Structures algébriques

$$\alpha 1 - MP^*$$

1 Groupes

1.1 Rappels

f un morphisme de groupes ; $\ker f = f^{-1}(\{e\})$.

groupe-produit : $(G,+)$ et $(G',\times)$ deux groupes. $\mathcal{G} = G \times G'$ est muni d'une structure de groupe : $(g,g') \bullet (h,h') = (g+g', h \times h')$. $e_{\mathcal{G}} = (e_G, e_{G'})$; l'inverse de (g,g') est $(-g, g'^{-1})$.

1.2 Sous-groupe engendré par une famille

$(G,+)$ un groupe, $\mathcal{F} = \{f_i / i \in \mathcal{I}, f_i \in G\}$ une famille dans G. On appelle *sous-groupe engendré par* $\mathcal{F}$ et on note $\text{gp}(\mathcal{F})$ l'intersection de tous les sous-groupes de G contenant $\mathcal{F}$. $\text{gp}(\mathcal{F})$ est alors le plus petit sous-groupe de G contenant $\mathcal{F}$ (au sens de l'inclusion).

Prop : $\text{gp}(\mathcal{F})$ est l'ensemble des expressions de la forme : $m_1 f_1 + \ldots + m_k f_k$ où $k \in \mathbb{N}$ (convention : si $k=0$, cette expression vaut 0_G), $m_1, \ldots, m_k \in \mathbb{Z}$ et $f_1, \ldots, f_k \in \mathcal{F}$. Si $\text{gp}(\mathcal{F}) = G$, on dit que $\mathcal{F}$ *engendre* G.

1.3 Sous-groupes de $\mathbb{Z}$

Si $k \in \mathbb{Z}$, on pose : $k\mathbb{Z} \overset{def}{=} \{km / m \in \mathbb{Z}\}$. $k\mathbb{Z}$ est alors un sous-groupe de $\mathbb{Z}$. Inversement, tout sous-groupe de $\mathbb{Z}$ est de cette forme.

2 Groupes $\mathbb{Z}/n\mathbb{Z}$

2.1 Définitions

Cougruences : Si $n \in \mathbb{Z}$, deux entiers p et q sont *congrus* modulo n si n divise $p-q$. Cela se note $p \equiv q \bmod n$. $\equiv$ est une relation d'équivalence (pour tout n).

Soit $n \in \mathbb{Z}$ fixé, on définit la *classe de p modulo n* : $\overline{p} = \{q \in \mathbb{Z} / q \equiv p \bmod n\} = \{p + kn, k \in \mathbb{Z}\}$. L'ensemble des classes d'équivalence est une partition de $\mathbb{Z}$; on le note $\mathbb{Z}/n\mathbb{Z}$. On a : $\text{card}(\mathbb{Z}/n\mathbb{Z}) = n$ dès que $n \geqslant 1$.

2.2 Addition dans $\mathbb{Z}/n\mathbb{Z}$

On munit $\mathbb{Z}/n\mathbb{Z}$ de la loi $+$: $\forall \overline{p}, \overline{q} \in \mathbb{Z}/n\mathbb{Z}, \overline{p} + \overline{q} = \overline{p+q}$. Muni de cette loi de composition interne, $\mathbb{Z}/n\mathbb{Z}$ est un groupe communtatif. $\overline{0}$ en est le neutre, l'opposé de $\overline{p}$ est $\overline{-p}$.

On définit la *surjection canonique* σ : $\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ p & \longmapsto & \overline{p} \end{array}$; c'est un morphisme surjectif de groupes.

Prop : soit $p \in \mathbb{Z}$, $\{\overline{p}\}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $p \wedge n = 1$.

2.3 Théorème de factorisation

Soit G un groupe, $f : \mathbb{Z} \longrightarrow G$ un morphisme. Soit $n \geqslant 1$. Alors : σ se factorise à droite dans f (c-à-d $\exists F : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$ morphisme tel que $f = F \circ \sigma$) si et seulement si $n\mathbb{Z} \subset \ker f$ si et seulement si $f(n) = 0_G$.

Lemme chinois : Soit $(p,q) \in \mathbb{N}^2$; si $p \wedge q = 1$, alors les groupes (même les anneaux) $\mathbb{Z}/pq\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ sont isomorphes.

3 Anneaux

3.1 Généralités

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

1. $1_A \in A'$
2. A' est stable pour $-$ et $\times$

Morphismes d'anneaux : A, A' deux anneaux. $f : A \longrightarrow A'$ est un morphisme d'anneaux si et seulement si :

1. $f(1_A) = 1_{A'}$
2. $\forall (a,b) \in A^2$, $f(a-b) = f(a) - f(b)$ et $f(a \times b) = f(a) \times f(b)$

$\ker f$ n'est pas seulement un sous-anneau de A : c'est un idéal de A.

Idéal d'anneau : Soit A un anneau ; $I \subset A$ est un idéal si

1. $0_A \in I$
2. I est stable pour la loi $-$
3. I est absorbant, c-à-d : $\forall i \in I, \forall a \in A, (ai \in I) \wedge (ia \in I)$ ou encore $(IA \subset I) \wedge (AI \subset I)$

Propriétés :

- $f : A \longrightarrow A'$ morphisme ; si I' est un idéal de A' alors $f^{-1}(I')$ est un idéal de A
- Soit $\mathcal{E}$ un ensemble d'idéaux de A, alors $\bigcap_{I \in \mathcal{E}} I$ est encore un idéal. On peut donc parler de l'*idéal engendré* par une partie de A : c'est l'intersection des idéaux qui la contiennent.
- On note $\text{Id}(\mathcal{P})$ l'idéal engendré par $\mathcal{P} \subset A$; c'est l'ensemble des éléments de la forme $\sum_{i=1}^{k} a_i x_i$ où : $k \in \mathbb{N}$, et $\forall i, a_i \in A, x_i \in \mathcal{P}$ si A est commutatif. Si A n'est pas commutatif, c'est $\sum_{i=1}^{k} a_i x_i a'_i$ (mêmes notations).Lorsque A est commutatif, l'idéal engendré par $\{x\}$ se note $Ax = \{ax, a \in A\}$.

Intégrité : Un anneau A est dit *intègre* s'il vérifie : $\forall (x,y) \in A^2, [(xy = 0) \Longrightarrow (x = 0) \vee (y = 0))]$. Si A est intègre, on dit que $x \mid y$ (dans A) s'il existe $y' \in A / y = xy'$. On a de plus : $(x \mid y) \Longleftrightarrow (yA \subset xA)$.

Un anneau commutatif intègre A est dit *principal* si tout idéal I de A est *principal*, c'est-à-dire de la forme xA $(x \in A)$. $\mathbb{Z}$ et $\mathbb{K}[X]$ (où $\mathbb{K}$ est un corps commutatif) sont principaux. $\mathbb{K}[X,Y]$ est non principal.

Sommes d'idéaux : Soit A commutatif, $I_1, \ldots, I_k$ des idéaux de A. Alors $I_1 + \ldots + I_k = \{x_1 + \ldots + x_k / \forall j, x_k \in I_j\}$ est un idéal de A.

3.2 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Si $\overline{p}, \overline{q} \in \mathbb{Z}/n\mathbb{Z}$, on définit $\overline{p} \times \overline{q} = \overline{p \times q}$. Muni de cette seconde loi, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

- Dans $\mathbb{Z}/n\mathbb{Z}$, $\overline{m}$ est inversible si et seulement si $m \wedge n = 1$.
- $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi $\mathbb{Z}/n\mathbb{Z}$ est intègre ssi n est premier

Factorisation à travers $\mathbb{Z}/n\mathbb{Z}$: Soit $n \in \mathbb{N}$, $f : \mathbb{Z} \longrightarrow A$ un morphisme d'anneaux. Alors : σ se factorise à droite dans f ssi $n\mathbb{Z} \subset \ker f$ ssi $f(n) = 0_A$.

Caractéristique : Soit A un anneau, il existe un unique morphisme dit *canonique* de $\mathbb{Z}$ dans A. Soit f ce morphisme.

- Si $\ker f = \mathbb{Z}$, A est l'anneau nul.
- Si $\ker f = n\mathbb{Z}$, $n \geqslant 2$, on dit que A est de *caractéristique* n.
- Si $\ker f = \{0\}$, A est de caractéristique nulle.

Propriété : Soit A de caractéristique $n \neq 0$; si A est intègre, alors n est premier.

3.3 Arithmétique dans $\mathbb{Z}$ et dans $\mathbb{K}[X]$

- Soient $(p,q) \in \mathbb{Z}^2$; si $d = p \wedge q$, alors $p\mathbb{Z} + q\mathbb{Z} = d\mathbb{Z}$.
- *Identité de Bezout* : $(p \wedge q = 1) \Longleftrightarrow (\exists (a,b) \in \mathbb{Z}^2 / ap + bq = 1)$.
- Soient $(p,q) \in \mathbb{Z}^2$, $M = p \vee q$, alors $p\mathbb{Z} \bigcap q\mathbb{Z} = M\mathbb{Z}$.
- Soit $p, q \in \mathbb{N}^*$, on décompose p et q en produit de facteurs premiers : $p = \prod_{i=1}^{r} p_i^{m_i}$, $q = \prod_{i=1}^{r} p_i^{l_i}$, alors $p \wedge q = \prod_{i=1}^{r} p_i^{\min(m_i,l_i)}$ et $p \vee q = \prod_{i=1}^{r} p_i^{\max(m_i,l_i)}$.
- *Lemme de Gauss* : Soit $m \in \mathbb{Z}$, $(a,b) \in \mathbb{Z}^2$, alors $[(m \mid ab) \wedge (m \wedge a = 1)] \Longrightarrow [m \mid b]$.

Toutes ces propriétés restent vraies dans $\mathbb{K}[X]$, en remplaçant opportunément les entiers par des polynômes.

4 Algèbres

Soit $\mathbb{K}$ un corps (commutatif), une $\mathbb{K}-$ algèbre est un ensemble E muni de trois lois $+, \times, \cdot$ où $+, \times$ sont internes, $\cdot$ est externe $\mathbb{K} \times E \longrightarrow E$ telles que :

1. $(E, +, \cdot)$ est un $\mathbb{K}-$ espace vectoriel.
2. $(E, +, \times)$ est un anneau.
3. $\forall \lambda \in \mathbb{K}, \forall (x,y) \in E^2, \lambda(x \times y) = (\lambda x) \times y = x \times (\lambda y)$.

4.1 Exemples

$\mathbb{K}[X]$, $\mathfrak{M}_n(\mathbb{K})$ sont des $\mathbb{K}-$ algèbres. Si E est un $\mathbb{K}-ev$, $\mathcal{L}(E)$ est une $\mathbb{K}-$ algèbre.

4.2 Définitions

Soit $(E, +, \times, \cdot)$ une $\mathbb{K}-$ algèbre, $F \subset E$ est une *sous-algèbre* de E si :

1. $1_F \in F$
2. F est stable pour $+$ et $\times$
3. Si $\lambda \in \mathbb{K}, x \in F$, alors $\lambda x \in F$.

Morphisme d'algèbres : Soit E, E' deux $\mathbb{K}-$ algèbres, $f : E \longrightarrow E'$ est un morphisme d'algèbres si

1. f est linéaire
2. $\forall (x,y) \in E$, $f(xy) = f(x)f(y)$
3. $f(1_E) = f(1_{E'})$.

f est aussi un morphisme d'anneaux.
Idéal d'algèbre : $I \subset E$ est un idéal si :

1. $0 \in I$
2. I est stable par soustraction
3. I est absorbant pour $\times$

On peut aussi établir que I est un sev absorbant.

4.3 Sous-algèbres de la forme $\mathbb{K}[a]$

Soit E une $\mathbb{K}-$ algèbre, $a \in E$, $P \in \mathbb{K}[X]$; si $p = \sum_{i=0}^{m} \lambda_i X^i$, on pose $P(a) = \sum_{i=0}^{m} \lambda_i X^i$. Alors $\varphi : \begin{array}{ccc} \mathbb{K}[X] & \longrightarrow & E \\ P & \longmapsto & P(a) \end{array}$ est un morphisme d'algèbres. $\mathrm{Im}(\varphi) = \{P(a)/P \in \mathbb{K}[X]\}$ est donc une sous-algèbre de E que nous noterons $\mathbb{K}[a]$. On l'appelle aussi *sous-algèbre de E engendrée par a*. (c'est la plus petite sous-algèbre de E qui contient a). $\mathbb{K}[a]$ est une sous-algèbre commutative.

- Si $\ker(\varphi) = \{0\}$, φ est injective. Alors la famille $(a^i)_{i \in \mathbb{N}}$ est libre dans $\mathbb{K}[a]$, donc $\mathbb{K}[a]$ n'est pas de dimension finie.
- Si $\ker(\varphi) \neq \{0\}$, soit $P \in \ker(\varphi) \backslash \{0\}$ de degré minimal $m \in \mathbb{N}$. Dans ce cas, $\mathbb{K}[a]$ est une sous-algèbre de dimension m. $\mathcal{F} = \{1, a, a^2, \ldots, a^m\}$ est une base de $\mathbb{K}[a]$.

Exemples : $\mathbb{C}$ est une $\mathbb{Q}-$ algèbre. On dit que $a \in \mathbb{C}$ est *transcendant* si $\mathbb{Q}[a]$ n'est pas de dimension finie. Par exemple, e et π sont transcendants. Si en revenche $\mathbb{Q}[a]$ est de dimension finie, on dit que a est *algébrique*. Par exemple $\sqrt{2}$, $\sqrt[2009]{56}$, i sont algébriques.