Corrigé du contrôle de maths spé : idéaux, congruences et indicatrice d'Euler

Barème du contrôle

Exercice	Points
Exercice 1 : Question de cours	4 points
Exercice 2 : Inversibles de Z/60Z	4 points
Exercice 3 : Théorème chinois	4 points
Exercice 4 : Théorème d'Euler	3 points
Exercice 5 : Le corps Z/pZ et une algèbre de matrices	5 points
Total	**20 points**

Exercice 1 : Question de cours (4 points)

a. *Existence.* L'ensemble des degrés des polynômes non nuls de I est une partie non vide de $\mathbb{N}$; elle admet un plus petit élément. Soit $P_0 \in I$ non nul de degré minimal, et P le polynôme unitaire obtenu en divisant P_0 par son coefficient dominant. Comme I est un idéal, $P \in I$, puis $P\,\mathbb{K}[X] \subset I$.

Réciproquement, soit $A \in I$. La division euclidienne donne $A = PQ + R$ avec $\deg R < \deg P$. Alors $R = A - PQ$ appartient à I, car I est stable par différence et par multiplication par un polynôme. Par minimalité du degré de P, on a $R = 0$, donc $A \in P\,\mathbb{K}[X]$. Ainsi $I = P\,\mathbb{K}[X]$.

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

Unicité. Si $P\,\mathbb{K}[X] = P_1\,\mathbb{K}[X]$ avec P et P_1 unitaires, alors P divise P_1 et P_1 divise P. Ils sont donc associés : $P_1 = \lambda P$ avec $\lambda \in \mathbb{K}^*$. La comparaison des coefficients dominants donne $\lambda = 1$. **Le générateur unitaire P est unique.**

b. D'abord, $0 = a \times 0 + b \times 0$ appartient à $a\mathbb{Z} + b\mathbb{Z}$. Ensuite, pour $x = au + bv$, $y = au' + bv'$ et $k \in \mathbb{Z}$, on a $x - y = a(u - u') + b(v - v')$ et $kx = a(ku) + b(kv)$. Ainsi $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe stable par multiplication par tout entier : c'est un idéal de $\mathbb{Z}$. Il s'écrit donc $\delta\mathbb{Z}$ avec $\delta \in \mathbb{N}$, et $\delta \neq 0$ car a ou b est non nul.

Comme $a = a \times 1 + b \times 0$ est dans $\delta\mathbb{Z}$, δ divise a ; de même δ divise b. De plus, δ s'écrit $au + bv$, donc tout diviseur commun de a et b divise δ. Par conséquent, δ est le plus grand diviseur commun positif : $\delta = d$. **Ainsi** $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$, et l'appartenance $d \in a\mathbb{Z} + b\mathbb{Z}$ fournit des entiers u et v tels que $au + bv = a \wedge b$: c'est la relation de Bézout.

Barème : a) 2 points : 0,5 pour le choix du degré minimal, 1 pour la division euclidienne, 0,5 pour l'unicité ; b) 2 points : 0,5 pour la structure d'idéal, 1 pour l'identification de δ au PGCD, 0,5 pour la relation de Bézout.

Exercice 2 : Inversibles de Z/60Z (4 points)

a. L'élément $\overline{k}$ est inversible si et seulement s'il existe $u \in \mathbb{Z}$ tel que $\overline{u}\,\overline{k} = \overline{1}$, c'est-à-dire $uk \equiv 1 \pmod{n}$. Cela revient à l'existence d'entiers u et v tels que $uk + vn = 1$. D'après le théorème de Bézout, $\overline{k}$ **est inversible si et seulement si** $k \wedge n = 1$**.**

b. Comme $60 = 2^2 \times 3 \times 5$ et que 17 est un nombre premier distinct de 2, 3 et 5, on a $17 \wedge 60 = 1$: $\overline{17}$ est inversible. L'algorithme d'Euclide donne :

$60 = 3 \times 17 + 9$;

$17 = 1 \times 9 + 8$;

$9 = 1 \times 8 + 1$.

On remonte les calculs :

$$1 = 9 - 8 = 9 - (17 - 9) = 2 \times 9 - 17 = 2 \times (60 - 3 \times 17) - 17 = 2 \times 60 - 7 \times 17.$$

Ainsi $-7 \times 17 \equiv 1 \pmod{60}$, et $-7 \equiv 53 \pmod{60}$. Vérification : $17 \times 53 = 901 = 15 \times 60 + 1$. **L'inverse de** $\overline{17}$ **dans** $\mathbb{Z}/60\mathbb{Z}$ **est** $\overline{53}$**.**

c. En multipliant par 53, qui est inversible modulo 60, on obtient une congruence équivalente : $x \equiv 5 \times 53 = 265 \equiv 25 \pmod{60}$. Vérification : $17 \times 25 = 425 = 7 \times 60 + 5$. **Les solutions sont les entiers** $x = 25 + 60k$**,** $k \in \mathbb{Z}$**.**

d. D'après a), le nombre d'inversibles est $\varphi(60)$. Avec $60 = 2^2 \times 3 \times 5$,

$$\varphi(60) = 60 \times \left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{3}\right)\left(1 - \tfrac{1}{5}\right) = 60 \times \tfrac{1}{2} \times \tfrac{2}{3} \times \tfrac{4}{5} = 16.$$

L'anneau $\mathbb{Z}/60\mathbb{Z}$ **a 16 inversibles ; ce n'est pas un corps**, car $\overline{2}$, par exemple, est non nul et non inversible.

Barème : a) 1 point ; b) 1,5 point : 0,5 pour la justification, 0,5 pour l'algorithme, 0,5 pour l'inverse ; c) 0,5 point ; d) 1 point : 0,5 pour $\varphi(60)$*, 0,5 pour la conclusion.*

Exercice 3 : Théorème chinois (4 points)

a. **Théorème chinois.** Si $m \wedge n = 1$, l'application $\theta : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, qui envoie la classe de k modulo mn sur le couple (classe de k modulo m, classe de k modulo n), est un isomorphisme d'anneaux.

Injectivité. L'application est bien définie, car m et n divisent mn, et c'est un morphisme d'anneaux. Si l'image de la classe de k est nulle, alors m et n divisent k. Comme $m \wedge n = 1$, le produit mn divise k, donc la classe de k modulo mn est nulle. Le noyau est trivial : θ **est injective**. Les deux ensembles ayant mn éléments, elle est même bijective.

b. Les modules 5, 7 et 9 sont deux à deux premiers entre eux et $5 \times 7 \times 9 = 315$. D'après le théorème chinois, les solutions forment une seule classe modulo 315.

D'abord, $x \equiv 2 \pmod{5}$ s'écrit $x = 2 + 5k$. La condition modulo 7 devient $5k \equiv 1 \pmod{7}$. Or $5 \times 3 = 15 \equiv 1 \pmod{7}$, donc $k \equiv 3 \pmod{7}$ et $x \equiv 17 \pmod{35}$.

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

Ensuite, on écrit $x = 17 + 35m$. Comme $17 \equiv 8$ et $35 \equiv 8 \pmod 9$, la condition devient $8 + 8m \equiv 1 \pmod 9$. Or $8 \equiv -1 \pmod 9$, d'où $-1 - m \equiv 1$, soit $m \equiv -2 \equiv 7 \pmod 9$. Ainsi $x \equiv 17 + 245 = 262 \pmod{315}$.

Vérification : $262 = 52 \times 5 + 2 = 37 \times 7 + 3 = 29 \times 9 + 1$. **Les solutions sont les entiers** $x = 262 + 315k$, $k \in \mathbb{Z}$.

c. Un isomorphisme d'anneaux envoie le groupe des inversibles sur le groupe des inversibles. Or un couple (α, β) est inversible dans l'anneau produit si et seulement si α et β sont inversibles. Donc θ réalise une bijection de $(\mathbb{Z}/mn\mathbb{Z})^\times$ sur $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. En comptant les éléments, $\varphi(mn) = \varphi(m)\varphi(n)$.

Barème : a) 1 point : 0,5 pour l'énoncé, 0,5 pour l'injectivité ; b) 2 points : 1 pour la première étape (classe modulo 35), 0,5 pour la seconde, 0,5 pour la vérification et la forme générale ; c) 1 point.

Exercice 4 : Théorème d'Euler (3 points)

a. Comme $100 = 2^2 \times 5^2$, on a $\varphi(100) = 100 \times \frac{1}{2} \times \frac{4}{5} = 40$. **Donc** $\varphi(100) = 40$.

b. **Théorème d'Euler.** Si $a \wedge n = 1$, alors $a^{\varphi(n)} \equiv 1 \pmod n$. En effet, $\bar{a}$ appartient au groupe commutatif $(\mathbb{Z}/n\mathbb{Z})^\times$, de cardinal $\varphi(n)$.

Ici $7 \wedge 100 = 1$, donc $7^{40} \equiv 1 \pmod{100}$. Comme $2026 = 40 \times 50 + 26$, on obtient $7^{2026} \equiv 7^{26} \pmod{100}$. Or $7^2 = 49$ et $7^4 = 2401 \equiv 1 \pmod{100}$. Ainsi $7^{26} = (7^4)^6 \times 7^2 \equiv 49 \pmod{100}$. **Les deux derniers chiffres de** 7^{2026} **sont 4 et 9 :** $7^{2026} \equiv 49 \pmod{100}$.

c. L'ordre de $\bar{7}$ divise 4, puisque $7^4 \equiv 1$. Il ne vaut pas 1, et il ne vaut pas 2 car $7^2 = 49 \not\equiv 1$. **Donc** $\bar{7}$ **est d'ordre 4.** Comme $2026 = 4 \times 506 + 2$, on retrouve directement $7^{2026} \equiv 7^2 = 49 \pmod{100}$.

Barème : a) 0,5 point ; b) 1,5 point : 0,5 pour l'énoncé, 0,5 pour la réduction de l'exposant, 0,5 pour le résultat ; c) 1 point : 0,5 pour l'ordre, 0,5 pour la conclusion.

Erreur fréquente : appliquer le théorème d'Euler sans vérifier que a et n sont premiers entre eux.

Exercice 5 : Le corps Z/pZ et une algèbre de matrices (5 points)

Partie A : le corps Z/pZ

a. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est commutatif et non nul, car $n \geq 2$. C'est un corps si et seulement si tout $\bar{k} \neq \bar{0}$ est inversible, c'est-à-dire, d'après l'exercice 2 a), si tout entier k compris entre 1 et $n-1$ est premier avec n. Cela signifie exactement que n n'a pas de diviseur strict autre que 1. **Donc $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.**

b. Le groupe $\mathbb{F}_p^*$ est commutatif, de cardinal $p-1$. Si p ne divise pas a, alors $\bar{a} \in \mathbb{F}_p^*$, et le théorème de Lagrange (cas commutatif) donne $\bar{a}^{\,p-1} = \bar{1}$. **Ainsi $a^{p-1} \equiv 1 \pmod p$.**

c. On a $x^2 - \bar{1} = (x-\bar{1})(x+\bar{1})$. Un corps est intègre, donc ce produit est nul si et seulement si l'un des facteurs est nul. **Les solutions sont $\bar{1}$ et $-\bar{1}$**, distinctes car $p \geq 3$.

d. Le produit $(p-1)!$ a pour classe le produit de tous les éléments de $\mathbb{F}_p^*$. D'après c), les seuls éléments égaux à leur inverse sont $\bar{1}$ et $-\bar{1}$. Les $p-3$ autres éléments se regroupent donc en paires $\{x, x^{-1}\}$ avec $x \neq x^{-1}$, et chaque paire a pour produit $\bar{1}$.

Par conséquent, le produit de tous les éléments de $\mathbb{F}_p^*$ vaut $\bar{1} \times (-\bar{1}) \times \bar{1} = -\bar{1}$. **Ainsi $(p-1)! \equiv -1 \pmod p$.** Par exemple, $6! = 720 = 103 \times 7 - 1$.

Partie B : une algèbre de matrices

e. On a $N^2 = 0$. L'ensemble $\mathcal{A} = \mathrm{Vect}(I_2, N)$ est un sous-espace vectoriel qui contient I_2. Par ailleurs,

$$(aI_2 + bN)(cI_2 + dN) = acI_2 + (ad+bc)N + bdN^2 = acI_2 + (ad+bc)N.$$

Ce produit appartient à $\mathcal{A}$, et l'expression est symétrique dans l'échange des deux facteurs. Enfin, I_2 et N ne sont pas colinéaires. **$\mathcal{A}$ est une sous-algèbre commutative de dimension 2.**

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

f. Pour $P = \sum_k a_k X^k$, on a $N^k = 0$ dès que $k \geq 2$, donc $P(N) = a_0 I_2 + a_1 N$. Tous les couples (a_0, a_1) sont atteints : **l'image de Φ est $\mathcal{A}$**. De plus, $P(N) = 0$ si et seulement si $a_0 = a_1 = 0$, c'est-à-dire si X^2 divise P. **Le noyau est l'idéal $X^2\,\mathbb{K}[X]$.**

Barème : a) 1 point ; b) 0,5 point ; c) 0,5 point ; d) 1,5 point : 0,5 pour les éléments égaux à leur inverse, 0,5 pour le regroupement en paires, 0,5 pour la conclusion ; e) 1 point : 0,5 pour la stabilité par produit, 0,5 pour la commutativité et la dimension ; f) 0,5 point.

Revenir à l'énoncé du contrôle

Après le corrigé du contrôle : idéaux, congruences et indicatrice d'Euler

Pour consolider ce que le corrigé vous a appris, relisez le cours « Anneaux, idéaux et Z/nZ » en maths spé puis entraînez-vous avec les **exercices corrigés** anneaux, idéaux et z/nz.

Retrouvez tous les **contrôles de maths spé** classés par chapitre, ou choisissez un autre niveau sur la page contrôles de maths du CP au post-bac.