**ENS 2010, MP, Maths 1**

## I

1. a) Pour tout $t \in \mathbb{R}$, on pose $\varphi(t) = e^{it}$. $\varphi$ est un morphisme de $(\mathbb{R}, +)$ dans $(S^1, \times)$ . Alors $g = f \circ \varphi$ est un morphisme de groupes (c'est la composée de deux morphismes).

   b) $f$ et $\varphi$ sont continus, donc $g$ est continu. En appelant $G$ une primitive de $g$ sur $\mathbb{R}$, on a :

   $$\forall x \in \mathbb{R}, \quad F(x) = G(a+x) - G(x)$$

   Donc $F$ est dérivable sur $\mathbb{R}$. Par ailleurs, le changement de variable affine $u = t - x$ dans l'intégrale définissant $F(x)$ donne :

   $$\forall x \in \mathbb{R}, \quad F(x) = \int_x^{a+x} g(t)\,\mathrm{d}t = \int_0^a g(x+u)\,\mathrm{d}u = \int_0^a g(x)\,g(u)\,\mathrm{d}u = g(x)\int_0^a g(u)\,\mathrm{d}u$$

   Si, pour tout $a \in \mathbb{R}$, $\int_0^a g(u)\,\mathrm{d}u = 0$, alors $g = 0$ (dériver la relation précédente par rapport à $a$). C'est impossible puisque $g$ est à valeurs dans $S^1$. Ainsi, il existe $a \in \mathbb{R}$ tel que $\int_0^a g(u)\,\mathrm{d}u \neq 0$. Pour cette valeur de $a$ :

   $$\forall x \in \mathbb{R}, \quad g(x) = \frac{1}{\int_0^a g(u)\,\mathrm{d}u}\,F(x)$$

   Cette écriture montre que $g$ est dérivable sur $\mathbb{R}$.

   c) On a la relation :

   $$\forall x,\, x' \in \mathbb{R}, \quad g(x+x') = g(x)\,g(x')$$

   On dérive la relation précédente par rapport à $x'$ et on a :

   $$\forall x,\, x' \in \mathbb{R}, \quad g'(x+x') = g(x)\,g'(x')$$

   Avec $x = a$ et $x' = 0$ on obtient la relation souhaitée :

   $$\boxed{\forall a \in \mathbb{R}, \quad g'(a) = g(a)\,g'(0)}$$

   d) La relation précédente nous apprend que $g$ est solution d'une équation différentielle linéaire du premier ordre. On sait donc qu'il existe $\alpha,\, \mu \in \mathbb{C}$ tels que :

   $$\forall t \in \mathbb{R}, \quad g(t) = \alpha\, e^{\mu\, t}$$

   Comme $g(0) = 1$ (puisque $g$ est un morphisme), $\alpha = 1$. Alors $g(t) = e^{\mu\, t}$ avec $\mu = g'(0)$. Comme $g$ est une application à valeurs dans $S^1$, alors, pour tout $t \in \mathbb{R}$, $|g(t)|^2 = 1$ soit $g(t)\overline{g(t)} = 1$. En dérivant cette relation, on obtient $g'(t)\overline{g(t)} + g(t)\overline{g'(t)} = 0$ soit $2\,\mathrm{Re}(g'(t)\,g(t)) = 0$. On a donc en particulier $\mathrm{Re}(g'(0)\,g(0)) = 0$ i.e. $\mathrm{Re}(g'(0)) = 0$. On peut donc bien poser $\mu = g'(0) = i\,\lambda$ avec $\lambda \in \mathbb{R}$.

   e) Pour tout $t \in \mathbb{R}$, $g(t) = f(e^{it}) = e^{i\lambda\, t}$. En particulier $f(e^{i\,2\pi}) = f(1) = 1 = e^{i\lambda\,2\pi}$ car $f$ est un morphisme de groupes. On en déduit que $\lambda\,2\pi \in 2\pi\mathbb{Z}$ soit $\lambda \in \mathbb{Z}$. En posant $\lambda = k$, on alors :

   $$\forall t \in \mathbb{R}, \quad f(e^{it}) = e^{i\,k\,t} = (e^{it})^k$$

   d'après la formule de Moivre. Comme $e^{it}$ parcourt $S^1$ lorsque $t$ parcourt $\mathbb{R}$ ($\varphi$ est une application surjective), alors :

   $$\boxed{\forall z \in S^1, \quad f(z) = z^k}$$

2. a)

   $$U_p = \{z \in \mathbb{C} \;/\; \exists n \in \mathbb{N}^*,\; z^{p^n} = 1\}$$

   En appelant, pour tout $k \in \mathbb{N}^*$, $\mathbb{U}_k$ l'ensemble des racines $k$-èmes de l'unité ($\mathbb{U}_k = \{z \in \mathbb{C} \;/\; z^k = 1\}$), on sait que $\mathbb{U}_k$ est un sous-groupe fini de $(S^1, \times)$ de cardinal $k$. On a de plus :

   $$U_p = \bigcup_{n \in \mathbb{N}^*} \mathbb{U}_{p^n}$$

$U_p$ est donc non vide et si $z$, $z' \in U_p$, alors il existe des entiers $n$, $n' \in \mathbb{N}^*$ tels que :

$$z^{p^n} = 1 \qquad \text{et} \qquad z'^{p^{n'}} = 1$$

Alors :

$$\left(\frac{z}{z'}\right)^{p^{\max(n,\,n')}} = \frac{z^{p^{\max(n,\,n')}}}{z'^{p^{\max(n,\,n')}}} = \frac{1}{1} = 1$$

et donc $z/z' \in U_p$. $U_p$ est donc un sous-groupe de $(S^1, \times)$.

Comme $\mathbb{U}_{p^n} \subset U_p$ pour tout $n \in \mathbb{N}^*$ et que $\mathbb{U}_{p^n}$ est de cardinal $p^n$, alors $U_p$ est infini.

b) On sait que l'application $\varphi : \mathbb{R} \to S^1,\ t \mapsto e^{it}$ est un morphisme de groupes. La partie $\varphi^{-1}(U_p)$ est donc un sous-groupe de $(\mathbb{R}, +)$ qui contient tous les réels de la forme $2\pi/p^n$. $\varphi^{-1}(U_p)$ est donc dense dans $\mathbb{R}$. Comme $\varphi$ est surjective et continue, $U_p$ est dense dans $S^1$.

3. a) Soit $\varepsilon > 0$ fixé. Comme $f$ est continue en 1 :

$$\exists \eta > 0 \ / \ \forall z \in U_p,\ |z-1| \leqslant \eta \ \Rightarrow\ |f(z)-1| \leqslant \varepsilon$$

Prenons $z$, $z' \in U_p$ tels que $|z'-z| \leqslant \eta$. Or :

$$|z'-z| = \left|z'\left(\frac{z}{z'}-1\right)\right| = |z'|\left|\frac{z}{z'}-1\right| = \left|\frac{z}{z'}-1\right|$$

car $U_p \subset S^1$. Ainsi $\left|\frac{z}{z'}-1\right| \leqslant \eta$ et de plus $\frac{z}{z'} \in U_p$ car $U_p$ est un sous-groupe de $S^1$. On en déduit que $\left|f\left(\frac{z}{z'}\right)-1\right| \leqslant \varepsilon$ puis $\left|\frac{f(z)}{f(z')}-1\right| \leqslant \varepsilon$ (car $f$ est un morphisme) et enfin $|f(z)-f(z')| \leqslant \varepsilon$ (car $|f(z')| = 1$). $f$ est donc bien une application uniformément continue.

b) La suite $(x_n)$ converge donc elle est de Cauchy. Comme $f$ est uniformément continue, la suite $(f(x_n))$ est de Cauchy dans $S^1$. Comme $\mathbb{C}$ est complet, cette suite converge dans $\mathbb{C}$ et comme $S^1$ est fermé, elle converge en fait dans $S^1$.

c) Il s'agit en fait de prouver le théorème de prolongement des applications uniformément continues.

• unicité :

Supposons qu'il existe deux applications continues $\overline{f}$ et $\tilde{f}$ de $S^1$ dans $S^1$ telles que :

$$\forall x \in U_p, \quad \overline{f}(x) = \tilde{f}(x) = f(x)$$

Soit $x \in S^1$. Comme $U_p$ est dense dans $S^1$, il existe une suite $(x_n)$ d'éléments de $U_p$ qui converge vers $x$. La continuité de $\overline{f}$ et $\tilde{f}$ assure alors que $\overline{f}(x) = \tilde{f}(x)$. On a donc $\overline{f} = \tilde{f}$.

• existence :

Soit $x \in S^1$. On va définir $\overline{f}(x)$ par :

$$\overline{f}(x) = \lim_{n \to +\infty} f(x_n)$$

où $(x_n)$ est une suite de $U_p$ qui converge vers $x$ (la limite existant d'après la question 3.b)). Pour que cette définition ait un sens il faut montrer que si $(y_n)$ est une autre suite de $U_p$ qui converge vers $x$, alors $\lim\limits_{n \to +\infty} f(x_n) = \lim\limits_{n \to +\infty} f(y_n)$. Pour cela il suffit de remarquer que $x_n - y_n$ converge vers 0, ce qui entraîne (par uniforme continuité de $f$) que $f(x_n) - f(y_n)$ converge également vers 0.

Si $x \in U_p$, $\overline{f}(x) = f(x)$, car la suite constante égale à $x$ converge vers $x$.

• continuité de $\overline{f}$ :

On peut montrer que $\overline{f}$ est une application uniformément continue. Soit $\varepsilon > 0$. Soit $x$, $x' \in S^1$ tels que $|x-x'| \leqslant \eta/2$ ($\eta$ est défini dans la question 3.a)). Soit enfin deux suites $(x_n)$ et $(x'_n)$ d'éléments de $U_p$ convergeant respectivement vers $x$ et $x'$. Pour $n$ suffisamment grand on a alors $|x_n - x'_n| \leqslant \eta$ et donc $|f(x_n) - f(x'_n)| \leqslant \varepsilon$. Un passage à la limite donne alors $|\overline{f}(x) - \overline{f}(x')| \leqslant \varepsilon$.

$\overline{f}$ est donc uniformément continue et donc en particulier continue.

• D'après la question 1.e), on peut alors en déduire :

$$\exists k \in \mathbb{Z} \ / \ \forall x \in U_p,\ f(x) = x^k$$

## II

1. On a :

$$B_a = \{b + k\,a,\ b \in B,\ k \in \mathbb{Z}\}$$

$B_a$ est donc le groupe engendré par $B$ et $a$ i.e. le plus petit sous-groupe de $A$ contenant $B$ et $a$.

a) Soit $x$ un élément de $B_a$. Il s'écrit, par définition de $B_a$, sous la forme $x = b + k\,a$ avec $b \in B$ et $k \in \mathbb{Z}$. S'il s'écrit d'une autre façon $x = b' + k'\,a$ avec $b' \in B$ et $k' \in \mathbb{Z}$ avec $k \leqslant k'$, alors $b - b' = (k' - k)\,a$. Comme $b - b' \in B$, l'hypothèse faite dans cette question entraîne $k' - k = 0$, puis $b - b' = 0$. L'écriture précédente est donc unique.

On peut alors définir une application $g$ sur $B_a$ de la façon suivante. On fixe $d \in D$ et pour tout $x$ de $B_a$ (s'écrivant de façon unique $x = b + k\,a$), on pose :

$$g(x) = f(b) + k\,d$$

On laisse au lecteur le soin de vérifier que $g$ est bien un morphisme de groupes prolongeant $f$.

b) L'application $\psi : \mathbb{Z} \to A,\ n \mapsto na$ est un morphisme de groupes. L'ensemble $G = \psi^{-1}(B)$ est donc un sous-groupe de $(\mathbb{Z}, +)$. Dans ce cas $G = m\,\mathbb{Z}$, ce qui signifie que $m$ est un générateur de $G$.

Montrons que la définition de $g$ fournie par l'énoncé a un sens. Pour cela prenons $x$ qui s'écrit de deux façons différentes $x = b + k\,a = b' + k'\,a$ avec $b, b' \in B$, $k, k' \in \mathbb{Z}$ , $k \leqslant k'$ et montrons que $f(b) + k\,d = f(b') + k'\,d'$.

$*$ Si $k = k'$, alors $b = b'$ et il n'y rien à démontrer.

$*$ Si $k < k'$, on a $b - b' = (k' - k)\,a$ donc $(k' - k)\,a \in B$. Il existe alors $l \in \mathbb{Z}$ tel que $k' - k = m\,l$. On a donc :

$$f(b - b') = f((k' - k)\,a) = f(m\,l\,a) = l\,f(m\,a) = l\,f(b_0) = l\,m\,d = (k' - k)\,d$$

On en déduit bien que $f(b) + k\,d = f(b') + k'\,d'$.

On vérifie alors sans peine que $g$ est un morphisme de groupes.

c) On suppose que $D$ est divisible. On utilise le résultat admis **A.**. Prenons un sous-groupe $B$ de $A$ avec $B \neq A$ et $f : B \to D$ un morphisme de groupes. Il existe alors $a \in A \setminus B$. Alors $B_a$ est un sous-groupe de $A$ contenant strictement $B$ et $g : B_a \to D$ est un morphisme de groupes dont la restriction à $B$ est $f$.

Ce morphisme $g$ existe bien d'après les questions 1.a) et b) de cette partie :

• S'il n'existe pas de $m > 0$ tel que $ma \in B$ cela résulte de la question a) ;
• S'il existe $m > 0$ tel que $ma \in B$, alors, puisque $D$ est divisible, il existe $d \in D$ tel que $f(b_0) = m\,d$ et donc la question b) s'applique.

Il existe bien un morphisme de groupes $h : A \to D$ tel que sa restriction à $B$ est $f$.

2. a) $\mathrm{Id}_D : D \to D,\ x \mapsto x$ est un morphisme de groupes. Comme $D$ est divisible, la question 1.c) donne l'existence d'un morphisme de groupes $\pi : A \to D$ dont la restriction à $D$ est $\mathrm{Id}_D$.

b) On prend $S = \ker \pi$ qui est un sous-groupe de $A$. On montre par analyse-synthèse que :

$$\forall x \in A,\ \exists!(d, s) \in D \times S \ /\ x = d + s$$

Soit $x \in A$.

$*$ Si $d$ et $s$ existent alors $\pi(x) = \pi(d + s) = \pi(d) + \pi(s) = d$ et $s = x - d = x - \pi(x)$ donc $d$ et $s$ sont uniques.

$*$ On a :

$$x = \pi(x) + (x - \pi(x))$$

avec $d = \pi(x) \in D$ et $s = x - \pi(x) \in \ker \pi = S$, donc $d$ et $s$ existent.

On va alors noter $A = D \oplus S$ (comme dans les espaces vectoriels) et on dira que $A$ est somme directe interne des sous-groupes $D$ et $S$. On laisse au lecteur le soin de vérifier que l'application $D \times S \to A,\ (d, s) \mapsto d + s$ est un isomorphisme de groupes. Le fait que $A$ et $D \times S$ sont isomorphes sera noté $A \simeq D \times S$. [1]

1. Le groupe produit $D \times S$ est appelé parfois somme directe externe des groupes $D$ et $S$.

## III

1. Puisque dans le groupe $(U_p, \times)$ la loi est notée multiplicativement, $U_p$ est $p$-primaire si pour tout $x$ de $U_p$, il existe $k \in \mathbb{N}^*$ tel que $x^{p^k} = 1$, ce qui est vrai par définition de $U_p$.

   Pour montrer que $U_p$ est $p$-divisible, il faut justifier que l'application $U_p \to U_p,\ x \mapsto x^p$ est surjective. Considérons $y \in U_p$. Le polynôme $X^p - y$ admet une racine $x$ dans $\mathbb{C}$, d'après le théorème de d'Alembert-Gauss. On a $x^p = y$ et il existe $k \in \mathbb{N}^*$ tel que $y^{p^k} = 1$. Alors :

   $$(x^p)^{p^k} = x^{p\,p^k} = x^{p^{k+1}} = 1$$

   donc $x \in U_p$. $U_p$ est donc bien $p$-divisible.

2. Soit $m \in \mathbb{N}^*$.

   $*$ **La condition pour que $\mathbb{Z}/m\mathbb{Z}$ soit $p$-primaire est que $m$ soit un puissance de $p$ :**

   • Si $m$ est une puissance de $p$ ($m = p^l$ avec $l \in \mathbb{N}^*$), pour tout $x \in \mathbb{Z}/m\mathbb{Z}$, $p^l x = m\,x = 0$, donc $\mathbb{Z}/m\mathbb{Z}$ est $p$-primaire.

   • Si $m$ n'est pas une puissance de $p$ ($m = p^l\,q$ avec $l \in \mathbb{N}$, $q \in \mathbb{N}^*$ et $p \not| q$). Prenons $x = 1 \in \mathbb{Z}/m\mathbb{Z}$. Pour tout $k \in \mathbb{N}^*$, $p^k\,x = p^k \neq 0$ car $m$ de divise pas $p^k$. $\mathbb{Z}/m\mathbb{Z}$ n'est donc pas $p$-primaire.

   $*$ **La condition pour que $\mathbb{Z}/m\mathbb{Z}$ soit $p$-divisible est que $m$ et $p$ soient premiers entre eux :**

   • Si $m$ et $p$ sont premiers entre eux, il existe des entiers $a$ et $b$ tels que $a\,m + b\,p = 1$. Si $k$ est un entier, on a donc $k\,a\,m + k\,b\,p = k$. Ainsi $k\,b\,p \equiv k\,[m]$. Ceci prouve que le morphisme $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z},\ x \mapsto p\,x$ est surjectif, donc que $\mathbb{Z}/m\mathbb{Z}$ est $p$-divisible.

   • Si $\mathbb{Z}/m\mathbb{Z}$ est $p$-divisible, le morphisme $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z},\ x \mapsto p\,x$ est surjectif donc il existe $\overline{k} \in \mathbb{Z}/m\mathbb{Z}$ tel que $p\,\overline{k} = 1$, $\overline{k}$ désignant la classe de $k$ dans $\mathbb{Z}/m\mathbb{Z}$. Il existe donc $l \in \mathbb{Z}$ tel que $p\,k + l\,m = 1$ donc $m$ et $p$ sont premiers entre eux.

3. Pour tout $M \in G$, il existe $k \in \mathbb{N}^*$ tel que $M^{p^k} = I_n$. Le polynôme $Q = X^{p^n} - 1$ est scindé à racines simples sur $\mathbb{C}$ et il annule $M$, donc $M$ est diagonalisable. $M$ est donc semblable à une matrice diagonale $D = \mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$, où $\lambda_i \in U_p$ pour tout $i \in [\![1, n]\!]$. Il existe donc $P \in \mathrm{GL}_n(\mathbb{C})$ telle que $D = PMP^{-1}$. Comme $G$ est commutatif, le résultat admis **B.** nous apprend que $P$ peut-être choisie la même pour toutes les matrices $M$ de $G$.

   On considère alors l'isomorphisme $\psi : \mathrm{GL}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C}),\ M \mapsto PMP^{-1}$. $\psi(G)$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ formé de matrices diagonales, $p$-primaire, il est donc isomorphe à un sous-groupe de $(U_p)^n$ (l'isomorphisme étant défini par $\psi(G) \to (U_p)^n,\ \mathrm{Diag}(\lambda_1, \ldots, \lambda_n) \mapsto (\lambda_1, \ldots, \lambda_n)$). $G$ est donc isomorphe à un sous-groupe de $(U_p)^n$.

4. a) Soit $\rho : A \to A,\ x \mapsto m\,x$ où $p$ ne divise pas $m$. $\rho$ est un morphisme de groupes.

      • Il est injectif, car si $x \in \ker\rho$, alors $m\,x = 0$. Comme $A$ est $p$-primaire, il existe $k \in \mathbb{N}^*$ tel que $p^k x = 0$. $p^k$ et $m$ sont premiers entre eux, donc il existe des entiers $a$ et $b$ tels que $a\,p^k + b\,m = 1$. On en déduit que $a\,p^k x + b\,m\,x = x$, puis que $x = 0$.

      • Il est surjectif, car si $x \in A$, avec les mêmes notations que ci-dessus, on obtient : $a\,p^k x + b\,m\,x = x$ soit $m\,b\,x = x$.

   b) Soit $A$ un groupe $p$-primaire et $p$-divisible. Soit $n \in \mathbb{N}^*$. On écrit $n$ sous la forme $n = p^l m$ avec $l \in \mathbb{N}$, $m \in \mathbb{N}^*$ tel que $p$ ne divise pas $m$. L'application $A \to A,\ x \mapsto n\,x$ est la composée de $x \mapsto m\,x$, surjective d'après la question a), et de $x \mapsto p\,x$ ($l$ fois), surjective car $A$ est $p$-primaire. Une composée de surjections étant une surjection, $A \to A,\ x \mapsto n\,x$ est une surjection, donc $A$ est divisible.

5. $A[p] = \{x \in A \ /\ p\,x = 0\}$ est un sous-groupe de $A$, donc $A[p]$ est un groupe abélien. L'énoncé nous donne une loi externe sur $A[p]$ qui est bien définie car si $\lambda$, $\lambda' \in \mathbb{Z}$ sont tels que $\overline{\lambda} = \overline{\lambda'}$, alors $\lambda - \lambda' = p\,k$ avec $k \in \mathbb{Z}$. Alors $(\lambda - \lambda')\,x = 0$ car $x \in A[p]$ et donc $\lambda\,x = \lambda'\,x'$.

Cette loi vérifie les quatre propriétés suivantes :

$\forall \lambda,\, \mu \in \mathbb{Z},\ \forall x,\, y \in A[p]$ :

$* \ (\overline{\lambda} + \overline{\mu}) \cdot x = \overline{\lambda} \cdot x + \overline{\mu} \cdot x\,;$

$* \ \overline{\lambda} \cdot (x + y) = \overline{\lambda} \cdot x + \overline{\lambda} \cdot y\,;$

$* \ (\overline{\lambda} \times \overline{\mu}) \cdot x = \overline{\lambda} \cdot (\overline{\mu} \cdot x)\,;$

$* \ \overline{1} \cdot x = x.$

Vérifions à titre d'exemple la première d'entre elles :

$$(\overline{\lambda} + \overline{\mu}) \cdot x = \overline{\lambda + \mu} \cdot x = (\lambda + \mu)\, x = \lambda\, x + \mu\, x = \overline{\lambda} \cdot x + \overline{\mu} \cdot x$$

6. a) L'ensemble $A[p]$ est supposé fini. Le $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $A[p]$ est donc de dimension finie (car il admet pour famille génératrice finie la famille de tous les éléments de $A[p]$).

   Dans le cas où $A[p] \neq \{0\}$, $A[p]$ admet une base $(e_1, \ldots, e_r)$ avec $r \in \mathbb{N}^*$. L'application $(\mathbb{Z}/p\mathbb{Z})^r \to A[p],\ (x_1, \ldots, x_r) \mapsto \sum_{i=1}^{r} x_i\, e_i$ est alors un isomorphisme d'espaces vectoriels, donc de groupes. Si $A[p] = \{0\}$, alors on peut prendre $r = 0$.

   b) Montrons par récurrence que pour tout $k \in \mathbb{N}^*$, $A[p^k]$ est fini de cardinal une puissance de $p$.

   Le résultat est vrai pour $k = 1$. En effet, $A[p]$ est fini, de cardinal $p^r$ (d'après la question précédente). On suppose la propriété vraie pour $k \in \mathbb{N}^*$. Le morphisme $u_k$ défini dans l'énoncé est tel que $\operatorname{Im} u_k \subset A[p^k]$. Par hypothèse de récurrence, $\operatorname{Im} u_k$ est donc fini. Par ailleurs $\ker u_k \subset A[p]$ donc $\ker u_k$ est fini. D'après le résultat admis **C.**, l'ensemble $A[p^{k+1}]$ est donc fini et son cardinal est égal au produit des cardinaux de $\operatorname{Im} u_k$ et de $\ker u_k$. $\operatorname{Im} u_k$ est un sous-groupe de $A[p^k]$ donc le cardinal de $\operatorname{Im} u_k$ divise le cardinal de $A[p^k]$. Par l'hypothèse de récurrence, le cardinal de $\operatorname{Im} u_k$ est donc une puissance de $p$. On démonte de même que le cardinal de $\ker u_k$ est une puissance de $p$. La propriété est donc vraie pour $k + 1$.

   Soit $A$ un groupe abélien fini. Montrons qu'il est $p$-primaire si et seulement si son cardinal est une puissance de $p$.

   Si $A$ est $p$-primaire, pour tout $x \in A$ il existe $k_x \in \mathbb{N}^*$ tel que $p^{k_x} x = 0$. On pose $k = \max_{x \in A} k_x$. On a $p^k x = 0$ soit $x \in A[p^k]$. On vient donc de prouver que $A \subset A[p^k]$ donc que $A = A[p^k]$. De plus $A[p]$ est fini car $A[p] \subset A$. Le résultat du début de cette question s'applique et donne que le cardinal de $A = A[p^k]$ est une puissance de $p$.

   Si le cardinal de $A$ est une puissance de $p$, $\operatorname{card}(A) = p^k$ avec $k \in \mathbb{N}$. On sait que :

   $$\forall x \in A, \quad \operatorname{card}(A)\, x = 0$$

   ce qui signifie que $A$ est $p$-primaire.

   c) Soit $x_0 \in \bigcap_{k \in \mathbb{N}^*} p^k A$. En particulier $x_0 \in p\, A$ donc l'équation $p\, x = x_0$ a au moins une solution $x_1 \in A$. L'ensemble des solutions de l'équation précédente est alors $x_1 + A[p]$. Cet ensemble est fini, car $A[p]$ est fini.

   Soit $x_0 \in \bigcap_{k \in \mathbb{N}^*} p^k A$. Il existe alors une suite $(x_k)$ d'éléments de $A$ telle que pour tout $k \in \mathbb{N}^*$, $x_0 = p^k x_k$. Alors $p\, p^{k-1} x_k = x_0$ donc $p^{k-1} x_k$ est solution de $p\, x = x_0$. Comme cette équation admet un nombre fini de solutions il existe une application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ strictement croissante telle que, pour tout $k \in \mathbb{N}^*$, $p^{\varphi(k)-1} x_{\varphi(k)} = y$, $y$ étant un élément fixe de $A$, solution de $p\, x = x_0$. Comme $\lim_{k \to +\infty} \varphi(k) = +\infty$, alors, pour tout $l \in \mathbb{N}^*$, il existe $k \in \mathbb{N}^*$ tel que $\varphi(k) - 1 \geqslant l$. Or $y \in p^{\varphi(k)-1} A$ et donc $y \in p^l A$. Finalement $y \in \bigcap_{l \in \mathbb{N}^*} p^l A$, ce qu'il fallait démontrer.

   Posons $A' = \bigcap_{k \in \mathbb{N}^*} p^k A$, qui est un sous-groupe de $A$ (c'est une intersection de sous-groupes de $A$). Le morphisme de groupes $A' \to A',\ x \mapsto p\, x$ est surjectif, ce qui signifie que $A'$ est $p$-divisible.

## IV

1. On emploie une technique similaire à celle utilisée pour faire la question III.6.c). On observe tout d'abord que pour tout $m \geqslant 1$, $A[p^m] \subset A[p^{m+1}]$. Montrons qu'il existe $m \in \mathbb{N}^*$ tel que $A[p^m] = A[p^{m+1}]$.

   On raisonne par l'absurde en supposant que pour tout $m \in \mathbb{N}^*$, on a $A[p^m] \subsetneq A[p^{m+1}]$. Il existe donc $a_m \in A[p^{m+1}] \setminus A[p^m]$ ce qui signifie que $p^{m+1}a_m = 0$ et que $p^m a_m \neq 0$. Pour tout $m \in \mathbb{N}^*$, on a donc $p^m a_m \in A[p]$. Comme $A[p]$ est fini, il existe $a_0 \in A[p]$ et une application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ telle que, pour tout $k \in \mathbb{N}^*$, $p^{\varphi(k)} a_{\varphi(k)} = a_0$. Par hypothèse, $a_0 \neq 0$. De plus $a_0 \in p^{\varphi(k)}A$, pour tout $k \in \mathbb{N}^*$ donc $a_0 \in p^l A$ pour tout $l \in \mathbb{N}^*$. Finalement, $a_0 \in \bigcap_{l\in\mathbb{N}^*} p^l A$, ce qui est en contradiction avec l'hypothèse $\bigcap_{l\in\mathbb{N}^*} p^l A = \{0\}$.

   Montrons alors que $p^m A \cap A[p] = \{0\}$. Soit $x \in p^m A \cap A[p]$. Alors $x = p^m a$ avec $a \in A$ et $p\,x = 0$. Ainsi $p^{m+1}a = 0$ i.e. $a \in A[p^{m+1}]$. On en déduit que $a \in A[p^m]$ soit $x = p^m a = 0$.

2. Comme $A[p^m] = A[p^{m+1}]$, alors pour tout $k \geqslant m$, $A[p^{k+1}] = A[p^k]$. En effet : $A[p^k] \subset A[p^{k+1}]$ est toujours vraie. On montre l'inclusion réciproque : si $x \in A[p^{k+1}]$, alors $p^{k+1}x = 0$. Ainsi $p^{m+1}\left(p^{k-m}x\right) = 0$ soit $p^{k-m}x \in A[p^{m+1}] = A[p^m]$. Finalement, $p^m\left(p^{k-m}x\right) = 0$, soit $x \in A[p^k]$.

   Comme $A$ est $p$-primaire, $A = \bigcup_{k\in\mathbb{N}^*} A[p^k]$. D'après ce qui précède, $A = \bigcup_{k=1}^{m} A[p^k]$ puis $A = A[p^m]$. On a démontré dans la question III.6.b) que $A[p^m]$ est fini (car $A[p]$ est fini). On en déduit bien que $A$ est fini.

## V

*On peut remarquer pour commencer qu'il est possible a priori que $A[p] = \{0\}$. Dans ce cas, on montre que $A[p^k] = \{0\}$ pour tout $k \in \mathbb{N}^*$. Comme $A$ est $p$-primaire, $A = \bigcup_{k\in\mathbb{N}^*} A[p^k]$, donc ici $A = \{0\}$.*
*On peut donc exclure ce cas et supposer que $\mathrm{card}\,(A[p]) = p^r$ avec $r \in \mathbb{N}^*$, ce qui est fait par l'énoncé.*

1. Soit $k \geqslant 1$. $A[p^{k+1}]$ est fini. En appliquant le résultat admis **C.** à l'application $u_k$, on obtient :

$$\begin{aligned}\mathrm{card}\,(A[p^{k+1}]) &= \mathrm{card}\,(\ker u_k) \times \mathrm{card}\,(\mathrm{Im}\, u_k)\\ &= \mathrm{card}\,(A[p^{k+1}] \cap A[p]) \times \mathrm{card}\,(A[p^k])\\ &= \mathrm{card}\,(A[p]) \times \mathrm{card}\,(A[p^k])\\ &= p^r \times \mathrm{card}\,(A[p^k]) \qquad (*)\end{aligned}$$

   En effet, $A[p^{k+1}] \cap A[p] = A[p]$ car $A[p] \subset A[p^{k+1}]$ et $\mathrm{Im}\, u_k = A[p^k]$. Montrons l'inclusion $\mathrm{Im}\, u_k \subset A[p^k]$ : si $y \in \mathrm{Im}\, u_k$, il existe $x \in A[p^{k+1}]$ tel que $y = p\,x$. Alors $p^k y = p^{k+1}x = 0$, donc $y \in A[p^k]$. Montrons ensuite que $A[p^k] \subset \mathrm{Im}\, u_k$ : si $y \in A[p^k]$, alors en particulier $y \in A$. Comme $A$ est $p$-divisible, il existe $x \in A$ tel que $y = p\,x$. Puisque $y \in A[p^k]$, on a $x \in A[p^{k+1}]$ et donc $y \in \mathrm{Im}\, u_k$.

   La formule $(*)$ permet alors de démontrer par récurrence que $\mathrm{card}\,(A[p^k]) = p^{k\,r}$.

2. a) La suite $(x_n)_{n\in\mathbb{N}^*}$ se construit par récurrence. Si $n \in \mathbb{N}^*$ et si on suppose l'existence de $x_n$, alors l'existence de $x_{n+1} \in A$ tel que $p\,x_{n+1} = x_n$ résulte de la $p$-divisibilité de $A$.

   Pour tout $n \in \mathbb{N}^*$, $p^n x_n = p\,x_1 = p\,a = 0$ donc $x_n \in A[p^n]$. On va démontrer par récurrence que $x_n$ engendre $A[p^n]$.

   $*$ $x_1 = a$ et on note $\mathrm{Gr}(a)$ le sous-groupe de $A[p]$ engendré par $a$. D'après le théorème de Lagrange, le cardinal de $\mathrm{Gr}(a)$ divise le cardinal de $A[p]$ qui est $p$. Comme $p$ est premier, $\mathrm{card}\,(\mathrm{Gr}(a)) \in \{1, p\}$. Si $\mathrm{card}\,(\mathrm{Gr}(a)) = 1$ alors $a = 0$, ce qui est exclu. Ainsi $\mathrm{card}\,(\mathrm{Gr}(a)) = p$ et donc $\mathrm{Gr}(a) = A[p]$ ce qui signifie précisément que $x_1 = a$ engendre $A[p]$.

   $*$ Soit $n \in \mathbb{N}^*$. On suppose que $x_n$ engendre $A[p^n]$. On a vu dans la question V.1. que le morphisme $A[p^{n+1}] \to A,\ x \mapsto p\,x$ avait pour image $A[p^n]$. Prenons $x \in A[p^{n+1}]$. Alors $p\,x \in A[p^n]$. Comme $x_n$ engendre $A[p^n]$, il existe $k \in \mathbb{Z}$ tel que $p\,x = k\,x_n$. Ainsi $p\,x = k\,p\,x_{n+1}$ puis $x - k\,x_{n+1} \in A[p]$. Comme $a$ engendre $A[p]$, il existe $l \in \mathbb{Z}$ tel que $x - k\,x_{n+1} = l\,a = l\,p^n x_{n+1}$. Finalement, $x = (k + l\,p^n)\,x_{n+1}$ donc $x_{n+1}$ engendre $A[p^{n+1}]$.

b) Soit $n \in \mathbb{N}^*$ fixé. On pose $z_n = e^{2i\pi/p^n} \in U_p$ et on définit l'application $A[p^n] \to U_p,\ k\,x_n \mapsto z_n^k$. Cette application est bien définie, car si $k\,x_n = k'\,x_n$ avec $k,\, k' \in \mathbb{Z}$, alors $(k-k')\,x_n = 0$. Comme $x_n$ engendre $A[p^n]$ et que $\operatorname{card}(A[p^n]) = p^n$ (car $r=1$), l'ordre de $x_n$ dans $A[p^n]$ est $p^n$. On en déduit que $k - k' \equiv 0\ [p^n]$. Par suite $k \equiv k'\ [p^n]$ et donc $z_n^k = z_n^{k'}$. Etant bien définie, elle est trivialement un morphisme.

Comme $A$ est $p$-primaire, $A = \bigcup_{n\in\mathbb{N}^*} A[p^n]$. On définit alors l'application $\theta : A \to U_p,\ x \mapsto z_n^{k_n}$ dans le cas où $x \in A[p^n]$ et une écriture de $x$ est $x = k_n\,x_n$ avec $k_n \in \mathbb{Z}$. Si on suppose que $x \in A[p^{n'}]$ avec $n' > n$, alors $x = k_n\,x_n = k_n\,p^{n'-n}x_{n'}$. On peut donc choisir $k_{n'} = k_n\,p^{n'-n}$. De plus :

$$z_{n'}^{k_{n'}} = \left(e^{2i\pi/p^{n'}}\right)^{k_n\,p^{n'-n}}\ e^{2i\pi k_n/p^n} = z_n^{k_n}$$

L'application ci-dessus est donc bien définie. C'est un morphisme. Il est injectif. En effet, prenons $x \in \ker\theta$ où $x = k_n\,x_n$. On a alors $z_n^{k_n} = 1$ donc $k_n \equiv 0\ [p^n]$ puis $x = k_n x_n = 0$. Ce morphisme est surjectif car tout élément de $U_p$ est une puissance de $z_n$ pour un certain $n \in \mathbb{N}$.

$A$ est donc isomorphe au groupe multiplicatif $(U_p,\ \times)$.

3. a) D'après la question III.6.a) $A[p]$, vu comme un $(\mathbb{Z}/p\mathbb{Z})$-espace vectoriel, est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^r$, donc il est de dimension $r$ sur $\mathbb{Z}/p\mathbb{Z}$. Il existe donc dans $A[p]$ une base $\mathcal{B} = (a_1, \ldots, a_r)$. Si $\sum_{i=1}^r k_i a_i = 0$, alors $\sum_{i=1}^r \overline{k_i}\cdot a_i = 0$ et donc $\overline{k_i} = 0$ pour tout $i \in [\![1,\, r]\!]$. Ceci signifie bien que tous les $k_i$ sont divisibles par $p$.

b) Soit $i \in [\![1,\, r]\!]$. L'existence de la suite $(x_{i,\,n})_{n\in\mathbb{N}^*}$ résulte de la $p$-divisibilité de $A$. On montre, comme dans la question V.2.a) que $x_{i,\,n} \in A[p^n]$ pour tout $n \in \mathbb{N}^*$. L'application donnée par l'énoncé est bien définie. En effet, si $\overline{\lambda_i} = \overline{\mu_i}$ pour tout $i \in [\![1,\, r]\!]$, alors $\lambda_i - \mu_i \equiv 0\ [p^n]$. Alors $\sum_{i=1}^r (\lambda_i - \mu_i)\,x_{i,\,n} = 0$ et donc $\sum_{i=1}^r \lambda_i\,x_{i,\,n} = \sum_{i=1}^r \mu_i\,x_{i,\,n}$. Il s'agit clairement d'un morphisme de groupes.

Montrons que le morphisme en question est injectif. Pour cela, on va montrer par récurrence sur $n \in \mathbb{N}^*$ que $\sum_{i=1}^r \lambda_i\,x_{i,\,n} = 0$ implique que tous les $\lambda_i$ sont divisibles par $p^n$.

$*$ La propriété est vraie pour $n = 1$ : c'est exactement le résultat de la question 3.a).

$*$ Soit $n \in \mathbb{N}^*$. On suppose la propriété vraie pour $n$. On suppose alors que :

$$\sum_{i=1}^r \lambda_i\,x_{i,\,n+1} = 0 \qquad (\dagger)$$

Par suite, $\sum_{i=1}^r \lambda_i p\,x_{i,\,n+1} = 0$ soit $\sum_{i=1}^r \lambda_i\,x_{i,\,n} = 0$. On en déduit, par hypothèse de récurrence, que pour tout $i \in [\![1,\, r]\!]$, $\lambda_i = \lambda_i'\,p^n$ avec $\lambda_i' \in \mathbb{Z}$. La relation $(\dagger)$ donne alors $\sum_{i=1}^r \lambda_i' p^n x_{i,\,n+1} = 0$ soit $\sum_{i=1}^r \lambda_i'\,x_{i,\,1} = \sum_{i=1}^r \lambda_i'\,a_i = 0$. La question a) nous apprend que tous les $\lambda_i'$ sont multiples de $p$, donc que tous les $\lambda_i$ sont multiples de $p^{n+1}$. La propriété est donc vraie pour $n+1$.

Enfin, le morphisme est surjectif car les groupes $(\mathbb{Z}/p^n\mathbb{Z})^r$ et $A[p^n]$ sont finis de même cardinal $p^{nr}$.

c) Montrons que $A_i$ est un sous-groupe de $A$. $A_i$ est non-vide car $a_i \in A_i$. Si $x,\, y \in A_i$, alors il existe des entiers $n,\, n' \in \mathbb{N}^*$ et $k,\, k' \in \mathbb{Z}$ tels que $x = k\,x_{i,\,n}$ et $y = k'\,x_{i,\,n'}$. Si $n' \geqslant n$, alors $x_{i,\,n} = p^{n'-n}x_{i,\,n'}$. Alors $x - y = (k\,p^{n'-n} - k')\,x_{i,\,n}$ donc $x - y \in A_i$. Si $n' < n$, on démontre de manière similaire que $x - y \in A_i$.

Le morphisme défini par l'énoncé est injectif. En effet, soit $(y_i)_{1\leqslant i\leqslant r} \in \prod_{i=1}^r A_i$ tel que $\sum_{i=1}^r y_i = 0$. Pour tout $i \in [\![1,\, r]\!]$, $y_i \in A_i$ donc il existe $n_i \in \mathbb{N}^*$ et $k_i \in \mathbb{Z}$ tel que $y_i = k_i\,x_{i,\,n_i}$. On considère $n = \max_{i\in[\![1,\,r]\!]} n_i$. Alors, pour tout $i \in [\![1,\, r]\!]$, $x_{i,\,n_i} \in A[p^n]$. On a alors :

$$\sum_{i=1}^r y_i = \sum_{i=1}^r k_i\,x_{i,\,n_i} = \sum_{i=1}^r k_i\,p^{n-n_i}x_{i,\,n} = 0$$

On peut alors appliquer le résultat de la question 3.b) : pour tout $i \in [\![1,\, r]\!]$, $k_i\,p^{n-n_i}$ est divisible par $p^n$, donc $k_i$ est divisible par $p^{n_i}$. Alors $y_i = k_i\,x_{i,\,n_i} = 0$ car $x_{i,\,n_i} \in A[p^{n_i}]$.

Montrons à présent que le morphisme est surjectif. Soit $x \in A$. Comme $A$ est $p$-primaire, il existe $n \in \mathbb{N}^*$ tel que $p^n x = 0$ donc $x \in A[p^n]$. Comme l'application définie dans la question b) est surjective, il existe $(\lambda_i)_{1 \leqslant i \leqslant r} \in \mathbb{Z}^r$ tel que $x = \sum_{i=1}^r \lambda_i \, x_{i,\,n}$. Si $i \in [\![1,\, r]\!]$, on pose $y_i = \lambda_i \, x_{i,\,n} \in A_i$ et on a bien $x = \sum_{i=1}^r y_i$.

d) Soit $i \in [\![1,\, r]\!]$. Le groupe $A_i$ est abélien, $p$-primaire et $p$-divisible. En effet, si $x = k \, x_{i,\,n} \in A_i$ alors $x = p \, k \, x_{i,\,n+1}$. On va s'intéresser à $A_i[p]$ (qui est fini car $A_i[p] \subset A[p]$) et montrer que $\operatorname{card}(A_i[p]) = p$. Dans un premier temps, on peut remarquer que $a_i \in A_i[p]$, puisque $a_i \in A[p] \cap A_i$. De plus $a_i \neq 0$ donc $A_i[p] \neq \{0\}$. On sait alors que le cardinal de $A_i[p]$ est une puissance de $p$ : il existe $r_i \in \mathbb{N}^*$ tel que $\operatorname{card}(A_i[p]) = p^{r_i}$.

L'isomorphisme de la question c) induit un isomorphisme $\prod_{i=1}^r A_i[p] \to A[p],\ (y_i)_{1 \leqslant i \leqslant r} \mapsto \sum_{i=1}^r y_i$. En effet, ce morphisme est clairement bien défini et injectif (comme restriction d'un morphisme injectif). Il est également surjectif car si $x \in A[p]$, alors $p \, x = 0$ et $x = \sum_{i=1}^r y_i$ où $y_i \in A_i$ pour tout $i \in [\![1,\, r]\!]$. Alors $\sum_{i=1}^r p \, y_i = 0$ avec $p \, y_i \in A_i$ pour tout $i \in [\![1,\, r]\!]$, ce qui signifie $y_i \in A_i[p]$.

Le cardinal de $\prod_{i=1}^r A_i[p]$ est donc égal au cardinal de $A[p]$ i.e. :

$$\prod_{i=1}^{r} p^{r_i} = p^r$$

On en tire que $r_i = 1$ pour tout $i \in [\![1,\, r]\!]$. On peut donc appliquer le résultat de V.2. qui nous apprend que $A_i$ est isomorphe à $U_p$. Le groupe $\prod_{i=1}^r A_i$ est donc isomorphe à $\prod_{i=1}^r U_p = (U_p)^r$ et donc $A$ aussi.

## VI

1. $\{0\}$ est un sous-groupe $p$-divisible de $A$, donc $D \neq \varnothing$. Soit $x,\, y \in D$ avec $x = \sum_{i \in I} x_i$ et $y = \sum_{i \in I} y_i$ où $(x_i)_{i \in I}$ et $(y_i)_{i \in I}$ sont des familles presque nulles de $A$ telles que $x_i,\, y_i \in D_i$ pour tout $i \in I$. Alors $x - y = \sum_{i \in I} x_i - \sum_{i \in I} y_i = \sum_{i \in I} (x_i - y_i)$ où $(x_i - y_i)_{i \in I}$ est une famille presque nulle de $A$ telle que $x_i - y_i \in D_i$ pour tout $i \in I$ (car $D_i$ est un sous-groupe de $A$). Ainsi $x - y \in D$.

   Montrons que $D$ est $p$-divisible. Soit $x \in D$ avec $x = \sum_{i \in I} x_i$. Comme $x_i \in D_i$ et que $D_i$ est $p$-divisible. $x_i = p \, x_i'$ avec $x_i' \in D_i$. Comme la famille $(x_i)_{i \in I}$ est presque nulle, on peut faire en sorte que la famille $(x_i')_{i \in I}$ le soit également (en prenant $x_i' = 0$ lorsque $x_i = 0$). On a alors : $x = p \sum_{i \in I} x_i' = p \, x'$ avec $x' = \sum_{i \in I} x_i' \in D$.

   D'après la question III.4.b), $D$ est $p$-primaire et $p$-divisible, donc divisible.

   Soit $H$ un sous-groupe $p$-divisible de $A$. Il existe donc $i \in I$ tel que $H = D_i$, donc $H \subset D$.

2. On a : $A = D \oplus S$.

   a) Le sous-groupe $\bigcap_{k \in \mathbb{N}^*} p^k A$ est $p$-divisible d'après la question III.6.c). Ainsi : $\bigcap_{k \in \mathbb{N}^*} p^k A \subset D$. Montrons l'inclusion réciproque. Si $x \in D$, alors $x = \sum_{i \in I} x_i$ où $(x_i)_{i \in I}$ est une famille presque nulle de $A$ telle que $x_i \in D_i$ pour tout $i \in I$. Soit $k \in \mathbb{N}^*$. Comme $D_i$ est $p$-divisible, alors $x_i = p \, x_{i,\,1}$ avec $x_{i,\,1} \in D_i$ et plus généralement $x_i = p^k \, x_{i,\,k}$ avec $x_{i,\,k} \in D_i$. Ainsi $x = p^k \sum_{i \in I} x_{i,\,k}$ donc $x \in p^k A$. Ceci étant vrai pour tout $k \in \mathbb{N}^*$, on a : $x \in \bigcap_{k \in \mathbb{N}^*} p^k A$.

   Comme $A[p]$ est fini, $S[p]$ est fini ($S[p] \subset A[p]$). Comme $A$ est $p$-primaire, alors $S$ est également $p$-primaire. Montrons que $\bigcap_{k \in \mathbb{N}^*} p^k S = \{0\}$. On a $\bigcap_{k \in \mathbb{N}^*} p^k S \subset S$ car $\bigcap_{k \in \mathbb{N}^*} p^k S$ est un sous-groupe de $S$. De plus $\bigcap_{k \in \mathbb{N}^*} p^k S \subset \bigcap_{k \in \mathbb{N}^*} p^k A$ i.e. $\bigcap_{k \in \mathbb{N}^*} p^k S \subset D$. Or $A = D \oplus S$, donc $D \cap S = \{0\}$. On en déduit que $\bigcap_{k \in \mathbb{N}^*} p^k S \subset \{0\}$ et donc que $\bigcap_{k \in \mathbb{N}^*} p^k S = \{0\}$.

   On peut donc utiliser la question IV.2. qui nous apprend que $S$ est fini.

   b) Comme $A = D \oplus S$ alors $A \simeq D \times S$. $S$ est un groupe abélien fini $p$-primaire (son cardinal est une puissance de $p$). $D$ est $p$-primaire et $p$-divisible avec $D[p]$ fini, donc il existe $r \in \mathbb{N}$ tel que $D \simeq (U_p)^r$. Ainsi, $A \simeq F \times (U_p)^r$ (en fait $F = S$).

3. $\mu_{p^\infty}$ est un sous-groupe de $(\mathbb{K}^*, \times)$ - cela se démontre de manière similaire que le fait que $U_p$ est un sous-groupe de $(S^1, \times)$. Il est $p$-primaire, par définition. Il est également $p$-divisible. En effet l'application $\mu_{p^\infty} \to \mu_{p^\infty},\ x \mapsto x^p$ est surjective (car, pour tout $x \in \mu_{p^\infty}$, le polynôme $X^p - x$ admet au moins une racine dans $\mathbb{K}$, racine qui est en fait dans $\mu_{p^\infty}$). Enfin $\mu_{p^\infty}[p] = \{x \in \mu_{p^\infty} \ / \ x^p = 1\}$ est fini de cardinal $p$. Pour le voir on considère le polynôme $X^p - 1$ de degré $p$. Comme $\mathbb{K}$ est algébriquement clos, ce polynôme admet $p$ racines dans $\mathbb{K}$ comptées avec leur ordre de multiplicité. La dérivée de ce polynôme est $p\,X^{p-1}$. Comme $\mathbb{K}$ est de caractéristique zéro, $X^p - 1$ et $p\,X^{p-1}$ sont premiers entre eux, donc les racines de $X^p - 1$ sont simples.

   La question V.2.b) nous apprend alors que $\mu_{p^\infty}$ est isomorphe à $U_p$.

---

*Correction par Marcin Pulkowski. Pour faire des remarques concernant ce corrigé ou pour me signaler les éventuelles erreurs, vous pouvez m'envoyer un mail à l'adresse : mpulko2@gmail.com .*