

TD 4

Exo 1 : $x = \text{âge de Hervé}$

On sait que :

$$\left. \begin{array}{l} x = k_1 \cdot 17 + 16 \\ x = k_2 \cdot 16 + 4 \\ x = k_3 \cdot 6 \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} x \equiv 16 \pmod{17} \\ x \equiv 4 \pmod{16} \\ x \equiv 0 \pmod{6} \end{array} \right.$$

On peut appliquer l'algorithme des restes chinois.

On note que $x \equiv 4 \pmod{16} \Rightarrow x = 16k_2 + 4$
 $\Rightarrow x \equiv 0 \pmod{4}$.

Donc il suffit de résoudre le système :

$$\left\{ \begin{array}{l} x \equiv 16 \pmod{17} \\ x \equiv 0 \pmod{4} \end{array} \right. \Rightarrow x \equiv 52 \pmod{16 \cdot 17}$$

Exo 2 : $\exists z \in \mathbb{Z}$ tel que $\left\{ \begin{array}{l} z \equiv a_1 \pmod{n_1} \\ z \equiv a_2 \pmod{n_2} \end{array} \right.$

 $\Leftrightarrow a_1 \equiv a_2 \pmod{\text{pgcd}(n_1, n_2)}$

(Cas d'un système de congruences où les n_i ne sont pas à deux à deux premiers entre eux)

Exo 3: $n_1, \dots, n_k \in \mathbb{Z}$, $\text{pgcd}(n_i, n_j) = 1$, $\forall i \neq j$. $N = \frac{\prod_{i=1}^k n_i}{\text{lcm}}.$

$$\Theta: \frac{\mathbb{Z}}{N\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{n_k\mathbb{Z}}$$

$$[a]_N \longmapsto ([a]_{n_1}, \dots, [a]_{n_k})$$

Rappel :

$$[a]_N = [b]_N \iff a \equiv b \pmod N \iff$$

$$\iff N \mid a - b$$

$$\iff \exists h \in \mathbb{Z} \text{ t.q. } a - b = hN.$$

a) Montrer que Θ est bien définie, c'est-à-dire montrer que si $x_1, x_2 \in \mathbb{Z}$ sont tels que $[x_1]_N = [x_2]_N$, alors $\Theta([x_1]_N) = \Theta([x_2]_N)$.

Soient $x_1, x_2 \in \mathbb{Z}$ tels que $[x_1]_N = [x_2]_N$ alors $\exists h \in \mathbb{Z}$ tels que $x_1 = x_2 + hN = x_2 + h(n_1 \dots n_k) = x_2 + \underbrace{(h n_1 \dots n_k)}_{\in \mathbb{Z}} \cdot n_1 \Rightarrow x_1 \equiv x_2 \pmod{n_1} \Rightarrow [x_1]_{n_1} = [x_2]_{n_1}$

De la même façon on montre que $[x_1]_{n_i} = [x_2]_{n_i}$, $\forall i = 2, \dots, k$.

On en déduit que $([x_1]_{n_1}, \dots, [x_1]_{n_k}) = ([x_2]_{n_1}, \dots, [x_2]_{n_k})$
 $\Rightarrow \Theta([x_1]_N) = \Theta([x_2]_N)$.

b) Montrer que Θ est une bijection, c'est-à-dire montrer que Θ est injective et surjective.

Rappel : $f: A \rightarrow B$ une application

- f est injective si

$$\forall x, y \in A, f(x) = f(y) \Rightarrow x = y$$

$$x \neq y \Rightarrow f(x) \neq f(y)$$

- f est surjective si

$$\forall y \in B, \exists x \in A \text{ t.q. } f(x) = y.$$

Montrons que θ est injective :

Soient $[x_1]_N, [x_2]_N \in \mathbb{Z}/N\mathbb{Z}$, tels que

$$\theta([x_1]_N) = \theta([x_2]_N) \Rightarrow ([x_1]_{n_1}, \dots, [x_1]_{n_k}) = ([x_2]_{n_1}, \dots, [x_2]_{n_k})$$

$$\Rightarrow \forall i=1, \dots, k \quad [x_1]_{n_i} = [x_2]_{n_i} \Rightarrow x_1 \equiv x_2 \pmod{n_i} \forall i$$

$$\Rightarrow n_i \mid (x_1 - x_2), \forall i \Rightarrow \prod_{i=1}^k n_i \mid (x_1 - x_2) \Rightarrow$$

\uparrow

$\text{pgcd}(n_i, n_j) = 1 \quad \text{et} \quad \prod_{i=1}^k n_i = N$

$\forall i \neq j$

$$\Rightarrow x_1 \equiv x_2 \pmod{N} \Rightarrow [x_1]_N = [x_2]_N.$$

Pour la surjectivité on rappelle que :

Si $f: A \rightarrow B$ est injective et $|A| = |B| < \infty$

$\Rightarrow f$ est surjective.

Dans notre cas θ est injective et $\left| \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{n_k\mathbb{Z}} \right| = n_1 \dots n_k = N = \left| \frac{\mathbb{Z}}{N\mathbb{Z}} \right| \Rightarrow \theta$ est surjective.

c) Soient $\alpha, \beta \in \mathbb{Z}/N\mathbb{Z}$ et soient $\alpha_i, \beta_i \in \mathbb{Z}_{n_i \mathbb{Z}}$
tels que $\Theta(\alpha) = (\alpha_1, \dots, \alpha_K)$ et $\Theta(\beta) = (\beta_1, \dots, \beta_K)$.

① Montrer que $\Theta(\alpha + \beta) = (\alpha_1 + \beta_1, \dots, \alpha_K + \beta_K)$:

Soient $a, b \in \mathbb{Z}$ tels que $\alpha = [a]_N$ et $\beta = [b]_N$.

$$\begin{aligned} \text{Alors } \Theta(\alpha + \beta) &= \Theta([a]_N + [b]_N) = \Theta([a+b]_N) = \\ &= ([a+b]_{n_1}, \dots, [a+b]_{n_K}) = ([a]_{n_1} + [b]_{n_1}, \dots, [a]_{n_K} + [b]_{n_K}) = \\ &= (\alpha_1 + \beta_1, \dots, \alpha_K + \beta_K). \end{aligned}$$

② Montrer que $\Theta(\alpha \beta) = (\alpha_1 \beta_1, \dots, \alpha_K \beta_K)$:

Soient $a, b \in \mathbb{Z}$ tels que $\alpha = [a]_N$ et $\beta = [b]_N$.

$$\begin{aligned} \text{Alors } \Theta(\alpha \beta) &= \Theta([a]_N [b]_N) = \Theta([ab]_N) = \\ &= ([ab]_{n_1}, \dots, [ab]_{n_K}) = ([a]_{n_1} [b]_{n_1}, \dots, [a]_{n_K} [b]_{n_K}) \\ &= (\alpha_1 \beta_1, \dots, \alpha_K \beta_K). \end{aligned}$$

d) $\forall m \geq 0$, montrer que $\Theta(\alpha^m) = (\alpha_1^m, \dots, \alpha_K^m)$.

Cela découle directement du point c :

$$\begin{aligned} \Theta(\alpha^m) &= \Theta(\underbrace{\alpha \cdots \alpha}_m \text{ fois}) = \underbrace{(\alpha_1 \cdots \alpha_1, \dots, \alpha_K \cdots \alpha_K)}_m \text{ fois} = \\ &= (\alpha_1^m, \dots, \alpha_K^m) \stackrel{(c)}{=} \end{aligned}$$

e) Montrer que α est inversible si et seulement si α_i est inversible.

Soit $a \in \mathbb{Z}$ tel que $\alpha = [a]_N$. Alors $\alpha_i = [a]_{n_i}$.

On montre de façon équivalente, que $\forall i=1, \dots, K$, $[a]_{n_i}$ est inversible si et seulement si $[a]_{n_i}$ est inversible.

\Rightarrow Soit $[a]_N$ inversible $\Rightarrow \exists z \in \mathbb{Z}$
 tel que $az = 1 \pmod N \Rightarrow \forall i=1,\dots,k$
 $az = 1 \pmod {n_i} \Rightarrow a$ est inversible
 $\pmod {n_i}$, c'est à dire $[a]_{n_i}$ est inversible
 dans $\mathbb{Z}/n_i\mathbb{Z}$.

\Leftarrow Supposons que $[a]_{n_i}$ est inversible pour tout i .
 $\Rightarrow \exists b_i \in \mathbb{Z}$ tel que $ab_i = 1 \pmod {n_i}, \forall i$.

Soit $b \in \mathbb{Z}$ tel que $\Theta([b]_N) = ([b]_{n_1}, \dots, [b]_{n_k})$

Alors on a :

$$\Theta([a]_N [b]_N) = ([ab_1]_{n_1}, \dots, [ab_k]_{n_k}) = ([1]_{n_1}, \dots, [1]_{n_k})$$

Mais aussi $\Theta([1]_N) = ([1]_{n_1}, \dots, [1]_{n_k})$. Puisque Θ est injective on en déduit que $[a]_N [b]_N = [1]_N$
 et donc que $[a]_N$ est inversible dans $\mathbb{Z}/N\mathbb{Z}$.

La démonstration de (\Leftarrow) implique aussi
 que :

$$\begin{aligned} \Theta(\alpha^{-1}) &= \Theta([a]_N^{-1}) = \Theta([b]_N) = ([b_1]_{n_1}, \dots, [b_k]_{n_k}) = \\ &= ([a]_{n_1}^{-1}, \dots, [a]_{n_k}^{-1}) = (\alpha_1^{-1}, \dots, \alpha_k^{-1}) \end{aligned}$$

Enfin on montre que l'application :

$$\begin{aligned} \varphi: (\mathbb{Z}/N\mathbb{Z})^\times &\longrightarrow (\mathbb{Z}/n_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})^\times \\ \alpha &\longmapsto (\alpha_1^{-1}, \dots, \alpha_k^{-1}) \end{aligned}$$

est une bijection.

INJECTIVITÉ : Soient $\alpha, \beta \in (\mathbb{Z}/N\mathbb{Z})^\times$ tels que

$$\varphi(\alpha) = \varphi(\beta) \Rightarrow (\alpha_1^{-1}, \dots, \alpha_k^{-1}) = (\beta_1^{-1}, \dots, \beta_k^{-1})$$

$$\Rightarrow \forall i=1, \dots, k \quad \alpha_i^{-1} = \beta_i^{-1} \Rightarrow$$

$$\Rightarrow \forall i=1, \dots, k \quad \alpha_i = \beta_i$$

Donc $\Theta(\alpha) = \Theta(\beta)$. Par injectivité de Θ on conclut que $\alpha = \beta$.

SURJECTIVITÉ : Soit $(x_1, \dots, x_k) \in (\mathbb{Z}/n_1\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/n_k\mathbb{Z})^\times$

et soit $x \in \mathbb{Z}/N\mathbb{Z}$ tel que $\Theta(x) = (x_1, \dots, x_k)$.

Mais x_i est inversible dans $\mathbb{Z}/n_i\mathbb{Z}$, $\forall i$, donc x est inversible aussi dans $\mathbb{Z}/N\mathbb{Z}$.

STRUCTURES ALGÉBRIQUES : Groupes

Def: Un groupe est un couple (G, \star) où G est un ensemble et \star est une opération binaire interne.

$$\begin{aligned}\star: G \times G &\longrightarrow G \\ (a, b) &\longmapsto a \star b\end{aligned}$$

[Opération interne: $\forall a, b \in G, a \star b \in G$]

telle que :

- (1) $\forall a, b, c \in G, a \star (b \star c) = (a \star b) \star c$
(associativité)
- (2) $\exists e \in G$ tel que, $\forall a \in G, a \star e = e \star a = a$
(élément neutre)
- (3) $\forall a \in G, \exists b \in G$ tel que $a \star b = b \star a = e$
(inverse pour tout élément)

Un groupe est abélien ou commutatif si en plus, $\forall a, b \in G, a \star b = b \star a$ (commutativité).

On parle de groupe additif si $\star = +$ et de groupe multiplicatif si $\star = \cdot$.

Exemples

1) $(\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{Z}/n\mathbb{Z}, +)$

$$G = \{f: \mathbb{R} \rightarrow \mathbb{R}, f \text{ bijective}\}, \quad \begin{aligned}G \times G &\longrightarrow G \\ (f, g) &\longmapsto f \circ g\end{aligned}$$

Oui, (G, \circ) est un groupe.

2) (\mathbb{Z}, \cdot) n'est pas un groupe car 0 n'est pas inversible

Même chose pour (\mathbb{R}, \cdot) , (\mathbb{Q}, \cdot) , (\mathbb{C}, \cdot) .

3) $(\{-1, 1\}, \cdot)$, où $\cdot : \{-1, 1\} \times \{-1, 1\} \rightarrow \{-1, 1\}$

$$\begin{array}{ccc} (\pm 1, \pm 1) & \mapsto & \pm 1 \\ (-1, -1) & \mapsto & -1 \\ (1, -1) & \mapsto & -1 \\ (-1, 1) & \mapsto & 1 \end{array}$$

est un groupe.

$(\mathbb{R} \setminus \{0\}, \cdot)$ est un groupe

$(\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ est un groupe.

Proposition: Soit (G, \star) un groupe. Alors:

1) G possède un unique élément neutre

2) $\forall a \in G$, il existe un unique inverse, note a^{-1} .

3) Si $a \star b = a \star c \Rightarrow b = c$.

4) $(ab)^{-1} = b^{-1} \star a^{-1}$, $\forall a, b \in G$.

A partir de maintenant on utilise la notation multiplicative:

1_G : élément neutre

$g^n := \underbrace{g \cdot \dots \cdot g}_{n \text{ fois}}$, $\forall n \in \mathbb{Z}_{>0}$

$g^0 = 1_G$ n fois

$g^{-n} := \underbrace{g^{-1} \cdot \dots \cdot g^{-1}}_{n \text{ fois}}$, $\forall n \in \mathbb{Z}_{>0}$.

Def: L'ordre d'un groupe (G, \cdot) , noté $|G|$, est le nombre d'éléments de G , qui est soit un entier >0 , soit ∞ .
 Un groupe d'ordre fini est appelé un groupe fini.

Théorème de Lagrange (version 1)

Soit (G, \cdot) un groupe abélien fini d'ordre n .
 Alors $\forall g \in G, g^n = 1_G$.

Démon

Soit $g \in G$ et on considère $A = \{gh, h \in G\}$.
 On montre que $A = G$.

Il est clair que $A \subseteq G$. Il suffit alors de montrer que $|A| = |G|$.

Si $gh_1 = gh_2$, $h_1, h_2 \in G \Rightarrow h_1 = h_2 \Rightarrow |A| = |G|$.
 Loi d'annulation

$$\Rightarrow A = G$$

On a alors que :

$$\underset{h \in G}{\prod} h = \prod_{h \in G} (hg) = g^n \underset{h \in G}{\prod} h \Rightarrow g^n = 1_G.$$

Def: Soit (G, \cdot) un groupe. Un sous-ensemble $H \subseteq G$ est un sous-groupe si (H, \cdot) est un groupe. Si H est un sous-ensemble de G on écrit $H \leq G$.

Exemples

1) Soit (G, \cdot) un groupe.

$\{1_G\}$ et G sont toujours deux sous-groupes de G .
(sous-groupes triviaux)

2) $G = (\mathbb{Z}, +)$

$2\mathbb{Z} = \{2k, k \in \mathbb{Z}\} \subset \mathbb{Z}$ est un sous-groupe non-trivial de \mathbb{Z} .

Plus en général, $\forall n \in \mathbb{Z}_{\geq 0}$, le sous-ensemble
 $n\mathbb{Z} := \{nk, k \in \mathbb{Z}\}$ (**multiples de n**)

est un sous-groupe de \mathbb{Z} :

- associativité induite de l'assoc. dans \mathbb{Z}
- $0 = n \cdot 0 \Rightarrow 0 \in n\mathbb{Z}$
- Soit $a \in n\mathbb{Z} \Rightarrow a = nk, k \in \mathbb{Z}$. Alors $-a = n \cdot (-k) \in n\mathbb{Z}$.

Proposition : Soit (G, \cdot) un groupe.

Un sous-ensemble non vide $H \subseteq G$

est un sous-groupe de G si et seulement si

$\forall a, b \in H, ab^{-1} \in H$.

Démonstration \Leftarrow (l'implication \Rightarrow est triviale)

Si $H = \{1_G\}$ c'est vrai.

Sinon $\exists a \in H, a \neq 1_G$.

Alors $a \cdot a^{-1} = 1_G \in H$.

Maintenant $1_G, a \in H \Rightarrow 1_G \cdot a^{-1} = a^{-1} \in H$.

Enfin si $a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a \cdot (b^{-1})^{-1} = ab \in H$.

L'associativité dans G découle de l'associativité dans H .

Def: Soit (G, \cdot) un groupe et soit $a \in G$.
L'ensemble

$$\langle a \rangle := \{a^n, n \in \mathbb{Z}\}$$

est un sous-groupe de G , appelé le sous-groupe engendré par a .

Déns: Soit $g_1, g_2 \in \langle a \rangle \Rightarrow \exists n, m \in \mathbb{Z}$ tels que
 $g_1 = a^n, g_2 = a^m \Rightarrow g_1 \cdot (g_2)^{-1} = a^n \cdot (a^m)^{-1} =$
 $= a^n \cdot a^{-m} = a^{n-m} \in \langle a \rangle$.
Donc $\langle a \rangle$ est un sous-groupe de G .

Def: Un groupe (G, \cdot) est dit cyclique s'il existe $g \in G$ tel que $G = \langle g \rangle$.

L'élément g est dit un générateur de G .

Def: Soit (G, \cdot) un groupe et $a \in G$.

L'ordre de a , noté $\text{ord}(a)$, est l'ordre du sous-groupe $\langle a \rangle$. C'est le plus petit entier $k > 0$ tel que $a^k = f_G$.