

Chapitre

Groupes

1.1 L'ensemble $\mathbb{Z}/n\mathbb{Z}$

1.1.1

Rappel

Définition

On appelle relation d'équivalence sur un ensemble E toute relation binaire $\mathcal{R}$ vérifiant

- 1) $\mathcal{R}$ est réflexive i.e. $\forall x \in E, x\mathcal{R}x$;
- 2) $\mathcal{R}$ est symétrique i.e. $\forall x, y \in E, x\mathcal{R}y \Rightarrow y\mathcal{R}x$;
- 3) $\mathcal{R}$ est transitive i.e. $\forall x, y, z \in E, x\mathcal{R}y \text{ et } y\mathcal{R}z \Rightarrow x\mathcal{R}z$;

Exemple L'égalité est une relation d'équivalence sur E .

Exemple L'équivalence des suites (ou de fonctions au voisinage de $a \in \bar{\mathbb{R}}$) est une relation d'équivalence.

Exemple L'équivalence des matrices de $M_{n,p}(\mathbb{K})$.

Remarque Plus généralement, pour une application $f : E \rightarrow F$, la relation $\mathcal{R}$ donnée par

$$x\mathcal{R}y \Leftrightarrow f(x) = f(y)$$

définit une relation d'équivalence sur E .

Remarque En fait, une relation d'équivalence se comprend comme « une égalité modulo certains critères ».

1.1.2 Classe d'équivalence

Soit $\mathcal{R}$ une relation d'équivalence sur E .

Définition

On appelle classe d'équivalence d'un élément x de E pour la relation $\mathcal{R}$, le sous-ensemble noté $Cl(x)$ formé des éléments qui sont en relation avec x

$$Cl(x) \stackrel{\text{def}}{=} \{y \in E / x\mathcal{R}y\}$$

La classe d'équivalence de x est encore souvent notée $x, \bar{x}, \dot{x}, \dots$

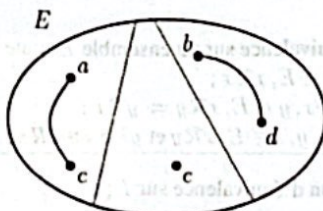
Exemple Considérons $E = \{a, b, c, d, e\}$ et $f : E \rightarrow \{0, 1, 2\}$ définie par

$$f(a) = 0, f(b) = 1, f(c) = 0, f(d) = 1 \text{ et } f(e) = 2$$

La relation $\mathcal{R}$ définie par

$$x\mathcal{R}y \Leftrightarrow f(x) = f(y)$$

est une relation d'équivalence que l'on peut visualiser ainsi



Pour celle-ci $Cl(a) = Cl(c) = \{a, c\}$, $Cl(b) = Cl(d) = \{b, d\}$ et $Cl(e) = \{e\}$.

Remarque $Cl(x)$ réunit les éléments de E qui sont « égaux modulo la relation $\mathcal{R}$ ».

Théorème

- a) $\forall x \in E, x \in Cl(x)$;
 - b) $\forall x, y \in E, x\mathcal{R}y \Rightarrow Cl(x) = Cl(y)$;
 - c) $\forall x, y \in E, x \not\mathcal{R}y \Rightarrow Cl(x) \cap Cl(y) = \emptyset$
- Ainsi une classe d'équivalence n'est jamais vide et deux classes d'équivalence distinctes sont disjointes.

dém. :

$x \in Cl(x)$ car la relation $\mathcal{R}$ est réflexive.

Si $x\mathcal{R}y$ alors pour tout $z \in Cl(y)$ on a $y\mathcal{R}z$ et donc $x\mathcal{R}z$ par transitivité. Ainsi $Cl(y) \subset Cl(x)$ et par symétrie on a l'autre inclusion et donc l'égalité.

Enfin, par contraposée, si $Cl(x) \cap Cl(y) \neq \emptyset$ alors pour un certain $z \in Cl(x) \cap Cl(y)$, on a $x\mathcal{R}z$ et $y\mathcal{R}z$ donc par symétrie et transitivité, on obtient $x\mathcal{R}y$.

□

Remarque Si y est élément d'une classe d'équivalence $Cl(x)$ alors $x\mathcal{R}y$ et donc $Cl(x) = Cl(y)$. Ainsi, tout élément d'une classe d'équivalence détermine celle-ci.

Définition

Tout élément y d'une classe d'équivalence est appelé représentant de celle-ci.

1.1.3 Ensemble quotient

Soit $\mathcal{R}$ une relation d'équivalence sur E . Les classes d'équivalence réalisent une partition de E ; cette partition est obtenue en regroupant entre eux les éléments qui sont « égaux modulo la relation $\mathcal{R}$ ».

Exemple Considérons la relation d'équivalence précédente sur $E = \{a, b, c, d, e\}$. Celle-ci réalise une partition de E en 3 classes d'équivalence.

Définition

On appelle ensemble quotient de E par $\mathcal{R}$ l'ensemble des classes d'équivalence pour relation $\mathcal{R}$.
On le note $E/\mathcal{R}$.

Remarque $E/\mathcal{R}$ se comprend comme l'ensemble obtenu lorsqu'on « identifie entre eux les éléments qui sont égaux modulo $\mathcal{R}$ ».

Exemple L'ensemble $\mathbb{Q}$ des nombres rationnels se construit comme l'ensemble quotient de $\mathbb{Z} \times \mathbb{Z}^*$ pour la relation

$$(a, b)\mathcal{R}(c, d) \Leftrightarrow ad = bc$$

La classe d'équivalence d'un couple (a, b) est alors notée a/b .

1.1.4 L'ensemble $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$.

Définition

On définit sur $\mathbb{Z}$ la relation de congruence modulo n par

$$a \equiv b \quad [n] \Leftrightarrow n \mid (b - a)$$

Proposition

La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

dém. :

La relation est réflexive car $a \equiv a \quad [n]$ puisque $n \mid (a - a)$.

La relation est symétrique car $a \equiv b \quad [n] \Rightarrow b \equiv a \quad [n]$ puisque $n \mid (b - a) \Rightarrow n \mid (a - b)$.

Enfin, la relation est transitive car $a \equiv b \quad [n]$ et $b \equiv c \quad [n] \Rightarrow a \equiv c \quad [n]$ puisque $n \mid (b - a)$ et $n \mid (c - b) \Rightarrow n \mid (c - a)$.

□

1.1. L'ENSEMBLE $\mathbb{Z}/n\mathbb{Z}$

Définition

Pour $a \in \mathbb{Z}$, on note $\bar{a}$ la classe d'équivalence de $a \in \mathbb{Z}$ pour la relation de congruence modulo n .

Ainsi

$$\bar{a} = \{a + kn/k \in \mathbb{Z}\} = a + n\mathbb{Z}$$

Définition

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ pour la relation de congruence modulo n .

Théorème

$\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini à n éléments qui sont

$$\bar{0}, \bar{1}, \dots, \overline{(n-1)}$$

dém. :

$\bar{0}, \bar{1}, \dots, \overline{(n-1)}$ sont des éléments de $\mathbb{Z}/n\mathbb{Z}$.

Pour $a, b \in \{0, \dots, n-1\}$,

$$\bar{a} = \bar{b} \Rightarrow n \mid (b - a) \Rightarrow a = b$$

Par suite, les classes $\bar{0}, \bar{1}, \dots, \overline{(n-1)}$ sont deux à deux distinctes.

Pour tout $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, en considérant le reste $r \in \{0, 1, \dots, n-1\}$ de la division euclidienne de a par n , on obtient $\bar{a} = \bar{r}$. Ainsi toutes les classes d'équivalence figurent parmi $\bar{0}, \bar{1}, \dots, \overline{(n-1)}$.

□

Exemple $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$, $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$, $\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, etc.

Proposition

Pour tout $a, b, a', b' \in \mathbb{Z}$,

$$a \equiv a' \pmod{n} \text{ et } b \equiv b' \pmod{n} \Rightarrow a + b \equiv a' + b' \pmod{n} \text{ et } ab \equiv a'b' \pmod{n}$$

dém. :

$n \mid a' - a$ et $n \mid b' - b$ entraînent $n \mid (a' + b') - (a + b) = (a' - a) + (b' - b)$ et $n \mid (a'b') - (ab) = (a' - a)b' + a(b' - b)$

□

Définition

On définit deux opérations $+$ et $\times$ sur $\mathbb{Z}/n\mathbb{Z}$ en posant

$$\bar{a} + \bar{b} \stackrel{\text{def}}{=} \overline{a + b} \text{ et } \bar{a} \times \bar{b} \stackrel{\text{def}}{=} \overline{ab}$$

Remarque La définition ci-dessus est consistante puisque le résultat de ces opérations ne dépend pas des représentants a, b choisis pour chaque classe.

Exemple Dans $\mathbb{Z}/6\mathbb{Z}$,

$$\bar{3} + \bar{5} = \bar{8} = \bar{2} \text{ ou encore } \bar{3} + \bar{5} = \bar{3} + \bar{-1} = \bar{2}.$$

$$\bar{3} \times \bar{5} = \bar{15} = \bar{3} \text{ ou encore } \bar{3} \times \bar{5} = \bar{3} \times \bar{-1} = \bar{-3} = \bar{3}.$$

1.2 Structure de groupe

1.2.1 Définition

Définition

On appelle groupe tout couple $(G, \star)$ formé d'un ensemble G et d'une loi de composition interne $\star$ sur G vérifiant :

1) $\star$ est associative i.e.

$$\forall a, b, c \in G, (a \star b) \star c = a \star (b \star c);$$

2) $\star$ possède un neutre i.e.

$$\exists e \in G, \forall a \in G, a \star e = a = e \star a$$

cet élément e est alors unique;

3) tout élément de G est symétrisable i.e.

$$\forall a \in G, \exists b \in G, a \star b = e = b \star a$$

cet élément b est alors unique et appelé symétrique de a , noté a^{-1} .

Si de plus la loi $\star$ est commutative, on parle de groupe abélien.

Lorsque la loi est notée $\times$ ou $\cdot$, on dit que le groupe est noté multiplicativement ($e \rightarrow 1$, $a \star b \rightarrow ab$).

Lorsque la loi est notée $+$, on dit que le groupe est noté additivement ($e \rightarrow 0$, $a \star b \rightarrow a + b$, $a^{-1} \rightarrow -a$). Cette dernière notation est réservée au groupe commutatif.

Attention : Lorsque la loi $\star$ n'est pas commutative :

- la neutralité de e se vérifie par deux compositions ;
- l'inversibilité d'un élément se vérifie par deux compositions ;
- on a $(a \star b)^{-1} = b^{-1} \star a^{-1}$.

Exemple $(\mathbb{C}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$ sont des groupes abéliens de neutre 0.

Exemple $(\mathbb{C}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{R}^{+*}, \times)$ sont des groupes abéliens de neutre 1.

Exemple $(GL_n(\mathbb{K}), \times)$ est un groupe non commutatif de neutre I_n .

1.2.2 Itéré d'un élément

Soit $(G, \star)$ un groupe de neutre e .

Définition

Pour $a \in G$ et $k \in \mathbb{Z}$, on note a^k l'itéré d'ordre k de l'élément a :

- pour $k > 0$, $a^k \stackrel{\text{def}}{=} a \star \dots \star a$ (k termes);
- pour $k = 0$, $a^0 \stackrel{\text{def}}{=} e$;
- pour $k < 0$, $a^k \stackrel{\text{def}}{=} a^{-1} \star \dots \star a^{-1}$ ($|k|$ termes).

Proposition

On a

$$\forall k, \ell \in \mathbb{Z}, a^k \star a^\ell = a^{k+\ell} \text{ et } (a^k)^\ell = a^{k\ell}$$

dém. :

Il suffit de discuter selon les signes des exposants d'itérations considérés, c'est un peu lourd...

□

Remarque Si le groupe est noté additivement, on note $k.a$ l'itéré d'ordre k de a . On a alors

$$k.a + \ell.a = (k + \ell).a \text{ et } \ell.(k.a) = (k\ell).a$$

Attention : En général

$$(a \star b)^p \neq a^p \star b^p$$

En effet

$$(a \star b)^p = (a \star b) \star (a \star b) \star \dots \star (a \star b)$$

et

$$a^p \star b^p = (a \star a \star \dots \star a) \star (b \star b \star \dots \star b)$$

Cependant, si a et b commutent alors $(a \star b)^p = a^p \star b^p$

1.2.3 Le groupe symétrique**Définition**

On note S_E l'ensemble des permutations de E i.e. des bijections de E vers E .

Théorème

$(S_E, \circ)$ est un groupe de neutre Id_E .

Ce groupe est non commutatif dès que $\text{Card} E \geq 3$.

Exemple $S_n = S(\{1, \dots, n\})$ est un groupe de cardinal $n!$.

Parmi ses éléments signalons :

- les transpositions $\tau = (i \ j)$ vérifiant $\tau^2 = \text{Id}$;

- les p -cycles $c = (a_1 \ a_2 \ \dots \ a_p)$ vérifiant $c^p = \text{Id}$.

1.2.4 Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Théorème

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien à n éléments de neutre $\bar{0}$.

De plus

$$\forall a \in \mathbb{Z}/n\mathbb{Z}, -a = \overline{(-a)}$$

dém. :

$\bar{a} + \bar{b} = \overline{(a+b)} = \overline{(b+a)} = \bar{b} + \bar{a}$ donc $+$ est commutative sur $\mathbb{Z}/n\mathbb{Z}$.

$(\bar{a} + \bar{b}) + \bar{c} = \overline{(a+b)} + \bar{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \bar{a} + (\bar{b} + \bar{c})$ donc $+$ est associative sur $\mathbb{Z}/n\mathbb{Z}$.

$\bar{a} + \bar{0} = \overline{a+0} = \bar{a} = \bar{0} + \bar{a}$ donc $\bar{0}$ est élément neutre de $(\mathbb{Z}/n\mathbb{Z}, +)$.

$\bar{a} + \overline{(-a)} = \overline{a+(-a)} = \bar{0} = \overline{(-a)} + \bar{a}$ donc $\bar{a}$ est symétrisable et $-\bar{a} = \overline{(-a)}$.

□

Exemple $n = 2, \mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$.

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

Exemple $n = 3, \mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Remarque Dans une table d'opérations, sur chaque ligne figure chaque élément de groupe ; cela provient de la bijectivité de l'application $x \mapsto a * x$ sur G . On a la même propriété sur les colonnes.

Théorème

Pour tout $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ et $k \in \mathbb{Z}$

$$k \cdot \bar{a} = \overline{k \times a}$$

dém. :

Par récurrence pour $k \in \mathbb{N}$.

Cas $k = 0$: $0 \cdot \bar{a} = \bar{0} = \overline{0 \cdot a}$.

Supposons la propriété vraie au rang $k \geq 0$.

$$(k+1) \cdot \bar{a} = k \cdot \bar{a} + \bar{a} = \overline{ka} + \bar{a} = \overline{ka+a} = \overline{(k+1)a}$$

Récurrence établie.

Pour $k \in \mathbb{Z}^-$, on peut écrire $k = -p$ avec $p \in \mathbb{N}$.

On a alors

$$k \cdot \bar{a} = -(p \cdot \bar{a}) = -\overline{pa} = \overline{-pa} = \overline{ka}$$

□

1.2.5 Produit fini de groupes

Définition

Soit $\star_1, \dots, \star_n$ des lois de composition interne sur des ensembles $E_1, \dots, E_n$. On appelle loi produit sur $E = E_1 \times \dots \times E_n$ la loi $\star$ définie par

$$(x_1, \dots, x_n) \star (y_1, \dots, y_n) \stackrel{\text{def}}{=} (x_1 \star_1 y_1, \dots, x_n \star_n y_n)$$

Proposition

Si $(G_1, \star_1), \dots, (G_n, \star_n)$ sont des groupes de neutres $e_1, \dots, e_n$ alors $G = G_1 \times \dots \times G_n$ muni de la loi produit $\star$ est un groupe de neutre $e = (e_1, \dots, e_n)$.

De plus :

- l'inverse d'un élément $(x_1, \dots, x_n) \in G$ est $(x_1^{-1}, \dots, x_n^{-1})$;
- si tous les groupes $(G_1, \star_1), \dots, (G_n, \star_n)$ sont commutatifs, le groupe $(G, \star)$ l'est aussi.

dém. :

Soit $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$ et $z = (z_1, \dots, z_n)$ éléments de $G_1 \times \dots \times G_n$.

On a

$$x \star (y \star z) = (\dots, x_i \star_i (y_i \star_i z_i), \dots)$$

et

$$(x \star y) \star z = (\dots, (x_i \star_i y_i) \star_i z_i, \dots)$$

Puisque les lois $\star_i$ sont associatives, on obtient

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

L'élément e est neutre car

$$x \star e = (\dots, x_i \star_i e_i, \dots) = x \text{ et } e \star x = (\dots, e_i \star_i x_i, \dots) = x$$

L'élément x est symétrisable de symétrique $x' = (x_1^{-1}, \dots, x_n^{-1})$ car

$$x \star x' = (\dots, x_i \star_i x_i^{-1}, \dots) = e \text{ et } x' \star x = (\dots, x_i^{-1} \star_i x_i, \dots) = e$$

Ainsi $(G, \star)$ est bien un groupe.

Si de plus les lois $\star_i$ sont toutes commutatives

$$x \star y = (\dots, x_i \star_i y_i, \dots) = (\dots, y_i \star_i x_i, \dots) = y \star x$$

□

Exemple Si $(G, \star)$ est un groupe de neutre e alors $(G^n, \star)$ est un groupe de neutre $(e, \dots, e)$.

Exemple Pour $(G_1, \star_1) = (G_2, \star_2) = (\mathbb{Z}, +)$, la loi produit sur $\mathbb{Z}^2$ que nous notons $+$ est définie par :

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$

$(\mathbb{Z}^2, +)$ est un groupe abélien de neutre $0_{\mathbb{Z}^2} = (0, 0)$.

Exemple Pour $(G_1, \star_1) = (\mathbb{R}^+, \times)$ et $(G_2, \star_2) = (\mathbb{R}, +)$, la loi produit sur $\mathbb{R}^+ \times \mathbb{R}$ que nous notons $\star$ est définie par :

$$(r, \theta) \star (r', \theta') = (rr', \theta + \theta')$$

$(\mathbb{R}^+ \times \mathbb{R}, \star)$ est alors un groupe abélien de neutre $e = (1, 0)$.

De plus

$$(r, \theta)^{-1} = (1/r, -\theta)$$

1.3 Sous-groupes

$(G, \star)$ désigne un groupe de neutre e .

1.3.1 Définition

Définition

On appelle sous-groupe d'un groupe $(G, \star)$ toute partie H de G vérifiant :

- 1) $e \in H$;
- 2) $\forall x, y \in H, x \star y^{-1} \in H$.

Exemple $\{e\}$ et G des sont sous-groupes de $(G, \star)$.

Remarque Le point 1) peut aussi être transposé en $H \neq \emptyset$ car alors $H \neq \emptyset$ et 2) entraîne $e \in H$.
Le point 2) peut aussi être transposé en 2a) $\forall x, y \in H, x \star y \in H$ et 2.b) $\forall x \in H, x^{-1} \in H$.

Remarque Si le groupe est noté additivement 1) et 2) se relisent $0 \in H$ et $\forall x, y \in H, x - y \in H$.

Théorème

Si H est un sous-groupe d'un groupe $(G, \star)$ alors $(H, \star)$ est un groupe de même neutre.

Exemple L'ensemble des racines n -ième de l'unité est

$$U_n = \{z \in \mathbb{C} / z^n = 1\}$$

C'est un sous-groupe de $(\mathbb{C}^*, \times)$.

$(U_n, \times)$ est le groupe des racines n -ième de l'unité.

Rappelons

$$U_n = \{e^{2ik\pi/n} / k \in [0, n-1]\} = \{\omega^k / k \in [0, n-1]\}$$

avec $\omega = e^{2i\pi/n}$.

Exemple L'ensemble des matrices orthogonale est

$$\mathcal{O}_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) / {}^tAA = I_n\}$$

C'est un sous-groupe de $(GL_n(\mathbb{R}), \times)$.

$(\mathcal{O}_n(\mathbb{R}), \times)$ est un groupe, c'est le groupe orthogonal d'ordre n .

1.3. SOUS-GROUPES

1.3.2 Intersection d'une famille de sous-groupes

Théorème

Si $(H_i)_{i \in I}$ est une famille de sous-groupes de $(G, *)$ alors leur intersection $H = \bigcap_{i \in I} H_i$ est un sous-groupe de $(G, *)$.

dém. :

$H \subset G$ et $e \in H$ car e est élément de chaque H_i .

Soit $x, y \in H$. Pour tout $i \in I$, $x, y \in H_i$ donc $x * y^{-1} \in H_i$ puis $x * y^{-1} \in H$.

□

Remarque La réunion de deux sous-groupes n'est pas un sous-groupe sauf cas d'inclusion de l'un dans l'autre.

1.3.3 Sous-groupe engendré par un élément

Définition

On appelle sous-groupe engendré par un élément $a \in G$ l'ensemble

$$\langle a \rangle = \{a^k / k \in \mathbb{Z}\}$$

Remarque En notation additive,

$$\langle a \rangle = \{k.a / k \in \mathbb{Z}\}$$

Théorème

$\langle a \rangle$ est un sous-groupe de $(G, *)$ contenant a .

De plus, pour tout sous-groupe H de G

$$a \in H \Rightarrow \langle a \rangle \subset H$$

Ainsi $\langle a \rangle$ apparaît comme le plus petit sous-groupe contenant a .

dém. :

$\langle a \rangle \subset G$, $e = a^0 \in \langle a \rangle$ et pour tout $x, y \in \langle a \rangle$, on peut écrire $x = a^k$, $y = a^l$ avec $k, l \in \mathbb{Z}$ et alors

$$x * y^{-1} = a^{k-l} \in \langle a \rangle$$

$\langle a \rangle$ est donc un sous-groupe de $(G, *)$ et $a = a^1 \in \langle a \rangle$.

De plus, si H est un sous-groupe de $(G, *)$ contenant a alors

$$a^0 = e \in H, a^1 = a \in H, a^2 = a * a \in H, a^3 = a^2 * a \in H, \dots$$

Par une récurrence facile,

$$\forall k \in \mathbb{N}, a^k \in H$$

Pour $k \in \mathbb{Z}^-$, $k = -p$ avec $p \in \mathbb{N}$, $a^k = a^{-p} = (a^p)^{-1} \in H$ car $a^p \in H$.

Ainsi

$$\forall k \in \mathbb{Z}, a^k \in H$$

ce qui signifie $\langle a \rangle \subset H$.

□

Remarque Même si la loi $\star$ n'est pas commutative, le sous-groupe $\langle a \rangle$ est commutatif car

$$a^k \star a^\ell = a^{k+\ell} = a^{\ell+k} = a^\ell \star a^k$$

□

Exemple Dans $(\mathbb{C}, +)$,

$$\langle a \rangle = \{ak/k \in \mathbb{Z}\} = a\mathbb{Z}$$

Exemple Dans $(\mathbb{C}^*, \times)$,

$$\langle a \rangle = \{a^k/k \in \mathbb{Z}\}$$

En particulier

$$\langle 2 \rangle = \{2^k/k \in \mathbb{Z}\} = \{\dots, 1/8, 1/4, 1/2, 1, 2, 4, 8, \dots\}$$

et pour $\omega = e^{2\pi i/n}$

$$\langle \omega \rangle = \{\omega^k/k \in \mathbb{Z}\} = \{1, \omega, \dots, \omega^{n-1}\} = U_n$$

car $\omega^n = 1$.

Exemple Dans $(S_4, \circ)$ considérons le cycle $c = (1 \ 2 \ 3 \ 4)$.

$$\langle c \rangle = \{\text{Id}, (1 \ 2 \ 3 \ 4), (1 \ 3 \ 2 \ 4), (2 \ 4 \ 1 \ 3), (4 \ 3 \ 2 \ 1)\}$$

1.3.4 Sous-groupe engendré par une partie

Définition

On appelle groupe engendré par une partie A de G l'intersection de tous les sous-groupes de $(G, \star)$ qui contiennent A . On le note $\langle A \rangle$.

Théorème

$\langle A \rangle$ est un sous-groupe de $(G, \star)$ qui contient A .

De plus, pour tout sous-groupe H de $(G, \star)$,

$$A \subset H \Rightarrow \langle A \rangle \subset H$$

Ainsi $\langle A \rangle$ apparaît comme le plus petit sous-groupe contenant A .

dém. :

Posons $\mathcal{S} = \{H \text{ sous-groupe de } (G, \star) / A \subset H\}$. Par définition

$$\langle A \rangle = \bigcap_{H \in \mathcal{S}} H$$

$\langle A \rangle$ est un sous-groupe car intersection d'une famille de sous-groupes.

Puisque A est inclus dans chaque $H \in \mathcal{S}$, on a $A \subset \langle A \rangle$.

Enfin, si H est un sous-groupe de $(G, *)$

$$A \subset H \Rightarrow H \in \mathcal{S} \Rightarrow \langle A \rangle \subset H$$

□

Exemple Pour $a \in G$,

$$\langle \{a\} \rangle = \{a^k / k \in \mathbb{Z}\} = \langle a \rangle$$

Exemple Pour $a, b \in G$,

$$\langle \{a, b\} \rangle = \{a^{k_1} b^{\ell_1} \dots a^{k_n} b^{\ell_n} / n \in \mathbb{N}^*, k_1, \dots, k_n, \ell_1, \dots, \ell_n \in \mathbb{Z}\}$$

En fait

$$\langle \{a, b\} \rangle = \{\text{produits finis d'itérés de } a \text{ et } b\}$$

Si a et b commutent, on peut simplifier

$$\langle \{a, b\} \rangle = \{a^k b^\ell / k, \ell \in \mathbb{Z}\}$$

Exemple Dans $(\mathbb{Z}^2, +)$

$$\langle \{(a, b), (c, d)\} \rangle = \{(ka + \ell c, kb + \ell d) / k, \ell \in \mathbb{Z}\}$$

On peut montrer que ce groupe se confond avec $\mathbb{Z}^2$ si, et seulement si, $ad - bc = \pm 1$.

Exemple Dans S_n , considérons $\mathcal{T}$ l'ensemble des transpositions éléments de S_n . On a

$$\langle \mathcal{T} \rangle = S_n$$

car il est connu que toute permutation peut s'écrire comme un produit de transpositions.

1.3.5 Les sous-groupes de $(\mathbb{Z}, +)$

Théorème

Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

dém. :

$n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ car

$$n\mathbb{Z} = \{kn / k \in \mathbb{Z}\} = \langle n \rangle$$

Inversement, soit H un sous-groupe de $(\mathbb{Z}, +)$.

Cas $H = \{0\}$: on a $H = n\mathbb{Z}$ avec $n = 0$.

Cas $H \neq \{0\}$: on introduit $H^+ = \{x \in H / x > 0\}$.

Il existe $x_0 \in H$ tel que $x_0 \neq 0$. Si $x_0 > 0$ alors $x_0 \in H^+$, sinon $-x_0 \in H^+$. Dans les deux cas $H^+ \neq \emptyset$.

Rappelons : Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Ici H^+ est une partie non vide de $\mathbb{N}$, on peut donc introduire $n = \min H^+$.

On a $n \in H$ donc $n\mathbb{Z} = \langle n \rangle \subset H$.

Inversement, soit $x \in H$. Par division euclidienne, $x = qn + r$ avec $0 \leq r < n$.

On a alors $r = x - qn \in H$ car $qn \in n\mathbb{Z} \subset H$.

Si $r > 0$ alors $r \in H^+$ ce qui est impossible car $r < n = \min H^+$.

Il reste $r = 0$ et donc $x = qn \in n\mathbb{Z}$.

Ainsi $H \subset n\mathbb{Z}$ puis par double inclusion $H = n\mathbb{Z}$.

□

Remarque Le naturel n tel que $H = n\mathbb{Z}$ est unique car
Si $H = \{0\}$ alors $n = 0$ et si $H \neq \{0\}$ alors $n = \min \{x \in H/x > 0\}$.

1.4 Morphisme de groupes

Soit $(G, *)$, $(G', \cdot)$ et $(G'', \cdot)$ des groupes.

1.4.1 Définition

Définition

On appelle morphisme du groupe $(G, *)$ vers le groupe $(G', \cdot)$ toute application $\varphi : G \rightarrow G'$ vérifiant

$$\forall x, y \in G, \varphi(x * y) = \varphi(x) \cdot \varphi(y)$$

Exemple L'application constante $\varphi : G \rightarrow G'$ définie par $\varphi(x) = e$ est un morphisme du groupe $(G, *)$ vers lui-même.

Exemple L'identité Id_G est un morphisme du groupe $(G, *)$ vers lui-même.

Remarque Un morphisme d'un groupe vers lui-même est souvent appelé endomorphisme.

Exemple $\ln$ est un morphisme de $(\mathbb{R}^{++}, \times)$ vers $(\mathbb{R}, +)$.

En effet, pour tout $a, b > 0$,

$$\ln(ab) = \ln(a) + \ln(b)$$

Exemple $\exp$ est un morphisme de $(\mathbb{C}, +)$ vers $(\mathbb{C}^*, \times)$.

En effet, pour tout $z, z' \in \mathbb{C}$,

$$\exp(z + z') = \exp(z) \exp(z')$$

Exemple Le déterminant définit par restriction un morphisme de $(\text{GL}_n(\mathbb{K}), \times)$ vers $(\mathbb{K}^*, \times)$

1.4. MORPHISME DE GROUPE

Exemple La signature $\varepsilon : S_n \rightarrow \{1, -1\}$ avec

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

est un morphisme du groupe $(S_n, \circ)$ vers $(\{1, -1\}, \times)$.

En effet,

$$\forall \sigma, \sigma' \in S_n, \varepsilon(\sigma \circ \sigma') = \varepsilon(\sigma) \times \varepsilon(\sigma')$$

Rappelons que si τ est une transposition alors $\varepsilon(\tau) = -1$.

En conséquence, si c est un cycle de longueur p alors $\varepsilon(c) = (-1)^{p-1}$ car c est un produit de $p-1$ transpositions

$$(a_1 \ a_2 \ \dots \ a_p) = (a_1 \ a_2) \circ (a_2 \ a_3) \circ \dots \circ (a_{p-1} \ a_p)$$

Exemple Soit a un élément d'un groupe $(G, *)$.

L'application $\varphi : \mathbb{Z} \rightarrow G$ définie par $\varphi(k) = a^k$ est un morphisme de groupes.

En effet

$$\varphi(n+p) = a^{n+p} = a^n * a^p = \varphi(n) * \varphi(p)$$

1.4.2 Propriétés

Proposition

Si $\varphi : G \rightarrow G'$ et $\psi : G' \rightarrow G''$ sont des morphismes de groupes alors $\psi \circ \varphi : G \rightarrow G''$ en est un aussi.

dém. :

Soit $x, y \in G$. On a

$$\psi \circ \varphi(x * y) = \psi(\varphi(x) \top \varphi(y)) = (\psi \circ \varphi(x)) \top (\psi \circ \varphi(y))$$

□

Remarque La composée de deux endomorphismes d'un groupe $(G, *)$ est un endomorphisme du groupe $(G, *)$.

Proposition

Si φ est un morphisme d'un groupe $(G, *)$ vers un groupe $(H, \top)$ alors

$$\varphi(e) = e' \text{ et } \forall x \in G, \varphi(x^{-1}) = \varphi(x)^{-1}$$

Plus généralement

$$\forall x \in G, \forall n \in \mathbb{Z}, \varphi(x^n) = \varphi(x)^n$$

dém. :

$\varphi(e) = \varphi(e * e) = \varphi(e) \top \varphi(e)$ et en composant par $\varphi(e)^{-1}$ on obtient $e' = \varphi(e)$.

Aussi $\varphi(x) \top \varphi(x^{-1}) = \varphi(x * x^{-1}) = \varphi(e) = e'$ donc en composant par $\varphi(x)^{-1}$ à gauche on obtient

$$\varphi(x^{-1}) = \varphi(x)^{-1}$$

Par récurrence, on vérifie aisément

$$\forall n \in \mathbb{N}, \varphi(x^n) = \varphi(x)^n$$

puis par passage au symétrique, on étend cette propriété à $n \in \mathbb{Z}$.

□

Remarque On peut aussi établir

$$\forall x_1, \dots, x_n \in G, f\left(\prod_{i=1}^n x_i\right) = \prod_{i=1}^n f(x_i)$$

Théorème

L'image directe (resp. réciproque) d'un sous-groupe par un morphisme de groupes est un sous-groupe.

dém. :

Soit $\varphi : G \rightarrow G'$ morphisme de groupes.

Soit H un sous-groupe de $(G, *)$. Montrons que

$$\varphi(H) = \{\varphi(x) \mid x \in H\}$$

est un sous-groupe de $(G', \top)$.

D'une part $e' \in \varphi(H)$ car $e' = \varphi(e)$ avec $e \in H$.

D'autre part, pour $x', y' \in \varphi(H)$, on peut écrire $x' = \varphi(x)$ et $y' = \varphi(y)$ avec $x, y \in H$ et alors

$$x' \top y'^{-1} = \varphi(x \star y^{-1}) \in \varphi(H)$$

car $x \star y^{-1} \in H$.

Ainsi $\varphi(H)$ est un sous-groupe de $(G', \top)$.

Soit H' un sous-groupe de $(G, \star)$. Montrons que

$$\varphi^{-1}(H') = \{x \in G \mid \varphi(x) \in H'\}$$

est un sous-groupe de $(G, \star)$.

D'une part $e \in \varphi^{-1}(H')$ car $\varphi(e) = e' \in H'$.

D'autre part, pour $x, y \in \varphi^{-1}(H')$, on a $\varphi(x \star y^{-1}) = \varphi(x) \top \varphi(y)^{-1} \in H'$ car $\varphi(x), \varphi(y) \in H'$.

Ainsi $\varphi^{-1}(H')$ est un sous-groupe de $(G, \star)$.

□

1.4.3 Noyau et image

Définition

Si φ est un morphisme du groupe $(G, \star)$ vers le groupe $(G', \top)$, on introduit

- son noyau $\ker \varphi = \varphi^{-1}(\{e'\})$ qui est un sous-groupe de $(G, \star)$;
- son image $\text{Im } \varphi = \varphi(G)$ qui est un sous-groupe de $(G', \top)$.

Exemple Déterminons image et noyau du morphisme de $\varphi : \mathbb{C}^* \rightarrow \mathbb{C}^*$ défini par $\varphi(z) = |z|$.

$\text{Im } \varphi = \mathbb{R}^{++}$ et $\ker \varphi = \mathbb{U}$

1.4. MORPHISME DE GROUPE

Exemple Déterminons image et noyau du morphisme $\exp : \mathbb{C} \rightarrow \mathbb{C}^*$.

Pour $z = a + ib$, on a $\exp(z) = e^a e^{ib}$.

Pour $Z \in \mathbb{C}^*$, on peut écrire $Z = re^{i\theta}$.

En posant $z = \ln r + i\theta$, on a $\exp(z) = Z$. Ainsi

$$\text{Im}(\exp) = \mathbb{C}^*$$

Aussi, pour $z = a + ib$

$$\exp(z) = 1 \Leftrightarrow e^a = 1 \text{ et } e^{ib} = 1$$

Par suite

$$\ker(\exp) = 2i\pi\mathbb{Z}$$

Exemple Déterminons image et noyau de $\det : \text{GL}_n(\mathbb{K}) \rightarrow \mathbb{K}^*$.

On a $\text{Im det} = \mathbb{K}^*$ car avec une matrice diagonale il est facile de construire une matrice inversible de déterminant tel que voulu. Aussi

$$\ker \det = \{M \in \text{GL}_n(\mathbb{K}) / \det M = 1\} = \text{SL}_n(\mathbb{K})$$

appelé groupe spécial linéaire d'ordre n .

Exemple Déterminons image et noyau de $\varepsilon : \mathfrak{S}_n \rightarrow \{-1, 1\}$ pour $n \geq 2$.

On a $\text{Im } \varepsilon = \{1, -1\}$ et

$$\ker \varepsilon = \mathfrak{A}_n$$

appelé groupe alterné (ou groupe des permutations paires).

Théorème

Soit φ un morphisme du groupe $(G, \star)$ vers le groupe $(G', \top)$.

a) φ est injectif si, et seulement si, $\ker \varphi = \{e\}$.

b) φ est surjectif si, et seulement si, $\text{Im } \varphi = G'$.

dém. :

a) Si φ est injectif, e' possède au plus un antécédent par φ . Puisque $\varphi(e) = e'$, on obtient

$$\ker \varphi = \{e\}$$

Inversement, supposons $\ker \varphi = \{e\}$. Soit $x, y \in G$ tels que $\varphi(x) = \varphi(y)$.

On a $\varphi(x \star y^{-1}) = \varphi(x) \top \varphi(y)^{-1} = e'$ et donc $x \star y^{-1} \in \ker \varphi$. Ainsi $x \star y^{-1} = e$ puis $x = y$.

b) C'est une évidence et ne dépend du fait que φ soit un morphisme.

□

1.4.4 Isomorphisme de groupes

Définition

On appelle isomorphisme de groupes tout morphisme de groupes bijectif.

Exemple $\ln : \mathbb{R}^{+*} \rightarrow \mathbb{R}$ est un isomorphisme de $(\mathbb{R}^{+*}, \times)$ vers $(\mathbb{R}, +)$.

Proposition

Si $\varphi : G \rightarrow G'$ et $\psi : G' \rightarrow G''$ sont des isomorphismes de groupes alors $\psi \circ \varphi : G \rightarrow G''$ en est un aussi.

Théorème

Si $\varphi : G \rightarrow G'$ est un isomorphisme de groupes alors $\varphi^{-1} : G' \rightarrow G$ est un isomorphisme de groupes.

dém. :

dém. :

Pour tout $x', y' \in G'$, il existe $x, y \in G$ tel que $\varphi(x) = x'$ et $\varphi(y) = y'$.

On a alors

$$\varphi^{-1}(x' \star y') = \varphi^{-1}(\varphi(x) \star \varphi(y)) = \varphi^{-1}(\varphi(x \star y)) = x \star y = \varphi^{-1}(x') \star \varphi^{-1}(y')$$

Ainsi φ^{-1} est un morphisme de groupes et il est de plus bien connu que φ^{-1} est bijective.

□

Définition

On appelle **automorphisme** du groupe $(G, \star)$ tout isomorphisme du groupe $(G, \star)$ dans lui-même.

Exemple Si a est un élément du groupe $(G, \star)$ alors l'application $\tau_a : G \rightarrow G$ définie par

$$\tau_a(x) = a \star x \star a^{-1}$$

est un automorphisme de groupe.

Proposition

L'ensemble $\text{Aut}(G)$ des automorphismes d'un groupe $(G, \star)$ est un sous-groupe de $(S_G, \circ)$.

dém. :

$\text{Aut}(G)$ est bien une partie de S_G .

L'identité est automorphisme de groupe, la composée de deux automorphismes de groupe est un automorphisme de groupe et, enfin, l'application réciproque d'un automorphisme de groupe est encore un automorphisme de groupe.

□

1.4.5 Groupes isomorphes**Définition**

S'il existe un isomorphisme entre deux groupes, ceux-ci sont dits **isomorphes**.
Ceux-ci se comportent alors de façon identique d'un point de vue calculatoire.

Exemple Les groupes $(\mathbb{R}^{++}, \times)$ et $(\mathbb{R}, +)$ sont isomorphes (via le logarithme népérien).

La multiplication sur $\mathbb{R}^{++}$ et l'addition sur $\mathbb{R}$ ont les mêmes propriétés.

En revanche les groupes $(\mathbb{R}^*, \times)$ et $(\mathbb{R}, +)$ ne sont pas isomorphes.

En effet, l'équation $x^2 = 1$ possède deux solutions dans $(\mathbb{R}^*, \times)$ alors que l'équation analogue $2x = 0$ n'en possède qu'une dans $(\mathbb{R}, +)$.

Exemple Comparons les tables d'opérations dans $(\mathbb{Z}/4\mathbb{Z}, +)$ et $(U_4, \times)$:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\times$	1	i	-1	-i
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	1	1	i	-1	-i
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	i	i	-1	-i	1
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	-1	-1	-i	1	i
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	-i	-i	1	i	-1

Les deux groupes $(\mathbb{Z}/4\mathbb{Z}, +)$ et $(U_4, \times)$ se comportent de façon semblables ; ils sont isomorphes via l'application φ qui envoie $\bar{k}$ sur i^k .

Exemple Considérons en revanche la table d'opérations dans $((\mathbb{Z}/2\mathbb{Z})^2, +)$:

+	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

en notant $\begin{cases} e = (\bar{0}, \bar{0}) \\ a = (\bar{1}, \bar{0}) \\ b = (\bar{0}, \bar{1}) \\ c = (\bar{1}, \bar{1}) \end{cases}$

$((\mathbb{Z}/2\mathbb{Z})^2, +)$ se comporte d'une façon différente ; il n'est pas isomorphe aux groupes précédents.

1.5 Groupes engendré par un élément

1.5.1 Groupes monogènes

Définition

Un groupe $(G, \star)$ est dit monogène s'il existe $a \in G$ tel que $G = \langle a \rangle$.
Cet élément a est alors appelé générateur du groupe.

Remarque Un groupe monogène est nécessairement commutatif car

$$a^k \star a^\ell = a^{k+\ell} = a^\ell \star a^k$$

Exemple $(\mathbb{Z}, +)$ est monogène car $\mathbb{Z} = \langle 1 \rangle$.

Exemple $(U_n, \times)$ est monogène car $U_n = \langle \omega \rangle$ avec $\omega = e^{2i\pi/n}$.

Exemple $(\mathbb{C}, +)$ et $(\mathbb{C}^*, \times)$ ne sont pas des groupes monogènes.

Exemple Pour $n \geq 3$, le groupe $(S_n, \circ)$ n'est pas monogène car non commutatif.

1.5.2 Groupes cycliques

Définition

Un groupe est dit cyclique s'il est monogène et fini.

Exemple $(U_n, \times)$ est un groupe cyclique.

Théorème

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique dont les générateurs sont les $\bar{m}$ pour $m \in \mathbb{Z}$ avec $m \wedge n = 1$.

dém. :

$\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$ car

$$\langle \bar{1} \rangle = \{k \cdot \bar{1} / k \in \mathbb{Z}\} = \{\bar{k} / k \in \mathbb{Z}\} = \mathbb{Z}/n\mathbb{Z}$$

Si $\bar{m}$ est générateur de $\mathbb{Z}/n\mathbb{Z}$ alors il existe $k \in \mathbb{Z}$ tel que $k \cdot \bar{m} = \bar{1}$ et donc $km \equiv 1 \pmod{n}$. Il existe alors $\ell \in \mathbb{Z}$ tel que

$$km + n\ell = 1$$

et ainsi $m \wedge n = 1$ en vertu du théorème de Bézout.

Inversement, si $m \wedge n = 1$ alors il existe $k, \ell \in \mathbb{Z}$ tels que $km + \ell n = 1$ et donc

$$km \equiv 1 \pmod{n}$$

d'où $k \cdot \bar{m} = \bar{1}$. Ainsi $\bar{1} \in \langle \bar{m} \rangle$ or $\langle \bar{1} \rangle = \mathbb{Z}/n\mathbb{Z}$ donc

$$\langle \bar{m} \rangle = \mathbb{Z}/n\mathbb{Z}$$

□

1.5.3 Description des groupes monogènes

Théorème

Soit $(G, \star)$ un groupe monogène.

Si $\text{Card}G = +\infty$ alors $(G, \star)$ est isomorphe à $(\mathbb{Z}, +)$.

Si $\text{Card}G = n \in \mathbb{N}^*$ alors $(G, \star)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

dém. :

Soit a un générateur de G . L'application $\varphi : \mathbb{Z} \rightarrow G$ définie par $\varphi(k) = a^k$ est un morphisme de groupes car

$$\varphi(k + \ell) = a^{k+\ell} = a^k \star a^\ell = \varphi(k) \star \varphi(\ell)$$

Il est de plus surjectif car a est générateur de G et donc

$$G = \{a^k / k \in \mathbb{Z}\}$$

Le noyau de φ est un sous-groupe de $(\mathbb{Z}, +)$. Il existe donc $n \in \mathbb{N}$ tel que $\ker \varphi = n\mathbb{Z}$.

Cas $n = 0$: φ est injectif, c'est un isomorphisme de groupes. $(G, \star)$ est alors isomorphe à $(\mathbb{Z}, +)$ et G est de cardinal infini.

Cas $n \neq 0$: On a

$$\varphi(k) = \varphi(\ell) \Leftrightarrow k - \ell \in \ker \varphi$$

donc

$$a^k = a^\ell \Leftrightarrow k \equiv \ell \pmod{n}$$

On peut alors considérer l'application $\varphi : \mathbb{Z}/n\mathbb{Z} \rightarrow G$ déterminée par $\varphi(\bar{k}) = a^k$.
 φ est un morphisme de groupes car

$$\varphi(\bar{k} + \bar{\ell}) = \varphi(\overline{k+\ell}) = a^{k+\ell} = a^k \star a^\ell = \varphi(\bar{k}) \star \varphi(\bar{\ell})$$

D'une part $\text{Im } \varphi = \{a^k / k \in \mathbb{Z}\} = G$ et d'autre part

$$\bar{k} \in \ker \varphi \Leftrightarrow a^k = a^0 \Leftrightarrow \bar{k} = \bar{0}$$

donc $\ker \varphi = \{\bar{0}\}$. On en déduit que φ définit un isomorphisme.

Le groupe $(G, \star)$ est alors isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$ et en particulier G est de cardinal n .

□

Corollaire

$(\mathbb{Z}/n\mathbb{Z}, +)$ et $(U_n, \times)$ sont isomorphes via l'application $\bar{k} \mapsto \omega^k = e^{2ik\pi/n}$.

Les générateurs de $(U_n, \times)$ sont donc les $\omega^m = e^{2im\pi/n}$ avec $m \wedge n = 1$.

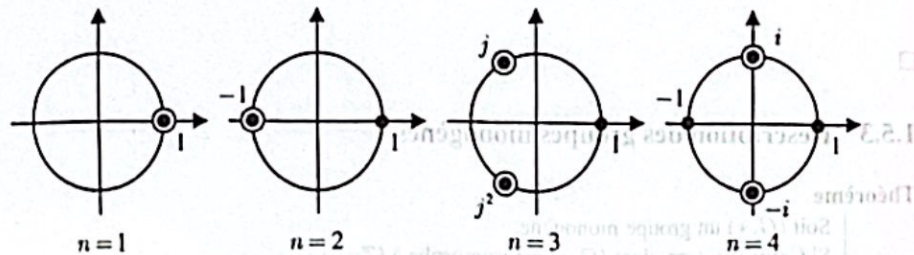
Ces éléments sont appelés racines primitives n -ième de l'unité.

dém. :

Puisque ω est générateur de $(U_n, \times)$, l'application $\varphi : \bar{k} \mapsto \omega^k$ est un isomorphisme de groupes. Celui-ci échange les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$ avec ceux de $(U_n, \times)$.

□

Exemple Déterminons les générateurs des groupes $(U_1, \times)$, $(U_2, \times)$, $(U_3, \times)$, $(U_4, \times)$.



1.5.4 Ordre d'un élément dans un groupe

Définition

On dit qu'un élément a d'un groupe $(G, \star)$ est d'ordre fini s'il existe $n \in \mathbb{N}^*$ vérifiant $a^n = e$.
 On appelle alors ordre de a le plus petit $n \in \mathbb{N}^*$ vérifiant $a^n = e$.

Exemple Dans $(\mathbb{C}^*, \times)$, l'élément 2 n'est pas d'ordre fini.

En revanche, l'élément $\omega = e^{2i\pi/n}$ est d'ordre fini égal à n .

Exemple Le neutre e est l'unique élément d'ordre fini égal à 1 du groupe $(G, \star)$.

Théorème

Si a est d'ordre fini égal à n alors

$$\forall m \in \mathbb{Z}, a^m = e \Leftrightarrow n \mid m$$

dém. :

($\Leftarrow$) immédiat.

($\Rightarrow$) Supposons $a^m = e$ et introduisons le reste r de la division euclidienne de m par n .

$$m = qn + r \text{ avec } 0 \leq r < n$$

On a

$$a^r = a^{m-qn} = a^m \cdot (a^n)^{-q} = e$$

Or n est le plus petit naturel non nul vérifiant $a^n = e$ donc $r = 0$ puis n divise m .

□

Exemple Si a est d'ordre n alors a^k est d'ordre $n/\text{pgcd}(n, k)$.

Corollaire

On a alors

$$\forall k, \ell \in \mathbb{Z}, a^k = a^\ell \Leftrightarrow k \equiv \ell \pmod{n}$$

dém. :

Car

$$a^k = a^\ell \Leftrightarrow a^{k-\ell} = e$$

□

Théorème

Si a est un élément d'ordre fini d'un groupe $(G, *)$ alors son ordre n est le cardinal du sous-groupe $\langle a \rangle$ qu'il engendre et ce dernier est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$

dém. :

$$\langle a \rangle = \{a^k / k \in \mathbb{Z}\} = \{e, a, \dots, a^{n-1}\}$$

avec $e, a, \dots, a^{n-1}$ deux à deux distincts.

$\langle a \rangle$ est un groupe cyclique à n éléments donc isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$ via $\varphi : k \mapsto a^k$.

□

1.5.5 Élément d'un groupe fini**Théorème**

Si $(G, *)$ est un groupe fini de cardinal n alors

$$\forall a \in G, a^n = e$$

$$(a^n)^{-1} = a^n$$

dém. :

Cas $(G, \star)$ commutatif

Soit $a \in G$. L'application $\tau : x \mapsto a \star x$ est une permutation de G . On en déduit

$$\prod_{x \in G} \tau(x) = \prod_{x \in G} x$$

Or

$$\prod_{x \in G} \tau(x) = \prod_{x \in G} (a \star x) = a^{\text{Card}G} \star \prod_{x \in G} x$$

Et par conséquent

$$a^{\text{Card}G} = e$$

Cas général

On définit sur G une relation binaire $\mathcal{R}$ en posant

$$x \mathcal{R} y \Leftrightarrow \exists k \in \mathbb{Z}, y = a^k \star x$$

On vérifie aisément que $\mathcal{R}$ est une relation d'équivalence et que pour tout $x \in G$

$$Cl(x) = \{b \star x / b \in \langle a \rangle\}$$

En particulier

$$\forall x \in G, \text{Card}Cl(x) = \text{Card} \langle a \rangle$$

En notant p le nombre de classe d'équivalence de la relation $\mathcal{R}$, on obtient

$$\text{Card}G = np$$

□

Corollaire

Si $(G, \star)$ est un groupe fini alors tous ses éléments sont d'ordre fini et leur ordre divise le cardinal du groupe.

Exemple Dans $(\mathbb{Z}/6\mathbb{Z}, +)$, $\bar{0}$ est d'ordre 1, $\bar{3}$ est d'ordre 2, $\bar{2}, \bar{4}$ sont d'ordre 3 et $\bar{1}, \bar{5}$ sont d'ordre 6.

Exemple Dans un groupe à 6 éléments, il peut y avoir des éléments d'ordre 2 et 3, mais pas d'éléments d'ordre 4.

1.5.6 Musculation : sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$

Exemple Montrer que les sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont cycliques. Soit H un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$.

Posons $A = \{x \in \mathbb{Z} / \bar{x} \in H\}$. On vérifie aisément que A est un sous-groupe de $(\mathbb{Z}, +)$ et donc il existe $c \in \mathbb{N}$ tel que $A = c\mathbb{Z}$. Pour $x \in \mathbb{Z}$, on a

$$\bar{x} \in H \Leftrightarrow \exists k \in \mathbb{Z}, x = kc \Leftrightarrow \exists k \in \mathbb{Z}, \bar{x} = k.\bar{c}$$

On en déduit

$$H = \langle \bar{c} \rangle$$

Exemple Montrons que $(\mathbb{Z}/n\mathbb{Z}, +)$ possède un unique sous-groupe de cardinal d pour chaque d divisant n . Soit d un diviseur de n . Posons $c = n/d$ et $H = \langle \bar{c} \rangle$. On a

$$H = \{\bar{0}, \bar{c}, 2\bar{c}, \dots, (d-1)\bar{c}\}$$

et H est un sous-groupe à exactement d éléments.

Inversement, soit H un sous-groupe à d éléments de $(\mathbb{Z}/n\mathbb{Z}, +)$.

Tout élément de H d'ordre divisant d et donc

$$\forall \bar{x} \in H, d \cdot \bar{x} = \bar{0}$$

i.e.

$$\forall \bar{x} \in H, n \mid dx$$

puis

$$\forall \bar{x} \in H, c \mid x$$

Ainsi

$$H \subset \{\bar{0}, \bar{c}, 2\bar{c}, \dots, (d-1)\bar{c}\}$$

et l'égalité est acquise par cardinalité.

II Anneaux

$\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

2.1 Structure d'anneau

2.1.1 Définition

Définition

On appelle anneau tout triplet $(A, +, \times)$ formé d'un ensemble A et de deux lois de composition internes usuellement notées $+$ et $\times$ sur A vérifiant :

- 1) $(A, +)$ est un groupe abélien de neutre 0_A ;
- 2) $\times$ est associative et possède un neutre 1_A ;
- 3) $\times$ est distributive sur $+$ i.e.

$$\forall a, b, c \in A, a(b+c) = ab+ac \text{ et } (b+c)a = ba+ca$$

Si de plus la loi $\times$ est commutative, on dit que l'anneau $(A, +, \times)$ est commutatif.

Exemple $(\mathbb{Z}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs de neutres 0 et 1.

Exemple Soit X un ensemble et $\mathcal{F}(X, \mathbb{K})$ l'ensemble des fonctions de X vers $\mathbb{K}$.

$(\mathcal{F}(X, \mathbb{K}), +, \times)$ est un anneau de neutres $\tilde{0}$ et $\tilde{1}$ (fonctions constantes).

En particulier, si $X = \mathbb{N}$, l'ensemble $\mathbb{K}^{\mathbb{N}}$ des suites d'éléments de $\mathbb{K}$ est un anneau.

Exemple $(\mathcal{M}_n(\mathbb{K}), +, \times)$ est un anneau de neutres O_n et I_n .

Exemple Si E est un $\mathbb{K}$ -espace vectoriel, $(\mathcal{L}(E), +, \circ)$ est un anneau de neutres $\tilde{0}$ et Id_E .

Exemple $A = \{0_A\}$ est un anneau (c'est le seul pour lequel $1_A = 0_A$).

2.1. STRUCTURE D'ANNEAU

2.1.2 Calculs dans un anneau

Proposition

On a

$$\forall a, b \in A, 0_A \times a = a \times 0_A = 0_A, (-a) \times b = -(ab) = a \times (-b)$$

Plus généralement

$$\forall n \in \mathbb{Z}, (n \cdot a) \times b = n \cdot (ab) = a \times (n \cdot b)$$

Théorème

Si a et b sont deux éléments commutant (i.e. $ab = ba$) d'un anneau A on a pour tout $n \in \mathbb{N}$

$$(ab)^n = a^n b^n, (a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

et

$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$$

2.1.3 Groupe des inversibles

Définition

Un élément a d'un anneau $(A, +, \times)$ est dit inversible s'il existe $b \in A$ tel que

$$ab = ba = 1$$

Cet élément b est alors unique, on l'appelle inverse de a et il est noté a^{-1} .

Exemple 1_A est inversible et $1_A^{-1} = 1_A$.

Exemple Si A n'est pas l'anneau nul, 0_A n'est pas inversible.

Exemple Si $x \in A$ est inversible alors x^{-1} aussi et $(x^{-1})^{-1} = x$.
Si x et $y \in A$ sont inversibles alors xy est inversible et $(xy)^{-1} = y^{-1}x^{-1}$.

Théorème

L'ensemble $U(A)$ des éléments inversibles de l'anneau $(A, +, \times)$ est un groupe multiplicatif.

Exemple $U(\mathbb{Z}) = \{1, -1\}$, $U(K) = K^*$,
 $U(M_n(K)) = GL_n(K)$ et $U(\mathcal{L}(E)) = GL(E)$.

2.1.4 Produit fini d'anneaux

Soit $(A_1, +, \times), \dots, (A_n, +, \times)$ des anneaux et $A = A_1 \times \dots \times A_n$.

On définit des lois $+$ et $\times$ sur A en posant

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$$

et

$$(x_1, \dots, x_n) \times (y_1, \dots, y_n) = (x_1 \times y_1, \dots, x_n \times y_n)$$

Théorème

L'ensemble A muni des lois $+$ et $\times$ définies ci-dessus est un anneau de neutres

$$0_A = (0_{A_1}, \dots, 0_{A_n}) \text{ et } 1_A = (1_{A_1}, \dots, 1_{A_n})$$

De plus, un élément $(a_1, \dots, a_n) \in A$ est inversible si, et seulement si, les $a_1, \dots, a_n$ le sont et son inverse est alors $(a_1^{-1}, \dots, a_n^{-1})$.

Corollaire

$$U(A) = U(A_1) \times \dots \times U(A_n)$$

Exemple $(A^n, +, \times)$ est un anneau de neutres $0_{A^n} = (0_A, \dots, 0_A)$ et $1_{A^n} = (1_A, \dots, 1_A)$.

Exemple $(\mathbb{Z}^2, +, \times)$ est un anneau commutatif où

$$(a, b) + (c, d) = (a + c, b + d) \text{ et } (a, b) \times (c, d) = (ac, bd)$$

On a

$$U(\mathbb{Z}^2) = \{(1, 1), (1, -1), (-1, 1), (-1, -1)\}$$

2.1.5 Sous-anneau

$(A, +, \times)$ désigne un anneau

Définition

On appelle sous-anneau de $(A, +, \times)$ toute partie B de A vérifiant :

- 1) $1_A \in B$;
- 2) $\forall x, y \in B, x - y \in B$;
- 3) $\forall x, y \in B, xy \in B$.

Attention : Vérifier $1_A \in B$ et non $0_A \in B$ ou seulement $B \neq \emptyset$.

Exemple $\mathbb{Z}$ est un sous-anneau de $(\mathbb{R}, +, \times)$ mais pas $2\mathbb{Z}$ bien que stable par différence et produit

Exemple A est un sous-anneau de $(A, +, \times)$, mais généralement pas $\{0_A\}$.

Exemple On note $\mathcal{C}$ l'ensemble des suites réelles convergentes.

Montrons que $\mathcal{C}$ est un sous-anneau de $(\mathbb{R}^{\mathbb{N}}, +, \times)$.

On a évidemment $\mathcal{C} \subset \mathbb{R}^{\mathbb{N}}$, la suite constante égale à 1 est convergente et la différence et le produit de deux suites convergentes sont des suites convergentes.

En revanche, l'ensemble des suites réelles convergeant vers 0 n'est pas un sous-anneau.

Exemple Soit I un intervalle de $\mathbb{R}$ d'intérieur non vide et $k \in \mathbb{N} \cup \{\infty\}$.

Vérifions que $\mathcal{C}^k(I, \mathbb{R})$ est un sous-anneau de $(\mathcal{F}(I, \mathbb{R}), +, \times)$.

On a évidemment $\mathcal{C}^k(I, \mathbb{R}) \subset \mathcal{F}(I, \mathbb{R})$, la fonction constante égale à 1 est de classe $\mathcal{C}^k$ et la différence et le produit de deux fonctions de classe $\mathcal{C}^k$ sont des fonctions de classe $\mathcal{C}^k$.

Théorème

Si B est un sous-anneau de $(A, +, \times)$ alors B peut être muni des lois $+$ et $\times$ définies par restriction des lois sur A et $(B, +, \times)$ est alors un anneau de mêmes neutres que A .

dém. :

B est un sous-groupe du groupe abélien $(A, +)$ donc $(B, +)$ est un groupe abélien.

B est stable par $\times$ donc on peut définir la restriction de la loi $\times$ sur B .

Celle-ci est associative sur A et possède un neutre $1_A \in B$ donc $\times$ est associative sur B et y possède un neutre.

Enfin, $\times$ est distributive sur $+$ sur A donc a fortiori aussi sur B .

□

Exemple Considérons

$$\mathbb{Z}[i] = \{a + ib/a, b \in \mathbb{Z}\}$$

et montrons que $(\mathbb{Z}[i], +, \times)$ est un anneau commutatif.

Montrons que $\mathbb{Z}[i]$ un sous-anneau de l'anneau commutatif $(\mathbb{C}, +, \times)$.

On a évidemment $\mathbb{Z}[i] \subset \mathbb{C}$.

$1 = 1 + i \cdot 0 \in \mathbb{Z}[i]$.

Pour $x, y \in \mathbb{Z}[i]$, on peut écrire $x = a + ib$ et $y = c + id$ avec $a, b, c, d \in \mathbb{Z}$.

On a

$$x - y = (a - c) + i(b - d) \in \mathbb{Z}[i]$$

car $a - c, b - d \in \mathbb{Z}$

et

$$xy = (ac - bd) + i(ad + bc) \in \mathbb{Z}[i]$$

Ainsi, $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$ et donc $(\mathbb{Z}[i], +, \times)$ est un anneau commutatif.

2.1.6 L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Théorème

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif de neutres $\bar{0}$ et $\bar{1}$.

De plus, dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, $\bar{m}$ est inversible si, et seulement si, $m \wedge n = 1$.

dém. :

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien de neutre $\bar{0}$.

On vérifie aisément que la loi $\times$ est commutative, associative sur $\mathbb{Z}/n\mathbb{Z}$ et possède un neutre $\bar{1}$. On vérifie aussi que la loi $\times$ est distributive sur $+$.

Soit $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$.

$\bar{m}$ inversible si, et seulement si, il existe $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ vérifiant $\bar{k}\bar{m} = \bar{1}$ i.e. si, et seulement si, il existe $k \in \mathbb{Z}$ tel que $km \equiv 1 \pmod{n}$. Ainsi $\bar{m}$ est inversible si, et seulement si, il existe $k, \ell \in \mathbb{Z}$ tels que

$$km + \ell n = 1$$

Par le théorème de Bézout, cela revient à affirmer $m \wedge n = 1$.

□

Remarque Si $m \wedge n = 1$ alors une égalité de Bézout $um + vn = 1$ fournit $\bar{m}^{-1} = \bar{u}$.

Exemple Résolvons l'équation $4x + 2 \equiv 0 \pmod{11}$

Dans $\mathbb{Z}/11\mathbb{Z}$ l'équation dévient

$$\bar{4}\bar{x} + \bar{2} = \bar{0}$$

Par opérations

$$\bar{4}\bar{x} + \bar{2} = \bar{0} \Leftrightarrow \bar{4}\bar{x} = \bar{9}$$

Puisque $4 \wedge 11 = 1$, $\bar{4}$ est inversible dans $\mathbb{Z}/11\mathbb{Z}$ et on observe

$$\bar{4}^{-1} = \bar{3}$$

On a alors

$$\bar{4}\bar{x} = \bar{9} \Leftrightarrow \bar{x} = \bar{3} \times \bar{9}$$

Ainsi

$$\bar{4}\bar{x} + \bar{2} = \bar{0} \Leftrightarrow \bar{x} = \bar{5}$$

Les solutions de l'équation étudiées sont donc les $5 + 11k$ avec $k \in \mathbb{Z}$.

Exemple Résolvons l'équation $4x \equiv 6 \pmod{10}$

Ici 4 et 10 ne sont pas premiers entre eux, mais l'équation est simplifiable par leur PGCD

$$4x \equiv 6 \pmod{10} \Leftrightarrow \exists k \in \mathbb{Z}, 4x = 6 + 10k \Leftrightarrow \exists k \in \mathbb{Z}, 2x = 3 + 5k$$

ce qui nous ramène à l'équation $2x \equiv 3 \pmod{5}$ avec $2 \wedge 5 = 1$ qu'on peut résoudre.

$$2x \equiv 3 \pmod{5} \Leftrightarrow x \equiv 3 \times 3 = 4 \pmod{5}$$

Les solutions sont les $4 + 5k$ avec $k \in \mathbb{Z}$.

Exemple Résolvons l'équation $4x \equiv 7 \pmod{10}$

Ici 4 et 10 ne sont pas premiers entre eux et l'équation n'est pas simplifiable : il n'y a pas de solutions.

2.1.7 Anneaux Intègres

Soit $(A, +, \times)$ un anneau.

2.1.7.1 Diviseurs de zéro

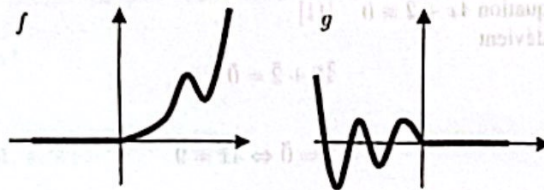
Attention : On sait

$$\forall a, b \in A, a = 0_A \text{ ou } b = 0_A \Rightarrow ab = 0_A$$

La réciproque n'est pas toujours vraie !

Exemple Dans l'anneau $(\mathbb{Z}^2, +, \times)$, on a $(1, 0) \times (0, 1) = (0, 0)$ alors que $(1, 0), (0, 1) \neq (0, 0)$

Exemple Dans l'anneau $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times)$, considérons les fonctions données par



On a $fg = \vec{0}$ alors que $f, g \neq \vec{0}$.

Exemple Dans $(\mathcal{M}_2(\mathbb{R}), +, \times)$, pour

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$$

on a $AB = O_2$ alors que $A, B \neq O_2$.

Exemple Dans $(\mathbb{Z}/6\mathbb{Z}, +, \times)$, $\bar{2} \times \bar{3} = \vec{0}$ alors que $\bar{2}, \bar{3} \neq \vec{0}$.

Définition

Lorsque $a, b \in A$ vérifient $ab = 0_A$ avec $a, b \neq 0_A$, on dit que a et b sont des diviseurs de zéro.

Attention : On ne considère pas que 0_A est un diviseur de zéro.

Exemple En général, les anneaux $\mathcal{F}(X, \mathbb{K})$, $\mathcal{L}(E)$ et $\mathcal{M}_n(\mathbb{K})$ possèdent des diviseurs de zéros.

Exemple Les éléments inversibles d'un anneau ne sont pas diviseurs de zéros.

En effet, si $ab = 0_A$ avec a inversible alors

$$b = a^{-1} \times (ab) = a^{-1} \times 0_A = 0_A$$

Exemple Dans $(\mathbb{R}^2, +, \times)$ les diviseurs de zéros sont les $(x, 0)$ et $(0, x)$ avec $x \neq 0$.

2.1.7.2 Intégrité

Définition

Un anneau $(A, +, \times)$ est dit **intègre** si

- 1) A non réduit à $\{0_A\}$;
- 2) A ne possède pas de diviseurs de zéros.

Exemple $(\mathbb{Z}, +, \times)$ est un anneau intègre.

Proposition

Dans un anneau intègre $(A, +, \times)$

$$\forall a, b \in A, ab = 0_A \Rightarrow a = 0_A \text{ ou } b = 0_A$$

dém. :

C'est l'absence de diviseurs de zéro !

□

Proposition

Dans un anneau intègre $(A, +, \times)$:

$$\forall a, b, c \in A, (ab = ac \text{ et } a \neq 0_A) \Rightarrow b = c$$

et

$$\forall a, b, c \in A, (ba = ca \text{ et } a \neq 0_A) \Rightarrow b = c$$

dém. :

Si $ab = ac$ alors $ab - ac = 0_A$ et donc $a(b - c) = 0_A$.

Si de plus $a \neq 0_A$ alors, par intégrité, $b - c = 0_A$ et donc $b = c$.

□

Remarque Dans un anneau intègre l'équation $x^2 = 1$ a pour seules solutions 1 et -1 car

$$x^2 = 1_A \Leftrightarrow (x - 1_A)(x + 1_A) = 0_A$$

Dans $(\mathbb{R}^2, +, \times)$, l'équation $x^2 = 1_{\mathbb{R}^2}$ a pour solutions

$$(1, 1), (-1, -1), (1, -1), (-1, 1)$$

Dans $(M_2(\mathbb{R}), +, \times)$, l'équation $A^2 = I_2$ a pour solutions

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & -3 \\ 1 & -2 \end{pmatrix}, \dots$$

2.1.7.3 Idempotence et nilpotence

Définition

Un élément $a \in A$ est dit **idempotent** si $a^2 = a$.

2.2. CORPS

Exemple Dans un anneau intègre seuls 0_A et 1_A sont idempotents.

Exemple Dans $(\mathbb{R}^2, +, \times)$, $(1, 0)$ et $(0, 1)$ sont aussi idempotents.

Exemple Dans $(\mathbb{Z}/6\mathbb{Z}, +, \times)$, l'élément $\bar{3}$ est idempotent.

Exemple Dans $(\mathcal{L}(E), +, \circ)$ les éléments idempotents sont les projecteurs.

Définition

Un élément $a \in A$ est dit nilpotent s'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0_A$.

Exemple Dans un anneau intègre seul 0_A est nilpotent.

Exemple Dans $(\mathbb{Z}/8\mathbb{Z}, +, \times)$, l'élément $\bar{2}$ est nilpotent.

Exemple Montrons que si a est nilpotent alors $1_A - a \in U(A)$.

Puisque a est nilpotent, il existe $n \in \mathbb{N}$ vérifiant $a^n = 0_A$.

Puisque 1_A et a commutent,

$$1_A = 1_A^n - a^n = (1 - a) \left(\sum_{k=0}^{n-1} a^k \right) = \left(\sum_{k=0}^{n-1} a^k \right) (1 - a)$$

Ainsi, $1_A - a$ est inversible et

$$(1_A - a)^{-1} = \sum_{k=0}^{n-1} a^k$$

2.2 Corps

2.2.1 Définition

Définition

On appelle corps tout anneau $(K, +, \times)$ vérifiant

- 1) $(K, +, \times)$ est commutatif;
- 2) K est non réduit à $\{0_K\}$ et
- 3) tous les éléments de K , sauf le nul, sont inversibles.

Exemple $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ et $(\mathbb{K}(X), +, \times)$ sont des corps usuels.

Proposition

Tout corps est intègre.

dém. :

Soit K un corps. K est commutatif et non réduit à $\{0_K\}$.

Pour $a, b \in K$, si $ab = 0_K$ et $a \neq 0_K$ alors on peut introduire a^{-1} et on a $b = a^{-1}(ab) = 0_K$.

Ainsi, K ne possède pas de diviseurs de zéro. Il est donc intègre.

□

2.2.2 Sous-corps

Soit $(K, +, \times)$ un corps.

Définition

On appelle sous-corps d'un corps $(K, +, \times)$ toute partie L de K vérifiant :

1) L est un sous-anneau de $(K, +, \times)$;

2) $\forall x \in L, x \neq 0_K \Rightarrow x^{-1} \in L$.

Exemple $\mathbb{Q}$ est un sous-corps de $(\mathbb{R}, +, \times)$.

Théorème

Si L est un sous-corps de $(K, +, \times)$ alors $(L, +, \times)$ est un corps.

dém. :

Puisque L est un sous-anneau de l'anneau commutatif $(K, +, \times)$, on peut affirmer que $(L, +, \times)$ est un anneau commutatif. Puisque $1_K \in L$, on peut affirmer que l'anneau $(L, +, \times)$ n'est pas réduit à 0. Enfin, puisque l'inverse d'un élément non nul de L est élément de L , on peut affirmer que tout élément non nul de l'anneau L est inversible dans celui-ci.

□

Exemple Considérons $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} / a, b \in \mathbb{Q}\}$.

Montrons que $(\mathbb{Q}[\sqrt{2}], +, \times)$ est un corps.

Pour cela montrons que $\mathbb{Q}[\sqrt{2}]$ est un sous-corps du corps $(\mathbb{R}, +, \times)$.

On a évidemment $\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$.

$1 = 1 + 0 \times \sqrt{2} \in \mathbb{Q}[\sqrt{2}]$.

Pour $x, y \in \mathbb{Q}[\sqrt{2}]$, on peut écrire $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$ avec $a, b, c, d \in \mathbb{Q}$.

On a alors

$$x - y = (a - c) + (b - d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

et

$$xy = (ab + 2dc) + \sqrt{2}(ad + bc) \in \mathbb{Q}[\sqrt{2}]$$

Enfin, si $x \neq 0$,

$$x^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

car $\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\sqrt{2} \in \mathbb{Q}$.

2.3. MORPHISMES D'ANNEAUX

2.2.3 Le corps $(\mathbb{Z}/p\mathbb{Z}, +, \times)$

Théorème

$(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps si, et seulement si, p est un nombre premier.

dém. :

Supposons que $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ soit un corps.

Pour tout $a \in \{2, \dots, p-1\}$, $\bar{a}$ est inversible dans $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ donc $a \wedge p = 1$ et par conséquent a ne divise pas p . On en déduit que p est un nombre premier.

Inversement, supposons p nombre premier.

$(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un anneau commutatif et $\mathbb{Z}/p\mathbb{Z} \neq \{\bar{0}\}$ car $p = \text{Card}(\mathbb{Z}/p\mathbb{Z}) \geq 2$.

Pour tout $\bar{m} \in \mathbb{Z}/p\mathbb{Z}$, si $\bar{m} \neq \bar{0}$ alors p ne divise pas m et donc, puisque p est un nombre premier,

$$m \wedge p = 1$$

On en déduit que $\bar{m}$ est inversible.

□

Remarque On note usuellement $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Exemple Soit $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$. $(\mathbb{F}_2, +, \times)$ est un corps pour les opérations suivantes

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

Exemple Soit $\mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$. $(\mathbb{F}_3, +, \times)$ est un corps pour les opérations suivantes

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

2.3 Morphismes d'anneaux

Soit $(A, +, \times)$ et $(A', +, \times)$ des anneaux.

2.3.1 Morphisme d'anneaux

Définition

On dit qu'une application $\varphi : A \rightarrow A'$ est un morphisme d'anneaux si

- 1) $\varphi(1_A) = 1_{A'}$;
- 2) $\forall x, y \in A, \varphi(x + y) = \varphi(x) + \varphi(y)$;
- 3) $\forall x, y \in A, \varphi(xy) = \varphi(x)\varphi(y)$.

Exemple L'application identité $\text{Id}_A : A \rightarrow A$ est un morphisme de l'anneau $(A, +, \times)$ vers lui-même.

Exemple Considérons $\mathbb{C}$ l'anneau des suites réelles convergentes.

L'application $\varphi : u \mapsto \lim_{n \rightarrow +\infty} u_n$ est un morphisme d'anneaux de $\mathbb{C}$ vers $\mathbb{R}$.

Exemple L'application $\varphi : \mathbb{Z} \rightarrow A$ définie par $\varphi(k) = k \cdot 1_A$ est un morphisme d'anneaux de $(\mathbb{Z}, +, \times)$ vers $(A, +, \times)$.

En effet, $\varphi(1) = 1_A$, $\varphi(k + \ell) = (k + \ell) \cdot 1_A = k \cdot 1_A + \ell \cdot 1_A = \varphi(k) + \varphi(\ell)$ et

$\varphi(k\ell) = (k\ell) \cdot 1_A = (k \cdot 1_A) \times (\ell \cdot 1_A) = \varphi(k)\varphi(\ell)$.

Exemple Soit $a \in U(A)$ et $\tau : A \rightarrow A$ définie par $\tau(x) = axa^{-1}$.

Vérifions que τ est un morphisme d'anneaux bijectif.

$\tau(1_A) = a \cdot 1_A \cdot a^{-1} = 1_A$, $\tau(x + y) = a(x + y)a^{-1} = axa^{-1} + aya^{-1} = \tau(x) + \tau(y)$ et

$\tau(xy) = axya^{-1} = ax(a^{-1}a)ya^{-1} = \tau(x)\tau(y)$.

Enfin,

$$y = \tau(x) \Leftrightarrow x = a^{-1}ya$$

donc

$\forall y \in A, \exists! x \in A, y = \tau(x)$

L'application τ est donc bijective.

Attention : Ne pas oublier d'étudier $\varphi(1_A)$!

L'application $x \in \mathbb{R} \mapsto (x, 0) \in \mathbb{R}^2$ n'est pas un morphisme d'anneaux !

2.3.2 Propriétés

Proposition

La composée de deux morphismes d'anneaux est un morphisme d'anneaux.

Proposition

Si $\varphi : A \rightarrow A'$ est un morphisme d'anneaux alors

- a) $\varphi(0_A) = 0_{A'}$;
- b) $\forall x \in A, \varphi(-x) = -\varphi(x)$;
- c) $\forall x \in A, \forall n \in \mathbb{Z}, \varphi(n \cdot x) = n \cdot \varphi(x)$;
- d) $\forall x \in A, \forall n \in \mathbb{N}, \varphi(x^n) = \varphi(x)^n$;
- e) $\forall x \in A, x \in U(A) \Rightarrow \varphi(x) \in U(A')$ avec $\varphi(x)^{-1} = \varphi(x^{-1})$

dém. :

φ est un morphisme du groupe $(A, +)$ vers $(A', +)$ donc

$$\forall x \in A, \forall n \in \mathbb{Z}, \varphi(n \cdot x) = n \cdot \varphi(x)$$

Par récurrence, on obtient aisément

$$\forall x \in A, \forall n \in \mathbb{N}, \varphi(x^n) = \varphi(x)^n$$

2.3. MORPHISMES D'ANNEAUX

Enfin, si $x \in U(A)$ alors $\varphi(xx^{-1}) = \varphi(1_A)$ donne $\varphi(x)\varphi(x^{-1}) = 1_{A'}$. Aussi $\varphi(x^{-1})\varphi(x) = 1_{A'}$ donc $\varphi(x) \in U(A')$ et $\varphi(x)^{-1} = \varphi(x^{-1})$.

□

2.3.3 Image et noyaux

Définition

Soit $\varphi : A \rightarrow A'$ un morphisme d'anneaux.

On appelle image et noyau du morphisme φ les ensembles

$$\text{Im } \varphi = \varphi(A) \text{ et } \ker \varphi = \varphi^{-1}(\{0_{A'}\})$$

Remarque Ce sont en fait les images et noyaux de φ en tant que morphisme de groupes additifs.

Remarque On vérifie aisément que $\text{Im } \varphi$ est un sous-anneau de A' .

En revanche, $\ker \varphi$ n'est généralement pas un sous-anneau de $(A, +, \times)$.

Proposition

φ est injective si, et seulement si, $\ker \varphi = \{0_A\}$.

φ est surjective si, et seulement si, $\text{Im } \varphi = A'$.

dém. :

Car φ est en particulier un morphisme de groupes additifs.

□

2.3.4 Isomorphisme d'anneaux

Définition

On dit qu'une application $\varphi : A \rightarrow A'$ est un isomorphisme d'anneaux si

a) φ est un morphisme d'anneaux ;

b) φ est bijective.

Proposition

La composée de deux isomorphismes d'anneaux est un isomorphisme d'anneaux.

L'application réciproque d'un isomorphisme d'anneaux est un isomorphisme d'anneaux.

Définition

On dit que deux anneaux A et A' sont isomorphes s'il existe un isomorphisme d'anneaux de l'un vers l'autre : ces deux anneaux possèdent alors les mêmes propriétés calculatoires.

Exemple Considérons $\varphi : \mathbb{C} \rightarrow \mathcal{M}_2(\mathbb{R})$ définie par

$$\varphi(a + i.b) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

On vérifie que φ est un morphisme d'anneaux injectifs.

2.3. MORPHISMES D'ANNEAUX

Enfin, si $x \in U(A)$ alors $\varphi(xx^{-1}) = \varphi(1_A)$ donne $\varphi(x)\varphi(x^{-1}) = 1_{A'}$. Aussi $\varphi(x^{-1})\varphi(x) = 1_{A'}$ donc $\varphi(x) \in U(A')$ et $\varphi(x)^{-1} = \varphi(x^{-1})$.

□

2.3.3 Image et noyaux

Définition

Soit $\varphi : A \rightarrow A'$ un morphisme d'anneaux.

On appelle image et noyau du morphisme φ les ensembles

$$\text{Im } \varphi = \varphi(A) \text{ et } \ker \varphi = \varphi^{-1}(\{0_{A'}\})$$

Remarque Ce sont en fait les images et noyaux de φ en tant que morphisme de groupes additifs.

Remarque On vérifie aisément que $\text{Im } \varphi$ est un sous-anneau de A' .

En revanche, $\ker \varphi$ n'est généralement pas un sous-anneau de $(A, +, \times)$.

Proposition

φ est injective si, et seulement si, $\ker \varphi = \{0_A\}$.

φ est surjective si, et seulement si, $\text{Im } \varphi = A'$.

dém. :

Car φ est en particulier un morphisme de groupes additifs.

□

2.3.4 Isomorphisme d'anneaux

Définition

On dit qu'une application $\varphi : A \rightarrow A'$ est un isomorphisme d'anneaux si

a) φ est un morphisme d'anneaux ;

b) φ est bijective.

Proposition

La composée de deux isomorphismes d'anneaux est un isomorphisme d'anneaux.

L'application réciproque d'un isomorphisme d'anneaux est un isomorphisme d'anneaux.

Définition

On dit que deux anneaux A et A' sont isomorphes s'il existe un isomorphisme d'anneaux de l'un vers l'autre : ces deux anneaux possèdent alors les mêmes propriétés calculatoires.

Exemple Considérons $\varphi : \mathbb{C} \rightarrow M_2(\mathbb{R})$ définie par

$$\varphi(a + i.b) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

On vérifie que φ est un morphisme d'anneaux injectifs.

En conséquence

$$\text{Im } \varphi = \left\{ \begin{pmatrix} a & -b \\ 0 & a \end{pmatrix} / a, b \in \mathbb{R} \right\}$$

est un sous-anneau de $M_2(\mathbb{R})$ isomorphe à $(\mathbb{C}, +, \times)$.

2.3.5 Théorème des restes chinois

Soit m et n deux entiers naturels non nuls. Pour $k \in \mathbb{Z}$, on note $\bar{k}$, $\hat{k}$ et k les classes d'équivalence de k dans $\mathbb{Z}/mn\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$.

Théorème

Si m et n sont premiers entre eux alors l'application

$$\pi : \mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

définie par

$$\pi(\bar{k}) = (\hat{k}, k)$$

est un isomorphisme d'anneaux.

dém. :

L'application est bien définie car

$$k = \ell \pmod{mn} \Rightarrow k = \ell \pmod{m} \text{ et } k = \ell \pmod{n}$$

et ainsi

$$\bar{k} = \bar{\ell} \Rightarrow \hat{k} = \hat{\ell} \text{ et } k = \ell$$

On vérifie aisément que cette application est un morphisme d'anneaux.

Étudions le noyau de π .

Si $\bar{x} \in \ker \pi$ alors $\pi(\bar{x}) = (0, 0)$ i.e. $\bar{x} = \bar{0}$ et $x = 0$. On alors $m \mid x$ et $n \mid x$ donc $mn \mid x$ puisque $m \wedge n = 1$. Ainsi $\bar{x} = \bar{0}$ ce qui permet d'affirmer $\ker \pi = \{\bar{0}\}$.

Le morphisme π est donc injectif.

Puisque

$$\text{Card}(\mathbb{Z}/mn\mathbb{Z}) = nm = \text{Card}(\mathbb{Z}/n\mathbb{Z})\text{Card}(\mathbb{Z}/m\mathbb{Z}) < +\infty$$

on peut affirmer par cardinalité que π est bijective et finalement π est un isomorphisme.

□

Remarque Soit à résoudre un système du type

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

avec $m \wedge n = 1$. Par ce qui précède, ce système possède une unique solution modulo mn .

Pour la déterminer, il suffit de trouver x_1 et x_2 solutions respectives des systèmes

$$\begin{cases} x \equiv 1 \pmod{m} \\ x \equiv 0 \pmod{n} \end{cases} \text{ et } \begin{cases} x \equiv 0 \pmod{m} \\ x \equiv 1 \pmod{n} \end{cases}$$

Par morphisme, $x = ax_1 + bx_2$ est alors solution du système initial.

Pour déterminer x_1 et x_2 , on part de la relation de Bézout

$$mu + nv = 1$$

et l'on prend $x_1 = nv$ et $x_2 = mu$.

Exemple Résolvons le système

$$\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 7 \pmod{9} \end{cases}$$

$5 \wedge 9 = 1$ avec la relation de Bézout $2 \times 5 - 9 = 1$.

-9 et 10 sont solutions des systèmes

$$\begin{cases} x \equiv 1 \pmod{5} \\ x \equiv 0 \pmod{9} \end{cases} \quad \text{et} \quad \begin{cases} x \equiv 0 \pmod{5} \\ x \equiv 1 \pmod{9} \end{cases}$$

donc $x = 1 \times (-9) + 7 \times 10 = 61$ est solution du système posé.

La solution générale est alors

$$16 + 45k \text{ avec } k \in \mathbb{Z}$$

Exemple Résolvons le système

$$\begin{cases} 9x \equiv 3 \pmod{21} \\ 5x \equiv 2 \pmod{8} \end{cases}$$

$$9x \equiv 3 \pmod{21} \Leftrightarrow 3x \equiv 1 \pmod{7}$$

Puisque $3 \wedge 7 = 1$, $\bar{3}$ est inversible et $\bar{3}^{-1} = \bar{5}$ dans $\mathbb{Z}/7\mathbb{Z}$.

Ainsi

$$3x \equiv 1 \pmod{7} \Leftrightarrow x \equiv 5 \pmod{7}$$

De même

$$5x \equiv 2 \pmod{8} \Leftrightarrow x \equiv 2 \pmod{8}$$

car $\bar{5}^{-1} = \bar{5}$ dans $\mathbb{Z}/8\mathbb{Z}$

Ainsi

$$\begin{cases} 9x \equiv 3 \pmod{21} \\ 5x \equiv 2 \pmod{8} \end{cases} \Leftrightarrow \begin{cases} x \equiv 5 \pmod{7} \\ x \equiv 2 \pmod{8} \end{cases}$$

$7 \wedge 8 = 1$ avec la relation de Bézout $(-1) \times 7 + 8 = 1$.

$x = 5 \times 8 + 2 \times (-7) = 26$ est solution de ce système dont la solution générale est

$$x = 26 + 56k \text{ avec } k \in \mathbb{Z}$$

2.4 Idéal d'un anneau commutatif

Soit $(A, +, \times)$ un anneau commutatif.

2.4.1 Définition

Définition

On appelle idéal de l'anneau $(A, +, \times)$ toute partie I de A vérifiant :

- 1) $0_A \in I$;
- 2) $\forall x, y \in I, x + y \in I$;
- 3) $\forall a \in A, \forall x \in I, ax \in I$ [absorption].

Remarque Un idéal est en particulier un sous-groupe additif (il suffit d'exploiter l'absorption avec $a = -1$)

Exemple $\{0_A\}$ et A sont des idéaux de $(A, +, \times)$.

Exemple $n\mathbb{Z}$ est un idéal de $(\mathbb{Z}, +, \times)$.

Exemple Le noyau d'un morphisme d'anneaux $\varphi : A \rightarrow A'$ est un idéal de $(A, +, \times)$.

En effet, $\ker \varphi \subset A$, $0_A \in \ker \varphi$ car $\varphi(0_A) = 0_{A'}$.

Soit $x, y \in \ker \varphi$.

$\varphi(x + y) = \varphi(x) + \varphi(y) = 0_{A'} + 0_{A'} = 0_{A'}$ donc $x + y \in \ker \varphi$.

Soit de plus $a \in A$.

$\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a) \times 0_{A'} = 0_{A'}$ donc $ax \in \ker \varphi$.

Proposition

Soit I un idéal de l'anneau $(A, +, \times)$

Si $1_A \in I$ alors $I = A$.

Si $I \cap U(A) \neq \emptyset$ alors $I = A$.

dém. :

Par absorption $1_A \in I$ entraîne $A \subset I$ puis $=$.

De même, par absorption, $I \cap U(A) \neq \emptyset$ entraîne $1_A \in I$ puis $I = A$.

□

Remarque Les seuls idéaux d'un corps sont $\{0_K\}$ et lui-même.

2.4.2 Opérations

Proposition

Si I et J sont deux idéaux de $(A, +, \times)$ alors $I \cap J$ est un idéal.

De plus, $I \cap J$ est inclus dans I et J et contient tout idéal inclus dans I et J .

dém. :

$I \cap J \subset A$, $0_A \in I$ et $0_A \in J$ donc $0_A \in I \cap J$.

Si $x, y \in I \cap J$ alors $x, y \in I$ donc $x + y \in I$. De même $x + y \in J$ donc $x + y \in I \cap J$.

Si $u \in A$ et $x \in I \cap J$ alors $x \in I$ donc $ux \in I$. De même $ux \in J$ donc $ux \in I \cap J$.

□

Proposition

Si I et J sont deux idéaux de $(A, +, \times)$ alors

$$I + J = \{x + y \mid x \in I, y \in J\}$$

est un idéal.

De plus, $I + J$ contient I et J et est inclus dans tout idéal contenant I et J .

dém. :

Pour $x \in I$, $x = x + 0_A \in I + J$ car $0_A \in J$. Ainsi $I \subset I + J$ et de même $J \subset I + J$.

$0_A \in I + J$ car $0_A = 0_A + 0_A$ avec $0_A \in I, J$.

Pour $x, y \in I + J$, on peut écrire $x = x' + x''$ et $y = y' + y''$ avec $x', y' \in I$ et $x'', y'' \in J$.
 On a alors $x + y = (x' + y') + (x'' + y'') \in I + J$ car $x' + y' \in I$ et $x'' + y'' \in J$.
 Enfin, pour $a \in A$, $ax = (ax') + (ax'') \in I + J$ car $ax' \in I$ et $ax'' \in J$.
 De plus, si K est un idéal contenant I et J alors K contient $I + J$ car stable pour l'addition.

□

2.4.3 Idéal engendré par un élément

Définition

On appelle idéal engendré par $x \in A$ l'ensemble

$$xA = \{xu/u \in A\}$$

Théorème

xA est un idéal contenant l'élément x et inclus dans tout idéal contenant x .

dém. :

$x = x \times 1 \in xA$ et si I est un idéal contenant x alors par absorption, il contient xA .

Il reste à montrer que xA est un idéal.

On a $xA \subset A$ et $0_A = x \times 0_A \in xA$.

Pour $y, z \in xA$, on peut écrire $y = xu$ et $z = xv$ avec $u, v \in A$ et alors $y + z = x(u + v) \in xA$.

Enfin, pour $a \in A$, $ay = x(au) \in xA$.

□

2.4.4 Idéaux de $(\mathbb{Z}, +, \times)$

Théorème

Les idéaux de $(\mathbb{Z}, +, \times)$ sont de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

dém. :

Les idéaux de $(\mathbb{Z}, +, \times)$ sont des sous-groupes de $(\mathbb{Z}, +)$ donc de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

□

2.5 Application à l'arithmétique

Soit $(A, +, \times)$ un anneau intègre commutatif

2.5.1 Divisibilité dans un anneau intègre

Définition

On dit que $a \in A$ divise $b \in A$ s'il existe $u \in A$ tel que $b = au$. On note alors $a \mid b$.

Exemple 1_A divise a et a divise a .

Exemple a divise 0_A et $0_A \mid a \Rightarrow a = 0_A$.

La notion de diviseurs de zéro dans le cadre arithmétique ne doit pas être confondue avec celle du cadre de l'intégrité !

Théorème

On a équivalence entre :

- (i) $a \mid b$;
- (ii) $b \in aA$;
- (iii) $bA \subset aA$.

dém. :

Par définition (i) $\Leftrightarrow$ (ii)(ii) $\Rightarrow$ (iii) Si $b \in aA$ alors $bA \subset aA$ car aA est un idéal.(iii) $\Rightarrow$ (ii) Supposons $bA \subset aA$. Puisque $b \in bA$, on a $b \in aA$.

□

PropositionSoit $a, b, c \in A$.

$$a \mid b \text{ et } b \mid c \Rightarrow a \mid c$$

dém. :

 $bA \subset aA$ et $cA \subset bA \Rightarrow cA \subset aA$.

□

PropositionSoit $a, b, c \in A$.

$$a \mid b \text{ et } a \mid c \Rightarrow a \mid (b+c)$$

dém. :

 $bA \subset aA$ et $cA \subset aA \Rightarrow (b+c)A \subset aA$ car aA est un idéal.

□

2.5.2 Association**Définition**On dit que $a \in A$ est associé à $b \in A$ si a et b se divisent mutuellement.**Proposition**Ceci définit une relation d'équivalence sur A .**Théorème**Soit $a, b \in A$. On a équivalence entre :

- (i) a et b sont associés;
- (ii) $aA = bA$;
- (iii) $\exists u \in U(A), b = au$.

dém. :

(i) $\Leftrightarrow bA \subset aA$ et $aA \subset bA \Leftrightarrow$ (ii)(i) $\Rightarrow$ (iii) Supposons a et b associés.Il existe $u, v \in A$ tels que $b = au$ et $a = bv$.On a alors $a = a(uv)$.Cas $a = 0_A$: $b = au = 0_A$ et donc $b = a \times 1_A$.Cas $a \neq 0_A$: Par intégrité, $uv = 1_A$ et donc $u \in U(A)$ puis $b = au$ avec $u \in U(A)$.

(iii) $\Rightarrow$ (i) Supposons qu'il existe $u \in U(A)$ tel que $b = au$.

On a donc $b \in aA$ puis $bA \subset aA$.

Aussi $a = bu^{-1}$ donc $aA \subset bA$ puis $=$.

□

Exemple Dans $\mathbb{Z}$, a et b sont associés si, et seulement si, $|a| = |b|$.

Ainsi, tout entier est associé à un unique entier naturel.

Exemple Dans $\mathbb{K}[X]$, A et B sont associés si, et seulement si,

$$\exists \lambda \in \mathbb{K}^*, A = \lambda B$$

Ainsi, tout polynôme non nul est associé à un unique polynôme unitaire.

2.5.3 Arithmétique dans $\mathbb{Z}$

Par ce qui précède

$$a \mid b \Leftrightarrow b\mathbb{Z} \subset a\mathbb{Z}$$

Dans la suite nous exploitons cette interprétation pour revoir l'arithmétique des entiers.

2.5.3.1 PGCD et PPCM

Théorème

Soit $a, b \in \mathbb{Z}$. Il existe unique $d \in \mathbb{N}$ tel que

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$$

On a alors

$$d \mid a, d \mid b \text{ et } \forall c \in \mathbb{Z}, (c \mid a \text{ et } c \mid b) \Rightarrow c \mid d$$

dém. :

$a\mathbb{Z}$ et $b\mathbb{Z}$ sont des idéaux de $\mathbb{Z}$ donc $a\mathbb{Z} + b\mathbb{Z}$ aussi.

Par suite, il existe $d \in \mathbb{N}$ unique vérifiant $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Puisque $a\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, on a $d \mid a$. De même $d \mid b$.

Si $c \mid a$ et $c \mid b$ alors $a\mathbb{Z} \subset c\mathbb{Z}$ et $b\mathbb{Z} \subset c\mathbb{Z}$ donc $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \subset c\mathbb{Z}$ puis $c \mid d$.

□

Définition

Ce naturel d est appelé PGCD de a et b

$$d = a \wedge b$$

def

Corollaire

Si $d = a \wedge b$ alors il existe $u, v \in \mathbb{Z}$ vérifiant $d = au + bv$.

Théorème

Soit $a, b \in \mathbb{Z}$. Il existe unique $m \in \mathbb{N}$ tel que

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$$

On a alors

$$a \mid m, b \mid m \text{ et } \forall c \in \mathbb{Z}, (a \mid c \text{ et } b \mid c) \Rightarrow m \mid c$$

dém. :

$a\mathbb{Z}$ et $b\mathbb{Z}$ sont des idéaux de $\mathbb{Z}$ donc $a\mathbb{Z} \cap b\mathbb{Z}$ aussi. Par suite, il existe $m \in \mathbb{N}$ unique vérifiant $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

Puisque $m\mathbb{Z} \subset a\mathbb{Z}$, on a $a \mid m$ et de même $b \mid m$.

Si $a \mid c$ et $b \mid c$ alors $c\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ donc $m \mid c$.

□

Définition

Ce naturel m est appelé PPCM de a et b :

$$m \stackrel{\text{def}}{=} a \vee b$$

Remarque On définit aussi le pgcd d et le ppcm m de plusieurs entiers $a_1, \dots, a_n$ par

$$d\mathbb{Z} = a_1\mathbb{Z} + \dots + a_n\mathbb{Z} \text{ et } m\mathbb{Z} = a_1\mathbb{Z} \cap \dots \cap a_n\mathbb{Z}$$

2.5.3.2 Entiers premiers entre eux

Définition

Deux entiers a et b sont dits premiers entre eux si $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ (autrement dit si leur PGCD vaut 1).

On note $a \wedge b = 1$.

Théorème

Soit $a, b \in \mathbb{Z}$. On a équivalence entre :

(i) a et b sont premiers entre eux ;

(ii) $\exists u, v \in \mathbb{Z}, au + bv = 1$.

dém. :

(i) $\Rightarrow$ (ii) via l'égalité de Bézout.

(ii) $\Rightarrow$ (i) via $1 \in a\mathbb{Z} + b\mathbb{Z}$ donc $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$.

□

Corollaire

On a

$$\forall a, b, c \in \mathbb{Z}, (a \wedge b = 1 \text{ et } a \wedge c = 1) \Rightarrow a \wedge (bc) = 1$$

$$\forall a, b \in \mathbb{Z}, a \wedge b = 1 \Rightarrow \forall \alpha, \beta \in \mathbb{N}, a^\alpha \wedge b^\beta = 1$$

Théorème

$$\forall a, b, c \in \mathbb{Z}, (a \mid bc \text{ et } a \wedge b = 1) \Rightarrow a \mid c$$

dém. :

$$c\mathbb{Z} = c(a\mathbb{Z} + b\mathbb{Z}) = ac\mathbb{Z} + bc\mathbb{Z} \subset a\mathbb{Z} \text{ donc } a \mid c.$$

□

Théorème

$$\forall a, b, c \in \mathbb{Z}, (a \wedge b = 1, a \mid c \text{ et } b \mid c) \Rightarrow ab \mid c$$

2.5.3.3 Nombre premiers**Définition**

Un naturel $p \geq 2$ est dit premier si ses seuls diviseurs positifs sont 1 et lui-même.

Exemple Deux entiers a et b sont premiers entre eux si, et seulement si, ils ne possèdent pas de facteurs premiers en commun.

Théorème

Pour tout $a \in \mathbb{N}$ tel que $a \geq 2$ on peut écrire

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_N^{\alpha_N}$$

avec $N \in \mathbb{N}^*$, $p_1, \dots, p_N$ nombres premiers deux à deux distincts et $\alpha_1, \dots, \alpha_N \in \mathbb{N}^*$.

De plus, cette décomposition est unique à l'ordre près des facteurs.

Exemple Si $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_N^{\alpha_N}$ et $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_N^{\beta_N}$ (écriture qu'il est possible d'obtenir en autorisant les exposants à être nuls) alors

$$a \wedge b = \prod_{i=1}^N p_i^{\min(\alpha_i, \beta_i)} \text{ et } a \vee b = \prod_{i=1}^N p_i^{\max(\alpha_i, \beta_i)}$$

En particulier, on constate

$$(a \wedge b) \times (a \vee b) = ab$$

2.5.4 Fonction indicatrice d'Euler**Définition**

On appelle fonction indicatrice d'Euler l'application $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$ définie par

$$\varphi(n) = \text{Card} \{k \in [1, n] / k \wedge n = 1\}$$

Exemple $\varphi(12) = \text{Card} \{1, 5, 7, 11\} = 4$.

Remarque $\varphi(n)$ est aussi :

- le nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$;
(c'est aussi le nombre de racines primitives n -ième de l'unité)
- le nombre d'éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.
(c'est donc le cardinal de $U(\mathbb{Z}/n\mathbb{Z})$)

Lemme

Si p est un nombre premier et $\alpha \in \mathbb{N}^*$ alors

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

dém. :

Pour $k \in [1, p^\alpha]$, le pgcd de k et p^α est un diviseur de p^α .

Puisque p est premier les naturels diviseurs de p^α sont $1, p, p^2, \dots, p^\alpha$.

Par suite $\text{pgcd}(k, p^\alpha) = 1, p, \dots$ ou p^α .

On en déduit

$$k \wedge p^\alpha \neq 1 \Leftrightarrow p \mid k$$

Par suite, les entiers $k \in [1, p^\alpha]$ qui ne sont pas premiers avec p^α sont ceux qui sont les multiples de p suivants

$$p, 2p, \dots, p^\alpha$$

Il y en a $p^{\alpha-1}$ et donc

$$\varphi(p^\alpha) = \text{Card}[1, p^\alpha] - p^{\alpha-1} = p^\alpha - p^{\alpha-1}$$

□

Lemme

Si n et m sont deux entiers naturels non nuls premiers entre eux alors

$$\varphi(nm) = \varphi(n)\varphi(m)$$

dém. :

Par le théorème Chinois, l'anneau $\mathbb{Z}/mn\mathbb{Z}$ est isomorphe à $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Il y a donc autant d'éléments inversibles dans $\mathbb{Z}/mn\mathbb{Z}$ que dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Il y a exactement $\varphi(mn)$ éléments inversibles dans $\mathbb{Z}/mn\mathbb{Z}$.

Les éléments inversibles de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont les couples formés par un élément inversible de $\mathbb{Z}/m\mathbb{Z}$ et un élément inversible de $\mathbb{Z}/n\mathbb{Z}$. Il y en a exactement $\varphi(m)\varphi(n)$.

Au final, on peut conclure

$$\varphi(mn) = \varphi(m)\varphi(n)$$

□

2.5. APPLICATION À L'ARITHMÉTIQUE

Théorème

Si $n \geq 2$ s'écrit

$$n = p_1^{\alpha_1} \dots p_N^{\alpha_N}$$

avec $p_1, \dots, p_N$ nombres premiers deux à deux distincts et $\alpha_1, \dots, \alpha_N \in \mathbb{N}^*$ alors

$$\varphi(n) = n \prod_{i=1}^N \left(1 - \frac{1}{p_i}\right)$$

dém. :

On a

$$\varphi(n) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_N^{\alpha_N}) = \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \dots \varphi(p_N^{\alpha_N})$$

car $p_1^{\alpha_1} \wedge (p_2^{\alpha_2} \dots p_N^{\alpha_N}) = 1$ puisque les nombres premiers p_i sont deux à deux distincts.

De même

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \dots \varphi(p_N^{\alpha_N}) = \prod_{i=1}^N \varphi(p_i^{\alpha_i})$$

Or

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right)$$

donc

$$\varphi(n) = \prod_{i=1}^N p_i^{\alpha_i} \prod_{i=1}^N \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^N \left(1 - \frac{1}{p_i}\right)$$

□

Exemple Les facteurs premiers de 12 sont 2 et 3.

$$\varphi(12) = 12 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) = 4$$

2.5.5 Théorème d'Euler

Théorème

Si a est un entier premier avec n alors

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

dém. :

$\bar{a}$ est un élément du groupe $(U(\mathbb{Z}/n\mathbb{Z}), \times)$. Ce groupe possède $\varphi(n)$ éléments donc

$$\bar{a}^{\varphi(n)} = \bar{1}$$

i.e.

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

□

Remarque Si p est un nombre premier, $\varphi(p) = p - 1$ et l'on retrouve le petit théorème de Fermat

$$a \not\equiv 0 \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

2.5.6 Musculations

2.5.6.1 Une relation

Proposition

$$\forall n \in \mathbb{N}^*, n = \sum_{d|n} \varphi(d)$$

dém. :

Considérons les n nombres rationnels

$$\frac{1}{n}, \frac{2}{n}, \dots, \frac{k}{n}, \dots, \frac{n}{n}$$

L'écriture irréductible de ces nombres est de la forme

$$\frac{k}{n} = \frac{p}{d} \text{ avec } d | n \text{ et } p \wedge d = 1$$

Il y a exactement $\varphi(d)$ fractions qui se réduisent avec le dénominateur d et donc

$$\varphi(n) = \sum_{d|n} \varphi(d)$$

□

2.5.6.2 Nombre de diviseurs

Exemple Pour $n \in \mathbb{N}^*$, notons

$$\text{Div}(n) = \{d \in \mathbb{N}^* / d | n\} \text{ et } \delta(n) = \text{CardDiv}(n)$$

Pour $n = 6$, $\text{Div}(6) = \{1, 2, 3, 6\}$ et $\delta(6) = 4$.

De façon générale, exprimons $\delta(n)$.

Pour $n = p^\alpha$ avec p nombre premier on a

$$\text{Div}(p^\alpha) = \{1, p, \dots, p^\alpha\} \text{ et } \delta(p^\alpha) = \alpha + 1$$

Pour $m \wedge n = 1$, montrons $\delta(mn) = \delta(m)\delta(n)$.

Considérons l'application $f : \text{Div}(m) \times \text{Div}(n) \rightarrow \text{Div}(mn)$ définie par $f(a, b) = ab$.

L'application considérée est bien définie par

$$(a | m \text{ et } b | n) \Rightarrow ab | mn$$

Montrons que f est bijective.

Supposons $f(a, b) = f(c, d)$. On a $ab = cd$.

a divise cd or $a \wedge d = 1$ (car a et d sont diviseurs de m et n premiers entre eux) donc a divise c .

IV LA STRUCTURE D'ALGÈBRE

1 Algèbre et sous-algèbre

Définition : Structure d'algèbre

On dit que $(\mathcal{A}, +, \times, \cdot)$ est une K -algèbre lorsque

- $(\mathcal{A}, +, \cdot)$ est une K -espace vectoriel,
- $(\mathcal{A}, +, \times)$ est un anneau,
- Pseudo-associativité : $\forall \lambda \in K, \forall x, y \in \mathcal{A}, \lambda \cdot (x \times y) = (\lambda \cdot x) \times y = x \times (\lambda \cdot y)$.

Exemples

- E1 - $(C, +, \times, \cdot)$ est une R -algèbre et une C -algèbre.
- E2 - $(K^X, +, \times, \cdot)$ est une K -algèbre.
- E3 - $(K^N, +, \times, \cdot)$ est une K -algèbre.
- E4 - $(K[X], +, \times, \cdot)$ est une K -algèbre.
- E5 - $(K(X), +, \times, \cdot)$ est une K -algèbre.

- E6 - Si E est un K -espace vectoriel, $(\mathcal{L}(E), +, \cdot, \cdot)$ est une K -algèbre.
- E7 - Si $n \in N^*$, $(M_n(K), +, \times, \cdot)$ est une K -algèbre.

Propriété : Caractérisation des sous-algèbres

Soit $(\mathcal{A}, +, \times, \cdot)$ est une K -algèbre. $\mathcal{B}$ est une sous-algèbre de $(\mathcal{A}, +, \times, \cdot)$ lorsque

- (SA1) $\mathcal{B} \subset \mathcal{A}$
- (SA2) $1_{\mathcal{A}} \in \mathcal{B}$
- (SA3) $\forall x, y \in \mathcal{B}, \forall \lambda \in K, x + \lambda y \in \mathcal{B}$
- (SA4) $\forall x, y \in \mathcal{B}, \forall \lambda \in K, x \times y \in \mathcal{B}$

Exemples

- E1 - $K[X]$ est une sous-algèbre de $K(X)$.
- E2 - $\mathcal{C}^k(I, K)$ est une sous-algèbre de K^I .
- E3 - L'ensemble des suites convergentes est une sous-algèbre de K^N .
- E4 - L'ensemble $K[x]$ des fonctions polynomiales est une sous-algèbre de K^K .

Définition

Si $P = a_0 + a_1 X + \dots + a_n X^n \in K[X]$ et $x \in \mathcal{A}$, on pose $P(x) = \sum_{k=0}^n a_k x^k = a_0 1_{\mathcal{A}} + a_1 x + \dots + a_n x^n$.

Attention à ne pas oublier l'unité de $\mathcal{A}$!

2 Morphismes d'algèbres

Définition : Morphisme d'algèbre

Soit $(\mathcal{A}, +, \times, \cdot)$, $(\mathcal{B}, +, \times, \cdot)$ et $f: \mathcal{A} \rightarrow \mathcal{B}$. On dit que f est un **morphisme d'algèbres** lorsque

- (MA1) f est linéaire ie, $\forall x, y \in \mathcal{A}, \forall \lambda \in K, f(x + \lambda y) = f(x) + \lambda f(y)$
- (MA2) $\forall x, y \in \mathcal{A}, f(x \times y) = f(x) \times f(y)$
- (MA3) $f(1_{\mathcal{A}}) = 1_{\mathcal{B}}$.

Exemples

- E1 - Si $X \neq \emptyset$, $\mathcal{A}$ une K -algèbre, $a \in X$, alors $u_a: \begin{matrix} \mathcal{A}^X & \longrightarrow & \mathcal{A} \\ f & \longmapsto & f(a) \end{matrix}$ est un morphisme de K -algèbres. (morphisme d'évaluation).
- E2 - $f: \begin{matrix} K[X] & \longrightarrow & K[x] \\ P & \longmapsto & \tilde{P} \end{matrix}$ est un isomorphisme d'algèbre si K est infini, et $g: \begin{matrix} K[X] & \longrightarrow & K(X) \\ P & \longmapsto & \frac{P}{1} \end{matrix}$ est un morphisme d'algèbres injectif.
- E3 - $f: \begin{matrix} K & \longrightarrow & M_1(K) \\ x & \longmapsto & (x) \end{matrix}$ est un isomorphisme de K -algèbres.

Propriété

Soit $(\mathcal{A}, +, \times, \cdot)$ une K -algèbre et $x \in \mathcal{A}$.

Alors l'application $f : \begin{cases} K[X] & \longrightarrow & \mathcal{A} \\ P & \longmapsto & P(x) \end{cases}$ est un morphisme de K -algèbres.

Démonstration

Soit $P = \sum_{k \geq 0} a_k X^k, Q = \sum_{k \geq 0} b_k X^k \in K[X]$ et $\lambda \in K$. L'associativité et la distributivité des lois sur $\mathcal{A}$, toutes les sommes étant finies, permettent d'écrire :

- $(P + \lambda Q)(x) = \sum_{k \geq 0} (a_k + \lambda b_k) x^k = \sum_{k \geq 0} a_k x^k + \lambda \sum_{k \geq 0} b_k x^k = P(x) + \lambda Q(x).$
- $(PQ)(x) = \sum_{k, \ell \geq 0} a_k b_\ell x^{k+\ell} = \left(\sum_{k \geq 0} a_k x^k \right) \times \left(\sum_{\ell \geq 0} b_\ell x^\ell \right) = P(x) \times Q(x).$
- $f(1_{K[X]}) = f(X^0) = x^0 = 1_{\mathcal{A}}.$

□

Remarque

En particulier, deux polynômes en $x \in \mathcal{A}$ commutent toujours.

V COMPLÉMENT : SOUS-GROUPES DE $(\mathbb{R}, +)$

Théorème : Hors-Programme

Soit G est un sous-groupe de $(\mathbb{R}, +)$.

Alors G est soit dense dans $\mathbb{R}$, soit discret (de la forme $\alpha\mathbb{Z}$).

1. Traiter le cas où $G = \{0\}$.
2. On suppose dorénavant que $G \neq \{0\}$.
 - (a) Montrer que $G \cap \mathbb{R}_+^*$ est non vide. En déduire que $G \cap \mathbb{R}_+^*$ admet une borne inférieure.
On note α cette borne inférieure.
 - (b) On suppose dans cette question que $\alpha = 0$.
Montrer que pour tout $\delta > 0$, il existe $x \in G$ tel que $0 < x < \delta$. En déduire que G est dense dans $\mathbb{R}$.
 - (c) On suppose dans cette question que $\alpha > 0$.
 - i. Montrer qu'il existe $x \in G$ tel que $\alpha \leq x < 2\alpha$. En déduire que $x = \alpha$, puis que $\alpha\mathbb{Z} \subset G$.
 - ii. Soit réciproquement $x \in G$. Montrer que l'on peut trouver $q \in \mathbb{Z}$ tel que $q\alpha \leq x < (q+1)\alpha$.
En déduire que $x = q\alpha$.
 - iii. Conclure.