de  $B$ .

**2.** Soit  $A$  un groupe abélien et soit  $D$  un sous-groupe divisible de  $A$ .

a) Montrer qu'il existe un morphisme  $\pi : A \rightarrow D$  tel que  $\pi(x) = x$  pour tout  $x$  de  $D$ .

b) En déduire qu'il existe un sous-groupe  $S$  de  $A$  tel que tout élément  $x$  de  $A$  s'écrit d'une manière unique  $x = d + s$  avec  $d \in D$  et  $s \in S$ , puis que  $A$  est isomorphe au groupe produit  $D \times S$ .

## III

Soit  $p$  un nombre premier. On dit qu'un groupe abélien (noté additive-ment)  $(A, +)$  est *p-primaire* si pour tout  $x$  de  $A$ , il existe un entier  $k \geq 1$  tel

que  $p^k x = 0$ . On dit que  $A$  est *p-divisible* si le morphisme de groupes  $x \mapsto px$  est une surjection de  $A$  dans  $A$ .

1. Montrer que  $(U_p, \times)$  est *p*- primaire. Est-il *p*- divisible ?
2. Pour quelles valeurs de  $m \in \mathbf{N}^*$  le groupe additif  $\mathbf{Z}/m\mathbf{Z}$  est-il *p*- primaire (respectivement *p*- divisible) ?
3. Soit  $n \in \mathbf{N}^*$ ; on note  $\mathrm{GL}_n(\mathbf{C})$  le groupe multiplicatif des matrices de taille  $n$  inversibles à coefficients dans  $\mathbf{C}$ . Soit  $G$  un sous-groupe abélien et *p*- primaire de  $\mathrm{GL}_n(\mathbf{C})$ . Montrer que  $G$  est isomorphe à un sous-groupe de  $(U_p)^n$ .
4. a) Soit  $m \in \mathbf{N}^*$  un nombre entier non divisible par  $p$ . Montrer que si  $(A, +)$  est un groupe abélien *p*- primaire, alors le morphisme de groupes  $x \mapsto mx$  est un isomorphisme de  $A$  dans  $A$ .  
b) En déduire que si  $A$  est un groupe abélien *p*- primaire et *p*- divisible, alors il est divisible.

*Dans toute la suite de cette partie III, on fixe un nombre premier  $p$  et un groupe abélien  $(A, +)$ .*

5. Montrer qu'on définit une structure de  $\mathbf{Z}/p\mathbf{Z}$ -espace vectoriel sur  $A[p]$  par la formule :

$$\bar{\lambda} \cdot x = \lambda x, \quad \lambda \in \mathbf{Z}, \quad x \in A[p]$$

où  $\bar{\lambda}$  désigne la classe de  $\lambda$  dans  $\mathbf{Z}/p\mathbf{Z}$ .

6. On suppose dans cette question III.6 que  $A[p]$  est fini.
  - a) Montrer que  $A[p]$  est isomorphe au groupe  $(\mathbf{Z}/p\mathbf{Z})^r$  pour un certain entier naturel  $r$ .
  - b) Montrer que pour tout  $k \in \mathbf{N}^*$  le groupe  $A[p^k]$  est fini de cardinal une puissance de  $p$  (on pourra considérer le morphisme  $u_k : A[p^{k+1}] \rightarrow A$  défini par  $u_k(x) = px$ ). En déduire qu'un groupe abélien fini est *p*- primaire si et seulement si son cardinal est une puissance de  $p$ .
  - c) Soit  $x_0 \in \bigcap_{k \in \mathbf{N}^*} p^k A$ . Montrer que l'équation  $px = x_0$  n'a qu'un nombre fini de solutions dans  $A$ ; en déduire qu'au moins l'une de ces solutions appartient encore à  $\bigcap_{k \in \mathbf{N}^*} p^k A$ . Que peut-on en conclure pour le groupe  $\bigcap_{k \in \mathbf{N}^*} p^k A$  ?

## IV

*Dans cette partie, on fixe un nombre premier  $p$  et un groupe abélien *p*- primaire  $A$ , qui vérifie de plus :  $A[p]$  est fini et  $\bigcap_{k \in \mathbf{N}^*} p^k A = \{0\}$ .*

1. Montrer qu'il existe un entier  $m \geq 1$  tel que  $p^m A \cap A[p] = \{0\}$ .
2. Montrer que  $A = A[p^m]$ , et en déduire que  $A$  est fini.

## V

*Dans toute cette partie V, on fixe un nombre premier  $p$  et un groupe abélien  $p$ - primaire et  $p$ - divisible  $A$  tel que  $A[p]$  soit fini. On note  $p^r$  le cardinal de  $A[p]$  (qui est une puissance de  $p$  d'après III.6.a).*

1. Soit  $k \geq 1$ . Montrer que le groupe  $A[p^k]$  est de cardinal  $p^{kr}$  (on pourra utiliser l'application  $u_k$  définie en III.6.b).

2. On suppose dans toute cette question V.2. que  $r = 1$  et on choisit  $a \neq 0$  dans  $A[p]$ .

a) Montrer qu'il existe une suite  $(x_n)_{n \in \mathbb{N}^*}$  d'éléments de  $A$  vérifiant  $x_1 = a$  et  $px_{n+1} = x_n$  pour tout  $n \in \mathbb{N}^*$ . Montrer qu'alors pour tout  $n \in \mathbb{N}^*$ ,  $x_n$  est un générateur du groupe  $A[p^n]$ .

b) En déduire que  $A$  est isomorphe au groupe multiplicatif  $(U_p, \times)$  (on pourra d'abord définir l'isomorphisme cherché sur  $A[p^n]$  pour  $n$  fixé).

3. On revient à  $r$  quelconque.

a) Montrer qu'il existe  $a_1, \dots, a_r$  dans  $A[p]$  tels que pour tout  $(k_1, \dots, k_r) \in \mathbb{Z}^r$ , l'égalité  $\sum_{i=1}^r k_i a_i = 0$  implique que tous les  $k_i$  sont divisibles par  $p$  (on pourra utiliser III.6.a).

b) Soit  $i \in \{1, \dots, r\}$ ; montrer qu'il existe une suite  $(x_{i,n})_{n \in \mathbb{N}^*}$  d'éléments de  $A$  vérifiant :  $x_{i,1} = a_i$  et  $px_{i,n+1} = x_{i,n}$  pour tout  $n \in \mathbb{N}^*$ . Montrer alors qu'on définit un isomorphisme de groupes de  $(\mathbb{Z}/p^n\mathbb{Z})^r$  sur  $A[p^n]$  par la formule :

$$(\bar{\lambda}_i)_{1 \leq i \leq r} \mapsto \sum_{i=1}^r \lambda_i x_{i,n}$$

où  $\bar{\lambda}_i$  désigne la classe dans  $\mathbb{Z}/p^n\mathbb{Z}$  de  $\lambda_i \in \mathbb{Z}$ .

c) Pour  $i \in \{1, \dots, r\}$  fixé, on note  $A_i$  l'ensemble des éléments  $x$  de  $A$  qui peuvent s'écrire  $x = kx_{i,n}$  avec  $n \in \mathbb{N}^*$  et  $k \in \mathbb{Z}$ . Montrer que  $A_i$  est un sous-groupe de  $A$  et que l'application

$$\prod_{i=1}^r A_i \rightarrow A, \quad (y_i)_{1 \leq i \leq r} \mapsto \sum_{i=1}^r y_i$$

est un isomorphisme de groupes.

d) En déduire que  $A$  est isomorphe au groupe multiplicatif  $(U_p)^r$ .

## VI

Soient  $p$  un nombre premier et  $A$  un groupe abélien  $p$ - primaire. Une famille  $(x_i)_{i \in I}$  d'éléments de  $A$  est dite *presque nulle* si  $x_i = 0$  pour tout indice  $i$  à l'exception d'un nombre fini d'entre eux.

On considère la famille  $(D_i)_{i \in I}$  de tous les sous-groupes  $p$ -divisibles de  $A$  et on appelle  $D$  l'ensemble des éléments  $x$  de  $A$  qui peuvent s'écrire  $x = \sum_{i \in I} x_i$  où  $(x_i)_{i \in I}$  est une famille presque nulle d'éléments de  $A$  telle que  $x_i \in D_i$  pour tout  $i$ .

**1.** Montrer que  $D$  est un sous-groupe divisible de  $A$  (on pourra utiliser III.4.b) et que tout sous-groupe  $p$ - divisible de  $A$  est inclus dans  $D$ .

**2.** On suppose de plus que  $A[p]$  est fini. Soit  $S$  un sous-groupe de  $A$  tel que tout élément  $x$  de  $A$  s'écrive d'une manière unique  $x = d + s$  avec  $d \in D$  et  $s \in S$  (l'existence de  $S$  est assurée par II.2.b).

a) Montrer que  $D = \bigcap_{k \in \mathbf{N}^*} p^k A$  (on pourra utiliser III.6.c)) et en déduire que  $S$  est fini (on pourra utiliser IV.2).

b) En déduire qu'il existe un entier  $r \in \mathbf{N}$  et un groupe abélien fini  $p$ - primaire  $F$  tels que  $A$  soit isomorphe au groupe produit  $F \times (U_p)^r$ .

**3.** On rappelle qu'un corps commutatif  $K$  est dit *algébriquement clos* si tout polynôme  $P$  de  $K[X]$  est scindé.

Soit  $K$  un corps commutatif algébriquement clos de caractéristique zéro. Soit  $p$  un nombre premier. On note  $\mu_{p^\infty}$  l'ensemble des éléments  $x$  de  $K$  tels qu'il existe  $k \in \mathbf{N}^*$  avec  $x^{p^k} = 1$ . Montrer que  $\mu_{p^\infty}$  est un sous-groupe du groupe multiplicatif  $K^*$  de  $K$ , et que  $\mu_{p^\infty}$  est isomorphe à  $U_p$ .

**FIN DE L'EPREUVE.**

