Modules : quelques définitions (J-Y D)

Définition

(a) Une *loi de composition* sur un ensemble E est une application $\star\colon E \times E \to E$.
Suivant l'usage, on notera $x \star y$ l'image par $\star$ de (x, y).

(b) Un *groupe* est un couple $(G, \star)$ où G est un ensemble, $\star$ est une loi de composition sur G, et
(i) pour tous $x, y, z \in G$, on a : $(x \star y) \star z = x \star (y \star z)$ « associativité » ;
(ii) il existe $e \in G$ tel que pour tout $x \in G$, on a : $e \star x = x \star e = x$ « élément neutre » ;
(iii) pour tout $x \in G$ il existe $x' \in G$ tel que : $x \star x' = x' \star x = e$ « inverse ».

Dans ce cas, l'élément e du (ii) est unique appelé *élément neutre de* G, et pour chaque $x \in G$ l'élément x' de G du (iii) est unique appelé *inverse de* x et noté x^{-1}.

(c) On dit qu'un groupe $(G, +)$ est *commutatif* si pour tous $x, y \in G$, on a : $x + y = y + x$.
Dans ce cas on peut noter 0_G l'élément neutre de G et $-x$ l'inverse (appelé *opposé*) d'un $x \in G$.

(d) Un *sous-groupe* d'un groupe $(G, \star)$ comme au (b) est une partie H de G vérifiant
(i) $e \in H$;
(ii) pour tous $x, y \in H$, on a : $x \star y^{-1} \in H$.
Dans ce cas, H muni de la restriction de $\star$ à $H \times H$ est un groupe.

Définition-Proposition

Soient $(G, \star)$ et $(G', \star')$ des groupes.

(a) Un *sous-groupe distingué de* $(G, \star)$ est un sous-groupe H de $(G, \star)$ vérifiant :
$$x \star y \star x^{-1} \in H \text{ pour tous } x \in G \text{ et } y \in H.$$
(Cette condition est automatiquement vérifiée quand G est commutatif.)

Dans ce cas, en notant $\dot{x} := \{x \star y \ ; \ y \in H\}$ pour tout $x \in G$ et $G/H := \{\dot{x} \ ; \ x \in G\}$, on munit G/H d'une structure de groupe avec la loi de composition — encore notée $\star$ — définie par : $u \star v := \widehat{x \star y}$ pour $u, v \in G/H$ indépendamment du choix de $x, y \in G$ tels que $u = \dot{x}$ et $v = \dot{y}$.

(b) Un *morphisme* de groupes de $(G, \star)$ dans $(G', \star')$ est une application $f\colon G \to G'$ vérifiant : $f(x \star y) = f(x) \star' f(y)$ pour tous $x, y \in G$.

Dans ce cas, on a : $f(e_G) = e_{G'}$ en notant e_G et $e_{G'}$ les éléments neutres de G et G', $\operatorname{Ker} f := \{x \in G \mid f(x) = e_{G'}\}$ est un sous-groupe distingué de $(G, \star)$, $\operatorname{Im} f$ est un sous-groupe de G', et l'application $\tilde{f}\colon \begin{array}{ccc} G/\operatorname{Ker} f & \longrightarrow & \operatorname{Im} f \\ u = \dot{x} & \longmapsto & \underbrace{f(x)}_{\text{ne dépend pas du choix de } x} \end{array}$ est un morphisme de groupes qui est bijectif.

Définition

(a) Un *anneau* est un triplet $(A, +, \times)$, où $(A, +)$ est un groupe commutatif et $\times$ est une loi de composition sur A, vérifiant
(i) $(x \times y) \times z = x \times (y \times z)$ pour tous $x, y, z \in A$;
(ii) $x \times (y + z) = (x \times y) + (x \times z)$ et $(x + y) \times z = (x \times z) + (y \times z)$ pour $x, y, z \in A$;
(iii) il existe $1 \in A$ tel que pour tout $x \in A$, on a : $1 \times x = x \times 1 = x$.

Dans ce cas, l'élément 1 du (iii) est unique et appelé *élément unité de* A.

En outre, on appelle *caractéristique de* A l'entier 0 si $n1_A \neq 0$ pour tout $n \in \mathbb{N} \setminus \{0\}$, ou le plus petit entier $n \in \mathbb{N} \setminus \{0\}$ tel que $n1_A = 0$ sinon.

(b) On dit qu'un anneau $(A, +, \times)$ est *commutatif* si pour tous $x, y \in A$, on a : $x \times y = y \times x$.

(c) Un *sous-anneau* d'un anneau $(A, +, \times)$ comme au (a) est un sous-groupe B de $(A, +)$ vérifiant
(i) $1 \in B$;
(ii) pour tous $x, y \in B$, on a : $x \times y \in B$.

Définition-Proposition

Soient $(A,+,\times)$ et $(A',+',\times')$ des anneaux. On note 1_A et $1_{A'}$ leur élément unité.

(a) Un *idéal bilatère* de $(A,+,\times)$ est un sous-groupe $\mathscr{I}$ de $(A,+)$ vérifiant :

$$x\times y \in \mathscr{I} \ \text{ et } \ y\times x \in \mathscr{I} \ \text{ pour tous } x\in A \text{ et } y\in\mathscr{I}.$$

Dans ce cas, le groupe $(A/\mathscr{I},+)$ a une structure d'anneau avec la loi $\times$ suivante :
$u\times v := \widehat{\dot{x}\times\dot{y}}$ pour $u,v\in A/\mathscr{I}$ indépendamment du choix de $x,y\in A$ tels que $u=\dot{x}$ et $v=\dot{y}$.

(b) Un *morphisme* d'anneaux de $(A,+,\times)$ dans $(A',+',\times')$ est un morphisme de groupes f de $(A,+)$ dans $(A',+')$ vérifiant : $f(1_A)=1_{A'}$ et $f(x\times y)=f(x)\times' f(y)$ pour tous $x,y\in A$.

Dans ce cas, on a : $\operatorname{Ker} f$ est un idéal bilatère de $(A,+,\times)$, $\operatorname{Im} f$ muni de $+'$ et $\times'$ est un anneau, et la bijection canonique $\tilde{f}\colon A/\operatorname{Ker} f \to \operatorname{Im} f$ pour l'addition est un morphisme d'anneaux.

Définition-Proposition

Soit $(A,+,\times)$ un anneau. On note 1 son élément unité.

(a) Soit $a\in A$. On dit que a est inversible s'il existe $a'\in A$ tel que $a\times a' = a'\times a = 1$.
Dans ce cas a' est unique et noté a^{-1}.

(b) On note $A^\times$ (parfois aussi A^*) l'ensemble des éléments inversibles de A.
L'ensemble $A^\times$ muni de $\times$ est un groupe d'élément neutre 1.

(c) Un *corps* est un anneau $(K,+,\times)$ qui vérifie :

$$\underbrace{K\neq\{0\} \text{ et tout élément non-nul de } K \text{ est inversible.}}_{\text{c'est-à-dire } K^\times = K\setminus\{0\}}$$

Définition

Soit $(A,+,\times)$ un anneau. On note 1 son élément unité.

(a) Un *A-module à gauche* est un groupe commutatif $(M,+)$ muni de $\begin{matrix}A\times M\to M\\(\alpha,v)\mapsto \alpha\,v\end{matrix}$ telle que :

(i) $\alpha\,(v+w)=(\alpha\,v)+(\alpha\,w)$ et $(\alpha+\beta)\,v=(\alpha\,v)+(\beta\,v)$ pour $\alpha,\beta\in A$ et $v,w\in M$;
(ii) $1\,v=v$ et $\alpha\,(\beta\,v)=(\alpha\beta)\,v$ pour tous $\alpha,\beta\in A$ et $v\in M$.

(b) Les groupes abéliens $(G,+)$ s'identifient aux $\mathbb{Z}$-modules pour les lois $\overbrace{(n,v)}^{\in\mathbb{Z}\times G}\mapsto \overbrace{v+\cdots+v}^{n \text{ termes}}$.

(c) Un *A-module à droite* est un groupe commutatif $(M,+)$ muni de $\begin{matrix}M\times A\to M\\(v,\alpha)\mapsto v\,\alpha\end{matrix}$ telle que :

(i) $(v+w)\,\alpha=(v\,\alpha)+(w\,\alpha)$ et $v\,(\alpha+\beta)\ =(v\,\alpha)+(v\,\beta)$ pour $\alpha,\beta\in A$ et $v,w\in M$;
(ii) $v\,1=v$ et $(v\,\alpha)\,\beta=v\,(\alpha\beta)$ pour tous $\alpha,\beta\in A$ et $v\in M$.

Il s'identifie donc à un A^{opp}-module à gauche, où A^{opp} est $\underbrace{\textit{l'anneau opposé de } (A,+,\times)}_{(A,+,\times) \text{ quand } A \text{ est commutatif}}$, c'est-à-dire l'ensemble A muni les lois $(\alpha,\beta)\mapsto\alpha+\beta$ et $(\alpha,\beta)\mapsto\beta\times\alpha$.

Définition-Proposition

Soient A un anneau, et M et M' des A-modules (sous-entendu à gauche).

(a) Un *sous-module de M* est une partie N de M vérifiant :
(i) $0_M\in N$;
(ii) pour tous $\alpha,\beta\in A$ et $v,w\in N$, on a $\alpha\,v+\beta\,w\in N$.

Dans ce cas, le groupe $(M/N,+)$ a une structure de A-module avec la loi suivante :
$\alpha u := \widehat{\alpha\dot{v}}$ pour $\alpha\in A$ et $u\in M/N$ indépendamment du choix de $v\in M$ tels que $u=\dot{v}$.

(b) Un *idéal à gauche de A* est un sous-module du A-module à gauche A pour le produit.

(c) Un *application A-linéaire* de M dans M' est une application $f\colon M\to M'$ vérifiant : $f(\alpha\,v+\beta\,w)=\alpha\,f(v)+\beta\,f(w)$ pour tous $\alpha,\beta\in A$ et $v,w\in M$.

Dans ce cas, on a : $\operatorname{Ker} f$ est un sous-module M, $\operatorname{Im} f$ est un sous-module de M', et la bijection canonique $\tilde{f}\colon A/\operatorname{Ker} f\to\operatorname{Im} f$ pour l'addition est un morphisme de A-modules.