Structures algébriques

1 Lois de composition interne

1.1 Définition

Soit E un ensemble, on appelle loi de composition interne (en abrégé l.c.i.) dans E toute application de $E \times E$ dans E.

De cette façon, à tout couple $(x, y) \in E^2$, on associe un élément de E généralement noté $x * y$ ou $x.y$, $x\#y$, etc.

Exemples.

- L'addition, la multiplication habituelles dans $\mathbb{N}$ sont des l.c.i., alors que la soustraction ne l'est pas. En revanche, c'est une l.c.i. dans $\mathbb{Z}$.
- Le produit vectoriel est une l.c.i dans l'ensemble des vecteurs de l'espace géométrique.

1.2 Propriétés éventuelles

Définition. Soit E un ensemble muni d'une l.c.i. notée $*$ (on dit que $(E, *)$ est un magma).

- On dit que la l.c.i. est associative quand
$$\text{pour tout } (x, y, z) \in E^3,\ x * (y * z) = (x * y) * z.$$
Dans ce cas, il est inutile de préciser les parenthèses, on note $x * y * z = x * (y * z) = (x * y) * z$.
- On dit que la l.c.i. est commutative quand
$$\text{pour tout } (x, y) \in E^2,\ x * y = y * x.$$

Exemples.

- L'addition, la multiplication usuelles dans $\mathbb{C}$ sont associatives et commutatives.
- Le produit vectoriel n'est ni associatif, ni commutatif.
- Soit A un ensemble, E l'ensemble des applications de A dans A, qu'on note souvent $\mathscr{F}(A)$. La composition des applications est une l.c.i. associative mais non commutative dans E (dès que A a plus de deux éléments).

1.3 Élément neutre

Définition. On dit que la l.c.i. admet un neutre quand il existe $e \in E$ tel que pour tout $x \in E$, $e * x = x * e = x$.

Proposition 1. *Si une l.c.i. $*$ a un neutre, alors il est unique.*

Exemples.

- 0 est le neutre de $+$ dans $\mathbb{C}$
- 1 est le neutre de . dans $\mathbb{C}$
- Id_A est le neutre de $\mathscr{F}(A)$

1.4 Symétrique d'un élément

Définition. Soit E un ensemble muni d'une l.c.i. notée $*$, possédant un neutre noté e.

Soit $x \in E$, on dit que x est symétrisable dans E pour la l.c.i $*$ (ou inversible pour $*$) quand
$$\text{il existe } x' \in E \text{ tel que } x * x' = x' * x = e.$$

Dans ce cas, x' est appelé un symétrique de x pour $*$ (ou un inverse de x pour $*$).

Rien dans la définition n'oblige à ce qu'un élément n'ait qu'un seul symétrique.

Proposition 2. *Si la loi $*$ est associative et si un élément x est symétrisable, alors il a un unique symétrique : on le note x^{-1} en général.*

Exemples.
- Tout élément de $\mathbb{C}$ est symétrisable pour $+$, son symétrique est son opposé.
- Tout élément non nul de $\mathbb{C}$ est symétrisable pour $.$, son symétrique est son inverse.
- Si $E = \mathscr{F}(A)$, les éléments symétrisables de E pour la loi $\circ$ sont les
  Dans ce cas, le symétrique d'un élément est

Proposition 3. *(toujours avec l'hypothèse d'associativité).*
Si x est symétrisable, alors x^{-1} l'est aussi et $(x^{-1})^{-1} =$
Si x, y sont symétrisables, alors $x * y$ l'est aussi et $(x * y)^{-1} =$

Remarque. On a coutume de réserver la notation $+$ uniquement lorsque la l.c.i.
- est associative,
- est commutative,
- a un neutre noté,
- et tout élément est symétrisable ; on note alors $-x$ le symétrique de x, appelé bien sûr opposé de x.

Dans toute la suite, la loi $+$ respecte cette contrainte !

1.5 Notations puissance (ou multiple)

Soit E un ensemble muni d'une l.c.i. notée $*$, supposée associative et ayant un neutre noté e.

Soit $a \in E$, $n \in \mathbb{N}^*$, on pose $a^{*0} = e$ et $a^{*(n+1)} = a^{*n} * a$ (s'il n'y a pas d'ambiguïté, on omet le symbôle $*$ et on note simplement a^n).

On remarque qu'il est important que la loi soit associative pour définir cette notation, indépendamment de l'ordre dans lequel on fait les calculs (par exemple, dans le cas d'une loi non associative, la notation a^3 n'est pas assez précise, car en général $a * (a * a) \neq (a * a) * a$). Dans le cas d'une loi additive $+$, on note plutôt $n.a$ au lieu de a^{*n}.

On vérifie que les règles habituelles de calcul restent valables :

Proposition 4.

▷ $\forall (m,n) \in \mathbb{N}^2 \quad a^{*(m+n)} = a^{*m} * a^{*n}$
▷ $\forall (m,n) \in \mathbb{N}^2 \quad a^{*(mn)} = (a^{*m})^{*n}$

En revanche, la règle habituelle de calcul $(a * b)^{*n} = a^{*n} * b^{*n}$ n'est pas toujours vraie !

Définition. On dit que deux éléments a et b commutent (pour une l.c.i. $*$) quand $a * b = b * a$.

Proposition 5. *Dans un ensemble muni d'une l.c.i. associative $*$, si a et b sont deux éléments qui commutent, alors pour tout $n \in \mathbb{N}^*$, $(a * b)^{*n} = a^{*n} * b^{*n}$.*

Remarque.
- Dans le cas d'une notation additive, on a $(m + n).a = m.a + n.a$ et $(mn).a = m.(n.a)$, et comme $+$ est commutative, $m.(a + b) = m.a + m.b$.
- Si a est de plus symétrisable pour la loi $*$, on pose $a^{*-n} = (a^{-1})^{*n}$ pour tout $n \in \mathbb{N}$ et on vérifie que les règles de calcul précédentes sont valables aussi avec m, n entiers relatifs.

1.6 Parties stables

Définition. Soit E un ensemble muni d'une l.c.i. $*$, A une partie de E.
On dit que A est stable par $*$ quand pour tout $(x, y) \in A^2$, $x * y \in A$.

Proposition 6. *Soit E un ensemble muni d'une l.c.i. $*$ associative, A une partie de E.*
Si A est stable par $*$, alors pour tout $n \in \mathbb{N}^*$, pour tout $(x_1, \dots, x_n) \in A^n$, $x_1 * x_2 * \dots * x_n \in A$;
en particulier, pour tout $n \in \mathbb{N}^*$ et $x \in A$, $x^{*n} \in A$.

2 Anneaux

2.1 Définition

Définition. Un anneau est un ensemble A muni de deux l.c.i. dont l'une est notée $+$ et l'autre est souvent notée $\times$ ou . tel que
- la loi $+$ respecte les contraintes énoncées précédemment
- $\times$ est associative
- $\times$ a un élément neutre, noté souvent 1_A ou 1 ou I ou ...
- $\times$ est distributive pour $+$:

$$\text{pour tout } (x,y,z) \in A^3,\ x(y+z) = xy + xz \text{ et } (x+y)z = xz + yz$$

Si de plus, la loi $\times$ est commutative, on dit que A est un anneau commutatif.

Exemples.
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux commutatifs pour les lois habituelles.
- Si X est un ensemble, l'ensemble des applications de X dans $\mathbb{R}$, $\mathscr{F}(X, \mathbb{R})$, est un anneau commutatif. Plus généralement, si A est un anneau, $\mathscr{F}(X, A)$ est un anneau pour les lois classique déduites de celles de A.
- Si $K = \mathbb{R}$ ou $\mathbb{C}$, $K[X]$ est un anneau commutatif pour les lois habituelles.
- L'ensemble des matrices $(2,2)$ à coefficients réels, noté $\mathscr{M}_2(\mathbb{R})$, est un anneau non commutatif.

On rappelle les opérations :

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{pmatrix} \quad ; \quad \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \times \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 \\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2 \end{pmatrix}$$

2.2 Sous-anneaux

Définition. Soit $(A, +, .)$ un anneau, B une partie de A. On dit que B est un sous-anneau de A (sous-entendu pour les lois $+$ et .) quand
- $1_A \in B$
- B est stable par $+$: pour tout $(x,y) \in B^2$, $x+y \in B$
- B est stable par opposition : pour tout $x \in B$, $-x \in B$
- B est stable par . : pour tout $(x,y) \in B^2$, $x.y \in B$

Un sous-anneau d'un anneau est donc lui-même un anneau. En général, pour montrer qu'un ensemble muni de deux l.c.i. est un anneau, on montre que c'est un sous-anneau d'un anneau connu (entre autres, les anneaux cités en exemples précédemment).

Exercices :
1) Montrez que l'ensemble des fonctions paires est un sous-anneau de $\mathscr{F}(\mathbb{R}, \mathbb{R})$
2) Montrez que l'ensemble des suites complexes bornées est un sous-anneau de l'anneau $\mathbb{C}^{\mathbb{N}}$.
3) Quels sont les sous-anneaux de l'anneau $\mathbb{Z}$?
4) On pose $A = \left\{ \frac{a}{b} \ / \ (a,b) \in \mathbb{Z} \times \mathbb{N}^* \text{ et } 3 \wedge b = 1 \right\}$. Montrez que A est un sous-anneau de $\mathbb{Q}$.

2.3 Calculs sans surprise dans un anneau

Proposition 7. *Soit $(A, +, .)$ un anneau. On note 0 le neutre de la loi $+$ et 1 le neutre de la loi .*
Alors
- ▷ *pour tout $x \in A$, $0.x = x.0 = 0$;*
- ▷ *pour tout $(x,y) \in A^2$, $-(x.y) = (-x).y = y.(-x)$ et donc $(-x).(-y) = x.y$: la « règle des signes » reste valable dans un anneau quelconque.*

Ces quelques résultats semblent triviaux, mais les calculs dans un anneau quelconque peuvent réserver quelques surprises (voir ci-dessous).

2.4 Intégrité

Définition. Un anneau A est dit intègre quand
- il est commutatif
- pour tout $(a,b) \in A^2$, $a \times b = 0 \Rightarrow a = 0$ ou $b = 0$.

Sinon, tout couple (a,b) tel que $ab = 0$, $a \neq 0$ et $b \neq 0$ est appelé couple de diviseurs de zéro.

Exemples.
- $\mathbb{Z}$ et plus généralement les anneaux de nombres sont intègres.
- L'anneau $K[X]$ est intègre.
- L'anneau $\mathscr{F}(X, \mathbb{R})$ est un anneau commutatif non intègre.

Remarque. En général, dans un anneau quelconque, on ne peut pas simplifier dans un produit :
$ab = ac$ n'implique pas en général $b = c$, même si $a \neq 0$
Si l'anneau est intègre et si $a \neq 0$, alors la simplification est correcte.

2.5 Formule du binôme et de Bernoulli

Proposition 8. *Soit A un anneau et a, b deux éléments de A qui commutent ($ab = ba$). Alors*

$$\forall n \in \mathbb{N} \quad (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

$$\forall n \in \mathbb{N}^* \quad a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + ... + ab^{n-2} + b^{n-1}) = (a-b)\sum_{i=0}^{n-1} a^i b^{n-1-i}$$

Remarque. Si les éléments ne commutent pas, c'est faux.

3 Corps

Définition. Un corps est un anneau commutatif dans lequel tous les éléments non nuls sont inversibles.

Exemple. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps.

Proposition 9. *Un corps est un anneau intègre.*

Dans un corps, il n'y a aucune surprise : tout se passe comme dans les ensembles de nombres habituels $\mathbb{R}$ et $\mathbb{C}$.

4 Groupes

4.1 Généralités

Définition. Soit G un ensemble. On dit que $(G, *)$ est un groupe quand
- $*$ est une loi de composition interne dans G
- $*$ est associative
- $*$ admet un neutre
- tout élément de G est symétrisable pour $*$ dans G

Si de plus, $*$ est commutative, on dit que $(G, *)$ est un groupe commutatif ou groupe abélien.

Tous les résultats précédents énoncés dans le cadre des l.c.i. associatives sont donc valables dans un groupe.

Proposition 10. *(Simplification) Dans un groupe muni d'une loi $*$,*
si $x * y = x * z$, alors $y = z$ et de même, si $y * x = z * x$, alors $y = z$.

(Attention à l'ordre des éléments si le groupe n'est pas commutatif !)

4.2 Exemples fondamentaux

— $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ sont des groupes abéliens, mais $(\mathbb{N},+)$ n'est pas un groupe puisque 1 n'est pas symétrisable dans $\mathbb{N}$.
— $\{-1,+1\}$, $\mathbb{R}^*$, $\mathbb{R}_+^*$, $\mathbb{C}^*$, $\mathbb{U}$ sont des groupes abéliens pour la multiplication.
— L'ensemble V des vecteurs du plan ou de l'espace est un groupe abélien pour l'addition des vecteurs.
— (Exemple anecdotique) Soit E l'ensemble des entiers de 1 à 12, muni de « l'addition des heures » (8h ++ 9h = 17h = 5h). $(E,++)$ est un groupe abélien, dont le neutre est 12.

Proposition 11. *Soit $(G,*)$ et (H,Δ) deux groupes.*
Alors la loi $(x,y).(x',y') = (x*x', y\Delta y')$ confère à l'ensemble $G\times H$ une structure de groupe.

Dans ce cas, le groupe $(G\times H,.)$ est appelé groupe-produit de G et H.

Proposition 12. *Soit A un ensemble, on note $S(A)$ l'ensemble des bijections de A dans A (appelées aussi permutations de A).*
Alors $(S(A),\circ)$ est un groupe, non abélien en général (dès que A a plus de trois éléments), appelé groupe symétrique de A.

4.3 Groupe des inversibles d'un anneau

Quand on parle d'élément inversible dans un anneau, on sous-entend toujours « pour la multiplication », car pour l'addition, tous les éléments sont inversibles !

Définition. Soit A un anneau. On appelle groupe des inversibles de A l'ensemble des éléments de A inversibles pour la loi $\times$: on le note $A^\times$.

Proposition 13. *Le groupe des inversibles $A^\times$ est un groupe pour la multiplication.*

Exercices :

5) Quel est le groupe des inversibles de l'anneau $\mathbb{Z}$?
6) Même question avec l'anneau $\mathscr{F}(X,\mathbb{R})$.

4.4 Sous-groupe

Définition. Soit $(G,*)$ un groupe, H une partie de G. On dit que H est un sous-groupe de G (sous-entendu pour la loi $*$) quand
— H est non vide
— H est stable par $*$: pour tout $(x,y)\in H^2$, $x*y\in H$
— H est stable par inversion pour $*$: pour tout $x\in H$, $x^{-1}\in H$

Une conséquence simple des 3 propriétés est que H contient forcément le neutre. En pratique, pour montrer que H est non vide, on montre donc souvent que H contient le neutre.

Il est facile de voir que $*$ induit une application de $H\times H$ dans H (qui est donc une l.c.i.), qu'on note encore abusivement $*$, et que cette l.c.i. $*$ dans H définit une structure de groupe, d'où le nom de sous-groupe.

Un sous-groupe d'un groupe est donc lui-même un groupe. En pratique, on démontre très rarement directement qu'un ensemble est un groupe. **Dans presque tous les cas, pour montrer qu'un ensemble muni d'une l.c.i. est un groupe, on montre que c'est un sous-groupe d'un groupe connu** (entre autres, les groupes cités en exemples précédemment : on en verra d'autres).

Exercices :

7) Soit $n\in\mathbb{N}^*$. Montrez que l'ensemble des racines n-èmes de l'unité est un sous-groupe de $(\mathbb{C}^*,\times)$
8) Soit A un ensemble non vide. Montrez que l'ensemble des bijections de A dans A qui laissent invariante une partie B de A (*i.e.* $f(B)=B$) est un sous-groupe de $(S(A),\circ)$.

Un exemple fondamental : les sous-groupes de $(\mathbb{Z},+)$.

Proposition 14. *Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les ensembles $n\mathbb{Z}$ pour $n \in \mathbb{N}$.*

5 Morphismes

5.1 Définition

Définition. Soit $(E, *)$ et $(F, \diamond)$ deux magmas, f une application de E dans F.
On dit que f est un morphisme de $(E, *)$ dans $(F, \diamond)$ quand pour tout $(a, b) \in E^2$, $f(a * b) = f(a) \diamond f(b)$.
Si de plus f est bijective, alors on dit que f est un isomorphisme.

Exemples.
- $x \mapsto \frac{1}{2}x$ est un morphisme de $(\mathbb{Z}, +)$ dans $(\mathbb{Q}, +)$.
- $t \mapsto e^{it}$ est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, \times)$.
- ln est un isomorphisme de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$.
- $P \mapsto P'$ est un morphisme de $(K[X], +)$ dans lui-même.
- deg est un morphisme de $(K[X]^*, \times)$ dans $(\mathbb{N}, +)$.

5.2 Morphismes de groupes

Définition. Soit $(E, *)$ et $(F, \diamond)$ deux groupes. Un morphisme de $(E, *)$ dans $(F, \diamond)$ est appelé un morphisme de groupes.

Proposition 15. *Soit $(E, *)$ et $(F, \diamond)$ deux groupes, e le neutre de E, ε celui de F. Soit f un morphisme de groupes de $(E, *)$ dans $(F, \diamond)$. Alors*
- ▷ *$f(e) = \varepsilon$;*
- ▷ *pour tout $x \in E$, $f(x^{-1}) = f(x)^{-1}$.*

Proposition 16. *Soit $(E, *)$ et $(F, \diamond)$ deux groupes. Soit f un morphisme de groupes de $(E, *)$ dans $(F, \diamond)$.*
Si G est un sous-groupe de E, alors $f(G)$ est un sous-groupe de F.
Si H est un sous-groupe de F, alors $f^{-1}(H)$ est un sous-groupe de E.

2 cas particuliers importants :
- $\operatorname{Im} f = f(E)$ est un sous-groupe de F.
- $f^{-1}(\{\varepsilon\}) = \{x \in E \ / \ f(x) = \varepsilon\}$ est un sous-groupe de E, appelé le noyau de f et noté $\operatorname{Ker} f$.

Proposition 17. *Soit $(E, *)$ et $(F, \diamond)$ deux groupes. Soit f un morphisme de groupes de $(E, *)$ dans $(F, \diamond)$.*
Alors f est injective si et s.si $\operatorname{Ker} f = \{e\}$.

5.3 Morphismes d'anneaux

Définition. Soit $(A, +.)$ et $(B, +, .)$ deux anneaux. Un morphisme d'anneaux de A dans B est une application $f : A \to B$ telle que
- f est un morphisme de $(A, +)$ dans $(B, +)$ (donc un morphisme de groupes abéliens) ;
- f est un morphisme de $(A, .)$ dans $(B, .)$;
- $f(1_A) = 1_B$.

Un morphisme de corps est un morphisme d'anneaux pour les deux lois de corps.

Comme un morphisme d'anneaux est en particulier un morphisme de groupes pour les lois $+$, on peut parler de son noyau : $\operatorname{Ker} f = \{x \in A \ / \ f(x) = 0\}$.

Hors-programme de MP2I (programme de MPI)

Soit $n \in \mathbb{N}^*$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes de congruence modulo n dans $\mathbb{Z}$ (lire « Z sur nZ »).
On sait que $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$.

On munit cet ensemble de deux lois de composition $+$ et $\times$:

si $\overline{a}$ et $\overline{b}$ sont deux éléments de $\mathbb{Z}/n\mathbb{Z}$, alors on pose $\overline{a} + \overline{b} = \overline{a+b}$ et $\overline{a} \times \overline{b} = \overline{ab}$.

Il est alors facile de vérifier que $\left(\mathbb{Z}/n\mathbb{Z}, +, \times\right)$ est un anneau commutatif dont le neutre pour $+$ est $\overline{0}$ et le neutre pour $\times$ est $\overline{1}$: les propriétés de $+$ et $\times$ dans $\mathbb{Z}/n\mathbb{Z}$ découlent des propriétés de $+$ et $\times$ dans $\mathbb{Z}$ et de la compatibilité de la congruence modulo n avec ces deux opérations.
Voici par exemple les tables d'addition et de multiplication dans $\mathbb{Z}/8\mathbb{Z}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{7}$	$\overline{7}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{2}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{6}$	$\overline{3}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

On voit sur cet exemple quelques-unes des bizarreries qu'on peut trouver dans un anneau :
- des couples de diviseurs de zéro : $(2, 4)$ par exemple ;
- $\overline{4} + \overline{4} = \overline{0}$: l'opposé d'un élément peut être lui-même ;
- $\overline{5} \times \overline{5} = \overline{1}$: l'inverse d'un élément autre que $\overline{1}$ et $\overline{-1} = \overline{7}$ peut être égal à lui-même ;
- $\overline{4}^2 = \overline{0}$: le carré d'un élément non nul peut être nul.

Il est facile de voir que $\mathbb{Z}/n\mathbb{Z}$ a des diviseurs de zéro si et s.si n n'est pas premier.
Le th. de Bézout montre que les inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les classes $\overline{k}$ telles que k est premier avec n.
Enfin, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.