# Plaquette 3 – Anneaux, idéaux, Z/nZ et théorème chinois

## Structures algébriques — Prépa MP / MPI (2e année)

Corrections détaillées

**Boîte à outils**

**Anneaux et idéaux.**

— Idéal $I$ de $A$ commutatif : sous-groupe additif stable par multiplication par tout élément de $A$ ; $aA$ est l'idéal engendré par $a$.

— $\mathbb{Z}$ et K[$X$] sont **principaux** : $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$, $(P) + (Q) = (P \wedge Q)$.

— Dans $\mathbb{Z}/n\mathbb{Z}$ : $\overline{k}$ inversible $\Leftrightarrow k \wedge n = 1$ ; sinon $\overline{k}$ est diviseur de zéro (ou nul). $\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow n$ premier.

— **Théorème chinois** : si $m \wedge n = 1$, la réduction $x \bmod mn \mapsto (x \bmod m, x \bmod n)$ est un isomorphisme d'anneaux

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

— $\varphi$ est multiplicative : $\varphi(n) = n\prod_{p \mid n}\left(1 - \frac{1}{p}\right)$ ; **Euler** : $a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$.

— **Caractéristique** d'un anneau intègre : 0 ou un nombre premier $p$ ; en caractéristique $p$, $(a+b)^p = a^p + b^p$.

## Correction de l'exercice 1 – Les idéaux de Z/nZ

a) $\pi^{-1}(J)$ est un sous-groupe de $\mathbb{Z}$ ; si $x \in \pi^{-1}(J)$ et $a \in \mathbb{Z}$, $\pi(ax) = \overline{a}\,\pi(x) \in J$. Il contient $\pi^{-1}(\{\overline{0}\}) = n\mathbb{Z}$.

b) $\pi^{-1}(J) = d\mathbb{Z}$ avec $n \in d\mathbb{Z}$, soit $d \mid n$, et $J = \pi(d\mathbb{Z}) = \overline{d}\,\mathbb{Z}/n\mathbb{Z}$ ($\pi$ surjective). Deux diviseurs positifs distincts donnent des idéaux distincts (de cardinaux $\frac{n}{d}$ différents).

c) Diviseurs de 12 : idéaux $(\overline{1}) = \mathbb{Z}/12\mathbb{Z}$, $(\overline{2})$, $(\overline{3})$, $(\overline{4})$, $(\overline{6})$, $(\overline{0})$. Inclusions : $(\overline{d}) \subset (\overline{d'}) \Leftrightarrow d' \mid d$. Idéaux maximaux :

$$(\overline{2}) \quad \text{et} \quad (\overline{3})$$

— correspondant aux diviseurs premiers de 12 ; les quotients $(\mathbb{Z}/12\mathbb{Z})/(\overline{2}) \simeq \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ sont des corps.

**Réponse.** Idéaux $(\overline{d})$ pour $d \mid n$ ; pour 12 : six idéaux, maximaux $(\overline{2})$ et $(\overline{3})$.

## Correction de l'exercice 2 – Diviseurs de zéro et nilpotents de Z/nZ

a) Si $d = k \wedge n = 1$, $\overline{k}$ est inversible (Bézout). Sinon, $\frac{n}{d} \cdot k = n\frac{k}{d} \equiv 0$ avec $\frac{n}{d} \not\equiv 0$ : $\overline{k}$ est diviseur de zéro.

b) $\overline{k}^m = \overline{0} \Leftrightarrow n \mid k^m$. Si $n = \prod p_i^{\alpha_i}$ et chaque $p_i \mid k$, alors pour $m \geq \max \alpha_i$, $p_i^{\alpha_i} \mid k^m$ pour tout $i$, donc $n \mid k^m$. Réciproquement, si $n \mid k^m$, chaque $p_i$ divise $k^m$, donc $k$ (lemme d'Euclide).

c) $12 = 2^2 \times 3$ : nilpotents = multiples de 6 : $\overline{0}, \overline{6}$. $72 = 2^3 \times 3^2$ : multiples de 6, soit $\frac{72}{6} = 12$ nilpotents.

d) Les nilpotents sont les multiples de $r = \prod_{p \mid n} p$ (le **radical**) ; il n'y a que $\overline{0}$ si et seulement si $r = n$, c'est-à-dire si $n$ est sans facteur carré.

**Réponse.** Inversible ou diviseur de zéro ; nilpotents = multiples du radical ; $\{0, 6\}$ dans $\mathbb{Z}/12$, 12 dans $\mathbb{Z}/72$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

## Correction de l'exercice 3 – Calculer un inverse modulaire

a) $26 = 3 \times 7 + 5$, $7 = 5 + 2$, $5 = 2 \times 2 + 1$. En remontant :

$$1 = 5 - 2 \times 2 = 5 - 2(7 - 5) = 3 \times 5 - 2 \times 7 = 3(26 - 3 \times 7) - 2 \times 7 = 3 \times 26 - 11 \times 7$$

— donc $-11 \times 7 \equiv 1$ et $\overline{7}^{-1} = \overline{-11} = \overline{15}$. Contrôle : $7 \times 15 = 105 = 4 \times 26 + 1$.

b) $7x \equiv 8$, donc $x \equiv 15 \times 8 = 120 \equiv 120 - 104 = 16 \pmod{26}$. Contrôle : $7 \times 16 + 3 = 115 = 4 \times 26 + 11$.

c) $6 \wedge 26 = 2$ divise 4 : on simplifie par 2, $3x \equiv 2 \pmod{13}$ ; l'inverse de 3 modulo 13 est 9 ($27 \equiv 1$), donc $x \equiv 18 \equiv 5 \pmod{13}$ : solutions $x \equiv 5$ ou $18 \pmod{26}$.

d) Avec $d = a \wedge n$ : solutions si et seulement si $d \mid b$, et il y en a alors exactement $d$ modulo $n$.

**Réponse.** $\overline{7}^{-1} = \overline{15}$ ; $x \equiv 16$ ; $6x \equiv 4$ : $x \equiv 5, 18 \pmod{26}$ ; condition $a \wedge n \mid b$, $a \wedge n$ solutions.

## Correction de l'exercice 4 – Résoudre un système de congruences

a) 3, 5, 7 sont deux à deux premiers entre eux : par le théorème chinois, $\mathbb{Z}/105\mathbb{Z} \simeq \mathbb{Z}/3 \times \mathbb{Z}/5 \times \mathbb{Z}/7$, et tout triplet de restes a un unique antécédent modulo 105.

b) $e_3$ est un multiple de 35 congru à 1 modulo 3 : $35 \equiv 2$, $70 \equiv 1$, donc $e_3 = 70$. $e_5$ multiple de 21 congru à 1 modulo 5 : $21 \equiv 1$, $e_5 = 21$. $e_7$ multiple de 15 congru à 1 modulo 7 : $15 \equiv 1$, $e_7 = 15$.

c) Par linéarité de l'isomorphisme :

$$x \equiv 2e_3 + 3e_5 + 2e_7 = 140 + 63 + 30 = 233 \equiv 233 - 210 = 23 \pmod{105}$$

— Contrôle : $23 = 7 \times 3 + 2 = 4 \times 5 + 3 = 3 \times 7 + 2$.

d) $x \equiv 1 \pmod{4}$ impose $x$ impair ; $x \equiv 3 \pmod{6}$ aussi ; modulo $\text{pgcd}(4, 6) = 2$, les deux conditions donnent $x \equiv 1$ : compatibles. Solutions modulo ppcm $= 12$ : $x \equiv 9 \pmod{12}$ ($9 \equiv 1 \pmod{4}$, $9 \equiv 3 \pmod{6}$).

**Réponse.** $x \equiv 23 \pmod{105}$ ; d) $x \equiv 9 \pmod{12}$.

## Correction de l'exercice 5 – Indicatrice d'Euler multiplicative

a) Un isomorphisme d'anneaux envoie les inversibles sur les inversibles, et les inversibles d'un produit sont les couples d'inversibles. En prenant les cardinaux : $\varphi(mn) = \varphi(m)\varphi(n)$.

b) Les non-inversibles de $\mathbb{Z}/p^\alpha\mathbb{Z}$ sont les multiples de $p$, au nombre de $p^{\alpha-1}$ :

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right)$$

c) On écrit $n = \prod p_i^{\alpha_i}$ et l'on multiplie. $360 = 2^3 \times 3^2 \times 5$ : $\varphi(360) = 360 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 96$.

d) Non : $\varphi(4) = 2$ alors que $\varphi(2)^2 = 1$. La coprimalité est nécessaire.

**Réponse.** $\varphi(mn) = \varphi(m)\varphi(n)$ si $m \wedge n = 1$ ; $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ ; $\varphi(360) = 96$.

## Correction de l'exercice 6 – Grandes puissances modulo n

a) $7^2 = 49$, $7^4 = 2\,401 \equiv 1 \pmod{100}$. Comme $2026 = 4 \times 506 + 2$ :

$$7^{2026} = (7^4)^{506} \times 7^2 \equiv 49 \pmod{100}$$

— les deux derniers chiffres sont 49.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

b) $3 \wedge 13 = 1$ donc $3^{12} \equiv 1$ ; $100 = 12 \times 8 + 4$ : $3^{100} \equiv 3^4 = 81 \equiv 81 - 78 = 3 \pmod{13}$.

c) Modulo 3 : $2 \equiv -1$, $2^{2026} \equiv 1$. Modulo 5 : $2^4 \equiv 1$ et $2026 \equiv 2 \pmod 4$, donc $2^{2026} \equiv 4$. Le reste modulo 15 vérifie $x \equiv 1 \pmod 3$ et $x \equiv 4 \pmod 5$ : $x = 4$.

d) Pour $p \in \{2, 3, 5, 7, 13\}$, $p - 1$ divise 12, donc $n^{13} = n \cdot (n^{p-1})^{12/(p-1)} \equiv n \pmod p$ si $p \nmid n$, et c'est évident si $p \mid n$. Les cinq premiers divisent $n^{13} - n$, donc leur produit 2 730 aussi.

**Réponse.** $7^{2026} \equiv 49 \pmod{100}$ ; $3^{100} \equiv 3 \pmod{13}$ ; $2^{2026} \equiv 4 \pmod{15}$ ; $2730 \mid n^{13} - n$.

## Correction de l'exercice 7 – Idempotents de Z/nZ

a) $e^2 = e \Leftrightarrow e(e-1) \equiv 0 \pmod{p^\alpha}$. Comme $e$ et $e - 1$ sont premiers entre eux, $p$ ne peut diviser les deux : $p^\alpha$ divise $e$ ou $e - 1$, donc $e \equiv 0$ ou $e \equiv 1$.

b) Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, $\mathbb{Z}/n\mathbb{Z} \simeq \prod \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$, et un élément du produit est idempotent si et seulement si chaque composante l'est : $2^r$ choix.

c) $12 = 4 \times 3$ : quatre idempotents, correspondant aux couples (mod 4, mod 3) $(0, 0)$, $(1, 1)$, $(1, 0)$, $(0, 1)$, soit $\overline{0}$, $\overline{1}$, $\overline{9}$ ($9 \equiv 1 \pmod 4$, $9 \equiv 0 \pmod 3$) et $\overline{4}$.

$$4^2 = 16 \equiv 4, \qquad 9^2 = 81 \equiv 9 \pmod{12}$$

**Réponse.** $\overline{0}, \overline{1}$ modulo $p^\alpha$ ; $2^r$ idempotents ; pour 12 : $0, 1, 4, 9$.

## Correction de l'exercice 8 – Racines carrées de l'unité modulo n

a) $p \mid (x-1)(x+1)$, et $p$ ne peut diviser les deux (sinon $p \mid 2$). Donc $p^\alpha$ divise entièrement $x - 1$ ou $x + 1$ : deux solutions $\pm 1$ modulo $p^\alpha$.

b) $15 = 3 \times 5$ : deux solutions modulo 3, deux modulo 5, donc $2 \times 2 = 4$ solutions modulo 15 :

$$x \in \{1, 4, 11, 14\} \pmod{15}$$

— ($4^2 = 16$, $11^2 = 121 = 8 \times 15 + 1$, $14 \equiv -1$).

c) $n \mid (x-1)(x+1)$ sans diviser $x - 1$ ni $x + 1$ (car $x \neq \pm 1$) : $\gcd(x - 1, n)$ n'est ni 1 (sinon $n \mid x + 1$ par Gauss) ni $n$. Pour $x = 4$ : $\gcd(3, 15) = 3$, et $\gcd(5, 15) = 5$. C'est le principe de plusieurs algorithmes de factorisation.

**Réponse.** $\pm 1$ modulo $p^\alpha$ ; 4 solutions modulo 15 : $1, 4, 11, 14$ ; $\gcd(x - 1, n)$ factorise $n$.

## Correction de l'exercice 9 – Idéaux de polynômes et pgcd

a) $P = (X-1)(X^2 + X + 1)$, $Q = (X-1)(X-2)$, et $X^2 + X + 1$ n'a pas de racine commune avec $X - 2$ ($4 + 2 + 1 \neq 0$). Donc $P \wedge Q = X - 1$ et

$$(P) + (Q) = (X - 1)$$

b) On divise par $X - 1$ : $A = X^2 + X + 1$, $B = X - 2$. Division : $A = (X + 3)B + 7$. Donc $7 = A - (X + 3)B$, et en multipliant par $\frac{X-1}{7}$ :

— $X - 1 = \frac{1}{7}P - \frac{X+3}{7}Q$.

c) $(P) \cap (Q) = (\mathrm{ppcm}(P, Q)) = ((X-1)(X-2)(X^2 + X + 1))$.

d) $(X - 1) \mid X^2 + 1$ si et seulement si 1 est racine : $1 + 1 = 2 \neq 0$. Non.

**Réponse.** $(P) + (Q) = (X - 1)$ ; $X - 1 = \frac{1}{7}P - \frac{X+3}{7}Q$ ; $(P) \cap (Q) = ((X-1)(X-2)(X^2 + X + 1))$ ; d) non.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

## Correction de l'exercice 10 – Un idéal non principal

a) $2A + XB$ a pour coefficient constant $2A(0)$, pair. Réciproquement, si $P(0) = 2c$, on écrit $P = 2c + X\dfrac{P - P(0)}{X}$.

b) $2 \in (D)$ : $2 = DE$ dans $\mathbb{Z}[X]$, donc $\deg D = 0$ et $D$ est un entier divisant 2. Si $D = \pm 1$, $I = \mathbb{Z}[X]$, or $1 \notin I$. Si $D = \pm 2$, tous les éléments de $I$ ont des coefficients pairs, or $X \in I$. Contradiction.

c) $\mathbb{Z}[X]$ n'est pas **principal** (bien qu'intègre). Dans $\mathbb{Q}[X]$, 2 est inversible : $(2, X) = \mathbb{Q}[X] = (1)$, l'idéal est principal. C'est la division euclidienne (possible car $\mathbb{Q}$ est un corps) qui rend $\mathrm{K}[X]$ principal.

**Réponse.** $I$ = polynômes à constante paire ; pas de générateur ; $\mathbb{Z}[X]$ non principal.

## Correction de l'exercice 11 – Un anneau intègre fini est un corps

a) $ax = ay \Rightarrow a(x - y) = 0 \Rightarrow x = y$ (intégrité). Une injection d'un ensemble fini dans lui-même est bijective.

b) 1 a un antécédent : il existe $b$ avec $ab = 1$.

$$A \text{ intègre et fini} \Longrightarrow A \text{ corps}$$

c) $\mathbb{Z}/p\mathbb{Z}$ est intègre ($p \mid xy \Rightarrow p \mid x$ ou $p \mid y$) et fini. Le quotient $\mathrm{F}_2[X]/(X^2 + X + 1)$ a 4 éléments ; intègre, c'est un corps à 4 éléments.

d) Oui : $\mathbb{Z}$ est intègre, infini, et 2 n'y est pas inversible.

**Réponse.** $x \mapsto ax$ bijective, donc $a$ inversible ; corps $\mathbb{Z}/p\mathbb{Z}$, $\mathrm{F}_4$ ; $\mathbb{Z}$ contre-exemple infini.

## Correction de l'exercice 12 – Morphismes d'anneaux entre Z/nZ

a) Un morphisme $f$ vérifie $f(\overline{1}) = \overline{1}$, donc $f(\overline{k}) = \overline{k}$ : il est unique. Il est bien défini si et seulement si $n \equiv 0$ implique $n \cdot \overline{1} = \overline{0}$ dans $\mathbb{Z}/m\mathbb{Z}$, soit $m \mid n$ ; c'est alors la réduction modulo $m$.

b) Morphismes de groupes : $12 \wedge 4 = 4$. Morphismes d'anneaux : $4 \mid 12$, un seul (la réduction modulo 4).

c) $\mathbb{Z}/2 \times \mathbb{Z}/2$ est de caractéristique 2 ($(1,1) + (1,1) = 0$) ; un morphisme $f$ vérifierait $f(\overline{2}) = 2f(\overline{1}) = 0$. Le morphisme $\overline{k} \mapsto (\overline{k}, \overline{k})$ convient (bien défini car $2 \mid 4$). Pas d'isomorphisme : $\mathbb{Z}/4\mathbb{Z}$ a un élément d'ordre additif 4, pas le produit (théorème chinois inapplicable car $2 \wedge 2 \neq 1$).

**Réponse.** Morphisme d'anneaux $\Leftrightarrow m \mid n$, unique ; b) 4 morphismes de groupes, 1 d'anneaux ; c) oui, pas d'isomorphisme.

## Correction de l'exercice 13 – Caractéristique d'un anneau intègre

a) Si $c = ab$ avec $1 < a, b < c$, alors $(a \cdot 1)(b \cdot 1) = c \cdot 1 = 0$ avec $a \cdot 1 \neq 0$ et $b \cdot 1 \neq 0$ (minimalité de $c$) : $A$ n'est pas intègre.

b) $A$ fini : $\chi$ n'est pas injective, donc $c \neq 0$, et $c = p$ premier (corps donc intègre). Par le théorème d'isomorphisme :

$$\mathbb{Z}/p\mathbb{Z} \simeq \mathrm{Im}\chi \subset A$$

c) $A$ est un espace vectoriel sur ce sous-corps $\mathrm{F}_p$ (la multiplication de $A$ fournit la loi externe), de dimension finie $k$ : $\mathrm{card} A = p^k$. Par exemple, il n'existe pas de corps à 6 éléments.

**Réponse.** Caractéristique 0 ou premier ; corps fini : sous-corps $\mathrm{F}_p$, cardinal $p^k$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

## Correction de l’exercice 14 – Le morphisme de Frobenius

a) $F(xy) = x^p y^p$ (commutativité), $F(1) = 1$ et, par le binôme,

$$(x+y)^p = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k} = x^p + y^p$$

— car chaque $\binom{p}{k}$ est multiple de $p$, donc nul dans $A$.

b) $x^p = 0 \Rightarrow x = 0$ par intégrité : noyau nul, $F$ injectif ; injectif sur un ensemble fini, il est bijectif.

c) Petit Fermat : $a^p = a$ dans $\mathrm{F}_p$. $F(1+X) = 1 + X^p$.

d) $(1+X)^9 = ((1+X)^3)^3 = (1+X^3)^3 = 1 + X^9$ dans $\mathrm{F}_3[X]$.

**Réponse.** $F$ morphisme ; bijectif sur un corps fini ; $(1+X)^p = 1 + X^p$ ; $(1+X)^9 = 1 + X^9$ dans $\mathrm{F}_3[X]$.

## Correction de l’exercice 15 – Synthèse : RSA avec le théorème chinois

a) $\varphi(55) = 4 \times 10 = 40$. $3d \equiv 1 \pmod{40}$ : $3 \times 27 = 81 = 2 \times 40 + 1$, donc $d = 27$.

b) $c = 2^3 = 8$.

c) $ed = 1 + 40k$, donc $c^d = m^{ed} = m \cdot (m^{40})^k \equiv m$ si $m \wedge 55 = 1$ (Euler). Sur l’exemple :

— modulo 5 : $8 \equiv 3$, $3^{27} = (3^4)^6 \times 3^3 \equiv 27 \equiv 2$ ;

— modulo 11 : $8^{27} = (8^{10})^2 \times 8^7 \equiv 8^7$, et $8^2 = 64 \equiv 9$, $8^4 \equiv 81 \equiv 4$, $8^7 = 8^4 \times 8^2 \times 8 \equiv 4 \times 9 \times 8 = 288 \equiv 2$.

— $c^d \equiv 2 \pmod{5}$ et $\pmod{11}$, donc $c^d \equiv 2 \pmod{55}$ (théorème chinois) : on retrouve $m$.

d) Si $5 \mid m$ : modulo 5, $m^{ed} \equiv 0 \equiv m$ ; modulo 11, $m \wedge 11 = 1$ ou $11 \mid m$, et dans les deux cas $m^{ed} \equiv m$ (Fermat, $10 \mid ed - 1$). Par le théorème chinois, $m^{ed} \equiv m \pmod{55}$ pour **tout** $m$.

**Réponse.** $\varphi = 40$, $d = 27$ ; $c = 8$ ; $8^{27} \equiv 2 \pmod{55}$ ; RSA fonctionne pour tout $m$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s’expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).