Agrégation Interne

L'anneau $\mathbb{Z}/n\mathbb{Z}$

[1]

Ce problème est en relation avec les leçons d'oral suivantes :

- 101 : Groupes monogènes, groupes cycliques. Exemples.
- 103 : Congruences dans $\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$. Applications.

On pourra consulter les ouvrages suivants.

- F. Combes — *Algèbre et géométrie.* Bréal (2003).
- S. Francinou, H. Gianella, S. Nicolas : *Exercices de mathématiques. Oraux X-ENS. Algèbre 1.* Cassini (2001).
- S. Francinou, H. Gianella. *Exercices de mathématiques pour l'agrégation. Algèbre 1.* Masson (1994).
- X. Gourdon. *Les Maths en tête. Algèbre.* Ellipses.
- K. Madere. *Préparation à l'oral de l'agrégation. Leçons d'algèbre.* Ellipses (1998).
- P. Ortiz. *Exercices d'algèbre.* Ellipses (2004).
- D. Perrin. *Cours d'algèbre.* Ellipses (1996).
- A. Szpirglas. *Mathématiques L3. Algèbre.* Pearson (2009).

1 Énoncé

Pour tout entier naturel $n \geq 0$, on note $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ l'anneau des classes résiduelles modulo n.
Si k est un entier relatif, on note $\overline{k} = k + n\mathbb{Z}$ la classe de k dans $\mathbb{Z}_n$.
Pour tout couple (a, b) d'entiers relatifs, on note $a \wedge b$ le pgcd de a et b et $a \vee b$ leur ppcm .

– I – Ordre d'un élément dans un groupe

On se donne un groupe additif $(G, +)$ non nécessairement commutatif et on note 0 son élément neutre.
Le cardinal de G est aussi appelé l'ordre de G.
Si H est une partie non vide G, on note, pour tout $g \in G$:

$$g + H = \{g + h \mid h \in H\}$$

Pour tout g dans G, on note $\langle g \rangle = \{kg \mid k \in \mathbb{Z}\}$ le sous groupe de G engendré par g.
Ce sous-groupe $\langle g \rangle$ est l'image du morphisme de groupes :

$$\begin{array}{rccc} \varphi_g : & \mathbb{Z} & \to & G \\ & k & \mapsto & kg \end{array}$$

L'ordre d'un élément g de G est l'élément $\theta(g) \in \mathbb{N}^* \cup \{+\infty\}$ défini par :

$$\theta(g) = \operatorname{card}(\langle g \rangle)$$

Si $\theta(g)$ est dans $\mathbb{N}^*$, on dit alors que g est d'ordre fini, sinon on dit qu'il est d'ordre infini.

1. Rappeler la démonstration du théorème de Lagrange : pour tout sous-groupe H d'un groupe fini G, l'ordre de H divise l'ordre de G.

1. Le 26/09/2013

2. Montrer que :

$$(\theta(g) = +\infty) \Leftrightarrow (\forall k \in \mathbb{Z}^*,\ kg \neq 0) \Leftrightarrow (\langle g \rangle \text{ est infini isomorphe à } \mathbb{Z})$$

(dans ce cas, on dit que $\langle g \rangle$ est monogène infini) et :

$$\begin{aligned}(\theta(g) = n \in \mathbb{N}^*) &\Leftrightarrow (\langle g \rangle = \{rg \mid 0 \leq r \leq n-1\}) \\ &\Leftrightarrow (k \in \mathbb{Z} \text{ et } kg = 0 \text{ équivaut à } k \equiv 0 \mod(n)) \\ &\Leftrightarrow (n \text{ est le plus petit entier naturel non nul tel que } ng = 0)\end{aligned}$$

(dans ce cas, $\langle g \rangle$ est dit cyclique d'ordre n et il est isomorphe à $\mathbb{Z}_n$).

3. Soient n un entier naturel non nul, $d \in \mathbb{N}^*$ un diviseur de n et $q = \dfrac{n}{d}$. Montrer que l'ensemble des éléments de $\mathbb{Z}_n$ d'ordre divisant d est le groupe cyclique :

$$H = \langle \overline{q} \rangle = \left\{\overline{0}, \overline{q}, \cdots, (d-1)\,\overline{q}\right\}$$

engendré par $\overline{q}$, ce groupe étant d'ordre d.

4. Pour $n \geq 1$, on désigne par Γ_n le groupe multiplicatif des racines complexes de l'unité.
   (a) Montrer que pour $n \geq 1$ et $m \geq 1$, on a $\Gamma_n \cap \Gamma_m = \Gamma_{n \wedge m}$.
   (b) Montrer que $(X^n - 1) \wedge (X^m - 1) = X^{n \wedge m} - 1$ dans $\mathbb{C}[X]$. Expliquer pourquoi ce résultat est encore vrai dans $\mathbb{R}[X]$.

– II – Morphismes de groupes, d'anneaux de $\mathbb{Z}_n$ dans $\mathbb{Z}_m$

On s'intéresse dans cette parties aux morphismes de groupes et d'anneaux de $\mathbb{Z}_n$ dans $\mathbb{Z}_m$ pour tout couple (n, m) d'entiers naturels.

Pour tout entier relatif k, on note respectivement $\overline{k}$ la classe de k modulo n et $\widehat{k}$ sa classe modulo m.

On suppose qu'un morphisme d'anneaux commutatifs unitaires $\varphi : \mathbb{A} \to \mathbb{B}$ est tel que $\varphi(1_{\mathbb{A}}) = 1_{\mathbb{B}}$.

On note $\mathrm{Hom}_{gr}(\mathbb{Z}_n, \mathbb{Z}_m)$ [resp. $\mathrm{Hom}_{Ann}(\mathbb{Z}_n, \mathbb{Z}_m)$] l'ensemble des morphismes de groupes [resp. d'anneaux] de $\mathbb{Z}_n$ dans $\mathbb{Z}_m$.

1. Étudier le cas $(n, m) = (0, 0)$.
2. Étudier le cas $n \geq 1$ et $m = 0$.
3. Étudier le cas $n = 0$ et $m \geq 1$.
4. Étudier le cas où $n \geq 1$, $m \geq 1$ sont premiers entre eux.
5. Étudier le cas où $n \geq 1$, $m \geq 1$ sont non premiers entre eux.
6. Montrer que pour tout entier $n \geq 2$, le groupe $(\mathrm{Aut}(\mathbb{Z}_n), \circ)$ des automorphismes du groupe additif $\mathbb{Z}_n$ est isomorphe au groupe $(\mathbb{Z}_n^\times, \cdot)$ des éléments inversibles de $\mathbb{Z}_n$.

– III – Éléments inversibles de $\mathbb{Z}_n$, fonction indicatrice d'Euler

Pour tout entier $n \geq 2$, on note $\mathbb{Z}_n^\times$ le groupe multiplicatif des éléments inversibles de $\mathbb{Z}_n$.

La fonction indicatrice d'Euler est la fonction qui associe à tout entier naturel non nul n, le nombre, noté $\varphi(n)$, d'entiers compris entre 1 et n qui sont premiers avec n (pour $n = 1$, on a $\varphi(1) = 1$).

1. Soit k un entier relatif. Montrer que les propriétés suivantes sont équivalentes :
   (a) $\overline{k}$ est inversible dans $\mathbb{Z}_n$;

(b) k est premier avec n ;

(c) $\overline{k}$ est un générateur de $(\mathbb{Z}_n, +)$.

2. Montrer que, pour tout entier relatif k premier avec n, on a $k^{\varphi(n)} \equiv 1 \ (n)$ (théorème d'Euler).
3. Soit p un entier naturel premier. Montrer que pour tout entier relatif k premier avec n, on a $k^{p-1} \equiv 1 \ (p)$ et pour tout entier relatif k, on a $k^p \equiv k \ (p)$ (petit théorème de Fermat).
4. Montrer que pour $n \geq 3$, $\varphi(n)$ est un entier pair.
5. Calculer le reste dans la division euclidienne de 5^{2008} par 11.
6.

(a) Soient a, b des entiers relatifs et $(n_k)_{1 \leq k \leq r}$ une suite finie d'entiers naturels non nuls. Monter que si $a \equiv b \bmod (n_k)$ pour tout k compris entre 1 et r, alors $a \equiv b \bmod (n_1 \vee \cdots \vee n_r)$.

(b) Montrer que pour tout entier relatif a premier avec 561, on a $a^{560} \equiv 1 \ (561)$, alors que 561 n'est pas premier (on dit que 561 est un nombre de Carmichaël).

7. Montrer qu'il y a équivalence entre :

(a) n est premier ;

(b) $\mathbb{Z}_n$ est un corps ;

(c) $\mathbb{Z}_n$ est un intègre.

8. Montrer qu'un entier p est premier si et seulement si $(p-1)! \equiv -1 \ (p)$ (théorème de Wilson).
9. Montrer qu'un entier p supérieur ou égal à 2 est premier si, et seulement si, $(p-2)!$ est congru à 1 modulo p.
10. Montrer que les entiers n et m sont premiers entre eux si, et seulement si, les anneaux $\mathbb{Z}_{nm}$ et $\mathbb{Z}_n \times \mathbb{Z}_m$ sont isomorphes.
11. Montrer que si $\mathbb{A}, \mathbb{B}$ sont deux anneaux commutatifs unitaires et φ est un isomorphisme d'anneaux de $\mathbb{A}$ sur $\mathbb{B}$, il réalise alors un isomorphisme de groupes de $\mathbb{A}^\times$ (groupe des éléments inversibles de $\mathbb{A}$) sur $\mathbb{B}^\times$.
12. Montrer que si n et m sont deux entiers naturels non nuls premiers entre eux, on a alors $\varphi(nm) = \varphi(n)\varphi(m)$.
13. Montrer que si $n \geq 2$ a pour décomposition en facteurs premiers $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec $2 \leq p_1 < \cdots < p_r$ premiers et les α_i entiers naturels non nuls, on a alors :

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

14. Pour tout entier $n \geq 2$, on note $\mathcal{D}_n$ l'ensemble des diviseurs positifs de n et pour tout $d \in \mathcal{D}_n$, on note :

$$S_d = \left\{ k \in \{1, \cdots, n\} \mid k \wedge n = \frac{n}{d} \right\}$$

Pour $d = n$, S_n est l'ensemble des entiers k compris entre 1 et n premier avec n.

(a) Montrer que les S_d, pour d décrivant $\mathcal{D}_n$, forment une partition de $\{1, \cdots, n\}$ et que pour tout $d \in \mathcal{D}_n$ on a $\operatorname{card}(S_d) = \varphi(d)$.

(b) Montrer que pour tout entier $n \geq 2$, on a :

$$n = \sum_{d \in \mathcal{D}_n} \varphi(d)$$

(formule de Möbius).

15. Soit p un nombre premier.
Pour tout $d \in \mathcal{D}_{p-1}$, on note $\psi(d)$ le nombre d'éléments d'ordre d dans le groupe multiplicatif $\mathbb{Z}_p^\times$.

    (a) Montrer que $\psi(d) = \varphi(d)$ pour tout $d \in \mathcal{D}_{p-1}$.

    (b) Montrer que le groupe $\mathbb{Z}_p^\times$ est cyclique.

16. Soient p un nombre premier impair et α un entier supérieur ou égal à 2. On se propose de montrer que le groupe multiplicatif $\mathbb{Z}_{p^\alpha}^\times$ est cyclique.

    (a) Montrer que pour tout entier k compris entre 1 et $p-1$, $\binom{p}{k}$ est divisible par p.

    (b) Montrer qu'il existe une suite d'entiers naturels non nuls $(\lambda_k)_{k\in\mathbb{N}}$ tous premiers avec p tels que :
    $$\forall k \in \mathbb{N},\ (1+p)^{p^k} = 1 + \lambda_k p^{k+1}$$

    (c) Montrer que la classe résiduelle modulo p^α, $\overline{1+p}$ est d'ordre $p^{\alpha-1}$ dans $\mathbb{Z}_{p^\alpha}^\times$.

    (d) Montrer que si $x = k + p\mathbb{Z}$ un générateur du groupe cyclique $\mathbb{Z}_p^\times$, alors $y = k^{p^{\alpha-1}} + p^\alpha\mathbb{Z}$ est d'ordre $p-1$ dans $\mathbb{Z}_{p^\alpha}^\times$.

    (e) En déduire que $\mathbb{Z}_{p^\alpha}^\times$ est cyclique.

17. Montrer que $\mathbb{Z}_2^\times$ et $\mathbb{Z}_{2^2}^\times$ sont cycliques.

18. On s'intéresse ici au groupe multiplicatif $\mathbb{Z}_{2^\alpha}^\times$ pour $\alpha \geq 3$.

    (a) Montrer qu'il existe une suite $(\lambda_k)_{k\in\mathbb{N}}$ d'entiers impairs tels que :
    $$\forall k \in \mathbb{N},\ 5^{2^k} = 1 + \lambda_k 2^{k+2}$$

    (b) Montrer que la classe résiduelle de 5 modulo 2^α est d'ordre $2^{\alpha-2}$ dans $\mathbb{Z}_{2^\alpha}^\times$.

    (c) On désigne par ψ l'application qui à toute classe résiduelle modulo 2^α, $k + 2^\alpha\mathbb{Z}$, associe la classe résiduelle modulo 4, $k + 4\mathbb{Z}$. Montrer que cette application est bien définie, qu'elle induit un morphisme surjectif de groupes multiplicatifs de $\mathbb{Z}_{2^\alpha}^\times$ sur $\mathbb{Z}_4^\times$ et que son noyau est un groupe cyclique d'ordre $2^{\alpha-2}$.

    (d) Montrer que l'application :
    $$\begin{array}{rccc} \pi : & \mathbb{Z}_{2^\alpha}^\times & \to & \mathbb{Z}_4^\times \times \ker(\psi) \\ & x & \mapsto & (\psi(x), \psi(x)\, x) \end{array}$$
    est un isomorphisme de groupes. En déduire que $\mathbb{Z}_{2^\alpha}^\times$ est isomorphe à $\mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$. Le groupe $\mathbb{Z}_{2^\alpha}^\times$ est-il cyclique ?

– IV – Idéaux de $\mathbb{Z}_n$

1. Soit $\varphi : \mathbb{A} \to \mathbb{B}$ un morphisme d'anneaux commutatifs, unitaires.

    (a) Montrer que pour tout idéal J de $\mathbb{B}$, $\varphi^{-1}(J)$ est un idéal de $\mathbb{A}$.

    (b) On suppose que φ est surjectif. Montrer que pour tout idéal I de $\mathbb{A}$, $\varphi(I)$ est un idéal de $\mathbb{B}$, puis que l'application Φ qui associe à tout idéal J de $\mathbb{B}$ l'idéal $\varphi^{-1}(J)$ de $\mathbb{A}$ réalise une bijection de l'ensemble des idéaux de $\mathbb{B}$ dans l'ensemble des idéaux de $\mathbb{A}$ qui contiennent $\ker(\varphi)$.

2. Soit I un idéal de $\mathbb{A}$. Montrer qu'il y a une bijection entre les idéaux de $\dfrac{\mathbb{A}}{I}$ et les idéaux de $\mathbb{A}$ qui contiennent I.

3.

(a) Soient $\mathbb{A}$ un anneau principal et I est un idéal non trivial de $\mathbb{A}$ (i. e. $I \neq \{0\}$ et $I \neq \mathbb{A}$). Montrer que tous les idéaux de $\dfrac{\mathbb{A}}{I}$ sont principaux. L'anneau $\dfrac{\mathbb{A}}{I}$ est-il principal ?

(b) Montrer que, pour tout entier naturel n, les idéaux de l'anneau $\mathbb{Z}_n$ sont ses sous-groupes additifs.

(c) Déterminer tous les idéaux de $\mathbb{Z}_n$, où $n \geq 2$ est un entier.

4. Quels sont les idéaux premiers de $\mathbb{Z}_n$ pour $n \geq 2$?

2 Solution

– I – Ordre d'un élément dans un groupe

1. On utilise les ensembles quotients.

(a) Pour tout sous-groupe H de G, la relation $\mathcal{R}$ définie sur G par :

$$g_1 \mathcal{R} g_2 \Leftrightarrow \exists h \in H \mid g_2 = g_1 + h \Leftrightarrow -g_1 + g_2 \in H$$

est une relation d'équivalence (attention G n'est pas nécessairement commutatif, donc $g_2 = g_1 + h$ n'équivaut pas à $g_2 - g_1 \in H$).
En effet :

i. Pour tout $g \in G$, on a $-g + g = 0 \in H$, donc $\mathcal{R}_g$ est réflexive.

ii. Si g_1, g_2 dans G sont tels que $-g_1 + g_2 \in H$, on a alors $-(-g_1 + g_2) = -g_2 + g_1 \in H$, ce qui signifie que $g_2 \mathcal{R} g_1$. Cette relation est donc symétrique.

iii. Si g_1, g_2, g_3 dans G sont tels que $-g_1 + g_2 \in H$ et $-g_2 + g_3 \in H$, on a alors :

$$-g_1 + g_3 = (-g_1 + g_2) + (-g_2 + g_3) \in H$$

ce qui signifie que $g_1 \mathcal{R} g_3$. Cette relation est donc transitive.

(b) On note, pour tout $g \in G$:

$$\overline{g} = \{g' \in G \mid g \mathcal{R} g'\} = \{g' \in G \mid -g + g' \in H\} = g + H$$

la classe d'équivalence de g modulo $\mathcal{R}$ et on dit que $\overline{g}$ est la classe à gauche modulo H de g.
L'ensemble de toutes ces classes d'équivalence est noté G/H et on l'appelle l'ensemble des classes à gauche modulo H.
Le cardinal de l'ensemble G/H est noté $[G : H]$ et on l'appelle l'indice de H dans G.

(c) Si H est un sous-groupe de G, alors l'ensemble des classes à gauche modulo H deux à deux distinctes forme une partition de G.
Notons :

$$G/H = \{\overline{g_i} = g_i + H \mid i \in I\}$$

l'ensemble des classes à gauche modulo H deux à deux distinctes.
Pour tout $g \in g$, il existe un unique indice $i \in I$ tel que $\overline{g} = \overline{g_i}$, donc $G = \bigcup_{i \in I} \overline{g_i}$. Dire que g est dans $\overline{g_j} \cap \overline{g_k}$ signifie que g est équivalent à gauche modulo H à g_j et g_k et donc par transitivité g_j et g_k sont équivalents, ce qui revient à dire que $\overline{g_j} = \overline{g_k}$. Les classes à gauche modulo H forment donc bien une partition de G.
On peut aussi tout simplement dire que dès qu'on a une relation d'équivalence, sur G les classes d'équivalence partitionnent G.

(d) Dans le cas où G est fini d'ordre $n \geq 1$, pour tout $g \in G$ on a $\text{card}\,(g+H) = \text{card}\,(H)$ et :

$$\text{card}\,(G) = [G : H]\,\text{card}\,(H)$$

c'est-à-dire que l'ordre de H divise celui de G.
En effet, pour g fixé dans le groupe G, la « translation à gauche » $h \mapsto g+h$ est une bijection de G sur G et sa restriction à H réalise une bijection de H sur $g+H$. Il en résulte que $g+H$ et H ont même cardinal.
L'ensemble des classes à gauche suivant H réalisant une partition de G, ces classes étant en nombre fini de même cardinal égal à celui de H, il en résulte que :

$$\text{card}\,(G) = [G : H]\,\text{card}\,(H)$$

et $\text{card}\,(H)$ divise $\text{card}\,(G)$.

2. On rappelle que les sous-groupes H de $\mathbb{Z}$ sont ses idéaux et qu'ils sont de la forme $n\mathbb{Z}$, l'entier naturel n étant uniquement déterminé : c'est 0 pour $H = \{0\}$ et le plus petit élément de $H \cap \mathbb{N}^*$ pour $H \neq \{0\}$.
Le noyau de φ_g étant un sous-groupe de $\mathbb{Z}$, il existe donc un unique entier $n \geq 0$ tel que $\ker(\varphi_g) = n\mathbb{Z}$, ce qui signifie que :

$$(k \in \mathbb{Z} \text{ et } kg = 0) \Leftrightarrow (\exists j \in \mathbb{Z} \mid k = nj)$$

De plus le morphisme φ_g passe au quotient en un isomorphisme :

$$\begin{array}{rccc} \overline{\varphi_g} : & \mathbb{Z}/\ker(\varphi_g) = \mathbb{Z}/n\mathbb{Z} & \to & \langle g\rangle = \text{Im}\,(\varphi_g) \\ & \overline{k} & \mapsto & kg \end{array}$$

On en déduit les équivalences :

$$\begin{aligned} (\varphi_g \text{ injectif}) &\Leftrightarrow (\ker(\varphi_g) = \{0\}) \Leftrightarrow (n = 0) \\ &\Leftrightarrow (\langle g\rangle \text{ est infini isomorphe à } \mathbb{Z}) \Leftrightarrow (\theta(g) = +\infty) \end{aligned}$$

et :

$$\begin{aligned} (\varphi_g \text{ non injectif}) &\Leftrightarrow (\ker(\varphi_g) \neq \{0\}) \Leftrightarrow (n \in \mathbb{N}^*) \\ &\Leftrightarrow (\langle g\rangle \text{ est fini isomorphe à } \mathbb{Z}/n\mathbb{Z}) \Leftrightarrow (\theta(g) = n) \\ &\Leftrightarrow (\langle g\rangle = \text{Im}\,(\overline{\varphi_g}) = \{rg \mid 0 \leq r \leq n-1\} \text{ est d'ordre } n \in \mathbb{N}^*) \end{aligned}$$

L'équivalence :

$$(\ker(\varphi_g) = n\mathbb{Z} \neq \{0\}) \Leftrightarrow (k \in \mathbb{Z} \text{ et } kg = 0 \text{ équivaut à } k \equiv 0 \mod(n))$$

est une évidence.
L'équivalence :

$$(\ker(\varphi_g) = n\mathbb{Z} \neq \{0\}) \Leftrightarrow (n \text{ est le plus petit entier naturel non nul tel que } ng = 0)$$

se déduit de la structure des sous-groupes de $\mathbb{Z}$.

3. Si $x = \overline{k} \in \mathbb{Z}_n$ est d'ordre δ divisant d, on a alors $d\overline{k} = \overline{dk} = \overline{0}$, donc $n = qd$ divise dk et q divise k, soit $\overline{k} = \overline{jq} = j\overline{q} \in \langle\overline{q}\rangle$.
Réciproquement, si $\overline{k} \in \langle\overline{q}\rangle$, on a alors $\overline{k} = j\overline{q}$ et $d\overline{k} = \overline{djq} = \overline{jn} = \overline{0}$, donc l'ordre de $\overline{k}$ divise d.
Si δ est l'ordre de $\langle\overline{q}\rangle$, on a alors $\delta\overline{q} = \overline{0}$, soit $\delta q = kn = kqd$ et $\delta = kd \geq d$. Mais on a aussi $d\overline{q} = \overline{0}$, donc $\delta = \theta(\overline{q})$ divise d, ce qui entraîne $\delta \leq d$ et $\delta = d$.
En fait, $\langle\overline{q}\rangle$ est l'unique sous-groupe de $\mathbb{Z}_n$ d'ordre d.

4.

(a) Notons $\delta = n \wedge m$ et $H = \Gamma_n \cap \Gamma_m$. Avec $H \subset \Gamma_n$ et $H \subset \Gamma_m$, on déduit que $\text{card}\,(H)$ divise n et m, il divise donc δ. Puis avec $\Gamma_\delta \subset \Gamma_n$ et $\Gamma_\delta \subset \Gamma_m$, on déduit que $\Gamma_\delta \subset H = \Gamma_n \cap \Gamma_m$ et $\delta = \text{card}\,(\Gamma_\delta)$ divise $\text{card}\,(H)$. On a donc $\text{card}\,(H) = \text{card}\,(\Gamma_\delta)$ et $H = \Gamma_\delta$.

(b) Pour tout $r \geq 1$, on a $X^r - 1 = \prod_{\lambda \in \Gamma_r} (X - \lambda)$. Donc $X^n - 1 = \prod_{\lambda \in \Gamma_n} (X - \lambda)$, $X^m - 1 = \prod_{\lambda \in \Gamma_m} (X - \lambda)$ et comme toutes ces racines sont simples :

$$(X^n - 1) \wedge (X^m - 1) = \prod_{\lambda \in \Gamma_n \cap \Gamma_m} (X - \lambda) = \prod_{\lambda \in \Gamma_{n \wedge m}} (X - \lambda) = X^{n \wedge m} - 1$$

Comme le pgcd dans $\mathbb{K}[X]$ se calcule en effectuant des divisions euclidiennes successives et que restes et quotients sont uniquement déterminés, on en déduit que le pgcd de deux polynômes de $\mathbb{R}[X]$ est le même dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

– II – Morphismes de groupes, d'anneaux de $\mathbb{Z}_n$ dans $\mathbb{Z}_m$

1. Pour $n = 0$, l'anneau $\mathbb{Z}_0$ est isomorphe à $\mathbb{Z}$ et il s'agit d'étudier les morphismes de groupes et d'anneaux de $\mathbb{Z}$ dans $\mathbb{Z}$.
Un morphisme d'anneaux $\varphi : \mathbb{Z} \to \mathbb{Z}$ est en particulier un morphisme de groupes, donc on a $\varphi(0) = 0$ et $\varphi(-k) = -\varphi(k)$ pour tout $k \in \mathbb{Z}$.
En notant $a = \varphi(1)$, on vérifie facilement par récurrence que $\varphi(k) = ka$ pour tout entier naturel k et en conséquence $\varphi(k) = ka$ pour tout entier relatif k.
Réciproquement, pour entier relatif a, l'application $\varphi : k \mapsto ka$ est un morphisme de groupes et c'est un morphisme d'anneaux si, et seulement si, $a = \varphi(1) = 1$. Donc :

$$\text{Hom}_{gr}(\mathbb{Z}, \mathbb{Z}) \backsimeq \mathbb{Z} \text{ et } \text{Hom}_{Ann}(\mathbb{Z}, \mathbb{Z}) = \{Id\}$$

2. Soient $n \in \mathbb{N}^*$, $\varphi : \mathbb{Z}_n \to \mathbb{Z}$ un morphisme de groupes et $a = \varphi\left(\overline{1}\right) \in \mathbb{Z}$. De :

$$0 = \varphi\left(\overline{0}\right) = \varphi(\overline{n}) = \varphi\left(n\overline{1}\right) = na$$

on déduit que $a = 0$. On a donc, pour $n \in \mathbb{N}^*$:

$$\text{Hom}_{gr}(\mathbb{Z}_n, \mathbb{Z}) = \{0\} \text{ et } \text{Hom}_{Ann}(\mathbb{Z}, \mathbb{Z}) = \emptyset$$

3. Soient $m \in \mathbb{N}^*$, $\varphi : \mathbb{Z} \to \mathbb{Z}_m$ un morphisme de groupes et $\widehat{a} = \varphi(1) \in \mathbb{Z}_m$ avec $a \in \{0, 1, \cdots, m-1\}$. Pour tout $k \in \mathbb{Z}$, on a :

$$\varphi(k) = k\varphi(1) = k\widehat{a} = \widehat{ka}$$

Réciproquement une telle application est un morphisme de groupes et c'est un morphisme d'anneaux si, et seulement si, $a = 1$, ce qui signifie que φ est la surjection canonique $\pi_m : k \mapsto \widehat{k}$. Donc :

$$\text{Hom}_{gr}(\mathbb{Z}, \mathbb{Z}_m) \backsimeq \mathbb{Z}_m \text{ et } \text{Hom}_{Ann}(\mathbb{Z}, \mathbb{Z}) = \{\pi_m\}$$

4. Soient $n \in \mathbb{N}^*$, $m \in \mathbb{N}^*$, $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$ un morphisme de groupes et $\widehat{a} = \varphi\left(\overline{1}\right) \in \mathbb{Z}_m$ avec $a \in \{1, \cdots, m\}$. De :

$$\widehat{0} = \varphi\left(\overline{0}\right) = \varphi(\overline{n}) = \varphi\left(n\overline{1}\right) = n\widehat{a} = \widehat{na}$$

on déduit que m divise na et comme il est premier avec n, il divise a, ce qui signifie que $a = m$. On a donc, pour $n \in \mathbb{N}^*$ et $m \in \mathbb{N}^*$:

$$\text{Hom}_{gr}(\mathbb{Z}_n, \mathbb{Z}) = \left\{\widehat{0}\right\} \text{ et } \text{Hom}_{Ann}(\mathbb{Z}, \mathbb{Z}) = \emptyset$$

5. On suppose que $\delta = n \wedge m \geq 2$ et on se donne un morphisme de groupes $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$. En notant $\widehat{a} = \varphi\left(\overline{1}\right) \in \mathbb{Z}_m$ avec $a \in \{1, \cdots, m\}$, on a :

$$\widehat{0} = \varphi\left(\overline{0}\right) = \varphi\left(\overline{n}\right) = \varphi\left(n\overline{1}\right) = n\widehat{a}$$

dans $\mathbb{Z}_m$, donc $\theta\left(\widehat{a}\right)$ divise n et comme $\theta\left(\widehat{a}\right)$ divise aussi m (théorème de Lagrange), il divise $\delta = n \wedge m$, donc $\widehat{a}$ est dans le groupe cyclique $H = \left\langle \dfrac{\widehat{m}}{\delta} \right\rangle$ des éléments de $\mathbb{Z}_m$ d'ordre divisant δ.
Réciproquement, pour tout $\widehat{a} \in \left\langle \dfrac{\widehat{m}}{\delta} \right\rangle$, l'application $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$ définie par $\varphi\left(\overline{k}\right) = k\widehat{a}$ est bien définie (si $j \equiv k \bmod (n)$, on a alors $j = k + pn = k + p'\delta$ et $p'\delta\widehat{a} = \widehat{0}$ puisque $\widehat{a}$ est d'ordre divisant δ, donc $k\widehat{a} = j\widehat{a}$) et c'est un morphisme de groupes.
On a donc :

$$\mathrm{Hom}_{gr}\left(\mathbb{Z}_n, \mathbb{Z}_m\right) \backsimeq \mathbb{Z}_\delta = \mathbb{Z}_{n \wedge m}$$

Si φ est un morphisme d'anneaux, on a alors $\widehat{a} = \varphi\left(\overline{1}\right) = \widehat{1}$ qui est d'ordre m divisant $\delta = n \wedge m$, ce qui revient à dire que $\delta = m$ ou encore que m divise n et dans ce cas $\varphi\left(\overline{k}\right) = k\widehat{1} = \widehat{k} = \pi_m\left(k\right)$.
Il y a donc un seul morphisme d'anneaux de $\mathbb{Z}_n$ dans $\mathbb{Z}_m$.
On a donc :

$$\mathrm{Hom}_{Ann}\left(\mathbb{Z}, \mathbb{Z}\right) = \begin{cases} \left\{\overline{k} \mapsto \widehat{k}\right\} \text{ si } m \text{ divise } n \\ \emptyset \text{ si } m \text{ ne divise pas } n \end{cases}$$

6. On vérifie tout d'abord que : pour tout $x \in \mathbb{Z}_n^\times$ l'application $\sigma\left(x\right)$ définie sur $\mathbb{Z}_n$ par :

$$\forall y \in \mathbb{Z}_n,\ \sigma\left(x\right)\left(y\right) = xy$$

est un automorphisme du groupe additif $\mathbb{Z}_n$.
Pour y, z dans $\mathbb{Z}_n$, on a :

$$\sigma\left(x\right)\left(y + z\right) = x\left(y + z\right) = xy + xz = \sigma\left(x\right)\left(y\right) + \sigma\left(x\right)\left(z\right)$$

c'est-à-dire que $\sigma\left(x\right)$ est un morphisme de groupes additifs.
Si $y \in \ker\left(\sigma\left(x\right)\right)$, alors $xy = \overline{0}$ et $y = x^{-1}xy = \overline{0}$, c'est-à-dire que $\sigma\left(x\right)$ est injectif et donc bijectif puisque $\mathbb{Z}_n$ est fini. On a donc bien $\sigma\left(x\right) \in \mathrm{Aut}\left(\mathbb{Z}_n\right)$.
Puis, on vérifie que l'application σ réalise un isomorphisme de $\left(\mathbb{Z}_n^\times, \cdot\right)$ sur $\left(\mathrm{Aut}\left(\mathbb{Z}_n\right), \circ\right)$.
Pour x, x' dans $\mathbb{Z}_n^\times$ et y dans $\mathbb{Z}_n$, on a :

$$\sigma\left(xx'\right)\left(y\right) = \left(xx'\right)y = x\left(x'y\right) = \left(\sigma\left(x\right) \circ \sigma\left(x'\right)\right)\left(y\right)$$

donc $\sigma\left(xx'\right) = \sigma\left(x\right) \circ \sigma\left(x'\right)$ et σ est un morphisme de groupes.
Si $\sigma\left(x\right) = I_d$, on a $\sigma\left(x\right)\left(\overline{1}\right) = \overline{1}$, soit $x = x\overline{1} = \overline{1}$, donc σ est injective.
Si $u \in \mathrm{Aut}\left(\mathbb{Z}_n\right)$ et $\overline{k} = u\left(\overline{1}\right)$, alors pour tout $\overline{p} \in \mathbb{Z}_n$, on a :

$$u\left(\overline{p}\right) = u\left(p\overline{1}\right) = pu\left(\overline{1}\right) = p\overline{k} = \overline{p}\overline{k} = \sigma\left(\overline{k}\right)\overline{p}$$

L'application σ est donc surjective. En définitive σ réalise un isomorphisme de groupes de $\left(\mathbb{Z}_n^\times, \cdot\right)$ sur $\left(\mathrm{Aut}\left(\mathbb{Z}_n\right), \circ\right)$.

– III – Éléments inversibles de $\mathbb{Z}_n$, fonction indicatrice d'Euler

1. C'est une application du théorème de Bézout.
   Dire que $\overline{k}$ est inversible dans $\mathbb{Z}_n$ équivaut à dire qu'il existe $\overline{u}$ dans $\mathbb{Z}_n$ tel que $\overline{k}\overline{u} = \overline{1}$, encore équivalent à dire qu'il existe u, v dans $\mathbb{Z}$ tels que $ku + nv = 1$, ce qui équivaut à dire que k et n sont premiers entre eux (théorème de Bézout).
   En traduisant le fait que $\overline{k}$ est inversible dans $\mathbb{Z}_n$ par l'existence d'un entier relatif u tel que $\overline{k}\overline{u} = u\overline{k} = \overline{1}$, on déduit que cela équivaut à dire que $\overline{1}$ est dans le groupe engendré par $\overline{k}$ et donc que ce groupe (qui est aussi un idéal) est $\mathbb{Z}_n$.
   On en déduit que $\varphi(n)$ est le nombre de générateurs du groupe cyclique $(\mathbb{Z}_n, +)$ (ou de n'importe quel groupe cyclique d'ordre n) ou encore que c'est le nombre d'éléments inversibles de $\mathbb{Z}_n$.
2. Si k est premier avec n, $\overline{k}$ appartient alors à $\mathbb{Z}_n^\times$ qui est un groupe d'ordre $\varphi(n)$ et en conséquence son ordre divise $\varphi(n)$ (théorème de Lagrange), ce qui entraîne $\overline{k}^{\varphi(n)} = \overline{1}$, ou encore $k^{\varphi(n)} \equiv 1\ (n)$.
3. Pour p premier, on a $\varphi(p) = p - 1$ et le théorème d'Euler devient le petit théorème de Fermat.
4. Avec $\overline{(-1)}^2 = \overline{(-1)^2} = \overline{1}$, on déduit que $\overline{(-1)}$ est d'ordre 1 ou 2 dans $\mathbb{Z}_n^\times$. Pour $n \geq 3$, on a $\overline{(-1)} \neq \overline{1}$, donc $\overline{(-1)}$ est d'ordre 2 qui va diviser l'ordre du groupe $\mathbb{Z}_n^\times$, soit $\varphi(n)$.
   On peut aussi montrer ce résultat en écrivant que :
   $$\mathbb{Z}_n^\times = \left\{-\overline{1}, \overline{1}\right\} \cup \left\{\overline{k}, \frac{1}{\overline{k}} \mid \overline{k} \notin \left\{-\overline{1}, \overline{1}\right\}\right\}$$
   Pour $n = 2$, on a $\mathbb{Z}_2 = \left\{\overline{0}, \overline{1}\right\}$ et $\mathbb{Z}_2^\times = \left\{\overline{1}\right\}$.
5. Le principe de cet exercice est le suivant.
   On cherche le reste dans la division euclidienne de a^b $(= 5^{2008})$ par p $(= 11)$, où $p \geq 3$ est premier.
   On effectue la division euclidienne de b par $p-1$, soit $b = q(p-1) + r$ avec $0 \leq r \leq p-2$ et on a $a^b = (a^{p-1})^q a^r$ avec $a^{p-1} \equiv 1\ (p)$ si p ne divise pas a, ce qui donne $a^b \equiv a^r\ (p)$ (on a diminué b). Ensuite $a \equiv s\ (p)$ avec $1 \leq s \leq p-1$ (on a diminué a) et $a^b \equiv s^r\ (p)$. On se débrouille pour construire un exercice où s^r est facile à calculer.
   Comme 11 est premier le théorème de Fermat nous dit que 5^{10} est congru à 1 modulo 11. On effectue alors la division euclidienne de 2008 par 10, soit $2008 = 200 \times 10 + 8$ et on déduit que 5^{2008} est congru à 5^8 modulo 11. Enfin avec $5^2 \equiv 3$, $5^4 \equiv 9 \equiv -2$, $5^8 \equiv 4$ modulo 11, on déduit que $5^{2008} \equiv 4$ modulo 11, ce qui signifie que 4 est le reste dans la division euclidienne de 5^{2008} par 11.
6. (a) Si $a \equiv b \bmod (n_k)$ pour tout k compris entre 1 et r, $b - a$ est un multiple commun aux n_k et en conséquence $n_1 \vee \cdots \vee n_r$ divise $b - a$, ce qui signifie que $a \equiv b \bmod (n_1 \vee \cdots \vee n_r)$.
   Dans le cas où les n_k sont deux à deux premiers entre eux, on a $n_1 \vee \cdots \vee n_r = \prod_{k=1}^{r} n_k$ et $a \equiv b \bmod \left(\prod_{k=1}^{r} n_k\right)$.

   (b) On a la décomposition en facteurs premiers $561 = 3 \cdot 11 \cdot 17 = \prod_{k=1}^{3} p_k$. Si a est premier avec 561, il est alors premier avec chaque p_k et le théorème de Fermat nous dit que $a^{p_k - 1} \equiv 1 \bmod (p_k)$ et en remarquant que 560 est divisible par chaque $p_k - 1$ ($560 = 2 \cdot 280 = 10 \cdot 56 = 16 \cdot 35$), on en déduit que $a^{560} \equiv 1 \bmod (p_k)$ pour $k = 1, 2, 3$ et la question précédente nous dit que $a^{560} \equiv 1\ (561)$.

7. Dans le cas où n est premier tous les éléments de $\mathbb{Z}_n \setminus \left\{\overline{0}\right\}$ sont inversibles et en conséquence $\mathbb{Z}_n$ est un corps, c'est donc un anneau intègre.
Supposons $\mathbb{Z}_n$ intègre et soit d un diviseur de n différent de n dans $\mathbb{N}$. Il existe donc un entier q compris entre 2 et n tel que $n = qd$ et dans $\mathbb{Z}_n$ on a $\overline{q}\overline{d} = \overline{0}$ avec $\overline{d} \neq \overline{0}$, ce qui impose $\overline{q} = \overline{0}$, donc $q = n$ et $d = 1$. L'entier n est donc premier.
De manière plus générale, si $\mathbb{A}$ est un anneau principal et $p \in \mathbb{A}$, on a alors :

$$(p \text{ premier}) \Leftrightarrow ((p) \text{ premier}) \Leftrightarrow \left(\frac{\mathbb{A}}{I} \text{ est intègre}\right)$$
$$\Leftrightarrow \left(\frac{\mathbb{A}}{I} \text{ est un corps}\right) \Leftrightarrow ((p) \text{ maximal}) \Leftrightarrow (p \text{ irréductible})$$

L'implication ($\mathbb{Z}_n$ est intègre) $\Rightarrow$ ($\mathbb{Z}_n$ est un corps) est aussi conséquence du fait que tout anneau unitaire fini et intègre est un corps (théorème de Wedderburn). Si $\mathbb{A}$ est un anneau fini intègre, alors pour tout $a \in \mathbb{A} \setminus \{0\}$ l'application $x \mapsto ax$ est injective de $\mathbb{A}$ dans $\mathbb{A}$, donc bijective, ce qui entraîne l'existence de $a' \in \mathbb{A}$ tel que $aa' = 1$.

8. Si p est premier, alors $\mathbb{Z}_p$ est un corps commutatif à p éléments et tout élément $\overline{k}$ du groupe $\mathbb{Z}_p^\times$ est racine du polynôme $X^{p-1} - \overline{1}$, on a donc $X^{p-1} - \overline{1} = \prod_{k=1}^{p-1}\left(X - \overline{k}\right)$ dans $\mathbb{Z}_p[X]$ et en évaluant ce polynôme en $\overline{0}$, il vient $-\overline{1} = \prod_{k=1}^{p-1}\left(-\overline{k}\right) = (-1)^{p-1}\,\overline{(p-1)!}$. Pour $p = 2$, on a $-\overline{1} = \overline{1}$ et pour p premier impair, on a $-\overline{1} = \overline{(p-1)!}$ dans $\mathbb{Z}_p$.
Réciproquement si $p \geq 2$ est tel que $\overline{(p-1)!} = -\overline{1}$ dans $\mathbb{Z}_p$, alors tout diviseur d de p compris entre 1 et $p-1$ divisant $(p-1)! = -1 + kp$ va diviser -1, ce qui donne $d = 1$ et l'entier p est premier.

9. Pour $p \geq 2$, on a $(p-1)! = (p-1)\,(p-2)! \equiv -\,(p-2)!$ modulo p, avec la convention $0! = 1$. Le résultat se déduit alors du théorème de Wilson.

10. Pour tout entier relatif k, on note $\overline{k}$ sa classe modulo nm, $\dot{k}$ sa classe modulo n et $\ddot{k}$ sa classe modulo m.
Le produit cartésien $\mathbb{Z}_n \times \mathbb{Z}_m$ est naturellement muni d'une structure d'anneau commutatif unitaire avec les lois $+$ et $\cdot$ définies par :

$$\begin{cases} \left(\dot{j}, \ddot{k}\right) + \left(\dot{j'}, \ddot{k'}\right) = \left(\dot{j + j'}, \ddot{k + k'}\right) \\ \left(\dot{j}, \ddot{k}\right) \cdot \left(\dot{j'}, \ddot{k'}\right) = \left(\dot{j \cdot j'}, \ddot{k \cdot k'}\right) \end{cases}$$

Supposons n et m premiers entre eux. L'application $f : k \mapsto \left(\dot{k}, \ddot{k}\right)$ est un morphisme d'anneaux de $\mathbb{Z}$ dans $\mathbb{Z}_n \times \mathbb{Z}_m$ et son noyau est formé des entiers divisibles par n et m donc par nm puisque ces entiers sont premiers entre eux, il se factorise donc en un morphisme injectif d'anneaux de $\mathbb{Z}_{nm}$ dans $\mathbb{Z}_n \times \mathbb{Z}_m$ par $\overline{f} : \overline{k} \mapsto \left(\dot{k}, \ddot{k}\right)$. Ces deux anneaux ayant même cardinal, l'application $\overline{f}$ réalise en fait un isomorphisme d'anneaux de $\mathbb{Z}_{nm}$ dans $\mathbb{Z}_n \times \mathbb{Z}_m$.
Si n et m ne sont pas premiers entre eux les groupes additifs $\mathbb{Z}_{nm}$ et $\mathbb{Z}_n \times \mathbb{Z}_m$ ne peuvent être isomorphes puisque $\overline{1}$ est d'ordre nm dans $\mathbb{Z}_{nm}$ et tous les éléments de $\mathbb{Z}_n \times \mathbb{Z}_m$ ont un ordre qui divise le ppcm de n et m qui est strictement inférieur à nm.

11. On a $\varphi(1_\mathbb{A}) = 1_\mathbb{B}$ et pour $a \in \mathbb{A}^\times$, de $1_\mathbb{B} = \varphi(1_\mathbb{A}) = \varphi(aa^{-1}) = \varphi(a)\,\varphi(a^{-1})$, on déduit que $\varphi(a) \in \mathbb{B}^\times$. Donc φ est un morphisme de groupes de $\mathbb{A}^\times$ dans $\mathbb{B}^\times$. Comme φ est injectif, il en est de même de sa restriction à $\mathbb{A}^\times$. Pour tout $b = \varphi(a) \in \mathbb{B}^\times$, il existe $c = \varphi(a') \in \mathbb{B}^\times$ tel que $1_\mathbb{B} = bc = \varphi(aa') = \varphi(1_\mathbb{A})$, donc $aa' = 1_\mathbb{A}$ et $a \in \mathbb{A}^\times$. La restriction de φ à $\mathbb{A}^\times$ est donc surjective sur $\mathbb{B}^\times$ et elle réalise un isomorphisme de $\mathbb{A}^\times$ sur $\mathbb{B}^\times$.

12. La restriction de l'isomorphisme $\overline{f}$ à $\mathbb{Z}_{nm}^{\times}$ réalise un isomorphisme de groupes multiplicatifs de $\mathbb{Z}_{nm}^{\times}$ sur $\mathbb{Z}_n^{\times} \times \mathbb{Z}_m^{\times}$, ce qui entraîne :

$$\varphi(nm) = \operatorname{card}\left(\mathbb{Z}_{nm}^{\times}\right) = \operatorname{card}\left(\mathbb{Z}_n^{\times}\right) \operatorname{card}\left(\mathbb{Z}_m^{\times}\right) = \varphi(n)\,\varphi(m)$$

13. Si p est premier, alors un entier k compris entre 1 et p^{α} n'est pas premier avec p^{α} si et seulement si il est divisible par p, ce qui équivaut à $k = mp$ avec $1 \leq m \leq p^{\alpha-1}$, il y a donc $p^{\alpha-1}$ possibilités. On en déduit alors que :

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = (p-1)\,p^{\alpha-1}$$

En utilisant les résultats précédents, on a :

$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{r} \varphi(p^{\alpha_i}) = \prod_{i=1}^{r} (p_i - 1)\,p_i^{\alpha_i - 1} = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

14.

(a) Il est clair que $S_d \cap S_{d'} = \emptyset$ pour $d \neq d'$ dans $\mathcal{D}_n$. Si k est un entier compris entre 1 et n, en notant δ le pgcd de k et n, $k = \delta k'$ et $n = \delta d$ avec k' et d premiers entre eux, on a $k \wedge n = \delta = \dfrac{n}{d}$ et $k \in S_d$ avec $d \in \mathcal{D}_n$. On a donc la partition :

$$\{1, \cdots, n\} = \bigcup_{d \in \mathcal{D}_n} S_d$$

(b) Un entier k compris entre 1 et n est dans S_d si et seulement si il s'écrit $k = \dfrac{n}{d}k'$ avec k' compris entre 1 et d premier avec d. On a donc :

$$\operatorname{card}(S_d) = \operatorname{card}\{k' \in \{1, \cdots, d\} \mid k' \wedge d = 1\} = \varphi(d)$$

(c) Des deux questions précédentes, on déduit que $n = \sum_{d \in \mathcal{D}_n} \varphi(d)$.

15.

(a) Dire que $\psi(d) > 0$ équivaut à dire qu'il existe dans $\mathbb{Z}_p^{\times}$ au moins un élément x d'ordre d et le groupe $G = \left\{\overline{1}, x, \cdots, x^{d-1}\right\}$ est alors formé de d solutions distinctes de l'équation $X^d - \overline{1} = \overline{0}$, or cette équation a au plus d solutions dans le corps commutatif $\mathbb{Z}_p$, donc G est exactement l'ensemble de toutes les solutions de cette équation. Les éléments d'ordre d dans $\mathbb{Z}_p^{\times}$ sont donc les générateurs du groupe cyclique G et il y a $\varphi(d)$ tels générateurs, donc $\psi(d) = \varphi(d)$ si $\psi(d) > 0$.
Comme tout élément de $\mathbb{Z}_p^{\times}$ a un ordre qui divise $p-1$, on a $p - 1 = \sum_{d \in \mathcal{D}_{p-1}} \psi(d)$ et avec la formule de Möbius, on en déduit que :

$$\sum_{d \in \mathcal{D}_{p-1}} \psi(d) = \sum_{d \in \mathcal{D}_{p-1}} \varphi(d)$$

avec $\psi(d) = 0$ ou $\psi(d) = \varphi(d)$, ce qui entraîne que $\psi(d) = \varphi(d)$ pour tout $d \in \mathcal{D}_{p-1}$.

(b) On a $\psi(p-1) = \varphi(p-1) > 0$, ce qui signifie qu'il existe dans $\mathbb{Z}_p^{\times}$ des éléments d'ordre $p-1$ et ce groupe est cyclique d'ordre $p-1$.
Ce résultat est un cas particulier du suivant : tout sous-groupe fini du groupe multiplicatif $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ d'un corps commutatif $\mathbb{K}$ est cyclique.

16.

(a) En effet, pour k compris entre 1 et $p-1$, p divise $k!\,(p-k)!\binom{p}{k} = p!$ et tout entier j compris entre 1 et $p-1$ est premier avec p, donc p divise $\binom{p}{k}$ (théorème de Gauss).

(b) On procède par récurrence sur $k \geq 0$. Pour $k=0$, on prend $\lambda_0 = 1$. Pour $k=1$, on a :

$$(1+p)^p = 1 + p^2 + \sum_{k=2}^{p} \binom{p}{k} p^k$$

avec $\binom{p}{k}p^k$ divisible par p^3 pour k compris entre 2 et p si $p \geq 3$, ce qui donne :

$$(1+p)^p = 1 + p^2 + \nu p^3 = 1 + \lambda_1 p^2$$

avec $\lambda_1 = 1 + \nu p$ premier avec p. En supposant le résultat acquis pour $k \geq 1$, on a :

$$(1+p)^{p^{k+1}} = \left(1 + \lambda_k p^{k+1}\right)^p = 1 + \lambda_k p^{k+2} + \sum_{j=2}^{p} \binom{p}{j} \lambda_k^j p^{j(k+1)}$$

avec $\binom{p}{j}\lambda_k^j p^{j(k+1)}$ divisible par p^{k+3}, pour j compris entre 2 et p, ce qui donne :

$$(1+p)^{p^{k+1}} = 1 + p^{k+2}\left(\lambda_k + \nu p\right) = 1 + \lambda_{k+1} p^{k+2}$$

avec $\lambda_{k+1} = \lambda_k + \nu p$ premier avec p si λ_k est premier avec p.

(c) $1+p$ étant premier avec p^α, on a bien $\overline{1+p} \in \mathbb{Z}_{p^\alpha}^\times$ et avec :

$$\begin{cases} (1+p)^{p^{\alpha-1}} = 1 + \lambda_{\alpha-1} p^\alpha \equiv 1 \pmod{p^\alpha} \\ (1+p)^{p^{\alpha-2}} = 1 + \lambda_{\alpha-2} p^{\alpha-1} \neq 1 \pmod{p^\alpha} \end{cases}$$

($\lambda_{\alpha-2}$ est premier avec p, donc $\lambda_{\alpha-2}p^{\alpha-1}$ ne peut être divisible par p^α) on déduit que $\overline{1+p}$ est d'ordre $p^{\alpha-1}$ dans $\mathbb{Z}_{p^\alpha}^\times$.

(d) Si $x = k + p\mathbb{Z}$ un générateur du groupe cyclique $\mathbb{Z}_p^\times$, $y = k^{p^{\alpha-1}} + p^\alpha\mathbb{Z}$ est alors d'ordre $p-1$ dans $\mathbb{Z}_{p^\alpha}^\times$.
La classe modulo p, $x = k + p\mathbb{Z}$ est d'ordre $p-1$ dans $\mathbb{Z}_p^\times$ et du fait que $p^{\alpha-1} - 1$ est divisible par $p-1$ pour $\alpha \geq 2$, on déduit que $k^{p^{\alpha-1}-1} \equiv 1 \pmod{p}$ et $k^{p^{\alpha-1}} \equiv k \pmod{p}$, ce qui entraîne que la classe modulo p de $j = k^{p^{\alpha-1}}$ est d'ordre $p-1$ dans $\mathbb{Z}_p^\times$. D'autre part avec :

$$j^{p-1} = k^{(p-1)p^{\alpha-1}} = k^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$$

on déduit que $y = j + p^\alpha\mathbb{Z} = k^{p^{\alpha-1}} + p^\alpha\mathbb{Z}$ est d'ordre $p-1$ dans $\mathbb{Z}_{p^\alpha}^\times$ (si $j^r \equiv 1 \pmod{p^\alpha}$ avec $r \geq 1$, alors p^α et donc p divise $j^r - 1$ ce qui entraîne $j^r \equiv 1 \pmod{p}$ et r est multiple de $p-1$).

(e) Dans $\mathbb{Z}_{p^\alpha}^\times$ on a $x = \overline{1+p}$ d'ordre $p^{\alpha-1}$ et un élément y d'ordre $p-1$ avec $p-1$ et $p^{\alpha-1}$ premiers entre eux, il en résulte que $z = xy$ est d'ordre $\text{ppcm}\,(p-1, p^{\alpha-1}) = (p-1)\,p^{\alpha-1} = \varphi(p^\alpha)$ dans $\mathbb{Z}_{p^\alpha}^\times$. En conséquence $\mathbb{Z}_{p^\alpha}^*$ est cyclique d'ordre $\varphi(p^\alpha)$.

17. On a $\mathbb{Z}_2^\times = \left\{\overline{1}\right\}$ et $\mathbb{Z}_4^\times = \left\{\overline{1}, \overline{-1}\right\} \backsimeq \mathbb{Z}_2$.

18.

(a) On procède par récurrence sur $k \geq 0$. Pour $k = 0$, on a $5 = 1 + 2^2$ et $\lambda_0 = 1$. Pour $k = 1$, on a $5^2 = 1 + 3 * 2^3$ et $\lambda_1 = 3$. En supposant le résultat acquis pour $k \geq 1$, on a :

$$5^{2^{k+1}} = \left(1 + \lambda_k 2^{k+2}\right)^2 = 1 + \lambda_{k+1} 2^{k+3}$$

avec $\lambda_{k+1} = \lambda_k + \lambda_k^2 2^{k+1} = \lambda_k \left(1 + \lambda_k 2^{k+1}\right)$ impair si λ_k l'est.

(b) On a $5^{2^{\alpha-2}} = 1 + \lambda_{\alpha-2} 2^\alpha \equiv 1 \pmod{2^\alpha}$ et $5^{2^{\alpha-3}} = 1 + \lambda_{\alpha-3} 2^{\alpha-1} \neq 1 \pmod{2^\alpha}$ du fait que $\lambda_{\alpha-3} \equiv 1 \pmod 2$. On a donc $5 + 2^\alpha\mathbb{Z}$ d'ordre $2^{\alpha-2}$ dans $\mathbb{Z}_{2^\alpha}^\times$ et $H = \langle 5 + 2^\alpha\mathbb{Z} \rangle$ est un sous-groupe cyclique d'ordre $2^{\alpha-2}$ de $\mathbb{Z}_{2^\alpha}^\times$, il est donc isomorphe à $\mathbb{Z}_{2^{\alpha-2}}$.

(c) Si $k \equiv k' \pmod{2^\alpha}$ alors 2^α divise $k - k'$ et $k \equiv k' \pmod 4$ ($\alpha \geq 2$), donc l'application ψ est bien définie. Dire que $k + 2^\alpha\mathbb{Z}$ est inversible dans $\mathbb{Z}_{2^\alpha}$ équivaut à dire que k est premier avec 2^α et donc avec 4, c'est-à-dire que ψ envoie $\mathbb{Z}_{2^\alpha}^*$ dans $\mathbb{Z}_4^*$. Il est facile de vérifier que ψ est un morphisme de groupes multiplicatifs. Si $x = k + 4\mathbb{Z}$ est inversible dans $\mathbb{Z}_4$ alors $k \equiv 1 \pmod 4$ ou $k \equiv -1 \pmod 4$ et $x = \psi(y)$ avec $y = 1 + 2^\alpha\mathbb{Z}$ ou $y = -1 + 2^\alpha\mathbb{Z}$ dans $\mathbb{Z}_{2^\alpha}^\times$, c'est-à-dire que ψ est surjective. Par passage au quotient ψ induit alors un isomorphisme de $\dfrac{\mathbb{Z}_{2^\alpha}^\times}{\ker(\psi)}$ sur $\mathbb{Z}_4^\times$, il en résulte que :

$$\operatorname{card}\left(\mathbb{Z}_{2^\alpha}^\times\right) = \operatorname{card}(\ker(\psi)) \operatorname{card}\left(\mathbb{Z}_4^\times\right) = 2 \operatorname{card}(\ker(\psi))$$

et $\operatorname{card}(\ker(\psi)) = 2^{\alpha-2}$. Avec $5 + 2^\alpha\mathbb{Z}$ d'ordre $2^{\alpha-2}$ dans $\ker(\psi)$ ($5 \equiv 1 \pmod 4$) on déduit que $\ker(\psi)$ est cyclique d'ordre $2^{\alpha-2}$ engendré par $5 + 2^\alpha\mathbb{Z}$.

(d) Pour $x \in \mathbb{Z}_{2^\alpha}^\times$, on a $\psi(x) \in \mathbb{Z}_4^* = \left\{\overline{1}, \overline{-1}\right\}$. Si $\psi(x) = \overline{1}$, alors $\psi(x)\, x = x \in \ker(\psi)$ et si $\psi(x) = \overline{-1}$, alors $\psi(x)\, x = -x$ et $\psi(\psi(x)\, x) = -\psi(x) = \overline{1}$ et $\psi(x)\, x \in \ker(\psi)$. Du fait que ψ est un morphisme de groupes multiplicatifs, on déduit qu'il en est de même de π.
Si $x \in \ker(\pi)$, alors $\psi(x) = \overline{1}$ et $\psi(x)\, x = \overline{1}$, donc $x = \overline{1}$ et π est injectif. Ces deux groupes ayant même cardinal, on déduit que π est un isomorphisme. En résumé $\mathbb{Z}_{2^\alpha}^\times$ est isomorphe à $\mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$ pour $\alpha \geq 3$ et $\mathbb{Z}_{2^\alpha}^\times$ n'est pas cyclique puisqu'il n'y a pas d'élément d'ordre $2^{\alpha-1}$ dans $\mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$.

– IV – Idéaux de $\mathbb{Z}_n = \dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

1.

(a) Soient J un idéal de $\mathbb{B}$ et :

$$I = \varphi^{-1}(J) = \{a \in \mathbb{A} \mid \varphi(a) \in J\}$$

Comme $\varphi(0_\mathbb{A}) = 0_\mathbb{B} \in J$, on a $0_\mathbb{A} \in I$.
Pour a, b dans I, on a $\varphi(a) \in J$ et $\varphi(b) \in J$, donc $\varphi(a - b) = \varphi(a) - \varphi(b) \in J$ et $a - b \in I$.
Pour $a \in I$ et $b \in \mathbb{A}$, on a $\varphi(a) \in J$, donc $\varphi(ab) = \varphi(a)\varphi(b) \in J$ et $ab \in I$.
En définitive, I est un idéal de $\mathbb{A}$.
En particulier, $\ker(\varphi) = \varphi^{-1}(\{0\})$ est un idéal de $\mathbb{A}$.

(b) Si φ n'est pas surjectif, $\varphi(I)$ n'est pas nécessairement un idéal de $\mathbb{B}$. Par exemple si φ est l'injection canonique de $\mathbb{Z}$ dans $\mathbb{R}$, $\varphi(\mathbb{Z}) = \mathbb{Z}$ n'est pas un idéal de $\mathbb{R}$ ($\frac{1}{2} \cdot 1 \notin \mathbb{Z}$).
Soient I un idéal de $\mathbb{A}$ et :

$$J = \varphi(I) = \{\varphi(a) \mid a \in I\}$$

On a $0_\mathbb{B} = \varphi(0_\mathbb{A}) \in J$ et pour $\varphi(a), \varphi(b)$ dans J, on a $a - b \in I$, donc $\varphi(a) - \varphi(b) = \varphi(a - b) \in J$. Pour $\varphi(a) \in J$ et $c \in \mathbb{B}$, dans le cas où φ est surjective, il existe $b \in \mathbb{A}$ tel que $c = \varphi(b)$ et $\varphi(a) \cdot c = \varphi(a)\varphi(b) = \varphi(ab) \in J(I)$.

En définitive, J est un idéal de $\mathbb{B}$.
Pour tout idéal J de $\mathbb{B}$ et tout $a \in \ker(\varphi)$, on a $\varphi(a) = 0_{\mathbb{B}} \in J$, soit $a \in \varphi^{-1}(J)$, donc $\varphi^{-1}(J)$ est un idéal de $\mathbb{A}$ qui contient $\ker(\varphi)$.
Comme φ est surjective, on a $\varphi(\varphi^{-1}(Y)) = Y$ pour toute partie Y de $\mathbb{B}$ (on a toujours $\varphi(\varphi^{-1}(Y)) \subset Y$ et pour tout $b \in Y$, il existe $a \in \mathbb{A}$ tel que $b = \varphi(a)$ par surjectivité de φ, donc $a \in \varphi^{-1}(Y)$ et $b \in \varphi(\varphi^{-1}(Y))$, ce qui nous donne l'égalité $\varphi(\varphi^{-1}(Y)) = Y$), donc l'application Φ est injective.
Si I est un idéal de $\mathbb{A}$ qui contient $\ker(\varphi)$, l'ensemble $J = \varphi(I)$ est un idéal de $\mathbb{B}$ puisque φ est surjective et $\Phi(J) = \varphi^{-1}(\varphi(I)) = I$ (il est clair que $I \subset \varphi^{-1}(\varphi(I))$ et pour $a \in \varphi^{-1}(\varphi(I))$, on a $\varphi(a) \in \varphi(I)$, soit $\varphi(a) = \varphi(b)$ avec $b \in I$, donc $a - b \in \ker(\varphi) \subset I$ et $a \in I$). L'application Φ est donc surjective.

2. Résulte du fait que π_I est un morphisme d'anneaux surjectif de $\mathbb{A}$ sur $\dfrac{\mathbb{A}}{I}$ de noyau $\ker(\pi_I) = I$.

3.

   (a) Pour $I = \{0\}$, $\dfrac{\mathbb{A}}{I} \backsimeq \mathbb{A}$ est principal et pour $I = \mathbb{A}$, $\dfrac{\mathbb{A}}{I} = \left\{\overline{0}\right\}$.
   Soit $I = (a)$ un idéal de l'anneau principal $\mathbb{A}$ avec $a \neq 0$ et a non inversible. Si J est un idéal de $\dfrac{\mathbb{A}}{I}$, en désignant par π_I la surjection canonique de $\mathbb{A}$ sur $\dfrac{\mathbb{A}}{I}$, $\pi_I^{-1}(J)$ est un idéal de $\mathbb{A}$ qui contient I, donc $\pi_I^{-1}(J) = (b) \supset (a)$ et b divise a. De plus, comme π_I est surjectif, on a $J = \pi_I\left(\pi_I^{-1}(J)\right) = \pi_I(b\mathbb{A}) = \left(\overline{b}\right)$.
   Tous les idéaux de $\dfrac{\mathbb{A}}{I} = \dfrac{\mathbb{A}}{(a)}$ sont donc principaux de la forme $\left(\overline{b}\right)$ où $b \in \mathbb{A}$ est un diviseur de a.
   L'anneau $\dfrac{\mathbb{A}}{I}$ est donc principal si, et seulement si, il est intègre, ce qui revient à dire que l'idéal $I = (a)$ est premier, ce qui revient à dire que a est premier.

   (b) Si I est un idéal de $\mathbb{Z}_n$, c'est en particulier un sous-groupe additif.
   Réciproquement si I est un sous-groupe additif de $\mathbb{Z}_n$, pour $\left(\overline{a}, \overline{b}\right) \in I \times \mathbb{Z}_n$, on a :

$$\overline{a} \cdot \overline{b} = \pm\overline{|b|\, a} = \pm\, |b|\, \overline{a} = \pm\left(\overline{a} + \cdots + \overline{a}\right) \in I$$

   et I est un idéal de $\mathbb{Z}_n$.

   (c) Pour $n \geq 2$, ce qui précède nous dit que les idéaux de $\mathbb{Z}_n$ sont les $(\overline{q})$ où $q \in \{1, \cdots, n\}$ est un diviseur de n.

4. Dans $\mathbb{Z}$ qui est principal, on a les équivalences :
   $((p) \text{ maximal}) \Leftrightarrow ((p) \text{ premier}) \Leftrightarrow (p \text{ premier})$.
   Pour $n \geq 2$, dans $\mathbb{Z}_n$ qui est fini, il y a équivalence entre idéal premier et maximal.
   Pour $n \geq 2$, on a vu que les idéaux de $\mathbb{Z}_n$ sont de la forme $I = (\overline{q})$ où $q = 0$ ou $q \neq 0$ est un diviseur de n.
   Pour n premier, $\mathbb{Z}_n$ est un corps et ses seuls idéaux sont $\mathbb{Z}_n$ et $\left\{\overline{0}\right\}$, seul $\left\{\overline{0}\right\}$ est maximal.
   Pour $n \geq 2$ non premier, on a deux possibilités, soit $I = (\overline{p})$ où $2 \leq p \leq n-1$ est un diviseur premier de n et dans ce cas I est maximal (on a $I \neq \mathbb{Z}_n$ puisque $\overline{p}$ qui divise $\overline{0}$ n'est pas inversible et si $(\overline{p}) \subset J = (\overline{q})$ avec q qui divise n, on a alors $\overline{p} = \overline{aq}$, soit $p = aq + kn = aq + kjq$ et q divise p, donc $q = 1$ ou $q = p$, soit $J = \mathbb{Z}_n$ ou $J = I$), soit $I = (\overline{q})$ où q est un diviseur non premier de n et I n'est pas maximal (pour $q = 1$, on a $I = \mathbb{Z}_n$ et pour $q \geq 2$, on a $q = ab$ avec $2 \leq a, b \leq q-1$ et $I = \left(\overline{ab}\right) \subsetneqq (\overline{a}) \subsetneqq \mathbb{Z}_n$).
   En définitive, les idéaux maximaux de $\mathbb{Z}_n$ sont les $(\overline{q})$ où q est un diviseur premier de n.