Groupes, anneaux, modules et algèbre tensorielle sur un corps

---

Notes extraites du cours de Mr Philippe Caldero

Contributeur(s)
Mr Payet Thibault Benjamin

Sommaire

1

Groupes libres et présentations

Notion clef du M1 d'algèbre :*le quotient*, le passage au quotient , les applications *bien définies*.
$\boxed{\text{Contre-exemple}}$: On considère

$$u : \mathbb{R}^2 \to \mathbb{R}^3, xe + yf + zg \mapsto (x, y, z)$$

Avec :

$$e = (1, 0)\ f = (0, 1)\ g = (1, 1)\ x, y, z \in \mathbb{R}$$

Ce n'est pas *bien défini*, en effet on peut assoscier à $(0, 0)$ le vecteur $(0, 0, 0)$ mais aussi le vecteur $(-1, -1, 1)$. Dans un e.v de dimension finie, on sait qu'il existe des bases.

Théorème 1.0.1 *Soit $\mathscr{B} = (e_i)_{1\leq i\leq n}$ une base d'un e.v E. Soit F un e.v et $f_1, \cdots, f_n$ des vecteurs de F.*
Alors $\exists!\varphi \in \mathscr{L}(E, F)$ tel que $\varphi(e_i) = f_i, \forall i \in [\![1, n]\!]$

Remarque Dans l'exemple précédant, l'application $\varphi \in \mathscr{L}(\mathbb{R}^2, \mathbb{R}^3)$ tel que

$$\varphi(e) = (1, 0, 0)\ , \varphi(f) = (0, 1, 0)\ , \varphi(g) = (0, 0, 1)$$

n'existe pas car (e, f, g) n'est pas une base. Pour les groupes, il n'y a en général pas de bases.
$\boxed{\text{But de la leçon}}$ Remplacer le théorème sur les bases par un théorème adapté. Introduire les groupes libres (un groupe où il existe une famille libre et génératrice).

1.1 Introduction aux groupes libres. Le groupe $\mathbb{Z}$

$(\mathbb{Z}, +)$ est un groupe

Proposition 1.1.1 *Soit G un groupe quelconque et g dans G. Alors il existe un unique morphisme de groupes de $\mathbb{Z}$ dans G qui envoie 1 sur g*

Idée : 1 joue le rôle d'une base.

Preuve Soit $\varphi : (\mathbb{Z}, +) \to (G, \cdot), 1 \mapsto g$
$\boxed{\text{Analyse}}$ $1 + 1 = 2 \mapsto g \cdot g = g^2$ car $\varphi(1 + 1) = \varphi(1) \cdot \varphi(1)$.
De même $n \mapsto g^n, \forall n > 0$ et $0 \mapsto e$ car l'image d'un neutre pour un morphisme est un neutre.
$-1 \mapsto g^{-1}$ car l'image de l'inverse est l'inverse de l'image , $-n \mapsto g^{-n}, \forall n > 0$.
$\boxed{\text{Synthèse}}$ On pose $\varphi(n) = g^n, \forall n \in \mathbb{Z}$, on a bien $\varphi(1) = g$, $\varphi(n+m) = g^{n+m} = g^n \cdot g^m = \varphi(n)\cdot\varphi(m)$.
Donc φ existe et son unicité provient de la partie "analyse".

Définition Le groupe G est dit monogène s'il est engendré par un seul générateur g.
i.e $G = \{g^n, n \in \mathbb{Z}\}$

Remarque Dans ce cas, on peut trouver un unique morphisme φ tel que $\varphi(1) = g, \varphi : \mathbb{Z} \to G$, ce morphisme est alors surjectif.

Preuve $\varphi(1) = g$ donc $\varphi(n) = g^n, \forall n \in \mathbb{Z}$ soit $h \in G$, par définition on a $h = g^n$ pour un $n \in \mathbb{Z}$. Donc $\varphi(n) = h$. On a donc φ surjectif

Le morphisme φ est-il injectif ? $\ker\varphi$ permet de répondre. $\ker\varphi \underset{\text{ss-grp}}{\subset} \mathbb{Z}$ donc $\ker\varphi = n\mathbb{Z}$.

Proposition 1.1.2 *Soit G un groupe monogène, alors soit :*

(i) $G \simeq \mathbb{Z}$

(ii) $G \simeq \mathbb{Z}/n\mathbb{Z}, n > 0$

Définition Dans le second cas, le groupe est dit cyclique

Preuve On a vu que $\varphi : \mathbb{Z} \to G$ est surjective
Si $\ker\varphi = 0$ alors φ est injective ,φ est un isomorphisme et on est dans le cas *(i)*.
Si $\ker\varphi \neq 0$ alors $\ker\varphi = n\mathbb{Z}$
$\boxed{\text{Passage au quotient}}$
$\boxed{\text{Principe 1}}$ Si $\varphi : G \to H$ est un morphisme, alors il définit un "isomorphisme canonique"

$$G/\ker\varphi \simeq \operatorname{Im}\varphi$$

On obtient le diagramme commutatif suivant :

Table des matières