1

Les anneaux $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$

[1]On suppose connus le théorème de division euclidienne ainsi que les notions de pgcd, de ppcm, de nombres premiers entre eux et de nombres premiers. Les théorème de Bézout et de Gauss sont supposés acquis.

On pourra se reporter aux chapitres **??**, **??** et **??**.

Les notions de base sur les groupes sont supposées connues. En particulier, les ensembles et groupes quotients sont supposés connus.

Pour des rappels, on pourra consulter le chapitre **??**.

1.1 Congruences dans $\mathbb{Z}$, anneaux $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$

Pour tout entier naturel n, on note :

$$n\mathbb{Z} = \{n \cdot q \mid q \in \mathbb{Z}\}$$

le sous-groupe additif de $\mathbb{Z}$ formé de tous les multiples de n.

On peut remarquer que pour tout $a = qn \in n\mathbb{Z}$ et tout $b \in \mathbb{Z}$, on a $ab = bqn \in n\mathbb{Z}$, ce qui se traduit en disant que $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

Du théorème de division euclidienne, on déduit que les $n\mathbb{Z}$ sont les seuls sous-groupes (ou idéaux) de $(\mathbb{Z}, +)$.

Définition 1.1 *Soient n un entier naturel et a, b deux entiers relatifs.*
On dit que a est congru à b modulo n si n divise $b - a$.
On note alors :

$$a \equiv b \ (n)$$

Dire que a est congru à b modulo n équivaut aussi à dire que $b - a \in n\mathbb{Z}$, ce qui est encore équivalent à dire que a et b ont le même reste dans la division euclidienne par n.

Pour $n = 0$, on a $0 \cdot \mathbb{Z} = \{0\}$ et $a \equiv b \ (0)$ revient à dire que $a = b$.

Pour $n = 1$, on a $1 \cdot \mathbb{Z} = \mathbb{Z}$ et la relation $a \equiv b \ (1)$ est toujours vérifiée.

Cette relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$ et pour tout entier relatif a, on note :

$$\begin{aligned}\overline{a} &= \{b \in \mathbb{Z} \mid b \equiv a \ (n)\} = \{b \in \mathbb{Z} \mid n \text{ divise } b - a\} \\ &= \{b = a + qn \mid q \in \mathbb{Z}\} = a + n\mathbb{Z}\end{aligned}$$

1. Version du 24/09/2016

sa classe d'équivalence modulo n.

L'ensemble de toutes ces classes d'équivalence modulo n est noté $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

C'est l'ensemble quotient de $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$.

On dit aussi que c'est l'ensemble des classes résiduelles modulo n.

On désigne par :

$$\begin{array}{rccc} \pi_n : & \mathbb{Z} & \to & \dfrac{\mathbb{Z}}{n\mathbb{Z}} \\ & k & \mapsto & \overline{k} \end{array}$$

la surjection canonique de $\mathbb{Z}$ sur $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

Tout antécédent par π_n d'un élément x de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est appelé un représentant de x.

Dans le cas particulier où $n = 0$, la congruence modulo 0 est tout simplement la relation d'égalité et pour tout entier relatif a, on a :

$$\overline{a} = a + 0\mathbb{Z} = \{a\}$$

de sorte que :

$$\frac{\mathbb{Z}}{0 \cdot \mathbb{Z}} = \{\{a\} \mid a \in \mathbb{Z}\}$$

est en bijection avec $\mathbb{Z}$.

On identifie donc $\dfrac{\mathbb{Z}}{0 \cdot \mathbb{Z}}$ à $\mathbb{Z}$.

Dans le cas particulier où $n = 1$, deux entiers relatifs quelconques sont toujours congrus modulo 1 et pour tout entier relatif a, on a :

$$\overline{a} = a + \mathbb{Z} = \mathbb{Z}$$

de sorte que :

$$\frac{\mathbb{Z}}{1 \cdot \mathbb{Z}} = \{\mathbb{Z}\} = \left\{\overline{0}\right\}$$

est identifié à $\{0\}$.

Dans ce qui suit, on suppose a priori que $n \geq 2$.

Théorème 1.1 *Pour tout entier naturel non nul n, on a :*

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\}$$

Cet ensemble est de cardinal égal à n et il est en bijection avec l'ensemble de tous les restes possibles dans la division euclidienne par n.

Démonstration. Le théorème de division euclidienne nous permet d'écrire tout entier relatif a sous la forme $a = qn + r$ avec $0 \leq r \leq n-1$, ce qui entraîne que $\overline{a} = \overline{r}$ dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

On a donc $\dfrac{\mathbb{Z}}{n\mathbb{Z}} = \left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\}$.

Pour montrer que cet ensemble est de cardinal égal à n, il nous reste à vérifier que tous ses éléments sont distincts.

Si $\overline{r} = \overline{s}$ avec r et s compris entre 0 et $n-1$, on a alors $s - r = qn$ avec $q \in \mathbb{Z}$ et l'encadrement $0 \leq |s - r| = |q|\, n \leq n - 1$ dans $\mathbb{N}$ impose $q = 0$, ce qui équivaut à $r = s$. ∎

La relation de congruence modulo n est compatible avec l'addition et la multiplication sur $\mathbb{Z}$, ce qui signifie que pour a, b, c, d dans $\mathbb{Z}$, on a :

$$(a \equiv b\ (n)\,,\ c \equiv d\ (n)) \ \Rightarrow\ (a+c \equiv b+d\ (n)\,,\ ac \equiv bd\ (n))$$

En effet $b-a \in n\mathbb{Z}$ et $d-c \in n\mathbb{Z}$ entraîne $b+d-(a+c) = (b-a)+(d-c) \in n\mathbb{Z}$ puisque $n\mathbb{Z}$ est un groupe et $bd-ac = d\,(b-a)+a\,(d-c) \in n\mathbb{Z}$ puisque $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

La notion de congruence peut être utile pour résoudre des exercices élémentaires d'arithmétique.

Exercice 1.1 *Soient* x *et* y *dans* $\mathbb{Z}$. *Montrer que si* $3x+7y$ *est multiple de* 11, $4x-9y$ *est alors multiple de* 11.

Solution 1.1 *On a* $3x \equiv -7y\ (11)$ *donc* $15x \equiv -35y\ (11)$ *avec* $15x \equiv 4x\ (11)$ *et* $-35y \equiv 9y\ (11)$.

Exercice 1.2 *Montrer que si un entier impair est somme de deux carrés d'entiers, il est alors congru à* 1 *modulo* 4 *(i. e.* $p-1$ *est multiple de* 4*).*
Le résultat de cet exercice est utile dans l'étude des entiers sommes de deux carrés (voir le paragraphe **??***).*

Solution 1.2 *Soit* $p = a^2+b^2$ *un entier impair somme de deux carrés.*
Le résultat étant trivial pour $p = 1$, *on suppose que* $p \geq 3$.
Tout entier relatif k *est congru à* $0, 1, 2$ *ou* 3 *modulo* 4, *donc* k^2 *est congru à* 0 *ou* 1 *modulo* 4 *et* a^2+b^2 *est congru à* $0, 1$ *ou* 2 *modulo* 4.
Si $p = a^2+b^2$ *est impair, il est alors congru à* 1 *modulo* 4, *ce qui signifie que* $p-1$ *est multiple de* 4.

Exercice 1.3 *Déterminer tous les couples* $(x, y) \in \mathbb{Z}^2$ *tels que :*

$$5x^2+3 = y^2$$

Solution 1.3 *Si* $(x, y) \in \mathbb{Z}^2$ *est une solution, on a alors* $y^2 \equiv 3 \bmod (5)$. *Pour* $y \in \mathbb{Z}$, *on a* $y \equiv 0, 1, 2, 3$ *ou* $4 \bmod (5)$, *donc* $y^2 \equiv 0, 1, 4$ *ou* $1 \bmod (5)$ *et on a une impossibilité. L'ensemble des solutions est donc vide.*

Exercice 1.4 *Montrer que pour tout entier* $n \geq 2$, *l'entier* $m = n^2(n^2-1)$ *est divisible par* 12, *puis que l'entier* $r = n^2(n^4-1)$ *est divisible par* 60.

Solution 1.4 *Comme* $n(n-1)$ *et* $n(n+1)$ *sont pairs,* m *est divisible par* 4. *Comme* $n \equiv 0, 1$ *ou* $2 \bmod (3)$, *on a* $m \equiv 0 \bmod (3)$.
Donc m *est divisible par* 3 *et* 4, *soit par* 12 *puisque* $3 \wedge 4 = 1$.
Comme $n \equiv 0, 1, 2, 3$ *ou* $4 \bmod (5)$, *on a* $r \equiv 0 \bmod (5)$. *Donc* r *est divisible par* 5 *et* 12, *soit par* 60 *puisque* $5 \wedge 12 = 1$.

On peut aussi utiliser les congruences pour obtenir des critères de divisibilité des entiers par $m = 2, 3, 5, 9$ et 11.

Soit a un entier naturel non nul d'écriture décimale :

$$a = \overline{a_p \cdots a_1 a_0}^{10} = \sum_{k=0}^{p} a_k 10^k$$

où les a_k sont des entiers compris entre 0 et 9, le coefficient a_p étant non nul.

Si $10^k \equiv r_k \pmod{m}$, on a alors $a \equiv \sum_{k=0}^{p} a_k r_k \pmod{m}$ et m divise a si, et seulement si, il divise $\sum_{k=0}^{p} a_k r_k$ (voir les exercices **??** et **??**).

La compatibilité de la relation de congruence modulo n avec l'addition et la multiplication sur $\mathbb{Z}$ va nous permettre de transporter la structure d'anneau de $\mathbb{Z}$ à $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ pour $n \geq 2$ (pour $n = 1$, $\dfrac{\mathbb{Z}}{1 \cdot \mathbb{Z}} = \left\{\overline{0}\right\}$ n'est pas un anneau unitaire), un tel prolongement étant unique.

Théorème 1.2 *Pour $n \geq 2$, il existe une unique structure d'anneau commutatif unitaire sur $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ telle que la surjection canonique π_n soit un morphisme d'anneaux.*

Démonstration. On vérifie tout d'abord qu'on définit deux opérations internes sur l'ensemble $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ avec :

$$\forall\,(x,y) \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^2,\ \begin{cases} x+y = \overline{a+b} \\ xy = \overline{ab} \end{cases}$$

où $a \in \mathbb{Z}$ est un représentant de x et $b \in \mathbb{Z}$ est un représentant de y.

En effet, si a' est un autre représentant de x et b' un autre représentant de y, on a alors $a \equiv a'$ et $b \equiv b'$ modulo n, ce qui entraîne $a + b \equiv a' + b'$ et $ab \equiv a'b'$ modulo n, soit $\overline{a+b} = \overline{a'+b'}$ et $\overline{ab} = \overline{a'b'}$, ce qui prouve que ces définitions de $x + y$ et xy ne dépendent pas des choix des représentants de x et y.

On vérifie ensuite facilement que ces deux lois confèrent à $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ une structure d'anneau commutatif unitaire et que π_n est bien un morphisme d'anneaux.

Réciproquement s'il existe une structure d'anneau commutatif unitaire sur $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ qui fait de π_n un morphisme d'anneaux, on a alors pour tous $x = \pi_n(a), y = \pi_n(b)$ dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$:

$$\begin{cases} x+y = \pi_n(a) + \pi_n(b) = \pi_n(a+b) = \overline{a+b} \\ xy = \pi_n(a)\,\pi_n(b) = \pi_n(ab) = \overline{ab} \end{cases}$$

ce qui prouve l'unicité. ■

Le théorème précédent est un cas particulier du théorème **??**.

On pourra se reporter au paragraphe **??** pour l'étude plus générale du quotient d'un anneau commutatif unitaire par un idéal.

Exercice 1.5 *Soit $n \geq 2$ un entier naturel. Quels sont les éléments nilpotents de l'anneau $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$?*

Solution 1.5 *Voir l'exercice* **??**.

Les groupes additifs $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sont cycliques et tout groupe cyclique d'ordre n est isomorphe à $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ (théorème 2.4).

Pour l'étude des groupes cycliques, on se reportera au chapitre 2.

Dans le cas particulier des groupes additifs $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$, on a le résultat suivant.

Théorème 1.3 *Pour $n \geq 2$, tous les sous-groupes de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sont cycliques d'ordre qui divise n.*
Réciproquement pour tout diviseur d de n, il existe un unique sous-groupe de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ d'ordre d, c'est le groupe cyclique :

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

où $q = \dfrac{n}{d}$.
Ce sous-groupe H est aussi l'ensemble des éléments de G dont l'ordre divise d et les générateurs de H sont tous les éléments d'ordre d de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

Pour ce qui est des idéaux de l'anneau $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$, pour $n \geq 2$, ce sont en fait ses sous-groupes (exercice **??**) et ils sont principaux (lemme **??**).

Avec l'exercice qui suit, on s'intéresse aux morphismes de groupes et d'anneaux de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ dans $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$.

Exercice 1.6

1. *Déteminer tous les morphismes de groupes de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ dans $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$, pour tous les entiers naturels n, m.*
2. *Déteminer tous les morphismes d'anneaux de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ dans $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$, pour tous les entiers naturels n, m différents de 1.*

Solution 1.6 *On note $\mathrm{Hom}_{gr}\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, \dfrac{\mathbb{Z}}{m\mathbb{Z}}\right)$ [resp. $\mathrm{Hom}_{Ann}\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, \dfrac{\mathbb{Z}}{m\mathbb{Z}}\right)$] l'ensemble des morphismes de groupes [resp. d'anneaux] de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ dans $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$.*
Pour simplifier, on notera $\overline{k} = \pi_n(k) = k + n\mathbb{Z}$ un élément de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ et $\widehat{k} = \pi_m(k) = k + m\mathbb{Z}$ un élément de $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$.

1. *Tout est basé sur le fait qu'un tel morphisme de groupes est uniquement déterminé par l'image de $\overline{1}$.*
   Cela se traduit en disant que l'application :

$$\begin{array}{rccc} \theta : & \mathrm{Hom}_{gr}\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, \dfrac{\mathbb{Z}}{m\mathbb{Z}}\right) & \to & \dfrac{\mathbb{Z}}{m\mathbb{Z}} \\ & \varphi & \mapsto & \alpha = \varphi\left(\overline{1}\right) \end{array}$$

   est un morphisme injectif de groupes additifs. Il en résulte que le groupe additif $\mathrm{Hom}_{gr}\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, \dfrac{\mathbb{Z}}{m\mathbb{Z}}\right)$ est isomorphe à $\mathrm{Im}(\theta)$ qui est un sous-groupe de $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$, donc cyclique d'ordre divisant m pour $m \geq 1$.

   (a) *Pour $m = 0$, $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$ est identifié à $\mathbb{Z}$ et $\mathrm{Im}(\theta)$ est un sous-groupe de $\mathbb{Z}$.*
   Pour $n \geq 1$, on a pour tout $\varphi \in \mathrm{Hom}_{gr}\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, \mathbb{Z}\right)$:

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

dans $\mathbb{Z}$, *donc* $\alpha = 0$.
Pour $n = 0$, *tout entier relatif* α *définit un unique morphisme de groupes* $\varphi : k \in \mathbb{Z} \mapsto k\alpha \in \mathbb{Z}$.
On a donc :

$$\mathrm{Hom}_{gr}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \mathbb{Z}\right) \backsimeq \begin{cases} \mathbb{Z} \text{ si } n = 0 \\ \{0\} \text{ si } n \geq 1 \end{cases}$$

(b) *Pour* $m \geq 1$, *on a pour tout* $\varphi \in \mathrm{Hom}_{gr}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \frac{\mathbb{Z}}{m\mathbb{Z}}\right)$, $m\alpha = \widehat{0}$ *(théorème de Lagrange) et :*

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

donc l'ordre de α *dans* $\frac{\mathbb{Z}}{m\mathbb{Z}}$ *est un diviseur de* n *et* m *et conséquence de leur* pgcd $\delta \geq 1$.
On a donc :

$$\mathrm{Im}\left(\theta\right) \subset H = \left\{\alpha \in \frac{\mathbb{Z}}{m\mathbb{Z}} \text{ d'ordre divisant } \delta\right\}$$

Réciproquement pour tout élément α *de* H, *le morphisme de groupes :*

$$\begin{array}{rccc} \varphi : & \mathbb{Z} & \to & \dfrac{\mathbb{Z}}{m\mathbb{Z}} \\ & k & \mapsto & k\alpha \end{array}$$

est tel que $n\mathbb{Z} \subset \ker\left(\varphi\right)$ $\left(n\alpha = \frac{n}{\delta}\delta\alpha = \widehat{0}\right)$ *et en conséquence il induit le morphisme de groupes :*

$$\begin{array}{rccc} \widehat{\varphi} : & \dfrac{\mathbb{Z}}{n\mathbb{Z}} & \to & \dfrac{\mathbb{Z}}{m\mathbb{Z}} \\ & \overline{k} & \mapsto & k\alpha \end{array}$$

ce qui nous donne $\alpha = \widehat{\varphi}\left(\overline{1}\right) = \theta\left(\widehat{\varphi}\right) \in \mathrm{Im}\left(\theta\right)$.
On a donc $\mathrm{Im}\left(\theta\right) = H$ *qui est l'unique sous-groupe d'ordre* δ *de* $\frac{\mathbb{Z}}{m\mathbb{Z}}$, *à savoir le groupe cyclique d'ordre* $\delta = n \wedge m$ *engendré par* $\widehat{\frac{m}{\delta}}$.
On a donc :

$$\mathrm{Hom}_{gr}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \frac{\mathbb{Z}}{m\mathbb{Z}}\right) \backsimeq \left\langle\widehat{\frac{m}{\delta}}\right\rangle \backsimeq \frac{\mathbb{Z}}{\left(n \wedge m\right)\mathbb{Z}}$$

Pour $n = 0$, *on a* $\delta = m$ *et* $\mathrm{Im}\left(\theta\right) = \frac{\mathbb{Z}}{m\mathbb{Z}}$.
Pour $n = m$, *on a* $\mathrm{Hom}_{gr}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \frac{\mathbb{Z}}{n\mathbb{Z}}\right) \backsimeq \frac{\mathbb{Z}}{n\mathbb{Z}}$ *et* $\mathrm{Aut}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) \backsimeq \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$, *où* $\mathrm{Aut}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)$ *est le groupe des automorphismes du groupe additif* $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

2. *Un morphisme d'anneaux* $\varphi : \frac{\mathbb{Z}}{n\mathbb{Z}} \to \frac{\mathbb{Z}}{m\mathbb{Z}}$ *étant aussi un morphisme de groupes, on a* $\mathrm{Hom}_{Ann}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \frac{\mathbb{Z}}{m\mathbb{Z}}\right) \subset \mathrm{Hom}_{gr}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \frac{\mathbb{Z}}{m\mathbb{Z}}\right)$.

(a) *Pour* $n = m = 0$, *l'application* $\varphi : k \mapsto ka$ *est un morphisme d'anneaux si, et seulement si,* $a = \varphi\left(1\right) = 1$, *donc :*

$$\mathrm{Hom}_{Ann}\left(\mathbb{Z}, \mathbb{Z}\right) = \{Id\}$$

(b) Pour $n \in \mathbb{N}^* \setminus \{1\}$ ($\dfrac{\mathbb{Z}}{1 \cdot \mathbb{Z}}$ n'est pas un anneau) et $m = 0$, on a $\mathrm{Hom}_{Ann}\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, \mathbb{Z}\right) = \emptyset$ (l'endomorphisme nul n'est pas un morphisme d'anneaux).

(c) Pour $n = 0$ et $m \in \mathbb{N}^* \setminus \{1\}$, l'application $\varphi : k \mapsto k\alpha$ est un morphisme d'anneaux si, et seulement si, $\alpha = \varphi(1) = \widehat{1}$, donc :

$$\mathrm{Hom}_{Ann}\left(\mathbb{Z}, \frac{\mathbb{Z}}{m\mathbb{Z}}\right) = \{\pi_m\}$$

(d) Pour n et m sont non nuls de pgcd *δ et pour un morphisme d'anneaux $\varphi : \overline{k} \mapsto k\alpha$, on a $\alpha = \varphi\left(\overline{1}\right) = \widehat{1}$ qui est d'ordre m divisant δ, donc $\delta = m$ et m divise n. Dans ce cas, on a $\varphi\left(\overline{k}\right) = k\widehat{1} = \widehat{k}$, ce qui signifie qu'il y a un seul morphisme d'anneaux de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ dans $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$.*
On a donc :

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

Le fait que $\mathrm{Aut}\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)$ est isomorphe à isomorphe à $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$ peut aussi se montrer comme suit.

Lemme 1.1 *Pour tout $x \in \left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$ l'application $\sigma(x)$ définie sur $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ par :*

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

est un automorphisme du groupe additif $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

Démonstration. Pour y, z dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$, on a :

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

c'est-à-dire que $\sigma(x)$ est un morphisme de groupes additifs.

Si $y \in \ker(\sigma(x))$, alors $xy = \overline{0}$ et $y = x^{-1}xy = \overline{0}$, c'est-à-dire que $\sigma(x)$ est injectif et donc bijectif puisque $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est fini. On a donc bien $\sigma(x) \in \mathrm{Aut}\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)$. ∎

Théorème 1.4 *L'application σ réalise un isomorphisme de $\left(\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}, \cdot\right)$ sur $\left(\mathrm{Aut}\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right), \circ\right)$.*

Démonstration. Pour x, x' dans $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$ et y dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$, on a :

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

On a donc $\sigma(xx') = \sigma(x) \circ \sigma(x')$ et σ est un morphisme de groupes.

Si $\sigma(x) = I_d$, on a $\sigma(x)\left(\overline{1}\right) = \overline{1}$, soit $x = x\overline{1} = \overline{1}$, donc σ est injective.

Si $u \in \mathrm{Aut}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)$ et $\overline{k} = u\left(\overline{1}\right)$, alors pour tout $\overline{j} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$, on a :

$$u\left(\overline{j}\right) = u\left(j\overline{1}\right) = ju\left(\overline{1}\right) = j\overline{k} = \overline{j}\overline{k} = \sigma\left(\overline{k}\right)\overline{j}$$

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

On déduit du théorème précédent que :

$$\mathrm{card}\left(\mathrm{Aut}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)\right) = \mathrm{card}\left(\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}\right) = \varphi(n)$$

Comme $\mathrm{Hom}_{Ann}\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \frac{\mathbb{Z}}{n\mathbb{Z}}\right) = \{Id\}$, on a un seul automorphisme d'anneaux.

Exercice 1.7 *Soit $p \geq 2$ un nombre premier. Quels sont les sous-groupes de $\frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}$.*

Solution 1.7 *Pour p premier, $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps et $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$ est un $\frac{\mathbb{Z}}{p\mathbb{Z}}$-espace vectoriel de de dimension 2.*

On remarque alors que les sous-groupes de $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$ sont ses sous-espaces vectoriels.

En effet un sous-espace vectoriel est un sous-groupe et pour tout sous-groupe H de $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$, on a pour tout $(x, y) \in H$ et tout $\overline{k} \in \frac{\mathbb{Z}}{p\mathbb{Z}}$:

$$\overline{k}(x, y) = \pm \sum (x, y) \in H$$

Les possibilités sont donc $H = \left\{\overline{0}\right\}$, $H = \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$ ou $\dim(H) = 1$, soit $H = \frac{\mathbb{Z}}{p\mathbb{Z}}(x, y)$ avec $(x, y) \neq \left(\overline{0}, \overline{0}\right)$.

Pour $x \neq \overline{0}$, on a $H = \frac{\mathbb{Z}}{p\mathbb{Z}}(1, z)$, ce qui donne p droites possibles et pour $x = 0$, on a $H = \frac{\mathbb{Z}}{p\mathbb{Z}}(0, 1)$, soit une droite.

On a donc au total $p + 3$ sous groupes possibles.

1.2 Le groupe multiplicatif $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$, fonction indicatrice d'Euler

Pour $n \geq 2$, on note $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$ le groupe multiplicatif des éléments inversibles de $\frac{\mathbb{Z}}{n\mathbb{Z}}$, c'est-à-dire l'ensemble des éléments $\overline{a}$ de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ pour lesquels il existe $\overline{b}$ dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ tel que $\overline{a}\overline{b} = \overline{1}$ (on vérifie facilement que cet ensemble est un groupe multiplicatif).

Pour $n=0$, on a $\mathbb{Z}^{\times}=\{-1,1\}$ et pour $n=1$, $\dfrac{\mathbb{Z}}{1\cdot\mathbb{Z}}=\left\{\overline{0}\right\}$ n'est pas un anneau.
Du théorème de Bézout, on déduit le résultat suivant.

Théorème 1.5 *Soit a un entier relatif. Les propriétés suivantes sont équivalentes :*

1. *$\overline{a}$ est inversible dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$;*
2. *a est premier avec n ;*
3. *$\overline{a}$ est un générateur du groupe cyclique $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}},+\right)$.*

Démonstration. Dire que $\overline{a}$ est inversible dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ équivaut à dire qu'il existe $\overline{b}$ dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ tel que $\overline{a}\overline{b}=\overline{1}$, ce qui est encore équivalent à dire qu'il existe b,q dans $\mathbb{Z}$ tels que $ab+qn=1$ et revient à dire que a et n sont premiers entre eux (théorème de Bézout).

En traduisant le fait que $\overline{a}$ est inversible dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ par l'existence d'un entier relatif b tel que $\overline{a}\overline{b}=b\overline{a}=\overline{1}$, on déduit que cela équivaut à dire que $\overline{1}$ est dans le groupe engendré par $\overline{a}$ et donc que ce groupe est $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$. ■

Exercice 1.8 *Montrer que, pour tout entier $n\geq 2$, un élément de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}\setminus\left\{\overline{0}\right\}$ est soit inversible, soit un diviseur de $\overline{0}$.*

Solution 1.8 *Ce résultat est en fait valable pour tout anneau $\mathbb{A}$ commutatif unitaire qui est fini (voir l'exercice* **??***).*
On peut aussi le montrer dans le cas particulier de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.
Soit $\overline{a}\in\dfrac{\mathbb{Z}}{n\mathbb{Z}}\setminus\left\{\overline{0}\right\}$ avec a compris entre 1 et $n-1$.
Si a est premier avec n, $\overline{a}$ est alors inversible, sinon le pgcd *δ de a et n est supérieur ou égal à 2 et $\overline{a}\dfrac{\overline{n}}{\delta}=\dfrac{\overline{a}}{\delta}\overline{n}=\overline{0}$ avec $\dfrac{\overline{n}}{\delta}\neq\overline{0}$ puisque $1\leq\dfrac{n}{\delta}\leq n-1$.*

Définition 1.2 *On appelle fonction indicatrice d'Euler la fonction 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 $\varphi(1)=1$).*

Le théorème précédent nous dit que pour tout entier $n\geq 2$, $\varphi(n)$ est le nombre de générateurs du groupe cyclique $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}},+\right)$ (ou de n'importe quel groupe cyclique d'ordre n) ou encore que c'est le nombre d'éléments inversibles de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

Exemple 1.1 *Si $p\geq 2$ est un nombre premier, tout entier compris entre 1 et $p-1$ est alors premier avec p, donc $\varphi(p)=p-1$.*

Du théorème de Lagrange, on déduit immédiatement le résultat suivant.

Théorème 1.6 (Euler) *Pour tout entier relatif a premier avec n, on a $a^{\varphi(n)}\equiv 1\ (n)$.*

Démonstration. Si a est premier avec n, alors $\overline{a}$ appartient à $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$ qui est un groupe d'ordre $\varphi(n)$ et en conséquence son ordre divise $\varphi(n)$ (théorème de Lagrange), ce qui entraîne $\overline{a}^{\varphi(n)} = \overline{1}$, ou encore $a^{\varphi(n)} \equiv 1\ (n)$. ■

Le théorème précédent nous dit que, pour a est premier avec n, l'inverse de $\overline{a}$ est $\overline{a}^{\varphi(n)-1}$.

Exercice 1.9 *Montrer le théorème d'Euler en utilisant le fait que, pour tout entier relatif a premier avec n, l'application $\tau_a : x \mapsto \overline{a}x$ est une bijection de $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$ sur lui même.*

Solution 1.9 *Pour a premier avec n, on a $\overline{a} \in \left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$ et l'application $\tau_a : x \mapsto \overline{a}x$ est bijective de $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$ sur lui même d'inverse $\tau_a^{-1} : x \mapsto (\overline{a})^{-1} x$.*
On en déduit alors que :

$$\prod_{x \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}} x = \prod_{x \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}} (\overline{a}x) = \overline{a}^{\varphi(n)} \prod_{x \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}} x$$

et en conséquence, $\overline{a}^{\varphi(n)} = \overline{1}$.

Pour p premier, on a $\varphi(p) = p - 1$ et le théorème d'Euler devient le petit théorème de Fermat.

Théorème 1.7 (Fermat) *Soit p un entier naturel premier. Pour tout entier relatif a premier avec p, on a $a^{p-1} \equiv 1\ (p)$ et pour tout entier relatif a, on a $a^p \equiv a\ (p)$.*

Exercice 1.10 *Montrer que pour tout entier $n \geq 3$, $\varphi(n)$ est un entier pair.*

Solution 1.10 *Pour $n \geq 3$, on a $\overline{(-1)} \neq \overline{1}$ et $\overline{(-1)}^2 = \overline{(-1)^2} = \overline{1}$, donc $\overline{(-1)}$ est d'ordre 2 qui va diviser l'ordre du groupe $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$, soit $\varphi(n)$.*
Pour $n = 2$, on a $\dfrac{\mathbb{Z}}{2\mathbb{Z}} = \{\overline{0}, \overline{1}\}$, $\left(\dfrac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\times} = \{\overline{1}\}$ et $\varphi(2) = 1$.

Le théorème de Fermat peut être utilisé pour résoudre des exercices élémentaires d'arithmétique.

Exercice 1.11 *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.

Solution 1.11 *Si p divise a, il divise aussi a^b et le reste cherché est nul.*
On suppose donc que p ne divise pas a.
Tout d'abord, en vue de diminuer b, 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 $a^{p-1} \equiv 1\ (p)$ puisque p ne divise pas a, ce qui donne $a^b \equiv a^r\ (p)$.
Ensuite, en vue de diminuer a, on effectue la division euclidienne de a par p, soit $a = q'p + s \equiv s\ (p)$ avec $1 \leq s \leq p-1$ et $a^b \equiv s^r\ (p)$.
Le reste cherché est donc celui de la division de s^r par p avec $1 \leq s \leq p-1$ et $0 \leq r \leq p-2$.
Pour $m = 115^{2013}$ et $p = 11$, on a $2013 \equiv 3\ (10)$ et $115 \equiv 5\ (11)$, donc $115^{2013} \equiv 5^3\ (11)$ et avec $5^2 \equiv 3$, $5^3 \equiv 4$ modulo 11, on déduit que $115^{2013} \equiv 4$ modulo 11, ce qui signifie que 4 est le reste dans la division euclidienne de 115^{2013} par 11.

Exercice 1.12 *Soit $p \geq 7$ un nombre premier. Montrer que $p^4 - 1$ est divisible par 240.*

Solution 1.12 *Comme $240 = 2^4 \cdot 3 \cdot 5$, il suffit de montrer que $p^4 - 1$ est multiple de 2^4, 3 et 5. Comme p est premier différent de 3 et 5, le petit théorème de Fermat nous dit que $p^4 - 1$ est congru à 0 modulo 5 et p^3 congru à p, modulo 3, donc p^4 est congru à p^2 qui est lui même congru à 1 modulo 3. L'entier $p^4 - 1$ est donc multiple de 3 et 5.*
D'autre part, on a $p^4 - 1 = (p-1)(p^3 + p^2 + p + 1)$ avec p congru à 1 ou 3 modulo 4, puisque p est premier différent de 2.
Si p est congru à 1 modulo 4, alors $p - 1$ est congru à 0 modulo 4, donc multiple de 4, et $p^3 + p^2 + p + 1$ est congru à 0, modulo 4, donc lui aussi multiple de 4 et $p^4 - 1$ est multiple de 16.
Si p est congru à 3 modulo 4, il s'écrit alors $p = 3 + 4q$ avec $q \geq 1$ et :

$$p^4 - 1 = 432q + 864q^2 + 768q^3 + 256q^4 + 80$$

chaque coefficient de ce polynôme étant multiple de 16, il en résulte que $p^4 - 1$ est multiple de 16. D'où le résultat annoncé.

Exercice 1.13 *Soit $n \geq 2$. Montrer que $n^5 - n$ est divisible par 30.*

Solution 1.13 *Comme $n(n-1)$ est pair et $n(n-1)(n+1)$ est multiple de 3 (n est congru à $-1, 0$ ou 1 modulo 3) $m = n^5 - n = n(n-1)(n+1)(n^2+1)$ est divisible par 2 et 3, donc par 6. Le théorème de Fermat nous dit que $m = n^5 - n$ est divisible par 5, donc m est divisible par $30 = 6 \times 5$ puisque 6 est premier avec 5.*

Exercice 1.14 *Soient a, b des entiers relatifs et $(n_k)_{1 \leq k \leq r}$ une suite finie de $r \geq 2$ entiers naturels non nuls.*

1. *Monter que si $a \equiv b \bmod (n_k)$ pour tout k compris entre 1 et r, alors $a \equiv b \bmod (n_1 \vee \cdots \vee n_r)$.*
   Dans le cas où les n_k sont deux à deux premiers entre eux, on a $a \equiv b \bmod \left(\prod_{k=1}^{r} n_k\right)$.
2. *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, voir le paragraphe 1.7).*

Solution 1.14

1. *Si $a \equiv b \bmod (n_k)$ pour tout k compris entre 1 et r, $b - a$ est alors un multiple commun aux n_k et en conséquence de $n_1 \vee \cdots \vee n_r$, 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 $n_1 \vee \cdots \vee n_r = \prod_{k=1}^{r} n_k$ (lemme 1.2).
2. *L'entier $n = 561$ est divisible par 3 (puisque $1+6+5 = 12$) et par 11 (puisque $1-6+5 = 0$).*
   Précisément, on a la décomposition en facteurs premiers $561 = 3 \cdot 11 \cdot 17 = \prod_{k=1}^{3} p_k$.
   Dire que a est premier avec 561 équivaut à dire qu'il est 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 $a^{560} \equiv 1 \ (561)$.

Dans le cas où n est premier tous les éléments de $\dfrac{\mathbb{Z}}{n\mathbb{Z}} \setminus \{\overline{0}\}$ sont inversibles et en conséquence $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps.

En fait on a le résultat plus précis suivant.

Théorème 1.8 *Pour tout entier $n \geq 2$, les assertions suivantes sont équivalentes : :*

1. *n est premier ;*
2. *pour tout entier naturel non nul α, on a $\varphi(n^\alpha) = (n-1)\, n^{\alpha-1}$;*
3. *$\varphi(n) = n-1$;*
4. *$\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps ;*
5. *$\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est un intègre ;*
6. *$(n-1)! \equiv -1 \ (n)$ (théorème de Wilson) ;*
7. *$(n-2)! \equiv 1 \ (n)$;*
8. *pour tout k compris entre 1 et n, on a $(n-k)!\,(k-1)! \equiv (-1)^k \pmod{n}$;*
9. *pour tout entier k compris entre 1 et $n-1$, on a $\binom{n}{k} \equiv 0 \pmod{n}$;*
10. *pour tout entier k compris entre 1 et $n-1$, on a $\binom{n}{k} \equiv 0 \pmod{n}$ et $\binom{n-1}{k} \equiv (-1)^k \pmod{n}$.*

Démonstration.

(1) $\Rightarrow$ (2) Pour n premier, un entier k compris entre 1 et n^α n'est pas premier avec n^α si, et seulement si, il est divisible par n, ce qui équivaut à dire qu'il existe un entier q compris entre 1 et $n^{\alpha-1}$ tel que $k = qn$ et cela nous donne $n^{\alpha-1}$ possibilités. Il en résulte que :

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

(2) $\Rightarrow$ (3) Il suffit de prendre $\alpha = 1$.

(3) $\Rightarrow$ (4) Si $\varphi(n) = n-1$, on a alors $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times = \dfrac{\mathbb{Z}}{n\mathbb{Z}} \setminus \{\overline{0}\}$ et $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps.

(4) $\Rightarrow$ (5) Résulte du fait qu'un corps est en particulier un anneau intègre.

(5) $\Rightarrow$ (1) Supposons que $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ soit intègre. Si d est un diviseur de n différent de n dans $\mathbb{N}$, il existe alors un entier q compris entre 2 et n tel que $n = qd$ et dans l'anneau intègre $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ on a $\overline{q}\overline{d} = \overline{0}$ avec $\overline{d} \neq \overline{0}$, ce qui impose $\overline{q} = \overline{0}$, soit $q = n$ et $d = 1$. L'entier n est donc premier.

(1) $\Rightarrow$ (6) Si n est premier, l'anneau $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est alors un corps et tout élément $\overline{k}$ de $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$ est racine du polynôme $X^{n-1} - \overline{1}$, donc $X^{n-1} - \overline{1} = \prod_{k=1}^{n-1} \left(X - \overline{k}\right)$ dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}[X]$ et en évaluant ce polynôme en $\overline{0}$, il vient $-\overline{1} = \prod_{k=1}^{n-1} \left(-\overline{k}\right) = (-1)^{n-1}\, \overline{(n-1)!} = \overline{(n-1)!}$ (pour $n = 2$, on a $(-1)^{n-1} = -\overline{1} = \overline{1}$ et $n \geq 3$ premier est impair, donc $(-1)^{n-1} = \overline{1}$).

(6) $\Rightarrow$ (1) Si $n \geq 2$ est tel que $\overline{(n-1)!} = -\overline{1}$ dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$, alors tout diviseur d de n compris entre 1 et $n-1$ divisant $(n-1)! = -1 + kn$ va diviser -1, ce qui impose $d = 1$ et l'entier n est premier.

(6) $\Leftrightarrow$ (7) Pour $n \geq 2$, on a $(n-1)! = (n-1)(n-2)! \equiv -(n-2)!$ modulo n.

(6) $\Leftrightarrow$ (8) L'implication (8) $\Rightarrow$ (6) est évidente (prendre $k = 1$).

Supposons que $(n-1)! \equiv -1 \ (n)$. Dans ce cas, n est premier.

Si $n = 2$, on a alors, pour $k = 1$ et $k = 2$:

$$(n-k)!\,(k-1)! = 1 \equiv (-1)^k \pmod 2$$

Pour $n \geq 3$ qui est premier impair, on procède par récurrence finie sur k.

Le résultat est acquis pour $k = 1$ et pour $k = n$ (puisque $(-1)^n = -1$).

En supposant le résultat acquis pour $k \in \{1, \cdots, n-2\}$, on a :

$$(n-(k+1))!k! = \frac{k}{n-k}(n-k)!\,(k-1)!$$

avec $\overline{n-k} = -\overline{k}$ qui est inversible dans le corps $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ puisque $\overline{k} \neq \overline{0}$, ce qui nous donne l'égalité dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$:

$$\overline{(n-(k+1))!k!} = \frac{\overline{k}}{\overline{-k}}\overline{(n-k)!\,(k-1)!} = -\overline{(-1)^k} = \overline{(-1)^{k+1}}$$

soit $(n-(k+1))!k! \equiv (-1)^{k+1} \pmod n$.

(1) $\Rightarrow$ (9) Si $n \geq 2$ est premier, comme il divise $n! = k!\,(n-k)!\binom{n}{k}$ et est premier avec $k!\,(n-k)!$ (sinon il diviserait ce produit et donc l'un des entiers j compris entre 1 et $n-1$, ce qui est impossible), il divise $\binom{n}{k}$ (théorème de Gauss), ce qui revient à dire que $\binom{n}{k} \equiv 0 \pmod n$.

(9) $\Rightarrow$ (10) Supposons que $\binom{n}{k} \equiv 0 \pmod n$ pour tout entier k compris entre 1 et $n-1$.

Pour tout entier k compris entre 1 et $n-1$, on a :

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

(triangle de Pascal), donc $\binom{n-1}{k} \equiv -\binom{n-1}{k-1}$ modulo p et par récurrence finie sur k compris entre 0 et $n-1$, on déduit que $\binom{n-1}{k}$ est congru à $(-1)^k$ modulo n. En effet, pour $k = 0$, on a $\binom{n-1}{0} = 1 \equiv (-1)^0$ modulo n ; pour $k = 1$, on a $\binom{n-1}{1} = n-1 \equiv -1$ modulo n ; puis en supposant le résultat acquis pour $k-1$ compris entre 0 et $n-2$, on a $\binom{n-1}{k} \equiv -\binom{n-1}{k-1} \equiv -(-1)^{n-1} = (-1)^k$ modulo n.

(10) $\Rightarrow$ (1) Supposons que $\binom{n}{k} \equiv 0 \pmod n$ et $\binom{n-1}{k} \equiv (-1)^k \pmod n$ pour tout entier k compris entre 1 et $n-1$.

Pour tout diviseur k de n compris entre 1 et $n-1$, on a :

$$0 \equiv \binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1} \equiv \frac{n}{k}(-1)^{k-1} \pmod n$$

(pour $k = 1$, on a bien $\binom{n-1}{0} = 1 \equiv (-1)^0$ modulo n), ce qui impose $k = 1$ (sinon n divise $\dfrac{n}{k} \in \{2, \cdots, n-1\}$, ce qui est impossible), donc n est premier. ∎

Remarque 1.1 *L'implication* $(5) \Rightarrow (4)$ *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* $aa' = 1$*.*

Exercice 1.15 *Soit* p *un nombre premier impair.*

1. *Montrer qu'il y a exactement* $\dfrac{p-1}{2}$ *carrés et* $\dfrac{p-1}{2}$ *non carrés dans* $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$.
2. *Montrer que l'ensemble des carrés de* $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ *est l'ensemble des racines du polynôme* $X^{\frac{p-1}{2}} - \overline{1}$ *et que l'ensemble des non carrés de* $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ *est l'ensemble des racines du polynôme* $X^{\frac{p-1}{2}} + \overline{1}$*.*
3. *Montrer que* $-\overline{1}$ *est un carré dans* $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ *si, et seulement si,* p *est congru à* 1 *modulo* 4*. Dans ce cas, donner une racine carrée explicite de* $-\overline{1}$*.*

Solution 1.15 *Pour* $p = 2$, $\left(\dfrac{\mathbb{Z}}{2\mathbb{Z}}\right)^* = \left\{\overline{1}\right\}$ *et* $\overline{1}$ *est le un seul carré.*
Pour $p \geq 3$ *premier, on note* $C_p = \left\{x^2 \mid x \in \left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^*\right\}$ *l'ensemble des carrés de* $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$.

1. *L'ensemble* C_p *est l'image du morphisme de groupes :*

$$\begin{array}{rccc} \varphi_p & \left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^* & \to & \left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \\ & x & \mapsto & x^2 \end{array}$$

et le noyau de ce morphisme est :

$$\ker(\varphi_p) = \left\{x \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \mid (x-\overline{1})(x+\overline{1}) = \overline{0}\right\} = \left\{-\overline{1}, \overline{1}\right\}$$

avec $-\overline{1} \neq \overline{1}$ *dans le corps* $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ *pour* $p \geq 3$ *premier, donc* $C_p = \mathrm{Im}(\varphi_p)$ *est isomorphe à* $\dfrac{\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*}{\left\{-\overline{1}, \overline{1}\right\}}$ *et :*

$$\mathrm{card}(C_p) = \mathrm{card}\left(\frac{\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*}{\left\{-\overline{1}, \overline{1}\right\}}\right) = \frac{p-1}{2}$$

ce qui signifie qu'il y a exactement $\dfrac{p-1}{2}$ *carrés et* $\dfrac{p-1}{2}$ *non carrés dans* $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$.

2. *Si* $y \in C_p$*, il existe alors* $x \in \left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ *tel que* $y = x^2$ *et* $y^{\frac{p-1}{2}} = x^{p-1} = \overline{1}$ *(Fermat ou Lagrange). Donc* C_p *est contenu dans l'ensemble des racines du polynôme* $P(X) = X^{\frac{p-1}{2}} - \overline{1}$ *et comme ce polynôme a au plus* $\dfrac{p-1}{2} = \mathrm{card}(C_p)$ *éléments,* C_p *est l'ensemble de ces racines.*

Si $y \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \setminus C_p$, *on a alors* $y^{\frac{p-1}{2}} \neq \overline{1}$ *et* $\left(y^{\frac{p-1}{2}}\right)^2 = y^{p-1} = \overline{1}$, *donc* $y^{\frac{p-1}{2}} = -\overline{1}$. *Donc* $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \setminus C_p$ *est contenu dans l'ensemble des racines du polynôme* $Q(X) = X^{\frac{p-1}{2}} + \overline{1}$ *et comme ce polynôme a au plus* $\frac{p-1}{2} = \operatorname{card}\left(\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \setminus C_p\right)$ *éléments,* $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \setminus C_p$ *est l'ensemble de ces racines.*

3. *On a :*

$$\left(-\overline{1} \in C_p\right) \Leftrightarrow \left((-1)^{\frac{p-1}{2}}\,\overline{1} = \overline{1}\right) \Leftrightarrow \left(\frac{p-1}{2} \equiv 0 \pmod 2\right)$$
$$\Leftrightarrow (p \equiv 1 \pmod 4)$$

Si $p \geq 3$ *est un nombre premier congru à* 1 *modulo* 4, *il s'écrit* $p = 4q+1$ *avec* $q \geq 1$ *et* $m = \frac{p-1}{2}$ *est un entier pair non nul.*
Tout entier k *compris entre* $m+1 = \frac{p+1}{2}$ *et* $p-1$ *s'écrit* $k = p-j$ *avec* $1 \leq j \leq m = \frac{p-1}{2}$, *donc* $k \equiv -j \bmod p$ *et :*

$$(p-1)! = 1 \cdot 2 \cdot \cdots \cdot m \cdot (m+1) \cdots (p-1)$$
$$\equiv (-1)^m (m!)^2 \equiv (m!)^2 \bmod p$$

puisque m *est pair.*
D'autre part, comme p *est premier, le théorème de Wilson nous dit que* $(p-1)! \equiv -1 \bmod p$, *donc* $(m!)^2 \equiv -1 \bmod (p)$.

1.3 Le théorème chinois

Lemme 1.2 *Soient* $(n_j)_{1 \leq j \leq r}$ *une suite de* $r \geq 2$ *entiers naturels distincts de* 0 *et* 1.

1. *Si les entiers* $n_1, \cdots, n_r$ *sont deux à deux premiers entre eux, leur* ppcm *est alors* $\prod_{j=1}^{r} n_j$.
2. *Si les entiers* $n_1, \cdots, n_r$ *ne sont sont pas deux à deux premiers entre eux, on a alors* $\operatorname{ppcm}(n_1, \cdots, n_r) < \prod_{j=1}^{r} n_j$.

Démonstration.

1. C'est vrai pour $r = 2$ puisque $n_1 \vee n_2 = \frac{n_1 n_2}{n_1 \wedge n_2}$ et supposant le résultat acquis pour $r = 2$, en utilisant l'associativité du ppcm, on a :

$$n_1 \vee \cdots \vee n_{r+1} = (n_1 \vee \cdots \vee n_r) \vee n_{r+1}$$
$$= \left(\prod_{k=1}^{r} n_k\right) \vee n_{r+1} = \prod_{k=1}^{r+1} n_k$$

puisque n_{r+1} qui est premier avec tous les n_k pour k compris entre 1 et r est premier avec leur produit (sinon il existe un diviseur premier p de n_{r+1} et de $\prod_{k=1}^{r} n_k$, donc p divise l'un des n_k pour k compris entre 1 et r, ce qui contredit $n_{r+1} \wedge n_k = 1$).

2. Si $n_1, \cdots, n_r$ ne sont sont pas deux à deux premiers entre eux, il existe alors deux indices $i \neq j$ compris entre 1 et r tels que $n_i \wedge n_j \geq 2$. Quitte à modifier la numérotation, on peut supposer que $(i,j) = (1,2)$. On a alors $n_1 \vee n_2 = \dfrac{n_1 n_2}{n_1 \wedge n_2} < n_1 n_2$ et :

$$\begin{aligned} n_1 \vee \cdots \vee n_r &= (n_1 \vee n_2) \vee (n_3 \vee \cdots \vee n_r) \\ &\leq (n_1 \vee n_2)(n_3 \vee \cdots \vee n_r) < (n_1 n_2)(n_3 \cdot \cdots \cdot n_r) \end{aligned}$$

■

Remarque 1.2 *Le résultat du point 1. du lemme précédent n'est plus valable si on suppose seulement que les n_j sont premiers entre eux dans leur ensemble comme le montre l'exemple suivant :*

$$2 \vee 3 \vee 4 = 12 < 2 \cdot 3 \cdot 4 = 24$$

Pour tout entier $n \geq 2$, on désigne toujours par π_n la surjection canonique de $\mathbb{Z}$ sur $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

Théorème 1.9 (chinois) *Soient $(n_j)_{1 \leq j \leq r}$ une suite de $r \geq 2$ entiers naturels distincts de 0 et 1 et $n = \prod_{j=1}^{r} n_j$.*

Les entiers $n_1, \cdots, n_r$ sont deux à deux premiers entre eux si, et seulement si, les anneaux $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ et $\prod_{j=1}^{r} \dfrac{\mathbb{Z}}{n_j\mathbb{Z}}$ sont isomorphes.
Dans ce cas, l'application :

$$\begin{array}{rccc} \psi : & \dfrac{\mathbb{Z}}{n\mathbb{Z}} & \to & \displaystyle\prod_{j=1}^{r} \frac{\mathbb{Z}}{n_j\mathbb{Z}} \\ & \pi_n(k) & \mapsto & (\pi_1(k), \cdots, \pi_r(k)) \end{array}$$

(où on a noté π_k la surjection canonique π_{n_k}) est un isomorphisme d'anneaux d'inverse :

$$\begin{array}{rccc} \psi^{-1} : & \displaystyle\prod_{j=1}^{r} \frac{\mathbb{Z}}{n_j\mathbb{Z}} & \to & \dfrac{\mathbb{Z}}{n\mathbb{Z}} \\ & (\pi_1(a_1), \cdots, \pi_r(a_r)) & \mapsto & \pi_n\left(\displaystyle\sum_{i=1}^{r} a_i u_i \frac{n}{n_i}\right) \end{array}$$

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

Démonstration. Voir le théorème **??** pour une démonstration plus générale dans le cadre d'un anneau principal.

Le produit cartésien $\displaystyle\prod_{j=1}^{r} \frac{\mathbb{Z}}{n_j\mathbb{Z}}$ est naturellement muni de la structure d'anneau produit.

Supposons les entiers $n_1, \cdots, n_r$ deux à deux premiers entre eux.

L'application :

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

est un morphisme d'anneaux et son noyau est formé des entiers multiples de tous les n_j, donc de leur ppcm $n = \prod_{j=1}^{r} n_j$ puisque ces entiers sont deux à deux premiers entre eux, il se factorise donc en un morphisme d'anneaux injectif :

$$\begin{array}{rccc} \psi : & \dfrac{\mathbb{Z}}{n\mathbb{Z}} & \to & \displaystyle\prod_{j=1}^{r} \frac{\mathbb{Z}}{n_j\mathbb{Z}} \\ & \pi_n(k) & \mapsto & (\pi_1(k), \cdots, \pi_r(k)) \end{array}$$

Ces deux anneaux ayant même cardinal n, l'application ψ réalise en fait un isomorphisme d'anneaux de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sur $\displaystyle\prod_{j=1}^{r} \frac{\mathbb{Z}}{n_j\mathbb{Z}}$.

Si les entiers $n_1, \cdots, n_r$ ne sont pas deux à deux premiers entre eux les groupes additifs $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ et $\displaystyle\prod_{j=1}^{r} \frac{\mathbb{Z}}{n_j\mathbb{Z}}$ ne peuvent être isomorphes puisque $\pi_n(1)$ est d'ordre n dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ et tous les éléments de $\displaystyle\prod_{j=1}^{r} \frac{\mathbb{Z}}{n_j\mathbb{Z}}$ ont un ordre qui divise le ppcm de $n_1, \cdots, n_r$ qui est strictement inférieur à n.

On désigne par $(m_j)_{1\leq j\leq r}$ la suite d'entiers définie par :

$$m_j = \frac{n}{n_j} = \prod_{\substack{i=1 \\ i\neq j}}^{r} n_i \ \ (1 \leq j \leq r)$$

Ces entiers sont premiers entre eux dans leur ensemble (sinon, il existe un nombre premier p qui divise tous les m_j, divisant $m_1 = \prod_{i=2}^{r} n_i$, il divise un n_i pour $2 \leq i \leq r$, mais divisant m_i, il divise un n_k pour $1 \leq k \neq i \leq r$, ce qui contredit le fait que n_i et n_k sont premiers entre eux) et le théorème de Bézout nous dit qu'il existe une suite $(u_j)_{1\leq j\leq r}$ d'entiers relatifs telle que $\displaystyle\sum_{j=1}^{r} u_j m_j = 1$.

Pour tout j compris entre 1 et r, on a :

$$\pi_j(1) = \pi_j\left(\sum_{i=1}^{r} u_i m_i\right) = \pi_j(u_j)\,\pi_j(m_j)$$

(ce qui signifie que $\pi_j(m_j)$ est inversible dans $\mathbb{Z}_{n_j}$ d'inverse $\pi_j(u_j)$) et posant :

$$k = \sum_{i=1}^{r} a_i u_i m_i$$

on a $\pi_j(k) = \pi_j(a_j)\,\pi_j(u_j)\,\pi_j(m_j) = \pi_j(a_j)$, donc :

$$\psi(\pi_n(k)) = (\pi_1(k), \cdots, \pi_r(k)) = (\pi_1(a_1), \cdots, \pi_r(a_r))$$

L'inverse de ψ est donc défini par :

$$\psi^{-1}(\pi_1(a_1), \cdots, \pi_r(a_r)) = \pi_n\left(\sum_{i=1}^{r} a_i u_i m_i\right)$$

■

Exercice 1.16 *Soient $n \geq 2$ et $m \geq 2$ deux entiers. Montrer que les anneaux $\dfrac{\mathbb{Z}}{n\mathbb{Z}} \times \dfrac{\mathbb{Z}}{m\mathbb{Z}}$ et $\dfrac{\mathbb{Z}}{(n \wedge m)\,\mathbb{Z}} \times \dfrac{\mathbb{Z}}{(n \vee m)\,\mathbb{Z}}$ sont isomorphes.*

Solution 1.16 *Si n et m sont premiers entre eux, le théorème chinois nous dit que l'anneau $\dfrac{\mathbb{Z}}{n\mathbb{Z}} \times \dfrac{\mathbb{Z}}{m\mathbb{Z}}$ est isomorphe à $\dfrac{\mathbb{Z}}{nm\mathbb{Z}}$ qui est bien isomorphe à $\dfrac{\mathbb{Z}}{(n \wedge m)\,\mathbb{Z}} \times \dfrac{\mathbb{Z}}{(n \vee m)\,\mathbb{Z}}$ puisque $\dfrac{\mathbb{Z}}{(n \wedge m)\,\mathbb{Z}} = \dfrac{\mathbb{Z}}{\mathbb{Z}} = \{\overline{0}\}$ et $n \vee m = nm$.*
Pour $\delta = n \wedge m \geq 2$, on écrit les décompositions en facteurs premiers de n et m sous la forme :

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=k+1}^{r} p_i^{\alpha_i},\ m = \prod_{i=1}^{k} p_i^{\beta_i} \prod_{i=k+1}^{r} p_i^{\beta_i}$$

où les facteurs premiers p_i ont été regroupés de sorte que $\alpha_i > \beta_i$ pour $1 \leq i \leq k$ et $\alpha_i \leq \beta_i$ pour $k+1 \leq i \leq r$, les exposants α_i, β_i étant positifs ou nuls (si l'une des conditions $\alpha_i > \beta_i$ ou $\alpha_i \leq \beta_i$ n'est jamais vérifiée, alors le produit correspondant vaut 1).
Avec ces écritures, on a :

$$\delta = n \wedge m = \prod_{i=1}^{k} p_i^{\beta_i} \prod_{i=k+1}^{r} p_i^{\alpha_i}$$

$$\mu = n \vee m = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=k+1}^{r} p_i^{\beta_i}$$

et le théorème chinois nous donne les isomorphismes d'anneaux :

$$\begin{aligned}
&\frac{\mathbb{Z}}{\delta\mathbb{Z}} \times \frac{\mathbb{Z}}{\mu\mathbb{Z}} \overset{\sim}{\to} \prod_{i=1}^{k} \frac{\mathbb{Z}}{p_i^{\beta_i}\mathbb{Z}} \times \prod_{i=k+1}^{r} \frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}} \times \prod_{i=1}^{k} \frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}} \times \prod_{i=k+1}^{r} \frac{\mathbb{Z}}{p_i^{\beta_i}\mathbb{Z}} \\
&\overset{\sim}{\to} \prod_{i=1}^{k} \frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}} \times \prod_{i=k+1}^{r} \frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}} \times \prod_{i=1}^{k} \frac{\mathbb{Z}}{p_i^{\beta_i}\mathbb{Z}} \times \prod_{i=k+1}^{r} \frac{\mathbb{Z}}{p_i^{\beta_i}\mathbb{Z}} \\
&\overset{\sim}{\to} \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}
\end{aligned}$$

Le calcul de $\varphi(n)$ pour $n \geq 2$ peut se faire en utilisant la décomposition de n en facteurs premiers grâce au théorème chinois.

Lemme 1.3 *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 $\mathbb{B}^\times$.*

Démonstration. 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 $\mathbb{B}^\times$. ∎

En utilisant la décomposition en facteurs premiers $n=\prod_{j=1}^{r}p_j^{\alpha_j}$ d'un entier $n\geq 2$, le théorème chinois nous dit qu'on a un isomorphisme d'anneaux :

$$\frac{\mathbb{Z}}{n\mathbb{Z}}\overset{\sim}{\to}\prod_{j=1}^{r}\frac{\mathbb{Z}}{p_j^{\alpha_j}\mathbb{Z}}$$

qui induit un isomorphisme de groupes :

$$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}\overset{\sim}{\to}\left(\prod_{j=1}^{r}\frac{\mathbb{Z}}{p_j^{\alpha_j}\mathbb{Z}}\right)^{\times}=\prod_{j=1}^{r}\left(\frac{\mathbb{Z}}{p_j^{\alpha_j}\mathbb{Z}}\right)^{\times}$$

et prenant les cardinaux, on en déduit que :

$$\varphi(n)=\prod_{i=1}^{r}\varphi\left(p_j^{\alpha_j}\right)$$

Le calcul de $\varphi(n)$ est alors ramené à celui de $\varphi(p^{\alpha})$ où p est un nombre premier et α un entier naturel non nul.

Lemme 1.4 *Pour tout nombre premier p et tout entier naturel non nul α, on a :*

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

Démonstration. 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 :

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

■

Théorème 1.10 *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 :*

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

Avec ce résultat on retrouve le fait que, pour tout $n\geq 3$ l'entier $\varphi(n)$ est pair. En effet, pour $n=2^{\alpha}$ avec $\alpha\geq 2$, on a $\varphi(n)=2^{\alpha-1}$ qui est pair et pour $n=2^{\alpha}\prod_{i=1}^{r}p_i^{\alpha_i}=p_1^{\alpha_1}m$ avec $\alpha\geq 0$, $r\geq 1$, tous les p_i étant premiers impairs, on a $\varphi(n)=(p_1-1)\,p_i^{\alpha_1-1}\varphi(m)$ qui est pair.

Exercice 1.17 *Montrer que pour tout diviseur positif d d'un entier $n\geq 2$, $\varphi(d)$ divise $\varphi(n)$.*

Solution 1.17 *Pour $d=1$ c'est clair et pour $d\geq 2$, on a les décompositions en facteurs premiers $n=\prod_{i=1}^{r}p_i^{\alpha_i}$ et $d=\prod_{i=1}^{s}p_i^{\beta_i}$ avec $1\leq\beta_i\leq\alpha_i$ pour $1\leq i\leq s\leq r$, donc :*

$$\frac{\varphi(n)}{\varphi(d)}=\prod_{i=1}^{s}p_i^{\alpha_i-\beta_i}\prod_{i=s+1}^{r}p_i^{\alpha_i-1}(p_i-1)\in\mathbb{N}^*$$

De la définition, on déduit que $\varphi(n)$ est compris entre 1 et $n-1$. Ce résultat peut être affiné comme suit.

Théorème 1.11 *Pour tout entier $n \geq 2$, on a :*

$$\sqrt{n} - 1 < \varphi(n) \leq n - 1$$

Démonstration. L'inégalité $\varphi(n) \leq n-1$ est une conséquence immédiate de la définition. Pour montrer l'autre inégalité on procède en plusieurs étapes.

On s'intéresse d'abord aux valeurs de n comprises entre 2 et 7. Pour ces valeurs, on a $\varphi(2) = 1 > \sqrt{2} - 1$, $\varphi(5) = 4 > \sqrt{5} - 1$ et $\varphi(3) = \varphi(4) = \varphi(6) = 2 > \sqrt{k} - 1$ pour $k = 3, 4, 6$.

On s'intéresse ensuite aux entiers de la forme $n = \prod_{i=1}^{r} p_i$ avec $3 \leq p_1 < \cdots < p_r$ premiers. Dans ce cas, on a :

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

Pour $p \geq 3$, on a $p(p-3) \geq 0$, soit $p^2 - 3p + 1 > 0$ ou encore $(p-1)^2 p$, c'est-à-dire $p - 1 > \sqrt{p}$. On en déduit donc que $\varphi(n) > \sqrt{n}$.

Considérons le cas de n impair supérieur ou égal à 7. Il s'écrit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec $3 \leq p_1 < \cdots < p_r$ premiers et $\alpha_i \geq 1$ pour tout i compris entre 1 et r. En posant $m = \prod_{i=1}^{r} p_i$, on a :

$$\varphi(n) = \frac{n}{m} \prod_{i=1}^{r} \varphi(p_i) = \frac{n}{m} \varphi(m)$$

et :

$$\frac{\varphi(n)}{\sqrt{n}} = \sqrt{\frac{n}{m}} \frac{\varphi(m)}{\sqrt{m}} \geq \frac{\varphi(m)}{\sqrt{m}} > 1$$

ce qui donne $\varphi(n) > \sqrt{n}$.

Pour $n = 2^\alpha$ avec $\alpha \geq 3$, on a :

$$\frac{\varphi(n)}{\sqrt{n}} = 2^{\frac{\alpha}{2} - 1} = \left(\sqrt{2}\right)^{\alpha - 2} > 1$$

et $\varphi(n) > \sqrt{n}$.

Pour $n = 2^\alpha 3^\beta$ avec $\alpha \geq 1$, $\beta \geq 1$ et $(\alpha, \beta) \neq (1, 1)$, on a :

$$\frac{\varphi(n)}{\sqrt{n}} = 2^{\frac{\alpha}{2}} 3^{\frac{\beta}{2} - 1} = \left(\sqrt{2}\right)^{\alpha} \left(\sqrt{3}\right)^{\beta - 2} > 1$$

(pour $\beta \geq 2$ il n'y a pas de problème et pour $\beta = 1$ on a $\alpha \geq 2$ et $\left(\sqrt{2}\right)^{\alpha} \left(\sqrt{3}\right)^{-1} \geq \dfrac{2}{\sqrt{3}} > 1$), ce qui donne $\varphi(n) > \sqrt{n}$.

Enfin, si n est pair supérieur ou égal à 7, il s'écrit $n = 2^{\alpha_1} \prod_{i=2}^{r} p_i^{\alpha_i}$ avec $3 \leq p_2 < \cdots < p_r$ premiers et $\alpha_i \geq 1$ pour tout i compris entre 1 et r. En posant $m = 2 \prod_{i=2}^{r} p_i$, on a : :

$$\frac{\varphi(n)}{\sqrt{n}} = \sqrt{\frac{n}{m}} \frac{\varphi(m)}{\sqrt{m}} \geq \frac{\varphi(m)}{\sqrt{m}}$$

avec :

$$\frac{\varphi(m)}{\sqrt{m}} = \frac{1}{\sqrt{2}} \prod_{i=2}^{r} \frac{p_i - 1}{\sqrt{p_i}}$$

Pour $p \geq 3$, on a $\dfrac{p-1}{\sqrt{p}} > 1$, donc $\dfrac{\varphi(m)}{\sqrt{m}} > \dfrac{p_2 - 1}{\sqrt{2}\sqrt{p_2}}$ et pour $p_2 \geq 5$, on a $\dfrac{p_2 - 1}{\sqrt{2}\sqrt{p_2}} > 1$. Il reste à étudier le cas $p_2 = 3$, soit $n = 2^{\alpha_1} 3^{\alpha_2} r$, avec $r = \prod_{i=3}^{r} p_i^{\alpha_i}$ où $5 \leq p_3 < \cdots < p_r$ sont premiers. Dans ce cas, on a :

$$\frac{\varphi(n)}{\sqrt{n}} = \frac{\varphi(2^{\alpha_1} 3^{\alpha_2})}{\sqrt{2^{\alpha_1} 3^{\alpha_2}}} \frac{\varphi(r)}{\sqrt{r}} > 1$$

d'après ce qui précède.

On a donc ainsi montré que $\varphi(n) > \sqrt{n}$ pour tout $n \geq 7$. ■

Le résultat de l'exercice qui suit est à la base du système cryptographique R.S.A. (pour Rivest, Shamir et Adleman).

Exercice 1.18 *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 $m^{ab} \equiv m \pmod{n}$.*

Solution 1.18 *Si $ab \equiv 1 \pmod{\varphi(n)}$, il existe alors un entier relatif k tel que :*

$$ab = 1 + k\varphi(n) = 1 + k(p-1)(q-1)$$

Si m est un entier relatif premier avec p, on a alors $m^{p-1} \equiv 1 \pmod{p}$ (théorème de Fermat) et :

$$m^{ab} = m m^{k(p-1)(q-1)} \equiv m \pmod{p}$$

Si l'entier relatif m n'est pas premier avec p, c'est nécessairement un multiple de p (qui est premier) et :

$$m^{ab} \equiv 0 \equiv m \pmod{p}$$

De manière analogue, on a $m^{ab} \equiv m \pmod{q}$ et avec p et q premiers entre eux il en résulte que $m^{ab} \equiv m \pmod{pq}$.

Le principe du système R. S. A. est le suivant. On se donne un ensemble $\{P_1, \cdots, P_n\}$ de $n \geq 2$ personnes qui souhaitent communiquer entre elles de façon codée. On attribue à chacune de ces personnes P_k un entier $n_k = p_k q_k$ produit de deux nombres premiers et un entier c_k premier avec $\varphi(n_k) = (p_k - 1)(q_k - 1)$. Les entiers n_k sont choisis très grands (de l'ordre de 10^{100}) de façon à rendre improbable les décompositions en facteurs premiers $n_k = p_k q_k$.

On dispose d'un annuaire public où est associé à chacun des P_k le couple (n_k, c_k). Comme c_k est premier avec $\varphi(n_k)$, il est inversible modulo $\varphi(n_k)$ et seul P_k qui connaît la factorisation de n_k est capable de calculer l'inverse d_k de c_k.

Un message est une succession d'entiers inférieurs aux n_k.

Si P_1 veut envoyer un message m codé à P_2, il lui envoie le plus petit entier positif m_2 congru à m^{c_2} modulo n_2. Il suffit alors à P_2 de calculer $m_2^{d_2}$ qui est congru à m modulo n_2 (de $c_2 d_2 \equiv 1 \pmod{\varphi(n_2)}$, on déduit que $m_2^{d_2} \equiv m^{c_2 d_2} \equiv m \pmod{n_2}$) pour décoder le message m_2.

Exercice 1.19 *On s'intéresse aux racines du polynôme $P(X) = X^2 - 1$ dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ pour $n \geq 2$.*

1. *Traiter le cas* $n = 2$.
2. *Traiter le cas où* $n \geq 3$ *est premier impair.*
3. *Traiter le cas où* $n = p^\alpha$ *où* $p \geq 3$ *est premier* $\alpha \geq 2$.
4. *Traiter le cas où* $n = 2^\alpha$ *où* $\alpha \geq 2$.
5. *Traiter le cas général* $n \geq 2$.

Solution 1.19

1. *Pour* $n = 2$, *on a* $\dfrac{\mathbb{Z}}{2\mathbb{Z}} = \left\{\overline{0}, \overline{1}\right\}$ *et* $\overline{1}$ *est l'unique solution.*
2. *Pour* $n \geq 3$ *premier impair,* $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ *est intègre avec* $-\overline{1} \neq \overline{1}$ *et* $-\overline{1}, \overline{1}$ *sont les deux seules solutions* ($x^2 - \overline{1} = \left(x - \overline{1}\right)\left(x + \overline{1}\right) = \overline{0}$ *si, et seulement si,* $x = -\overline{1}$ *ou* $x = \overline{1}$).
3. *Soit* $n = p^\alpha$ *où* $p \geq 3$ *est premier* $\alpha \geq 2$.
   On a déjà deux solutions distinctes $-\overline{1}$ *et* $\overline{1}$.
   Si $x = \overline{k} \in \dfrac{\mathbb{Z}}{p^\alpha\mathbb{Z}} \setminus \left\{-\overline{1}, \overline{1}\right\}$ *est une solution,* p^α *divise* $\left(x - \overline{1}\right)\left(x + \overline{1}\right)$, *ce qui équivaut à dire qu'il existe des entiers relatifs non nuls* u, v *premiers avec* p *et des entiers naturels* r, s *tels que* $r + s \geq \alpha$ *et* $k = 1 + up^r = -1 + vp^s$ (*on a* $(k-1)(k+1) = wp^\beta$ *avec* $\beta \geq \alpha$ *et* w *non nul premier avec* p).
   Si $r \geq 1$ *et* $s \geq 1$, *on a alors* $2 = vp^s - up^r$ *qui est divisible par* $p \geq 3$, *ce qui est impossible.*
   On a donc $r = 0$ *ou* $s = 0$, *donc* $s \geq \alpha$ *ou* $r \geq \alpha$, *soit* $\overline{k} = -\overline{1}$ *ou* $\overline{k} = \overline{1}$, *ce qui est exclu.*
   En définitive, $-\overline{1}$ *et* $\overline{1}$ *sont les deux seules solutions.*
4. *Soit* $n = 2^\alpha$ *où* $\alpha \geq 2$.
   On a déjà deux solutions distinctes $-\overline{1}$ *et* $\overline{1}$.
   Reprenant les notations et le raisonnement précédent, on a $k = 1 + u2^r = -1 + v2^s$ *avec* u, v *impairs non nuls et* $r + s \geq \alpha$, *donc* $2 = v \cdot 2^s - u \cdot 2^r$.
   Si $r = 0$ *[resp.* $s = 0$*]*, *on a alors* $s \geq \alpha$ *et* $u = 2\left(2^{s-1} - 1\right)$ *[resp.* $r \geq \alpha$ *et* $v = 2\left(2^{r-1} + 1\right)$*]* *avec* u *[resp.* v*]* *impair, ce qui est impossible.*
   Donc $r \geq 1$, $s \geq 1$ *et* $1 = v \cdot 2^{s-1} - u \cdot 2^{r-1}$, *ce qui impose* $s = 1$ *ou* $r = 1$ (*sinon le théorème de Bézout nous dit que* 2^{s-1} *et* 2^{r-1} *sont premiers entre eux, ce qui n'est pas pour* $r \geq 2$ *et* $r \geq 2$), *soit* $r \geq \alpha - 1$ *ou* $s \geq \alpha - 1$, *donc* $r = \alpha - 1$ *ou* $s = \alpha - 1$ (*sinon* $\overline{k} = \overline{1}$ *ou* $\overline{k} = -\overline{1}$, *ce qui est exclu), soit* $\overline{k} = \overline{1 + u2^{\alpha-1}} = \overline{1 + 2^{\alpha-1}}$ *ou* $\overline{k} = \overline{-1 + v2^{\alpha-1}} = \overline{-1 + 2^{\alpha-1}}$*puisque* u *et* v *sont impairs. On vérifie que réciproquement, ces deux éléments sont bien solutions distinctes.*
   En définitive, on a quatre solutions :

$$-\overline{1},\ \overline{1},\ \overline{1 + 2^{\alpha-1}},\ \overline{-1 + 2^{\alpha-1}}$$

   pour $\alpha \geq 3$ *et 2 solutions :*

$$-\overline{1} = \overline{1 + 2},\ \overline{1} = \overline{-1 + 2}$$

   pour $\alpha = 2$.
5. *En dehors des cas déjà traités, l'entier* n *s'écrit* $n = 2^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ *avec* $p_1 = 2 < p_2 < \cdots < p_r$ *premiers,* $\alpha_1 \geq 0$, $\alpha_k \geq 1$ *pour* k *compris entre* 1 *et* r.
   En notant, pour tout j *compris entre* 1 *et* r, $\overline{k}^{(j)}$ *la classe de* k *modulo* $p_j^{\alpha_j}$, *le théorème chinois nous dit que l'application :*

$$\varphi : \overline{k} \in \frac{\mathbb{Z}}{n\mathbb{Z}} \mapsto \left(\overline{k}^{(1)}, \cdots, \overline{k}^{(r)}\right)$$

est un isomorphisme d'anneaux (pour $\alpha_1 = 0$*, on se contente de* $\overline{k} \in \dfrac{\mathbb{Z}}{n\mathbb{Z}} \mapsto \left(\overline{k}^{(2)}, \cdots, \overline{k}^{(r)}\right)$*)*
et l'équation $\overline{k}^2 = \overline{1}$ *équivaut à* $\left(\overline{k}^{(j)}\right)^2 = \overline{1}^{(j)}$ *pour tout* j*. Le nombre de solutions est donc :*

$$\begin{cases} 2^{r-1} \text{ pour } \alpha_1 = 0 \text{ ou } 1 \\ 2^r \text{ pour } \alpha_1 = 2 \\ 2^{r+1} \text{ pour } \alpha_1 \geq 3 \end{cases}$$

1.4 Équations et système d'équations diophantiennes

Soient $n \geq 2$ un entier, a un entier naturel non nul et b un entier relatif.
On veut résoudre dans $\mathbb{Z}$ l'équation diophantienne :

$$ax \equiv b \ (n) \tag{1.1}$$

Dans le cas où $b = 1$, cette équation a des solutions si, et seulement si $\overline{a}$ est inversible dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$, ce qui équivaut à dire que a est premier avec n.

Dans ce cas l'algorithme d'Euclide nous permet de trouver une solution $x_0 \in \mathbb{Z}$ de (1.1) .

Si $x \in \mathbb{Z}$ est une autre solution, alors $a(x - x_0)$ est divisible par n qui est premier avec a et le théorème de Gauss nous dit que n doit diviser $x - x_0$.

Réciproquement on vérifie facilement que pour tout $k \in \mathbb{Z}$, $x_0 + kn$ est solution de (1.1) .

En définitive, dans le cas où a et n sont premiers entre eux, l'ensemble des solutions de $ax \equiv 1 \ (n)$ est :

$$S = \{x_0 + kn \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de cette équation.

Dans le cas où les entiers a et n sont premiers entre eux et b est un entier relatif quelconque, pour toute solution particulière u_0 de l'équation $ax \equiv 1 \ (n)$ l'entier $x_0 = bu_0$ est solution de (1.1) .

Comme précédemment, on en déduit que l'ensemble des solutions de (1.1) est :

$$S = \{bx_0 + kn \mid k \in \mathbb{Z}\}$$

où x_0 est une solution particulière de cette équation.

Considérons maintenant le cas général.

On note δ le pgcd de a et n et on a $a = \delta a'$, $n = \delta n'$ avec a' et n' premiers entre eux.

Théorème 1.12 *L'équation diophantienne* (1.1) *a des solutions entières si, et seulement si,* δ *divise* b*.*
Dans ce cas, l'ensemble des solutions de cette équation est :

$$S = \{b'x'_0 + kn' \mid k \in \mathbb{Z}\}$$

où x'_0 *est une solution particulière de* $a'x \equiv 1$ *modulo* n'*.*

Démonstration. Si l'équation (1.1) admet une solution $x \in \mathbb{Z}$ alors $\delta n'$ divise $\delta a' - b$ et δ divise b.

Si b est un multiple de δ, il s'écrit $b = \delta b'$ et toute solution de $a'x \equiv b' \ (n')$ est aussi solution de (1.1) .

On a vu que les solutions de $a'x \equiv b' \ (n')$ sont de la forme $x = b'x'_0 + kn'$ où x'_0 est une solution de $a'x \equiv 1 \ (n')$ et k est un entier relatif. Réciproquement on vérifie facilement que pour tout entier $k \in \mathbb{Z}$, $x = b'x'_0 + kn'$ est solution de (1.1). ■

Le théorème chinois peut être utilisé 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.

Dans le cas où les entiers $n_1, \cdots, n_r$ sont deux à deux premiers entre eux, cela revient à trouver l'antécédent dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ de $(\pi_1(a_1), \cdots, \pi_r(a_r))$ par l'isomorphisme :

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

Cet antécédent est $\overline{k_0}$, où $k_0 = \sum_{i=1}^{r} a_i u_i m_i$, en désignant par $(u_j)_{1\leq j\leq r}$ une suite d'entiers relatifs telle que $\sum_{j=1}^{r} u_j \frac{n}{n_j} = 1$. On a donc ainsi une solution particulière et les autres solutions sont les entiers $k = k_0 + q \cdot n$, où q est un entier relatif.

Exemple 1.2 *Considérons le système d'équations diophantiennes :*

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

Comme $n_1 = 4$, $n_2 = 5$, $n_3 = 9$ *sont deux à deux premiers entre eux, ce système a des solutions données en déterminant des coefficients dans une relation de Bézout* $u_1m_1 + u_2m_2 + u_3m_3 = 1$, *où* $m_1 = n_2n_3 = 45$, $m_2 = n_1n_3 = 36$, $m_3 = n_1n_2 = 20$. *Pour ce faire, on utilise l'associativité du* pgcd *en écrivant que :*

$$\begin{cases} m_2 \wedge m_3 = 4 = (-1) \cdot 36 + 2 \cdot 20 \\ 1 = m_1 \wedge (m_2 \wedge m_3) = 1 \cdot 45 + (-11) \cdot 4 \\ 1 = 1 \cdot 45 + 11 \cdot 36 + (-22) \cdot 20 \end{cases}$$

ce qui donne la solution particulière :

$$k_0 = 2 \cdot 45 + 33 \cdot 36 - 22 \cdot 20 = 838$$

et la solution générale :

$$k = 838 + 180q = 118 + 180q' \ (q' \in \mathbb{Z})$$

(on a effectué la division euclidienne de 838 *par* $n = 180$*).*

Dans le cas où les entiers $n_1, \cdots, n_r$ ne sont pas deux à deux premiers entre eux, c'est un plus délicat.

Considérons tout d'abord le cas de deux équations :

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{cases}$$

avec $\delta = n_1 \wedge n_2 \geq 2$.

On a $n_1 = \delta n_1'$, $n_2 = \delta n_2'$ avec $n_1' \wedge n_2' = 1$ et il existe $(u_1, u_2) \in \mathbb{Z}^2$ tel que $u_1 n_1' + u_2 n_2' = 1$.

Montrons que ce système a des solutions si, et seulement si, $a_2 - a_1$ est multiple de δ.

Si $k \in \mathbb{Z}$ est une solution, δ qui divise n_1 et n_2 va alors diviser $k - a_1$ et $k - a_2$ et aussi la différence $a_2 - a_1$.

Réciproquement, supposons $a_2 - a_1$ multiple de δ, soit $a_2 - a_1 = q\delta$.

En posant :

$$k_0 = a_2 u_1 n_1' + a_1 u_2 n_2'$$

on a :

$$\begin{aligned} k_0 &= a_2 \left(1 - u_2 n_2'\right) + a_1 u_2 n_2' \\ &= a_2 + \left(a_1 - a_2\right) u_2 n_2' = a_2 + q\delta u_2 n_2' \\ &= a_2 + q u_2 n_2 \equiv a_2 \pmod{n_2} \end{aligned}$$

et de manière analogue on voit que $k_0 \equiv a_1 \pmod{n_1}$. L'entier k_0 est donc une solution de notre système.

Si $k \in \mathbb{Z}$ est une autre solution de notre système, cet entier est alors congru à k_0 modulo n_1 et modulo n_2, soit :

$$\begin{aligned} k - k_0 &= q_1 n_1 = q_1 \delta n_1' \\ &= q_2 n_2 = q_2 \delta n_2' \end{aligned}$$

donc :

$$\frac{k - k_0}{\delta} = q_1 n_1' = q_2 n_2'$$

et comme $n_1' \wedge n_2' = 1$, le théorème de Gauss nous dit que n_2' divise q_1, donc :

$$\frac{k - k_0}{\delta} = q_3 n_1' n_2'$$

avec $q_3 \in \mathbb{Z}$, ce qui peut aussi s'écrire :

$$k - k_0 = q_3 \delta n_1' n_2' = q_3 \frac{n_1 n_2}{\delta} = q_3 n_1 \vee n_2$$

Réciproquement on vérifie facilement que pour tout entier relatif q_3, $k_0 + q_3 n_1 \vee n_2$ est solution de notre système.

En définitive, l'ensemble des solutions est :

$$S = \{k_0 + q_3 n_1 \vee n_2 \mid q_3 \in \mathbb{Z}\}$$

où k_0 est une solution particulière.

1.5 Formule de Möbius

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 :

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

Pour $d = 1$, S_1 est l'ensemble des entiers k compris entre 1 et n premier avec n.

Lemme 1.5 *Les S_d, pour d décrivant $\mathcal{D}_n$, forment une partition de $\{1,\cdots,n\}$ et pour tout $d\in\mathcal{D}_n$ on a* $\operatorname{card}(S_d)=\varphi\left(\dfrac{n}{d}\right)$.

Démonstration. Il est clair que $S_d\cap S_{d'}=\emptyset$ pour $d\neq d'$ dans $\mathcal{D}_n$ et tout entier $k\in\{1,\cdots,n\}$ est dans $S_{k\wedge n}$ avec $k\wedge n\in\mathcal{D}_n$.

On a donc la partition :

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

Un entier k compris entre 1 et n est dans S_d si et seulement si il s'écrit $k=dk'$ avec k' compris entre 1 et $\dfrac{n}{d}$ qui est premier avec $\dfrac{n}{d}$, donc :

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

■

Théorème 1.13 *Pour tout entier $n\geq 2$, on a :*

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

(formule de Möbius).

Démonstration. Du lemme précédent, on déduit que :

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

(l'application $d\mapsto\dfrac{n}{d}$ est une permutation de $\mathcal{D}_n$). ■

Au paragraphe 2.3 nous donnons une autre démonstration de la formule de Möbius.

De cette formule, on peut déduire que tout sous-groupe fini du groupe multiplicatif $\mathbb{K}^*$ d'un corps commutatif $\mathbb{K}$ est cyclique (théorème 2.13).

Pour tout entier $n\geq 1$, on désigne par Φ_n le n-ème polynôme cyclotomique défini par :

$$\Phi_n(X)=\prod_{k\in S_1}\left(X-\omega_n^k\right)$$

où $\omega_n=e^{\frac{2i\pi}{n}}$.

Ce polynôme est de degré $\operatorname{card}(S_1)=\varphi(n)$.

Théorème 1.14 *On a $X^n-1=\prod\limits_{d\in\mathcal{D}_n}\Phi_d$.*

Démonstration. Pour $d\in\mathcal{D}_n$, le polynôme :

$$\Phi_d(X)=\prod_{k\wedge d=1}\left(X-\omega_d^k\right)$$

est un diviseur de X^n-1 puisqu'il est scindé à racines simples de racines :

$$\omega_d^k=e^{\frac{2ik\pi}{d}}=\left(e^{\frac{2i\pi}{n}}\right)^{k\frac{n}{d}}$$

avec $k\frac{n}{d}$ compris entre 1 et n.

Comme $\left(k\frac{n}{d}\right) \wedge n = \left(k\frac{n}{d}\right) \wedge \left(d\frac{n}{d}\right) = \frac{n}{d}(k \wedge d) = \frac{n}{d}$, les polynômes Φ_d, pour d décrivant $\mathcal{D}_n$, sont deux à deux premiers entre eux.

Le polynôme $X^n - 1$ est donc multiple du ppcm des Φ_d, pour d décrivant $\mathcal{D}_n$, soit de leur produit $\prod_{d\in\mathcal{D}_n} \Phi_d$.

Comme ces polynômes sont unitaires de même degré (formule de Möbius), on en déduit l'égalité $X^n - 1 = \prod_{d\in\mathcal{D}_n} \Phi_d$. ■

1.6 $\left(\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times$ est cyclique pour $p \geq 3$ premier et $\alpha \geq 1$

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 $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$.

Lemme 1.6 *On a* $\psi(d) = \varphi(d)$ *pour tout* $d \in \mathcal{D}_{p-1}$.

Démonstration. Dire que $\psi(d) > 0$ équivaut à dire qu'il existe dans $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$ 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 $\frac{\mathbb{Z}}{p\mathbb{Z}}$, donc G est exactement l'ensemble de toutes les solutions de cette équation. Les éléments d'ordre d dans $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$ 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 $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$ 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 $d \in \mathcal{D}_{p-1}$. ■

Théorème 1.15 *Le groupe* $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$ *est cyclique.*

Démonstration. On a $\psi(p-1) = \varphi(p-1) > 0$, ce qui signifie qu'il existe dans $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$ des éléments d'ordre $p-1$ et ce groupe est cyclique d'ordre $p-1$. ■

Remarque 1.3 *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 (théorème 2.13).*

Théorème 1.16 *Si p est un nombre premier impair et α un entier supérieur ou égal à 2, alors le groupe multiplicatif $\left(\dfrac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times$ est cyclique.*

Démonstration. Cela résulte des points suivants.

1. Pour tout entier k compris entre 1 et $p-1$, $\binom{p}{k}$ est divisible par p.
   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).
2. Il existe une suite d'entiers naturels non nuls $(\lambda_k)_{k\in\mathbb{N}}$ tous premiers avec p tels que :

$$\forall k \in \mathbb{N},\ (1+p)^{p^k} = 1 + \lambda_k p^{k+1}$$

   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.
3. La classe résiduelle modulo p^α, $\overline{1+p}$ est d'ordre $p^{\alpha-1}$ dans $\left(\dfrac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times$.

   $1+p$ étant premier avec p^α, on a bien $\overline{1+p} \in \left(\dfrac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times$ 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 $\left(\dfrac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times$.
4. Si $x = k + p\mathbb{Z}$ un générateur du groupe cyclique $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$, alors $y = k^{p^{\alpha-1}} + p^\alpha\mathbb{Z}$ est d'ordre $p-1$ dans $\left(\dfrac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times$.

   La classe modulo p, $x = k + p\mathbb{Z}$ est d'ordre $p-1$ dans $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$ 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 $\left(\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times$ (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 $p-1$).

5. On en déduit que $\left(\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times$ est cyclique.

   Dans $\left(\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times$ 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 $\left(\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times$. En conséquence $\left(\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times$ est cyclique d'ordre $\varphi(p^\alpha)$.

■

Exercice 1.20

1. *Montrer que* $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^\times$ *et* $\left(\frac{\mathbb{Z}}{2^2\mathbb{Z}}\right)^\times$ *sont cycliques.*

2. *Dans cette question on s'intéresse au groupe multiplicatif* $\left(\frac{\mathbb{Z}}{2^\alpha\mathbb{Z}}\right)^\times$ *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* $\left(\frac{\mathbb{Z}}{2^\alpha\mathbb{Z}}\right)^\times$.

   (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* $\left(\frac{\mathbb{Z}}{2^\alpha\mathbb{Z}}\right)^\times$ *sur* $\left(\frac{\mathbb{Z}}{2^2\mathbb{Z}}\right)^\times$ *et que son noyau est un groupe cyclique d'ordre* $2^{\alpha-2}$.

   (d) *Montrer que l'application :*

   $$\begin{array}{rccc} \pi : & \left(\frac{\mathbb{Z}}{2^\alpha\mathbb{Z}}\right)^\times & \to & \left(\frac{\mathbb{Z}}{2^2\mathbb{Z}}\right)^\times \times \ker(\psi) \\ & x & \mapsto & (\psi(x), \psi(x)\,x) \end{array}$$

   est un isomorphisme de groupes. En déduire que $\left(\frac{\mathbb{Z}}{2^\alpha\mathbb{Z}}\right)^\times$ *est isomorphe à* $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{p^{\alpha-2}\mathbb{Z}}$. *Le groupe* $\left(\frac{\mathbb{Z}}{2^\alpha\mathbb{Z}}\right)^\times$ *est-il cyclique ?*

Solution 1.20

1. *On a* $\left(\dfrac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\times} = \left\{\overline{1}\right\}$ *et* $\left(\dfrac{\mathbb{Z}}{2^2\mathbb{Z}}\right)^{\times} = \left\{\overline{1}, \overline{-1}\right\} \approx \dfrac{\mathbb{Z}}{2\mathbb{Z}}$.

2. (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* $\left(\dfrac{\mathbb{Z}}{2^{\alpha}\mathbb{Z}}\right)^{\times}$, *il est donc isomorphe à* $\dfrac{\mathbb{Z}}{p^{\alpha-2}\mathbb{Z}}$.

   (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* $\dfrac{\left(\frac{\mathbb{Z}}{2^{\alpha}\mathbb{Z}}\right)^{\times}}{\ker(\psi)}$ *sur* $\left(\dfrac{\mathbb{Z}}{2^2\mathbb{Z}}\right)^{\times}$, *il en résulte que :*
$$\operatorname{card}\left(\left(\frac{\mathbb{Z}}{2^{\alpha}\mathbb{Z}}\right)^{\times}\right) = \operatorname{card}(\ker(\psi)) \operatorname{card}\left(\left(\frac{\mathbb{Z}}{2^2\mathbb{Z}}\right)^{\times}\right) = 2 \operatorname{card}(\ker(\psi))$$
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* $x \in \left(\frac{\mathbb{Z}}{2^{\alpha}\mathbb{Z}}\right)^{\times}$, *on a* $\psi(x) \in \left(\frac{\mathbb{Z}}{2^2\mathbb{Z}}\right)^{\times} = \left\{\overline{1}, \overline{-1}\right\}$. *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* $\left(\dfrac{\mathbb{Z}}{2^{\alpha}\mathbb{Z}}\right)^{\times}$ *est isomorphe à* $\dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\mathbb{Z}}{2^{\alpha-2}\mathbb{Z}}$ *pour* $\alpha \geq 3$ *et* $\left(\dfrac{\mathbb{Z}}{2^{\alpha}\mathbb{Z}}\right)^{\times}$ *n'est pas cyclique puisqu'il n'y a pas d'élément d'ordre* $2^{\alpha-1}$ *dans* $\dfrac{\mathbb{Z}}{2\mathbb{Z}} \times \dfrac{\mathbb{Z}}{2^{\alpha-2}\mathbb{Z}}$.

On peut montrer le résultat suivant (voir [**?**], page 7).

Théorème 1.17 *Le groupe multiplicatif* $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$ *est cyclique si, et seulement si,* $n = 2$, 4, p^{α} *ou* $2p^{\alpha}$ *avec* p *premier impair et* $\alpha \geq 1$.

1.7 Nombres de Carmichaël

Un théorème de Fermat nous dit que si p est premier et a premier avec p, on a alors $a^{p-1} \equiv 1 \pmod{p}$.

On s'intéresse ici à la « réciproque » de ce résultat : que peut-on dire de n tel que $a^{n-1} \equiv 1 \pmod{n}$ pour tout entier relatif a premier avec n ?

Définition 1.3 *On appelle nombre de Carmichaël tout entier $n \geq 2$ non premier tel que :*

$$\forall x \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times},\ x^{n-1} = \overline{1}$$

ce qui revient à dire que n est non premier et $k^{n-1} \equiv 1 \pmod{n}$ pour tout entier k premier avec n.

Remarque 1.4 *Un nombre de Carmichaël est impair. En effet, dans le cas contraire on a, $\left(\overline{-1}\right)^{n-1} = \overline{-1} \neq \overline{1}$ ($n \neq 2$ puisqu'il est non premier) et n n'est pas un nombre de Carmichaël.*

Exemple 1.3 *On a vu avec l'exercice 1.14 que 561 est un nombre de Carmichaël.*

Lemme 1.7 *Un nombre de Carmichaël est sans facteur carré.*

Démonstration. Soit $n \geq 3$ un nombre de Carmichaël.

S'il admet un facteur carré, il existe alors un nombre premier $p \geq 3$ (n est impair) et un entier $q \geq 1$ tels que $n = p^2 q$.

Avec :

$$(1 + pq)(1 - pq) = 1 - p^2q^2 = 1 - qn \equiv 1 \pmod{n}$$

on déduit que $x = \overline{1 + pq} \in \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est inversible d'inverse $\overline{1 - pq}$.

Comme $pq \not\equiv 0 \pmod{n}$ ($n = p^2q$ ne peut diviser pq), on a $x \neq \overline{1}$ et avec :

$$(1 + pq)^p = 1 + p^2q + p^2q \sum_{j=2}^{p} \binom{p}{j} p^{j-2} q^{p-j-1} \equiv 1 \pmod{n}$$

on déduit que x est d'ordre p dans $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$.

Comme n est de Carmichaël, on a aussi $x^{n-1} = \overline{1}$ et l'ordre p de x va diviser $n - 1 = p^2q - 1$, ce qui est impossible.

En définitive n est sans facteurs carrés. ∎

Théorème 1.18 *Soit $n \geq 3$ un entier. Les propriétés suivantes sont équivalentes :*

1. *n est un nombre de Carmichaël ;*
2. *il existe un entier $r \geq 3$ et des nombres premiers $3 \leq p_1 < \cdots < p_r$ tels que $n = \prod_{j=1}^{r} p_j$ et, pour tout indice j compris entre 1 et r, $p_j - 1$ divise $n - 1$;*
3. *n est non premier et :*

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

Démonstration. (1) $\Rightarrow$ (2) Si n est un nombre de Carmichaël, il est alors non premier sans facteurs carrés et sa décomposition en facteurs premiers est de la forme $n=\prod_{j=1}^{r} p_j$, où $r\geq 2$ et $3\leq p_1<\cdots<p_r$ sont premiers.

Si $r=2$, comme p_2-1 divise $n-1=(p_1-1)+p_1(p_2-1)$, il divise aussi p_1-1 ce qui est impossible puisque $p_2>p_1$.

On a donc $r\geq 3$, c'est-à-dire qu'un nombre de Carmichaël a au moins trois facteurs premiers.

Pour tout j compris entre 1 et r le groupe multiplicatif $\mathbb{Z}_{p_j}^{\times}$ est cyclique d'ordre p_j-1, donc il existe un élément $x_j=\pi_j(a_j)$ d'ordre p_j-1 dans $\left(\dfrac{\mathbb{Z}}{p_j\mathbb{Z}}\right)^{\times}$ (π_j est la surjection canonique de $\mathbb{Z}$ sur $\dfrac{\mathbb{Z}}{p_j\mathbb{Z}}$).

En utilisant le théorème chinois on peut trouver un entier k tel que $x_j=\pi_j(k)$ pour tout j compris entre 1 et r, la classe de k modulo n étant inversible dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ (l'application $\pi_n(k)\mapsto(\pi_j(k))_{1\leq j\leq r}$ réalise isomorphisme de groupes de $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$ sur $\prod_{j=1}^{r}\left(\dfrac{\mathbb{Z}}{p_j\mathbb{Z}}\right)^{\times}$) et comme n est de Carmichaël, on a aussi $(\pi_n(k))^{n-1}=\overline{1}$ dans $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$, donc $x_j^{n-1}=(\pi_j(k))^{n-1}=\overline{1}$ dans $\left(\dfrac{\mathbb{Z}}{p_j\mathbb{Z}}\right)^{\times}$ et l'ordre p_j-1 de x_j divise $n-1$.

(2) $\Rightarrow$ (3) Soit $n=\prod_{j=1}^{r} p_j$, où $r\geq 3$, $3\leq p_1<\cdots<p_r$ sont premiers tels que chaque p_j-1, pour j compris entre 1 et r, divise $n-1$.

Un tel entier, produit d'au moins trois nombres premiers est non premier.

Soit $x=\pi_n(k)\in\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ avec $k\in\{1,\cdots,n\}$.

Pour vérifier que $x^n=x$, il suffit de vérifier que $k^n\equiv k\pmod{p_j}$ pour tout j compris entre 1 et r (dans ce cas k^n-k qui est multiple de tous les p_j est multiple de leur ppcm, c'est-à-dire de n, ce qui revient à dire que $k^n\equiv k\pmod{n}$).

Pour j compris entre 1 et r on a deux possibilités :

soit p_j divise k et dans ce cas, il divise aussi k^n-k ;

soit p_j ne divise pas k et dans ce cas, il est premier avec k, donc $k^{p_j-1}\equiv 1\pmod{p_j}$ (théorème de Fermat) et comme $n-1$ est multiple de p_j-1, on a aussi $k^{n-1}\equiv 1\pmod{p_j}$ et $k^n\equiv k\pmod{p_j}$.

(3) $\Rightarrow$ (1) Supposons que n soit non premier et que $x^n=x$ pour tout $x\in\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

Pour $x\in\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$, on peut simplifier par x et on obtient $x^{n-1}=\overline{1}$. L'entier n est donc de Carmichaël. ∎

Exemple 1.4 *Les entiers* $561=3\times 11\times 17$, $1105=5\times 13\times 17$ *et* $1729=7\times 13\times 19$ *sont des nombres de Carmichaël puisque* $560=2\cdot 280=10\cdot 56=16\cdot 35$, $1104=4\cdot 276=12\cdot 92=16\cdot 69$ *et* $1728=6\cdot 288=12\cdot 144=18\cdot 96$.

On a aussi :

$2465=5\cdot 17\cdot 29$ *;* $2821=7\cdot 13\cdot 31$ *;* $6601=7\cdot 23\cdot 41$ *;* $8911=7\cdot 19\cdot 67$ *;* $10585=5\cdot 29\cdot 73$ *;* $15841=7\cdot 31\cdot 73$ *;* $29341=13\cdot 37\cdot 61$.

Exercice 1.21 *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.

Solution 1.21 *L'entier n est non premier et on a $n \equiv 1 \pmod{6a}$, $n \equiv (6a+1)^2 \equiv 1 \pmod{12a}$, $n \equiv (6a+1)(12a+1) \equiv 1 \pmod{18a}$, ce qui signifie que $p_j - 1$ divise $n-1$ pour $j = 1, 2, 3$. Donc n est de Carmichaël.*
Pour $a = 1$, on obtient $n = 7 \cdot 13 \cdot 19 = 1729$.
Pour $a = 5$, on obtient $n = 31 \cdot 61 \cdot 91 = 172\,081$.

1.8 Le théorème de Frobénius-Zolotarev

Pour ce paragraphe, $p \geq 3$ est un nombre premier impair et $n \geq 2$ est un entier.

Définition 1.4 *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 $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$.*

Pour tout $\lambda \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$, on définit le symbole de Legendre $\left(\frac{\lambda}{p}\right)$ par :

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

Lemme 1.8 *Si $\varphi : \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \to \{-1, 1\}$ est un morphisme de groupes non trivial, on a alors :*

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

Démonstration. Le groupe $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ étantcyclique d'ordre $p-1$, il existe $\mu \in \mathbb{F}_p^*$ tel que $\mathbb{F}_p^* = \langle \mu \rangle = \{1, \mu, \cdots, \mu^{p-2}\}$.

Donc pour tout élément λ de $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$, il existe un unique entier k compris entre 0 et $q-2$ tel que $\lambda = \mu^k$ et on a :

$$\varphi(\lambda) = (\varphi(\mu))^k$$

avec $\varphi(\mu) = \pm 1$.

Si $\varphi(\mu) = 1$, on a alors $\varphi(\lambda) = 1$ pour tout $\lambda \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ et φ est trivial contrairement à l'hypothèse.

On a donc $\varphi(\mu) = -1$ et $\varphi(\lambda) = (-1)^k$ pour tout $\lambda \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$.

Si λ est un carré dans $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$, il s'écrit alors $\lambda = \nu^2$ et on a $\varphi(\lambda) = (\varphi(\nu))^2 = (\pm 1)^2 = 1$.

Si λ est un non carré dans $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$, il s'écrit alors $\lambda = \mu^k$ avec k impair et on a $\varphi(\lambda) = (-1)^k = -1$.

En conclusion, $\varphi(\lambda) = \left(\frac{\lambda}{p}\right)$ pour tout $\lambda \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$. ∎

Lemme 1.9 *Si* $\gamma : GL_n\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right) \to \{-1,1\}$ *est un morphisme de groupes non trivial, on a alors :*

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

Démonstration. On vérifie tout d'abord que $\gamma(A) = 1$ pour toute matrice de transvection A.

Pour $1 \leq i \neq j \leq n$ fixés, on note $T_{ij}(\lambda) = I_n + \lambda E_{ij}$ une matrice de transvection et l'application :

$$\varphi : \lambda \in \frac{\mathbb{Z}}{p\mathbb{Z}} \mapsto \gamma(T_{ij}(\lambda)) \in \{-1,1\}$$

est un morphisme de groupes de $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}, +\right)$ dans $(\{-1,1\}, \cdot)$.

En effet, pour λ, μ dans $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$, on a $\varphi(\lambda+\mu) = \gamma(T_{ij}(\lambda+\mu))$ avec :

$$\begin{aligned} T_{ij}(\lambda+\mu) &= I_n + (\lambda+\mu)E_{ij} = (I_n + \lambda E_{ij})(I_n + \mu E_{ij}) \\ &= T_{ij}(\lambda)\, T_{ij}(\mu) \end{aligned}$$

puisque $E_{ij}^2 = 0$ pour $i \neq j$, donc :

$$\begin{aligned} \varphi(\lambda+\mu) &= \gamma(T_{ij}(\lambda)\, T_{ij}(\mu)) = \gamma(T_{ij}(\lambda))\,\gamma(T_{ij}(\mu)) \\ &= \varphi(\lambda)\,\varphi(\mu) \end{aligned}$$

Ces groupes étant finis, on a :

$$\operatorname{card}\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right) = \operatorname{card}(\ker(\varphi))\operatorname{card}(\operatorname{Im}(\varphi))$$

c'est-à-dire que $\operatorname{card}(\operatorname{Im}(\varphi))$ divise $p = \operatorname{card}\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)$.

Mais $\operatorname{Im}(\varphi)$ étant un sous-groupe de $\{-1,1\}$ est de cardinal égal à 1 ou 2 et nécessairement $\operatorname{card}(\operatorname{Im}(\varphi)) = 1$ puisque p est impair.

On a donc $\operatorname{Im}(\varphi) = \{\varphi(0)\} = \{1\}$, ce qui signifie que φ est la fonction constante égale à 1 ou encore que $\gamma(T_{ij}(\lambda)) = 1$ pour tout $\lambda \in \dfrac{\mathbb{Z}}{p\mathbb{Z}}$.

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

En notant $D_n(\lambda) = \begin{pmatrix} I_{n-1} & 0 \\ 0 & \lambda \end{pmatrix}$ une matrice de la dilatation avec $\lambda \in \left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$, l'application :

$$\varphi : \lambda \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \mapsto \gamma(D_n(\lambda)) \in \{-1,1\}$$

est un morphisme de groupes (puisque $D_n(\lambda\mu) = D_n(\lambda)\, D_n(\mu)$) et ce morphisme est non trivial puisque c'est le cas pour γ qui est trivial sur les transvections, donc $\gamma(D_n(\lambda)) = \left(\dfrac{\lambda}{p}\right) = \left(\dfrac{\det(A)}{p}\right)$.

Le lemme se déduit alors du fait que toute matrice $A \in GL_n\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)$ est produit de matrices de transvections (si elle est dans $SL_n\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)$) ou d'une matrice de dilatation de rapport $\det(A)$ et de matrices de transvections (si elle n'est pas dans $SL_n\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)$). ■

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

Théorème 1.19 (Frobénius-Zolotarev) *On a :*

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

Démonstration. Il s'agit de montrer que le morphisme de groupes $\varepsilon : GL_n\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right) \to \{-1,1\}$ est non trivial, ce qui revient à trouver un automorphisme $u \in GL\left(\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^n\right)$ de signature -1.

Un corps fini $\mathbb{F}_{p^n}$ à p^n éléments est aussi un $\frac{\mathbb{Z}}{p\mathbb{Z}}$-espace vectoriel de dimension n, donc isomorphe à $\mathbb{Z}_p^n$.

Il nous suffit donc de trouver un $\frac{\mathbb{Z}}{p\mathbb{Z}}$-automorphisme de $\mathbb{F}_{p^n}$ de signature -1.

Comme $\mathbb{F}_{p^n}^*$ est cyclique d'ordre p^n-1, il est engendré par un élément g d'ordre p^n-1.

On vérifie alors que le $\frac{\mathbb{Z}}{p\mathbb{Z}}$-automorphisme $\sigma : x \mapsto gx$ est de signature -1.

En effet, c'est la permutation de $\mathbb{F}_{p^n}$:

$$\sigma = \begin{pmatrix} 0 & 1 & g & g^2 & \cdots & g^{p^n-2} \\ 0 & g & g^2 & g^3 & \cdots & 1 \end{pmatrix}$$

soit le (p^n-1)-cycle $\begin{pmatrix} 1 & g & g^2 & \cdots & g^{p^n-2} \end{pmatrix}$ qui est de signature $(-1)^{p^n} = -1$ puisque p est impair. ■

2

Groupes monogènes, groupes cycliques

Les anneaux $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ sont supposés connus (voir le chapitre 1).
Pour ce chapitre, on se donne un groupe multiplicatif $(G,\cdot)$.

2.1 Sous-groupe engendré par une partie d'un groupe

Théorème 2.1 *L'intersection d'une famille quelconque $(H_i)_{i\in I}$ de sous-groupes de G est un sous-groupe de G.*

Démonstration. Soient $(H_i)_{i\in I}$ une famille de sous-groupes de G et $H=\bigcap_{i\in I} H_i$.
Comme l'élément neutre 1 est dans tous les H_i, il est aussi dans H et $H\neq\emptyset$.
Si g_1,g_2 sont dans H, ils sont alors dans tous les H_i, donc $g_1g_2^{-1}\in H_i$ pour tout $i\in I$, ce qui signifie que $g_1g_2^{-1}\in H$.
On a donc montré que H un sous-groupe de G. ■

Corollaire 2.1 *Si X est une partie de $(G,\cdot)$, l'intersection de tous les sous-groupes de G qui contiennent X est un sous-groupe de G.*

Démonstration. L'ensemble des sous-groupes de G qui contiennent X est non vide puisque G en fait partie et le théorème précédent nous dit que l'intersection de tous ces sous-groupes est un sous-groupe de G. ■

Définition 2.1 *Si X est une partie de $(G,\cdot)$, le sous-groupe de G engendré par X est l'intersection de tous les sous-groupes de G qui contiennent X.*

On note $\langle X\rangle$ le sous-groupe de G engendré par X et ce sous-groupe $\langle X\rangle$ est le plus petit (pour l'ordre de l'inclusion) des sous-groupes de G qui contiennent X.
Dans le cas où X est l'ensemble vide, on a $\langle X\rangle=\{1\}$.
Si X est une partie non vide de G formée d'un nombre fini d'éléments, $x_1,\cdots,x_n$, on note $\langle X\rangle=\langle x_1,\cdots,x_n\rangle$ le groupe engendré par X.

Définition 2.2 *Si X est une partie de $(G,\cdot)$, on dit que X engendre G (ou que X est une partie génératrice de G), si $G=\langle X\rangle$.*

Définition 2.3 *On dit que G est de type fini s'il admet une partie génératrice finie.*

Théorème 2.2 *Soient X,Y deux parties de G.*

1. *On a $X \subset \langle X \rangle$ et l'égalité est réalisée si, et seulement si X est un sous-groupe de G.*
2. *Si $X \subset Y$, on a alors $\langle X \rangle \subset \langle Y \rangle$.*
3. *En notant, pour X non vide, X^{-1} l'ensemble formé des symétriques des éléments de X, soit $X^{-1} = \{x^{-1} \mid x \in X\}$, les éléments de $\langle X \rangle$ sont de la forme $x_1 \cdot \cdots \cdot x_r$ où $r \in \mathbb{N}^*$ et les x_k sont dans $X \cup X^{-1}$ pour tout k compris entre 1 et r.*

Démonstration. Les points **1.** et **2.** se déduisent immédiatement des définitions.
Pour le point **3.** on montre tout d'abord que l'ensemble :

$$H = \left\{x_1 \cdot \cdots \cdot x_r \mid r \in \mathbb{N}^* \text{ et } x_k \in X \cup X^{-1} \text{ pour } 1 \leq k \leq r\right\}$$

est un sous-groupe de G.
Pour $x_1 \in X$, on a $1 = x_1 \cdot x_1^{-1} \in H$ et pour $x = x_1 \cdot \cdots \cdot x_r$, $y = y_1 \cdot \cdots \cdot y_s$ dans H, on a :

$$x \cdot y^{-1} = x_1 \cdot \cdots \cdot x_r \cdot y_s^{-1} \cdot \cdots \cdot y_1^{-1} \in H$$

Donc H est bien un sous-groupe de G.
Comme H est un sous-groupe de G qui contient X, on a $\langle X \rangle \subset H$.
Réciproquement, tout élément $h = x_1 \cdot \cdots \cdot x_r$ de H est un produit d'éléments de $X \cup X^{-1} \subset \langle X \rangle$, donc dans $\langle X \rangle$ et on a bien $\langle X \rangle = H$. ∎

Remarque 2.1 *Le point **3.** du théorème précédent nous dit aussi que $\langle X \rangle = \langle X^{-1} \rangle = \langle X \cup X^{-1} \rangle$.*

Remarque 2.2 *On a aussi :*

$$\langle X \rangle = \left\{ \prod_{k=1}^{r} x_k^{\varepsilon_k} \mid r \in \mathbb{N}^*,\ x_k \in X \text{ et } \varepsilon_k \in \{-1, 1\} \text{ pour } 1 \leq k \leq r \right\}$$

Dans le cas où les éléments de X sont en nombre fini et commutent, on a le résultat suivant.

Théorème 2.3 *Pour tout entier $p \geq 1$ et tout p-uplet $(g_1, \cdots, g_p)$ d'éléments de G qui commutent deux à deux, on a :*

$$\langle g_1, \cdots, g_p \rangle = \left\{ \prod_{k=1}^{p} g_k^{\alpha_k} \mid (\alpha_1, \cdots, \alpha_p) \in \mathbb{Z}^p \right\}$$

et ce groupe $\langle g_1, \cdots, g_p \rangle$ est commutatif.

Démonstration. En notant $X = \{g_1, \cdots, g_p\}$, on a $X^{-1} = \left\{g_1^{-1}, \cdots, g_p^{-1}\right\}$ et comme les g_k commutent, on déduit que :

$$\begin{aligned}\langle g_1, \cdots, g_p \rangle &= \left\{ \prod_{k=1}^{m} h_k \mid m \in \mathbb{N}^* \text{ et } h_k \in X \cup X^{-1} \text{ pour } 1 \leq k \leq m \right\} \\ &= \left\{ \prod_{k=1}^{p} g_k^{\alpha_k} \mid (\alpha_1, \cdots, \alpha_p) \in \mathbb{Z}^p \right\}\end{aligned}$$

($g_k g_j = g_j g_k$ entraîne $g_j^{-1} g_k = g_j^{-1} g_k g_j g_j^{-1} = g_j^{-1} g_j g_k g_j^{-1} = g_k g_j^{-1}$ et les éléments de $X \cup X^{-1}$ commutent).
Comme les g_k commutent, ce groupe est commutatif. ∎

Pour une loi de groupe notée additivement, on a dans le cas où G est commutatif :

$$\langle g_1, \cdots, g_p \rangle = \left\{ \sum_{k=1}^{p} \alpha_k g_k \mid (\alpha_1, \cdots, \alpha_p) \in \mathbb{Z}^p \right\}$$

Par exemple pour le groupe additif $G = \mathbb{Z}$, on a :

$$\langle g_1, \cdots, g_p \rangle = \sum_{k=1}^{p} g_k \mathbb{Z} = \delta \mathbb{Z}$$

où $\delta \in \mathbb{N}$ est le pgcd de $g_1, \cdots, g_p$.

2.2 Groupes monogènes, groupes cycliques

Définition 2.4 *On dit que G est monogène s'il existe un élément g de G tel que $G = \langle g \rangle$. Si de plus G est fini, on dit alors qu'il est cyclique.*

Le théorème 2.3, nous dit en particulier que :

$$\langle g \rangle = \left\{ \prod_{k=1}^{r} g^{\varepsilon_k} \mid r \in \mathbb{N}^*,\ \varepsilon_k = \pm 1 \text{ pour } 1 \leq k \leq r \right\} = \{ g^n \mid n \in \mathbb{Z} \}$$

Pour un groupe additif, on a :

$$\langle g \rangle = \{ ng \mid n \in \mathbb{Z} \}$$

On rappelle qu'un élément $g \in G$ est dit d'ordre fini si le groupe $\langle g \rangle$ est fini et l'ordre de g est alors le cardinal de $\langle g \rangle$.

On note $\theta(g)$ cet ordre et on a :

$$\begin{aligned} (\theta(g) = n \in \mathbb{N}^*) &\Leftrightarrow (\langle g \rangle = \{ g^r \mid 0 \leq r \leq n-1 \}) \\ &\Leftrightarrow \big(k \in \mathbb{Z} \text{ et } g^k = 1 \text{ équivaut à } k \equiv 0 \mod(n) \big) \end{aligned}$$

$\theta(g)$ est le plus petit entier naturel non nul tel que $g^n = 1$ (ou $ng = 0$ pour un groupe additif).

Le théorème de Lagrange nous dit que si G est fini, l'ordre de $g \in G$ divise alors l'ordre de G.

Remarque 2.3 *Un groupe cyclique est nécessairement commutatif.*

Remarque 2.4 *Un groupe cyclique engendré par un élément $g \neq 1$ a au moins deux élément, 1 et g.*

Exemple 2.1 *Le groupe additif $(\mathbb{Z}, +)$ est monogène engendré par 1.*
Les sous-groupes de $(\mathbb{Z}, +)$ qui sont tous de la forme $n\mathbb{Z}$ avec $n \geq 0$ sont monogènes et comme $(\mathbb{Z}, +)$ est commutatif, chaque ensemble quotient $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est naturellement muni d'une structure de groupe.
D'autre part, le théorème de division euclidienne nous permet d'écrire tout entier relatif k sous la forme $k = qn + r$ avec $0 \leq r \leq n-1$, ce qui entraîne $k - r \in n\mathbb{Z}$ et $\overline{k} = \overline{r}$. Et comme $\overline{r} \neq \overline{s}$ pour $0 \leq r \neq s \leq n-1$ (on a $0 < |r - s| < n$ et $r - s$ ne peut être multiple de n), on en déduit que le groupe :

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \left\{ \overline{0}, \overline{1}, \cdots, \overline{n-1} \right\}$$

a n éléments.
Ce groupe est cyclique d'ordre n engendré par $\overline{1}$.

Exercice 2.1 *Soit $X = \{r_1, \cdots, r_n\}$ une partie finie de $\mathbb{Q}$ et $G = \langle X \rangle$ le sous-groupe de $(\mathbb{Q}, +)$ engendré par X.*
Montrer que G est monogène infini.

Solution 2.1 *En désignant par μ le* ppcm *des dénominateurs de $r_1, \cdots, r_n$, il existe des entiers relatifs $a_1, \cdots, a_n$ tels que $r_k = \dfrac{a_k}{\mu}$ pour tout k compris entre 1 et n et en désignant par δ le* pgcd *de $a_1, \cdots, a_n$, on a :*

$$G = \left\{ \sum_{k=1}^{n} \alpha_k \frac{a_k}{\mu} \mid (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n \right\}$$
$$= \left\{ \frac{\delta}{\mu} \sum_{k=1}^{n} \alpha_k b_k \mid (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n \right\}$$

où $b_1, \cdots, b_n$ sont des entiers relatifs premiers entre eux dans leur ensemble.
On a donc $G = \dfrac{\delta}{\mu}\mathbb{Z}$, ce qui signifie que G est monogène engendré par $\dfrac{\delta}{\mu}$.

Théorème 2.4 *Soit G un groupe monogène.*
S'il est infini, il est alors isomorphe à $\mathbb{Z}$.
S'il est cyclique d'ordre n, il est alors isomorphe au groupe $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

Démonstration. Si $G = \langle g \rangle$ est un groupe monogène, l'application $\varphi : k \mapsto g^k$ est alors un morphisme de groupes surjectif de $(\mathbb{Z}, +)$ sur G et son noyau est un sous-groupe additif de $\mathbb{Z}$, donc de la forme $\ker(\varphi) = n\mathbb{Z}$ avec $n \in \mathbb{N}$.

Pour $n = 0$, φ est injectif et G est infini isomorphe à $\mathbb{Z}$.

Pour $n \geq 1$, le théorème d'isomorphisme nous dit que $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est isomorphe à G et $G = \langle g \rangle$ est cyclique d'ordre n. ∎

Remarque 2.5 *Dire que G est cyclique d'ordre n, signifie que G est de cardinal égal à n et qu'il existe dans G au moins un élément g d'ordre n.*
Dans ce cas, on a :

$$G = \langle g \rangle = \left\{1, g, \cdots, g^{n-1}\right\}$$

Théorème 2.5 *Soit $G = \langle g \rangle$ un groupe cyclique d'ordre n.*
Les générateurs de G sont les g^k, où k est un entier compris entre 1 et $n-1$ premier avec n.

Démonstration. Si $k \in \{1, \cdots, n-1\}$ est premier avec n, le théorème de Bézout nous dit qu'il existe deux entiers relatifs u, v tels que $uk + vn = 1$, ce qui entraîne $g = \left(g^k\right)^u \in \left\langle g^k \right\rangle$ et $G = \left\langle g^k \right\rangle$.

Réciproquement si $k \in \{1, \cdots, n-1\}$ est tel que $G = \left\langle g^k \right\rangle$, il existe un entier relatif u tel que $g = \left(g^k\right)^u = g^{ku}$, ce qui s'écrit aussi $g^{1-ku} = 1$ et n divise ku (puisque n est l'ordre de g), ce qui signifie qu'il existe un entier relatif v tel que $1 - ku = vn$, donc $uk + vn = 1$ et k est premier avec n. ∎

On rappelle que 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 $\varphi(1) = 1$).

Le nombre de générateurs d'un groupe cyclique G d'ordre n est donc égal à $\varphi(n)$.

On pourra consulter le paragraphe 1.2 pour une étude plus détaillée de cette fonction d'Euler.

Exemple 2.2 *Le groupe multiplicatif Γ_n des racines n-èmes de l'unité, qui est cyclique d'ordre n, est isomorphe à $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ par l'application $\overline{k} \mapsto e^{\frac{2ik\pi}{n}}$.*

Exercice 2.2 *Montrer que, pour tout entier $n \geq 1$, il existe un unique sous-groupe de $(\mathbb{Q}/\mathbb{Z}, +)$ d'ordre n et que ce groupe est cyclique.*

Solution 2.2 *Supposons que G soit un sous-groupe de $(\mathbb{Q}/\mathbb{Z}, +)$ d'ordre n. Tout $\overline{r} \in G$ a un ordre qui divise n (théorème de Lagrange), donc $n\overline{r} = \overline{0}$, c'est-à-dire qu'il existe $q \in \mathbb{Z}$ tel que $nr = q$ et $r = \dfrac{q}{n}$. On a donc $\overline{r} = \dfrac{\overline{q}}{n} = q\dfrac{\overline{1}}{n} \in \left\langle \dfrac{\overline{1}}{n} \right\rangle$ et $G \subset \left\langle \dfrac{\overline{1}}{n} \right\rangle$. Comme $\dfrac{\overline{1}}{n}$ est d'ordre n dans $\mathbb{Q}/\mathbb{Z}$ (on a $k\dfrac{\overline{1}}{n} = \dfrac{\overline{k}}{n} = \overline{0}$ si, et seulement si, $\dfrac{k}{n} \in \mathbb{Z}$, ce qui équivaut à dire que k est multiple de n), on a nécessairement $G = \left\langle \dfrac{\overline{1}}{n} \right\rangle$. D'où l'unicité d'un groupe d'ordre n et ce groupe existe (c'est $\left\langle \dfrac{\overline{1}}{n} \right\rangle$).*

Le théorème qui suit nous dit qu'à isomorphisme près, il y a un seul groupe d'ordre p premier, à savoir $\mathbb{Z}_p$.

Théorème 2.6 *Un groupe de cardinal premier est cyclique.*

Démonstration. Soit $(G, \cdot)$ un groupe de cardinal premier $p \geq 2$. Si $g \in G \setminus \{1\}$, il est d'ordre différent de 1 qui divise p, donc cet ordre est p et G est cyclique engendré par g.

L'application $[k] = k + p\mathbb{Z} \in \mathbb{Z}_p \mapsto g^k$ réalise alors un isomorphisme du groupe $(\mathbb{Z}_p, +)$ sur $(G, \cdot)$. ■

Si p et q sont deux nombres premiers, un groupe d'ordre pq n'est pas nécessairement cyclique comme le montre l'exemple du groupe symétrique $\mathcal{S}_3$ qui est d'ordre 6 non commutatif et donc non cyclique. Mais pour G commutatif d'ordre pq avec $p \neq q$, on a le résultat suivant.

Théorème 2.7 *Un groupe commutatif d'ordre pq, où p et q sont deux nombres premiers distincts, est cyclique.*

Démonstration. Soit G commutatif d'ordre pq avec $2 \leq p < q$ premiers.

On peut montrer que G est cyclique en utilisant le théorème de Cauchy qui nous dit qu'il existe dans G un groupe d'ordre p et un d'ordre q (voir le paragraphe **??**), ces groupes sont cycliques et on a ainsi un élément g d'ordre p et un élément h d'ordre q. L'élément gh est alors d'ordre pq (théorème **??** pour G commutatif) et G est cyclique.

On peut se passer du théorème de Cauchy en procédant comme suit.

S'il existe dans G un élément g d'ordre p et un élément h d'ordre q, alors gh est d'ordre pq et G est cyclique.

Sinon les éléments de $G \setminus \{1\}$ sont tous d'ordre p ou tous d'ordre q. Supposons les tous d'ordre p. Si $g \in G$ est d'ordre p, alors le groupe quotient $G/\langle g \rangle$ est d'ordre q premier, donc cyclique engendré par $\overline{g_0}$ d'ordre q dans $G/\langle g \rangle$, ce qui entraîne que $\theta(g_0) = p$ divise q (puisque $\overline{g_0}^p = \overline{g_0^p} = \overline{1}$), ce qui est impossible pour $p \neq q$ premiers. ■

Le théorème précédent nous dit que pour p, q premiers distincts, il existe à isomorphisme près, un seul groupe d'ordre pq, à savoir $\mathbb{Z}_{pq}$.

Pour $p = q$ premier, le théorème précédent est faux comme le montre l'exemple de $(\mathbb{Z}_p)^2$ qui est d'ordre p^2 non cyclique puisque tous ses éléments distincts du neutre sont d'ordre p.

En utilisant le théorème 2.6 et les actions de groupe (paragraphe **??**), on peut montrer qu'un groupe d'ordre p^2 avec p premier est commutatif isomorphe au groupe cyclique $\dfrac{\mathbb{Z}}{p^2\mathbb{Z}}$ ou au groupe non cyclique $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$ (théorème **??**).

Théorème 2.8 *Si $n \geq 2$ est un entier premier avec $\varphi(n)$, alors tout groupe commutatif d'ordre n est cyclique.*

Démonstration. Comme $m = \text{ppcm}\{\theta(g) \mid g \in G\} = \theta(g_0)$ et n ont les mêmes facteurs premiers (théorème **??**), on a les décompositions en facteurs premiers $n = \prod_{k=1}^{r} p_k^{\alpha_k}$ et $m = \prod_{k=1}^{r} p_k^{\beta_k}$, où les p_k sont premiers deux à deux distincts et $1 \leq \beta_k \leq \alpha_k$ pour tout k compris entre 1 et n.

Sachant que :

$$\varphi(n) = \prod_{k=1}^{r} p_k^{\alpha_k - 1}(p_k - 1)$$

on déduit que si $\varphi(n)$ est premier avec n, alors tous les α_k valent 1 (sinon p_k divise $\varphi(n)$ et n) et les β_k valent aussi 1, ce qui donne $n = m$ et G est cyclique puisque g_0 est d'ordre $n = \text{card}(G)$.

On peut aussi utiliser le théorème de Cauchy.

Si n est premier avec $\varphi(n)$, on a alors $n = \prod_{k=1}^{r} p_k$, où les p_k sont premiers deux à deux distincts. Le théorème de Cauchy nous assure l'existence, pour tout entier k compris entre 1 et n, d'un élément g_k d'ordre p_k dans G. Comme G est commutatif, le produit $g = \prod_{k=1}^{r} g_k$ est d'ordre n. ■

Réciproquement, on peut montrer que la réciproque est vrai, c'est-à-dire qu'un entier $n \geq 2$ est premier avec $\varphi(n)$ si, et seulement si, tout groupe commutatif d'ordre n est cyclique (voir [**?**], page 30).

2.3 Sous-groupes d'un groupe cyclique

Soient n un entier naturel non nul et $G = \langle a \rangle = \{1, a, \cdots, a^{n-1}\}$ un groupe cyclique d'ordre n.

Pour $n = 1$, $G = \{1\}$ est son seul sous-groupe.

On suppose donc pour ce paragraphe que $n \geq 2$.

Théorème 2.9

1. *Les sous-groupes de G sont tous cycliques d'ordre divisant n.*
2. *Pour tout diviseur positif d de n, il existe un unique sous-groupe d'ordre d de G. Ce sous-groupe est le groupe cyclique :*

$$H = \left\langle a^{\frac{n}{d}} \right\rangle$$

C'est également l'ensemble de tous les éléments de G d'ordre divisant d et les générateurs de H sont tous les éléments d'ordre d de G.

Démonstration.

1. Soit H un sous-groupe de G d'ordre d.
   Le théorème de Lagrange nous dit que d divise n, donc $n = qd$ avec $q \in \mathbb{N}^*$.
   Pour tout élément $h = a^k$ de H, on a $h^d = a^{kd} = 1$, donc l'ordre n de a divise kd et il existe un entier $j \in \mathbb{N}^*$ tel que $kd = jn = jqd$ et $k = jq$, ce qui nous dit que $h = a^k = (a^q)^j \in \langle a^q \rangle$
   On a donc $H \subset \langle a^q \rangle$ et d divise $\text{card}\left(\langle a^q \rangle\right)$.
   Mais $(a^q)^d = a^n = 1$, donc l'ordre de a^q divise d, soit $\text{card}\left(\langle a^q \rangle\right)$ divise d et $\text{card}\left(\langle a^q \rangle\right) = d$, ce qui nous dit que $H = \langle a^q \rangle$.
   Un sous-groupe d'ordre d de G, s'il existe, est donc unique.
2. Réciproquement, soient d un diviseur de n, $q = \dfrac{n}{d}$ et $H = \langle a^q \rangle$ le sous-groupe de G engendré par a^q.
   Si δ est l'ordre de H, on a $(a^q)^\delta = a^{q\delta} = 1$ et n divise $q\delta$, soit $\delta q = kn = kqd$ et d divise δ. Mais on a aussi $(a^q)^d = a^n = 1$, donc δ divise d et $\delta = d$.
   En conclusion $\langle a^q \rangle$ est l'unique sous-groupe d'ordre d de G.
   Le théorème de Lagrange nous dit que tous les éléments de H ont un ordre qui divise d.
   Réciproquement si $h = a^k \in G$ est d'ordre divisant d, on a alors $h^d = a^{kd} = 1$ et $n = qd$ divise kd, donc q divise k et $h = (a^q)^j \in H$.
   Le groupe H est donc l'ensemble de tous les éléments de G d'ordre divisant d.
   Les générateurs de H sont tous d'ordre d et réciproquement tout élément de G d'ordre d est dans H et l'engendre.

■

Le résultat précédent est en fait caractéristique des groupes cycliques.

Théorème 2.10 *Un groupe commutatif fini d'ordre $n \geq 1$ est cyclique si, et seulement si, pour tout diviseur d de n, il existe un unique sous-groupe d'ordre d de G.*

Démonstration. Le théorème précédent nous dit que la condition est nécessaire.

Pour la réciproque, on utilise le théorème de structure des groupes abéliens finis démontré plus loin (théorème 2.16).

Si G est groupe commutatif fini d'ordre $n \geq 2$ non cyclique, il est alors isomorphe à un groupe $\Gamma = \prod_{k=1}^{r} \dfrac{\mathbb{Z}}{n_k\mathbb{Z}}$ produit de $r \geq 2$ groupes cycliques, où $(n_k)_{1\leq k\leq r}$ est une suite d'entiers $(n_k)_{1\leq k\leq r}$ telle que $n_1 \geq 2$, n_2 est multiple de $n_1, \cdots, n_r$ est multiple de n_{r-1}.

Dans Γ, il y a au moins deux sous-groupes cycliques d'ordre n_1 (diviseur de n), à savoir :

$$H_1 = \left\{ (x_1, \pi_2(1), \cdots, \pi_r(1)) \mid x_1 \in \frac{\mathbb{Z}}{n_1\mathbb{Z}} \right\}$$

où on a noté π_k la projection canonique de $\mathbb{Z}$ sur $\dfrac{\mathbb{Z}}{n_k\mathbb{Z}}$ et :

$$H_2 = \{(\pi_1(1), x_2, \cdots, \pi_r(1)) \mid x_2 \in K_2\}$$

où K_2 est l'unique sous-groupe de $\dfrac{\mathbb{Z}}{n_2\mathbb{Z}}$ d'ordre n_1 (qui divise n_2). ■

Remarque 2.6 *Si $G = \langle a \rangle$ est un groupe cyclique d'ordre $n \geq 1$, il y a autant de sous-groupes de G que de diviseurs de n puisque l'application :*

$$d \in \mathcal{D}_n \mapsto \left\langle a^{\frac{n}{d}} \right\rangle$$

réalise une bijection de l'ensemble $\mathcal{D}_n$ des diviseurs positifs de n sur l'ensemble des sous-groupes de G.

Remarque 2.7 *Du théorème de structure des groupes abéliens finis (théorème 2.16), on déduit que si G est un groupe commutatif fini d'ordre $n \geq 1$, il existe alors, pour tout diviseur d de n, un sous-groupe d'ordre d (non unique pour G non cyclique).*

Remarque 2.8 *Pour un groupe fini non commutatif d'ordre $n \geq 4$, il n'existe pas nécessairement de sous-groupe d'ordre tout diviseur de n.*
Par exemple dans$\mathcal{A}_4$ qui est d'ordre 12, il n'y a pas de sous-groupes d'ordre 6 (exercice ??).
Mais pour tout diviseur premier p de n, il existe un sous-groupe de G d'ordre p (théorème ??).

Pour $G = \dfrac{\mathbb{Z}}{n\mathbb{Z}}$, d diviseur de n, l'unique sous-groupe d'ordre d de G est $H = \left\langle q\overline{1} \right\rangle = \dfrac{q\mathbb{Z}}{n\mathbb{Z}}$, où $q = \dfrac{n}{d}$ et ce sous-groupe est isomorphe à $\dfrac{\mathbb{Z}}{d\mathbb{Z}}$.
Ce résultat est en fait un cas particulier du suivant.

Théorème 2.11 *Soient G un groupe et H un sous-groupe distingué de G. Les sous-groupes du groupe quotient G/H sont de la forme K/H où K est un sous-groupe de G qui contient H.*

Démonstration. Soit K un sous-groupe de G qui contient H. Comme H est distingué dans G, il l'est aussi dans K et :

$$K/H = \{gH \mid g \in K\} \subset G/H = \{gH \mid g \in G\}$$

est un sous-groupe de G/H.
Réciproquement soit L un sous-groupe de G/H et :

$$K = \{g \in G \mid gH \in L\}$$

On a $H \subset L$ (pour $g \in H$, on a $gH = H = \overline{1} \in L$ puisque L est un groupe) et K est un sous-groupe de G (si $g \in K$, on a $gH = \overline{g} \in L$, donc $g^{-1}H = \overline{g^{-1}} = \overline{g}^{-1} \in L$ et pour g_1, g_2 dans K, on a $g_1g_2H = \overline{g_1g_2} \in L$). Comme H est distingué dans G, il l'est dans K et $K/H = \{gH \mid g \in K\} = L$ par construction. ∎

Le théorème précédent nous dit que si H est un sous-groupe distingué de G, on a alors une bijection entre les sous groupes de G/H et les sous-groupes de G qui contiennent H.

Exemple 2.3 *Les sous-groupes de $\Gamma_n = \{z \in C \mid z^n = 1\} = \left\langle e^{\frac{2i\pi}{n}} \right\rangle$ sont les $\left\langle \left(e^{\frac{2i\pi}{n}}\right)^{\frac{n}{d}} \right\rangle = \left\langle e^{\frac{2i\pi}{d}} \right\rangle = \Gamma_d$ où d est un diviseur de n et il y en a autant que de diviseurs de n.*

Corollaire 2.2 *Pour tout entier $n \geq 2$, on a :*

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

où $\mathcal{D}_n$ est l'ensemble des diviseurs strictement positifs de n (formule de Möbius).

Démonstration. Pour tout $d \in \mathcal{D}_n$, $H = \left\langle \dfrac{\overline{n}}{d} \right\rangle \backsimeq \dfrac{\mathbb{Z}}{d\mathbb{Z}}$ est l'unique sous-groupe d'ordre d de $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$, donc :

$$\begin{aligned} \varphi(d) &= \operatorname{card}\{\text{générateurs de } H\} \\ &= \operatorname{card}\left\{x \in \frac{\mathbb{Z}}{n\mathbb{Z}} \mid \theta(x) = d\right\} \end{aligned}$$

($\theta(x)$ est l'ordre de x dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$).

Le théorème de Lagrange nous dit que les ensembles $\left\{x \in \dfrac{\mathbb{Z}}{n\mathbb{Z}} \mid \theta(x) = d\right\}$, pour d décrivant $\mathcal{D}_n$, forment une partition de $\{1, \cdots, n\}$, ce qui nous donne la formule de Möbius. ■

Au paragraphe 1.5 nous donnons une autre démonstration de la formule de Möbius.

Le théorème 2.10 nous permet de montrer le théorème de Cauchy dans le cas commutatif.

Théorème 2.12 (Cauchy) *Soit G un groupe commutatif fini d'ordre $n \geq 2$. Pour tout diviseur premier p de n il existe dans G un élément d'ordre p.*

Démonstration. On procède par récurrence sur l'ordre $n \geq 2$ de G.

Pour $n = 2$, c'est clair puisque $G = \{1, g\}$ est le seul sous-groupe d'ordre 2.

Supposons le acquis pour les groupes commutatifs d'ordre $m < n$, où $n \geq 3$. On se donne un groupe commutatif G d'ordre n, un diviseur premier p de n et un élément $a \in G \setminus \{1\}$.

Si $G = \langle a \rangle$, alors G est cyclique et a est d'ordre n. Pour tout diviseur premier p de n, on a vu que $a^{\frac{n}{p}}$ est d'ordre p dans G.

Si $G \neq \langle a \rangle$ et p divise $m = \operatorname{card}(\langle a \rangle) < n$, alors l'hypothèse de récurrence nous assure de l'existence d'un élément h dans $\langle a \rangle$ qui est d'ordre p.

Supposons enfin que $G \neq \langle a \rangle$ et p ne divise pas $m = \operatorname{card}(\langle a \rangle)$. Comme p est premier ne divisant pas m, il est premier avec m et le groupe quotient $G/\langle a \rangle$ est commutatif d'ordre $r = \dfrac{n}{m} < n$ divisible par p (p divise $n = rm$ et p est premier avec m, le théorème de Gauss nous dit alors que p divise r). L'hypothèse de récurrence nous assure alors de l'existence d'un élément $\overline{h}$ d'ordre p dans $G/\langle a \rangle$. Comme l'ordre s de h est multiple de $\theta\left(\overline{h}\right) = p$ (exercice **??**), $k = h^{\frac{s}{p}}$ est d'ordre p dans G. ■

Remarque 2.9 *Pour G commutatif non cyclique et d diviseur quelconque de n, il n'existe pas nécessairement d'élément d'ordre d dans G. Par exemple, $G = (\mathbb{Z}_2)^3$ est d'ordre 8 avec tous ses éléments distincts du neutre d'ordre 2 et il n'existe pas d'élément d'ordre 4.*
Ou plus simplement, pour G non cyclique et $d = n$, il n'existe pas d'élément d'ordre n.

2.4 Sous-groupes multiplicatifs d'un corps commutatif

Dans ce paragraphe, nous allons vérifier que, pour tout corps commutatif $\mathbb{K}$, les sous-groupes finis du groupe multiplicatif $\mathbb{K}^*$ sont cycliques.

Exercice 2.3 *Montrer que, pour tout entier $n \geq 1$, il existe un unique sous-groupe de $(\mathbb{C}^*, \cdot)$ d'ordre n et que ce groupe est cyclique.*

Solution 2.3 *Si G est un sous-groupe d'ordre $n \geq 1$ de $(\mathbb{C}^*, \cdot)$, on a alors $z^n = 1$ pour tout $z \in G$ (théorème de Lagrange), donc G est contenu dans le groupe Γ_n des racines n-èmes de l'unité et $G = \Gamma_n$ puisque ces ensembles sont de même cardinal.*

Exercice 2.4 *Déterminer les sous-groupes finis du groupe multiplicatif $\mathbb{R}^*$.*

Solution 2.4 *Si $G \subset \mathbb{R}^*$ est un groupe d'ordre $n \geq 1$, on a alors $x^n = 1$ pour $x \in G$ et G est contenu dans l'ensemble :*

$$\Delta_n = \{x \in \mathbb{R} \mid x^n = 1\} = \begin{cases} \{-1, 1\} & \text{si } n \text{ est pair} \\ \{1\} & \text{si } n \text{ est impair} \end{cases}$$

On a donc nécessairement $n = 1$ et $G = \{1\}$ ou $n = 2$ et $G = \{-1, 1\}$.

Exercice 2.5 *Montrer que tout sous-groupe d'ordre $n \geq 1$ du groupe $O_2^+(\mathbb{R})$ des matrices de rotations du plan vectoriel euclidien $\mathbb{R}^2$ est cyclique engendré par $R\left(\frac{2\pi}{n}\right)$ (rotation d'angle $\frac{2\pi}{n}$).*

Solution 2.5 *Le groupe $O_2^+(\mathbb{R})$ est isomorphe au groupe multiplicatif Γ des nombres complexes de module égal à 1, un isomorphisme étant défini par l'application :*

$$R(\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \mapsto e^{i\theta}.$$

Un sous-groupe fini de $O_2^+(\mathbb{R})$ est donc identifié à un sous-groupe fini de Γ, donc de $\mathbb{C}^*$, et en conséquence il est cyclique engendré par $R\left(\frac{2\pi}{n}\right)$.

Théorème 2.13 *Tout sous-groupe fini du groupe multiplicatif $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ d'un corps commutatif $\mathbb{K}$ est cyclique.*

Démonstration. Soit $(G, \cdot)$ un sous-groupe d'ordre n de $\mathbb{K}^*$. Il existe dans le groupe fini commutatif G un élément g_0 d'ordre $m \leq n$ égal au ppcm des ordres des éléments de G (théorème **??**). L'ordre de tout élément de G divisant m, on déduit que tout $g \in G$ est racine du polynôme $P(X) = X^m - 1$, ce qui donne n racines distinctes de P dans $\mathbb{K}$, mais sur un corps commutatif un polynôme de degré m a au plus m racines [1], on a donc $n \leq m$ et $m = n$. Le groupe G d'ordre n ayant un élément d'ordre n est cyclique.

On peut aussi montrer ce résultat en utilisant la formule de Möbius.

Pour $n = 1$, le résultat est clair.

On suppose donc que G est d'ordre $n \geq 2$ et pour tout diviseur d de n, on note :

$$\psi(d) = \operatorname{card}\{g \in G \mid \theta(g) = d\}$$

Le théorème de Lagrange nous dit que les ensembles $\{g \in G \mid \theta(g) = d\}$, pour d décrivant l'ensemble $\mathcal{D}_n$ des diviseurs de n, forment une partition de $\{1, \cdots, n\}$, donc $n = \sum_{d \in \mathcal{D}_n} \psi(d)$.

Pour $d \in \mathcal{D}_n$ tel que $\psi(d) \geq 1$ (les $\psi(d)$ ne peuvent pas être tous nuls), il existe dans G au moins un élément g d'ordre d et le groupe $H = \langle g \rangle$ est formé de d solutions distinctes de l'équation $X^d - 1 = \overline{0}$, or cette équation a au plus d solutions dans le corps commutatif $\mathbb{K}$, donc H est exactement l'ensemble de toutes les solutions de cette équation.

Les éléments d'ordre d dans G sont donc les générateurs du groupe cyclique H et il y a $\varphi(d)$ tels générateurs, donc $\psi(d) = \varphi(d)$ si $\psi(d) \geq 1$.

Avec la formule de Möbius, on en déduit que :

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

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

En particulier, on a $\psi(n) \geq 1$, ce qui signifie qu'il existe dans G au moins un élément d'ordre n et en conséquence, G est cyclique. ∎

Si $\mathbb{K}$ est un corps fini, il est alors commutatif (démonstration non évidente) et en conséquence $\mathbb{K}^*$ est cyclique.

En particulier, pour $p \geq 2$ premier, le groupe $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ est cyclique d'ordre $p - 1$.

De manière plus générale, on peut montrer le résultat suivant.

1. Ce résultat est faux sur un corps non commutatif, voir par exemple le corps des quaternions.

Théorème 2.14 *Si p est un nombre premier impair et α un entier supérieur ou égal à 2, alors le groupe multiplicatif $\left(\dfrac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times$ des éléments inversibles de $\dfrac{\mathbb{Z}}{p^\alpha\mathbb{Z}}$ est cyclique.*

Pour $p=2$, le groupe multiplicatif $\left(\dfrac{\mathbb{Z}}{2^\alpha\mathbb{Z}}\right)^\times$ est cyclique pour $\alpha=1$, $\alpha=2$ et non cyclique pour $\alpha\geq 3$.

Démonstration. Voir le paragraphe 1.6. ∎

2.5 Théorème de structure des 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.

On rappelle que $e(G)=\text{ppcm}\{\theta(g)\mid g\in G\}$ (théorème **??**).

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 $\mathbb{C}^*$.

Dans ce qui suit, on se donne un groupe commutatif G d'ordre $n\geq 2$ et en utilisant les caractères nous allons montrer que G est isomorphe à un produit $\prod\limits_{k=1}^{r}\Gamma_{n_k}$ où la 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} est uniquement déterminée.

Lemme 2.1 *Soit H un sous-groupe de G. Tout caractère $\varphi: H\to\mathbb{C}^*$ peut se prolonger en un caractère sur G.*

Démonstration. Si $H=G$, c'est terminé.

On suppose que $H\neq G$, on se donne un élément g de $G\setminus H$ et on vérifie 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.

Comme $g^{\theta(g)}=1\in H$ (ou $g^n=1\in H$), on peut définir l'entier :

$$r=\min\left\{k\in\mathbb{N}^*\mid g^k\in H\right\}$$

et comme $\mathbb{C}$ est algébriquement clos, il existe $\alpha\in\mathbb{C}^*$ tel que $\varphi(g^r)=\alpha^r$.

On note :

$$K=\left\{g^kh\mid k\in\mathbb{Z},\ h\in H\right\}$$

le sous-groupe de G engendré par g et H et on vérifie que l'application :

$$\begin{array}{rccc}\varphi_K: & K & \to & \mathbb{C}^* \\ & g^kh & \mapsto & \alpha^k\varphi(h)\end{array}$$

est bien définie, puis que c'est un morphisme de groupes.

Si $g^kh=g^{k'}h'$ avec $k\geq k'$ dans $\mathbb{Z}$ et h,h' dans H, on a alors $g^{k-k'}=h'h^{-1}\in H$ et $k-k'=qr$ (la division euclidienne par r nous donne $k-k'=qr+s$ avec $0\leq s\leq r-1$, donc $h'h^{-1}=g^{k-k'}=(g^r)^q g^s$ et $g^s=((g^r)^q)^{-1}h'h^{-1}\in H$, ce qui impose $s=0$ par le caractère minimal de r), donc :

$$\varphi\left(h'h^{-1}\right)=\varphi\left(g^{k-k'}\right)=\varphi(g^r)^q=(\alpha^r)^q=\alpha^{k-k'}$$

et $\alpha^k\varphi(h)=\alpha^{k'}\varphi(h')$.

Donc l'application φ_K est bien définie.
On vérifie facilement que c'est un morphisme de groupes.
En effet, pour $g^k h$ et $g^{k'} h'$ dans K, on a :

$$\begin{aligned}\varphi_K\left(\left(g^k h\right)\left(g^{k'} h'\right)\right) &= \varphi_K\left(g^{k+k'} hh'\right) = \alpha^{k+k'}\varphi\left(hh'\right) \\ &= \alpha^k \varphi\left(h\right)\alpha^{k'}\varphi\left(h'\right) = \varphi_K\left(g^k h\right)\varphi_K\left(g^{k'} h'\right)\end{aligned}$$

Avec la construction précédente, si $K = G$, on a bien prolongé φ à G. Sinon on reprend cette construction à partir de K.
Comme le groupe G est fini, on aura prolongé φ à G par ces itérations. ■

Lemme 2.2 *On se donne un élément g_0 de G d'ordre égal à l'exposant de G, soit :*

$$m = \theta\left(g_0\right) = \max_{g\in G}\theta\left(g\right) = \operatorname{ppcm}\left\{\theta\left(g\right) \mid g \in G\right\}$$

et en supposant que $m \leq n-1$, on note $K = \langle g_0\rangle$ le sous groupe cyclique de G engendré par g_0.

1. *Il existe un unique caractère $\varphi_0 : K \to \mathbb{C}^*$ tel que $\varphi_0\left(g_0\right) = \omega = e^{\frac{2i\pi}{m}}$.*
2. *En prolongeant le caractère φ_0 en un caractère φ de G, l'application :*

$$\begin{array}{rccc}\theta : & \langle g_0\rangle \times \ker\left(\varphi\right) & \to & G \\ & \left(g_0^k, h\right) & \mapsto & g_0^k h\end{array}$$

est un isomorphisme de groupes.

Démonstration. Comme G n'est pas réduit à $\{1\}$, on a $2 \leq m \leq n-1$ en supposant que $m \neq n$.

1. Si un tel caractère existe, on a alors pour tout entier relatif k, $\varphi_0\left(g_0^k\right) = \omega^k$, ce qui prouve son unicité.
   Définissant l'application φ_0 de la sorte, on vérifie que c'est un caractère de K.
   D'une part cette application est bien définie puisque l'égalité $g_0^k = g_0^{k'}$ dans G équivaut à $k \equiv k' \pmod{m}$, ce qui donne $\omega^k = \omega^{k'}$ et d'autre part, on vérifie facilement que c'est un morphisme de groupes.
2. Comme le groupe G est commutatif, l'application θ est bien un morphisme de groupes.
   Si $\left(g_0^k, h\right) \in \ker\left(\theta\right)$, on a alors $g_0^k h = 1$ et $\varphi\left(g_0^k h\right) = \omega^k = 1$, donc $k \equiv 0 \pmod{m}$, ce qui nous donne $g_0^k = 1$ et $h = 1$.
   Donc θ est injective.
   Pour tout $g \in G$, on a $g^m = 1$, donc $\varphi\left(g^m\right) = \left(\varphi\left(g\right)\right)^m = 1$ et $\varphi\left(g\right) \in \Gamma_m$, soit $\varphi\left(g\right) = \omega^k = \varphi\left(g_0^k\right)$ pour un entier k et $h = g\left(g_0^k\right)^{-1} \in \ker\left(\varphi\right)$, ce qui nous donne $g = g_0^k h = \theta\left(g_0^k, h\right)$.
   Donc θ est surjective et θ est un isomorphisme.

■

De ces deux lemmes, on déduit l'existence d'une décomposition de G en produit direct de groupes cycliques.

Théorème 2.15 *Il existe une suite d'entiers $\left(n_k\right)_{1\leq k\leq r}$ 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 $\Gamma = \prod_{k=1}^{r}\Gamma_{n_k}$.*

Démonstration. On prouve l'existence d'une telle suite d'entiers par récurrence sur l'ordre $n \geq 2$ du groupe commutatif G.

Pour $n = 2$, le groupe G est cyclique isomorphe à $\Gamma_2 = \{-1, 1\}$.

Supposons le résultat acquis pour les groupes commutatifs d'ordre au plus égal à $n-1 \geq 2$ et soit G un groupe commutatif d'ordre $n \geq 3$.

Si, avec les notations introduites avec les lemmes précédents, on a $m = n$, le groupe G est alors cyclique d'ordre n isomorphe à Γ_n.

Supposons que $2 \leq m \leq n-1$.

On a alors $\text{card}\,(\ker(\varphi)) = \dfrac{\text{card}\,(G)}{\text{card}\,(\langle g_0 \rangle)} = \dfrac{n}{m} \in \{2, \cdots, n-1\}$ et par hypothèse de récurrence, $\ker(\varphi)$ est isomorphe à un groupe produit $\Gamma = \prod_{k=1}^{r} \Gamma_{n_k}$ avec $n_1 \geq 2$ qui divise n_2, ..., n_{k-1} qui divise n_k.

Le groupe cyclique $\langle g_0 \rangle$ étant isomorphe à $\Gamma_m = \Gamma_{n_{r+1}}$, on en déduit un isomorphisme de $\prod_{k=1}^{r+1} \Gamma_{n_k}$ sur G.

Comme m est le ppcm des ordres des éléments de G, c'est aussi le ppcm des ordres des éléments du groupe produit $\Gamma = \prod_{k=1}^{r+1} \Gamma_{n_k}$ et en particulier, il multiple de n_k qui est l'ordre de $\left(1, \cdots, e^{\frac{2i\pi}{n_k}}, 1\right)$. ∎

Pour prouver l'unicité d'une telle décompositions, nous utilisons le résultat suivant.

Lemme 2.3 *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. Ces suites sont identiques si, et seulement si, on a :*

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

Démonstration. La condition nécessaire est évidente.

Supposons que :

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

Prenant $m = \prod_{k=1}^{r} n_k \prod_{j=1}^{j} m_j$, on a $\text{pgcd}\,(m, n_k) = n_k$ pour tout k compris entre 1 et r et $\text{pgcd}\,(m, m_j) = m_j$ pour tout j compris entre 1 et s, donc :

$$\prod_{k=1}^{r} n_k = \prod_{j=1}^{s} m_j$$

Prenant $m = n_r$ qui est multiple de tous les n_k, on a $\text{pgcd}\,(m, n_k) = n_k$ pour tout k compris entre 1 et r et :

$$\prod_{k=1}^{r} n_k = \prod_{j=1}^{s} \text{pgcd}\,(n_r, m_j)$$

donc :

$$\prod_{j=1}^{j} m_j = \prod_{j=1}^{j} \text{pgcd}\,(n_r, m_j)$$

ou encore :

$$\prod_{j=1}^{s} \frac{m_j}{\operatorname{pgcd}(n_r, m_j)} = 1 \text{ dans } \mathbb{N}^*$$

ce qui équivaut à dire que :

$$\operatorname{pgcd}(n_r, m_j) = m_j \ \ (1 \leq j \leq s)$$

En particulier, on a $m_s = \operatorname{pgcd}(n_r, m_s)$ divise n_r.

Comme les suites $(n_k)_{1\leq k\leq r}$ et $(m_j)_{1\leq j\leq s}$ jouent des rôles symétriques, on a aussi n_r qui divise m_s et l'égalité $n_r = m_s$.

Par récurrence, on en déduit que $r = s$ et $n_k = m_k$ pour tout k compris entre 1 et r. ■

Théorème 2.16 (Kronecker) *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).*

Démonstration. On remarque que l'exposant d'un groupe $\Gamma = \prod_{k=1}^{r} \Gamma_{n_k}$ est n_r.

En effet, comme n_r est multiple de tous les n_k, on a $(z_1, \cdots, z_r)^{n_r} = (z_1^{n_r}, \cdots, z_r^{n_r}) = (1, \cdots, 1)$, donc les éléments de Γ sont d'ordre au plus égal à n_r et comme $(1, \cdots 1, , \omega_{n_r})$ est d'ordre n_r, cet entier n_r est bien l'exposant de Γ.

Supposons qu'il existe deux suites d'entiers $(n_k)_{1\leq k\leq r}$ et $(m_j)_{1\leq j\leq s}$ avec les propriétés voulues.

Si $r = 1$, on a alors $n = n_1 = e(G) = m_s$ et nécessairement $s = 1$ (sinon $n = \operatorname{card}(\Gamma) = m_1 \cdots m_s \geq 2m_s = 2n$, ce qui n'est pas).

Si $r \geq 2$, on a alors $s \geq 2$.

Pour tout entier $m \geq 1$ l'image du groupe $\prod_{k=1}^{r} \Gamma_{n_k} \backsimeq \prod_{j=1}^{s} \Gamma_{m_j}$ par le morphisme de groupe $\varphi_m : x \mapsto x^m$ est le groupe :

$$\prod_{k=1}^{r} \left\langle \omega_{n_k}^m \right\rangle \backsimeq \prod_{j=1}^{s} \left\langle \omega_{m_j}^m \right\rangle$$

On utilise alors le fait que si dans un groupe un élément ω est d'ordre p, l'élément ω^m est d'ordre $p' = \dfrac{p}{\operatorname{pgcd}(m,p)}$ (en effet, en notant $\delta = \operatorname{pgcd}(m,p)$, on a $p = \delta p'$, $m = \delta m'$, avec $\operatorname{pgcd}(m', p') = 1$ et pour tout entier k, l'égalité $(\omega^m)^k = 1$ équivaut à $km = \alpha p$, soit à $km' = \alpha p'$ ce qui revient à dire que p' divise k puisque $\operatorname{pgcd}(m', p') = 1$, donc $p' = \theta(\omega^m)$).

On a donc l'égalité des cardinaux :

$$\prod_{k=1}^{r} \frac{n_k}{\operatorname{pgcd}(m, n_k)} = \prod_{j=1}^{s} \frac{m_j}{\operatorname{pgcd}(m, m_j)}$$

pour tout entier $m \geq 1$.

De l'égalité $\prod_{k=1}^{r} n_k = \prod_{j=1}^{s} m_j$, on déduit les égalités $\prod_{k=1}^{r} \operatorname{pgcd}(m, n_k) = \prod_{j=1}^{s} \operatorname{pgcd}(m, m_j)$ pour tout $m \geq 1$, ce qui équivaut à l'unicité de la suite $(n_k)_{1\leq k\leq r}$. ■

La suite $(n_k)_{1\leq k\leq r}$ est la suite des invariants de G et elle caractérise G à isomorphisme près.