Résumé 21 – Structures algébriques

Structure de groupe

→ Groupes et sous-groupes

Définition : Groupe

Un groupe est un couple $(G,*)$ où G est un ensemble et $*$ une loi de composition interne tels que :

(i) la loi $*$ est associative :

$$\forall x,y,z\in G,\quad x*(y*z)=(x*y)*z$$

(ii) il existe un élément neutre :

$$\forall x\in G,\quad x*e=e*x=x$$

(iii) tout élément de G possède un inverse :

$$\forall x\in G,\quad \exists y\in G,\quad x*y=y*x=e$$

Proposition

Soit $(G,*)$ un groupe. $H\subset G$ est un sous-groupe de G si H est *non vide* et si :

$$\forall x,y\in H,\quad x*y^{-1}\in H$$

- Le produit fini de groupes est encore un groupe.
- L'intersection (quelconque) de sous-groupes de G est un sous-groupe de G.

Théorème : Sous-groupes de $\mathbb{Z}$

Si G est un sous-groupe de $(\mathbb{Z},+)$, alors il existe un unique $n\in\mathbb{N}$ tel que $G=n\mathbb{Z}$.

→ Morphismes de groupes

Définition : Morphisme de groupes

Un morphisme du groupe $(G,*)$ dans le groupe $(G',\star)$ est une application $\phi : G\to G'$ qui vérifie :

$$\forall x,y\in G,\quad \phi(x*y)=\phi(x)\star\phi(y)$$

Parmi les morphismes classiques, on rencontre exp, ln, det et la signature d'une permutation.

Les images directe et réciproque d'un sous-groupe par un morphisme de groupes est un sous-groupe.

Définition : Noyau et image d'un morphisme

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

- On appelle image de ϕ et on note $\mathrm{Im}(\phi)$ le sous-groupe $\phi(G)=\{\phi(x),x\in G\}$.
- On appelle noyau de ϕ et on note $\mathrm{Ker}(\phi)$ le sous-groupe $\phi^{-1}(\{e'\})=\{x\in G,\phi(x)=e'\}$.

Le noyau permet de caractériser l'injectivité.

→ Groupe $(\mathbb{Z}/n\mathbb{Z},+)$

On suppose ici $n\in\mathbb{N}^*$. Rappelons que si $a,b\in\mathbb{Z}$,

$$a\equiv b\,[n]\iff n\mid(a-b)\iff a-b\in n\mathbb{Z}$$

La congruence modulo n est une relation d'équivalence. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence de $\mathbb{Z}$ pour cette relation.

On munit alors $\mathbb{Z}/n\mathbb{Z}$ d'une addition et d'une multiplication (qui ne dépendent pas du choix du représentant).

Théorème

Pour tout $n\in\mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe abélien.

→ Groupes monogènes et groupes cycliques

Définition

Un groupe $(G,*)$ est dit :

- monogène s'il est engendré par un élément :
$$G=\langle a\rangle=\{a^k,k\in\mathbb{Z}\}$$
- cyclique s'il est monogène et fini.

Théorème

- Le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ est cyclique.
- $\mathbb{Z}/n\mathbb{Z}=\langle\overline{k}\rangle$ si et seulement si $k\wedge n=1$.

Théorème : Classification des groupes monogènes

Soit G un groupe monogène.

- Si G est infini, $G\simeq\mathbb{Z}$.
- Si G est cyclique, $G\simeq\mathbb{Z}/n\mathbb{Z}$ avec $\mathrm{card}(G)=n$.

→ Ordre d'un élément dans un groupe

Définition

Soient $(G,*)$ un groupe dont l'élément neutre est noté e et a un élément de G.

- a est d'ordre fini s'il existe $n\in\mathbb{N}^*$ tel que $a^n=e$.
- L'ordre de a est alors $\min\{n\in\mathbb{N}^*\mid a^n=e\}$.

L'ordre de a est aussi le cardinal du sous-groupe engendré par a. De plus, si a est d'ordre fini d, alors,

$$a^n=e\iff d\mid n$$

Théorème

L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.

Structures d'anneau et de corps

→ Anneaux et corps

Définition : Anneau

Un anneau est un triplet $(A,+,\times)$ où l'ensemble A est muni de deux lois de composition de sorte que :

(i) $(A,+)$ est un groupe commutatif ;

(ii) la loi $\times$ est associative, admet un élément neutre et est distributive sur $+$:

$$\forall x,y,z\in A,\quad x\times(y+z)=x\times y+x\times z \quad\text{et}\quad (x+y)\times z=x\times z+y\times z$$

- L'anneau est *commutatif* si la loi $\times$ est commutative.
- Un anneau commutatif est dit *intègre* si :

$$\forall (x,y)\in A^2,\quad x\times y=0_A \implies x=0_A \text{ ou } y=0_A$$

- Tout produit fini d'anneaux est un anneau.
- Si x et y commutent,

$$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}\,;\; x^n-y^n=(x-y)\sum_{k=0}^{n-1}x^k y^{n-1-k}$$

Proposition : Caractérisation d'un sous-anneau

Soit $(A,+,\times)$ un anneau. B est un sous-anneau de A si et seulement si $1_A\in B$ et :

$$\forall x,y\in B,\quad x-y\in B \quad\text{et}\quad x\times y\in B$$

Définition : Corps

Un corps $\mathbb{K}$ est un anneau commutatif pour lequel tout élément non nul admet un inverse pour la loi $\times$.

Dans le cadre du programme, les corps sont supposés commutatifs. Un corps est un anneau intègre.

Définition : Sous-corps

Soit $\mathbb{K}$ un corps. $\mathbb{K}'\subset\mathbb{K}$ est un sous-corps de $\mathbb{K}$ si :

$$\forall x,y\in\mathbb{K}'\times\mathbb{K}'^*,\quad x-y\in\mathbb{K}' \quad\text{et}\quad x\times y^{-1}\in\mathbb{K}'$$

→ Morphismes d'anneaux

Définition : Morphisme d'anneaux

Soient A et B deux anneaux. On appelle morphisme de A dans B toute application $\phi : A\to B$ qui vérifie :

(i) $\forall x,y\in G,\ \phi(x+y)=\phi(x)+\phi(y)$

(ii) $\forall x,y\in G,\ \phi(x\times y)=\phi(x)\times\phi(y)$

(iii) $\phi(1_A)=1_B$.

Un morphisme d'anneaux est un morphisme de groupes.

Définition : Noyau et image d'un morphisme

Si ϕ un morphisme de l'anneau A dans l'anneau B,

- $\mathrm{Im}(\phi)=\phi(A)=\{\phi(x),x\in A\}$;
- $\mathrm{Ker}(\phi)=\phi^{-1}(\{0_B\})=\{x\in A,\phi(x)=0_B\}$.

L'image d'un morphisme d'anneaux est un anneau, mais pas le noyau.

→ Idéaux d'un anneau commutatif

Définition : Idéal d'un anneau commutatif

Soit $(A,+,\times)$ un anneau commutatif. On appelle idéal de A toute partie I de A tel que :

(i) $(I,+)$ est un sous-groupe de $(A,+)$;

(ii) $\forall x\in I,\quad \forall a\in A,\quad xa\in I$.

Le noyau d'un morphisme d'anneaux est un idéal.

Si I_1 et I_2 sont deux idéaux d'un anneau commutatif A, $I_1\cap I_2$ et I_1+I_2 sont des idéaux de A.

Soit x un élément d'un anneau commutatif A.

$$(x)=xA=\{xa\mid a\in A\}$$

est le plus petit idéal de A contenant x. De plus,

$$x\mid y \iff yA\subset xA \iff (y)\subset(x)$$

→ Arithmétique dans $\mathbb{Z}$

Théorème

Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, où $n\in\mathbb{N}$.

Soient $a,b\in\mathbb{Z}$ non nuls. On appelle :

- plus grand diviseur commun de a et b l'unique entier naturel d tel que $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$. Notation : $a\wedge b$.
- plus petit commun multiple de a et b l'unique entier naturel c tel que $a\mathbb{Z}\cap b\mathbb{Z}=c\mathbb{Z}$. Notation : $a\vee b$.

Théorème : Théorème de Bézout

Soient $a,b\in\mathbb{Z}$. Alors $a\wedge b=1$ si et seulement s'il existe un couple $(u,v)\in\mathbb{Z}^2$ tel que $au+bv=1$.

L'algorithme d'Euclide permet de déterminer le pgcd de deux entiers ou une relation de Bézout.

Théorème : Lemme de Gauss

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

Si p est premier et $p\mid ab$, alors $p\mid a$ ou $p\mid b$.

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

Théorème

$(\mathbb{Z}/n\mathbb{Z},+,\times)$ est un anneau.

Théorème

Les assertions suivantes sont équivalentes :

(i) $\mathbb{Z}/n\mathbb{Z}$ est un corps.

(ii) $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.

(iii) n est premier.

L'élément $\overline{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k\wedge n=1$.

Théorème : Lemme chinois

Si m et n sont deux entiers premiers entre eux,

$$\mathbb{Z}/mn\mathbb{Z} \text{ est isomorphe à } \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

Définition : Indicatrice d'Euler

Pour $n \in \mathbb{N}^*$, on pose $\varphi(n) = \text{card}\{k \in [\![1, n]\!] \mid k \wedge n = 1\}$.
La fonction φ est appelée indicatrice d'Euler.

$\varphi(n)$ représente :

- le nombre d'entiers inférieurs à n et premiers avec n ;
- le nombre d'éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$;
- le nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, donc celui de $(\mathbb{U}_n, \times)$.

Proposition

Soient $m, n \in \mathbb{N}^*$. Si $m \wedge n = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$.

Proposition

Pour tout $n \in \mathbb{N}^*$, $\varphi(n) = n \cdot \prod_{\substack{p \text{ premier} \\ p|n}} \left(1 - \frac{1}{p}\right)$.

Proposition : Théorème d'Euler

Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N} \setminus \{0, 1\}$. Si $a \wedge n = 1$, alors :

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

Corollaire : Petit théorème de Fermat

Soient p un entier premier et $a \in \mathbb{Z}$. Alors,

$$a^p \equiv a\ [p]$$

Si de plus p ne divise pas a, $a^{p-1} \equiv 1\ [p]$.

Structure d'algèbre

Définition : $\mathbb{K}$-algèbre

Une algèbre sur un corps $\mathbb{K}$, ou $\mathbb{K}$-algèbre, est un ensemble $\mathscr{A}$ munis de trois lois $+$, $\times$ et $\cdot$ tels que :

(i) $(\mathscr{A}, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel ;

(ii) $(\mathscr{A}, +, \times)$ est un anneau ;

(iii) les lois $\times$ et $\cdot$ sont compatibles :

$$\forall a, b \in \mathbb{K},\ \forall x, y \in \mathscr{A},\ (a \cdot x) \times (b \cdot y) = ab \cdot (x \times y)$$

Une sous-algèbre de $\mathscr{A}$ est une partie $\mathscr{B}$ de $\mathscr{A}$ telle que $\mathscr{B}$ est à la fois un sous-anneau de $\mathscr{A}$ et un sous-espace vectoriel de $\mathscr{A}$.

Définition : Morphisme d'algèbres

Soient $\mathscr{A}$ et $\mathscr{B}$ deux $\mathbb{K}$-algèbres. On appelle morphisme de $\mathscr{A}$ dans $\mathscr{B}$ toute application $\phi : \mathscr{A} \to \mathscr{B}$ telle que ϕ est un morphisme d'anneaux et ϕ un morphisme d'espaces vectoriels.