Chap. 1 : Rappels sur les congruences et $\mathbb{Z}/n\mathbb{Z}$

<u>Notation</u> : $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$. entiers naturels ($= \mathbb{Z}_+$)

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ entiers relatifs

avec deux lois de composition : $+$ et $\cdot$

$$\mathbb{N}^* = \mathbb{N} - \{0\} \qquad \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}.$$

$$\mathbb{Q} = \left\{ x = \frac{a}{b} \;;\; a \in \mathbb{Z},\ b \in \mathbb{Z}^* = \mathbb{Z} - \{0\} \right\}$$

nombres rationnels.

<u>Rem</u> : $\mathbb{Q} \neq \mathbb{Z} \times \mathbb{Z}^*$ on identifie $\frac{a}{b} = \frac{c}{d}$

si $ad = cb$.

On a les inclusions.

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

$a \mapsto \frac{a}{1}$. nombres réels, nombres complexes.

Rappels sur la divisibilité dans $\mathbb{Z}$:

- On dit que <u>a divise n</u> ($a, n \in \mathbb{Z}$) s'il existe $b \in \mathbb{Z}$ tel que $a \cdot b = n$. On écrit $a | n$ et on dit que a est un <u>diviseur</u> de n
- On dit que $n \in \mathbb{N}$ est un nombre <u>premier</u> s'il a exactement <u>deux</u> <u>diviseurs positifs</u> (qui sont 1 et n).
- Liste des nombres premiers.
  2, 3, 5, 7, 11, 13, 17, 23, ... (nb. infini de nb. premiers)
- <u>Thm</u> : Tout ~~entier~~ $n \in \mathbb{N}$ est produit de nombres premiers.

$a, b \in \mathbb{Z}$ $n \in \mathbb{N}$

Déf : On dit que a est congru à b modulo n si $n \mid a-b$ et on écrit $a \equiv b \mod n$

La congruence est une relation d'équivalence

1) $a \equiv a \mod n$
2) Si $a \equiv b \mod n$, alors $b \equiv a \mod n$
3) Si $a \equiv b \mod n$ et $b \equiv c \mod n$, alors $a \equiv c \mod n$

Rem. : (1) $a \equiv b \mod n \iff a$ et b ont le même reste modulo n

(2) Si r = reste de la division euclidienne de a par n, alors $a \equiv r \mod n$

On peut donc considérer les classes d'équivalences par cette relation d'équivalence

Les classes d'équivalences sont notées

$$a + n\mathbb{Z} = \{ b \in \mathbb{Z} \mid b \equiv a \mod n \} \subset \mathbb{Z}.$$

~~est appelée~~ On dit que $a + n\mathbb{Z}$ est la classe résiduelle de a modulo n, noté $\bar{a}$ ou $a \mod n$.

Exemple : $n = 4$.

$\bar{1} = 1 + 4\mathbb{Z} = \{ \ldots -11, -7, -3, 1, 5, 9, \ldots \}$

Notation

$\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes résiduelles modulo n.

Rem : $| \mathbb{Z}/n\mathbb{Z} | = n$ "cardinal" = "nb d'éléments".

<u>Exemple</u> : $\mathbb{Z}/_{4\mathbb{Z}} = \{ \underset{\overline{0}}{\underset{\shortparallel}{0+4\mathbb{Z}}}, \underset{\overline{1}}{\underset{\shortparallel}{1+4\mathbb{Z}}}, \underset{\overline{2}}{\underset{\shortparallel}{2+4\mathbb{Z}}}, \underset{\overline{3}}{\underset{\shortparallel}{3+4\mathbb{Z}}} \}$

<u>Def</u> : Un ensemble de représentants des classes résiduelles modulo n est un ensemble ayant un unique élément dans chaque classe résiduelle.

<u>Exemple</u> : Un ensemble de représentants de $\mathbb{Z}/_{4\mathbb{Z}}$ est

$$\{4, 5, 2, -1\}, \text{ ou bien } \{0, 1, 2, 3\}.$$

<u>Prop</u> : Si $a \equiv b \mod n$ et $c \equiv d \mod n$, alors

1) $-a \equiv -b \mod n$
2) $a + c \equiv b + d \mod n$ $\forall a, b, c, d \in \mathbb{Z}$.
3) $ac \equiv bd \mod n$

<u>Preuve</u> : 1) si $n \mid a-b$, alors $n \mid b-a \iff -a \equiv -b \mod n$

2) Si $n \mid c-d$, alors $n \mid (a-b)+(c-d) = n \mid (a+c)-(b+d)$
et $n \mid a-b$ $\iff a+c \equiv b+d \mod n$

3) si $n \mid a-b$, alors $\exists k \in \mathbb{Z}$ t.q. $a = b + km$
si $n \mid c-d$, alors $\exists k' \in \mathbb{Z}$ t.q. $c = d + k'n$

$$\Rightarrow ac = (b+kn)(d+k'n)$$
$$= bd + knd + k'nb + kk'n^2$$
$$= bd + n(kd + k'b + kk'n)$$
$$\Rightarrow ac \equiv bd \mod n.$$

<u>Déf</u> : Une loi de composition sur un ensemble X est une application

$$X \times X \longrightarrow X$$

On va définir deux opérations sur l'ensemble fini $\mathbb{Z}/n\mathbb{Z}$:

$$(a+n\mathbb{Z}) + (b+n\mathbb{Z}) = (a+b)+n\mathbb{Z}$$

$$(a+n\mathbb{Z}) \cdot (b+n\mathbb{Z}) = (ab)+n\mathbb{Z}$$

D'après la proposition précédente, ces opérations sont bien définies car elles ne dépendent pas du choix des représentants des classes résiduelles.

<u>Exemples</u> : $(3+5\mathbb{Z})+(2+5\mathbb{Z}) = (5+5\mathbb{Z}) = (0+5\mathbb{Z})$

$$(3+5\mathbb{Z}) \cdot (2+5\mathbb{Z}) = 6+5\mathbb{Z} = 1+5\mathbb{Z}$$

et on note aussi $\overline{3}+\overline{2} = \overline{0}$ dans $\mathbb{Z}/5\mathbb{Z}$

$\overline{3} \cdot \overline{2} = \overline{1}$ dans $\mathbb{Z}/5\mathbb{Z}$

<u>Chap. 2</u> $\boxed{\text{Groupes}}$

<u>Déf</u> : Soit X un ensemble muni d'une loi de composition $\circ$. On dit que la loi $\circ$ est <u>associative</u> si $\forall x, y, z \in X$

$$(x \circ y) \circ z = x \circ (y \circ z)$$

<u>commutative</u> si $\forall x, y \in X$
ou <u>abélienne</u>.

$$x \circ y = y \circ x.$$

Exemples: $(\mathbb{Z},+)$, $(\mathbb{Z},\cdot)$ lois associatives, commutatifs

$(\mathbb{Z}/n\mathbb{Z},+)$, $(\mathbb{Z},\cdot)$ ——————————

mais: $(M_2(\mathbb{R}), \circ)$ (la loi ($\circ$ = mult. matrices) n'est pas commutative)

$M_2(\mathbb{R})$ = matrices carrées d'ordre 2 à coeff. réels, $\circ$ = multiplication des matrices.

Def: 1) $(X,\circ)$ est appelé semi-groupe si $\circ$ est associative.

2) $(X,\circ)$ admet un élément neutre, noté e, si

$$x \circ e = e \circ x = x \quad \forall x \in X$$

3) Soit $(X,\circ)$ un semigroupe avec un neutre $e \in X$.
On dit que $a \in X$ admet un inverse s'il existe un élément $b \in X$ tel que

$$a \circ b = b \circ a = e.$$

Règles de calcul si $(X,\circ)$ est un semi-groupe.

alors $a^n \stackrel{DEF}{=} \underbrace{a \circ a \circ \cdots \circ a}_{n \text{ fois}}$

on a les formules 1) $a^n \circ a^m = a^{n+m}$

2) $(a^n)^m = a^{n \cdot m}$

de même, si $(X,\circ)$ est abélien $(a \circ b)^n = a^n \circ b^n$

<u>Exemples</u>: 1) $(\mathbb{Z},+)$ semi-groupe abélien.

. neutre $= 0$

. inverse de $a = -a$ (aussi appelé l'opposé de a).

2) $(\mathbb{Z},\cdot)$ semi-groupe abélien

. neutre $= 1$

. $a \in \mathbb{Z}$ inversible $a \cdot b = 1$

$\Rightarrow a = \pm 1$.

3) $(\mathbb{Z}/_{n\mathbb{Z}},+)$ semi-groupe abélien.

. neutre $= 0 + n\mathbb{Z} = \overline{0}$

. inverse de $a + n\mathbb{Z} = \overline{a}$ ~~est~~ $-a + n\mathbb{Z} = \overline{-a}$.

4) $(\mathbb{Z}/_{n\mathbb{Z}},\cdot)$ semi-groupe abélien.

. neutre $= 1 + n\mathbb{Z} = \overline{1}$

inversibles ... (plus tard)

<u>Déf</u>: On dit que $(X,\circ)$ est un <u>groupe</u> si ~~[illegible]~~

1) $(X,\circ)$ est un semi-groupe, c'est-à-dire la loi $\circ$ est <u>associative</u>.

2) $(X,\circ)$ admet un élément <u>neutre</u>

3) Tout élément $x \in X$ admet un <u>inverse</u>.

<u>Exemples</u>: 1) $(\mathbb{Z},+)$ et 3) $(\mathbb{Z}/_{n\mathbb{Z}},+)$ sont des groupes.

mais 2) $(\mathbb{Z},\cdot)$ et 4) $(\mathbb{Z}/_{n\mathbb{Z}},\cdot)$ ne sont pas des groupes.

2) p.ex. 2 n'est pas inversible.

4) p.ex. $\overline{0}$ n'est pas inversible.

Rem : Soit $(G,\cdot)$ un groupe et $a \in G$. L'inverse de $a \in G$ est noté a^{-1} et on pose $a^{-n} = (a^{-1})^n$ $\forall n \in \mathbb{N}$.

Dans un groupe $(G,\cdot)$ on a les règles de simplifications

$$\left.\begin{array}{l} a\cdot c = bc \\ ca = cb \end{array}\right\} \Rightarrow a = b$$

on multiplie à gauche/droite avec l'inverse c^{-1} de c.

Def : Le nombre d'éléments d'un groupe G est appelé l'ordre du groupe, noté $|G|$ (si ce nombre est fini).

Exemples : $|\mathbb{Z}/n\mathbb{Z}| = n$.

Autres exemples de groupes

$(\mathbb{Z},+)$; $(\mathbb{Q},+)$; $(\mathbb{R},+)$; $(\mathbb{C},+)$ sont des groupes abéliens.

pareil pour $(\mathbb{Q}^*,\cdot)$; $(\mathbb{R}^*,\cdot)$; $(\mathbb{C}^*,\cdot)$ groupes abéliens.

$*$ = on enlève le 0.

(mais $(\mathbb{Z}^*,\cdot)$ n'est pas un groupes)

ce sont des groupes d'ordre infini

Parmi les groupes finis, les plus simples sont les groupes abéliens finis. $(\mathbb{Z}/n\mathbb{Z},+)$,

↑ cycliques.

ou produits $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

$$= \{(\bar{a},\bar{b}) \; ; \; \bar{a} \in \mathbb{Z}/n\mathbb{Z} \text{ et } \bar{b} \in \mathbb{Z}/m\mathbb{Z}\}.$$

Exemples de groupes non-abéliens finis.

1) groupe symétrique $S_n = \{$ permutations = bijections d'un ensemble de cardinal $n \}$

pour $n \geq 3$

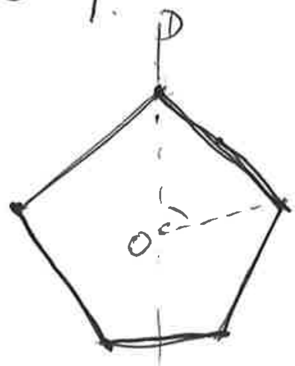
(voir plus tard TD)

$|S_n| = n!$

2) groupe diédral D_{2n} pour $n \geq 3$.

$D_{2n} = \{$ isométries du plan préservant un polygône régulier à n côtés $\}$. $|D_{2n}| = 2n$

p.ex. $n=5$ pentagone.



deux éléments

r = rotation d'angle $\frac{2\pi}{5}$.

σ = symétrie par rapport à un axe donné p.ex. D

alors on a les relations $r^5 = \mathrm{Id} = e$

$\sigma^2 = e$.

et $\sigma r \sigma^{-1} = r^{-1}$

$D_{10} = \{1, r, r^2, r^3, r^4, \sigma, \sigma r, \sigma r^2, \sigma r^3, \sigma r^4\}$.

Soit G un groupe, noté multiplicativement.

<u>Def</u>: Soit $g \in G$. S'il existe un entier positif $r \in \mathbb{N}^*$ tel que $g^r = e$, alors le plus petit des entiers non-nuls ayant cette propriété est appelé l'ordre de g, noté $\mathrm{ord}_G(g)$

$$\mathrm{ord}_G(g) = \min\{r \in \mathbb{N}^* \mid g^r = e\}.$$

<u>Rem.</u>: Si on définit

$$\langle g \rangle = \{\ldots, g^{-3}, \underbrace{g^{-2}}_{(g^{-1})^2}, g^{-1}, e, g, g^2, g^3, \ldots\} \subset G$$

Si ce sous-ensemble $\langle g \rangle$ est fini (on verra plus tard que c'est un sous-groupe), alors

$$\mathrm{ord}_G(g) = |\langle g \rangle|.$$

<u>Exemples</u>: 1) $G = (\mathbb{Z}, +)$ Le seul élément d'ordre fini est 0.

2) $G = (\mathbb{Z}/8\mathbb{Z}, +)$ $\quad \mathrm{ord}_G(\bar{1}) = 8$, $\mathrm{ord}_G(\bar{2}) = 4$

$\mathrm{ord}_G(\bar{3}) = 8$, ...

<u>Prop.</u> : Soit $g \in G$ et $n \in \mathbb{Z}$. Alors

$$g^n = e \iff r = \mathrm{ord}_G(g) \mid n$$

<u>Preuve</u> : $\boxed{\Leftarrow}$ Si $n = r \cdot k$, alors $g^n = g^{rk} = (g^r)^k = e^k = e$

$\boxed{\Rightarrow}$ Si on suppose ~~que~~ $g^n = e$, on considère la division euclidienne de n par $r = \mathrm{ord}_G(g)$

$$n = qr + a \quad \text{avec} \quad 0 \leq a < r$$

donc $g^a = g^{n-qr} = (g^n)(g^r)^{-q} = e \cdot e^{-q} = e$

par minimalité de r, on a donc $a = 0$

$\Rightarrow n = qr$. □

<u>Cor.</u> : Soit $g \in G$ et $l, m \in \mathbb{Z}$. Alors

$$g^l = g^m \iff l \equiv m \mod r$$

<u>Preuve</u> On multiplie par g^{-m} : $g^{l-m} = e \underset{\text{prop. préc.}}{\iff} r \mid l-m$

$\iff l \equiv m \mod r$. □

<u>Déf.</u> : Soit G un groupe. On dit qu'un sous-ensemble $H \subset G$ est un <u>sous-groupe</u> de G si H est aussi un groupe.

(Critère)
<u>Prop.</u> : Soit $H \subset G$ un sous-ensemble de G. Alors H est un sous-groupe de G ssi

1) $e_G \in H$ (et $e_H = e_G$).

2) Si $x \in H$, alors $x^{-1} \in H$.

3) Si $x, y \in H$, alors $x \cdot y \in H$.

On dit que H est stable par la loi de composition et par passage à l'inverse.

Preuve : évident.

Def : Soit G un groupe. On dit que G est cyclique s'il existe un élément $g \in G$ tel que

$$\langle g \rangle = \{ \ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots \} = G$$
$$= \{ g^n \mid n \in \mathbb{Z} \}.$$

Si G est un groupe fini, alors G est cyclique s'il existe un élément $g \in G$ tel que

$$\mathrm{ord}_G(g) = |G|.$$

Exemples 1) $G = (\mathbb{Z}, +)$ est cyclique, car $G = \langle 1 \rangle = \langle -1 \rangle$

2) $G = (\mathbb{Z}/7\mathbb{Z}, +)$ est cyclique, car $G = \langle \bar{1} \rangle$ $(= \langle \bar{2} \rangle = \langle \bar{3} \rangle = \langle \bar{4} \rangle = \langle \bar{5} \rangle = \langle \bar{6} \rangle)$

3) $G = (\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, +)$ n'est pas cyclique car tous ses éléments sont d'ordre 1 ou 7

4) $G = (\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}, +)$ est cyclique, car $G = \langle (\bar{1}, \bar{1}) \rangle$

(on verra plus tard que $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \cong \mathbb{Z}/56\mathbb{Z}$).

<u>théorème</u> (Lagrange)

Soit G un groupe fini et H ~~un~~ sous-groupe de G.
Alors. $|H|$ divise $|G|$.

<u>Preuve</u>: On va montrer que G est une réunion disjointe de sous-ensembles ayant le même cardinal $d = |H|$.

① Soit $g \in G$ et considérons l'application

$$\mu_g : H \longrightarrow G$$
$$h \longmapsto g \cdot h$$

On montre d'abord que l'application μ_g est injective. $gh_1 = gh_2 \in G$

On multiplie par l'inverse g^{-1} de g

$$g^{-1} \cdot g\, h_1 = g^{-1} \cdot g\, h_2 \iff h_1 = h_2$$

On va noter gH l'image de l'application μ_g.

<u>Attention</u>: gH n'est pas (en général) un sous-groupe de G et μ_g n'est pas un (homomorphisme) de groupes. gH est seulement un sous-ensemble de G.

② On va montrer

si $gH \cap g'H \neq \phi$, alors $gH = g'H$.

Soit $x \in gH \cap g'H \iff$ il existe $h \in H$ et $h' \in H$ tels que $x = gh = g'h'$ (on multiplie à droite par $(h')^{-1}$).

$$\Longrightarrow gh(h')^{-1} = g' \underbrace{h'(h')^{-1}}_{e} = g'.$$

$$\text{donc } g\, h(h')^{-1} = g'$$

$$\text{Donc } g' h'' = g \underbrace{h(h')^{-1} h''}_{\in H} \in gH \qquad \forall h'' \in H.$$

$$\Rightarrow g'H \subset gH$$

et on obtient ainsi une égalité $g'H = gH$, car ces ensembles ont le même cardinal.

③ $G = \bigcup_{g \in G} gH$, car $g = g \cdot e$ et $e \in H$

$\Rightarrow$ Comme on peut extraire de la famille $\{gH\}_{g \in G}$ une sous-famille $\{gH\}_{g \in S}$ qui donne une réunion disjointe, on a prouvé que

$$|G| = |H| \cdot (\# S)$$

cardinal de S.

$\square$.

Déf : Soit G et H deux groupes, notés multiplicativement. On dit qu'une application

$$f : G \to H.$$

est un homomorphisme de groupes, si $\forall g_1, g_2 \in G$

$$f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2).$$

Prop : Si f est un homomorphisme de groupes,

1) $f(e_G) = e_H$ neutre de H

neutre de G

2) $f(g^{-1}) = f(g)^{-1}$.

Preuve 1) Si $g \in G$ on a $e_G \cdot g = g$

donc, en appliquant f, on obtient

$$f(e_G) \cdot f(g) = f(g)$$

en multipliant par $f(g)^{-1} \in H$, $f(e_G) = e_H$.

2) ~~D'apr~~ $f(g \cdot g^{-1}) = f(g) \cdot f(g^{-1})$

$$\overset{\shortparallel}{f(e_G)} = e_H.$$

Donc $f(g)^{-1} = f(g^{-1})$ $\square$

Exemples : (1) $G = (\mathbb{Z}, +)$ et $H = (\mathbb{Z}, +)$

$f : \mathbb{Z} \to \mathbb{Z}$ $f(x) = 2x$ est un homomorphisme de groupes.

(2) $G = (\mathbb{Z}, +)$ et $H = (\mathbb{Z}/_{n\mathbb{Z}}, +)$

$f : \mathbb{Z} \to \mathbb{Z}/_{n\mathbb{Z}}$ $f(x) = x \bmod n = \overline{x}$ est un homomorphisme de groupes.

(3) $G = (\mathbb{R}, +)$ et $H = (\mathbb{R}_+^*, \cdot)$

$f = \exp : \mathbb{R} \to \mathbb{R}_+^*$ $f(x) = \exp(x) = e^x$ est un homomorphisme de groupes.

Déf : Si $f : G \to H$ est un homomorphisme de groupes, on définit le noyau de f, noté

$$\ker(f) = \{ g \in G \mid f(g) = e_H \}.$$

. image de f, noté

$$\mathrm{im}(f) = \{ h \in H \mid \exists g \in G \mid h = f(g) \}.$$

Prop : Si $f : G \to H$ homomorphisme de groupes, alors

. $\ker(f)$ sous-groupe de G

. $\mathrm{im}(f)$ sous-groupe de H.

Preuve : . Il suffit de montrer que $\ker(f)$ est un groupe.

1) $e_G \in \ker(f)$ 2) Si $g_1, g_2 \in \ker(f)$, alors

$$f(g_1 g_2) = f(g_1) \cdot f(g_2) = e_H \cdot e_H = e_H$$

$$\Longleftrightarrow \quad g_1 \cdot g_2 \in \ker(f).$$

3) Si $g \in \ker(f)$, alors $f(g^{-1}) = f(g)^{-1} = e_H^{-1} = e_H$.

. Il suffit de montrer que $\mathrm{im}(f)$ est un groupe.

1) $f(e_G) = e_H \in \mathrm{Im}(f)$ 2) Si $h_1, h_2 \in \mathrm{Im}(f)$, alors $h_1 \cdot h_2 = f(g_1) \cdot f(g_2)$

$$= f(g_1 \cdot g_2)$$

3) $h \in \mathrm{im}(f)$, alors $h^{-1} = f(g)^{-1} = f(g^{-1})$

(voir prop. préc.)

Exemples (voir plus haut)

(1) $\ker(f) = \{0\}$ $\quad \mathrm{im}(f) = 2\mathbb{Z} = \{ 2x \mid x \in \mathbb{Z} \}$

nombres pairs.

(2) $\ker(f) = n\mathbb{Z} = \{ nx \mid x \in \mathbb{Z} \}$.

$$\mathrm{im}(f) = \mathbb{Z}/n\mathbb{Z}.$$

(3) $\ker(f) = \{0\}$ $\quad \mathrm{im}(f) = \mathbb{R}_+^*$

Déf : On dit qu'un homomorphisme de groupes $f : G \to H$ est un **isomorphisme** (de groupes) si f est aussi <u>bijectif</u>. (= injectif et surjectif)

f = homomorphisme de groupes $f : G \to H$

Prop : 1) f injectif $\Longleftrightarrow$ $\ker(f) = \{e_G\}$.

2) f surjectif $\Longleftrightarrow$ $\operatorname{im}(f) = H$.

Preuve : 1) $\boxed{\Rightarrow}$ clair.

$\boxed{\Leftarrow}$ Supposons $f(g_1) = f(g_2)$. Alors $f(g_1 g_2^{-1})$

$= f(g_1) \cdot f(g_2)^{-1} = e_H$

Donc comme on a supposé $\ker(f) = \{e_G\}$,

$g_1 g_2^{-1} = e_G$, donc $g_1 = g_2$.

2) clair. $\square$

Anneaux et corps.

Def : Un anneau est un triplet $(A,+,\cdot)$ tel que.

- $(A,+)$ est un groupe abélien
- $(A,\cdot)$ est un semi-groupe

$\boxed{\text{On dit que } (A,+,\cdot) \text{ est commutatif (ou abélien) si } (A,\cdot) \text{ est abélien}}$

De plus $\forall x,y,z \in A$

$$x\cdot(y+z) = x\cdot y + x\cdot z$$
$$(x+y)\cdot z = xz + yz$$

L'élément neutre de $(A,\cdot)$, s'il existe, est appelé l'élément unité de A. Dans ce cas on dit que A est un anneau unitaire.

Def : Soit $(A,+,\cdot)$ ~~est~~ un anneau. et $a \in A$

- On dit que a est inversible dans $(A,+,\cdot)$ si a est inversible dans le semi-groupe $(A,\cdot)$
- On dit que a est un diviseur de zéro si $a \neq 0$ et s'il existe $b \neq 0$ tel que $a\cdot b = 0$.

Exemple : 1) $(\mathbb{Z},+,\cdot)$ est un anneau unitaire (unité $=1$) commutatif

2) $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ est un anneau unitaire commutatif.