HAX501X – Groupes et anneaux 1

CM4 15/09/2023

Clément Dupont

2. Étude de $\mathbb{Z}/n\mathbb{Z}$

3. Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

3.1 Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ engendrés par un élément

3.2 Une vision axiomatique des sous-groupes

2. Étude de $\mathbb{Z}/n\mathbb{Z}$

3. Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

3.1 Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ engendrés par un élément

3.2 Une vision axiomatique des sous-groupes

Retour sur les exercices du cours

Exercice 17

Écrire la table de multiplication de $\mathbb{Z}/7\mathbb{Z}$.

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Exercice 18

Montrer que $\overline{13}$ est inversible dans $\mathbb{Z}/57\mathbb{Z}$ et calculer son inverse.

- Comme $13 \wedge 57 = 1$ (par exemple parce que 13 est premier et ne divise pas 57), $\overline{13}$ est inversible dans $\mathbb{Z}/57\mathbb{Z}$.
- L'algorithme d'Euclide étendu donne une relation de Bézout :

$$-57 \times 5 + 13 \times 22 = 1.$$

- On a donc, dans $\mathbb{Z}/57\mathbb{Z}$:

$$\overline{13 \times 22} = \overline{1},$$

d'où

$$\overline{13} \times \overline{22} = \overline{1}$$

et donc

$$\overline{13}^{-1} = \overline{22}.$$

Exercice 19

Calculer les inverses de $\overline{1}, \ldots, \overline{12}$ dans $\mathbb{Z}/13\mathbb{Z}$.

- On a $\overline{1} \times \overline{1} = \overline{1}$ donc $\overline{1}^{-1} = \overline{1}$.
- On a $\overline{2} \times \overline{7} = \overline{14} = \overline{1}$ donc $\overline{2}^{-1} = \overline{7}$ et $\overline{7}^{-1} = \overline{2}$.
- On a $\overline{3} \times \overline{9} = \overline{27} = \overline{1}$ donc $\overline{3}^{-1} = \overline{9}$ et $\overline{9}^{-1} = \overline{3}$.
- On a $\overline{4} \times \overline{10} = \overline{40} = \overline{1}$ donc $\overline{4}^{-1} = \overline{10}$ et $\overline{10}^{-1} = \overline{4}$.
- On a $\overline{5} \times \overline{8} = \overline{40} = \overline{1}$ donc $\overline{5}^{-1} = \overline{8}$ et $\overline{8}^{-1} = \overline{5}$.
- On a $\overline{6} \times \overline{11} = \overline{66} = \overline{1}$ donc $\overline{6}^{-1} = \overline{11}$ et $\overline{11}^{-1} = \overline{6}$.
- On a $\overline{12} = \overline{-1}$ et donc $\overline{12} \times \overline{12} = \overline{-1} \times \overline{-1} = \overline{1}$ donc $\overline{12}^{-1} = \overline{12}$.

Exercice 20

Soit p un nombre premier. Montrer qu'on a, pour tous $\overline{a}, \overline{b} \in \mathbb{Z}/p\mathbb{Z}$:

$$\overline{a} \times \overline{b} = \overline{0} \iff (\overline{a} = \overline{0} \text{ ou } \overline{b} = \overline{0}).$$

Montrer que cette propriété est fausse dans $\mathbb{Z}/n\mathbb{Z}$ si n est composé.

- L'implication $\Longleftarrow$ est évidente. Réciproquement, supposons que $\overline{a} \times \overline{b} = \overline{0}$. On veut montre que $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$. Supposons que $\overline{a} \neq \overline{0}$. Alors comme $\mathbb{Z}/p\mathbb{Z}$ est un corps (vu que p est premier), $\overline{a}$ est inversible et en multipliant l'égalité $\overline{a} \times \overline{b} = \overline{0}$ par $\overline{a}^{-1}$ on obtient $\overline{b} = \overline{0}$.
- On peut aussi revenir aux définitions. Vu que $\overline{a} \times \overline{b} = \overline{ab}$, l'équivalence à démontrer peut s'écrire :

$$p|ab \iff (p|a \text{ ou } p|b).$$

C'est le lemme d'Euclide !

- Si n est composé on peut écrire $n = ab$ avec $1 < a, b < n$. On a alors $\overline{a} \neq \overline{0}$, $\overline{b} \neq \overline{0}$, et $\overline{a} \times \overline{b} = \overline{ab} = \overline{n} = \overline{0}$.

Exercice 21

Soit n un nombre composé. Montrer que $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps, c'est-à-dire qu'il existe un élément $\neq \overline{0}$ dans $\mathbb{Z}/n\mathbb{Z}$ qui n'est pas inversible.

Si n est composé on peut écrire $n = ab$ avec $1 < a, b < n$. Par le même calcul que précédemment, on a $\overline{a} \neq \overline{0}$, $\overline{b} \neq \overline{0}$, et $\overline{a} \times \overline{b} = \overline{0}$.

Si $\overline{a}$ était inversible dans $\mathbb{Z}/n\mathbb{Z}$ alors en multipliant l'égalité $\overline{a} \times \overline{b} = \overline{0}$ par $\overline{a}^{-1}$ on obtiendrait $\overline{b} = \overline{0}$, ce qui serait une contradiction. Donc $\overline{a}$ est $\neq \overline{0}$ et n'est pas inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 22

1) Pour $n = 1, \ldots, 12$, lister les inversibles de $\mathbb{Z}/n\mathbb{Z}$ et calculer $\varphi(n)$.
2) Pour un nombre premier p, calculer $\varphi(p)$.
3) Pour un nombre premier p et un entier $r \geqslant 1$, calculer $\varphi(p^r)$.

1) On a $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$, $\varphi(9) = 6$, $\varphi(10) = 4$, $\varphi(11) = 10$, $\varphi(12) = 4$. Par exemple, les éléments inversibles de $\mathbb{Z}/12\mathbb{Z}$ sont $\overline{1}$, $\overline{5}$, $\overline{7}$, $\overline{11}$.

2) Pour p premier, les inversibles de $\mathbb{Z}/p\mathbb{Z}$ sont tous les éléments $\neq \overline{0}$. (Ou dit autrement, les $k \in \{1, \ldots, p\}$ qui sont premiers avec p sont $1, \ldots, p-1$.) Donc $\varphi(p) = p - 1$.

3) Pour $k \in \mathbb{Z}$, $k \wedge p^r = 1$ si et seulement si k n'est pas divisible par p. Entre 1 et p^r il y a $p^r/p = p^{r-1}$ multiples de p, et donc

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

Exercice 23

Écrire explicitement l'application g dans le cas $m = 3$, $n = 4$, et vérifier qu'elle est bijective.

$\overline{k} \in \mathbb{Z}/12\mathbb{Z}$	$g(\overline{k}) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
$\overline{0}$	$(\widetilde{0}, \widehat{0})$
$\overline{1}$	$(\widetilde{1}, \widehat{1})$
$\overline{2}$	$(\widetilde{2}, \widehat{2})$
$\overline{3}$	$(\widetilde{0}, \widehat{3})$
$\overline{4}$	$(\widetilde{1}, \widehat{0})$
$\overline{5}$	$(\widetilde{2}, \widehat{1})$
$\overline{6}$	$(\widetilde{0}, \widehat{2})$
$\overline{7}$	$(\widetilde{1}, \widehat{3})$
$\overline{8}$	$(\widetilde{2}, \widehat{0})$
$\overline{9}$	$(\widetilde{0}, \widehat{1})$
$\overline{10}$	$(\widetilde{1}, \widehat{2})$
$\overline{11}$	$(\widetilde{2}, \widehat{3})$

Exercice 23

Faire de même dans le cas $m = 2$, $n = 4$, et montrer que dans ce cas-là elle n'est pas bijective.

$\overline{k} \in \mathbb{Z}/8\mathbb{Z}$	$g(\overline{k}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
$\overline{0}$	$(\widetilde{0}, \widehat{0})$
$\overline{1}$	$(\widetilde{1}, \widehat{1})$
$\overline{2}$	$(\widetilde{0}, \widehat{2})$
$\overline{3}$	$(\widetilde{1}, \widehat{3})$
$\overline{4}$	$(\widetilde{0}, \widehat{0})$
$\overline{5}$	$(\widetilde{1}, \widehat{1})$
$\overline{6}$	$(\widetilde{0}, \widehat{2})$
$\overline{7}$	$(\widetilde{1}, \widehat{3})$

Exercice 24

Déduire du théorème précédent et de l'exercice 22 la formule suivante pour l'indicatrice d'Euler :

$$\varphi(n) = n \times \prod_{\substack{p \text{ premier} \\ p|n}} \left(1 - \frac{1}{p}\right).$$

- Écrivons la décomposition de n comme produit de nombres premiers sous la forme
$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$$
où les p_i sont des nombres premiers deux à deux distincts ($p_i \neq p_j$ si $i \neq j$) et les r_i sont des entiers $\geqslant 1$.
- Pour $i \neq j$ on a $p_i^{r_i} \wedge p_j^{r_j} = 1$ et donc on peut appliquer la multiplicativité de la caractéristique d'Euler :
$$\varphi(n) = \varphi(p_1^{r_1})\varphi(p_2^{r_2}) \cdots \varphi(p_k^{r_k}).$$
- On a calculé, pour un nombre premier p et un entier $r \geqslant 1$:
$$\varphi(p^r) = p^r - p^{r-1} = p^r(1 - \tfrac{1}{p}).$$
On obtient donc :
$$\begin{aligned}\varphi(n) &= p_1^{r_1}\left(1 - \tfrac{1}{p_1}\right) p_2^{r_2}\left(1 - \tfrac{1}{p_2}\right) \cdots p_k^{r_k}\left(1 - \tfrac{1}{p_k}\right) \\ &= n\left(1 - \tfrac{1}{p_1}\right)\left(1 - \tfrac{1}{p_2}\right) \cdots \left(1 - \tfrac{1}{p_k}\right) \\ &= n \times \prod_{\substack{p \text{ premier} \\ p|n}} \left(1 - \tfrac{1}{p}\right).\end{aligned}$$

Définition

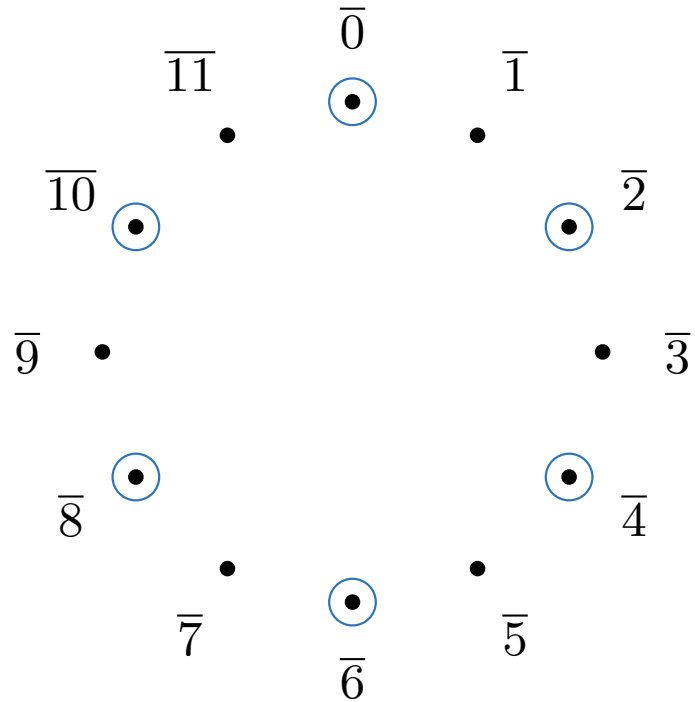
Définition

Soit $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Le **sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par $\overline{a}$** *est le sous-ensemble formé par les classes des multiples de a dans $\mathbb{Z}/n\mathbb{Z}$:*

$$\langle \overline{a} \rangle = \{\overline{ka}\,,\ k \in \mathbb{Z}\}.$$

Exemple

Dans $\mathbb{Z}/12\mathbb{Z}$ on a $\langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}$.



Le cas d'un diviseur de n

On commence par étudier le cas où a est un diviseur de n.

Proposition

Soit $d \in \mathbb{N}^*$ un diviseur de n et notons $e = \frac{n}{d}$ le "diviseur complémentaire".

1) *Le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par $\overline{d}$ est un ensemble à e éléments :*

$$\langle\, \overline{d}\,\rangle = \{\overline{0}, \overline{d}, \overline{2d}, \overline{3d}, \ldots, \overline{(e-1)d}\}.$$

(Remarquer que $\overline{ed} = \overline{n} = \overline{0}$.)

2) *Plus précisément, on a une bijection :*

$$\mathbb{Z}/e\mathbb{Z} \longrightarrow \langle\, \overline{d}\,\rangle \quad , \quad \widetilde{k} \mapsto \overline{kd}.$$

(Où l'on utilise la notation $\widetilde{k}$ pour les classes d'entiers dans $\mathbb{Z}/e\mathbb{Z}$ pour éviter la confusion avec la notation $\overline{k}$ qui correspond aux classes d'entiers dans $\mathbb{Z}/n\mathbb{Z}$.)

3) *Pour $d, d' \in \mathbb{N}^*$ deux diviseurs de n, on a : $\langle\, \overline{d}\,\rangle = \langle\, \overline{d'}\,\rangle \iff d = d'$.*

Exemple

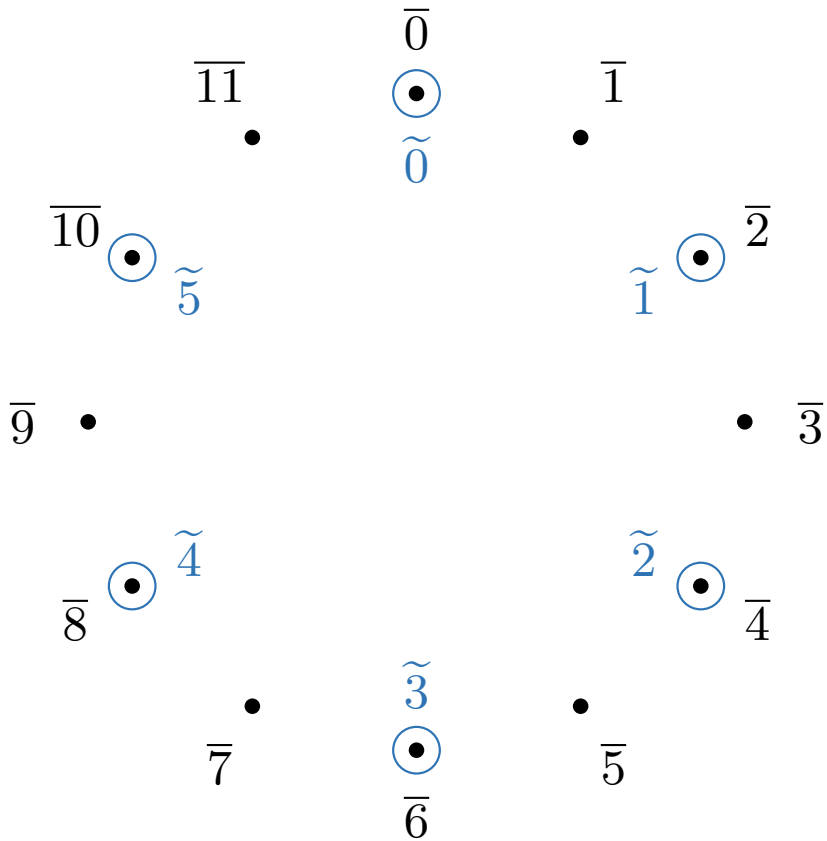
Soit $n = 12$ et $d = 2$, d'où $e = 6$.

1) Le sous-groupe de $\mathbb{Z}/12\mathbb{Z}$ engendré par $\overline{2}$ est

$$\langle\, \overline{2}\,\rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}.$$

2) On a une bijection

$$\mathbb{Z}/6\mathbb{Z} \longrightarrow \langle\, \overline{2}\,\rangle \quad , \quad \widetilde{k} \mapsto \overline{2k}.$$



Un autre exemple

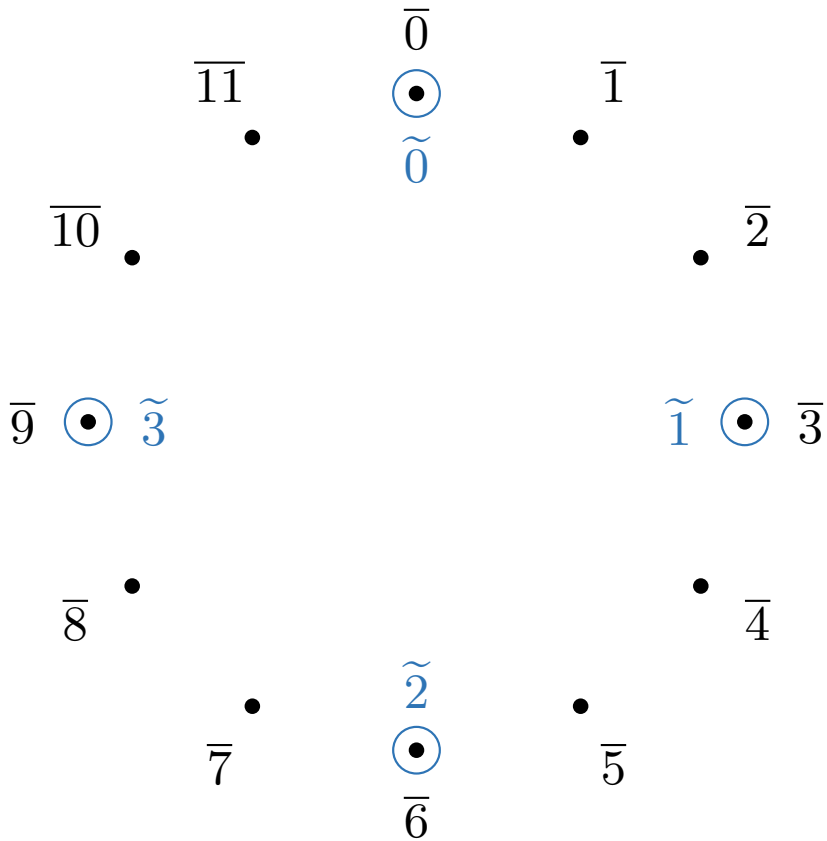
Soit $n = 12$ et $d = 3$, d'où $e = 4$.

1) Le sous-groupe de $\mathbb{Z}/12\mathbb{Z}$ engendré par $\overline{3}$ est

$$\langle \overline{3} \rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}.$$

2) On a une bijection

$$\mathbb{Z}/4\mathbb{Z} \longrightarrow \langle \overline{3} \rangle \quad , \quad \widetilde{k} \mapsto \overline{3k}.$$



Deux remarques

Remarque

Cas particuliers "extrêmes" $d = 1$ et $d = n$: $\langle \overline{1} \rangle = \mathbb{Z}/n\mathbb{Z}$ et $\langle \overline{n} \rangle = \{\overline{0}\}$.

Remarque

On verra au chapitre suivant que la bijection

$$g : \mathbb{Z}/e\mathbb{Z} \longrightarrow \langle \overline{d} \rangle$$

est un **isomorphisme de groupes** au sens où il respecte les lois $+$. En effet, on a pour tous $\widetilde{k}, \widetilde{l} \in \mathbb{Z}/e\mathbb{Z}$:

$$g(\widetilde{k} + \widetilde{l}) = g(\widetilde{k + l}) = \overline{(k + l)d} = \overline{kd + ld} = \overline{kd} + \overline{ld} = g(\widetilde{k}) + g(\widetilde{l}).$$

Le cas général

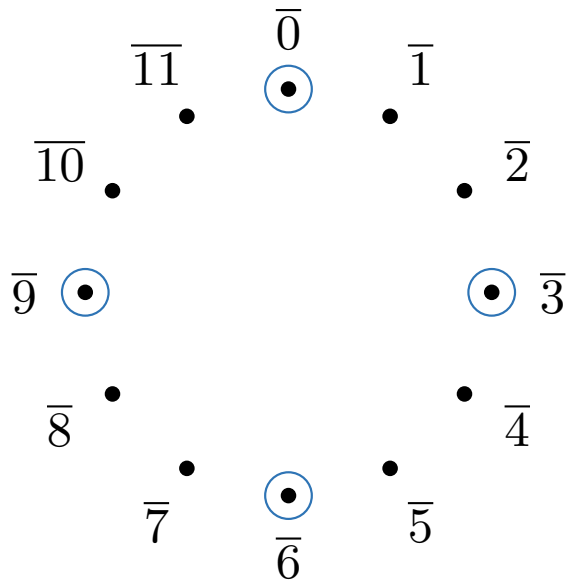
Proposition

1) *Soit* $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ *et notons* $d = a \wedge n$. *Alors* $\langle \overline{a} \rangle = \langle \overline{d} \rangle$.
2) *Soient* $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$. *Alors on a :*

$$\langle \overline{a} \rangle = \langle \overline{b} \rangle \iff a \wedge n = b \wedge n.$$

Exemple

Le sous-groupe de $\mathbb{Z}/12\mathbb{Z}$ engendré par $\overline{9}$ est le même que celui engendré par $\overline{3}$ puisque $9 \wedge 12 = 3$: $\langle \overline{9} \rangle = \langle \overline{3} \rangle$.



Le cas général

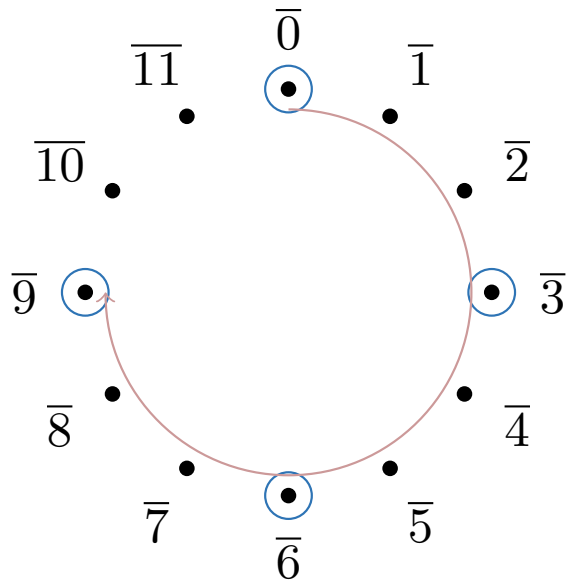
Proposition

1) *Soit* $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ *et notons* $d = a \wedge n$. *Alors* $\langle \overline{a} \rangle = \langle \overline{d} \rangle$.
2) *Soient* $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$. *Alors on a :*

$$\langle \overline{a} \rangle = \langle \overline{b} \rangle \iff a \wedge n = b \wedge n.$$

Exemple

Le sous-groupe de $\mathbb{Z}/12\mathbb{Z}$ engendré par $\overline{9}$ est le même que celui engendré par $\overline{3}$ puisque $9 \wedge 12 = 3$: $\langle \overline{9} \rangle = \langle \overline{3} \rangle$.



Le cas général

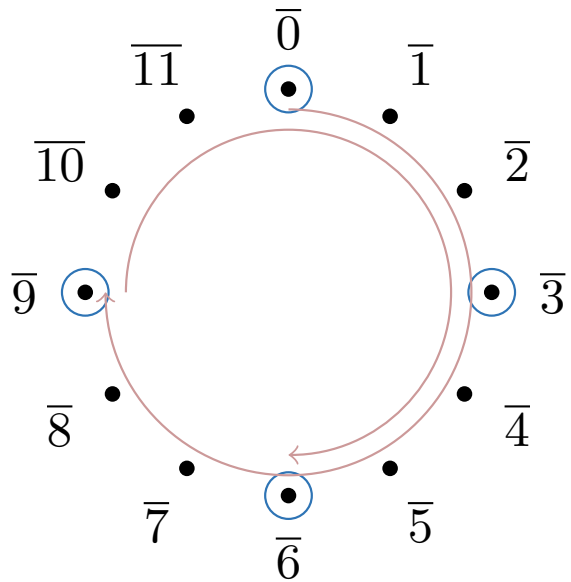
Proposition

1) *Soit* $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ *et notons* $d = a \wedge n$. *Alors* $\langle \overline{a} \rangle = \langle \overline{d} \rangle$.
2) *Soient* $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$. *Alors on a :*

$$\langle \overline{a} \rangle = \langle \overline{b} \rangle \iff a \wedge n = b \wedge n.$$

Exemple

Le sous-groupe de $\mathbb{Z}/12\mathbb{Z}$ engendré par $\overline{9}$ est le même que celui engendré par $\overline{3}$ puisque $9 \wedge 12 = 3$: $\langle \overline{9} \rangle = \langle \overline{3} \rangle$.



Le cas général

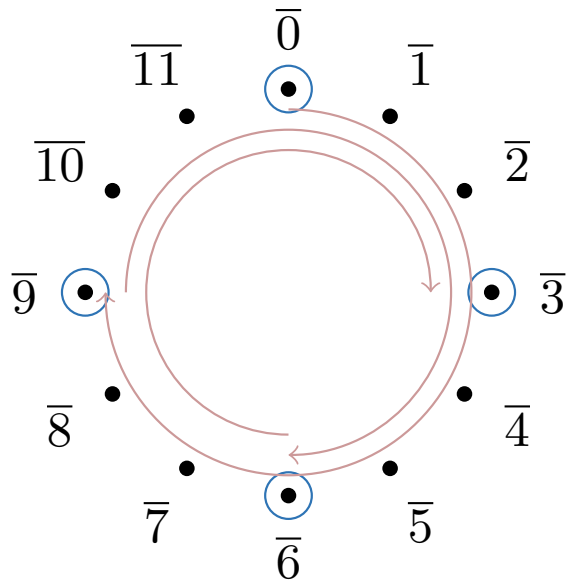
Proposition

1) *Soit* $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ *et notons* $d = a \wedge n$. *Alors* $\langle \overline{a} \rangle = \langle \overline{d} \rangle$.
2) *Soient* $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$. *Alors on a :*

$$\langle \overline{a} \rangle = \langle \overline{b} \rangle \iff a \wedge n = b \wedge n.$$

Exemple

Le sous-groupe de $\mathbb{Z}/12\mathbb{Z}$ engendré par $\overline{9}$ est le même que celui engendré par $\overline{3}$ puisque $9 \wedge 12 = 3$: $\langle \overline{9} \rangle = \langle \overline{3} \rangle$.



Le cas général

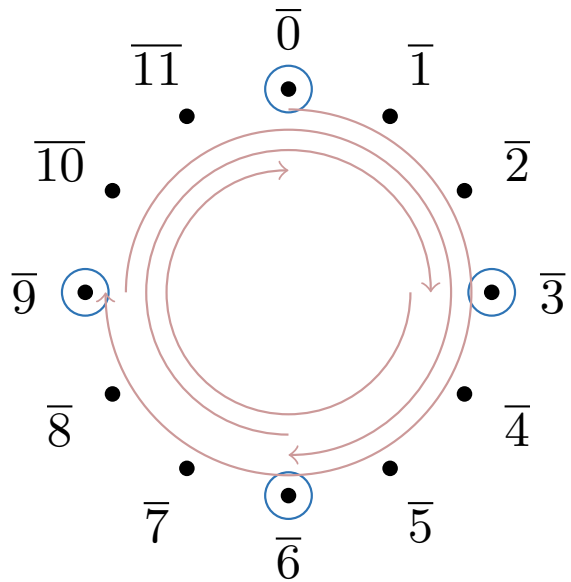
Proposition

1) *Soit* $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ *et notons* $d = a \wedge n$. *Alors* $\langle \overline{a} \rangle = \langle \overline{d} \rangle$.
2) *Soient* $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$. *Alors on a :*

$$\langle \overline{a} \rangle = \langle \overline{b} \rangle \iff a \wedge n = b \wedge n.$$

Exemple

Le sous-groupe de $\mathbb{Z}/12\mathbb{Z}$ engendré par $\overline{9}$ est le même que celui engendré par $\overline{3}$ puisque $9 \wedge 12 = 3$: $\langle \overline{9} \rangle = \langle \overline{3} \rangle$.



Générateurs de $\mathbb{Z}/n\mathbb{Z}$

- Cas particulier de la proposition précédente : pour $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ on a :

$$\langle \overline{a} \rangle = \mathbb{Z}/n\mathbb{Z} \quad \Longleftrightarrow \quad a \wedge n = 1.$$

Définition

Un élément $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\langle \overline{a} \rangle = \mathbb{Z}/n\mathbb{Z}$ est appelé un **générateur** *de $\mathbb{Z}/n\mathbb{Z}$.*

- Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont donc aussi, d'après une proposition déjà vue, les inversibles de $\mathbb{Z}/n\mathbb{Z}$.
- Ils sont donc au nombre de $\varphi(n)$.

Deux exercices

Exercice 25

Pour $n = 12$, quels sont les générateurs de $\mathbb{Z}/12\mathbb{Z}$? Pour chacun de ces générateurs, vérifiez que vous avez compris ce que cela veut dire en faisant tourner les aiguilles d'une horloge.

Exercice 26

Supposons que toutes les années ont 365 jours. Ma comète préférée passe à proximité de la Terre tous les 146 jours. Y aura-t-il une année où elle passera un 14 juillet ? Le résultat change-t-il si la comète passe à proximité de la Terre tous les 147 jours ?

Définition

Dans le chapitre suivant on prendra un point de vue plus axiomatique sur les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ (comparer la définition suivante avec la définition de la notion de sous-groupe de $\mathbb{Z}$).

Définition

Un **sous-groupe de** $\mathbb{Z}/n\mathbb{Z}$ *est un sous-ensemble* $H \subset \mathbb{Z}/n\mathbb{Z}$ *qui vérifie les conditions suivantes :*

1) $\overline{0} \in H$;
2) H *est stable par somme :* $\forall \overline{a}, \overline{b} \in H,\ \overline{a} + \overline{b} \in H$;
3) H *est stable par passage à l'opposé :* $\forall \overline{a} \in H,\ -\overline{a} \in H$.

Proposition

Pour tout $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, $\langle \overline{a} \rangle$ *est bien un sous-groupe de* $\mathbb{Z}/n\mathbb{Z}$.

Démonstration. Laissé au lecteur en exercice (faites-le !). □

Classification des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

Proposition

Soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. Alors il existe un unique diviseur positif d de n tel que $H = \langle \overline{d} \rangle$.

Démonstration. On a déjà vu l'unicité, démontrons l'existence. On définit

$$H' = \{k \in \mathbb{Z} \mid \overline{k} \in H\} \quad \subset \mathbb{Z}.$$

On montre (faites-le !) que H' est un sous-groupe de $\mathbb{Z}$. Le théorème de classification des sous-groupes de $\mathbb{Z}$ implique donc qu'il existe un entier $d \in \mathbb{N}$ tel que $H' = d\mathbb{Z}$. On en déduit que $H = \langle \overline{d} \rangle$. On prouve enfin que d divise n : comme $\overline{n} = \overline{0} \in H$, on a que $n \in H' = d\mathbb{Z}$, donc d divise n. □