Chapitre 2 : compléments d'aglèbre

19/9/2011

---

1 Compléments sur les groupes

Définition : Structure de groupe : Soit G un ensemble et $*$ une loi de composition interne sur G.
On dit que $(G, *)$ a une structure de groupe lorsque :

- $*$ est une lci sur G ;
- $*$ est associative ;
- $*$ admet un élément neutre $e \in G$;
- tout élément $x \in G$ doit admettre un symétrique pour $*$ dans G.

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

Caractérisation des sous-groupes : Soit $(G, *)$ un groupen et $H \subset G$.
$(H, *)$ sous-groupe de $(G, *)$ si et seulement si :

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

OU

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

Définition / Théorème : groupe produit : Soit $(G, *)$ et $(G', \bullet)$ deux groupes (resp. commutatifs).
En définissant dans $G \times G'$ la loi $\square$ par :

$$\forall (a, b) \in G \times G',\ \forall (c, d) \in G \times G',\ (a, b) \square (c, d) = (a * c, b \bullet d)$$

alors $(G \times G', \square)$ est un groupe produit (resp. commutatif).

Définition : sous-goupe engendré : Soit $(G, *)$ un groupe et A une partie de G. On appelle sous-groupe engendré par A, noté $Gr(A)$, le plus petit sous-groupe (au sens de l'inclusion) contenant A.

Définition : relation d'équivalence : Soit $\mathscr{R}$ une relation (binaire) définie sur un ensemble E. On dit que $\mathscr{R}$ est une relation d'équivalence si elle est :

- réflexive : $\forall a \in E,\ a \mathscr{R} a$;
- symétrique : $\forall (a, b) \in E^2$, si $a \mathscr{R} b$ alors $b \mathscr{R} a$;
- transitive : $\forall (a, b, c) \in E^3$, si $a \mathscr{R} b$ et $b \mathscr{R} c$, alors $a \mathscr{R} c$.

Définition : classes d'équivalences : Soit $\mathscr{R}$ une relation d'équivalence sur un ensemble E. Soit $x \in E$. La classe d'équivalence de x est définie par :

$$Cl(x) = \{y \in E \mid y \mathscr{R} x\}$$

Propriétés :

- $Cl(x) = Cl(y) \Leftrightarrow [x \mathscr{R} y]$
- $\forall (x, y) \in E^2$ ou bien $Cl(x) = Cl(y)$ ou bien $Cl(x) \cap Cl(y) = \varnothing$
- L'ensemble des classes d'équivalences forme une partition de E, ce qui signifie qu'on obtient un ensemble de parties de E tel que :
  - aucune n'est vide ;
  - deux disctinctes sont nécessairement disjointes ;
  - leur réunion est égale à E.

Définition : relation de congruence modulo n ($n \in \mathbb{N}$) : On définit sur $\mathbb{Z}$ la relation de congruence modulo n par : $\forall (a, b) \in \mathbb{Z}^2 : a \equiv b[n] \Leftrightarrow n|(a - b) \Leftrightarrow \exists k \in \mathbb{Z}/a = b + kn$.

Définition : L'ensemble des classes d'équivalence s'appelle l'ensemble quotient de E par $\mathscr{R}$ et est noté $E/\mathscr{R}$.

Proposition préliminaire : Soit $a, b \in \mathbb{Z}$, soit $n \in \mathbb{N}$. Si $a \equiv a'[n]$ et $b \equiv b'[n]$, alors $a + b \equiv a' + b'[n]$.

Définition : Soient $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$. $\overline{a} \oplus \overline{b} = \overline{a + b}$.

Théorème : $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.

Propriétés :

- $\overline{1}$ est toujours générateur de $\mathbb{Z}/n\mathbb{Z}$.
- $\overline{k}$ est toujours générateur de $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow \overline{1} \in Gr\left(\overline{k}\right) \Leftrightarrow \exists u \in \mathbb{Z}$ tel que $\overline{1} = u\overline{k}$.

Théorème : Soient $n \in \mathbb{N}$ et $k \in \mathbb{Z}$. $\left[\overline{k} \text{ est générateur de } \mathbb{Z}/n\mathbb{Z}\right] \Leftrightarrow [k \wedge n = 1]$.

Lemme fondamental : Les sous-groupes de $\mathbb{Z}$ s'écrivent de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$.

Théorème : Soit $(G, \cdot)$ un groupe de neutre e. Soit $a \in G$. Soit $Gr(a)$ le groupe engendré par a (des puissances de a). Alors :

- ou bien $Gr(a) \simeq \mathbb{Z}$: on dit que a est d'ordre infini.
  - $Card\left(Gr\left(a\right)\right) = \infty$;
  - $a^n = e \Leftrightarrow n = 0$;
  - $Gr(a) = \left\{\ldots, a^{-2}, a^{-1}, e, a^1, a^2, \ldots\right\}$.
- ou bien $Gr(a) \simeq \mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}^\star$: on dit que a est d'ordre n.
  - $Card\left(Gr\left(a\right)\right) = n$;
  - $n = Min\left(\left\{k \in \mathbb{N}^\star / a^k = 0\right\}\right)$;
  - $Gr(a) = \left\{e, a^1, a^2, \ldots, a^{n-1}\right\}$.

Groupes monogène, cyclique : Un groupe G est dit :

- monogène s'il existe $a \in G$ tel que $G = Gr(a)$;
- cyclique s'il est monogène et fini.

2 Compléments sur les anneaux

Définition : anneau : Soit A un ensemble et $\oplus$ et $*$ deux lois de composition interne sur A. On dit que $(A, \oplus, *)$ a une structure d'anneau lorsque :

- $(A, \oplus)$ est un groupe commutatif ;
- $*$ est associative ;
- $*$ admet un élément neutre ;
- $*$ est distributive par rapport à $\oplus$: $\forall x, y, z \in A,\ x * (y \oplus z) = (x * y) \oplus (x * z)$ et $(y \oplus z) * x = (y * x) \oplus (z * x)$.

Si de plus $*$ est commutative, on dit que $(A, \oplus, *)$ est un anneau commutatif.

Proposition : caractérisation des sous-anneaux : Soit $(A, +, \cdot)$ un anneau et $A' \subset A$. $(A', +, \cdot)$ sous-anneau de $(A, +, \cdot)$ si et seulement si :

- $1_A \in A'$;
- $\forall a, b \in A'$,
  1. $a + (-b) \in A'$;
  2. $a \cdot b \in A'$.

Morphisme d'anneau : Soit $(A, +, \cdot)$ et $(A', \oplus, \otimes)$ deux anneaux. Soit $f : A \to A'$ une application. On dit que f est un morphisme de l'anneau $(A, +, \cdot)$ dans l'anneau $(A', \oplus, \otimes)$ lorsque :

- $f(1_A) = 1_{A'}$;
- $\forall a, b \in A$,
  1. $f(a + b) = f(a) \oplus f(b)$;
  2. $f(a \cdot b) = f(a) \otimes f(b)$.

Théorème : Soit $(A, +, \times)$ un anneau.
Soit $A^\star$ l'ensemble des éléments inversibles i.e. « x inversible »$\Leftrightarrow \exists x' \in A$ tel que $x \times x' = 1_A = x' \times x$, alors $(A^\star, \times)$ est un groupe appelé groupe des inversibles.

Définition : idéal d'un anneau commutatif : Soit $(A, +, \times)$ un anneau commutatif.
Soit $\mathcal{I}$ une partie de A. On dit que $\mathcal{I}$ est idéal de A si :

- $(\mathcal{I}, +)$ est un sous-groupe de $(A, +)$;
- « sur-stabilité » : $\forall a \in A,\ \forall x \in I,\ a \times x \in I$.

Propriété : $[\mathcal{I} = A] \Leftrightarrow [1_A \in \mathcal{I}]$.

Définition : notion de divisibilité : Soit $(A, +, \times)$ un anneau commutatif. Soient $a, b \in A$. On dit que b divise a ou que a est un multiple de b que l'on écrit $b|a$ lorsque : $\exists k \in A$ tel que $a = b \times k$ ou encore $a \in bA$.

Propriété : Soient a et b deux éléments d'un anneau A. $b|a \Leftrightarrow aA \subset bA$.

Propriété : noyau d'un morphisme d'anneau : Soit Φ un morphisme d'anneau de A vers A'. Soit $Ker\ \Phi = \{x \in A\ /\ \Phi(x) = 0_{A'}\}$. Alors $Ker\ \Phi$ est un idéal de l'anneau A.

Proposition : intersection et somme de deux idéaux : Soient $\mathcal{I}$ et $\mathcal{J}$ deux idéaux d'un anneau A. Alors :

- $\mathcal{I} \cap \mathcal{J}$ est un idéal de A. C'est le plus grand idéal (au sens de l'inclusion) inclus dans $\mathcal{I}$ et dans $\mathcal{J}$.
- $\mathcal{I} + \mathcal{J} = \{a + b \ / \ a \in \mathcal{I}, b \in \mathcal{J}\}$ est un idéal de A, c'est le plus petit idéal (au sens de l'inclusion) contenant à la fois $\mathcal{I}$ et $\mathcal{J}$ et doonc $\mathcal{I} \cup \mathcal{J}$.

Application 1 : arithmétique dans $\mathbb{Z}$:

PPCM : $m = PPCM(a,b) = a \vee b$ si et seulement si $\left| \begin{array}{l} m \in \mathbb{N} \\ m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z} \end{array} \right.$

PGCD : $d = PGCD(a,b) = a \wedge b$ si et seulement si $\left| \begin{array}{l} d \in \mathbb{N} \\ d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \end{array} \right.$

Application 2 : arithmétique dans $\mathbb{K}[X]$:

Théorème de base : Les seuls idéaux de $\mathbb{K}[X]$ s'écrivent, avec $P \in \mathbb{K}[X]$:

$$P \cdot \mathbb{K}[X] = \{P \times A \ / \ A \in \mathbb{K}[X]\} = (P)$$

PPCM :

- si $A = 0$ ou $B = 0$, le PPCM de A et B est 0 ;
- sinon, $M = A \vee B$ est l'unique polynôme unitaire tel que $(A) \cap (B) = (M)$.

Ceci traduit que $\forall P \in \mathbb{K}[X]$, $\left\{ \begin{array}{l} A|P \\ B|P \end{array} \right. \Leftrightarrow (A \vee B)|P$.

PGCD :

- si $A = 0$ et $B = 0$, le PGCD de A et B est 0 ;
- sinon, $D = A \wedge B$ est l'unique polynôme unitaire tel que $(A) + (B) = (D)$.

Ceci traduit que $\forall \Delta \in \mathbb{K}[X]$, $\left\{ \begin{array}{l} \Delta|A \\ \Delta|B \end{array} \right. \Leftrightarrow \Delta|(A \vee B)$.

Compatibilité de la loi $\times$ avec la relation de congruence :

Propriété : Soit $n \in \mathbb{N}$, $\forall (a,b,c,d) \in \mathbb{Z}^4$. Si $a \equiv b[n]$ et $c \equiv d[n]$, alors $a \times c \equiv b \times d[n]$.

Corolaire : Soit $n \in \mathbb{N}$. Soient $(a,b) \in \mathbb{Z}^2$ et $k \in \mathbb{Z}$. Si $a \equiv b[n]$, alors $a^k \equiv b^k[n]$.

Conséquence : On n'a donc aucun problème à définir dans $\mathbb{Z}/n\mathbb{Z}$ $\overline{a} \otimes \overline{b} = \overline{a \times b}$.

Autre propriété intéressante : $\left[\begin{array}{l} a \equiv b[m] \\ a \equiv b[n] \\ m \wedge n = 1 \end{array} \right] \Rightarrow \left[a \equiv b\,[mn] \right]$

Théorème : éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ pour $\times$:

$$\left[\overline{k} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z} \text{ pour } \times \right] \Leftrightarrow [k \wedge n = 1]$$

Théorème : l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$: $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

- Il est intègre si $n \in \mathbb{P} \cup \{0\}$.
- C'est un corps si $n \in \mathbb{P}$.

Définition : la fonction indicatrice d'Euler : On appelle fonction indicatrice d'Euler la fonction $\Phi : \mathbb{N} \to \mathbb{N}$ définie par : $\forall n \in \mathbb{N}$, $\Phi(n) = Card\left((\mathbb{Z}/n\mathbb{Z})^\star\right)$.

Théorème : théorème de factorisation : Soit Ψ un morphsime d'anneau de $\mathbb{Z}$ sur A. Soit $Ker\ \Psi = n\mathbb{Z}$ (puisque c'est un sous-groupe de $(\mathbb{Z},+)$ / un idéal de $(\mathbb{Z},+,\times)$). Soit $S : \begin{cases} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \\ k \mapsto \overline{k} \end{cases}$. Alors il existe un morphisme $\widetilde{\Psi}$ tel que $\widetilde{\Psi} : \mathbb{Z}/n\mathbb{Z} \to A$ et $\Psi = \widetilde{\Psi} \circ S$.

Application 1 : caractéristique d'un corps :

Définition : caractéristique d'un corps : La caractéristique d'un corps K est :

- égale à 0 si $\forall m \in \mathbb{Z},\ m \cdot 1_K \Leftrightarrow m = 0$;
- égale à $Min\left\{m \in \mathbb{N}^\star | m \cdot 1_K = 0_K\right\}$ sinon.

C'est aussi le nombre q tel que $Ker\ \Psi = q\mathbb{Z}$ pour $\Psi : \begin{cases} \mathbb{Z} \to K \\ m \mapsto m \cdot 1_K \end{cases}$.

Propriétés :

1. Si K est un corps de caractéristique q, $\forall n \in \mathbb{Z},\ m \cdot 1_K = 0_K \Leftrightarrow m \in q\mathbb{Z},\ m \in Ker\ \Psi$;
2. Si $q \neq 0$, $q \in \mathbb{P}$.

Application 2 : théorème chinois : Soient $m, n \in \mathbb{N}$ tels que $m \wedge n = 1$, $(a,b) \in \mathbb{Z}^2$. Le système d'équation $\begin{cases} x \equiv a[m] \\ x \equiv b[n] \end{cases}$ où x est une inconnue entière admet au moins une solution x_0. L'ensemble des solutions est alors $\mathcal{S} = x_0 + (mn)\mathbb{Z}$.