

Structures algébriques usuelles Résumé

2) **Produit fini de groupes**

Soient $(G_1, *_1), \dots, (G_n, *_n)$ des groupes.

– loi produit définie sur le produit cartésien $G_1 \times \dots \times G_n$:

$$(x_1, \dots, x_n) * (y_1, \dots, y_n) = (x_1 *_1 y_1, \dots, x_n *_n y_n)$$

Prop :

Si $(G_1, *_1), \dots, (G_n, *_n)$ des groupes d'éléments neutres respectifs $e_1, \dots, e_n$, alors $G_1 \times \dots \times G_n$ est un groupe de neutre le n-uplet $(e_1, \dots, e_n)$.

Il est à noter que :

– si $(G_1, *_1), \dots, (G_n, *_n)$ sont abéliens alors $G_1 \times \dots \times G_n$ l'est aussi.

– L'inverse de $(x_1, \dots, x_n)$ est $(x_1, \dots, x_n)^{-1} = (x_1^{-1}, \dots, x_n^{-1})$

3) **L'ensemble $\mathbb{Z}/n\mathbb{Z}$**

Prop :

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

NB :

— $\bar{a}$, la classe d'équivalence de a , est donnée par :

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

— $\bar{a} = \bar{b} \Leftrightarrow a \equiv b[n]$

— $\bar{a} = \bar{0} \Leftrightarrow n/a$,

Notation :

L'ensemble quotient de $\mathbb{Z}$ est noté $\mathbb{Z}/n\mathbb{Z}$.

NB :

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

Prop :

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \overline{n-1}\}$$

Prop :

$$\begin{cases} a \equiv b [n] \\ c \equiv d [n] \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d [n] \\ ac \equiv bd [n] \end{cases}$$

Deux ici se définissent sur $\mathbb{Z}/n\mathbb{Z}$; la somme et le produit :

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

Prop :

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

4) Sous-groupes

NB :

$\{e\}$ et G sont des sous groupes triviaux de G .

Prop :

Un ssgr est aussi un groupe.

Prop :

Les ssgr de $(\mathbb{Z}, +)$ sont exactement les $n\mathbb{Z}$ avec $n \in \mathbb{N}$; où $n\mathbb{Z} = \{nk/k \in \mathbb{Z}\}$

Prop :

L'intersection d'une famille de ssgr est un ssgr :

Si tous les F_i sont des ssgr de G , alors $\bigcap_{i \in I} H_i$ l'est aussi.

NB :

la réunion de 2 ssgr n'est en général pas un ssgr. Toutefois, on a :

$$H \cup K \text{ est un ssgr} \Leftrightarrow (H \subset K \text{ ou } K \subset H)$$

5) **Sous-groupe engendré par une partie**

$(G, .)$ sera un groupe.

Déf :

Soit A une partie de G .

Le sous-groupe de G engendré par A est l'intersection de tous les sous-groupes de G contenant A .

On le note $\langle A \rangle$.

NB :

$$\langle A \rangle = \bigcap_{H \in I} H$$

où $I = \{H \text{ ssgr de } G / A \subset H\}$; l'ensemble des sous-groupes contenant A .

Prop :

$\langle A \rangle$ est le plus petit sous-groupe de G contenant A .

Vocab :

Si $G = \langle A \rangle$, A est dite *partie génératrice* de G . On dit aussi que G est *engendré* par A .

– Ainsi A est une *partie génératrice* du groupe $\langle A \rangle$

Prop :

Soit A une partie d'un groupe $(G, .)$.

Si tout élément de G s'écrit comme produit d'éléments de A **alors** A est une *partie génératrice* de G ; càd que G est engendré par A .

Prop :

Soit $a \in G$.

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

Notation et vocabulaire :

Soit $a \in G$.

$\{a^k / k \in \mathbb{Z}\}$ se note aussi $\langle a \rangle$ et s'appelle *le sous-groupe engendré par a*.

NB :

Si $(G, +)$ est additif, on a

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

Par exemple dans le groupe $(\mathbb{Z}, +)$, on a $\langle n \rangle = \{kn / k \in \mathbb{Z}\}$ qui se note $n\mathbb{Z}$.

6) Morphisme de groupes**Déf :**

On appelle morphisme du groupe (G_1, T_1) vers le groupe (G_2, T_2) toute application f définie de G_1 vers G_2 vérifiant

$$\forall x, y \in G, f(xT_1y) = f(x)T_2f(y)$$

Vocabulaire :

- i) Si f est un morphisme de G vers lui-même, on dit que f est un *endomorphisme* de G .
- ii) Un morphisme bijectif est dit *isomorphisme*.
- iii) Un endomorphisme bijectif de G est dit *automorphisme* de G .
- iv) Deux groupes sont dits *isomorphes* s'il existe un isomorphisme entre eux.

Prop :

- 1) La composée de deux morphismes (resp. endomorphismes)(resp. isomorphismes) est un morphisme (resp. endomorphisme)(resp. isomorphisme)
- 2) La réciproque d'un isomorphisme est un isomorphisme.

NB :

$(\text{Aut}(G), \circ)$ est un groupe ; où $\text{Aut}(G)$ est l'ensemble des automorphismes de G .

Prop

Soit f un morphisme du groupe G vers G' . Soient e et e' les éléments neutres respectifs. On a :

- 1) $f(e) = e'$
- 2) $\forall x \in G, f(x^{-1}) = f(x)^{-1}$
- 3) $\forall x \in G, \forall m \in \mathbb{Z}, f(x^m) = f(x)^m$

Définition et proposition : (Noyau et image d'un morphisme)

Soit f un morphisme du groupe G vers G' . Soit e' l'élément neutre de G' .

- 1) Le *noyau* de f est

$$\ker(f) = f^{-1}(\{e'\}) = \{x \in G / f(x) = e'\}$$

- 2) L'*image* de f est

$$\text{Im}(f) = f(G) = \{f(x) / x \in G\}$$

- 3) $\text{Ker}(f)$ et $\text{Im}(f)$ sont des sous-groupes resp de G et G' .

Prop :

Soit f un morphisme du groupe G vers G' . Soit e le neutre de G .

- 1) f est injectif $\Leftrightarrow \ker(f) = \{e\}$
- 2) f est surjectif $\Leftrightarrow \text{Im}(f) = G'$

7) Groupes monogènes. Groupes cycliques

Déf :

- i) Un groupe G est dit *monogène* s'il existe un élément $a \in G$ tel que $G = \langle a \rangle$.
 a est dit dans ce cas *un générateur* de G .
- ii) Un groupe monogène fini est dit groupe *cyclique*.

NB :

Tout groupe monogène est commutatif.

La réciproque est en général fausse :

Clé à retenir :

Soit H un sous-groupe de G . Soit $a \in G$. On a

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

Prop :

$\overline{m}$ est générateur de $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow m \wedge n = 1$

Prop :

- 1) Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$
- 2) Tout groupe cyclique de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$

8) **Ordre d'un élément**

Déf :

Soit $(G, \cdot)$ un groupe de neutre e . Soit $a \in G$.

- 1) a est dit *d'ordre fini* si et seulement s'il existe $n \in \mathbb{N}^*$ tel que $a^n = e$
- 2) Dans ce cas, *l'ordre de a* est le plus petit entier $n \in \mathbb{N}^*$ vérifiant $a^n = e$.

Cas d'un groupe additif $(G, +)$:

- 1) a est dit *d'ordre fini* si et seulement s'il existe $n \in \mathbb{N}^*$ tel que $na = 0$
- 2) Dans ce cas, *l'ordre de a* est le plus petit entier n vérifiant $na = 0$.

Prop :

Supposons $o(a)=n$, on a :

- 1) $a^k = e \Leftrightarrow n/k$
- 2) $a^k = a^l \Leftrightarrow n/(k-l) \Leftrightarrow k \equiv l[n]$

Prop

Si $o(a)=n$ alors $\langle a \rangle$, le sous-groupe engendré par a , est de cardinal n .

On a précisément : $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$

Prop

Supposons que G est un groupe fini et $\text{card}(G)=n$. Alors on a :

- 1) $\forall a \in G, a^n = e$
- 2) Tout élément a de G est d'ordre fini, et on a $o(a)/n$

II) Structure d'anneau

1) Rappels et compléments de SUP

Calcul dans un anneau :

$(A, +, \times)$ un anneau et $a, b \in A$ tels que $ab=ba$. On a :

- i. $(ab)^n = a^n b^n$
- ii. $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$: **Binôme de Newton**
- iii. $a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$: **Egalité de Bernoulli**

Prop :

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

NB :

$U(A)$ se note aussi $A^\times$.

$U(A)$ s'appelle le groupe des *unités* de A .

Prop :

Dans un anneau intègre, on a

$$ab = 0 \Leftrightarrow (a = 0 \text{ ou } b = 0)$$

Déf :

a est *nilpotent* si et ss'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$

L'*indice de nilpotence* de a est le plus petit entier p tel que $a^p = 0$

2) Produit fini d'anneaux

Soient $(A_1, +, \times), \dots, (A_n, +, \times)$ des anneaux.

Considérons les deux lois $+$ et $\times$ définies naturellement sur le produit cartésien $A_1 \times \dots \times A_n$ par

$$\begin{cases} (a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n) \\ (a_1, \dots, a_n) \times (b_1, \dots, b_n) = (a_1 \times b_1, \dots, a_n \times b_n) \end{cases}$$

Prop :

1) $(A_1 \times \cdots \times A_n, +, \times)$ est un anneau et que

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

2) $(a_1, \dots, a_n)$ est inversible $\Leftrightarrow a_1, \dots, a_n$ le sont.

$$\text{Dans ce cas } (a_1, \dots, a_n)^{-1} = (a_1^{-1}, \dots, a_n^{-1})$$

3) $U(A_1 \times \cdots \times A_n) = U(A_1) \times \cdots \times U(A_n)$

4) *En particulier*, si $(A, +, \times)$ est un anneau, alors $(A^n, +, \times)$ l'est aussi et on

$$U(A^n) = (U(A))^n$$

3) Sous-anneaux

Déf :

Soit $(A, +, \times)$ un anneau. Soit B une partie de A .

B est dite *sous-anneau* de A si et ssi

$$\begin{cases} a) 1 \in B \\ b) \forall x, y \in B, x - y \in B \\ c) \forall x, y \in B, x \times y \in B \end{cases}$$

Prop :

Un sous-anneau est à son tour un anneau.

4) Morphisme d'anneaux

Déf :

Soit f une application définie d'un anneau A vers un anneau B .

f est dite *morphisme d'anneaux* si et ssi

1) $f(1)=1$

2) $\forall x, y \in A, f(x + y) = f(x) + f(y)$

3) $\forall x, y \in A, f(x \times y) = f(x) \times f(y)$

Vocabulaire :

- 1) Un morphisme d'anneaux *bijectif* est dit *isomorphisme* d'anneaux.
- 2) Deux anneaux sont dits *isomorphes* s'il existe un morphisme d'anneaux entre eux.

Prop :

- 1) La *composée* de deux morphismes d'anneaux est un morphisme d'anneaux.
- 2) La *composée* de deux isomorphismes d'anneaux est un isomorphisme d'anneaux.
- 3) La *reciproque* d'un isomorphisme d'anneaux est un isomorphisme d'anneaux.

Prop :

- 1) La *composée* de deux morphismes d'anneaux est un morphisme d'anneaux.
- 2) La *composée* de deux isomorphismes d'anneaux est un isomorphisme d'anneaux.
- 3) La *reciproque* d'un isomorphisme d'anneaux est un isomorphisme d'anneaux.

Prop :

Soit f un morphisme d'anneaux de A vers B . On a :

- 1) $f(0)=0$
- 2) $\forall x \in A, \forall n \in \mathbb{N}, f(x^n) = (f(x))^n$
- 3) $\forall x \in A, \forall m \in \mathbb{Z}, f(mx) = mf(x)$
- 4) Si $x \in A$ est inversible alors son image $f(x)$ l'est aussi, et on a $(f(x))^{-1} = f(x^{-1})$

5) Noyau et image d'un morphisme d'anneaux

Déf :(noyau et image) ²

Soit f un morphisme d'anneaux de A vers B .

1) *Le noyau* de f :

$$\ker(f) = \{x \in A / f(x) = 0\} = f^{-1}\{0\}$$

2) *L'image* de f :

$$\operatorname{Im}(f) = \{f(x) / x \in A\} = f(A)$$

Prop :

Soit f un morphisme d'anneaux de A vers B . On a :

- 1) $\operatorname{Im}(f)$ est un sous-anneau de B
- 2) f est injective $\Leftrightarrow \ker(f) = \{0\}$
- 3) f est surjective $\Leftrightarrow \operatorname{Im}(f) = B$

6) Sous-corps

Déf :

Soit $(K, +, \times)$ un corps. Soit B une partie de K .

B est dite *sous-corps* de K si et ssi

$$\left\{ \begin{array}{l} a) 1 \in B \\ b) \forall x, y \in B, x - y \in B \\ c) \forall x, y \in B, x \times y \in B \\ d) \forall x \in B \setminus \{0\}, x^{-1} \in B \end{array} \right.$$

Prop : Un sous-corps est à son tour un corps.

7) L'anneau $\mathbb{Z}/n\mathbb{Z}$

Prop : Soit $n \geq 2$.

- 1) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif de neutres $\bar{0}$ et $\bar{1}$
- 2) $\bar{m}$ est inversible dans $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow m \wedge n = 1$
- 3) $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps $\Leftrightarrow p$ est un nombre premier

8) Idéal d'un anneau commutatif

$(A, +, \times)$ sera dans ce paragraphe un anneau commutatif de neutre 1.

Déf : Soit $I \subset A$.

I est un *idéal* de A si et ssi les trois conditions suivantes sont satisfaites :

- 1) $0 \in I$
- 2) $\forall x, y \in I, x + y \in I$
- 3) $\forall x \in I, \forall y \in A, x \times y \in I$

NB :

- a) $\forall x \in I, -x \in I$ (*vient de 3*))
- b) I est un sous-groupe de $(A, +)$
- c) $\{0\}$ et A sont des idéaux de A

Prop :

- 1) Les idéaux de $(\mathbb{Z}, +, \times)$ sont les $n\mathbb{Z}$.
- 2) Soit I un idéal de A . On a

$$I = A \Leftrightarrow 1 \in I$$

- 3) Le noyau d'un morphisme d'anneaux est un idéal.
- 4) L'intersection de deux idéaux est un idéal.
- 5) La somme de deux idéaux est un idéal ; avec la notation naturelle suivante

$$I + J = \{x + y / x \in I \text{ et } y \in J\}$$

Prop et déf : Soit $a \in A$.

- 1) $aA = \{ax/x \in A\}$ est un idéal de A .
- 2) aA s'appelle *l'idéal engendré par a* .
- 3) aA est le plus petit idéal de A contenant a .

9) **Divisibilité dans un anneau commutatif intègre**

$(A, +, \times)$ sera dans ce paragraphe un anneau commutatif intègre.

Déf : Soient $a, b \in A$

- 1) a *divise* b si et ss'il existe $c \in A$ tel que $b = ca$.
- 2) On note $a|b$

Propriétés immédiates : Soient $a, b, c \in A$.

- 1) $1|a, a|a, a|0$
- 2) $a|b \Leftrightarrow b \in aA \Leftrightarrow bA \subset aA$
- 3) $(a|b \text{ et } a|c) \Rightarrow a|(b + c)$
- 4) $(a|b \text{ et } b|c) \Rightarrow a|c$

Déf : a et b sont dits *associés* si et ssi $a|b$ et $b|a$

Prop : Les assertions suivantes sont équivalentes

- 1) a et b sont associés
- 2) $aA = bA$
- 3) $\exists u \in U(A) / a = bu$
- 4) $\exists v \in U(A) / b = av$

NB :

- 1) L'association est une relation d'équivalence sur A .
- 2) Soient $a, b \in \mathbb{Z}$. On a

$$a \text{ et } b \text{ sont associés} \Leftrightarrow |a| = |b| \Leftrightarrow a = \pm b$$

- 3) Soient $P, Q \in \mathbb{K}[X]$. On a

$$P \text{ et } Q \text{ sont associés} \Leftrightarrow \exists \lambda \in \mathbb{K}^*, P = \lambda Q$$

10) **Théorème chinois**

Prop : (Théorème chinois)

Si $m \wedge n = 1$ alors $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes par l'isomorphisme naturel

$$\begin{aligned}\mathbb{Z}/mn\mathbb{Z} &\rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \bar{k} &\mapsto (\widehat{k}, \widetilde{k})\end{aligned}$$

11) **Indicatrice d'Euler**

Déf : (Fonction indicatrice d'Euler)

C'est l'application $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$ définie par

$$\varphi(n) = \text{card}(\{1 \leq k \leq n / k \wedge n = 1\})$$

Prop :

$\varphi(n)$ est le nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, et c'est aussi le nombre d'éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

Prop :

1) $m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$

2) $\varphi(p^r) = p^r - p^{r-1}$, où p un nombre premier et $r \in \mathbb{N}^*$.

3) Si $n = \prod_{i=1}^s p_i^{r_i}$ est la décomposition de n en facteurs premiers

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

12) **Théorème d'Euler**

Prop : (Théorème d'Euler)

$$a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1 [n]$$

Corollaire :

Soit p un nombre premier. On a :

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

III) Anneaux de polynômes à une indéterminée

$\mathbb{K}$ sera un sous-corps de $\mathbb{C}$, par exemple $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$

Idéaux de l'anneau $\mathbb{K}[X]$

Prop :

I est un idéal de $(\mathbb{K}[X], +, \times)$ si et ssi I est de la forme $AK[X]$

Prop :

Soit I est un idéal **non nul** de $(\mathbb{K}[X], +, \times)$.

- 1) Il existe un **unique** polynôme **unitaire** A_0 tel que $I = A_0\mathbb{K}[X]$.
- 2) A_0 est de degré **minimal** parmi les polynômes **non nuls** de I .

PGCD de deux polynômes

Théorème et définition :

Soient A et $B \in \mathbb{K}[X]$ non nuls. Il existe un unique polynôme unitaire $D \in \mathbb{K}[X]$ tel que

$$A.\mathbb{K}[X] + B.\mathbb{K}[X] = D.\mathbb{K}[X]$$

D s'appelle le PGCD de A et B , et se note $D = A \wedge B$

NB :

Supposons $D = A \wedge B$. On a alors :

$$D|A, D|B, \text{ et si } (C|A, C|B) \text{ alors } C|D$$

Prop : $D = A \wedge B \Rightarrow (\exists U, V \in \mathbb{K}[X] \text{ tels que } D = AU + BV)$

Déf :

A et B sont dits premiers entre eux si et ssi $A \wedge B = 1$.

Autrement dit :

$$A.\mathbb{K}[X] + B.\mathbb{K}[X] = \mathbb{K}[X]$$

Prop :

Si $a \neq b$ alors $(X - a)$ et $(X - b)$ sont premiers entre eux.

Prop :

$A \wedge B = 1 \Leftrightarrow \exists U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$

Prop : (théorème de Gauss)

$(A|BC \text{ et } A \wedge B = 1) \Rightarrow A|C$

Irréductibles de $\mathbb{K}[X]$

La définition d'un polynôme irréductible dans $\mathbb{K}[X]$ est la même que celle vue au sup.

Les polynômes de degré 1 sont irréductibles dans $\mathbb{K}[X]$.

On a de même encore la décomposition d'un polynôme non constant en produit de facteurs irréductibles :

$$P = \alpha \prod_{i=1}^n P_i^{r_i}$$

où les P_i sont unitaires, irréductibles et distincts deux à deux.

Et que cette décomposition est unique à ordre près.

On rappelle que les polynômes irréductibles dans $\mathbb{C}[X]$ sont ceux de degré 1. Et les polynômes irréductibles dans $\mathbb{R}[X]$ sont ceux de degré 1 et ceux de degré 2 à discriminant strictement négatif.

IV) Structure d'algèbre

$\mathbb{K}$ est un sous-corps de $\mathbb{C}$

1) Algèbre

Déf : $(A, +, \cdot, \times)$ est une ***K*-algèbre** si et ssi les conditions suivantes sont satisfaites :

a) $(A, +, \cdot)$ est un K -espace vectoriel.

b) $(A, +, \times)$ est un anneau.

c) $\forall x, y \in A, \forall \lambda, \mu \in K, (\lambda x) \times (\mu y) = (\lambda \mu)(x \times y)$

Exemples usuels d'algèbres :

$(K[X], +, \cdot, \times)$, $(L(E), +, \cdot, \circ)$, $(M_n(K), +, \cdot, \times)$, $(F(X, K), +, \cdot, \times)$

2) Sous-algèbre

Déf :

Soit $B \subset A$, où $(A, +, \cdot, \times)$ est une algèbre.

B est une *sous-algèbre* de A si et ssi

$$1 \in B$$

$$\forall x, y \in B, \forall \lambda \in K, (\lambda x + y) \in B$$

$$\forall x, y \in B, x \times y \in B$$

Prop :

Toute sous-algèbre est une algèbre (pour les lois héritées de A)

3) Morphisme d'algèbre

Prop :

Soient A et B deux algèbres et $f : A \mapsto B$ une application.

f est dite *morphisme d'algèbres* si et ssi

$$f(1) = 1$$

$$\forall x, y \in A, \forall \lambda \in K, f(\lambda x + y) = \lambda f(x) + f(y)$$

$$\forall x, y \in A, f(x \times y) = f(x) \times f(y)$$

Prop :

Soient A et B deux algèbres et $f : A \mapsto B$ un morphisme d'algèbres.

1) $Im(f)$ est une *sous-algèbre* de B .

2) $Ker(f)$ est un *idéal* de A .

FIN