Agrégation Externe

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

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

– 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
– 121 : Nombres premiers. Applications.
– 126 : Exemples d'équations diophantiennes.

On pourra consulter les ouvrages suivants.

– P. Boyer, J. J. Risler : *Algèbre pour la licence 3. Groupes, anneaux, corps.* Dunod (2006).
– F. Combes — *Algèbre et géométrie.* Bréal (2003).
– M. Demazure. *Cours d'algèbre.* Cassini. (1997).
– 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).
– H. Gianella, F. Krust, F. Taieb, N. Tosel : *Problèmes choisis de mathématiques supérieures.* Springer (2001).
– 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).
– G. Rauch. *Les groupes finis et leurs représentations.* Ellipses (2000).

Pour tout entier naturel $n \geq 0$, on note $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes résiduelles modulo n et, pour $n \neq 1$, $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{\overline{0}\}$.

Pour $n = 0$, l'anneau $\mathbb{Z}_0$ est isomorphe à $\mathbb{Z}$ et pour $n = 1$, le groupe $\mathbb{Z}_1$ est réduit à $\{\overline{0}\}$.

Pour ce qui suit, on suppose que $n \geq 2$ et on note $\mathbb{Z}_n^\times$ le groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}_n$.

Si k est un entier relatif, on note $\overline{k} = k + n\mathbb{Z}$ la classe de k dans $\mathbb{Z}_n$ et en utilisant le théorème de division euclidienne, on vérifie que :

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\} = \{\overline{1}, \cdots, \overline{n}\}$$

est d'ordre 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.

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

Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}_n$.

– I – Généralités sur $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$

1. Montrer qu'il existe une unique structure d'anneau commutatif unitaire sur $\mathbb{Z}_n$ telle que la surjection canonique π_n soit un morphisme d'anneaux.
   Plus généralement, pour tout idéal I d'un anneau commutatif unitaire $\mathbb{A}$, Il existe une unique structure d'anneau commutatif unitaire sur $\dfrac{\mathbb{A}}{I}$ telle que la surjection canonique $\pi_I : a \in \mathbb{A} \to \overline{a} = a + I \in \dfrac{\mathbb{A}}{I}$ soit un morphisme d'anneaux.
2. Montrer qu'un élément de $\mathbb{Z}_n \setminus \{\overline{0}\}$ est soit inversible, soit un diviseur de $\overline{0}$.
3. Quels sont les éléments nilpotents de l'anneau $\mathbb{Z}_n$?
4. Montrer que tous les sous-groupes de $\mathbb{Z}_n$ sont cycliques et que pour tout diviseur d de n, il existe un unique sous-groupe de $\mathbb{Z}_n$ d'ordre d.
5. Montrer que les idéaux de l'anneau $\mathbb{Z}_n$ sont ses sous-groupes additifs.
6. Déterminer tous les idéaux de $\mathbb{Z}_n$.
7. Quels sont les idéaux premiers, maximaux de $\mathbb{Z}_n = \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ pour $n \geq 2$?

– II – Morphismes de groupes, d'anneaux de $\mathbb{Z}_n$ dans $\mathbb{Z}_m$. Le groupe $\mathrm{Aut}(\mathbb{Z}_n)$

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

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 $\mathbb{Z}_m$.

Pour tout entier $n \geq 2$, on note $\mathrm{Aut}(\mathbb{Z}_n)$ le groupe des automorphismes du groupe additif $\mathbb{Z}_n$.

1. Montrer que pour $n = m = 0$, on a :

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

2. Montrer que pour tout $n \in \mathbb{N}^*$, on a :

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

3. Montrer que pour tout $m \in \mathbb{N}^*$, on a :

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

4. Montrer que pour n, m premiers entre eux dans $\mathbb{N}^*$, on a :

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

5. Montrer que pour n, m non premiers entre eux dans $\mathbb{N}^*$, on a :

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

et :

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

6. Montrer que pour tout $x \in \mathbb{Z}_n^\times$ l'application $\sigma(x)$ définie sur $\mathbb{Z}_n$ par :

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

est un automorphisme du groupe additif $\mathbb{Z}_n$, puis que l'application σ réalise un isomorphisme de $(\mathbb{Z}_n^\times, \cdot)$ sur $(\mathrm{Aut}(\mathbb{Z}_n), \circ)$.

7. Montrer que pour tout entier $n \geq 2$, les idéaux de l'anneau $\mathbb{Z}_n$ sont principaux. L'anneau $\mathbb{Z}_n$ est-il principal ? Quels sont les quotients de $\mathbb{Z}_n$?

– III – Le groupe multiplicatif $\mathbb{Z}_n^\times$, fonction indicatrice d'Euler

1. Soit a un entier relatif. Montrer que les propriétés suivantes sont équivalentes :
   (a) $\overline{a}$ est inversible dans $\mathbb{Z}_n$;
   (b) a est premier avec n ;
   (c) $\overline{a}$ est un générateur de $(\mathbb{Z}_n, +)$.
2. Montrer que pour tout entier relatif a premier avec n, on a $a^{\varphi(n)} \equiv 1 \ (n)$ (théorème d'Euler).
3. Soit p un entier naturel premier. Montrer que pour tout entier relatif a premier avec n, on a $a^{p-1} \equiv 1 \ (p)$ et pour tout entier relatif a, on a $a^p \equiv a \ (p)$ (théorème de Fermat).
4. Montrer que pour tout entier $n \geq 3$, $\varphi(n)$ est un entier pair.
5. Soit $p \geq 2$ un nombre premier. Expliquer comment utiliser le théorème de Fermat pour simplifier le calcul du reste dans la division euclidienne par p d'un entier de la forme a^b, où a, b sont des entiers plus grands que p, l'entier p ne divisant pas a.
   Par exemple, calculer le reste dans la division euclidienne de 115^{2013} par 11.
6. Montrer que, pour tout entier $n \geq 2$, les assertions suivantes sont équivalentes :
   (a) n est premier ;
   (b) pour tout entier naturel non nul α, on a $\varphi(n^\alpha) = (n-1)n^{\alpha-1}$;
   (c) $\varphi(n) = n - 1$;
   (d) $\mathbb{Z}_n$ est un corps ;
   (e) $\mathbb{Z}_n$ est un intègre ;
   (f) $(n-1)! \equiv -1 \ (n)$ (théorème de Wilson) ;
   (g) $(n-2)! \equiv 1 \ (n)$;

(h) pour tout k compris entre 1 et n, on a $(n-k)!\,(k-1)! \equiv (-1)^k \pmod{n}$;

(i) pour tout entier k compris entre 1 et $n-1$, on a $\binom{n}{k} \equiv 0 \pmod{n}$;

(j) pour tout entier k compris entre 1 et $n-1$, on a $\binom{n}{k} \equiv 0 \pmod{n}$ et $\binom{n-1}{k} \equiv (-1)^k \pmod{n}$.

7. Soit p un nombre premier impair.

(a) Montrer qu'il y a exactement $\frac{p-1}{2}$ carrés et $\frac{p-1}{2}$ non carrés dans $\mathbb{Z}_p^*$.

(b) Montrer que l'ensemble des carrés de $\mathbb{Z}_p^*$ est l'ensemble des racines du polynôme $X^{\frac{p-1}{2}} - \overline{1}$ et que l'ensemble des non carrés de $\mathbb{Z}_p^*$ est l'ensemble des racines du polynôme $X^{\frac{p-1}{2}} + \overline{1}$.

(c) Montrer que $-\overline{1}$ est un carré dans $\mathbb{Z}_p$ si, et seulement si, p est congru à 1 modulo 4. Dans ce cas, donner une racine carrée explicite de $-\overline{1}$.

8. On s'intéresse aux racines du polynôme $P(X) = X^2 - 1$ dans $\mathbb{Z}_n$ pour $n \geq 2$.

(a) Traiter le cas où $n = p^\alpha$ où $p \geq 3$ est premier et $\alpha \geq 1$.

(b) Traiter le cas où $n = 2^\alpha$ où $\alpha \geq 1$.

(c) Traiter le cas général $n \geq 2$.

9. Montrer que pour tout entier $n \geq 2$, on a :

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

(formule de Möbius).

– IV – Le théorème chinois

1. Soient $(n_j)_{1 \leq j \leq r}$ une suite de $r \geq 2$ entiers naturels distincts de 0 et 1 et $n = \prod_{j=1}^{r} n_j$.

(a) Montrer que les entiers $n_1, \cdots, n_r$ sont deux à deux premiers entre eux si, et seulement si, les anneaux $\mathbb{Z}_n$ et $\prod_{j=1}^{r} \mathbb{Z}_{n_j}$ sont isomorphes.

(b) Pour $n_1, \cdots, n_r$ sont deux à deux premiers entre eux, montrer que l'application :

$$\begin{array}{rccc} \psi : & \mathbb{Z}_n & \to & \prod_{j=1}^{r} \mathbb{Z}_{n_j} \\ & \overline{k} & \mapsto & (\pi_1(k), \cdots, \pi_r(k)) \end{array}$$

est un isomorphisme d'anneaux d'inverse :

$$\begin{array}{rccc} \psi^{-1} : & \prod_{j=1}^{r} \mathbb{Z}_{n_j} & \to & \mathbb{Z}_n \\ & (\pi_1(a_1), \cdots, \pi_r(a_r)) & \mapsto & \overline{\sum_{i=1}^{r} a_i u_i m_i} \end{array}$$

où $(u_j)_{1 \leq j \leq r}$ est une suite d'entiers relatifs telle que $\sum_{j=1}^{r} u_j \frac{n}{n_j} = 1$.

2. Expliquer comment utiliser le théorème chinois pour étudier un système d'équations diophantiennes :

$$k \equiv a_j \pmod{n_j} \ (1 \leq j \leq r)$$

où $(a_j)_{1\leq j\leq r}$ est une suite donnée d'entiers relatifs.

3. Résoudre le système d'équations diophantiennes :

$$\begin{cases} k \equiv 2 \pmod 4 \\ k \equiv 3 \pmod 5 \\ k \equiv 1 \pmod 9 \end{cases}$$

4. Montrer que si $\mathbb{A}, \mathbb{B}$ sont deux anneaux 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 $\mathbb{B}^{\times}$.

5. 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 :

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

6. Soient p et q deux nombres premiers distincts et $n = pq$.
Montrer que si a et b sont deux entiers naturels tels que $ab \equiv 1 \pmod{\varphi(n)}$, alors pour tout entier relatif m, on a $m^{ab} \equiv m \pmod{n}$.
Ce résultat est à la base du système cryptographique R.S.A.

– V – $\mathbb{Z}_{p^\alpha}^{\times}$ est cyclique pour $p \geq 3$ premier et $\alpha \geq 1$

1. On se propose de montrer que, pour tout nombre premier p, le groupe $\mathbb{Z}_p^*$ est cyclique.
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.
Pour $\mathbb{Z}_p^*$, on peut en donner une démonstration directe basée sur des considérations arithmétiques relativement simples.
On peut aussi en donner une démonstration qui utilise la formule de Möbius.
   (a) Soient $(G, \cdot)$ un groupe commutatif, $r \geq 2$ un entier et $g_1, \cdots, g_r$ dans G des éléments d'ordres finis respectifs $n_1, \cdots, n_r$ deux à deux premiers entre eux. Montrer que $g = g_1 \cdot \cdots \cdot g_r$ est d'ordre $n = \prod_{k=1}^{r} n_k$.
   (b) Soient $p \geq 3$ un nombre premier impair et $p - 1 = \prod_{j=1}^{r} p_j^{\alpha_j}$ sa décomposition en facteurs premiers où $2 \leq p_1 < \cdots < p_r$ sont premiers et les α_j, pour j compris entre 1 et r, sont des entiers naturels non nuls.
      i. Soient j compris entre 1 et r, $q_j = \dfrac{p-1}{p_j^{\alpha_j}}$ et $x \in \mathbb{Z}_p^*$. Montrer que x^{q_j} est d'ordre $p_j^{r_{x,j}}$ où $0 \leq r_{x,j} \leq \alpha_j$.
      ii. Montrer que, pour j compris entre 1 et r, il existe dans $\mathbb{Z}_p^*$ un élément d'ordre $p_j^{\alpha_j}$.
      iii. En déduire que $\mathbb{Z}_p^*$ est cyclique.

(c) Soit p un nombre premier et $\mathcal{D}_{p-1}$ l'ensemble des diviseurs de $p-1$ dans $\mathbb{N}^*$.
Pour tout $d \in \mathcal{D}_{p-1}$, on note $\psi(d)$ le nombre d'éléments d'ordre d dans le groupe multiplicatif $\mathbb{Z}_p^*$.

i. Montrer que $p - 1 = \sum\limits_{d \in \mathcal{D}_{p-1}} \psi(d)$.

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

iii. En utilisant la formule de Möbius, montrer que $\psi(d) = \varphi(d)$ pour tout $d \in \mathcal{D}_{p-1}$ et en déduire que $\mathbb{Z}_p^*$ est cyclique.

2. Montrer que si p est un nombre premier impair et α un entier supérieur ou égal à 2, alors le groupe multiplicatif $\mathbb{Z}_{p^\alpha}^\times$ est cyclique.
3. Montrer que $\mathbb{Z}_2^\times$ et $\mathbb{Z}_{2^2}^\times$ sont cycliques.
4. On s'intéresse 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 :

$$\begin{array}{llll} \pi : & \mathbb{Z}_{2^\alpha}^\times & \to & \mathbb{Z}_4^\times \times \ker(\psi) \\ & x & \mapsto & (\psi(x), \psi(x)\, x) \end{array}$$

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 ?

On peut montrer le résultat suivant.

Théorème 1 *Le groupe multiplicatif $\mathbb{Z}_n^\times$ est cyclique si, et seulement si, $n = 2,\ 4,\ p^\alpha$ ou $2p^\alpha$ avec p premier impair et $\alpha \geq 1$.*

– VI – Nombres de Carmichaël

On appelle nombre de Carmichaël tout entier $n \geq 2$ non premier tel que :

$$\forall x \in \mathbb{Z}_n^\times,\ x^{n-1} = \overline{1}$$

1. Montrer qu'un nombre de Carmichaël est impair.
2. Montrer que 561 est un nombre de Carmichaël.
3. Soit $n \geq 3$ un entier admettant un facteur carré, c'est-à-dire qu'il existe un nombre premier $p \geq 2$ et un entier $q \geq 1$ tels que $n = p^2 q$.
Montrer que n n'est pas un nombre de Carmichaël.
4. Soit $n \geq 3$ un entier. Montrer que les propriétés suivantes sont équivalentes :

(a) il existe un entier $r \geq 3$ et des nombres premiers $3 \leq p_1 < \cdots < p_r$ tels que $n = \prod\limits_{j=1}^{r} p_j$ et, pour tout indice j compris entre 1 et r, $p_j - 1$ divise $n - 1$;

(b) n est non premier et :

$$\forall x \in \mathbb{Z}_n,\ x^n = x$$

(c) n est un nombre de Carmichaël.

5. Soit $a \in \mathbb{N}^*$ tel que les entiers $p_1 = 6a+1$, $p_2 = 12a+1$ et $p_3 = 18a+1$ soient premiers. Montrer que $n = p_1p_2p_3$ est un nombre de Carmichaël.

– VII – Le théorème de Frobénius-Zolotarev

Pour cette partie, $p \geq 3$ est un nombre premier impair et $n \geq 2$ est un entier.
Pour tout entier relatif a, on note $\overline{a} \in \mathbb{Z}_p$ la classe résiduelle de a modulo p.
On dit qu'un entier a non multiple de p est un résidu quadratique modulo p si il existe un entier k tel que $k^2 \equiv a \pmod{p}$, ce qui signifie que $\overline{a}$ est un carré dans $\mathbb{Z}_p^*$.
Pour tout $\lambda \in \mathbb{Z}_p^*$, on définit le symbole de Legendre $\left(\dfrac{\lambda}{p}\right)$ par :

$$\left(\frac{\lambda}{p}\right) = \begin{cases} 1 \text{ si } \lambda \text{ est un carré dans } \mathbb{Z}_p^* \\ -1 \text{ sinon} \end{cases}$$

1. Soit $\varphi : \mathbb{Z}_p^* \to \{-1, 1\}$ un morphisme de groupes non trivial.
Montrer que :

$$\forall \lambda \in \mathbb{Z}_p^*,\ \varphi(\lambda) = \left(\frac{\lambda}{p}\right)$$

2. Soit $\gamma : GL_n(\mathbb{Z}_p) \to \{-1, 1\}$ un morphisme de groupes non trivial.

(a) Montrer que $\gamma(A) = 1$ pour toute matrice de transvection A.

(b) Montrer que $\gamma(A) = \left(\dfrac{\det(A)}{p}\right)$ pour toute matrice de dilatation A.

(c) Montrer que $\gamma(A) = \left(\dfrac{\det(A)}{p}\right)$ pour toute matrice $A \in GL_n(\mathbb{Z}_p)$.

3. Une matrice $A \in GL_n(\mathbb{Z}_p)$ peut être identifiée à un automorphisme de $\mathbb{Z}_p^n$ qui est une permutation particulière de l'ensemble fini $\mathbb{Z}_p^n$, donc la restriction de la signature des permutations à $GL\left(\mathbb{Z}_p^n\right)$ permet de définir une morphisme de groupes ε de $GL_n(\mathbb{Z}_p)$ dans $\{-1, 1\}$.
Montrer que :

$$\forall A \in GL_n(\mathbb{Z}_p),\ \varepsilon(A) = \left(\frac{\det(A)}{p}\right)$$

– VIII – Groupes abéliens finis

On note $\theta(g)$ l'ordre d'un élément g d'un groupe G.
Pour un groupe fini G, l'entier $e(G) = \max\limits_{g \in G} \theta(g)$ est l'exposant du groupe.
Un caractère d'un groupe G est un morphisme de groupes de G dans $\mathbb{C}^*$.
Pour tout entier $m \geq 2$, on note Γ_m le groupe cyclique des racines m-èmes de l'unité dans $\mathbb{C}^*$.

1. Soient $(G, \cdot)$ un groupe commutatif, $r \geq 2$ un entier et $g_1, g_2, \cdots, g_r$ des éléments deux à deux distincts de G d'ordres respectifs $m_1, m_2, \cdots, m_r$.
Montrer qu'il existe dans G un élément g_0 d'ordre égal au ppcm de ces ordres.

2. Soit $(G, \cdot)$ un groupe commutatif fini. Montrer que :

$$e(G) = \max_{g \in G} \theta(g) = \text{ppcm}\{\theta(g) \mid g \in G\}$$

3. Soit $(G, \cdot)$ un groupe commutatif fini d'ordre $n \geq 2$. Montrer que n et son exposant $m = \max_{g \in G} \theta(g)$ ont les mêmes facteurs premiers.
4. Montrer qu'un groupe de cardinal $p \geq 2$ premier est cyclique (donc commutatif et isomorphe à $\mathbb{Z}_p$).
5. Montrer qu'un groupe commutatif d'ordre pq, où p et q sont deux nombres premiers distincts, est cyclique. Il est donc commutatif et isomorphe à $\mathbb{Z}_{pq}$.
6. Montrer que si $n \geq 2$ est un entier premier avec $\varphi(n)$, alors tout groupe commutatif d'ordre n est cyclique.
7. Montrer que si $n \geq 2$ est un entier premier avec $\varphi(n)$, alors tout groupe d'ordre n est cyclique.
8. Montrer que si $n \geq 2$ est un entier non premier avec $\varphi(n)$, il existe alors un groupe non cyclique d'ordre n.
   On a donc montré qu'un entier $n \geq 2$ est premier avec $\varphi(n)$ si, et seulement si, tout groupe d'ordre n est cyclique.
9. Soit G un groupe commutatif d'ordre $n \geq 2$.
   (a) Soient H un sous-groupe de G distinct de G, $\varphi : H \to \mathbb{C}^*$ un caractère et g un élément de $G \setminus H$.
      i. Justifier la définition de l'entier :
      $$r = \min\left\{k \in \mathbb{N}^* \mid g^k \in H\right\}$$
      ainsi que l'existence d'un nombre complexe $\alpha \in \mathbb{C}^*$ tel que $\varphi(g^r) = \alpha^r$.
      ii. Montrer que le caractère $\varphi : H \to \mathbb{C}^*$ peut se prolonger en un caractère sur le groupe $\langle g, H\rangle$ engendré par g et H.
      iii. Déduire de ce qui précède que le caractère $\varphi : H \to \mathbb{C}^*$ peut se prolonger en un caractère sur G.
   (b) On se donne un élément g_0 de G d'ordre égal à l'exposant de G, soit :
   $$m = \theta(g_0) = \max_{g \in G} \theta(g) = \text{ppcm}\{\theta(g) \mid g \in G\}$$
   En supposant que $m \leq n - 1$, on note $K = \langle g_0 \rangle$ le sous groupe cyclique de G engendré par g_0.
      i. Montrer qu'il existe un unique caractère $\varphi_0 : K \to \mathbb{C}^*$ tel que $\varphi_0(g_0) = \omega = e^{\frac{2i\pi}{m}}$.
      ii. En prolongeant le caractère φ_0 en un caractère φ de G, montrer que l'application :
      $$\begin{array}{rccc} \theta : & \langle g_0 \rangle \times \ker(\varphi) & \to & G \\ & \left(g_0^k, h\right) & \mapsto & g_0^k h \end{array}$$
      est un isomorphisme de groupes.
   (c) Déduire de ce qui précède, qu'il existe une suite d'entiers $(n_k)_{1 \leq k \leq r}$ telle que $n_1 \geq 2$, n_2 est multiple de n_1, ..., n_k est multiple de n_{k-1} et G est isomorphe au groupe produit $\Gamma = \prod_{k=1}^{r} \Gamma_{n_k}$.

(d) Soient $(n_k)_{1\leq k\leq r}$ et $(m_j)_{1\leq j\leq s}$ deux suites d'entiers telles que $r \geq 2$, $s \geq 2$, $n_1 \geq 2$, $m_1 \geq 2$, n_{k-1} divise n_k et m_{j-1} divise m_j pour k compris entre 2 et r et j compris entre 2 et s. Montrer que ces suites sont identiques si, et seulement si, on a :

$$\forall m \in \mathbb{N}^*, \ \prod_{k=1}^{r} \operatorname{pgcd}(m, n_k) = \prod_{j=1}^{s} \operatorname{pgcd}(m, m_j)$$

(e) En utilisant le résultat précédent, montrer qu'il existe une unique suite d'entiers $(n_k)_{1\leq k\leq r}$ telle que $n_1 \geq 2$, n_2 est multiple de n_1, ..., n_k est multiple de n_{k-1} et G est isomorphe au groupe produit $\Gamma = \prod_{k=1}^{r} \Gamma_{n_k}$ (théorème de Kronecker).
La suite $(n_k)_{1\leq k\leq r}$ est la suite des invariants de G et elle caractérise G à isomorphisme près.