Université Paris Saclay **MDD 102**
L1S1 **Algèbre**

Corrigé de l'Examen du 20 décembre 2024

Exercice 1.

1. Montrer que 125 et 51 sont premiers entre eux et trouver u_0 et v_0 dans $\mathbb{Z}$ tels que $125u_0 + 51v_0 = 1$.
   Réponse : On utilise l'alogorithme d'Euclide :
$$\begin{aligned} 125 &= 2 \times 51 + 23 \\ 51 &= 2 \times 23 + 5 \\ 23 &= 4 \times 5 + 3 \\ 5 &= 1 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \end{aligned}$$
   Le pgcd de 125 et 51 est donc 1, le dernier reste non-nul, c'est-à-dire 125 et 51 sont premiers entre eux. Pour trouver les coefficients u_0 et v_0, on remonte l'algorithme d'Euclide :
$$\begin{aligned} 1 &= 3 - 2 \\ &= -5 + 2 \times 3 \\ &= 2 \times 23 - 9 \times 5 \\ &= -9 \times 51 + 20 \times 23 \\ &= 20 \times 125 - 49 \times 51 \end{aligned}$$
   On peut donc prendre $u_0 = 20$ et $v_0 = -49$.
2. On souhaite maintenant trouver tous les couples $(u, v) \in \mathbb{Z}^2$ tels que $125u + 51v = 1$. On utilisera encore u_0 et v_0 trouvés à la question précédente ; on pourra répondre à cette question même sans valeurs explicites pour u_0 et v_0.
   (a) Soit $t \in \mathbb{Z}$ quelconque. Montrer que $u = u_0 + 51t$ et $v = v_0 - 125t$ vérifient $125u + 51v = 1$.
   Réponse : On calcule :
$$125(u_0+51t)+51(v_0-125t) = 125u_0+51v_0+125\times51t-51\times125t = 1$$
   car on sait que u_0 et v_0 vérifient l'égalité voulue.

(b) On souhaite maintenent montrer la réciproque. Soit $(u, v) \in \mathbb{Z}^2$ tel que $125u + 51v = 1$, montrer que $125(u - u_0) = 51(v_0 - v)$.

Réponse : En soustrayant l'égalité $125u_0 + 51v_0 = 1$ à l'égalité $125u + 51v = 1$, on trouve $125(u - u_0) + 51(v - v_0) = 0$, ce qui donne le résultat voulu.

(c) Que vaut $\text{ppcm}(125, 51)$? On pourra donner la réponse sous la forme d'un produit sans le calculer explicitement.

Réponse : Comme $\text{pgcd}(125, 51) = 1$, on sait par le cours que $\text{ppcm}(125, 51) = 125 \times 51$.

(d) En déduire que si $(u, v) \in \mathbb{Z}^2$ vérifie $125u + 51v = 1$, alors il existe $t \in \mathbb{Z}$ tel que $u = u_0 + 51t$ et $v = v_0 - 125t$.

Réponse : En utilisant la question 2.(b), on voit que l'entier $125(u - u_0) = 51(v_0 - v)$ est à la fois un multiple de 125 et de 51, donc par définition du ppcm, c'est un multiple de 125×51. On peut donc écrire $125(u - u_0) = 51(v_0 - v) = 125 \times 51t$ pour un certain $t \in \mathbb{Z}$, ce qui donne, après simplification par 125 dans un cas et par 51 dans l'autre : $u = u_0 + 51t$ et $v = v_0 - 125t$.

3. On se place dans $\mathbb{Z}/125\mathbb{Z}$.

(a) Trouver $z \in \mathbb{Z}/125\mathbb{Z}$ tel que $\overline{51} \times z = \overline{1}$. On donnera le résultat sous la forme $z = \overline{n}$ avec $0 \leq n \leq 124$.

Réponse : En utilisant les résultats précédents, on obtient

$$1 = 20 \times 125 - 49 \times 51 = (20 - 51) \times 125 + (125 - 49) \times 51.$$

En prenant les classes modulo 125, on obtient, dans $\mathbb{Z}/125\mathbb{Z}$:

$$\overline{1} = \overline{125 - 49} \times \overline{51},$$

donc $z = \overline{125 - 49} = \overline{76}$ convient.

(b) Soit l'application $f : \mathbb{Z}/125\mathbb{Z} \to \mathbb{Z}/125\mathbb{Z}$ définie par $f(x) = \overline{51} \times x$. Montrer que f est bijective.

Réponse : On vérifie tout d'abord que f est injective : supposons que $f(x) = f(y)$, c'est-à-dire $\overline{51} \times x = \overline{51} \times y$. Puisque $\overline{76} \times \overline{51} = \overline{1}$, on obtient en multipliant par $\overline{76}$ que $x = y$, donc f est injective. Puis, comme l'ensemble de départ et l'ensemble d'arrivée de f ont le même nombre d'éléments, à savoir 125, on peut appliquer le théorème du cours pour obtenir que f est bijective.

Exercice 2. On définit une relation R sur l'ensemble $\mathbb{N}^2$ par :

$$(x,y)R(x',y') \Leftrightarrow \begin{cases} x+y < x'+y' \\ \text{ ou } (x+y = x'+y' \text{ et } x < x') \\ \text{ ou } (x+y = x'+y' \text{ et } x = x' \text{ et } y \leq y') \end{cases}$$

1. Montrer que R est une relation d'ordre totale.

   Réponse : R est réflexive : $(x,y)R(x,y)$ car $x+y = x+y$ et $x = x$ et $y \leq y$.

   R est antisymétrique : supposons $(x,y)R(x',y')$ et $(x',y')R(x,y)$. En distribuant et sur ou, on trouve a priori 9 (!) cas possibles :

   — Cas 1 : $x+y < x'+y'$ et $x'+y' < x+y$: incompatible

   — Cas 2 et 3 : $x+y < x'+y'$ et ($x'+y' = x+y$ et ...) : incompatible

   — Cas 4 et 5 : ($x+y = x'+y'$ et ...) et $x'+y' < x+y$: incompatible

   — Cas 6 : ($x+y = x'+y'$ et $x < x'$) et ($x'+y' = x+y$ et $x' < x$) : incompatible

   — Cas 7 : ($x+y = x'+y'$ et $x < x'$) et ($x'+y' = x+y$ et $x' = x$ et $y' \leq y$) : incompatible

   — Cas 8 : même chose en échangeant (x,y) et (x',y') : incompatible

   — Cas 9 : ($x+y = x'+y'$ et $x = x'$ et $y \leq y'$) et ($x'+y' = x+y$ et $x' = x$ et $y' \leq y$) : c'est le seul cas possible, et il donne $x = x'$ et $y = y'$ par antisymétrie de $\leq$.

   R est transitive : supposons $(x,y)R(x',y')$ et $(x',y')R(x'',y'')$. On trouve également 9 cas possibles, que l'on peut regrouper comme suit :

   — si $x+y < x'+y'$, comme on a aussi $x'+y' \leq x''+y''$, on obtient $x+y < x''+y''$ donc $(x,y)R(x'',y'')$.

   — même chose si $x+y \leq x'+y'$ et $x'+y' < x''+y''$; on a traité 5 cas

   — si $x+y = x'+y' = x''+y''$ et $x < x'$ et $x' < x''$, alors $x+y = x''+y''$ et $x < x''$ donc $(x,y)R(x'',y'')$

   — si $x+y = x'+y' = x''+y''$ et $x < x'$ et $x' = x''$ et $y' \leq y''$, alors $x+y = x''+y''$ et $x < x''$ donc $(x,y)R(x'',y'')$

   — si $x+y = x'+y' = x''+y''$ et $x = x'$ et $y \leq y'$ et $x' < x''$, alors $x+y = x''+y''$ et $x < x''$ donc $(x,y)R(x'',y'')$

   — si $x+y = x'+y' = x''+y''$ et $x = x'$ et $y \leq y'$ et $x' = x''$ et $y' \leq y''$, alors $x+y = x''+y''$ et $x = x''$ et $y \leq y''$ donc $(x,y)R(x'',y'')$

   Montrons finalement que c'est une relation d'ordre totale : on veut comparer (x,y) et (x',y').

— cas 1 : si $x + y < x' + y'$, alors $(x, y)R(x', y')$
— cas 2 : si $x' + y' < x + y$, alors $(x', y')R(x, y)$
— cas 3.1 : si $x + y = x' + y'$ et $x < x'$, alors $(x, y)R(x', y')$
— cas 3.2 : si $x + y = x' + y'$ et $x' < x$, alors $(x', y')R(x, y)$
— cas 3.3.1 : si $x+y = x'+y'$ et $x = x'$ et $y \leq y'$, alors $(x, y)R(x', y')$
— cas 3.3.2 : $x + y = x' + y'$ et $x = x'$ et $y' < y$, alors $(x', y')R(x, y)$

Donc (x, y) et (x', y') sont toujours comparables.

2. Soit $n \in \mathbb{N}$ quelconque. Montrer que l'ensemble formé des $(x, y) \in \mathbb{N}^2$ tels que $x + y = n$ est fini.

   Réponse : Il y a exactement $n + 1$ couples $(x, y) \in \mathbb{N}^2$ qui vérifient $x + y = n$: les couples $(x, n - x)$ pour $0 \leq x \leq n$.

3. Soit $(x_0, y_0) \in \mathbb{N}^2$ quelconque. Montrer que l'ensemble formé des $(x, y) \in \mathbb{N}^2$ tels que $(x, y)R(x_0, y_0)$ est fini.

   Réponse : Par définition de la relation R, si $(x, y)R(x_0, y_0)$, on a $x + y \leq x_0 + y_0$. Donc $x + y$ ne peut prendre que $x_0 + y_0 + 1$ valeurs possibles, à savoir les entiers n tels que $0 \leq n \leq x_0 + y_0$. Or, par la question précédente, pour chacune de ces valeurs de n, il n'y a qu'un nombre fini de couples $(x, y) \in \mathbb{N}^2$ tels que $x + y = n$: cela donne donc bien au total un nombre fini de possibilités pour que $(x, y)R(x_0, y_0)$

On définit maintenant une relation S sur l'ensemble $\mathbb{N}^2$ par :

$$(x, y)S(x', y') \Leftrightarrow (x < x' \text{ ou } (x = x' \text{ et } y \leq y'))$$

On peut montrer comme à la question 1 que S est une relation d'ordre totale, on l'admet sans démonstration.

4. Montrer que l'ensemble formé des $(x, y) \in \mathbb{N}^2$ tels que $(x, y)S(1, 0)$ est infini.

   Réponse : On voit que pour $n \in \mathbb{N}$ quelconque, $(0, n)S(1, 0)$ puisque $0 < 1$. On a donc trouvé une infinité de couples $(x, y) \in \mathbb{N}^2$ tels que $(x, y)S(1, 0)$.

Exercice 3. L'objectif de cet exercice est le calcul de quelques valeurs de cosinus et sinus. On ne supposera donc pas déjà connues ces valeurs, sauf pour la question 2.(a).

1. Soit $P(X) = X^3 - 1$.

   (a) Donner les racines complexes de P sous forme exponentielle.

   Réponse : Les racines de P sont par définition les racines troisièmes de l'unité, c'est-à-dire 1, $e^{2i\pi/3}$ et $e^{4i\pi/3}$.

(b) Trouver $Q(X)$ tel que $P(X) = (X-1)Q(X)$.

Réponse : Comme 1 est une racine de P, on sait que $X-1$ divise $P(X)$, et on peut trouver le quotient en posant la division euclidienne : $Q(X) = X^2 + X + 1$.

(c) Trouver les racines de Q sous forme algébrique.

Réponse : Comme Q est un polynôme du second degré, on trouve ses racines en calculant son discriminant $\Delta = -3$, ce qui donne les racines $\frac{-1+i\sqrt{3}}{2}$ et $\frac{-1-i\sqrt{3}}{2}$.

(d) Déduire des questions précédentes les valeurs de $\cos(2\pi/3)$ et $\sin(2\pi/3)$.

Réponse : On a trouvé deux écritures différentes pour les racines de P : d'une part 1, $e^{2i\pi/3}$ et $e^{4i\pi/3}$, et d'autre part 1, $\frac{-1+i\sqrt{3}}{2}$ et $\frac{-1-i\sqrt{3}}{2}$. Pour les identifier, on utilise le fait que $0 < \frac{2\pi}{3} < \pi$, et donc $\sin(2\pi/3) > 0$. Cela donne $e^{2i\pi/3} = \frac{-1+i\sqrt{3}}{2}$, et donc

$$\cos(2\pi/3) = -\frac{1}{2} \text{ et } \sin(2\pi/3) = \frac{\sqrt{3}}{2}$$

2. Soient $z_1 = e^{2i\pi/3}$ et $z_2 = i$.

(a) Écrire z_2 sous forme exponentielle.

Réponse : $z_2 = i = e^{i\pi/2}$

(b) En utilisant les résultats des questions précédentes, écrire $\frac{z_1}{z_2}$ sous forme algébrique et sous forme exponentielle.

Réponse : Sous forme algébrique, puisque $-1/i = i$,

$$\frac{z_1}{z_2} = \frac{-1+i\sqrt{3}}{2i} = \frac{\sqrt{3}}{2} + \frac{1}{2}i$$

Sous forme exponentielle,

$$\frac{z_1}{z_2} = e^{2i\pi/3 - i\pi/2} = e^{i\pi/6}$$

(c) En déduire les valeurs de $\cos(\pi/6)$ et $\sin(\pi/6)$.

Réponse : En identifiant les parties réelles et les parties imaginaires, on trouve

$$\cos(\pi/6) = \frac{\sqrt{3}}{2} \text{ et } \sin(\pi/6) = \frac{1}{2}$$

3. (a) Calculer les racines carrées de $\frac{\sqrt{3}}{2} + \frac{1}{2}i$ sous forme algébrique.

Réponse : On cherche $z = a + ib$ tel que $z^2 = \frac{\sqrt{3}}{2} + \frac{1}{2}i$. On développe $z^2 = (a^2 - b^2) + 2iab$ et on identifie parties réelles et parties imaginaires, on utilise aussi le module $|z^2| = a^2 + b^2 = |\frac{\sqrt{3}}{2} + \frac{1}{2}i| = 1$. On obtient finalement le système

$$\begin{cases} a^2 - b^2 = \frac{\sqrt{3}}{2} \\ 2ab = \frac{1}{2} \\ a^2 + b^2 = 1 \end{cases} \quad \Leftrightarrow \begin{cases} a^2 = \frac{2+\sqrt{3}}{4} \\ b^2 = \frac{2-\sqrt{3}}{4} \\ 2ab = \frac{1}{2} \end{cases}$$

Comme a et b doivent être de même signe, on obtient les solutions

$$z = \pm\Big(\frac{\sqrt{2+\sqrt{3}}}{2} + i\frac{\sqrt{2-\sqrt{3}}}{2}\Big)$$

(b) Calculer les racines carrées de $e^{i\pi/6}$ sous forme exponentielle.

Réponse : On cherche $z = re^i\theta$, avec $r > 0$, tel que $z^2 = e^{i\pi/6}$. En identifiant les modules et les arguments, on obtient le système

$$\begin{cases} r^2 = 1 \\ 2\theta \equiv \pi/6\ [2\pi] \end{cases} \quad \Leftrightarrow \begin{cases} r = 1 \\ \theta \equiv \pi/12\ [\pi] \end{cases}$$

Cela donne les racines carrées $z = \pm e^{i\pi/12}$.

(c) Déduire des questions précédentes les valeurs de $\cos(\pi/12)$ et $\sin(\pi/12)$.

Réponse : Comme $e^{i\pi/6} = \frac{\sqrt{3}}{2} + \frac{1}{2}i$ d'après la question 2.(c), on peut identifier les racines carrées trouvées dans les deux questions précédentes. Puisque $0 < \frac{\pi}{12} < \pi$, $\sin(\pi/12) > 0$ et donc

$$\cos(\pi/12) = \frac{\sqrt{2+\sqrt{3}}}{2} \text{ et } \sin(\pi/12) = \frac{\sqrt{2-\sqrt{3}}}{2}$$