

Fiche d'exercices n° 2 - Corrigés

Groupes et géométrie

Groupes monogènes

Exercice 1. *Théorème de Gauß.*

Montrons que, a, b, c étant trois éléments non nuls de $\mathbb{Z}$, si a et b sont premiers entre eux et si a divise bc , alors a divise c .

$$pgcd(a, b) = 1 \xRightarrow{\text{Bézout}} \exists u, v \in \mathbb{Z}, au + bv = 1.$$

De plus, $a \mid bc$, donc $\exists q \in \mathbb{Z}, bc = aq$.

$$\begin{aligned} au + bv = 1 &\implies auc + bcv = c \\ &\implies auc + aqv = c \\ &\implies a(uc + qv) = c \\ &\implies a \mid c \end{aligned}$$

Exercice 2.

m et n sont des entiers strictement positifs.

On rappelle que :

Si $a, b \in \mathbb{Z}$ et $d = pgcd(a, b)$, $a = a'd$, $b = b'd$ avec a' et b' premiers entre eux, et $\frac{ab}{d} = ab' = ba'$.

On définit alors $ppcm(a, b) = \frac{|ab|}{d}$.

L'exercice est basé sur le théorème suivant :

Tout multiple commun à a et b est un multiple de leur ppcm.

(voir les compléments à la fin de ce document, pour une démonstration).

- a.** On démontre ainsi immédiatement que $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z} \Leftrightarrow (m, n) = 1$
En effet,

$$\begin{aligned} m\mathbb{Z} \cap n\mathbb{Z} &= ppcm(m, n)\mathbb{Z} \text{ (par double inclusion)} \\ &\implies ppcm(m, n) = mn \\ &\implies pgcd(m, n) = 1 \end{aligned}$$

- b.** Démontrons le théorème 11, chapitre 3 :

- i) Sens direct : On suppose que $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
 En particulier, le noyau du morphisme associé est réduit à $\bar{0}$.
 donc $\alpha \equiv 0[m]$ et $\alpha \equiv 0[n] \Leftrightarrow \alpha \equiv 0[mn]$
 donc $\text{ppcm}(m, n) = mn$
 donc $\text{pgcd}(m, n) = 1$.
- ii) Réciproquement : on suppose que $\text{pgcd}(m, n) = 1$.
 Alors $\varphi : \mathbb{Z}/\text{ppcm}(m, n)\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est un isomorphisme.
 En effet, ces deux ensembles ont même cardinal, il nous reste donc à montrer que φ est injectif.
 Si $\alpha \equiv 0[m]$ et $\alpha \equiv 0[n]$, alors α est multiple de m et de n , et donc de leur ppcm .
 Donc, $\alpha \equiv 0[\text{ppcm}(m, n)]$, donc φ est un isomorphisme.
 Or, $\text{ppcm}(m, n) = mn$, donc $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Conclusion : $\boxed{\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \Leftrightarrow \text{pgcd}(m, n) = 1}$

Exercice 3. *Théorème de Wedderburn.*

Soit $n \geq 1$ un entier naturel.

- a.** Soit d un diviseur de n . Combien y a-t-il d'éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$?

Un élément d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ est un générateur du sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$.

Ce sous-groupe est cyclique, isomorphe à $\mathbb{Z}/d\mathbb{Z}$, il a $\varphi(d)$ générateurs.

On partitionne $\mathbb{Z}/n\mathbb{Z}$ en classes d'éléments de même ordre.

On obtient $\boxed{\sum_{d|n} \varphi(d) = n}$.

- b.** Soit G un sous-groupe fini du groupe multiplicatif d'un corps commutatif, et n son ordre. Pour chaque diviseur d de n , on note $\psi(d)$ le nombre d'éléments de G qui sont d'ordre d . Montrons que $\psi(d)$ vaut 0 ou $\phi(d)$.

Si $\psi(d) \neq 0$, il y a un élément de G d'ordre d .

Cet élément engendre un sous-groupe H d'ordre d composé d'éléments tous racines de $X^d - 1$.

Ce polynôme n'a donc pas d'autres racines (on est à coefficients dans un

corps).

Tous les éléments d'ordre d de G sont donc g{énérateurs de H qui est cyclique. Il y en a $\varphi(d)$.

c. On regroupe les éléments de G selon leur ordre, et on obtient : $\sum_{d|n} \psi(d) = n$

d. Dédisons-en que tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

$$n = \sum_{d|n} \varphi(d) = \sum_{d|n} \psi(d) \implies \sum_{d|n} (\varphi(d) - \psi(d)) = 0.$$

Comme chacun des termes de la somme est positif ou nul,

$$\varphi(d) = \psi(d) > 0, \forall d | n.$$

En particulier, $\psi(n) = \varphi(n) > 0$ et G admet au moins un élément d'ordre n .

Donc G est cyclique.

Exercice 4.

Soit $n \geq 1$ un entier naturel.

a. Soit $k \in \mathbb{Z}$ un entier. Déterminons le cardinal du sous groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par la classe de k modulo n .

$$x \in \langle \bar{k} \rangle \text{ dans } \mathbb{Z}/n\mathbb{Z} \Leftrightarrow \exists u, v \in \mathbb{Z}, x = ku + nv$$

donc x est un multiple de $d = \text{pgcd}(k, n)$.

Ils sont au nombre de $\frac{n}{d}$ dans $\mathbb{Z}/n\mathbb{Z}$.

Donc $\bar{k}$ engendre le sous-groupe d'ordre $\frac{n}{d}$.

En particulier :

si $\text{pgcd}(k, n) = 1$, on retrouve que $\langle \bar{k} \rangle = \mathbb{Z}/n\mathbb{Z}$

si $\text{pgcd}(k, n) = k$, on retrouve que $\langle \bar{k} \rangle = \mathbb{Z}/\left(\frac{n}{k}\right)\mathbb{Z}$

b. Si $m \geq 1$, déterminons le nombre de morphismes de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.

Soit $\varphi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ un morphisme.

On utilisera les notations $m = m'd$, et $n = n'd$ où $\text{pgcd}(m', n') = 1$

φ est déterminé par l'image de $\bar{1}$, et cette image doit vérifier la seule condition $m\varphi(\bar{1}) = \varphi(m\bar{1}) = \hat{0}$.

Si $\varphi(\bar{1}) = \hat{k}$, on a $n \mid mk$ d'où $n' \mid m'k$ d'où $n' \mid k$ car $\text{pgcd}(m', n') = 1$

Ainsi, φ est défini par $\varphi(\bar{1}) = \widehat{n'a}$ pour un $a \in \mathbb{Z}$

et il y a $d = \text{pgcd}(m, n)$ choix pour $a : a \in \{\hat{0}, \hat{1}, \dots, \widehat{d-1}\}$ (et $\widehat{n'd} = \hat{n} = \hat{0}$)

c. Montrons que $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

Considérons l'application :

$$\begin{aligned} \varphi : \text{End}(\mathbb{Z}/n\mathbb{Z}) &\longrightarrow (\mathbb{Z}/n\mathbb{Z}) \\ f &\longmapsto f(1) \end{aligned}$$

qui est une bijection.

Sa réciproque envoie k sur $f_k : x \mapsto kx$.

De plus, $f_k \circ f_l = f_{kl}$, et la bijection est un isomorphisme d'anneaux de $\text{End}(\mathbb{Z}/n\mathbb{Z}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})$.

La restriction aux inversibles donne $\boxed{\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times}$

En particulier, $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ est abélien !

Exercice 5. *Deux classiques.*

a. Théorème d'Euler

Soit $n \in \mathbb{N}^*$, soit $a \in \mathbb{Z}^*$, *premier avec* n .

φ désignant la fonction d'Euler, démontrer que : $a^{\varphi(n)} \equiv 1 \pmod{n}$

Démonstration :

Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}^*$ tels que $\text{pgcd}(a, n) = 1$.

Dans $\mathbb{Z}/n\mathbb{Z}$, $\text{pgcd}(a, n) = 1 \implies \bar{a}$ inversible et générateur.

$\langle a \rangle \simeq ((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ a pour cardinal $\varphi(n)$.

Donc $a^{\varphi(n)} \equiv 1[n]$.

b. Théorème de Fermat

Soient p un nombre *premier*, et $a \in \mathbb{Z}$.

Démontrer que $a^p \equiv a \pmod{p}$

Démonstration :

p est premier, donc $\mathbb{Z}/p\mathbb{Z}$ est un corps, et donc son sous-groupe des inversibles est cyclique de cardinal $p - 1$.

$$\left(\mathbb{Z}/p\mathbb{Z}, \times\right)^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}.$$

Donc $\bar{a}^{p-1} \equiv 1[p]$, et donc $\bar{a}^p \equiv a[p]$

Exercice 6.

Soit G un groupe commutatif, et x, y deux éléments de G d'ordre respectif m et n .

a. Montrons que si m et n sont premiers entre eux, xy est d'ordre mn .

G commutatif, donc $(xy)^{mn} = x^{mn}y^{mn} = (x^m)^n(y^n)^m = 1$.

Donc $o(xy) \mid mn$.

Puis, si $k \geq 1$ est tel que $(xy)^k = 1$, on a $1 = (xy)^{km} = x^{km}y^{km} = y^{km}$. Donc $n \mid km$ et donc $n \mid k$ car $\text{pgcd}(m, n) = 1$ (Gauß).

De même $m \mid k$ et donc $mn \mid k$.

Donc $mn \mid o(xy)$.

Enfin, $o(xy) = mn$.

b. Montrons que, dans le cas général, il existe un diviseur m' de m et un diviseur n' de n tels que m' et n' soient premiers entre eux et $m'n' = \text{ppcm}(m, n)$.

Par définition du pgcd , $d = \text{pgcd}(m, n) \implies \exists m', n'$ tel que $m = m'd$ et $n = n'd$ avec $\text{pgcd}(m', n') = 1$.

$$\left(\text{Sinon, prendre } m' = \prod_{v_p(m) \geq v_p(n)} p^{v_p(m)} \text{ et } n' = \prod_{v_p(n) > v_p(m)} p^{v_p(n)} \right).$$

c. Montrons qu'il existe dans G un élément d'ordre $\text{ppcm}(m, n)$.

Constatons que :

x est d'ordre $m \implies x^{\frac{m}{m'}}$ est d'ordre m'

y est d'ordre $n \implies y^{\frac{n}{n'}}$ est d'ordre n'

Mais comme $\text{pgcd}(m', n') = 1$, on a, d'après la question a), que :

$x^{\frac{m}{m'}} y^{\frac{n}{n'}}$ est d'ordre $m'n' = \text{ppcm}(m, n)$.

- d.** i) Montrons que si G est d'exposant N , (c'est à dire $\forall g \in G, g^N = 1$ et N est le plus petit entier non nul jouissant de cette propriété), G admet un élément d'ordre N .

Comme l'ordre des éléments de G est borné, il existe un élément x d'ordre maximal, disons $m = o(x)$ et supposons que $m \mid N$, $m \neq N$.

$\exists y \in G, y^m \neq 1$

Si $n = o(y)$, on a montré qu'il existe z d'ordre $\text{ppcm}(m, n) > m$. Contradiction.

- ii) Montrons que ce n'est pas forcément le cas si G n'est pas commutatif.

Penser par exemple à S_3 (non abélien) qui est d'exposant 6 et ne contient pas d'élément d'ordre 6.

- e.** Déduisons-en une autre démonstration du théorème de Wedderburn (tout sous-groupe fini du groupe multiplicatif d'un corps (commutatif) est cyclique).

Si G est un sous-groupe du groupe multiplicatif d'un corps.

Il a un exposant N , et $\exists x \in G$ d'ordre N .

x engendre un sous-groupe H de G d'ordre N .

Tout élément de H est racine de $X^N - 1$, et ce polynôme n'a pas d'autre racine.

Mais par définition de l'exposant, tout élément de G est racine.

Donc $G \subset H$, et $G = H$ est cyclique.

Exercice 7. *Théorème de Wilson.*

Soit $p \geq 2$ un nombre premier.

- a. Dans $\mathbb{Z}/p\mathbb{Z}$, l'équation $x^2 = 1 \Leftrightarrow x = x^{-1}$ possède uniquement deux solutions : 1 et -1.
- b. Considérons le produit $(p-1)! = 1 \times 2 \times \dots \times (p-1)$ dans $\mathbb{Z}/p\mathbb{Z}$,
 $\bar{1}$ et $\overline{p-1} = \overline{-1}$ sont leur propre inverse, et chacun des autres éléments s'apparie avec son inverse. Leur produit vaut donc 1 modulo p .
 Donc $(p-1)! \equiv p-1 = -1[p]$, ou encore $(p-1)! + 1 \equiv [p]$.
- c. Réciproquement, soit $n \geq 2$ divisant $(n-1)! + 1$,
 alors dans $\mathbb{Z}/n\mathbb{Z}$, $(n-1) \times (n-2) \times \dots \times 2 \times 1 = -1$,
 mais donc chaque $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ y est inversible.
 Donc $\mathbb{Z}/n\mathbb{Z}$ est un corps, et n est premier.

Exercice 8.

Soit p un entier premier, $k \in \mathbb{N}$.

Soit $a \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$, $x \mapsto ax$ est une permutation de $\mathbb{F}_p$.

$$\text{Donc, } a^k \sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} (ax)^k = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k.$$

$$\text{Donc, } (a^k - 1) \sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k = 0.$$

- S'il existe $a \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ tel que $a^k \neq 1$, $\sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k = 0$.
- Sinon, tout a inversible vérifie $a^k = 1$ d'où
 $\sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k = 0 + \sum_{x \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times} x^k = 0 + p-1 = -1$

Exercice 9. (*Théorème 12 du cours*).

- a. Montrons le lemme suivant :

Si p est un nombre premier, pour tout $\alpha \geq 1 \in \mathbb{N}$, on a :

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

$\varphi(p^\alpha)$ est le nombre d'entiers k tel que $1 \leq k \leq p^\alpha$ et $k \nmid p$.
Or, les multiples m de p tel que $1 \leq m \leq p^\alpha$
sont tels que $m = pq$ avec $1 \leq q \leq p^{\alpha-1}$, il y en a $p^{\alpha-1}$
Donc $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p - 1)$

b. Dédisons-en que :

Soit $n > 1$ un entier.

Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ est la décomposition en facteurs premiers de n , alors :

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

Les $p_i^{\alpha_i}$ étant premiers entre eux, on a :

$$\begin{aligned} \varphi(n) &= \prod_{i=1}^k \varphi(p_i^{\alpha_i}) = p_1^{\alpha_1-1}(p_1 - 1) \dots p_k^{\alpha_k-1}(p_k - 1) \\ &= p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_k^{\alpha_k-1} (p_1 - 1) \dots (p_k - 1) \\ &= \frac{n}{p_1 \dots p_k} (p_1 - 1) \dots (p_k - 1) \\ &= n \times \left(\frac{p_1 - 1}{p_1}\right) \times \dots \times \left(\frac{p_k - 1}{p_k}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \times \dots \times \left(1 - \frac{1}{p_k}\right) \end{aligned}$$

c. Application : Calculons $\varphi(3960)$.

$3960 = 2^3 \times 3^2 \times 5 \times 11$ d'où :

$$\varphi(3960) = 3960 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) \times \left(1 - \frac{1}{5}\right) \times \left(1 - \frac{1}{11}\right) = 960...$$

Exercice 10. Inversibles de $(\mathbb{Z}/2^\alpha\mathbb{Z})$ et de $(\mathbb{Z}/p^\alpha\mathbb{Z})$ avec $p \geq 3$ premier.

- a. Montrons que si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ est la décomposition en facteurs premiers de n , alors :

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^k (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$$

Le théorème chinois nous dit que dans ce cas, $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^k \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$.

Mais cela implique que leur groupe d'inversibles sont isomorphes, et c'est le résultat demandé.

- b. Soit $p \geq 3$ un nombre premier.

Montrons que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique. On aura alors :

$$\begin{aligned} (\mathbb{Z}/p^\alpha\mathbb{Z})^\times &\simeq \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z} \\ &\simeq \mathbb{Z}/(p^{\alpha-1})(p-1)\mathbb{Z} \quad \text{d'après l'exercice 9} \\ &\simeq (\mathbb{Z}/p^{\alpha-1}\mathbb{Z}) \times (\mathbb{Z}/(p-1)\mathbb{Z}) \quad \text{car } p^{\alpha-1} \text{ et } p-1 \text{ sont premiers entre eux} \end{aligned}$$

- Montrons que la classe de $p+1$ est d'ordre $p^{\alpha-1}$.

On montre par récurrence sur k que,

$$\forall k \in \mathbb{N}, \exists \lambda \in \mathbb{N}, (1+p)^{p^k} = 1 + p^{k+1}\lambda \text{ avec } \lambda \text{ premier à } p.$$

Initialisation :

pour $k=0$, $(1+p)^1 = 1 + p^1 \times 1$, et $\lambda=1$ convient.

Hérédité :

Si la proposition est vraie à un certain rang k , alors :

$$\begin{aligned} (1+p)^{p^{k+1}} &= \left((1+p)^{p^k}\right)^p \\ &= (1 + p^{k+1}\lambda)^p \\ &= 1 + p^{k+1}(\lambda + pm) \text{ pour un certain } m \in \mathbb{N}, \text{ d'après le binôme de Newton} \end{aligned}$$

De plus, si $k \mid (\lambda + pm)$ et $k \mid p$, alors $k \mid \lambda$

Mais le seul diviseur commun à λ et p est 1.

Donc $k=1$ et $\text{pgcd}(\lambda + pm; p) = 1$.

Appliquons alors ce résultat avec $k = \alpha - 1$.

On a donc $(1+p)^{p^{\alpha-1}} = 1 + p^\alpha \lambda = 1[p^\alpha]$.

Donc $o(1+p) \mid p^{\alpha-1}$ ($p^{\alpha-1}$ a pour seul diviseur premier p).

Supposons $(1+p)^{p^k} = 1[p^\alpha]$, alors $p^{k+1}\lambda = 0[p^\alpha]$ et $\text{pgcd}(\lambda; p) = 1$.
 Mais $p^\alpha \mid p^{k+1}\lambda$ et

$$\begin{aligned} \text{pgcd}(p^\alpha; \lambda) = 1 &\xRightarrow{\text{Gau\ss}} p^\alpha \mid p^{k+1} \\ &\implies \alpha \leq k+1 \\ &\text{c\`ad } k \geq \alpha - 1 \end{aligned}$$

En particulier $o(1+p) \geq p^{\alpha-1}$, donc $\boxed{o(1+p) = p^{\alpha-1}}$.

- Montrons que le groupe des unit s contient un  l ment d'ordre $p-1$
 $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$. Soit donc $a \in \mathbb{Z}$ tel que $a^{p-1} = 1[p]$.
 Alors $\bar{a}$, modulo p^α , est d'ordre un multiple de $(p-1)$.
 (en effet, les $\bar{a}^k$ vont  tre plus nombreux modulo p^α mais contiennent les $\bar{a}^k$ modulo p)
 Si on note $k = l(p-1)$ l'ordre de $\bar{a}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, alors $b = \bar{a}^l$ est d'ordre $p-1$.
- Montrons que le groupe des unit s est cyclique.
 Comme $\bar{b}$ et $\overline{p+1}$ commutent et que leur ordre sont premiers entre eux, leur produit est d'ordre le produit des ordres : $(p-1)p^{\alpha-1} = \varphi(p^\alpha)$
 Ce groupe est donc cyclique, engendr  par $\bar{c} = \overline{b(p+1)}$.

c. Cas $p = 2$.

Montrons que $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2}\mathbb{Z})$

Plus pr c d ment, c'est le produit direct interne du sous-groupe engendr  par $\overline{-1}$ et du sous-groupe d'ordre $2^{\alpha-2}$ engendr  par $\bar{5}$.

- Montrons que la classe de 5 est d'ordre $2^{\alpha-2}$.
 D montrons par r currence que :

$$\forall k \in \mathbb{N}, \exists \lambda \in \mathbb{N}, 5^{2^k} = 1 + 2^{k-2}\lambda \text{ avec } \lambda \text{ impair}$$

Initialisation :

pour $k = 0$, OK avec $\lambda = 1$.

H r dit  : Si la proposition est vrai   un certain rang k , alors :

$$\begin{aligned} 5^{2^{k+1}} &= 5^{2^k \times 2} \\ &= \left(5^{2^k}\right)^2 \\ &= \left(1 + 2^{k-2}\lambda\right)^2 \\ &= 1 + 2^{k+3}\lambda + 2^{2k-4}\lambda^2 \\ &= 1 + 2^{k+3}(\lambda + 2^{k-1}\lambda^2) \end{aligned}$$

Mais comme 2^{k+1} est pair et λ^2 est impair, leur produit $2^{k+1}\lambda^2$ est pair.
 Mais comme λ est impair, la somme $\lambda + 2^{k+1}\lambda^2$ est impair, et le r sultat

est démontré.

Appliquons maintenant avec $k = \alpha - 2$

On obtient $5^{2^{\alpha-2}} = 1 + 2^\alpha \lambda = 1[2^\alpha]$

Donc $o(5) \mid 2^{\alpha-2}$

Mais si $5^{2^k} = 1[2^\alpha]$ alors $2^{k+2}\lambda = 0[2^\alpha]$.

Et comme λ est impair, cela implique que $k + 2 \geq \alpha$, c'est à dire que $k \geq \alpha - 2$, et donc que $o(5) \geq 2^{\alpha-2}$.

Au final, $o(5) = 2^{\alpha-2}$.

- Montrons que le groupe des unités est le produit direct interne des deux sous-groupes engendrés par $\bar{5}$ et $\overline{-1}$.

Modulo 4, toutes les puissances de 5 sont congrues à 1, donc pas à -1.

À fortiori, modulo 2^α ($\alpha \geq 2$), $\overline{-1}$ n'est pas une puissance de $\bar{5}$.

L'intersection de $\langle \overline{-1} \rangle$ et $\langle \bar{5} \rangle$ est réduite au neutre.

Le produit de leur ordre est égal à $2^{\alpha-1} = \varphi(2^\alpha) = o((\mathbb{Z}/2^\alpha\mathbb{Z})^\times)$. CQFD

Exercice 11.

Déterminons la structure des quelques groupes suivant :

a. $15 = 3 \times 5$ donc

$$\begin{aligned} (\mathbb{Z}/15\mathbb{Z})^\times &\simeq (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \\ &\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \end{aligned}$$

b. $55 = 5 \times 11$ donc

$$\begin{aligned} (\mathbb{Z}/55\mathbb{Z})^\times &\simeq (\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/11\mathbb{Z})^\times \\ &\simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \\ &\simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ &\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z} \end{aligned}$$

c. $27 = 3^3$ donc

$$\begin{aligned} (\mathbb{Z}/27\mathbb{Z})^\times &\simeq (\mathbb{Z}/3^2(3-1)\mathbb{Z}) \\ &\simeq (\mathbb{Z}/18\mathbb{Z}) \end{aligned}$$

d. $16 = 2^4$ donc

$$(\mathbb{Z}/16\mathbb{Z})^\times \simeq (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$$

COMPLEMENTS :

I. Théorème de Bézout :

Soient $a, b \in \mathbb{Z}$ tel que $d = \text{pgcd}(a, b)$.

Il existe alors $u, v \in \mathbb{Z}$, tel que $au + bv = d$.

On considère pour cela l'ensemble $I = \{au + bv > 0, \text{ où } u, v \in \mathbb{Z}\}$.

Cet ensemble est non vide car il contient $|a|$ et $|b|$.

Il contient donc un plus petit élément d_0 .

Montrons que $d_0 = au_0 + bv_0 = d$.

$a = d_0q + r$ avec $0 \leq r < d_0$ (division euclidienne)

$r = a - d_0q = a - (au_0 + bv_0)q = a(1 - u_0q) + b(-v_0q)$.

Donc $r \in I$, et $r < d_0$.

Par définition de d_0 , cela implique que $r = 0$, et donc $a = d_0q$, et $d_0 \mid a$.

De même, on montre que $d_0 \mid b$, et d_0 est alors un diviseur commun à a et à b .

Mais, tous les diviseurs communs à a et à b divisent $au_0 + bv_0 = d_0$.

Donc d_0 est le plus grand, et $d_0 = d$.

II. Tout multiple commun à a et b est un multiple de leur ppcm.

En effet, soit $n \in \mathbb{Z}$, $\text{pgcd}(na', nb') = n\text{pgcd}(a', b') = n$

donc :

$$\begin{aligned}(a \mid n \text{ et } b \mid n) &\implies (ab' \mid nb' \text{ et } ba' \mid na') \\ &\implies (\text{ppcm}(a, b) \mid nb' \text{ et } \text{ppcm}(a, b)') \\ &\implies \text{ppcm}(a, b) \mid \text{pgcd}(nb', na') \\ &\implies \text{ppcm}(a, b) \mid n\end{aligned}$$

III. Pour compléter l'exercice 4.

Considérons :

$p : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ la surjection canonique.

$\delta = \text{pgcd}(m, n)$ et $m = \delta m', n = \delta n'$ avec $\text{pgcd}(m', n') = 1$.

Alors, :

$$\begin{aligned}\varphi : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \text{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \\ f \circ p(1) &\longmapsto f\end{aligned}$$

est telle que $\text{Ker}\varphi \simeq \mathbb{Z}/n'\mathbb{Z} < \mathbb{Z}/n\mathbb{Z}$

φ induit l'isomorphisme : $\frac{\mathbb{Z}/n\mathbb{Z}}{\mathbb{Z}/n'\mathbb{Z}} \simeq \text{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$.

c'est à dire $\frac{n'\mathbb{Z}}{n\mathbb{Z}} \simeq \text{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$.

Soit $\boxed{\mathbb{Z}/\delta\mathbb{Z} \simeq \text{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})}$.