4

Structures algébriques

I Groupes et sous-groupes

1 Structure de groupe (MP2I)

Remarque : Quelques rappels

R 1 –

- **Loi de composition interne** sur un ensemble E : toute application
$$\star : \left| \begin{array}{ccc} E \times E & \longrightarrow & E \\ (x,y) & \longmapsto & x \star y \end{array} \right. .$$
- Elle est dite
  - ⋆ **associative** lorsque
  $$\forall (x,y,z) \in E^3, \quad (x \star y) \star z = x \star (y \star z)$$
  (que l'on peut alors noter $x \star y \star z$.)
  - ⋆ **commutative** lorsque
  $$\forall (x,y) \in E^2, \quad x \star y = y \star x.$$
- On dit que e est **élément neutre** pour $\star$ si pour tout $x \in E$, $x \star e = e \star x = x$.

Exercice 1

S'il existe, l'élément neutre est unique.

  - ⋆ **Notation additive** : $0x = e$ avec e souvent noté 0 ou 0_E appelé élément nul.
  - ⋆ **Notation multiplicative** : $x^0 = e$ avec e souvent noté 1 ou 1_E appelé élément unité.
- Un élément x de E est dit **symétrisable** pour $\star$ si on a $y \in E$ tel que $x \star y = y \star x = e$.

Exercice 2

S'il existe, y est unique.

  - ⋆ **Notation additive** : on parle d'opposé, noté $-x$. Pour $x + (-y)$, on note $x - y$.
  - ⋆ **Notation multiplicative** : on parle d'inverse, noté x^{-1}.

  ⚠ $\frac{x}{y}$ n'a pas de sens en général : cela désigne $x \star y^{-1}$ ou $y^{-1} \star x$?

Exemple

E 1 – L'élément neutre e (lorsqu'il existe) est toujours symétrisable, de symétrique lui-même.

Être symétrisable à gauche ou à droite ne suffit pas.

Exemple

E 2 – Sur E^E pour $\circ$, l'élément neutre est id_E.

- ⋆ $(\exists g \in E^E, \quad f \circ g = g \circ f = \mathrm{id}_E) \Longleftrightarrow$
- ⋆ $(\exists g \in E^E, \quad f \circ g = \mathrm{id}_E) \Longleftrightarrow$
- ⋆ $(\exists g \in E^E, \quad g \circ f = \mathrm{id}_E) \Longleftrightarrow$

- Soit $\star$ une loi de composition interne associative sur E notée multiplicativement.
  Si x et y sont symétrisables, alors
  - ⋆ $x \star y$ l'est aussi. De plus, $(x \star y)^{-1} = y^{-1} \star x^{-1}$.
  - ⋆ x^{-1} l'est aussi et $\left(x^{-1}\right)^{-1} = x$.

Définition 1 : Groupe

On appelle **groupe** tout couple $(G,\star)$ où G est un ensemble tel que

(i) $\star$ est une loi de composition interne sur G

(ii) $\star$ est associative

(iii) G admet un élément neutre pour $\star$

(iv) Tout élément de G admet un symétrique dans G pour $\star$.

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

Remarque

R 2 – En particulier, un groupe n'est jamais vide.

Exemple

E 3 – $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes commutatifs de neutre 0.

E 4 – Si D est un ensemble non vide, $(\mathbb{R}^D,+)$ et $(\mathbb{C}^D,+)$ et en particulier $\left(\mathbb{R}^{\mathbb{N}},+\right)$ et $\left(\mathbb{C}^{\mathbb{N}},+\right)$ sont des groupes commutatifs, de neutre la fonction / suite nulle.

E 5 – $(\mathbb{Q}^*,\times)$, $(\mathbb{Q}_+^*,\times)$, $(\mathbb{R}^*,\times)$, $(\mathbb{R}_+^*,\times)$ et $(\mathbb{C}^*,\times)$ sont des groupes commutatifs de neutre 1.

E 6 – Si E est un ensemble non vide, on note $\mathfrak{S}(E)$ l'ensemble des permutations de E (bijection de E sur E). Alors $(\mathfrak{S}(E),\circ)$ est un groupe d'élément neutre id_E.
Si $|E|\geqslant 3$, ce groupe n'est pas commutatif.
Si $n\in\mathbb{N}\setminus\{0,1\}$, et $E=[\![1,n]\!]$, on note $\mathfrak{S}_n=\mathfrak{S}([\![1,n]\!])$.
$(\mathfrak{S}_n,\circ)$ est appelé **groupe symétrique d'ordre** n (et contient $n!$ éléments).

Voir exercice du TD : 6, 13

2 Puissances ou itérées d'un élément (MP2I)

Définition 2 : Itérées d'un élément

Soir E un ensemble muni d'une loi de composition interne $\star$ (notée multiplicativement) **associative** et possédant un élément neutre e.
Pour tout $x\in E$ et tout $n\in\mathbb{N}$, on définit récursivement

$$x^n=\begin{cases}e & \text{si } n=0\\ x^{n-1}\star x & \text{sinon.}\end{cases}$$

Remarque

R 3 – Autrement dit, $x^n=\prod_{k=1}^{n}x=\underbrace{x\star\cdots\star x}_{n\text{ fois}}$.

R 4 – En notation additive,

$$n\cdot x=\begin{cases}0 & \text{si } n=0\\ (n-1)\cdot x+x & \text{sinon.}\end{cases}$$

Propriété 1 : des exposants

Soient $x,y\in E$ et $n,m\in\mathbb{N}$.

(i) $x^{n+m}=x^n\star x^m=x^m\star x^n$.

(ii) $(x^n)^m=x^{nm}=(x^m)^n$.

(iii) Si $x\star y=y\star x$, $(x\star y)^n=x^n\star y^n$.

(iv) Si x est inversible, x^n est inversible et $(x^n)^{-1}=\left(x^{-1}\right)^n$.

Notation 1 : Exposant négatif

Si $x\in E$ inversible et $n\in\mathbb{N}$, on note x^{-n} l'élément $\left(x^{-1}\right)^n=(x^n)^{-1}$.

Remarque

R 5 – Les propriétés (i) à (iii) restent vraies pour $n, m \in \mathbb{Z}$ lorsque x et y sont inversibles.

3 Régularité

Soit [1] E un ensemble muni d'une loi de composition interne associative $\star$ et possédant un élément neutre e.

Définition 3 : Régularité

Soit $x \in E$. On dit que x est **régulier** (ou **simplifiable**)

- **à gauche** lorsque
$$\forall\, a, b \in E,\quad x \star a = x \star b \Longrightarrow a = b$$
- **à droite** lorsque
$$\forall\, a, b \in E,\quad a \star x = b \star x \Longrightarrow a = b$$

On dit que x est **régulier** lorsqu'il l'est à gauche et à droite.

Voir exercice du TD : 5

Propriété 2 : Régularité d'un inversible

Tout élément inversible de $(E, \star)$ est régulier.

Corollaire 1 : Régularité dans un groupe

Si $(G, \star)$ est un groupe, alors tout élément de G est régulier.

1. On dit que $(E, \star)$ est un **monoïde**.

Corollaire 2 : Bijectivité des translations

Si $(G, \star)$ est une groupe et $a \in G$ fixé.

Les applications $\varphi_a : \left|\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & a \star x \end{array}\right.$ *et* $\psi_a : \left|\begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x \star a \end{array}\right.$ *(appelées translations à gauche et à droite) sont bijectives.*

Corollaire 3

Si $(G, \star)$ est une groupe et $a \in G$ fixé.

$$G = \{a \star x,\ x \in G\} = \{x \star a,\ x \in G\}.$$

Remarque

R 6 – Cela signifie que dans la table de la loi $\star$ du groupe G, chaque élément de G apparaît une et une seule fois sur chaque ligne et sur chaque colonne.

Exemple

E 7 – Si on considère le groupe des racines cubique de l'unité : $\mathbb{U}_3 = \{1, \mathrm{j}, \mathrm{j}^2\}$ muni de la loi $\times$, quelle est sa table ?

4 Groupe produit (MP2I)

Propriété 3 : Groupe produit

Soit $(G, \star)$ et (H, Δ) des groupes.
Pour tout (g, h) et (g', h') dans $G \times H$, on pose

$$(g, h) \top (g', h') = (g \star g', h \Delta h').$$

Alors $(G \times H, \top)$ a une structure de groupe.
Si, de plus, les lois $\star$ et Δ sont commutatives, alors $\top$ l'est.

Remarque

R7 – Cela se généralise à un nombre de groupes quelconque $\left(G_1, \underset{1}{\star}\right), \ldots, \left(G_p, \underset{p}{\star}\right)$ avec pour tout $(x_1, \ldots, x_p)$ et $(y_1, \ldots, y_p)$ dans $G_1 \times \cdots \times G_p$,

$$(x_1, \ldots, x_p) \top (y_1, \ldots, y_p) = \left(x_1 \underset{1}{\star} y_1, \ldots, x_p \underset{p}{\star} y_p\right).$$

5 Sous-groupes

a Définition et caractérisation (MP2I)

Définition 4 : Sous-groupe

Soit $(G, \star)$ groupe. On note $\star|_{H^2}$ la restriction à H^2 de la loi $\star$.
On dit que H est un **sous-groupe** de $(G, \star)$ si $H \subset G$ et $\left(H, \star|_{H^2}\right)$ est un groupe.

Propriété 4 : Sous-groupes triviaux

*Soit $(G, \star)$ groupe. G et $\{e_G\}$ sont des sous-groupes de $(G, \star)$ appelés **sous-groupes triviaux**.*

Propriété 5

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

(i) $(H, \star)$ possède le même élément neutre que $(G, \star)$.

(ii) Si $x \in H$, alors x a même inverse dans $(H, \star)$ et dans $(G, \star)$.

Voir exercice du TD : 7

Propriété 6 : caractérisation des sous-groupes

Soit $(G, \star)$ un groupe (multiplicatif). Les propositions suivantes sont équivalentes :

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

(ii)
$$\begin{cases} H \subset G \\ H \neq \varnothing \quad (e_G \in H) \\ H \text{ est stable par } \star : \\ \qquad \forall x, y \in H, \quad x \star y \in H \\ H \text{ est stable par inverse} \ : \\ \qquad \forall x \in H, \quad x^{-1} \in H \end{cases}$$

(iii)
$$\begin{cases} H \subset G \\ H \neq \varnothing \quad (e_G \in H) \\ \forall x, y \in H, \quad x \star y^{-1} \in H \end{cases}$$

Remarque

R8 – En notation additive, (ii) devient
$$\begin{cases} H \subset G \\ H \neq \varnothing \quad (0_G \in H) \\ H \text{ est stable par } \star \ : \ \forall x, y \in H, \quad x + y \in H \\ H \text{ est stable par opposé} \ : \ \forall x \in H, \quad -x \in H \end{cases}$$
et (iii) devient
$$\begin{cases} H \subset G, \ H \neq \varnothing \quad (0_G \in H) \\ \forall x, y \in H, \quad x - y \in H \end{cases}$$

Remarque

R9 – Un sous-groupe d'un groupe abélien est facilement encore commutatif.

Exemple

E 8 – $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sont des sous-groupes (additifs et abéliens) de $(\mathbb{C}, +)$.

E 9 – $\mathbb{R}^D$ où $D \neq \varnothing$ est un sous-groupe additif abélien de $(\mathbb{C}^D, +)$.

E 10 – $\mathbb{Q}^*$, $\mathbb{Q}_+^*$, $\mathbb{R}^*$, $\mathbb{R}_+^*$, $\mathbb{U}$, $\mathbb{U}_n$ pour $n \in \mathbb{N}^*$ sont des sous-groupes multiplicatifs abéliens de $(\mathbb{C}^*, \times)$. (On rappelle que $\mathbb{U} = \{z \in \mathbb{C},\ |z| = 1\}$ et pour $n \in \mathbb{N}^*$, $\mathbb{U}_n = \{z \in \mathbb{C},\ z^n = 1\} = \left\{e^{\frac{2ik\pi}{n}},\ k \in [\![0, n-1]\!]\right\}$.)

Voir exercice du TD : 9, 10, 12

Exercice 3 : Théorème de Lagrange

Soit $(G, *)$ un groupe d'ordre (c'est-à-dire de cardinal) fini, H un sous-groupe de G.

1. **Montrer que la relation définie par $x \mathcal{R} y \iff x^{-1} * y \in H$ est une relation d'équivalence sur G.**
2. **Vérifier que les classes d'équivalence ont toutes le même cardinal.**
3. **Démontrer le théorème de Lagrange : $|H|$ divise $|G|$.**

b Intersection et réunion (MPI)

Propriété 7 : Intersection de sous-groupes

Soit $(G, \star)$ un groupe et $(H_i)_{i \in I}$ une famille de sous-groupes de $(G, \star)$. Alors $\bigcap_{i \in I} H_i$ est un sous-groupe de $(G, \star)$.

Exercice 4 : Réunion de sous-groupes

Soit $(G, \star)$ un groupe, H, K sont des sous groupes de $(G, \star)$, alors

$$H \cup K \text{ sous-groupe de } G \iff H \subset K \text{ ou } K \subset H.$$

c Sous-groupes de $(\mathbb{Z}, +)$ (MPI)

Notation 2

Pour tout $a \in \mathbb{Z}$, on note $a\mathbb{Z} = \{ak,\ k \in \mathbb{Z}\}$.

Remarque

R 10 – On vérifie avec la caractérisation que $a\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.
Avec $a\mathbb{Z} = \{\ldots, -2a, -a, 0, a, 2a, \ldots\}$, il s'agit du plus petit sous-groupe (au sens de l'inclusion) contenant a. On dit qu'il est engendré par a (sur le même principe que les Vect en algèbre linéaire.)

Propriété 8 : Sous-groupes de $(\mathbb{Z}, +)$

Les sous-groupes G de $(\mathbb{Z}, +)$ sont exactement les

6 Morphismes (MP2I)

a Définition

Définition 5 : Morphisme de groupe

Soient $(G, \star)$ et $(G', \bullet)$ deux groupes.
$f : (G, \star) \to (G', \bullet)$ est un **morphisme de groupes** si et seulement si

$$\forall (x, y) \in G^2,\quad f(x \star y) = f(x) \bullet f(y)$$

Lorsque $(G, \star) = (G', \bullet)$, on parle d'**endomorphisme** de groupes.
Lorsque f est bijective, on parle d'**isomorphisme**.
Lorsqu'il existe un isomorphisme entre G et G', on dit que G et G' sont **isomorphes.**
Lorsque f est bijective et $G = G'$, on parle d'**automorphisme**.

Exemple

E 11 – $\ln : (\mathbb{R}_+^*, \times) \to (\mathbb{R}, +)$ isomorphisme de groupes.

E 12 – $\exp : (\mathbb{R}, +) \to (\mathbb{R}_+^*, \times)$ isomorphisme de groupes.

E 13 – $\left|\begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{U}, \times) \\ \theta & \longmapsto & \mathrm{e}^{\mathrm{i}\theta} \end{array}\right.$ morphisme de groupes (non injectif).

E 14 – Si $n \in \mathbb{N}^*$, $\sigma \in \mathfrak{S}_n$, $\varepsilon(\sigma)$ sa signature [a], alors $\varepsilon : (\mathfrak{S}_n, \circ) \to (\{-1, 1\}, \times)$ est un morphisme de groupes, c'est-à-dire

$$\forall \sigma, \sigma' \in \mathfrak{S}_n, \quad \varepsilon(\sigma \circ \sigma') = \varepsilon(\sigma) \times \varepsilon(\sigma').$$

E 15 – $\det : (\mathcal{GL}(E), \circ) \to (\mathbb{R}^*, \times)$ et $\det : (\mathcal{GL}_n(\mathbb{K}), \times) \to (\mathbb{R}^*, \times)$ sont des morphismes de groupes.

a. C'est-à-dire $(-1)^{I(\sigma)}$ où $I(\sigma)$ est le nombre d'inversions de σ ou encore $(-1)^N$ si σ s'écrit comme produit (composée) de N transpositions.

Voir exercice du TD : 8, 15, 16

Propriété 9 : Image du neutre et du symétrique par un morphisme de groupes

Si $f : (G, \star) \to (G', \bullet)$ est un morphisme de groupes, alors $f(e_G) = e_{G'}$ et pour tout $x \in G$, $f(\mathrm{sym}(x)) = \mathrm{sym}(f(x))$.

Remarque

R 11 – En notation multiplicative : $f(x^{-1}) = (f(x))^{-1}$.
En notation additive : $f(-x) = -f(x)$.
On peut avoir un mix des deux : par exemple, si c'est additif au départ et multiplicatif à l'arrivée, ça devient $f(-x) = (f(x))^{-1}$.

Propriété 10 : Image d'une itérée

En notation multiplicative, si $f : (G, \star) \to (G', \bullet)$ est un morphisme de groupes, pour tout $x \in G$ et pour tout $k \in \mathbb{Z}$, $f(x^k) = f(x)^k$.

Propriété 11 : Composée de morphismes

Si $f : (G, \star) \to (G', \bullet)$ et $g : (G', \bullet) \to (G'', \Delta)$ sont des morphismes de groupes, alors $g \circ f$ en est encore un.

b Noyau et image

Définition 6 : Image et noyau d'un morphisme

Soit $f : (G, \star) \to (G', \bullet)$ un morphisme de groupes.

- On appelle **noyau** de f l'ensemble

$$\mathrm{Ker}\, f =$$

Ainsi, $x \in \mathrm{Ker}\, f \iff f(x) = e_{G'}$.

- On appelle **image** de f l'ensemble

$$\mathrm{Im}\, f =$$

Ainsi, $y \in \mathrm{Im}\, f \iff \exists x \in G, \quad y = f(x)$.

Exemple

E 16 – $f : \left|\begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{U}, \times) \\ \theta & \longmapsto & \mathrm{e}^{\mathrm{i}\theta} \end{array}\right.$

Propriété 12 : Caractérisations de l'injectivité et de la surjectivité

Soit $f : (G, \star) \to (G', \bullet)$ un morphisme de groupe.

- *f est injectif si et seulement si $\operatorname{Ker} f = \{e_G\}$.*
- *f est surjectif si et seulement si $\operatorname{Im} f = G'$.*

Remarque

R 12 – Ainsi, f est injective si et seulement si $f(x) = e_{G'} (= f(e_G)) \Longrightarrow x = e_G$!

Exemple

E 17 – La fonction f de l'exemple précédent est donc non injective car $\operatorname{Ker} f = 2\pi\mathbb{Z} \neq \{0\}$.

Propriété 13 : Images directe et réciproque d'un sous-groupe

Soit $f : (G, \star) \to (G', \bullet)$ un morphisme de groupes.

(i) Si H est un sous-groupe de $(G, \star)$, alors $f(H)$ est un sous-groupe de $(G', \bullet)$

(ii) Si H' est un sous-groupe de $(G', \bullet)$, $f^{(-1)}(H')$ est un sous-groupe de $(G, \star)$.

Corollaire 4 : Cas particulier du noyau et de l'image

Soit $f : (G, \star) \to (G', \bullet)$ un morphisme de groupes.
Alors $\operatorname{Ker} f$ est un sous-groupe de $(G, \star)$ et $\operatorname{Im} f$ est un sous-groupe de $(G', \bullet)$.

Exemple

E 18 – $f : \left| \begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{C}^*, \times) \\ \theta & \longmapsto & \mathrm{e}^{\mathrm{i}\theta} \end{array} \right.$

E 19 – $f : \left| \begin{array}{ccc} (\mathbb{C}^*, \times) & \longrightarrow & (\mathbb{C}^*, \times) \\ z & \longmapsto & z^n \end{array} \right.$

c Isomorphismes

Propriété 14 : Réciproque d'un isomorphisme

Soit $f : (G, \star) \to (G', \bullet)$ un isomorphisme de groupes.
Alors f^{-1} est un isomorphisme du groupe $(G', \bullet)$ sur le groupe $(G, \star)$.

Remarque

R 13 – « Être isomorphe à » est une relation d'équivalence sur l'ensemble des groupes.

7 Groupes monogènes (MPI)

a Sous-groupes engendré par une partie

Définition 7 : Groupe engendré par une partie

Soit $(G, *)$ un groupe, A partie non vide de G.
On appelle **sous-groupe engendré par** A le plus petit (au sens de l'inclusion) sous-groupe de G contenant A, noté $\langle A \rangle$.
On dit alors que A est une **partie génératrice** de $\langle A \rangle$.

Remarque

R 14 – À mettre en parallèle avec la définition de Vect en algèbre linéaire.

Propriété 15 : Éléments de $\langle A\rangle$

Les éléments de $\langle A\rangle$ sont exactement les produits (pour $*$) d'éléments de A ou de A^{-1}.

Autrement dit, $x\in\langle A\rangle$ si et seulement s'il existe $k\in\mathbb{N}$, $(a_1,\dots,a_k)\in A^k$ et $(\varepsilon_1,\dots,\varepsilon_k)\in\{-1,1\}^k$ tel que

Remarque

R 15 – On a aussi que $\langle A\rangle$ est l'intersection de tous les sous-groupes contenant A (car c'est un sous-groupe, contenant A, plus petit que tous les autres.)

Exemple

E 20 – $\mathfrak{S}_n$ est engendré par les cycles.
(*Toute permutation se décompose en produit de cycles à supports disjoints. La décomposition est unique à l'ordre des facteurs près.*)

E 21 – $\mathfrak{S}_n$ est engendré par les transpositions.
(*Les cycles eux-mêmes se décomposent en produit de transpositions. Cette fois, il n'y a plus unicité de la décomposition, mais seulement de la parité du nombre de termes.*)

E 22 – Soit $\mathbb{K}$ un corps. $\mathcal{GL}_n(\mathbb{K})$ est engendré par les matrices de transvection $T_{i,j}(\lambda)$ (avec $i\neq j$), de dilatation $D_i(a)$ (avec $a\neq 0$) et de permutation $P_{i,j}$.
(*C'est une conséquence du pivot de Gauß : par opérations élémentaires, on peut transformer une matrice inversible en I_n.*)

b Groupes monogènes et cycliques

Propriété 16 : Sous-groupe engendré par un élément

*Soit $a\in G$. Le sous-groupe **engendré par** a noté $\langle a\rangle$ plutôt que $\langle\{a\}\rangle$ est*

*On dit que a en est un **générateur**.*

Remarque

R 16 – En notation additive, on a $\langle a\rangle=\{ka,\ k\in\mathbb{Z}\}$.

Définition 8 : Groupe monogène

Un groupe G est dit **monogène** s'il est engendré par un seul élément, c'est-à-dire s'il existe $a\in G$ tel que $G=\langle a\rangle$.
Un groupe G est dite **cyclique** si et seulement s'il est monogène et fini.

Exemple

E 23 – Tout sous-groupe de $(\mathbb{Z},+)$ est

E 24 – $(\mathbb{U}_n,\times)$ est cyclique engendré par

Exercice 5 : Montrer que les générateurs de $\mathbb{U}_n$ sont les $e^{\frac{2ik\pi}{n}}$ avec $k\wedge n=1$, appelées racines primitives n^{e} de l'unité.

Exemple : À observer sur un dessin

E 25 – Générateurs de $\mathbb{U}_6$ et détails de la génération pour $k=5$ par exemple.

c Ordre d'un élément dans un groupe

$(G,*)$ est un groupe d'élément neutre e.

Définition 9 : Ordre d'un élément

On dit que $a\in G$ est **d'ordre fini** s'il existe $k\in\mathbb{N}^*$ tel que $a^k=e$.
Dans ce cas, on appelle **ordre de** a le plus petit $k\in\mathbb{N}^*$ tel que $a^k=e$.

Remarque

R 17 – $f:\left|\begin{array}{ccc}\mathbb{Z}&\longrightarrow&G\\ k&\longmapsto&a^k\end{array}\right.$ est un morphisme de groupe donc son noyau est de la forme $m\mathbb{Z}$ où $m\in\mathbb{N}$.
En distinguant les cas $m=0$ et $m\neq 0$, on obtient des informations sur l'ordre de a.

Exemple : À observer sur un dessin

E 26 – Dans $\mathbb{U}_6$, $e^{5i\pi/3}$ est d'ordre 6 et $e^{2i\pi/3}$ est d'ordre 3.

Exercice 6 : Sans calcul !

Montrer que $\begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}$ **est d'ordre fini.**

Exercice 7

Caractériser dans $(\mathbb{U}, \times)$ **les** $e^{i\theta}$ **qui sont d'ordre fini.**

Propriété 17 : de l'ordre d'un élément

Soit a un élément de G d'ordre fini m.

- *Si $k \in \mathbb{Z}$, $a^k = e$ si et seulement si*
- $\langle a \rangle =$

  $|\langle a \rangle| =$

Remarque

R 18 – Ainsi, $a^k = a^\ell$ peut se traduire par la congruence

Exercice 8

Soit $(G, *)$ un groupe commutatif. On suppose que g_1 et g_2 sont d'ordres n_1 et n_2.

1. **On suppose n_1 et n_2 premiers entre eux. Montrer que $g_1 * g_2$ est d'ordre fini et calculer cet ordre.**
2. **Si $G = \mathcal{GL}_2(\mathbb{R})$, $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et $B = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$, vérifier que A et B sont d'ordre fini, mais pas AB.**
3. **Si n_1 et n_2 ne sont pas premiers entre eux, montrer que $g_1 * g_2$ n'est pas nécessairement d'ordre $n_1 n_2$ ou $n_1 \vee n_2$.**
4. - **Si d_1 est un diviseur de n_1, montrer qu'il existe un élément d'ordre d_1 dans G.**
   - **En déduire que G admet des éléments d'ordre $n_1 \vee n_2$.**
   - **Si G est fini, montrer que G admet un élément d'ordre le ppcm de l'ordre des éléments de G.**

Propriété 18 : Morphie des groupes monogènes

Tout groupe monogène infini est isomorphe à
Tout groupe monogène fini (donc cyclique) de cardinal n est isomorphe à

Propriété 19 : de l'ordre

Soit $(G, *)$ un groupe fini de neutre e.

(i) Tout élément de G est d'ordre fini.

(ii) L'ordre de tout élément de G divise le cardinal de G.

(iii) Pour tout $a \in G$, $a^{|G|} = e$.

Exercice 9 : Quels sont les sous-groupes finis de $(\mathbb{C}^*, \times)$?

II Anneaux et Corps

1 Anneaux (MP2I)

Définition 10 : Distributivité

Soit E un ensemble et $\star$ et $\top$ deux lois de composition interne sur E, on dit que $\star$ est **distributive** sur $\top$ lorsque $\forall (x, y, z) \in E^3$,

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

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

Définition 11 : Anneau

On dit que $(A,+,\times)$ est un **anneau** lorsque

(i) $(A,+)$ est un groupe abélien. L'élément neutre est noté 0_A.

(ii) $\times$ est une loi de composition interne associative admettant un élément neutre appelé unité de A, noté 1_A.

(iii) $\times$ est distributive sur $+$.

Lorsque, de plus, $\times$ est commutative, on dit que $(A,+,\times)$ est un **anneau commutatif.**

Exemple

E 27 – $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$, $(\mathbb{C}^D,+,\times)$ et $(\mathbb{R}^D,+,\times)$ (avec $D\neq\varnothing$), $\left(\mathbb{C}^{\mathbb{N}},+,\times\right)$ et $\left(\mathbb{R}^{\mathbb{N}},+,\times\right)$ sont des anneaux commutatifs.

E 28 – $(\mathcal{M}_n(\mathbb{R}),+,\times)$ et $(\mathcal{M}_n(\mathbb{C}),+,\times)$ sont des anneaux non commutatifs si $n\geqslant 2$.

Remarque

R 19 – 0_A est **absorbant** :

$$\forall\, a\in A,\quad a\times 0_A=0_A\times a=0_A.$$

En effet, $0_A=a\times(0_A+0_A)=a\times 0_A+a\times 0_A$ donc $a\times 0_A=0_A$. Idem à droite.

R 20 – Si $1_A=0_A$, alors pour tout $a\in A$, $a=a\times 1_A=a\times 0_A=0_A$, donc $A=\{0_A\}$.

R 21 – Si $A\neq\{0_1\}$, alors 0_A n'est pas inversible (pour $\times$).

R 22 – Pour tout $a,b\in A$, $-ab=(-a)\times b=a\times(-b)$.

2 Groupe des inversibles (MP2I)

Définition 12 : Inversibles d'un anneau

Soit $(A,+,\times)$ un anneau.
$a\in A$ est dit **inversible** si et seulement s'il est symétrisable pour $\times$.
Son symétrique est appelé **inverse** de a, noté a^{-1}.
On note U_A ou $U(A)$ ou $A^\times$ l'ensemble des inversibles de A.

Remarque

R 23 – On parle parfois d'unités de A, d'où la notation...

Exemple

E 29 – $U_{\mathbb{R}}=$

E 30 – $U_{\mathbb{Z}}=$

E 31 – $U_{\mathbb{C}^{\mathbb{N}}}=$

E 32 – $U_{\mathbb{C}^D}=$

E 33 – $U_{\mathcal{M}_n(\mathbb{K})}=$

Propriété 20 : Groupe des inversibles

Si $(A,+,\times)$ anneau, alors $(U_A,\times)$ est un groupe appelé ***groupe des inversibles*** *de A.*

3 Calculs dans un anneau (MP2I)

Propriété 21 : Calculs dans un anneau

Soit $(A,+,\times)$ un anneau. Soient $a,b\in A$ et $n\in\mathbb{N}$.

- *Si $a\times b=b\times a$,*
$$(ab)^n=a^nb^n.$$
- ***Formule du binôme de Newton** : Si $a\times b=b\times a$,*
$$(a+b)^n=$$
- ***Factorisation**[a] **de** a^n-b^n : Si $a\times b=b\times a$*
$$a^n-b^n=$$
$$=$$

- ***Somme géométrique*** *: En particulier, pour tout $x \in A$;*

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

a. parfois appelée formule de Bernoulli

Remarque

R 24 – Si a et b ne commutent pas,

$$(ab)^n = abab\cdots ab$$
$$(a+b)^2 = a^2 + ab + ba + b^2$$
$$(a+b)^3 = a^3 + a^2b + aba + ba^2 + ab^2 + bab + b^2a + b^3$$

etc.

4 Corps (MP2I)

Définition 13 : Corps

Soit $\mathbb{K}$ un ensemble, $+, \times$ deux lois de composition internes sur $\mathbb{K}$. On dit que $(\mathbb{K}, +, \times)$ est un **corps** lorsque

- $(\mathbb{K}, +, \times)$ est un anneau commutatif.
- $\mathbb{K} \setminus \{0_\mathbb{K}\}$ est non vide et tous ses éléments sont inversibles (c'est-à-dire $\mathbb{K} \neq \{0_\mathbb{K}\}$ et $U_\mathbb{K} = \mathbb{K}^\times = \mathbb{K} \setminus \{0_\mathbb{K}\}$.)

ou, de manière équivalente,

- $(\mathbb{K}, +)$ est un groupe abélien,
- $(\mathbb{K} \setminus \{0_\mathbb{K}\}, \times)$ est un groupe,
- $\times$ est commutative et distributive sur $+$.

Exemple

E 34 – $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ munis des lois $+$ et $\times$ sont des corps, mais pas $\mathbb{Z}$.

Voir exercice du TD : 28

5 Intégrité (MP2I)

Définition 14 : Anneau intègre

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

- A est commutatif,
- $A \neq \{0_A\}$ c'est-à-dire $1_A \neq 0_A$,
- A n'admet aucun diviseur de zéro, c'est-à-dire

$$\forall\, a, b \in A,\quad a \times b = 0_A \Longrightarrow a = 0_A \text{ ou } b = 0_A.$$

Exemple

E 35 – $\mathbb{R}, \mathbb{Z}, \mathbb{C}, \mathbb{Q}$ sont des anneaux intègres. $\mathbb{R}^\mathbb{N}$ et plus généralement $\mathbb{R}^D$ avec D contenant au moins deux éléments ne le sont pas.

Propriété 22 : Généralisation

Soit $(A, +, \times)$ un anneau intègre, $n \in \mathbb{N}^*$ et $(a_1, \ldots, a_n) \in A^n$.
Si pour tout $k \in [\![1, n]\!]$, $a_k \neq 0_A$, alors $a_1 \times \cdots \times a_n \neq 0_A$.

Propriété 23 : Régularité dans un anneau intègre

Soit $(A, +, \times)$ un anneau intègre.
Tout élément non nul de A est régulier (ie simplifiable) pour $\times$

Propriété 24 : Intégrité d'un corps

Tout corps est un anneau commutatif intègre. La réciproque est fausse.

Voir exercice du TD : 22

6 Anneau produit (MPI)

Propriété 25 : Anneau produit

Soit $(A,\dot{+},\dot{\times})$ et $(B,\oplus,\otimes)$ des anneaux.
Pour tout (a,b) et (a',b') dans $A\times B$, on pose

$$(a,b)+(a',b')=(a\dot{+}a',b\oplus b')$$
$$(a,b)\times(a',b')=(a\dot{\times}a',b\otimes b')$$

Alors $(A\times B,+,\times)$ a une structure d'anneau.
Si, de plus, les lois $\dot{\times}$ et $\otimes$ sont commutatives, alors $\times$ l'est.

Remarque

R 25 – Cela se généralise à un nombre d'anneaux quelconque $\left(A_1,\underset{(1)}{+},\underset{(1)}{\times}\right),\dots,\left(A_p,\underset{(p)}{+},\underset{(p)}{\times}\right)$ avec pour tout $(x_1,\dots,x_p)$ et $(y_1,\dots,y_p)$ dans $A_1\times\cdots\times A_p$,

$$(x_1,\dots,x_p)+(y_1,\dots,y_p)=\left(x_1\underset{(1)}{+}y_1,\dots,x_p\underset{(p)}{+}y_p\right)$$
$$(x_1,\dots,x_p)+(y_1,\dots,y_p)=\left(x_1\underset{(1)}{\times}y_1,\dots,x_p\underset{(p)}{\times}y_p\right)$$

Propriété 26 : Inversion dans un anneau produit

Si $(A,+,\times)$ et $(B,+,\times)$ sont deux anneaux, alors $U_{A\times B}=U_A\times U_B$.
De plus, si $(a,b)\in U_{A\times B}$, alors

$$(a,b)^{-1}=\left(a^{-1},b^{-1}\right).$$

7 Sous-anneau et sous-corps (MP2I)

Définition 15 : Sous-anneau

Soit $(A,+,\times)$ un anneau. On dit que B est un **sous-anneau** de $(A,+,\times)$ lorsque

- $B\subset A$
- **Important :** $1_A\in B$
- $\left(B,+|_{B^2},\times|_{B^2}\right)$ est un anneau.

Remarque

R 26 – Une partie peut avoir une structure d'anneau pour les lois induites sans avoir la même unité (ce n'est pas un sous-anneau au sens de la définition précédente.) C'est le cas trivialement de $\{0_A\}$.

Exemple

E 36 – Soit, dans l'anneau des matrices 2×2, l'ensemble B des matrices $\left(\begin{smallmatrix}a&0\\0&0\end{smallmatrix}\right)$ pour $a\in\mathbb{K}$. Alors $(B,+,\times)$ est un anneau d'unité $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)\neq I_2$.

Propriété 27 : Caractérisation des sous-anneaux

B est un sous-anneau de $(A,+,\times)$ si et seulement si

$$\begin{cases} B \subset A \\ (B,+) \text{ est un sous-groupe de } (A,+) \\ B \text{ est stable par } \times \ : \ \forall\, x,y \in B, \quad x \times y \in B \\ 1_A \in B \end{cases}$$

ou, de manière équivalente,

$$\begin{cases} B \subset A \\ 1_A \in B \\ \forall\, x,y \in B, \quad x+y \in B, \ -x \in B \ \text{ et } \ x \times y \in B \end{cases}$$

ou encore

$$\begin{cases} B \subset A \\ 1_A \in B \\ \forall\, x,y \in B, \quad x-y \in B \ \text{ et } \ x \times y \in B \end{cases}$$

Exemple

E 37 – Anneau des entiers de Gauß : $\mathbb{Z}[\mathrm{i}] = \mathbb{Z} + \mathrm{i}\mathbb{Z}$ est un sous-anneau de $(\mathbb{C},+,\times)$.

E 38 – $\mathcal{T}_n^+(\mathbb{K})$ est un sous-anneau de $(\mathcal{M}_n(\mathbb{K}),+,\times)$

E 39 – L'ensemble $\mathscr{B}(\mathbb{R})$ des fonctions bornées est un sous-anneau de $\left(\mathbb{R}^{\mathbb{R}},+,\times\right)$.

Définition 16 : Sous-corps

Soit $(\mathbb{K},+,\times)$ un corps. On dit que $(\mathbb{L},+,\times)$ est un **sous-corps** de $(\mathbb{K},+,\times)$ lorsque $\mathbb{L} \subset \mathbb{K}$ et $(\mathbb{L},+|_{\mathbb{L}^2},\times|_{\mathbb{L}^2})$ est un corps.

Propriété 28 : Caractérisation des sous-corps

$(\mathbb{L},+,\times)$ est un sous-corps de $(\mathbb{K},+,\times)$ si et seulement si

$$\begin{cases} \mathbb{L} \subset \mathbb{K} \\ (\mathbb{L},+) \text{ est un sous-groupe de } (\mathbb{K},+) \\ (\mathbb{L}\setminus\{0_{\mathbb{K}}\},\times) \text{ est un sous-groupe de} \\ (\mathbb{K}\setminus\{0_{\mathbb{K}}\},\times) \end{cases}$$

ou, de manière équivalente,

$$\begin{cases} \mathbb{L} \subset \mathbb{K} \\ \mathbb{L}\setminus\{0_{\mathbb{K}}\} \neq \varnothing \quad (1_{\mathbb{K}} \in \mathbb{L}) \\ \forall\, x,y \in \mathbb{L}, \quad x-y \in \mathbb{L} \\ \forall\, x,y \in \mathbb{L}\setminus\{0_{\mathbb{K}}\}, \quad xy^{-1} \in \mathbb{L} \end{cases}$$

Voir exercice du TD : 23

8 Morphismes d'anneaux (MP2I)

Définition 17 : Morphisme d'anneaux

Soient $(A,+,\times)$ et $\left(A',\oplus,\otimes\right)$ deux anneaux.
$f : (A,+,\times) \to \left(A',\oplus,\otimes\right)$ est un **morphisme d'anneaux** si et seulement si

(i) $\forall\,(a,b) \in A^2, \quad f(a+b) = f(a) \oplus f(b)$
(ie $f : (A,+) \to \left(A',\oplus\right)$ morphisme de groupes)

(ii) $\forall\,(a,b) \in A^2, \quad f(a \times b) = f(a) \otimes f(b)$

(iii) $f(1_A) = 1_{A'}$

On parle aussi, d'**endomorphisme**, d'**isomorphisme** et d'**automorphisme** d'anneaux.

$\operatorname{Ker} f = f^{(-1)}(\{0_{A'}\}) = \{a \in A \mid f(a) = 0_{A'}\}$ est le **noyau** de f.

$\operatorname{Im} f = f(A) = \{f(x),\ x \in A\}$ est l'**image** de f.

Remarque

R 27 – Comme on a en particulier un morphisme de groupes additifs, on peut utiliser les propriétés de ceux-ci :

- $f(0_A) = 0_{A'}$,
- Pour tout $a \in A$, $f(-a) = -f(a)$,
- f est injective si et seulement si $\operatorname{Ker} f = \{0_A\}$.

R 28 – En général, $\operatorname{Ker} f$ n'est pas un sous-anneau de A. C'est un sous-groupe additif stable par multiplication... Nous les étudions juste après !

Exemple

E 40 – $f : \left| \begin{array}{ccc} \mathbb{R}[X] & \longrightarrow & \mathbb{C} \\ P & \longmapsto & \tilde{P}(\mathrm{i}) \end{array} \right.$

Propriété 29 : des morphismes d'anneaux

Soit $f : (A,+,\times) \to (B,\oplus,\otimes)$ est un morphisme d'anneaux.

(i) Si a est inversible dans A, alors $f(a)$ l'est dans B et $f\left(a^{-1}\right) = \left(f(a)\right)^{-1}$.

(ii) Si f est un isomorphisme alors $f^{-1} : (B,\oplus,\otimes) \to (A,+,\times)$ est aussi un isomorphisme d'anneau.

(iii) Si $g : (B,\oplus,\otimes) \to (C,\dot{+},\dot{\times})$ est aussi un morphisme d'anneau, alors $g \circ f : (A,+,\times) \to (C,\dot{+},\dot{\times})$ l'est encore.

Définition 18 : Morphisme de corps

Soient $(\mathbb{K},+,\times)$ et $(\mathbb{K}',\oplus,\otimes)$ deux corps.
$f : (\mathbb{K},+,\times) \to (\mathbb{K}',\oplus,\otimes)$ est un **morphisme de corps** si et seulement s'il s'agit d'un morphisme d'anneaux.

Remarque

R 29 – Avec (i) et (ii), $f(1_{\mathbb{K}}) = \left(f(1_{\mathbb{K}})\right)^2$ et comme $\mathbb{K}'$ est intègre, $f(1_{\mathbb{K}})$ vaut $1_{\mathbb{K}'}$ ou $0_{\mathbb{K}'}$. S'il vaut $0_{\mathbb{K}'}$ et si (ii) est vérifiée, alors $f \equiv 0_{\mathbb{K}'}$.

Exemple

E 41 – $\mathrm{id}_{\mathbb{C}}$, $z \mapsto \overline{z}$ sont des automorphismes (involutifs) du corps $\mathbb{C}$.

E 42 – Tout morphisme de corps est injectif.

Voir exercice du TD : 25 à 27, 31

III Idéal d'un anneau commutatif (MPI)

1 Généralités

Définition 19 : Idéal

Soit $(A,+,\times)$ un anneau **commutatif** et $I \subset A$. On dit que I est un **idéal** de $(A,+,\times)$ lorsque

(i)

(ii)

Remarque

R 30 – Finalement, I est un **idéal** de $(A,+,\times)$ lorsque

- $I \subset A$
- $I \neq \varnothing$
- $\forall x,y \in I,\ \ x-y \in I$
- $\forall a \in A,\ \ \forall x \in I,\ \ ax \in I$.

Comme $-1_A \in A$, on peut se contenter de

- $I \subset A$
- $I \neq \varnothing$
- $\forall\, x, y \in I,\ \ x+y \in I$
- $\forall\, a \in A,\ \ \forall\, x \in I,\ \ ax \in I.$

Exemple

E 43 – $2\mathbb{Z}$ est un idéal de $(\mathbb{Z}, +, \times)$.

E 44 – L'ensemble des suites convergeant vers 0 est un idéal de l'anneau des suites bornées.

Remarque

R 31 – Si un idéal contient l'unité 1_A ou plus généralement un élément inversible, il est égal à

Propriété 30 : Idéaux triviaux

Soit $(A, +, \times)$ un anneau commutatif. $\{0_A\}$ et A sont des idéaux (triviaux) de $(A, +, \times)$.
Ce sont les seuls idéaux si de plus $(A, +, \times)$ est un corps.

Propriété 31 : Noyau d'un morphisme d'anneaux

Soit $f : (A, +, \times) \to (A', \oplus, \otimes)$ un morphisme d'anneaux. Alors $\operatorname{Ker} f$ est un idéal de $(A, +, \times)$.

Remarque

R 32 – $\operatorname{Im} f$ est un sous-anneau de $(A', \oplus, \otimes)$.
En général, $\operatorname{Ker} A$ n'est pas un sous-anneau de $(A, +, \times)$.

Exercice 10

Montrer que si $f : (A, +, \times) \to (A', \oplus, \otimes)$ est un morphisme d'anneaux :

- **L'image réciproque d'un sous-anneau de $(A', \oplus, \otimes)$ est un sous-anneau de $(A, +, \times)$.**
- **L'image directe d'un sous-anneau de $(A, +, \times)$ est un sous-anneau de $(A', \oplus, \otimes)$.**
- **L'image réciproque d'un idéal de $(A', \oplus, \otimes)$ par f est un idéal de $(A, +, \times)$.**
- **L'image directe d'un idéal de $(A, +, \times)$ par f est un idéal de $(f(A) = \operatorname{Im} f, \oplus, \otimes)$.**

Voir exercice du TD : 17 à 21, 29, 30

2 Somme et intersection d'idéaux

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

Propriété 32 : Somme et intersection d'idéaux

(*i*) *Soient $I_1, \dots, I_n$ des idéaux de $(A, +, \times)$. On note*

$$I_1 + \cdots + I_n =$$

Il s'agit d'un idéal de $(A, +, \times)$.
Il s'agit plus précisément du plus petit idéal de $(A, +, \times)$ (au sens de l'inclusion) contenant tous les idéaux I_j pour $1 \leqslant j \leqslant n$.

(*ii*) *Soient $(I_j)_{j \in J}$ une famille d'idéaux de $(A, +, \times)$.*
Alors $\bigcap_{j \in J} I_j$ est un idéal de $(A, +, \times)$.
Il s'agit du plus grand idéal de $(A, +, \times)$ (au sens de l'inclusion) contenu dans les idéaux I et J.

3 Idéal principal

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

Propriété 33 : Idéal engendré par un élément

Soit $x \in A$. On note

$$(x) = xA =$$

*C'est un idéal de A, appelé **idéal engendré** par x.*

Remarque

R 33 – C'est aussi le plus petit idéal contenant x, et donc l'intersection de tous les idéaux contenant x par unicité du plus petit élément.
Cette notion se généralise à plus d'un élément, un peu comme avec les Vect en algèbre linéaire.
Ainsi, l'idéal engendré par un nombre quelconque d'élément est l'ensemble des combinaisons linéaires (finies) de ces éléments, à cœfficients dans A.

Définition 20 : Idéal et anneau principal (HP)

- Tout idéal de la forme xA (donc engendré par un seul élément) est dit **principal**.
- Un anneau commutatif est dit **principal** lorsque

(i)
(ii)

Théorème 1 : Principalité de $\mathbb{Z}$

L'anneau $\mathbb{Z}$ est principal.

Remarque

R 34 – Les idéaux de $\mathbb{Z}$ sont donc principaux, c'est-à-dire engendré par un élément. Tous les générateurs sont associés.
Donc, quitte à choisir un générateur positif (ou nul), on a de plus unicité de celui-ci.

4 Divisibilité dans un anneau intègre

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

Définition 21 : Divisibilité

Soient $a,b \in A$.
On dit que b **divise** a ou que a est multiple de b lorsqu'il existe $q \in A$ tel que $a = bq$. On note $b|a$.
a et b sont dit associés lorsque $a|b$ et $b|a$.

Propriété 34 : Caractérisation avec les idéaux

Soient $a,b \in A$.
b divise a si et seulement si $a \in bA$ si et seulement si $aA \subset bA$.

Remarque

R 35 – Soit encore ssi tous les multiples de a sont des multiples de b.

Propriété 35 : Éléments associés

*On rappelle que $(A,+,\times)$ est un anneau commutatif **intègre**. Soient $a,b \in A$.*
a et b sont associés si et seulement si $aA = bA$ si et seulement si

Exemple

E 45 – Dans $\mathbb{Z}$, a,b sont associés si et seulement si

IV ARITHMÉTIQUE SUR $\mathbb{Z}$ (MP2I)

1 PGCD

Définition 22 : PGCD

Soient $a, b \in \mathbb{Z}$.
$I = (a) + (b) = a\mathbb{Z} + b\mathbb{Z} = \{au + bv,\ u, v \in \mathbb{Z}\}$ est un idéal non réduit à $\{0\}$ de $(\mathbb{Z}, +, \times)$ qui est un anneau principal.
Son unique générateur positif est appelé **pgcd de a et b**, noté $a \wedge b$.
On a donc, par définition, $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.

Propriété 36 : Relation de Bézout

Si $a, b \in \mathbb{Z}$, on peut trouver $a, b \in \mathbb{Z}$ tels que $au + bv = a \wedge b$.

Propriété 37 : Caractérisation

Soit $(a, b) \in \mathbb{Z}^2$.

$$d = a \wedge b \iff \begin{cases} d \in \mathbb{N} \\ d|a \text{ et } d|b \\ \forall\, c \in \mathbb{Z},\ \ (c|a \text{ et } c|b) \Longrightarrow c|d \end{cases}$$

Il s'agit donc du plus grand diviseur positif au sens de la division.
Par conséquent, les diviseurs de $a \wedge b$ sont exactement les diviseurs communs de a et de b.

Propriété 38 : Propriété d'Euclide

Si $a, b, q \in \mathbb{Z}$, $a \wedge b = (a - bq) \wedge b$ (pas nécessairement une division euclidienne).

Voir exercice du TD : 34

Définition 23 : Nombre entiers premiers entre eux

$a, b \in \mathbb{Z}$ sont dits **premiers entre eux** lorsque $a \wedge b = 1$, c'est-à-dire lorsque les seuls diviseurs communs ± 1.

Théorème 2 : de Bézout

Soit $a, b \in \mathbb{Z}$.

$$a \wedge b = 1 \iff \exists\, u, v \in \mathbb{Z},\ \ au + bv = 1$$

Corollaire 5

Soient $a, b, c \in \mathbb{Z}$.

(i) $a \wedge bc = 1 \iff a \wedge b = a \wedge c = 1$

(ii) *Si $d = a \wedge b$, on a $a', b' \in \mathbb{Z}$ tels que $a = da'$, $b = db'$ et $a' \wedge b' = 1$.*

Théorème 3 : Lemme de Gauß

Soient $a, b, c \in \mathbb{Z}$. Si $a|bc$ et $a \wedge b = 1$, alors $a|c$.

Voir exercice du TD : 41, 47

Méthode 1 : résolution des équations diophantiennes $ax + by = c$

où $a, b, c \in \mathbb{Z}^*$ sont fixés, on cherche les solutions entières.
On a facilement qu'il y a des solutions si et seulement si $\boxed{d = a \wedge b | c.}$

Lorsque c'est le cas, on peut trouver une solution particulière (x_0, y_0) avec l'algorithme d'Euclide par exemple.

Alors, si (x, y) solution , $ax + by = ax_0 + by_0$ puis $a(x - x_0) = b(y_0 - y)$ donc $a'(x - x_0) = b'(y_0 - y)$ avec $a' \wedge b' = 1$ en divisant par d.

Par lemme de Gauß, on a $k \in \mathbb{Z}$ tel que $x = x_0 + b'k$ puis en réinjectant $y = y_0 - a'k$.

On vérifie enfin que la réciproque étant vraie. Ensemble des solutions :

$$\{(x_0 + b'k, y_0 - a'k),\ k \in \mathbb{Z}\}.$$

Exercice 11 : Résoudre $199x+54y=4$ dans $\mathbb{Z}^2$.

Voir exercice du TD : 33

2 PPCM

Définition 24 : PPCM

Le PPCM de deux entiers a,b est l'unique générateur positif $a\vee b$ de l'idéal $a\mathbb{Z}\cap b\mathbb{Z}$ des multiples communs à a et à b.
On a donc $a\mathbb{Z}\cap b\mathbb{Z}=(a\vee b)\mathbb{Z}$.

Remarque

R 36 – Cette fois, il s'agit clairement de la même définition qu'en première année : le plus petit multiple commun positif.

Propriété 39 : du PPCM

(i) *Il s'agit du plus petit multiple positif commun à a et à b au sens de la division.*

(ii) *On a toujours que $|ab|=(a\wedge b)(a\vee b)$.*

3 Nombres premiers

Définition 25 : Nombre premier

Un **nombre premier** est un entier naturel $p\geqslant 2$ dont les seuls diviseurs positifs sont 1 et p.
On notera $\mathscr{P}$ l'ensemble des nombres premiers.

Remarque

R 37 – 1 n'est pas premier.

R 38 – 2 est le seul nombre premier pair.

R 39 – Un nombre premier possède exactement 4 diviseurs : ± 1 et $\pm p$.

R 40 – Pour qu'un nombre entier n soit premier, il faut et il suffit qu'il n'ait pas de diviseur entre 2 et $\sqrt{n}$.

Voir exercice du TD : 35, 36, 38, 40, 44

Propriété 40 : d'Euclide

L'ensemble des nombres premiers est infini.

Voir exercice du TD : 37

Propriété 41 : Diviseur premier ou non

Si $p\in\mathscr{P}$ et $n\in\mathbb{Z}$, alors $p|n$ ou (exclusif) $p\wedge n=1$.

Corollaire 6 : Nombre premier divisant un produit

Soient $p\in\mathscr{P}$ et $a_1,\dots,a_n\in\mathbb{Z}$.

$$p|(a_1\times\cdots\times a_n) \text{ si et seulement si } p \text{ divise l'un des } a_k.$$

Théorème 4 : fondamental de l'arithmétique – Décomposition primaire

Soit $n \in \mathbb{Z}^*$. On peut trouver $k \in \mathbb{N}$, $p_1, \dots, p_k$ premiers deux à deux distincts, $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$ tels que

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

appelée décomposition primaire de n.
De plus, cette écriture est unique à l'ordre des facteurs près.
$p_1, \dots, p_k$ sont les diviseurs premiers de n.

Définition 26 : Valuation p-adique

Soit $p \in \mathscr{P}$ et $n \in \mathbb{Z}^*$. On appelle **valuation p-adique** de n l'entier

$$v_p(n) = \max \{i \in \mathbb{N} \mid p^i \text{ divise } n\}.$$

Remarque

R 41 – La décomposition primaire se réécrit $n = \pm \prod_{p \in \mathscr{P},\ p|n} p^{v_p(n)} = \pm \prod_{p \in \mathscr{P}} p^{v_p(n)}$.

Propriété 42 : des valuations p-adiques

Soient $n, m \in \mathbb{Z}^*$, $p \in \mathscr{P}$.

(i) $v_p(n) \neq 0 \iff p|n$

(ii) $v_p(n \times m) = v_p(n) + v_p(m)$

(iii) $n|m \iff \forall\, p \in \mathscr{P},\ \ v_p(n) \leqslant v_p(m)$

(iv) $v_p(n \wedge m) = \min(v_p(n), v_p(m))$ *et* $v_p(n \vee m) = \max(v_p(n), v_p(m))$

Remarque

R 42 – Si $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ et $b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ avec des exposants éventuellement nuls, alors

$$a \wedge b = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)}$$

$$a \vee b = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)}$$

Exercice 12 : Montrer que $\sqrt{n} \in \mathbb{Q}$ si et seulement si n est un carré parfait.

Exercice 13 : Exprimer le nombre de diviseurs positifs de n à l'aide de ses valuations p-adiques.

Voir exercice du TD : 39

4 Congruences

Définition 27 : Congruence

Soit $n \in \mathbb{N}^*$. On dit que $a, b \in \mathbb{Z}$ sont **congrus modulo** n et on note $a \equiv b\ [n]$ lorsque $n|(a-b)$ ie lorsqu'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.

Propriété 43 : Relation d'équivalence

C'est une relation d'équivalence sur $\mathbb{Z}$.

Propriété 44 : Nombre d'entiers modulo n

$\forall\, a \in \mathbb{Z},\ \ \exists!\, r \in [\![0, n-1]\!],\ \ a \equiv r\ [n]$. r est le reste de la division euclidienne de k par n.
Ainsi, la relation d'équivalence $\cdot \equiv \cdot\ [n]$ possède exactement n classes d'équivalences.

Remarque

R 43 – On étudiera plus tard dans l'année l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes d'équivalences pour cette relation : les entiers modulo n.

Propriété 45 : Compatibilité de $+$ et $\times$

Soient $n \in \mathbb{N}^*$ et $a,b,c,d \in \mathbb{Z}$ tels que $a \equiv b\ [n]$ et $c \equiv d\ [n]$. Alors $a+c \equiv b+d\ [n]$ et $a \times c \equiv b \times d\ [n]$.
Plus généralement, si $m \in \mathbb{N}$, $a^m \equiv b^m\ [n]$.

Remarque

R 44 – Ce qui dotera $\mathbb{Z}/n\mathbb{Z}$ d'une structure d'anneau.

Remarque

R 45 – Les règles de divisibilité par 2, 3, 4, 5, 8, 9, 11 sont à connaître.

Propriété 46 : Petit théorème de Fermat

Si p est premier et $a \in \mathbb{Z}^*$ non divisible par p, alors

Dans tous les cas (que a soit divisible ou non par p),

Exercice 14 : CCINP 86

Théorème 5 : de Fermat-Wiles, ou grand théorème de Fermat

Si $n \in \mathbb{N}$ tel que $n \geqslant 3$, alors l'équation

$$x^n + y^n = z^n$$

n'admet aucune solution dans $\mathbb{N}_*^3$.

Démonstration : Non exigible[1]

1. J ai découvert une démonstration véritablement merveilleuse que ce cadre est trop étroit pour contenir...

Voir exercice du TD : 42, 43, 45, 46

V Structure d'algèbre (MPI)

1 Algèbre et sous-algèbre

Définition 28 : Structure d'algèbre

On dit que $(\mathscr{A},+,\times,\cdot)$ est une $\mathbb{K}$**-algèbre** lorsque

- $(\mathscr{A},+,\cdot)$ est une $\mathbb{K}$-espace vectoriel,
- $(\mathscr{A},+,\times)$ est un anneau,
- *Pseudo-associativité* : $\forall\,\lambda\in\mathbb{K},\ \ \forall\,x,y\in\mathscr{A}$,

$$\lambda\cdot(x\times y)=(\lambda\cdot x)\times y=x\times(\lambda\cdot y).$$

Exemple

E 46 – $(\mathbb{C},+,\times,\cdot)$ est une $\mathbb{R}$-algèbre et une $\mathbb{C}$-algèbre.

E 47 – $\left(\mathbb{K}^X,+,\times,\cdot\right)$ est une $\mathbb{K}$-algèbre.

E 48 – $\left(\mathbb{K}^{\mathbb{N}},+,\times,\cdot\right)$ est une $\mathbb{K}$-algèbre.

E 49 – $(\mathbb{K}[X],+,\times,\cdot)$ est une $\mathbb{K}$-algèbre.

E 50 – $(\mathbb{K}(X),+,\times,\cdot)$ est une $\mathbb{K}$-algèbre.

E 51 – Si E est un $\mathbb{K}$-espace vectoriel, $(\mathscr{L}(E),+,\circ,\cdot)$ est une $\mathbb{K}$-algèbre.

E 52 – Si $n\in\mathbb{N}^*$, $(\mathscr{M}_n(\mathbb{K}),+,\times,\cdot)$ est une $\mathbb{K}$-algèbre.

On a aussi une notion de sous-algèbre : c'est simultanément un sous-espace vectoriel et un sous-anneau, donc stable par combinaisons linéaires et par produit et contenant l'unité.

Propriété 47 : Caractérisation des sous-algèbres

Soit $(\mathscr{A},+,\times,\cdot)$ est une $\mathbb{K}$-algèbre. $\mathscr{B}$ est une sous-algèbre de $(\mathscr{A},+,\times,\cdot)$ lorsque

(i)

(ii)

(iii)

(iv)

Exemple

E 53 – $\mathbb{K}[X]$

E 54 – $\mathscr{C}^k(I,\mathbb{K})$

E 55 – L'ensemble des suites convergentes

E 56 – L'ensemble $\mathbb{K}[x]$ des fonctions polynomiales

L'intérêt principal des algèbres est de pouvoir évaluer un polynôme à coefficients dans $\mathbb{K}$ en un élément d'une $\mathbb{K}$-algèbre :

Définition 29 : Polynôme en un élément d'une algèbre

Si $P=a_0+a_1X+\cdots+a_nX^n\in\mathbb{K}[X]$ et $x\in\mathscr{A}$, on pose

$$P(x)=$$

Attention à ne pas oublier l'unité de $\mathscr{A}$!

2 Morphismes d'algèbres

Définition 30 : Morphisme d'algèbre

Soit $(\mathscr{A},+,\times,\cdot)$, $(\mathscr{B},+,\times,\cdot)$ et $f:\mathscr{A}\to\mathscr{B}$. On dit que f est un **morphisme d'algèbres** lorsque

(i) f est linéaire ie

(ii)

(iii)

Exemple

E 57 – Si $X\neq\varnothing$, $\mathscr{A}$ une $\mathbb{K}$-algèbre, $a\in X$, $u_a:\left|\begin{array}{ccc}\mathscr{A}^X&\longrightarrow&\mathscr{A}\\ f&\longmapsto&f(a)\end{array}\right.$

E 58 – $f:\left|\begin{array}{ccc}\mathbb{K}[X]&\longrightarrow&\mathbb{K}[x]\\ P&\longmapsto&\tilde{P}\end{array}\right.$

Propriété 48 : Morphisme d'évaluation polynomiale

Soit $(\mathscr{A},+,\times,\cdot)$ une $\mathbb{K}$-algèbre et $x\in\mathscr{A}$.

Alors l'application $f : \left|\begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & \mathscr{A} \\ P & \longmapsto & P(x) \end{array}\right.$ *est un morphisme de $\mathbb{K}$-algèbres.*

Remarque

R 46 – En particulier, deux polynômes en $x\in\mathscr{A}$ commutent toujours.

VI Complément (HP) : sous-groupes de $(\mathbb{R},+)$

Théorème 6 : Hors-Programme

Soit G est un sous-groupe de $(\mathbb{R},+)$.
Alors G est soit dense dans $\mathbb{R}$, soit discret (de la forme $\alpha\mathbb{Z}$).

Exercice 15 : Démonstration

Traiter le cas où $G=\{0\}$. On suppose dorénavant que $G\neq\{0\}$.

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.

Cas où $\alpha=0$ Montrer que G est dense dans $\mathbb{R}$ *en s'inspirant de la démonstration de la densité de $\mathbb{Q}$ dans $\mathbb{R}$.*

Cas où $\alpha>0$ *On s'inspire de la démonstration des sous-groupes de $(\mathbb{Z},+)$.*

Montrer qu'il existe $x\in G$ tel que $\alpha\leqslant x<2\alpha$.

En déduire que $x=\alpha$, puis que $\alpha\mathbb{Z}\subset G$.

Soit réciproquement $x\in G$. *On simule une division euclidienne.*

Montrer que l'on peut trouver $q\in\mathbb{Z}$ tel que $q\alpha\leqslant x<(q+1)\alpha$.

En déduire que $x=q\alpha$. Conclure.