

Corrigé du contrôle de maths L3 : partiel d'algèbre : groupes, anneaux et corps

Barème du contrôle

Exercice	Points
Exercice 1 : Questions de cours	4 points
Exercice 2 : Idéaux, nilpotents et inversibles de $\mathbb{Z}/45\mathbb{Z}$	5 points
Exercice 3 : Action de S_4 sur les appariements	4 points
Exercice 4 : Problème : polynômes irréductibles sur $\mathbb{F}_3$ et corps à 9 éléments	7 points
Total	20 points

Exercice 1 : Questions de cours (4 points)

- a. **Relation orbite-stabilisateur.** On a $|\omega(x)| = [G : \text{Stab}(x)] = \frac{|G|}{|\text{Stab}(x)|}$, où $\omega(x)$ désigne l'orbite de x .

Démonstration. Posons $H = \text{Stab}(x)$, qui est un sous-groupe de G . Considérons l'application $\Phi : G/H \rightarrow \omega(x)$, $gH \rightarrow g \cdot x$.

Elle est bien définie et injective, car $gH = g'H$ équivaut à $g^{-1}g' \in H$, c'est-à-dire à $g^{-1}g' \cdot x = x$, soit $g \cdot x = g' \cdot x$. Elle est surjective par définition de l'orbite. **Donc** $|\omega(x)| = [G : H]$, et le théorème de Lagrange donne la seconde égalité.

- b. Soit A un anneau intègre fini et $a \in A$ non nul. L'application $m_a : x \rightarrow ax$ est injective. En effet, $ax = ay$ donne $a(x - y) = 0$, donc $x = y$ par intégrité.

Une application injective d'un ensemble fini dans lui-même est bijective. Il existe donc $b \in A$ tel que $ab = 1$. **Tout élément non nul est inversible : A est un corps.**

- c. Le morphisme d'anneaux $\mathbb{Z} \rightarrow K, k \rightarrow k \cdot 1_K$, ne peut pas être injectif, car K est fini. Son noyau est donc $p\mathbb{Z}$ avec $p \geq 2$. Alors $\mathbb{Z}/p\mathbb{Z}$ s'identifie à un sous-anneau de K , donc il est intègre : **p est premier.**

Ainsi K contient un sous-corps isomorphe à $\mathbb{F}_p$. C'est donc un $\mathbb{F}_p$ -espace vectoriel, de dimension finie r puisque K est fini. **Par conséquent $|K| = p^r$.**

Barème : a) 0,5 point pour l'énoncé, 1 point pour la démonstration ; b) 1 point pour l'injectivité, 0,5 point pour la conclusion ; c) 0,5 point pour la caractéristique, 0,5 point pour le cardinal.

Exercice 2 : Idéaux, nilpotents et inversibles de $\mathbb{Z}/45\mathbb{Z}$ (5 points)

- a. La classe $\bar{k}$ est inversible si et seulement s'il existe u tel que $ku \equiv 1 \pmod{45}$. Cela revient à l'existence d'entiers u et v tels que $ku + 45v = 1$. **Par le théorème de Bézout, cela équivaut à $\text{pgcd}(k, 45) = 1$.**

- b. On effectue les divisions $45 = 6 \times 7 + 3$, puis $7 = 2 \times 3 + 1$. On remonte ensuite les calculs :

$$1 = 7 - 2 \times 3 = 7 - 2(45 - 6 \times 7) = 13 \times 7 - 2 \times 45.$$

Vérification : $7 \times 13 = 91 = 2 \times 45 + 1$. **L'inverse de $\bar{7}$ est $\bar{13}$.**

- c. Les diviseurs positifs de $45 = 3^2 \times 5$ sont 1, 3, 5, 9, 15 et 45. **Les idéaux de A sont donc $A, (\bar{3}), (\bar{5}), (\bar{9}), (\bar{15})$ et $\{0\}$.**

Le quotient $A/(\bar{d})$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$, qui est un corps si et seulement si d est premier.

Les idéaux maximaux sont $(\bar{3})$ et $(\bar{5})$.

Si $\bar{x}$ est nilpotent, alors 45 divise x^k . Donc 3 et 5 divisent x^k , puis divisent x car ils sont premiers. Ainsi 15 divise x . Réciproquement, si $x = 15m$, alors

$$x^2 = 225m^2 = 45 \times 5m^2, \text{ donc } \bar{x}^2 = \bar{0}. \text{ Les nilpotents forment l'idéal } (\bar{15}) = \{\bar{0}, \bar{15}, \bar{30}\}.$$

d. D'après a), $|A^*| = \varphi(45) = \varphi(9)\varphi(5) = 6 \times 4 = 24$.

Soit x premier avec 45. Le théorème d'Euler donne $x^6 \equiv 1 \pmod{9}$, car $\varphi(9) = 6$. Le petit théorème de Fermat donne $x^4 \equiv 1 \pmod{5}$. Donc $x^{12} \equiv 1$ modulo 9 et modulo 5. Comme 9 et 5 sont premiers entre eux, le théorème chinois donne $x^{12} \equiv 1 \pmod{45}$.

Tout élément de A^* est donc d'ordre au plus 12, alors que $|A^*| = 24$. **Le groupe A^* n'est pas cyclique.**

Testons $\bar{2}$. On a $2^4 = 16$ et $2^6 = 64 \equiv 19 \pmod{45}$, qui diffèrent de 1. Or $2^{12} = 4096 = 91 \times 45 + 1$. L'ordre de $\bar{2}$ divise 12, mais ne divise ni 4 ni 6. **Donc $\bar{2}$ est d'ordre 12.**

Barème : a) 1 point ; b) 0,5 point pour l'algorithme, 0,5 point pour l'inverse vérifié ; c) 0,5 point pour la liste, 0,5 point pour les maximaux, 0,5 point pour les nilpotents ; d) 0,5 point pour $\varphi(45)$, 0,5 point pour $x^{12} = 1$ et la non-cyclicité, 0,5 point pour l'élément d'ordre 12.

Exercice 3 : Action de S_4 sur les appariements (4 points)

a. Comme σ est une bijection, les paires $\{\sigma(a), \sigma(b)\}$ et $\{\sigma(c), \sigma(d)\}$ sont disjointes et recouvrent $\{1, 2, 3, 4\}$. Donc $\sigma \cdot x \in X$. De plus, $\text{id} \cdot x = x$ et $\sigma \cdot (\tau \cdot x) = (\sigma \circ \tau) \cdot x$. **C'est bien une action.**

b. On a $(2\ 3) \cdot x_1 = \{\{1, 3\}, \{2, 4\}\} = x_2$ et $(2\ 4) \cdot x_1 = \{\{1, 4\}, \{3, 2\}\} = x_3$.

L'orbite de x_1 est donc X tout entier.

Par la relation orbite-stabilisateur, $|\text{Stab}(x_1)| = \frac{24}{3} = 8$. Il s'agit des permutations qui conservent la paire $\{1, 2\}$ ou l'échangent avec $\{3, 4\}$:

$$\text{Stab}(x_1) = \{\text{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\}.$$

- c. Le noyau de ρ est l'intersection des stabilisateurs de x_1 , x_2 et x_3 . Cherchons les éléments de $\text{Stab}(x_1)$ qui fixent aussi $x_2 = \{\{1, 3\}, \{2, 4\}\}$.

D'abord, $(1\ 2)$, $(3\ 4)$, $(1\ 3\ 2\ 4)$ et $(1\ 4\ 2\ 3)$ envoient x_2 sur x_3 . Par exemple, $(1\ 2)$ envoie $\{1, 3\}$ sur $\{2, 3\}$.

En revanche, les trois doubles transpositions fixent x_2 . Par exemple, $(1\ 2)(3\ 4)$ envoie $\{1, 3\}$ sur $\{2, 4\}$, et $\{2, 4\}$ sur $\{1, 3\}$. Un élément qui fixe x_1 et x_2 fixe aussi x_3 , car il permute les trois appariements.

Donc $\text{Ker } \rho = V_4$.

- d. Un noyau de morphisme est distingué : **V_4 est distingué dans S_4** . Par le premier théorème d'isomorphisme, $S_4 / V_4 \simeq \text{Im } \rho$.

Cette image est d'ordre $\frac{24}{4} = 6 = |S(X)|$, donc ρ est surjectif. Enfin, $S(X)$ est isomorphe à S_3 , puisque X a trois éléments. **Par conséquent $S_4 / V_4 \simeq S_3$.**

Barème : a) 0,5 point ; b) 0,5 point pour l'orbite et l'ordre, 0,5 point pour la liste ; c) 1,5 point (intersection des stabilisateurs, exclusion des quatre autres éléments, vérification sur V_4) ; d) 0,5 point pour la distinction, 0,5 point pour l'isomorphisme.

Erreur fréquente : affirmer que ρ est surjectif sans argument ; ici, c'est le calcul du noyau qui le donne.

Exercice 4 : Problème : polynômes irréductibles sur $\mathbb{F}_3$ et corps à 9 éléments (7 points)

Partie A : un corps à 9 éléments

a. Le polynôme $X^2 + 1$ prend les valeurs 1, 2 et $5 \equiv 2$ en 0, 1 et 2. De degré 2 sans racine dans $\mathbb{F}_3$, il est irréductible. L'idéal $(X^2 + 1)$ est donc maximal dans l'anneau principal $\mathbb{F}_3[X]$, et K est un corps. Tout élément de K s'écrit de façon unique $a + bi$ avec $a, b \in \mathbb{F}_3$ (reste de la division euclidienne). **Donc** $|K| = 9$.

b. On a $i^2 = -1 \neq 1$ et $i^4 = 1$, donc i est d'ordre 4. **Il n'engendre pas K^* , qui est d'ordre 8.**

Ensuite, $(1 + i)^2 = 1 + 2i + i^2 = 2i$, puis $(1 + i)^4 = (2i)^2 = 4i^2 = -4 = -1$ dans $\mathbb{F}_3$. L'ordre de $1 + i$ divise 8 mais pas 4. **Il vaut donc 8, et $1 + i$ engendre K^* .**

k	1	2	3	4	5	6	7	8
$(1 + i)^k$	$1 + i$	$2i$	$1 + 2i$	2	$2 + 2i$	i	$2 + i$	1

Par exemple, $(1 + i)^3 = 2i(1 + i) = 2i + 2i^2 = -2 + 2i = 1 + 2i$. Les huit éléments non nuls apparaissent chacun une fois.

c. Posons $\alpha = 1 + i$. On a $(\alpha - 1)^2 = i^2 = -1$, soit $\alpha^2 - 2\alpha + 2 = 0$. Dans $\mathbb{F}_3$, $-2 = 1$, d'où $\alpha^2 + \alpha + 2 = 0$. Contrôle : $2i + (1 + i) + 2 = 3 + 3i = 0$.

Comme $\alpha \notin \mathbb{F}_3$, son degré vaut 2. **Son polynôme minimal est donc $X^2 + X + 2$.**

Le morphisme $\mathbb{F}_3[X] \rightarrow K, P \mapsto P(\alpha)$, est surjectif. En effet, son image est un sous-anneau contenant α , donc $i = \alpha - 1$. Son noyau est l'idéal engendré par le polynôme minimal. **Par le premier théorème d'isomorphisme, $K \simeq \mathbb{F}_3[X]/(X^2 + X + 2)$.**

Partie B : dénombrement de polynômes irréductibles

d. Il y a 9 polynômes unitaires $X^2 + aX + b$. Les réductibles s'écrivent $(X - u)(X - v)$. On en compte 3 avec $u = v$ et 3 avec $\{u, v\}$ formé de deux éléments distincts, soit 6. Il reste donc 3 irréductibles. **Ce sont** $X^2 + 1$, $X^2 + X + 2$ **et** $X^2 + 2X + 2$. Pour le dernier, les valeurs en 0, 1 et 2 sont 2, 2 et 1 : il n'a pas de racine.

e. Soit $L = \mathbb{F}_3[X]/(Q)$, corps à 3^d éléments, et x la classe de X . Le polynôme Q est le polynôme minimal de x .

Supposons $d \in \{1, 2\}$. Alors $|L^*| = 3^d - 1$ divise 8, donc $y^8 = 1$ pour tout $y \neq 0$ par le théorème de Lagrange. Ainsi $y^9 = y$ pour tout $y \in L$. En particulier, $x^9 = x$, donc Q divise $X^9 - X$.

Réciproquement, supposons que Q divise $X^9 - X$, donc $x^9 = x$. L'application $y \rightarrow y^9$ est un morphisme d'anneaux, car c'est le carré du morphisme de Frobenius $y \rightarrow y^3$. Elle fixe $\mathbb{F}_3$ et x , donc tout $L = \mathbb{F}_3[x]$. Ainsi $y^8 = 1$ pour tout $y \in L^*$. Si g engendre le groupe cyclique L^* , son ordre $3^d - 1$ divise 8. Par conséquent $d \leq 2$.

Enfin, $X^9 - X$ a pour dérivée $9X^8 - 1 = -1$, qui est premier avec lui : il n'a pas de facteur carré. Il est donc le produit de ses facteurs irréductibles unitaires distincts, qui sont exactement ceux de degré 1 ou 2. **Ainsi**

$X^9 - X = X(X - 1)(X - 2)(X^2 + 1)(X^2 + X + 2)(X^2 + 2X + 2)$. Contrôle des degrés : $3 \times 1 + 3 \times 2 = 9$.

f. Le même raisonnement montre que Q divise $X^{27} - X$ si et seulement si $3^d - 1$ divise 26. Or les diviseurs de 26 sont 1, 2, 13 et 26, et $3^d - 1$ vaut 2, 8, 26, puis dépasse 26. Donc $d \in \{1, 3\}$.

De plus, $X^{27} - X$ est sans facteur carré, car sa dérivée vaut -1 . En notant N_3 le nombre d'irréductibles unitaires de degré 3, les degrés donnent $27 = 3 \times 1 + 3 N_3$. **Il y a donc**
 $N_3 = 8$ polynômes unitaires irréductibles de degré 3 sur $\mathbb{F}_3$.

Barème : a) 0,5 point pour l'irréductibilité, 0,5 point pour le cardinal ; b) 0,5 point pour l'ordre de i , 0,5 point pour l'ordre de $1 + i$, 0,5 point pour le tableau ; c) 0,5 point pour le polynôme minimal, 0,5 point pour l'isomorphisme ; d) 1 point ; e) 0,5 point par sens de l'équivalence, 0,5 point pour la factorisation ; f) 0,5 point pour la condition sur d , 0,5 point pour le résultat 8.

Erreur fréquente : oublier que $X^9 - X$ est sans facteur carré, ce qui empêche de conclure au produit exact.

[Revenir à l'énoncé du contrôle](#)

Après le corrigé du contrôle : partiel d'algèbre : groupes, anneaux et corps

Pour consolider ce que le corrigé vous a appris, relisez le cours « [Groupes et actions](#) » en L3 et « [Anneaux et idéaux](#) » en L3 et « [Corps et extensions](#) » en L3 puis entraînez-vous avec les **exercices corrigés** [groupes et actions](#), [anneaux et idéaux](#), [corps et extensions](#).

Retrouvez tous les [contrôles de maths de L3 classés par chapitre](#), ou choisissez un autre niveau sur la page [contrôles de maths du CP au post-bac](#).

Autres contrôles de maths de L3 sur ce thème

- [Contrôle de maths L3 : groupes quotients et actions de groupes](#)
- [Contrôle de maths L3 : anneaux, idéaux et polynômes irréductibles](#)
- [Contrôle de maths L3 : extensions de corps et corps finis](#)