

Chapitre I : Structures algébriques usuelles

On suppose connues la définition et les propriétés principales des ensembles de nombres \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} , et \mathbb{C} .

Si E, F sont deux ensembles, on appelle que le produit cartésien $E \times F$ est l'ensemble :

$$E \times F = \{(e, f); e \in E, f \in F\}$$

(ensemble des paires d'éléments de E et F).

1) Lois de composition internes

Déf: Soit E un ensemble. On appelle loi de composition interne dans E une application $* : E \times E \rightarrow E$

$$(a, b) \mapsto a * b$$

En d'autres termes la loi de composition interne associe à toute paire (a, b) d'éléments de E un nouvel élément de E , noté ici $a * b$. On dit aussi que la loi $*$ est une opération sur E .

Exemples:

L'addition $+ : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ est une loi de composition interne dans \mathbb{N}

$$(m, m) \mapsto m + m$$

(et aussi dans $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et \mathbb{C}).

La multiplication $\cdot : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ est une loi de composition interne dans \mathbb{N}

$$(m, m) \mapsto m \cdot m$$

dans \mathbb{N} (et aussi dans $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, et \mathbb{C}).

Déf: Soit E un ensemble muni d'une loi de composition interne $*$.

On dit que:

- la loi est commutative si, $\forall a, b \in E$, on a $a * b = b * a$.
- la loi est associative si, $\forall a, b, c \in E$, on a $(a * b) * c = a * (b * c)$.

On dit que $e \in E$ est un élément neutre pour la loi $*$ si

$$\forall a \in E \text{ on a: } a * e = e * a = a.$$

Ex:

- L'addition $+$ sur \mathbb{N} (ou $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$) est commutative, associative, et 0 est un élément neutre.
- La multiplication \cdot sur \mathbb{N} (ou $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$) est commutative, associative, et 1 est un élément neutre.

Rapp: Si une loi $*$ dans E admet un élément neutre, celui-ci est nécessairement unique (\Rightarrow on l'appelle l'élément neutre). En effet, supposons que $e, e' \in E$ soient deux éléments neutres. Alors:

$$e = e * e' = e' \quad \Rightarrow \quad e = e'. \\ \begin{matrix} \uparrow & \uparrow \\ \text{car } e \text{ est neutre} & \text{car } e' \text{ est neutre} \end{matrix}$$

Déf: Soit E un ensemble muni d'une loi de composition interne $*$.

On dit qu'un sous-ensemble $F \subset E$ est stable par $*$ si

$$\forall a, b \in F \text{ on a } a * b \in F.$$

Ex: • $\mathbb{N} \subset \mathbb{Z}$ est stable par les lois $+$ et \cdot .

• $\mathbb{R}_+ = \{x \in \mathbb{R}; x \geq 0\} \subset \mathbb{R}$ est stable par les lois $+$ et \cdot . (et $\mathbb{R}-$?)

• $\mathbb{R} \subset \mathbb{C}$ est stable par les lois $+$ et \cdot .

2) Groupes

Déf: On appelle groupe un ensemble G muni d'une loi de composition interne $*$ possédant les propriétés suivantes:

- 1) La loi est associative: $\forall a, b, c \in G, a * (b * c) = (a * b) * c$
- 2) Il existe un élément neutre $e \in G$: $\forall a \in G, a * e = e * a = a$
- 3) Tout élément $a \in G$ possède un élément symétrique $a' \in G$ tel que $a * a' = a' * a = e$

On dit que $(G, *)$ est un groupe commutatif (ou abélien) si en outre

- 4) La loi est commutative: $\forall a, b \in G, a * b = b * a$.

Rem: (sur l'élément symétrique) On dit parfois que a' est l'inverse de a pour la loi $*$, mais cette terminologie peut prêter à confusion, cf. ci-dessous.
Il est clair que l'élément symétrique est unique:

Si $a * a' = a' * a = e$ et $a * a'' = a'' * a = e$,

alors

$$a'' = e * a'' = (a' * a) * a'' = a' * (a * a'') = a' * e = a'.$$

Exemple 1 (groupes de nombres additifs)

L'ensemble \mathbb{Z} muni de l'addition $+$ est un groupe abélien.

L'élément neutre est 0 , et le symétrique d'un entier $m \in \mathbb{Z}$ est

son opposé $m' = -m$: $m + (-m) = (-m) + m = 0$.

Si $m, n \in \mathbb{Z}$, on note usuellement $m - n := m + (-n)$.

De même, \mathbb{Q} , \mathbb{R} , et \mathbb{C} sont des groupes abéliens pour l'addition $+$, l'élément neutre étant 0 et le symétrique étant l'opposé.

⚠ $(\mathbb{N}, +)$ n'est pas un groupe!

Exemple 2 (groupes de nombres multiplicatifs)

L'ensemble $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ muni de la multiplication \cdot est un groupe abélien. L'élément neutre est 1, et le symétrique d'un rationnel non nul $x = \frac{p}{q}$ est son inverse $x^{-1} = \frac{q}{p}$.

Si $x, y \in \mathbb{Q}^*$, on note usuellement $\frac{x}{y} := x \cdot y^{-1}$ et $xy := x \cdot y$.

De même \mathbb{R}^* et \mathbb{C}^* sont des groupes abéliens pour la multiplication \cdot .

⚠ (\mathbb{Z}^*, \cdot) n'est pas un groupe!

Exemple 3 (groupe symétrique)

Soit E un ensemble et $G = \{f: E \rightarrow E; f \text{ est bijective}\}$.

On munit G de la loi de composition $f * g = f \circ g$, où \circ désigne la composition de deux applications:

$$\forall f, g \in G, \forall a \in E: (f \circ g)(a) = f(g(a)).$$

L'associativité est facile à vérifier. L'élément neutre est l'application identité $\text{Id}: E \rightarrow E$ t.q. $\text{Id}(a) = a \quad \forall a \in E$. Le symétrique d'une bijection $f \in G$ est l'application réciproque $f^{-1}: E \rightarrow E$.

L'ensemble G muni de la loi \circ forme donc un groupe, appelé groupe symétrique $S(E)$. Ce groupe n'est pas commutatif si E possède au moins trois éléments.

Si $E = \{1; 2; \dots; n\}$ possède n éléments, le groupe $S(E)$ est noté S_n .

Il possède exactement $n!$ éléments (= $n!$ de permutations de n objets).

Si $\sigma \in S_n$ est une permutation, on peut noter:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}.$$

Cas particulier $m=3$ (peut se faire en exercice)

$S_3 = \{ \text{Id}; \tau_1; \tau_2; \tau_3; c_1; c_2 \}$ avec

$$\text{Id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$c_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, c_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}. \quad \begin{cases} \tau_i = \text{transpositions} \\ c_i = \text{cycles} \end{cases}$$

On a

$$\tau_1^2 = \tau_1 \circ \tau_1 = \text{Id}, \text{ et de même } \tau_2^2 = \tau_3^2 = \text{Id}$$

$$c_1^2 = c_2, c_1^3 = \text{Id}, \text{ et de même } c_2^2 = c_3, c_2^3 = \text{Id}$$

¶ $c_1 \circ \tau_1 = \tau_3 \neq \tau_2 = \tau_1 \circ c_1$: S_3 n'est pas commutatif.

Remarques: (peuvent être placées avant)

- Un groupe $(G, *)$ est nécessairement non vide, puisqu'il contient l'élément neutre e de la loi $*$.
- Quel que soit $a \in G$, on a $\forall x, y \in G$ l'équivalence

$$a * x = a * y \iff x = y$$

\Rightarrow multiplier à gauche par a'

\Leftarrow multiplier à gauche par a

De même :

$$x * a = y * a \iff x = y \quad (\text{multiplication à droite})$$

- Quels que soient $a, b \in G$, l'équation $a * x = b$ d'inconnue x possède dans G la solution unique $x = a' * b$.
De même, l'unique solution de $x * a = b$ est $x = b * a'$.
- $\forall a, b \in G$, on a : $(a * b)' = b' * a'$, $(a')' = a$.

3) Sous-groupes et morphismes de groupes (facultatif?)

Déf: Soit $(G, *)$ un groupe. Une partie $H \subset G$ est un sous-groupe de G si elle possède les propriétés suivantes :

- i) $e \in H$
- ii) $\forall a, b \in H$ on a $a * b \in H$ (H est stable par $*$)
- iii) $\forall a \in H$, l'élément symétrique a' appartient à H .

Remarque : cette définition signifie exactement que H , muni de la loi $*$ (i.e. de la restriction à H de la loi $*$ sur G) est un groupe.

Proposition : une partie non vide $H \subset G$ est un sous-groupe si et seulement si

$$\forall a, b \in H \text{ on a } a * b' \in H. \quad (1)$$

Dém:

- 1) Si H est un sous-groupe, alors $\forall a, b \in H$ on a $b' \in H$ par iii), et donc $a * b' \in H$ par ii). Ainsi (1) est vrai.
- 2) Soit $H \subset G$ une partie non vide telle que (1) soit vrai.

Il existe $a \in H$ (car H non vide) et en appliquant (1) avec $b = a$ on trouve $e = a * a' \in H$. Ainsi i) est vérifié.

En appliquant ensuite (1) avec e, a au lieu de a, b on obtient $a' = e * a' \in H$ quel que soit $a \in H$. Ainsi iii) est vérifié.

En appliquant enfin (1) à la paire a, b' avec $a, b \in H$ on trouve $a * b = a * (b')' \in H$. Ainsi ii) est vérifié. \square

\uparrow car $b' \in H$ par iii)

Remarques:

Le plus petit sous-groupe de G est $H = \{e\}$, le plus grand est $H = G$, les sous-groupes non triviaux sont intermédiaires.

Si H_1, H_2 sont deux sous-groupes de G , on vérifie que $H = H_1 \cap H_2$ est encore un sous-groupe de G . Cette propriété se généralise à une intersection quelconque de sous-groupes de G .

Exemples:

1) $(G, *) = (\mathbb{R}, +)$. Étant donné $a > 0$, on définit

$$H = \{ma ; m \in \mathbb{Z}\}, \text{ et on note } H = a\mathbb{Z}. \quad \|$$

Clairement $0 \in H$ et si $ma, mb \in H$ alors

$$ma + (mb)' = ma + (-mb) = (m-m)a \in H. \quad (m, m' \in \mathbb{Z})$$

Par la proposition, H est un sous-groupe de $(\mathbb{R}, +)$. C'est manifestement le plus petit sous-groupe de $(\mathbb{R}, +)$ contenant l'élément a .

Rem: On peut montrer que les sous-groupes $a\mathbb{Z}$ sont les seuls sous-groupes "discrets" de $(\mathbb{R}, +)$. Tous les autres sous-groupes sont "obscurs" dans \mathbb{R} .

Par exemple, \mathbb{Q} est un sous-groupe de $(\mathbb{R}, +)$.

2) $(G, *) = (\mathbb{C}^*, \cdot)$. On considère le sous-ensemble

$$H = U := \{z \in \mathbb{C} ; |z| = 1\}. \quad \| \quad (\text{groupe unitaire})$$

On note que $1 \in U$, et que si $z_1, z_2 \in U$ alors $z_1 * z_2' = z_1 \cdot z_2^{-1} \in U$

$$\text{Car } |z_1 \cdot z_2^{-1}| = |z_1| \cdot |z_2^{-1}| = \frac{|z_1|}{|z_2|} = 1 \text{ puisque } |z_1| = |z_2| = 1.$$

Par la proposition, U est donc un sous-groupe de (\mathbb{C}^*, \cdot) .

Par ailleurs, étant donné $m \in \mathbb{N}^*$, on définit

$$U_m = \left\{ z \in \mathbb{C}; z^m = 1 \right\}. \quad \| \quad (\text{racines } m^{\text{èmes}} \text{ de l'unité})$$

On sait (cf. cours MAT101) que

$$U_m = \left\{ \exp\left(\frac{2ik\pi}{m}\right); k=0, \dots, m-1 \right\} \Rightarrow \text{Card}(U_m) = m.$$

On vérifie grâce à la proposition que U_m est un sous-groupe de \mathbb{U} , et donc également un sous-groupe de (\mathbb{C}^*, \cdot) .

Déf: Soient $(G, *)$ et (\tilde{G}, \times) deux groupes. On dit qu'une application $f: G \rightarrow \tilde{G}$ est un morphisme de groupes si

$$\forall a, b \in G: f(a * b) = f(a) \times f(b). \quad (2)$$

\uparrow loi de G \uparrow loi de \tilde{G}

Proposition: Si $f: G \rightarrow \tilde{G}$ est un morphisme de groupes, alors

i) $f(e) = \tilde{e}$ (e neutre de G , \tilde{e} neutre de \tilde{G})

ii) $\forall a \in G: (f(a))' = f(a')$.

\uparrow symétrique dans \tilde{G} . \uparrow symétrique dans G

mult. par $f(e)'$

Dém: On a $f(e) = f(e * e) \stackrel{(2)}{=} f(e) \times f(e) \Rightarrow f(e) = \tilde{e}$.

Par ailleurs, si $a \in G$, on a :

$$\begin{aligned} \tilde{e} &= f(e) = f(a * a') \stackrel{(2)}{=} f(a) \times f(a') \\ &= f(a' * a) \stackrel{(2)}{=} f(a') \times f(a) \end{aligned} \quad \Rightarrow f(a') = (f(a))'. \quad \square$$

Exemple 1: $(G, *) = (\mathbb{C}, +)$, $(\tilde{G}, \times) = (\mathbb{C}^*, \cdot)$

$$\begin{aligned} f: \mathbb{C} &\longrightarrow \mathbb{C}^* \\ z &\longmapsto \exp(z) = e^z \end{aligned}$$

On sait que $\exp(z_1 + z_2) = \exp(z_1) \cdot \exp(z_2) \quad \forall z_1, z_2 \in \mathbb{C}$ donc f est un morphisme de groupes.

Exemple 2: $(G, *) = (\mathbb{R}, +)$, $(\tilde{G}, \times) = (\mathbb{U}, \cdot)$

$$\begin{aligned} g: \mathbb{R} &\longrightarrow \mathbb{U} \\ x &\longmapsto \exp(ix) = e^{ix} \end{aligned}$$

Pour la même raison, g est un morphisme de groupes.

Vocabulaire: Soit $f: (G, *) \rightarrow (\tilde{G}, \cdot)$ un morphisme de groupes.

On dit que:

- f est un endomorphisme si $(\tilde{G}, \cdot) = (G, *)$;
- f est un isomorphisme si f est bijectif;
- f est un automorphisme si $(\tilde{G}, \cdot) = (G, *)$ et f est bijectif.

Déf: Soit $f: (G, *) \rightarrow (\tilde{G}, \times)$ un morphisme de groupes.

a) On appelle moyau de f le sous-ensemble de G défini par

$$\text{Ker}(f) = \{a \in G; f(a) = \tilde{e}\} = f^{-1}(\tilde{e}).$$

$\text{Ker}(f)$ est un sous-groupe de G , et $\text{Ker}(f) = \{e\}$ ssi f est injectif.

b) On appelle image de f le sous-ensemble de \tilde{G} défini par

$$\text{Im}(f) = \{f(a) \in \tilde{G}; a \in G\} = f(G).$$

$\text{Im}(f)$ est un sous-groupe de \tilde{G} , et $\text{Im}(f) = \tilde{G}$ ssi f est surjectif.

Démonstration (des affirmations dans la définition ci-dessus)

a) On sait que $f(e) = \tilde{e}$, donc $e \in \ker(f)$. Si $a, b \in \ker(f)$, on a:

$$f(a * b') = f(a) \times f(b') = f(a) \times (f(b))' = \tilde{e} \times \tilde{e} = \tilde{e},$$

donc $a * b' \in \ker(f)$. Ainsi $\ker(f)$ est un sous-groupe.

Si f est injectif, alors $\ker(f) = \{e\}$ par définition. Inversement, supposons que $\ker(f) = \{e\}$. Si $a, b \in G$ vérifient $f(a) = f(b)$, alors

$$f(a * b') = f(a) \times (f(b))' = \tilde{e} \Rightarrow a * b' \in \ker(f) = \{e\}$$

$\Rightarrow a * b' = e \Rightarrow a = b$. Ainsi f est injectif.

b) On sait que $f(e) = \tilde{e}$, donc $\tilde{e} \in \text{Im}(f)$. Si $b_1, b_2 \in \text{Im}(f)$, il existe $a_1, a_2 \in G$ t.q. $f(a_1) = b_1, f(a_2) = b_2$. Alors

$$b_1 \times b_2' = f(a_1) \times f(a_2)' = f(a_1) \times f(a_2) = f(a_1 * a_2') \in \text{Im}(f),$$

donc $\text{Im}(f)$ est un sous-groupe.

Par définition, f est sujectif ssi $\text{Im}(f) = G'$. \square

Retour sur l'exemple 1 : $f: \mathbb{C} \rightarrow \mathbb{C}^*, f(z) = \exp(z)$.

On a $\ker(f) = 2\pi i \mathbb{Z} = \{2\pi i m; m \in \mathbb{Z}\}$, $\text{Im}(f) = \mathbb{C}^*$.

En effet, si $z = a + ib$ avec $a, b \in \mathbb{R}$, on a $\exp(z) = e^a e^{ib}$,

$$\cdot \exp(z) = 1 \Leftrightarrow e^a = 1 \text{ et } e^{ib} = \cos(b) + i \sin(b) = 1 \quad (\text{N.B. } |e^z| = e^a)$$

$$\Leftrightarrow a = 0 \text{ et } b = 2\pi m \text{ pour un } m \in \mathbb{Z}$$

$$\Leftrightarrow z \in 2\pi i \mathbb{Z}.$$

• si $z = \pi e^{i\vartheta} \in \mathbb{C}^*$, alors en posant $a = \ln(\pi)$ et $b = \vartheta$ on a

$$\exp(a + ib) = e^a e^{ib} = \pi e^{ib} = z.$$

4) Anneaux et corps

Déf: On appelle anneau un ensemble A muni de deux lois de composition internes, notées $+$ et \cdot , telles que:

- i) $(A, +)$ est un groupe abélien, dont l'élément neutre est noté 0 ;
- ii) La loi \cdot est associative et possède un élément neutre, noté 1 ;
- iii) La loi \cdot est distributive par rapport à la loi $+$: $\forall a, b, c \in A$ on a
 $a \cdot (b+c) = a \cdot b + a \cdot c$, et $(b+c) \cdot a = b \cdot a + c \cdot a$.

On dit que l'anneau est commutatif si, de plus, la loi \cdot est commutative.

Remarque: Si $(A, +, \cdot)$ est un anneau, alors $\forall a \in A$ on a nécessairement $0 \cdot a = a \cdot 0 = 0$. En effet:

$$0 \cdot a = (0+0) \cdot a = \underset{0+0=0}{\overset{\uparrow}{0 \cdot a + 0 \cdot a}} \underset{\text{distributivité}}{\overset{\uparrow}{\Rightarrow 0 \cdot a + 0 \cdot a}} \underset{\text{ajouter } -(0 \cdot a) \text{ aux deux membres.}}{\overset{\uparrow}{\Rightarrow 0 \cdot a = 0}}.$$

En revanche, il peut se produire que $a \cdot b = 0$ alors que $a \neq 0$ et $b \neq 0$, cf exemple 1 ci-dessous.

Exemple 1: $(\mathbb{Z}, +, \cdot)$ muni de l'addition et de la multiplication usuelles est un anneau commutatif. Il en va de même de \mathbb{Q} , \mathbb{R} , et \mathbb{C} .

Exemple 2: (Anneau $\mathbb{Z}/m\mathbb{Z}$) "entiers modulo m "

Soit $m \in \mathbb{N}$, $m \geq 2$. On rappelle que tout entier $k \in \mathbb{N}$ s'écrit de façon unique $k = qm + r$ où "division euclidienne"

$$\begin{cases} q \in \mathbb{N} \text{ est le quotient de la division euclidienne de } k \text{ par } m, \text{ et} \\ r \in \{0, 1, \dots, m-1\} \text{ est le reste de la division euclidienne de } k \text{ par } m. \end{cases}$$

On note dans la suite $\mathbb{Z} = \mathbb{Z} \bmod m$ (\mathbb{Z} modulo m).

Soit $A = \{0, 1, 2, \dots, m-1\}$. On munit A de deux lois :

- l'addition : $(k, l) \mapsto k+l \bmod m$
- la multiplication : $(k, l) \mapsto k \cdot l \bmod m$.

On vérifie que $(A, +, \cdot)$ est un anneau commutatif. On le note usuellement $A = \mathbb{Z}/m\mathbb{Z}$ "anneau des entiers modulo m ".

Cas particulier $m=5$: on a les tables suivantes

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

⚠ Si m n'est pas un nombre premier, alors $m = k \cdot l$ avec $k, l \in \{2, \dots, m-1\}$.

Dans $\mathbb{Z}/m\mathbb{Z}$ on a donc $k \cdot l = 0$ alors que $k \neq 0$ et $l \neq 0$!

Déf: Soit $(A, +, \cdot)$ un anneau. On dit qu'un élément $a \in A$ est inversible s'il existe un élément $b \in A$ t.q. $a \cdot b = b \cdot a = 1$.
On dit que b est l'inverse de a , et on note $b = a^{-1}$.

En d'autres termes, a^{-1} est le symétrique de a pour la multiplication.
(si a est inversible!). Le symétrique de a pour la loi $+$ existe toujours:
c'est l'opposé de a , noté $-a$.

Rém: Si $G = \{a \in A; a \text{ est inversible}\}$, on vérifie que (G, \cdot) est un groupe (le groupe des éléments inversibles de l'anneau A).

Exemples:

- Dans \mathbb{Z} , le groupe des inversibles est $G = \{+1, -1\}$.
- Dans \mathbb{R} , le groupe des inversibles est $G = \mathbb{R}^*$ (idem dans \mathbb{Q} ou \mathbb{C}).

Déf: Un anneau commutatif $(A, +, \cdot)$ est appelé un corps si $A \neq \{0\}$ et si tout élément de $A \setminus \{0\}$ est inversible.

L'hypothèse $A \neq \{0\}$ équivaut à imposer que $1 \neq 0$ (les él. neutres des deux lois diffèrent) \Rightarrow Un corps contient au minimum 2 éléments (0 et 1).

Dans un corps, si $a \neq 0$ et $b \neq 0$, on a nécessairement $a \cdot b \neq 0$.
En effet, $a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = b \neq 0$, donc $(a \cdot b) \neq 0$.

Exemples: \mathbb{Q} , \mathbb{R} , et \mathbb{C} sont des corps.

Exemple: L'anneau $\mathbb{Z}/m\mathbb{Z}$ est un corps ssi $m \geq 2$ est un nombre premier.

On a déjà vu que si $m = kl$ m'est pas premier, alors $kl = 0$ dans $\mathbb{Z}/m\mathbb{Z}$ alors que $k \neq 0$ et $l \neq 0 \Rightarrow \mathbb{Z}/m\mathbb{Z}$ n'est pas un corps.

Supposons que $m \geq 2$ est premier. On sait que $\mathbb{Z}/m\mathbb{Z}$ est un anneau commutatif et que $1 \neq 0$. Soit $k \in \{1, \dots, m-1\} = (\mathbb{Z}/m\mathbb{Z}) \setminus \{0\}$.
On prétend que les entiers $\{k \cdot l \text{ mod } m ; l=0, 1, \dots, m-1\}$ sont tous distincts: en effet si $k \cdot l_1 \text{ mod } m = k \cdot l_2 \text{ mod } m$ pour certains $l_1, l_2 \in \{0, \dots, m-1\}$, $l_1 \neq l_2$, alors en supposant $l_2 > l_1$ et en posant $\ell = l_2 - l_1$ on trouve que $k \cdot \ell$ est un multiple de m , ce qui est impossible puisque m est premier et $k, \ell \in \{1, \dots, m-1\}$.

Ainsi il existe $\ell \in \{0, \dots, m-1\}$ (en fait, $\ell \neq 0$) t.q. $k \cdot \ell \text{ mod } m = 1$, de sorte que k est inversible dans $\mathbb{Z}/m\mathbb{Z}$. On conclut que $\mathbb{Z}/m\mathbb{Z}$ est un corps.