IV . −Produits, sommes directes,, quotients, suites exactes, propriétés universelles

IV.1 . −Produits

La construction du *produit* est d'abord une construction ensembliste comme expliqué en IV.1.1. À ce stade déjà le produit possède une *propriété universelle* IV.1.1.iii) qui ne peut être formulée sans le secours des projections introduites en IV.1.1.ii). Ces dernières sont, en définitives partie prenantes du produit qui n'est en réalité pas constitué du seul ensemble produit mais aussi des projections. Ce sont, comme on va le voir, les idées qui guident la construction du produit, lorsque les ensembles impliqués acquièrent davantage de structure notamment algébrique. La « bonne structure » sur le produit cartésien sera celle qui aura tendance à préserver une propriété universelle analogue pour la structure algébrique considérée. De tels énoncés ne pourront être raisonnablement formulés que si les projections deviennent des morphismes pour la structure considérée. Dès lors on s'apercevra que, pour les structures algébriques considérées au moins (groupes abéliens, anneaux, modules algèbres) cette seule exigence sur les projections suffisent à déterminer uniquement la structure sur le produit.

Proposition IV.1.1 *Soient $n \in \mathbb{N}^*$, et E_k $_{,1 \leq k \leq n}$, des ensembles.*

i) On définit par récurrence le produit cartésien *des ensembles E_k $_{,1 \leq k \leq n}$ par*

$$\prod_{k=1}^{n+1} E_k := \prod_{k=1}^{n} E_k \times E_{n+1} .$$

ii) On définit également des projections

$$p_k : P := \prod_{i=1}^{n+1} E_k \to E_k \; _{,1 \leq k \leq n+1}$$

en supposant construites p_k $_{,1 \leq k \leq n}$, on définit p_{n+1} par

$$p_{n+1} : \Big(\prod_{k=1}^{n} E_k\Big) \times E_{n+1} \to (x, y) \, , \, y \mapsto \, .$$

Ce qu'on peut écrire

$$p_k(x_1, \ldots, x_n) = x_k .$$

iii) Pour tout ensemble F et tout n-uplet d'applications $f_k : F \to E_k$ $_{,1 \leq k \leq n}$, il existe une unique application

$$f : F \to P := \prod_{k=1}^{n} E_k \text{ telle que } \forall 1 \leq k \leq n, \; f_k = p_k \circ f .$$

iv) Dans le cas où il existe un ensemble E tel que $\forall 1 \leq k \leq n, \; E_k = E$, on rappelle que $E^{[1;n]}$ désigne l'ensemble des applications de $[1; n]$ à valeurs dans E. Pour tout $1 \leq k \leq n$, on définit

$$q_k : E^{[1;n]} \to E \, , \, f \mapsto f(k) .$$

En vertu de iii), il existe une unique application

$$\phi : E^{[1;n]} \to \prod_{k=1}^{n} E \text{ telle que } \forall 1 \leq k \leq n, \; q_k = p_k \circ \phi .$$

L'application ϕ est alors une bijection ;

***Preuve** : Pour tout $y \in \prod_{k=1}^{n} E$, l'application $f : [1; n] \to E$ définie par*

$$\forall 1 \leq k \leq n,\ f(k) := p_k(y)$$

vérifie évidemment $\phi(f) = y$ ce qui assure que ϕ est surjective ;

Pour tout $(f, g) \in E^{[1;n]} \times E^{[1;n]}$, $\phi(f) = \phi(g)$ entraîne que pour tout $1 \leq k \leq n$, $p_k[\phi(f)] = p_k[\phi(g)]$ c'est-à-dire $q_k(f) = q_k(g)$ ou encore $f(k) = g(k)$ ce qui entraîne $f = g$, et assure donc finalement que ϕ est injective.

Remarque IV.1.2 Les constructions précédentes (cf. IV.1.1,) ne permettent cependant pas de définir des produits infinis auxquels d'ailleurs nous auront assez peu affaire dans ce cours. Cependant si $\mathcal{E}$ est un ensemble (d'ensembles) on not $U := \bigcup_{E \in \mathcal{E}} E$. Notons alors

$$P := \{f \in U^{\mathcal{E}} ;\ \forall E \in \mathcal{E},\ f(E) \in E\} \subset U^{\mathcal{E}}$$

le sous-ensemble des applications de $\mathcal{E}$ à valeurs dans U telles que l'image de tout ensemble E appartient à E. On appelle P *produit* des éléments de $\mathcal{E}$ et l'on note

$$P = \prod_{E \in \mathcal{E}} E\,.$$

La plupart du temps on considère une « famille » d'ensembles indexée par un ensemble (arbitraire et en particulier pas nécessairement fini) I. Ceci revient à se donner en fait une bijection $I \to \mathcal{E}\,,\ i \mapsto E_i$. Les éléments de P donnent alors (de manière bijective) par composition avec cette dernière des applications $I \to U$ tells que pour tout $i \in I$, $f(i) \in E_i$; ce qu'on note $f_i \in E_i$ usuellement. On parle de « famille $f_{i\ ,i \in I}$ » qui ne sont en définitive que des application $I \to U$, ayant une bonne propriété. Cette définition assure, qu'aux termes de l'axiomatique **ZFC**, P est bien un ensemble.

Les projections sont alors définie par

$$p_E : P \to E\,,\ f \mapsto t(E)\,.$$

On laisse alors le lecteur vérifier que dans le cas où $\mathcal{E}$ est fini, la définition du produit et des projections données ici coïncident bien avec celles données en IV.1.1.iv) et IV.1.1.ii).

On laisse le lecteurs vérifier également que l'objet P ainsi construit vérifie bien la propriété universelle IV.1.1.iii).

Notation IV.1.3 Dans tout le paragraphe IV.1, on garde les notations de la proposition IV.1.1, à savoir que, $n \in \mathbb{N}^*$ est un entier, $E_{k\ ,1 \leq k \leq n}$ des ensembles dont on note

$$P := \prod_{k=1}^{n} E_k$$

le produit cartésien *i.e.*

$$P = \left\{(x_1, \ldots, x_n) \forall 1 \leq k \leq n,\ x_k \in E_k\right\}.$$

On note enfin

$$\forall 1 \leq k \leq n,\ p_k : P \to E_k\,,\ (x_1, \ldots, x_n) \mapsto x_k$$

la *projection sur le k^ième facteur*.

Pour tout $1 \leq k \leq n$, on considérera les cas où E_k est muni de l'une des structures algébriques suivantes (en sachant que la structure de magma n'est pas étudiée en soit mais comme ingrédient pour la construction des autres structures algébriques) :

0) (**magma**)
$(E_k, \dagger_k)$ est un *magma associatif* (cf. 0.2 ;)

i) (**groupe**)
$(E_k, *_k)$ est un *groupe* (éventuellement abélien) (cf. 0.13) d'élément neutre ε_k ;

ii) (**anneau**)
$(E_k, +_k, *_k, 0_k, 1_k)$ est un anneau (éventuellement commutatif) (cf. 0.14 ;)

iii) (**$\mathbb{K}$-espace vectoriel**)
$(E_k, +_k, \cdot_k)$ est un $\mathbb{K}$-espace vectoriel (cf. 0.18,) pour $\mathbb{K}$ un corps (cf. 0.17 ;)

iv) (**A-module**)
$(E_k, +_k, \cdot_k)$ est un A-module pour A un anneau fixé, (cf. III.1.1 ;)

v) (**A-algèbre**)
$(E_k, +_k, *_k, s_k \ : \ A \ \to \ E_k)$ est une A-algèbre (cf. III.1.6.)

Proposition IV.1.4 (Existence de produits) *Si pour tout $1 \leq k \leq n$, E_k est muni de l'une des structures algébrique IV.1.3.0) à IV.1.3.v) il existe une unique structure de même nature sur le produit P et telle que*

$$\forall 1 \leq k \leq n, \ p_k \ : \ P \ \to \ E_k \text{ est un morphisme}$$

pour la structure correspondante sur les $E_{k\ ,1 \leq k \leq n}$, (i.e. un morphisme de magmas (cf. 0.8,) (resp. de groupes (cf. 0.20,)) (resp. d'anneaux (cf. 0.21,)) (resp. de $\mathbb{K}$-espaces vectoriels i.e. une application linéaire (cf. 0.18,)) (resp. de A-modules (cf. III.2.1,)) (resp. de A-algèbres (cf. III.2.2.)))

Si $\forall 1 \leq k \leq n,$ on a une loi interne $\dagger_k$ sur E_k, la loit interne correspondante sur $\prod_{k=1}^{n} E_k$ est donnée par :

$$\begin{gathered} \forall\big((x_1, \ldots, x_n), (y_1, \ldots, x_n)\big) \in P \times P, \\ (x_1, \ldots, x_n) \ \dagger \ (y_1, \ldots, y_n) \ = \ (x_1 \dagger_1 y_1, \ldots, x_n \dagger_n y_n) \ ; \end{gathered} \qquad \text{IV.1.4.1}$$

si $\forall 1 \leq k \leq n, \ \varepsilon_k$ est un élément neutre pour $\dagger_k$, alors

$$(\varepsilon_1, \ldots, \varepsilon_n) \text{ est un l'élément neutre pour } \dagger \ ; \qquad \text{IV.1.4.2}$$

si

$$\forall 1 \leq k \leq n, \ \forall x_k \in E_k,$$

y_k est le symétrique de x_k pour $\dagger_k$,

$$(y_1, \ldots, y_n) \text{ est le symétrique de } (x_1, \ldots, x_n) \text{ pour } \dagger \ ; \qquad \text{IV.1.4.3}$$

si $\forall 1 \leq k \leq n,$ on a une loi externe $\cdot_k \ : \ A \times E_k \ \to \ E_k$, la loi externe correspondante sur $\prod_{k=1}^{n} E_k$ est donnée par :

$$\begin{gathered} \forall (x_1, \ldots, x_n) \in P, \ \forall a \in a, \ A \\ a \cdot (x_1, \ldots, x_n) \ = \ (a \cdot_1 x_1, \ldots, a \cdot_n x_n) \ . \end{gathered} \qquad \text{IV.1.4.4}$$

***Preuve** :*

0) ***(Le cas des magmas)***
Si

$$\forall 1 \leq k \leq n,\ p_k \ :\ \big(P, \dagger\big) \ \rightarrow\ (E_k, \dagger_k)$$

est un morphisme, alors :

$$\begin{array}{llcl} \forall (x_1, \ldots, x_n) \in P, & & & \\ \forall (y_1, \ldots, x_n) \in P, & p_k\big((x_1, \ldots, x_n) \dagger (y_1, \ldots, y_n)\big) & = & p_k\big((x_1, \ldots, x_n)\big) \dagger_k p_k\big((y_1, \ldots, y_n)\big) \\ & & = & x_k \dagger_k y_k\ , \end{array}$$

ce qui assure, d'une part l'unicité de la loi $\dagger$ et, d'autre part, au cas où elle existe, qu'elle est définie par la formule IV.1.4.1. Reste à vérifier, ce qui est très élémentaire, qu'ainsi définie, elle convient bien et a les propriétés requises.

i) ***(Le cas des groupes)***
Un groupe étant en particulier un magma associatif le point 0) assure que si

$$\forall 1 \leq k \leq n,\ (E_k, *_k) \text{ est un groupe d'élément neutre } \varepsilon_k,$$

il existe une unique loi $*$ sur P telle que

$$\forall 1 \leq k \leq n,\ \forall (x, y) \in P \times P,\ p_k(x * y) \ =\ p_k(x) *_k p_k(y)$$

i.e. les p_k sont des morphismes de groupe en particulier. Il suffit alors, ce qui est très élémentaire, de vérifier que les formules IV.1.4.2 et IV.1.4.3 sont satisfaites.

ii) ***(Le cas des anneaux)***
Si

$$\forall 1 \leq k \leq n,\ (E_k, +_k, *_k, 0_k, 1_k) \text{ est un anneau,}$$

$(E_k, +_k, 0_k)$ est un groupe abélien et le point i) assure donc qu'il existe une unique structure de groupes $+$ sur P telle que

$$\forall 1 \leq k \leq n,\ p_k \ :\ P \ \rightarrow\ E_k \text{ est un morphisme de groupes }.$$

Il est en outre immédiat de vérifier, en utilisant par exemple l'expression IV.1.4.1 de $+$ que cette dernière est commutative.

En appliquant le point 0) aux $(E_k, *_k)$ on conclut à l'existence et à l'unicité d'une loi $*$ sur P faisant de P un anneau et des $p_{k\ ,1\ \leq\ k\ \leq\ n}$ des morphismes d'anneaux.

iii) ***($\mathbb{K}$-espaces vectoriels (resp. A-modules))***
Si

$$\forall 1 \leq k \leq n,\ (E_k, +_k, \cdot_k) \text{ est un } \mathbb{K}\text{-espace vectoriel (resp . } A\text{-module pour un anneau } A \text{ fixé ,)}$$

$(E_k, +_k)$ est en particulier un groupe abélien et P hérite dès lors d'une structure de groupe en vertu du point i) telle que les $p_{k\ ,1\ \leq\ k\ \leq\ n}$ soient des morphismes de groupes. Reste alors à vérifier la formule IV.1.4.4 ce qui est sans difficulté.

*iv) (A-**algèbres**)*
Si

$$\forall 1 \leq k \leq n, \ , (E_k, +_k, *_k, s_k \ : \ A \ \rightarrow \ E_k) \text{ est une } A\text{-algèbre pour un anneau } A \text{ fixé,}$$

en particulier $(E_k, +_k, *_k)$ est un anneau et le point ii) assure qu'il existe une unique structure d'anneau $(+, *)$ sur P telle que les $p_k \ ,_{1 \leq k \leq n}$ soient des morphismes.

Pour construire le morphisme structural $s \ : \ A \ \rightarrow \ P$ il faut disposer du résultat de la proposition IV.1.6 pour les anneaux. En dépit du fait que celui-ci est présenté immédiatement après, aucun défaut de logique n'est cependant à déplorer.

Définition IV.1.5 (Structure produit) Avec les notations IV.1.3, si P est muni de l'unique structure faisant de $p_k \ ,_{1 \leq k \leq n}$ des morphismes on dit que P est muni de la *structure produit*. On parlera ainsi de *groupe produit* d'*anneau produit* de $\mathbb{K}$*-espace vectoriel produit* de A*-module produit* de A*-algèbre produit* ....

Lorsqu'on écrira $P \ = \ \prod_{k=1}^{n} E_k$ sans précision supplémentaire c'est que P sera muni de la structure produit héritée des structures des E_k.

Proposition IV.1.6 (Propriété universelle du produit) *Pour tout ensemble F et tout*

$$n - \text{uplet de morphismes, } f_k \ : \ F \ \rightarrow \ E_k \text{ pour l'une des structures IV.1.3.0) à IV.1.3.v)}$$

il existe un unique morphisme

$$f \ : \ F \ \rightarrow \ P \text{ tel que } \forall 1 \leq k \leq n, \ f_k \ = \ p_k \ \circ \ f \ .$$

Remarque IV.1.6.1 i) Dès l'instant où l'on fait l'hypothèse que $\forall 1 \ \leq \ k \ \leq \ n, \ f_k \ : \ F \ \rightarrow \ E_k$ est un morphisme c'est qu'on suppose implicitement que F et E_k sont munis de la structure algébrique (IV.1.3.0) à IV.1.3.v)) correspondante.

ii) Le résultat de cette proposition est, bien entendu, une particularisation au cas des morphismes de l'énoncé IV.1.1.iii) ; ce dernier constituant d'ailleurs l'ingrédient principal de la preuve qui suit.

***Preuve** (**de la proposition IV.1.6**): Les $f_k \ ,_{1 \leq k \leq n}$ étant en particulier des applications il existe (cf. IV.1.1.iii),) une unique application*

$$f \ : \ F \ \rightarrow \ P \text{ telle que } \forall 1 \leq k \leq n, \ f_k \ = \ p_k \ \circ \ f \ .$$

Il suffit donc de vérifier que f est un morphisme pour les structures considérées ; ce qui est tout à fait facile et laissé au lecteur.

Remarque IV.1.6.1 (Le cas des A-algèbrs) On peut alors compléter le point IV.1.4.iv) de la preuve de la proposition IV.1.4 tout en justifiant aussi la proposition IV.1.6 dans le cas des A-algèbres. Si, en effet les $E_k \ ,_{1 \leq k \leq n}$ sont des A-algèbres ce sont des anneaux si bien que P acquiert, en vertu de IV.1.4.ii) une unique structure d'anneau telle que les $p_k \ ,_{1 \leq k \leq n}$ sont des morphismes. Les morphismes structuraux $s_k \ : \ A \ \rightarrow \ E_k$ étant, par définition, des morphismes d'anneaux, la proposition IV.1.6 appliquée au cas des anneaux assure qu'il existe un unique morphisme d'anneaux

$$s \ : \ A \ \rightarrow \ P \text{ tel que } \forall 1 \leq k \leq n, \ s_k \ = \ p_k \ \circ \ s \ .$$

Si maintenant $f_k : F \to E_k$ sont des morphismes de A-algèbres ce sont en particulier des morphismes d'anneaux, et il existe donc, en vertu de la proposition IV.1.6 un unique morphisme d'anneaux

$$f : F \to P \text{ tel que } \forall 1 \leq k \leq n,\ f_k = p_k \circ f\ .$$

Reste à vérifier que ce dernier morphisme est bien compatible aux morphismes structuraux

$$u : A \to F \text{ et } s : A \to P\ ;$$

cette vérification étant laissée en exercice.

Proposition IV.1.7 *Dans le cas où il existe E tel que*

$$\forall 1 \leq k \leq n,\ E_k = E,\ \text{la bijection } \phi : M^{[1;n]} \cong \prod_{k=1}^{n} M$$

définie par la proposition IV.1.1.iv) est un isomorphisme pour l'une des structure IV.1.3.0) à à IV.1.3.v), pour peu que $E^{[1;n]}$ soit muni de la structure considérée en 0.12, (resp. 0.27.i),) (resp. 0.27.ii),) (resp. III.1.2.d) . . . .)

Proposition IV.1.8 *Supposons que $\forall 1 \leq k \leq n,\ (E_k, +_k)$ (resp. $(E_k, +_k, \cdot_k)$) est un groupe (abélien) (resp. un $\mathbb{K}$-espace vectoriel,) (resp. un A-module.) Soit alors*

$$i_k : E_k \to P\ ,\ x \mapsto (0_1, \ldots, 0_{k-1}, x, 0_{k+1}, \ldots, 0_n)\ ;$$

ce qui revient à dire que i_k est caractérisée par le fait que

$$\forall 1 \leq j \leq n,\ p_j \circ i_k \text{ est } \begin{array}{cc} \mathrm{Id}_{E_j} & \text{si } j = k \\ 0 & \text{sinon .} \end{array}$$

L'existence et l'unicité d'un tel morphisme sont assurées par la proposition IV.1.6.

i) Pour tout $1 \leq k \leq n$

$$i_k \text{ est un morphisme injectif et } p_k \circ i_k = \mathrm{Id}_{E_k}\ .$$

***Preuve** : Immédiat sur la définition de i_k.*

ii) Le groupe (resp. $\mathbb{K}$-espace vectoriel,) (resp. A-module,) P est la somme directe (cf. MAG303 Algèbre 1 TD n° VIII, exercice C, question 8),) (resp. (cf. IV.4.6.ii),)) des images des i_k :

$$P = \bigoplus_{k=1}^{n} \mathrm{Im}\, i_k$$

qu'on écrira, dans l'a mesure où

$$i_k \text{ induit un isomorphisme } E_k \cong \mathrm{Im}\, i_k,$$

$$P = \bigoplus_{k=1}^{n} E_k\ .$$

Remarque IV.1.9 (Attention !) Dans la proposition IV.1.8, ci-dessus on a uniquement considéré le cas des groupes , des $\mathbb{K}$-espaces vectoriels et des A-modules mais on n'a pas de résultat analogue pour les anneaux ou les A-algèbnres (cf. TD n° II, exercice A.)

Remarque IV.1.10 Si l'on considère avec attention les propriétés universelles énoncées d'une part en IV.1.6 et d'autre part au TD n° VIII, exercice C, question 8) (MAG*303 Algèbre 1*) (resp. IV.4.8,) on constate qu'elles sont en fait, en un certain sens « duales » l'une de l'autre au sens où la structure de produit permet de construire des morphismes de but P tandis que la structure de somme directe permet de construire des morphisme dont la source est précisément la somme directe.

La proposition IV.1.8 réconcilie les deux aspects mais il faut quand-même bien avouer que c'est un petit miracle qui ne concerne, parmi les structures que nous avons envisagées (cf. IV.1.3.0)à IV.1.3.v)) que les groupes abéliens et les A-modules. Il faut notamment prêter toute l'attention qu'il mérite à l'élément neutre 0_k de E_k qui permet de construire le morphisme i_k de manière suffisamment naturelle.

IV.2 . $-$Quotients

De même que pour le produit traité au paragraphe IV.1, la question des quotients comence avec une construction ensembliste qui s'enrichit en même temps que les structures dont on peut disposer sur les ensembles considérés.

Rappel IV.2.0 (sur les relations d'équivalence) On rappelle (cf. MAG*303 Algèbre 1* 1.1,) que si E est un ensemble muni d'une relation déquivalence $\sim$, et qu'on note $E/\sim$ l'ensemble des classes d'équivalence, on dispose d'une application surjective $\pi : E \to E/\sim$ qu'on appelle *surjection canonique*. Cette dernière, pou plus exactement le couple $(E/\sim, \pi)$ a la propriété universelle suivante :

Proposition IV.2.0.1 (Propriété universelle) *Pour toute application $f : E \to F$, les assertions suivantes sont équivalentes :*

a)

$$\forall (x,y) \in E \times E,\ x \sim y \Rightarrow f(x) = f(y)\ .$$

b) *Il existe une unique application*

$$g : E/\sim \to F \text{ tel que } g \circ \pi = f\ .$$

De plus, si f est surjective g l'est aussi et g est injective si l'implication dans a) est une équivalence.

Corollaire IV.2.0.2 *En particulier si $p : E \to F$ est une application surjective et que l'on définit la relation $\sim$ sur E, par :*

$$\forall (x,y) \in E \times E,\ x \sim y \Leftrightarrow p(x) = p(y), \qquad \text{IV.2.0.2.1}$$

on a un unique diagramme commutatif :

$$\begin{array}{ccc} E & & \\ {\scriptstyle\pi}\downarrow & \searrow p & \\ E/\sim & \xrightarrow{g} & F \end{array} \qquad \text{IV.2.0.2.2}$$

où g est bijective.

Lemme IV.2.0.3 *Ceci établit une correspondance bijective entre relations déquivalences et applications surjectives qui a toute relation déquivalence associe sa surjection canonique et à toute application surjective la relation d'équivalence définie comme en IV.2.0.2.1.*

Lemme IV.2.0.4 *Pour toute relation d'équivalence $\sim$ sur E, l'ensemble $E/\sim$ des classes d'équivalence est une partition de E.*

Réciproquement pour toute partition P de E, la relation $\sim$ définie sur E par

$$\forall (x,y) \in E \times E,\ x \sim y \Leftrightarrow \exists A \in P,\ x \in Ay \in A$$

est une relation d'équivalence telle que

$$E/\sim \cong P\,.$$

Remarque IV.2.0.5 Les lemmes IV.2.0.3 et IV.2.0.4 devraient donc établir une correspondance bijective entre applications surjective $p : E \to F$ et partitions de E. On peut expliciter cette correspondance en remarquant que l'ensemble des *fibres* de p

$$\{y \in F\,;\, p^{-1}(\{y\})\}$$

est une partition de E qui correspond bien à la relation d'équivalence IV.2.0.2.1

Les relations d'équivalences sur E, les partitions de E ou les applications surjectives $p : E \to F$ sont donc en fait trois manières de rendre compte d'une même réalité.

Néanmoins on constatera assez rapidement que si l'on ajoute des structures sur E et notamment des structures algébriques (groupe (cf. 0.13,) anneau (cf. 0.14,) $\mathbb{K}$-*espace vectoriel* (cf. 0.18,) A-module (cf. III.1.1,)) le choix d'une relation d'équivalence ne sera pas indifférent si l'on veut que le quotient $E/\sim$ soit muni d'une structure de même nature et tant qu'à faire de manière canonique (c'est-à-dire unique,) que la surjection canonique soit alors un morphisme et qu'on ait une propriété universelle analogue à IV.2.0.1 mais mettant cette fois en jeu des morphismes pour la structure considérée.

On est alors amené à donner la définition suivante :

Définition IV.2.1 Étant donné un magma associatif $(M, *)$, on dit qu'une relation d'équivalence $\sim$ sur l'ensemble M est *compatible à la loi* $*$ ou simplement compatible si

$$\forall (x,y,z,t) \in M \times M \times M \times M,\ \big(x \sim z \text{ et } y \sim t\big) \Rightarrow x * y \sim z * t\,.$$

Définition IV.2.2 De même si A est un anneau et M est muni dune loi externe $\cdot\ : A \times M \to M$, ce qui est le cas d'un $\mathbb{K}$-espace vectoriel lorsque l'anneau A est un corps $\mathbb{K}$, une relation d'équivalence $\sim$ sur M sera dite *compatible* à $\cdot$ si

$$\forall (a,x,y) \in A \times M \times M,\ \big(x \sim y\big) \Rightarrow a \cdot x \sim a \cdot y\,.$$

Notation IV.2.3 Dans la suite de ce paragraphe (IV.2,) les structures algébriques considérées sont (cf. IV.1.3.i) – IV.1.3.v),) celles déjà considérées au paraghraphe IV.1. Plus précisément dans toute la suite du paragraphe IV.2, les symbole X (resp. Y,) (resp. Z,) correspondrons à l'une des situations suivantes :

i) **(groupe)**
- — $(X, +)$ est un *groupe* (cf. 0.13,) dont l'élément neutre sera noté 0_X ou même 0 ;
- — Y et Z sont des sous-groupes distingués (cf. MAG*303 Algèbre 1* 2.1 ;) (cette dernière hypothèse étant automatiquement satisfaite dans le cas où $(X, +)$ est un *groupe abélien* (cf. MAG*303 Algèbre 1* 1.4.1 ;))
- — $MorfXW$ est un morphisme de groupes (cf. 0.20.)

ii) **(anneau)**
- — $(X, +, *)$ est un *anneau commutatif* (cf. MAG*303 Algèbre 1* 1.4.2 ;)
- — Y et Z sont des *idéaux* (cf. 0.16 ;)
- — $f : X \to W$ est un morphisme d'anneaux (cf. 0.21.)

iii) ($\mathbb{K}$**-espace vectoriel**)
- — $(X, +, \cdot)$ est un $\mathbb{K}$-*espace vectoriel* (cf. 0.18,) pour $\mathbb{K}$ un corps (cf. 0.17 ;)
- — Y et Z sont des sous-espaces vectoriels de X ;
- — $f \,:\, X \,\to\, W$ est un morphisme d'espaces vectoriels *i.e.* une application linéaire.

iv) (A**-module**)
- — $(X, +, \cdot)$ est un A-*module* (cf. III.1.1,)pour A un anneau commutatif ;
- — Y et Z sont des sous-A-modules de X ;
- — $f \,:\, X \,\to\, W$ est un morphisme de A-modules (cf. III.2.1.)

v) (A**-algèbre**)
- — $(X, +, *, s \,:\, A \,\to\, X)$ est une A-*algèbre* (cf. III.1.6,) commutative sur un anneau commutatif A ;
- — Y et Z sont des idéaux de X .
- — $f \,:\, X \,\to\, W$ est un morphisme de A-algèbres (cf. III.2.2.)

Lemme IV.2.4 *Soit X comme en IV.2.3.i) – IV.2.3.v).*
Soit $\sim$ une relation d'équivalence sur X, alors les assertions suivantes sont équivalentes :

a) La relation $\sim$ est compatible avec la loi $+$ (resp. avec les lois $+$ et $*$,) (resp. avec les lois $+$ et $\cdot$.)

b) Si $\overline{0_X}$ est la classe modulo $\sim$ de l'élément neutre 0_X de $(X, +)$), $\overline{0_X}$ est un sous-groupe (cf. IV.2.3.i),) de $(X, +)$
(resp. un idéal de $(X, +, *)$ (cf. IV.2.3.ii),)) (resp. un sous-espace vectoriel de $(X, +, \cdot)$ (cf. IV.2.3.iii),)) (resp un sous-A-module de $(X, +, \cdot)$ (cf. IV.2.3.iv),)) (resp. un idéal de $(X, +, *)$ (cf. IV.2.3.v) ;)) et

$$\forall x \in X,\ \overline{x} \;=\; x + \overline{0_X} \;=\; \{y \;\in\; \overline{0_X} \;;\; x + y\}\ .$$

c) $\overline{0_X}$ est un sous-groupe (resp. idéal) (resp. sous-espace vectoriel) (resp. sous-module) de X (resp. idéal,) et

$$\forall (x, y) \in X \times X,\ x \sim y \;\Leftrightarrow\; x - y \;\in\; \overline{0_X}\ .$$

Preuve *:*

*i) (**a)** $\Rightarrow$ **b)**)*
Si $\sim$ est compatible, comme $0_X \;\in\; \overline{0_X}, \overline{0_X} \;\neq\; \emptyset$. En outre

$$\begin{array}{llllll}\forall (x, y) \in \overline{0_X} \times \overline{0_X}, & x \sim 0_X \text{ et } y \sim 0_X & \Rightarrow & x + y \sim 0 & \Leftrightarrow & x + y \;\in\; \overline{0_X} \\ & x \sim 0 \text{et } -x \sim -x & \Rightarrow & 0 = x - x \sim -x & \Leftrightarrow & -x \;\in\; \overline{0_X}\ ; \end{array}$$

ce qui prouve que $\overline{0_X}$ est un sous-groupe de $(X, +)$
Par ailleurs :

$$\begin{array}{lrcl}\forall (x, y) \in X \times X, & x & \sim & y \\ \Leftrightarrow & x \sim y & \text{et} & -x \sim -x \\ \Rightarrow & y - x & \sim & 0 \\ \Rightarrow & y - x & \in & \overline{0_X} \\ \Rightarrow & y & \in & x + \overline{0_X} \\ \textit{i.e.} & \overline{x} & \subset & x + \overline{0_X}\ ; \\ \textit{Réciproquement} & y & \in & x + \overline{0_X} \\ \Rightarrow & x - y & \in & \overline{0_X} \\ \Rightarrow & y - x & \sim & 0_X \\ \Rightarrow & y - x \sim 0_X & \text{et} & x \sim x \\ \Rightarrow & y = y - x + x & \sim & x = 0_X + x \\ \textit{i.e.} & x + \overline{0_X} & \subset & \overline{x}\ . \end{array}$$

Si l'on suppose de plus que $(X, +, *)$ *est un anneau commutatif et que* $\sim$ *est compatible à* $*$,

$$\forall (ax) \in X \times X,\ x \ \in \ \overline{0_X} \ \Rightarrow \ x \sim 0 \ \Rightarrow \ a * x \sim 0 = a * 0 \ \Rightarrow \ a * x \ \in \ \overline{0_X}$$

ce qui prouve que $\overline{0_X}$ *est un idéal de* X.

On laisse le lecteur traiter le cas d'un $\mathbb{K}$*-espace vectoriel et d'un* A*-module en utilisant par exemple la caractérisation des sous-modules donnée en III.3.6.*

ii) ***(b)*** $\Rightarrow$ ***c))***

Est presque tautologique.

iii) ***(c)*** $\Rightarrow$ ***a))***

$$\begin{array}{lrcl} \forall (x,y,z,t) \in X \times X \times X \times X, & x \sim y & \text{et} & z \sim t \\ \Leftrightarrow & y - x \ \in \ \overline{0_X} & \text{et} & t - z \ \in \ \overline{0_X} \\ \Rightarrow & y + t - (x + z) = y - x + z - t & \in & \overline{0_X} \\ \Rightarrow & x + z & \sim & y + t \end{array} \qquad 1$$

en utilisant le fait que $\overline{0_X}$ *est un sous-groupe de* $(X, +)$.

Dans le cas où c'est un idéal (si bien entendu $(X, +, *)$ *est un anneau commutatif,) il est tout aussi immédiat de montrer que*

$$x \sim y \ \Rightarrow \ a * x \sim a * y \ .$$

Enfin le cas d'un $\mathbb{K}$*-espace vectoriel ou d'un* A*-module est laissé encore en exercice mais consiste en réalité formellement à remplacer* $*$ *par* $\cdot$ *dans la formule ci-dessus.*

Lemme IV.2.5 *Soient* X *et* Y *comme en IV.2.3.i) – IV.2.3.v). Alors il existe une unique relation d'équivalence* $\sim$ *sur* X *compatible à* $+$, *(resp. à* $+$ *et* $*$,*) (resp. à* $+$ *et* $\cdot$,*) telle que* $Y = \overline{0_X}$ *(où* $\overline{0_X}$ *est la classe de* 0_X *modulo* $\sim$*). Elle est caractérisée par le fait que*

$$\forall (x,y) \in X \times X,\ x \ \sim \ y \ \Leftrightarrow \ y - x \ \in \ Y \ = \ \overline{0_X} \ . \qquad \textit{IV.2.5.1}$$

Preuve *: Il faut remarquer que le fait que* $\sim$ *soit compatible à* $+$ *ce qui est exigé dans tous les cas entraîne que* $\sim$ *est nécessairement définie par la formule IV.2.5.1. L'unicité est ainsi assurée et la formule IV.2.5.1 définit bien une relation binaire. Le fait que* Y *soit un sous groupe assure que* $\sim$ *est bien une relation d'équivalence.*

Le fait que Y *soit un idéal (resp. un sous-espace vectoriel,) (resp. un sous-module,) (resp. un idéal,) entraînera que* $\sim$ *est compatible à* $*$ *(resp.* $\cdot$*.)*

Définition IV.2.6 (Relation compatible) Si X est comme en IV.2.3.i) – IV.2.3.v), on dira simplement qu'une relation d'équivalence $\sim$ sur X est *compatible* à la structur de groupe (resp. d'anneau) (resp. d'espace vectoriel,) (resp. de A-module) (resp. de A-algèbre,) ou même *compatible* (sans précision supplémentaire si le contexte est clair) si elle est compatible à la loi $+$ (resp. aux lois $+$ et $*$,) (resp. aux lois $+$ et $\cdot$.)

Les lemmes IV.2.4 et IV.2.5 assurent que $\sim$ est alors la relation d'équivalence donnée par un sous-ensemble Y comme en IV.2.3.i) – IV.2.3.v) de X et la formule IV.2.5.1.

On parlera alors indifféremment de *congruence modulo* $\sim$ ou de *congruence modulo* Y et de *classes selon* $\sim$ ou de *classes selon* Y.

Remarque IV.2.7 Le caractère un peu disparate de la définition ci-dessus ainsi que des constructions dans les lemmes IV.2.4 et IV.2.5, tiens au fait qu'on n'a pas formulé ces énoncé dans le langage des A-modules.

Si en effet on considère un groupe abélien $(X,+)$ muni de sa structure naturelle de $\mathbb{Z}$-module (cf. III.1.11.i),) il est équivalent pour une relation d'équivalence $\sim$ d'être compatible à la structure de groupe où à la structure de $\mathbb{Z}$-module (la compatibilité à $\cdot$ étant une conséquence de la compatibilité à $+$.) La condition que $\overline{0_X}$ soit un sous-groupe équivaut alors à ce que ce soit un sous-$\mathbb{Z}$-module (cf. III.3.10.i).)

De même si $(X,+,*)$ est un anneau commutatif, la compatibilité d'une relation d'équivalence $\sim$ à la structure d'anneau sur X n'est autre que la compatibilité à sa structure de X-module sur lui-même (cf. III.1.2.b),) et la condition pour $\overline{0_X}$ d'être un idéal équivaut à celle d'être un sous-X-module de X (cf. III.3.2.b).) Bien entendu le cas des $\mathbb{K}$-espaces vectoriels qui ne sont rien d'autre que des $\mathbb{K}$-modules entre parfaitement dans le cadre ci-dessus.

Remarque IV.2.8 Dans les énoncés IV.2.4 à IV.2.7, on n'a considéré que des groupes abéliens. On laisse le lecteur rappeler ses souvenirs dans le cas d'un groupe quelconque et formuler des énoncé analogue ; ce qui revient grosso modo à remplacer sous-groupe par sous-groupe distingué (cf. MAG*303 Algèbre 1* 2.1.)

Proposition IV.2.9 (existence de quotients) *Soient X et Y comme en IV.2.3.i) – IV.2.3.v), ou, de manière équivalente (cf. IV.2.4,) une relation d'équivalence compatible $\sim$ sur X, il existe une unique structure de groupe (resp. d'anneau,) (resp. de $\mathbb{K}$-espace vectoriel,) (resp. de A-module,) (resp. de A-algèbre,) sur l'ensemble $X/\sim$ des classes d'équivalence modulo $\sim$ (ou modulo Y) telle que la surjection canonique $\pi : X \to X/\sim$ soit un morphisme de groupes (cf. 0.20,) (resp. d'anneaux (cf. 0.21,)) (resp. de $\mathbb{K}$-espace vectoriel i.e. une application linéaire (cf. 0.18,)) (resp. de A-modules (cf. III.2.1,)) (resp. de A-algèbres (cf. III.2.2.))*

On a alors :

$$Y = \overline{0_X} = \operatorname{Ker}\pi \qquad \text{IV.2.9.1}$$

et

$$\forall (x,y) \in X \times X,\ x \sim y \Leftrightarrow y - x \in Y\,. \qquad \text{IV.2.9.2}$$

Preuve :

Lemme IV.2.9.1 *Si $(M,*)$ est un magma associatif, et $\sim$ une relation d'équivalence compatible,*

i) il existe une unique structure de magma sur l'ensemble quotient $M/\sim$ (ensemble des classes d'équivalence pour la relation $\sim$,) telle que la surjection canonique $\pi : M \to M/\sim$ soit un morphisme.

ii) Le magma $M/\sim$ est alors associatif (resp. commutatif) (resp. possède un élément neutre) s'il en est ainsi pour $(M,*)$.

Grâce au lemme IV.2.9.1, on peut munir $X/\sim$ d'une unique structure de groupe (resp. d'anneau.) Le cas des $\mathbb{K}$-espaces vectoriels ou des A-modules consiste à faire des vérifications analogues à celles du lemme IV.2.9.1 dans le cas d'une loi externe ce qui est tout à fait formel et laissé en exercice.

Définition IV.2.10 (Structure quotient) Pour X et Y comme en IV.2.3.i) – IV.2.3.v), on notera X/Y l'ensemble $X/\sim$ muni de la structure de groupe (resp. d'anneau,) (resp. d'espace vectoriel,) (resp. de A-module,) (resp. de A-algèbre,) définie par la proposition IV.2.9 que l'on appellera *structure quotient*.

On appellera

$$X/Y \text{ ou même le couple } \big(X/Y, \pi \,:\, X \,\to\, X/Y\big)$$

groupe quotient (resp. *anneau quotient*,) (resp. *espace vectoriel quotient*,) (resp. *module quotient*) (resp. *algèbre quotient*.)

Remarque IV.2.11 Dans la définition ci-dessus il s'agit en fait dans tous les cas de modules quotient, qui peuvent éventuellement disposer d'autres structures.

Définition IV.2.12 (Codimention d'un sous-espace vectoriel) Étant donné un $\mathbb{K}$-espace vectoriel (cf. 0.18,) E et F un sous-espace, le quotient E/F a alors une structure de $\mathbb{K}$-espace vectoriel. Si ce dernier est *de dimension finie*, (cf. 0.19.iv).c),) cette dernière s'appelle la *codimension* de F et est notée

$$\operatorname{codim}_{\mathbb{K}}(F) \;:=\; \dim_{\mathbb{K}} E/F \text{ ou simplement } \operatorname{codim}(F)\;.$$

Remarque IV.2.13 (Codimension) Pour E un $\mathbb{K}$-espace vectoriel et F un sous-espace,

i) il se peut tout à fait que ni E ni F ne soient de dimension finie mais que E/F le soit et que par conséquent on puisse définir $\operatorname{codim}(F)$;

ii) si F est de codimension finie c'est alors la dimension de n'importe quel supplémentaire de F (cf. TD n° V, exercice D, question 1), TD n° V, exercice D, question 2).)

La proposition qui suit assure que les quotients au sens où on les a construits par la proposition IV.2.9 l'ont été de manière à « prolonger » la propriété universelle dont on disposait dans le cadre ensembliste (cf. IV.2.0.1.) Il s'agit en quelque sorte de « remplacer » les applications par des morphismes pour la structure algébrique à laquelle on a affaire :

Proposition IV.2.14 (Propriété universelle des quotients) *Soit $MorfXW$ et Y comme en IV.2.3.i) – IV.2.3.v). Notons*

$$\forall (x,y) \in X \times X,\; x \,\sim\, y \;\Leftrightarrow\; y - x \,\in\, Y\;.$$

Alors les assertions suivantes sont équivalentes :

a)

$$\forall (x,y) \in X \times X,\; x \,\sim\, y \;\Rightarrow\; f(x) \,=\, f(y)\;;$$

b)

$$f(Y) \,=\, \{0_W\} \text{ i.e. } Y \,\subset\, \operatorname{Ker} f\;.$$

c) Il existe un unique morphisme de groupes (resp. d'anneaux) (resp. d'espaces vectoriels,) (resp. de A-modules,) (resp. de A-algèbres,)

$$g \,:\, X/Y \,\to\, W \text{ tel que } f \,=\, g \circ \pi \;\text{ où } \pi \,:\, X \,\to\, X/Y$$

est la surjection canonique.

De plus le morphisme g est injectif si et seulement si $Y = \operatorname{Ker} f$, ou de manière équivalente si et seulement si l'implication dans a) est une équivalence.

Le morphisme g est surjectif si et seulement si f l'est.

***Preuve** :*

i) ***(a)** $\Leftrightarrow$ **b))***
C'est une conséquence immédiate du lemme IV.2.4.

ii) ***(c)** $\Rightarrow$ **b))***
Est immédiat.

iii) ***(b)** $\Rightarrow$ **c))***
On est alors dans la situation de l'implication IV.2.0.1.a) entraîne IV.2.0.1.b) si bien qu'il

existe une unique application $g : X/Y \to W$ *tel que* $f = g \circ \pi$.

Reste donc uniquement à prouver que g est un morphisme :

$*$*)* ***(de magmas)***

$$\begin{array}{lrcl} \forall (u,v) \in X/Y \times X/Y,\ \exists (x,y) \in X \times X, & \pi(x) = u & \text{et} & \pi(y) = v \\ \textit{ce qui entraîne que} & g(u \dagger v) & = & g[\pi(x) \dagger \pi(y)] \\ & & = & g[\pi(x \dagger y)] \\ & & = & f(x \dagger y) \\ & & = & f(x) \dagger f(y) \\ & & = & g[\pi(x)] \dagger g[\pi(y)] \\ & & = & g(u) \dagger g(v) \end{array}$$

f est π étant des morphismes.

$\dagger$*)* ***(de groupes)***
Cela découle immédiatement de $*$).

$\ddagger$*)* ***(d'anneaux)***
Cela découle immédiatement de $*$) appliqué aux lois $+$ et $*$ et au fait que

$$g(1_{X/Y}) = g[\pi(1_X)] = f(1_X) = 1_W$$

puisque f et π sont des morphismes d'anneaux.

§) ***($\mathbb{K}$-espace vectoriel (resp. A-modules))***
D'après $\dagger$), g est déjà un morphisme de groupes. De plus

$$\begin{array}{lrcl} \forall (a,u) \in \mathbb{K}(\textit{resp. } A) \times X/Y,\ \exists x \in X, & u & = & \pi(x) \\ \textit{d'où} & g(a \cdot_{X/Y} u) & = & g[a \cdot_{X/Y} \pi(x)] \\ & & = & g[\pi(a \cdot_X x)] \\ & & = & f(a \cdot_X x) \\ & & = & a \cdot_Y f(x) \\ & & = & a \cdot_Y g[\pi(x)] \\ & & = & a \cdot_Y g(u) \end{array}$$

f et π étant des morphismes.

¶) *(A-**algèbres**)*
Il résulte de ‡) que g est d'ores et déjà un morphisme d'anneaux. De plus

$$g \circ s_{X/Y} = g \circ \pi \circ s_X = f \circ s_X = s_W .$$

*iv) (**Injectivité/surjectivité**)*
Sont des questions purement ensemblistes déjà établies en IV.2.0.1.

Notation IV.2.15 On dit souvent, dans la situation de la proposition IV.2.14, que f *se factorise à travers* X/Z ou encore à travers π.

Corollaire IV.2.16 *Étant donné un morphisme $f : X \to W$ comme en IV.2.3.i) – IV.2.3.v) qu'on suppose de plus surjectif, il existe un isomorphisme (pour la même structure algébrique,)*

$$\phi : X/\mathrm{Ker}\, f \to W \text{ tel que } \phi \circ \pi = q \text{ où } \pi : X \to X/\mathrm{Ker}\, q , \text{ est la surjection canonique.}$$

Corollaire IV.2.17 (Factorisation canonique des morphismes) *Étant donné un morphisme*

$$f : X \to W \text{ comme en IV.2.3.i) – IV.2.3.v),}$$

il existe un unique isomorphisme de groupes (resp. d'anneaux,) (resp. d'espaces vectoriels,) (resp. de A-modules,) (resp. de A-algèbres,)

$$\phi : X/\mathrm{Ker}\, f \cong \mathrm{Im}\, f \text{ tel que } \phi \circ \pi = f$$

où π est la surjection canonique.

Corollaire IV.2.18 *Soient X, Y et Z comme en IV.2.3.i), ou IV.2.3.iii) ou IV.2.3.iv).*

i) Si $Z \subset Y$, la surjection canonique $\pi_Y : X \to X/Y$ se factorise à travers le quotient X/Z en un morphisme surjectif π tel que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} X & & \\ {\scriptstyle \pi_Z}\downarrow & \searrow \pi_Y & \\ X/Z & \xrightarrow{\pi} & X/Y . \end{array}$$

ii) Si $Z \subset Y$, la restriction $\pi_{Z|Y}$ à Y de la surjection canonique $\pi_Z : X \to X/Z$ se factorise en un diagramme commutatif où j et injective :

$$\begin{array}{ccc} Y & \to & Y/Z \\ {\scriptstyle \mathrm{Id}_{X|Y}}\downarrow & & \downarrow {\scriptstyle j} \\ X & \xrightarrow{\pi_Z} & X/Z . \end{array}$$

iii) Toujours sous l'hypothèse que $Z \subset Y$, et avec les notations du point ii), notons

$$(X/Z)/(Y/Z) := (X/Z)/\mathrm{Im}\, j \text{ et } \pi : X/Z \to (X/Z)/(Y/Z) \text{ la surjection canonique.}$$

Alors la composée $\pi \circ \pi_Z$ ce factorise à travers la surjection canonique $\pi_Y : X \to X/Y$ de sorte que le diagramme du point ii) se complète en un diagramme commutatif où ϕ est un isomorphisme :

$$\begin{array}{ccc} Y & \to & Y/Z \\ {\scriptstyle \mathrm{Id}_{X|Y}}\downarrow & & \downarrow{\scriptstyle j} \\ X & \xrightarrow{\pi_Z} & X/Z \\ {\scriptstyle \pi_Y}\downarrow & & \downarrow{\scriptstyle \pi} \\ X/Y & \xrightarrow{\phi} & (X/Z)/(Y/Z)\ . \end{array}$$

***Preuve** : (cf. TD n° V, exercice C, question 2).)*

iv) En ne supposant plus nécessairement que $Z \subset Y$, la composée de la surjection canonique $Y + Z \to Z$ avec l'inclusion naturelle $Y \subset Y + Z$, se factorise à travers le quotient $Y/(Y \cap Z)$, donnant lieu au diagramme commutatif suivant où ϕ est un isomorphisme :

$$\begin{array}{ccc} Y & \to & Y+Z \\ \downarrow & & \downarrow \\ Y/(Y\cap Z) & \xrightarrow{\phi} & (Y+Z)/Z\ . \end{array}$$

***Preuve** : (cf. TD n° V, exercice C, question 1).)*

Corollaire IV.2.19 *Soient X et Y comme en IV.2.3.i) – IV.2.3.v).*

Soit $\pi : X \to X/Y$ la surjection canonique.

Un sous-ensemble U de X/Y est un sous-groupe (resp. un idéal,) (resp. un sous-espace vectoriel,) (resp. un sous- A-module,) (resp. un idéal,) de X/Y si et seulement si $\pi^{-1}(U)$ est un sous-groupe (resp. un idéal,) (resp. un sous-espace vectoriel,) (resp. un sous- A-module,) (resp. un idéal,) de X.

On a alors

$$U \cong \pi^{-1}(U)/Y\ .$$

L'application $U \mapsto \pi^{-1}(U)$ est alors une bijection croissante (pour la relation d'inclusion) de l'ensemble des sous-groupes (resp. idéaux,) (resp. sous-espaces vectoriels,) (resp. sous- A-modules,) (resp. idéaux,) de X/Y, dans l'ensemble des sous-groupes (resp. idéaux,) (resp. sous-espaces vectoriels,) (resp. sous- A-modules,) (resp. idéaux) de X contenant Y.

Remarque IV.2.20 Étant donné un groupe abélien, (resp. un $\mathbb{K}$-espace vectoriel,) (resp. un A-module,) X. les données suivantes sont équivalentes au sens où la donnée de l'une d'entre elles permet de construire canoniquement les trois autres :

a) Un sous-groupe (resp. sous-espace vectoriel,) (resp. sous- A-module,) Y de X.

b) Un morphisme injectif $i : Y \hookrightarrow X$.

c) Une relation d'équivalence compatible sur X.

d) Un morphisme surjectif $q : X \to Z$.

Par exemple d) $\Rightarrow$ a) consiste à prendre le noyau du morphisme surjectif, tandis que a) $\Rightarrow$ d) consiste à prendre le quotient par le sous-groupe (resp. sous-espace,) (resp. sous-A-module.)

L'équivalence a) $\Leftrightarrow$ c) a été établie dans le lemme IV.2.4.

Le reste des vérifications est laissé au lecteur.

Remarque IV.2.21 (Le cas des A-algèbres) Le cas des A-algèbres apparaît toujours à l'intersection des A-modules et des anneaux et il convient toujours de vérifier que lorsqu'une consttruction est possible dans les deux cadres, elle coïncide bien dans le cas des A-algèbres.

Proposition IV.2.22 *Étant donné un anneau A, un idéal $\mathfrak{I}$ de A est premier (cf. II.2.16,) (resp. maximal (cf. II.2.17)) si le quotient $A/\mathfrak{I}$ est intègre (cf.* MAG*303 Algèbre 1 1.4.2,) (resp. est un corps (cf. 0.17.))*

***Preuve** : (cf. TD n° II, exercice E, question 1), TD n° II, exercice E, question 2).)*

Corollaire IV.2.23 *Tout idéal maximal est premier.*

***Preuve** : (cf. TD n° II, exercice E, question 3).)*

Proposition IV.2.24 (théorème chinois des restes) Notation IV.2.24.1 i) Pour tout idéal $\mathfrak{I}$ de A, on notera

$\pi_I : A \to A/\mathfrak{I}$ la surjection canonique (cf. IV.2.10.)

Pour $n \in \mathbb{N}$ et $\mathcal{I} := \mathfrak{I}_{k\ ,1 \leq k \leq n}$ une famille d'idéaux, on notera :

ii)

$$\forall 1 \leq k \leq n,\ p_k : \prod_j 1nA/\mathfrak{I}_j \to A/\mathfrak{I}_k$$

la projection du produit sur le $k^{\text{ième}}$ facteur (cf. IV.1.3,)

iii) Il existe alors un unique morphisme d'anneaux

$$\pi_{\mathcal{I}} : A \to \prod_j 1nA/\mathfrak{I}_j$$

caractérisé par le fait que

$$\forall 1 \leq k \leq n,\ p_k \circ \pi_{\mathcal{I}} = \pi_{\mathfrak{I}_k}$$

(cf. IV.1.6,) Plus explicitement, pour tout $x \in A$,

$$\pi_{\mathcal{I}}(x) = \big(\pi_{\mathfrak{I}_1}(x), \ldots, \pi_{\mathfrak{I}_n}(x)\big)\ .$$

iv) On simplifiera autant que possible la notation $\pi_{\mathfrak{I}_k}$ en π_k si aucune confusion ne peut en résulter. De même on notera simplement π au lieu de $\pi_{\mathcal{I}}$ s'il n'y a pas d'ambiguîté sur la famille d'idéaux considérée.

v) Enfin on notera

$$\psi_{\mathcal{I}} \text{ ou simplement } \psi \ : \ A \ \to \ A/\big(\bigcap_{j=1}^{n} A/\mathfrak{I}_j\big)$$

la surjection canonique.

On peut synthétiser ces notations dans le diagramme suivant :

$$\begin{array}{ccc} A & \xrightarrow{\pi_{\mathcal{I}}} & \prod_j 1nA/\mathfrak{I}_j \\ \psi_{\mathcal{I}} \big\downarrow & \searrow \pi_{\mathfrak{I}_k} & \big\downarrow p_k \\ A/\big(\bigcap_{j=1}^{n} A/\mathfrak{I}_j\big) & & A/\mathfrak{I}_k\ . \end{array} \qquad \text{IV.2.24.1.1}$$

Soient $n \ \in \ \mathbb{N}, \mathcal{I} \ := \ \mathfrak{I}_{k\ ,1\ \leq\ k\ \leq\ n}$ *un* n*-uplet d'idéaux de* A.

ii) Il existe un unique morphisme injectif d'anneaux

$$\gamma \ : \ A/\big(\bigcap_{j=1}^{n} A/\mathfrak{I}_j\big) \ \to \ \prod_j 1nA/\mathfrak{I}_j \ \text{ tel que } \gamma \ \circ \ \psi \ = \ \pi\ .$$

***Preuve** : (cf. TD n° II, exercice G, question 3), a).)*

iii) Si les idéaux $\mathfrak{I}_{k\ ,1\ \leq\ k\ \leq\ n}$ *sont deux à deux comaximaux (cf. II.2.xviii),)* π *est surjective et partant* γ *est surjective et donc un isomorphisme.*

***Preuve** : (cf. TD n° II, exercice G, question 3), e).)*

Remarque IV.2.25 On donnera une version plus explicite du théorème chinois des restes (théorème V.5.2,) dans le cadre des anneaux principaux (cf. V.1.)

IV.3 . −Suites exactes

Dans toute cette section (IV.3,) A désigne un anneau commutatif (cf. MAG*303 Algèbre 1* 1.4.2.)

Définition IV.3.1 (Suite exacte courte) La notation

$$0 \ \to \ N \xrightarrow{\ \ i\ \ } X \xrightarrow{\ \ p\ \ } Q \ \to \ 0 \qquad \text{IV.3.1.1}$$

signifie que :

Ex$_1$) N, X et Q sont des groupes abéliens (resp. des A-modules.)

Ex$_2$) i et p sont des morphismes de groupes (resp. de A-modules.)

Ex$_3$)

$$\operatorname{Im} i \ = \ \operatorname{Ker} p\ .$$

Ex_4) i est un morphisme injectif (*i.e.* le noyau de i est l'image du morphisme nul $\{0\} \to N$.)

Ex_5) p est un morphisme surjectif

(*i.e.* l'image de p est le noyau du morphisme nul $Q \to \{0\}$.)

On dit alors que IV.3.1.1 est une *suite exacte courte de groupes abéliens* (resp. *de A-modules*.)

On dira aussi que

$$N \xrightarrow{\ i\ } X \xrightarrow{\ p\ } Q$$

est une *suite exacte* si l'on exige seulement que la condition Ex_3) soit satisfaite.

On peut encore généraliser la notion à

$$\ldots \to X_i \xrightarrow{f_i} X_{i+1} \xrightarrow{f_{i+1}} X_{i+2} \to \ldots$$

dont on dit que c'est une *suite exacte longue* si pour tout i, $\mathrm{Im}\, f_i = \mathrm{Ker}\, f_{i+1}$.

Remarque IV.3.2 La donnée d'une suite exacte courte de groupes abéliens (resp. de A-modules,) équivaut à l'une des données équivalentes de la remarque IV.2.20.

Plus précisément si $i : N \hookrightarrow X$ est un morphisme injectif il se complète en une suite exacte courte $0 \to N \xrightarrow{\ i\ } X \xrightarrow{\ p\ } Q \to 0$ en prenant $Q := X/\mathrm{Im}\, i$ et p la surjection canonique. On notera d'ailleurs souvent $X/N := X/\mathrm{Im}\, i$ puisque le morphisme injectif i induit un isomorphisme $i : N \cong \mathrm{Im}\, i$.

De même si $p : X \to Q$ est un morphisme surjectif, il se complète en une suite exacte courte $0 \to N \xrightarrow{\ i\ } X \xrightarrow{\ p\ } Q \to 0$ en prenant $N := \mathrm{Ker}\, p$; Le morphisme p se factorise alors en un isomorphisme

$$X/\mathrm{Ker}\, p = X/\mathrm{Im}\, i = X/N \cong Q \text{ (cf. IV.2.17 .)}$$

Remarque IV.3.3 Dans le cas d'un morphisme de A-modules les notions de noyau et d'image étant celle du morphisme de groupes sous-jacent une suite est exacte au sens des A-modules si et seulement si elle l'est au sens des groupes abéliens sous-jacents. En particulier pour une suite de groupes abéliens il est équivalent d'être exacte comme suite de groupes abéliens ou comme suite de $\mathbb{Z}$-modules.

Définition IV.3.4 Étant donnée une suite exacte courte de groupes abéliens (resp. A-modules,)

$$0 \to N \xrightarrow{\ i\ } X \xrightarrow{\ p\ } Q \to 0,$$

on dira que :

i) **(quotient)**
Q, ou le couple (Q, p) ou même p est un *quotient* de X ;

ii) **(Sous-module)**
N, ou le couple (N, i) ou même i est un *sous-groupe* (resp. *sous-module*,) de M. Cette dernière définition ne représentant d'ailleurs presque aucune nouveauté par rapport à celles qui ont été données dans la section 1.4.5 (MAG*303 Algèbre 1*) (resp. III.3.)

Remarque IV.3.5 Les deux notions définies ci-dessus de quotient et de sous-groupe (resp. sous- A-module,) ont « rarement » tendance à coïncider pour une paire de sous-modules donnée : si X et Y sont des groupes abéliens (resp. A-modules,) « généralement » Y n'est pas simultanément un quotient et un sous-groupe (resp. sous- A-module,) de X.

Le cadre des $\mathbb{K}$-espaces vectoriels, qui rappelons-le, sont un cas particulier de groupes abéliens (resp. A-modules,) peut induire en erreur. En effet dans ce cas la distinction entre quotient et sous-module n'est pas nécessairement facile à faire. Cela est lié, comme nous allons le voir précisément dans la suite à l'existence de supplémentaires pour un sous-espace, ou de scindage pour les suites exactes ce qui revient au même.

L'exemple suivant est néanmoins peut-être plus éclairant et il srait bon de le garder à l'esprit :

Exemple IV.3.6 a) Dans la proposition IV.1.8 on a donné les ingrédients permettant de construires les couples de suites exactes

$$0 \to X_1 \xrightarrow{i_1} X_1 \times X_2 \xrightarrow{p_2} X_2 \to 0 \text{ et } 0 \to X_2 \xrightarrow{i_2} X_2 \times X_1 \xrightarrow{p_1} X_1 \to 0$$

qui font manifestement apparaître les objets X_1 et X_2 simultanément comme des quotients et des sous-objets de $X_1 \times X_2$.

Cependant, on est parti de la situation d'un produit ce qui n'est pas forcément le cas général mais bel et bien celui développé dans les propositions IV.3.9 et IV.3.10.

b) Pour un entier $d \geq 2$, on a une suite exacte de groupes abéliens bien connue :

$$0 \to d\mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z} \to 0$$

qui fait naturellement de $\mathbb{Z}/d\mathbb{Z}$ un <u>quotient</u> de $\mathbb{Z}$.

On a établi dans un ou plusieurs exercices et si on l'a oublié il serait opportun désormais de ne pas le perdre de vue, qu'<u>il n'existe pas de morphisme de groupes injectif</u> de $\mathbb{Z}/d\mathbb{Z}$ dans $\mathbb{Z}$. Ainsi $\mathbb{Z}/d\mathbb{Z}$ <u>ne peut en aucun cas</u> se réaliser <u>comme (ous-groupe (sous-$\mathbb{Z}$-module)</u> de $\mathbb{Z}$. Il résulte de a) ou plus exactement de la proposition IV.1.8 qu'<u>on ne peut pas écrire</u> $\mathbb{Z} = d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$.

Définition IV.3.7 (Projecteur) On dit qu'un endomorphisme p d'un groupe abélien (resp. A-module,) X est un *projecteur* si (come dans le cas de l'algèbre linéaire) $p \circ p = p$.

Lemme IV.3.8 (Propriétés des projecteurs) *Soit* $p : X \to X$ *un projecteur (où* X *est un groupe abélien (resp.* A*-module :)*

i)

$$X = \operatorname{Ker} p \oplus \operatorname{Im} p\,;$$

ii)

$$\mathrm{Id}_X - p \text{ est un projecteur, } \operatorname{Ker} p = \operatorname{Im}(\mathrm{Id}_X - p)\,,\ \operatorname{Im} p = \operatorname{Ker} \mathrm{Id}_X - p\,.$$

Proposition IV.3.9 *Soient*

$$0 \to N \xrightarrow{i} X \xrightarrow{p} Q \to 0, \qquad \text{IV.3.9.1}$$

une suite exacte courte de groupes abéliens (resp. A*-modules,) et un morphisme*

$$s : Q \to X \text{ tel que } p \circ s = \mathrm{Id}_Q\,. \qquad \text{IV.3.9.2}$$

i) Le morphisme s *est injectif.*

ii)

$$X \;=\; \mathrm{Im}\, s \;\oplus\; \mathrm{Im}\,(\mathrm{Id}_X - s \circ p) \text{ et } \mathrm{Im}\,(\mathrm{Id}_X - s \circ p) \;=\; \mathrm{Ker}\, p \;=\; \mathrm{Im}\, i\,.$$

***Preuve** : Remarquons d'abord que*

$$(s \circ p)^2 \;=\; s \circ p \circ s \circ p \;=\; s \circ p$$

si bien que $s \circ p$ est un projecteur et que l'on peut appliquer le lemme IV.3.8. On a donc

$$X \;=\; \mathrm{Im}\,(s \circ p) \;\oplus\; \mathrm{Ker}\,(s \circ p)\,.$$

Le morphisme p étant surjectif, $\mathrm{Im}\,(s \circ p) \;=\; \mathrm{Im}\, s$. Le morphisme s étant injectif,

$$\mathrm{Ker}\,(s \circ p) \;=\; \mathrm{Ker}\, p \;=\; \mathrm{Im}\, i$$

puisque la suite IV.3.9.1 est exacte.

iii) On peut donc noter

$$r \;:=\; i^{-1} \circ (\mathrm{Id}_X - s \circ p) \;:\; X \;\to\; N$$

et l'on a

$$r \;\circ\; i \;=\; \mathrm{Id}_N \;:$$

En effet

$$r \;\circ i \;=\; i^{-1} \;\circ\; (\mathrm{Id}_X - s \circ p) \;\circ\; i \;=\; i^{-1} \;\circ\; (i - s \circ p \circ i) \;=\; i^{-1} \;\circ\; i \;=\; \mathrm{Id}_N\,.$$

Ce qui entraîne que r est surjectif. De plus $r \;\circ\; i$ est un projecteur et

$$(r \;\circ\; i) \;+\; (s \;\circ\; p) \;=\; \mathrm{Id}_X\,.$$

iv)

$$\mathrm{Im}\, s \;=\; \mathrm{Ker}\, r\,.$$

***Preuve** : En effet,*

$$\mathrm{Ker}\, r \;=\; \mathrm{Ker}\,(i^{-1} \circ (\mathrm{Id}_{-} s \circ p)) \;=\; \mathrm{Ker}\,(IdM - s \circ p)$$

puisque i^{-1} est injectif. Or

$$\mathrm{Ker}\,(\mathrm{Id}_X - s \circ p) \;=\; \mathrm{Im}\,(s \circ p)$$

en vertu du lemme IV.3.8. Or p étant surjectif, $\mathrm{Im}\, s \circ p \;=\; \mathrm{Im}\, s$.

v) Il résulte de ce qui précède que

$$0 \;\to\; Q \xrightarrow{\quad s \quad} M \xrightarrow{\quad r \quad} N \;\to\; 0$$

est une suite exacte courte.

Proposition IV.3.10 *Soient*

$$0 \to N \xrightarrow{i} X \xrightarrow{p} Q \to 0, \qquad \text{IV.3.10.1}$$

une suite exacte courte de groupes abéliens (resp. A-modules,) et un morphisme

$$r : X \to N \text{ tel que } r \circ i = \mathrm{Id}_N . \qquad \text{IV.3.10.2}$$

i) Le morphisme r est surjectif.

ii)

$$X = \mathrm{Im}\, i \oplus \mathrm{Im}\,(\mathrm{Id}_X - i \circ r) \text{ et } \mathrm{Im}\, i = \mathrm{Ker}\, p .$$

Preuve : *Remarquons d'abord que*

$$(i \circ r)^2 = i \circ r \circ i \circ r = i \circ r$$

si bien que$i \circ r$ est un projecteur et que l'on peut appliquer le lemme IV.3.8. On a donc

$$X = \mathrm{Ker}\,(i \circ r) \oplus \mathrm{Im}\,(i \circ r) .$$

De plus $\mathrm{Ker}\,(i \circ r) = \mathrm{Im}\,(\mathrm{Id}_X - i \circ r)$. *Enfin, r étant surjectif,*

$$\mathrm{Im}\,(i \circ r) = \mathrm{Im}\, i = \mathrm{Ker}\, p$$

puisque la suite IV.3.10.1 est exacte.

iii) Il en résulte que $p_{|\mathrm{Im}\,(\mathrm{Id}_X - i \circ r)}$ est un isomorphisme. On note $s : Q \to M$ son isomorphisme inverse. Il s'ensuit immédiatement que s est injectif et

$$p \circ s = \mathrm{Id}_Q .$$

De plus $s \circ p$ est un projecteur et

$$(r \circ i) + (s \circ p = \mathrm{Id}_X .$$

iv)

$$\mathrm{Im}\, s = \mathrm{Ker}\, r .$$

Preuve : *En effet, en utilisant encore le lemme IV.3.8,*

$$\mathrm{Im}\, s = \mathrm{Im}\, \mathrm{Id}_X - i \circ r = \mathrm{Ker}\, i \circ r = \mathrm{Ker}\, r$$

puisque i est injectif.

v) Il résulte de ce qui précède que

$$0 \to Q \xrightarrow{s} M \xrightarrow{r} N \to 0$$

est une suite exacte courte.

Définition IV.3.11 i) (**Section**)
Un morphisme $s : Q \to M$ comme en IV.3.9.2 est usuellement appelée une *section* de p ou un *scindage de la suite exacte* et l'on di que la suite exacte courte IV.3.9.1 est *scindée* ;

ii) (**Rétraction**)
On dit qu'un morphisme $r : M \to N$ come en IV.3.10.2 est une *rétraction* de i et l'on dit que la suite exacte courte IV.3.10.1 est *rétractée*.

En fait les proposition IV.3.9 et IV.3.10 montrent qu'une suite exacte courte de groupes abéliens (resp. A-modules,) est scindée si et seulement si elle est rétractée ;

Exemple IV.3.12 a) Bien entendu les situations envisagées en IV.1.8 fournissent des exemples de suites exactes courtes scindées (ou de manière équivalente rétractée.) Nous allons en fait voir à la proposition IV.3.13, qu'on a là en quelque sorte une situation modèle de suites scindées ou rétractées.

b) Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie m et F un sous espace vectoriel de E de dimension $n \leq m$. notons $G := E/F$ si bien qu'on a une suite exacte

$$0 \to F \xrightarrow{i} E \xrightarrow{p} G \to 0$$

où p est la surjection canonique et i l'inclusion naturelle de F dans E (*i.e.* la restriction de l'identité Id_E à F.) Une base $(u_1, \dots, u_n)$ de F se complète en une base $(u_1, \dots, u_m)$ de E. C'est précisément un des points essentiels de la théorie des espaces vectoriels et qui nous fera défaut dans le cadre des groupes abéliens (resp. A-modules,) et auquel nous chercherons les meilleurs paliatifs possibles.

C'est alors un exercice facile (mais qu'ill est néanmoins bon d'avoir fait au moins une fois) que de montrer que $p(u_i)_{,n+1 \leq i \leq m}$ est une base de G qui se trouve donc être de dimension finie également.

On définit $s : G \to E$ comme l'unique morphisme (application linéaire) tel que

$$\forall n+1 \leq i \leq m,\ s[p(u_i)] = u_i\ .$$

Il est alors immédiat de vérifier que $p \circ s = \mathrm{Id}_G$ c'est-à-dire que s est une section de p.

La proposition suivante est une sorte de réciproque de l'exemple IV.3.6.a) :

Proposition IV.3.13 *Étant donnée une suite exacte courte de groupes abéliens (resp. A-modules,)*

$$0 \to N \xrightarrow{i} X \xrightarrow{p} Q \to 0,$$

s'il existe

une section $s : Q \to M$ de p (cf. IV.3.9.2 ,)

(resp. une rétraction $r : M \to N$ de i (cf. IV.3.10.2 ,)

il existe une rétraction r de i (resp. une section s de p,) et le morphismes

$$f : M \to N \times Q\ ,\ x \mapsto \big(r(x), p(x)\big) \text{ et } g : N \times Q \to M\ ,\ (y, z) \mapsto i(y) + s(z)$$

sont des isomorphismes inverses l'un de l'autre.

Preuve *: En effet :*

$$\begin{array}{rcl} \forall x \in M, \quad g[f(x)] & = & g[r(x), p(x)] \\ & = & i[r(x)] + p[p(x)] \\ & = & x \text{ (cf. IV.3.9.iii) ou IV.3.10.iii)) .} \end{array}$$

Réciproquement :

$$\begin{array}{rcl} \forall (y,z) \in N \times Q, \quad f[g[(y,z)]] & = & f[i(y) + s(z)] \\ & = & \big(f[i(y)], p[s(z)]\big) \\ & = & (y,z) \;. \end{array}$$

Remarque IV.3.14 La proposition IV.3.13 ci-dessus est en fait un énoncé réciproque de la proposition IV.1.8. En effet, avec les notations de la proposition IV.1.8, les points IV.1.8.i) à IV.1.8.ii) assurent que l'on a deux suites exactes scindées

$$0 \;\to\; X_1 \xrightarrow{i_1} M \xrightarrow{p_2} X_2 \;\to\; 0 \text{ et } 0 \;\to\; X_2 \xrightarrow{i_2} M \xrightarrow{p_1} X_1 \;\to\; 0 \;.$$

On pourrait synthétiser ces résultats dans l'énoncé suivant :

Théorème IV.3.15 *Soient X et Y deux groupes abéliens (resp. A-modules,) alors les données suivantes sont équivalentes :*

a) Un morphisme injectif $i \;:\; Y \;\hookrightarrow\; X$ tel que la suite exacte

$$0 \;\to\; Y \xrightarrow{i} X \xrightarrow{p} Q \;\to\; 0$$

qui s'en déduit soit scindée/rétractée.

b) Un morphisme surjectif $p \;:\; X \;\to\; Y$ tel que la suite exacte

$$0 \;\to\; N \xrightarrow{i} X \xrightarrow{p} Y \;\to\; 0$$

qui s'en déduit soit scindée/rétractée.

c) Un morphisme injectif $i \;:\; Y \;\to\; X$ et un sous-groupe (resp. sous- A-module,) $Z \;\subset\; X$ tel que

$$X \;=\; i(Y) \;\oplus\; Z \;.$$

d) Un groupe abélien (resp. A-module,) Z et un isomorphisme

$$f \;:\; Y \times Y \;\cong\; X \;.$$

Définition IV.3.16 (Facteur direct) Dans le cas où X et Y sont des groupes abéliens (resp. A-modules,) vérifiant les conditions équivalentes du théorème IV.3.15, on dit que Y est un *facteur direct* de X. Ceci signifie que Y est à la fois un quotient et un sous-groupe (resp. sous- A-module,) de X.

Corollaire IV.3.17 *Étant donné un groupe abélien (resp. A-module,) X,*

i) si Y et Z sont des sous-groupes (resp. sous- A-modules,) de X tels que

$$X \;=\; Y \;\oplus\; Z,$$

le morphissme naturel $Y \times Z \;\to\; M$, $(x,y) \;\mapsto\; x+y$ est un isomorphisme ;

ii) Réciproquement, si Y et Z sont des groupes abéliens (resp. A-modules,) tels qu'on ait un isomorphisme

$$f \,:\, Y \times Z \;\cong\; X,$$

que lon note

$$i \,:\, Y \;\to\; X \;,\; x \;\mapsto\; f(x,0) \text{ et } j \,:\, Z \;\to\; X \;,\; x \;\mapsto\; f(0,x),$$
$$X \;=\; i(Y) \;\oplus\; j(Z)$$

qu'on abrègera, si aucune confusion n'est à craindre en

$$X \;=\; Y \;\oplus\; Z \;.$$

Proposition IV.3.18 *Soient $f \,:\, X_1 \;\to\; X_2$ un morphisme de groupes abéliens (resp. A-modules,), (Y_i, Z_i) un couple de sous-groupes (resp. sous- A-modules,) de $X_{i\ ,i\ =\ 1 \text{ ou } 2}$, tel que*

$$X_i \;=\; Y_i \;\oplus\; Z_i \;,\; f(Y_1) \;\subset\; Y_2 \text{ et } f(Z_1) \;\subset\; Z_2 \;.$$

On note alors

$$f_Y \;:=\; f_{|Y_1} \text{ (resp. } f_Y \;:=\; f_{|Z_1} \text{) la restriction de } f \text{ à } Y_1 \text{ (resp. } .Z_1 \text{ .)}$$

i)

$$\operatorname{Ker} f \;=\; \operatorname{Ker} f_Y \;\oplus\; \operatorname{Ker} f_Z \;.$$

Preuve : *Puisque*

$$\operatorname{Ker} f_Y \;\subset\; Y_1 \text{ et } \operatorname{Ker} f_Z \;\subset\; Z_1,$$

que Z_1 et Y_1 sont en somme directe, la somme $\operatorname{Ker} f_Y \;+\; \operatorname{Ker} f_Z$ est nécessairement directe. Or pour tout $x \;\in\; X_1$, il existe un unique couple $(y,z) \;\in\; Y_1 \times Z_1$ tel que $x \;=\; y+z$. Or

$$f(x) \;=\; 0 \;\Leftrightarrow f(y+z) \;=\; 0 \;\Leftrightarrow\; f_Y(y) + f_Z(z) \;=\; 0,$$

$f_Y(y) \;\in\; Y_2$ $f_Z(z) \;\in\; Z_2$, Y_2 et Z_2 sont en somme directe si bien que

$$f_Y(y) + f_Z(z) \;=\; 0 \;\Leftrightarrow\; f_Y(y) \;=\; f_Z(z) \;=\; 0 \;\Leftrightarrow\; y \;\in\; \operatorname{Ker} f_Y \text{ et } z \;\in\; \operatorname{Ker} f_Z \;.$$

ii)

$$\operatorname{Im} f \;=\; \operatorname{Im} f_Y \;\oplus\; \operatorname{Im} f_Z \;.$$

Preuve : *Ici encore, comme ci-dessus, la somme $\operatorname{Im} f_Y \;+\; \operatorname{Im} f_Z$ est directe ; l'inclusion $\operatorname{Im} f_Y \;+\; \operatorname{Im} f_Z \;\subset\; \operatorname{Im} f$ est immédiate.*

Pour tout $x \;\in\; \operatorname{Im} f$, il existe $u \;\in\; X_1$ tel que $x \;=\; f(u)$. Or il existe $(v,w) \;\in\; Y_1 \times Z_1$ tel que $u \;=\; v+w$ si bien que

$$x \;=\; f(u) \;=\; f(v+w) \;=\; f_Y(v) + f_Z(w) \;\in\; \operatorname{Im} f_Y \;+\; \operatorname{Im} f_Z \;.$$

Théorème IV.3.19 (Principe d'EULER–POINCARÉ) *i) Si*

$$0 \to K \longrightarrow G \longrightarrow H \to 0$$

est une suite exacte courte de groupes abéliens, G est un groupe fini si et seulement si il en est de même de K et H et dans ce cas

$$\#(G) = \#(K) * \#(H) .$$

ii) Si

$$0 \to N \longrightarrow E \longrightarrow Q \to 0$$

est une suite exacte courte de $\mathbb{K}$-espaces vectoriels, E est de dimension finie si et seulement si N et Q le sont et dans ce cas

$$\dim_{\mathbb{K}} E = \dim_{\mathbb{K}} N + \dim_{\mathbb{K}} Q .$$

IV.4 . −Intersection, somme, engendrement

Corollaire IV.4.1 (de la proposition III.3.9) *Étant donnés un anneau commutatif A, un A-module (resp. une A-algèbre) X, et $S \subset X$ une partie de X, l'ensemble $\mathcal{Y}$ des sous-modules (resp. sous-algèbres) de X contenant S possède un plus petit élément*

$$< S > = \bigcap_{Y \in \mathcal{Y}} Y .$$

Définition IV.4.2 (Sous-module (resp. sous-algèbre) engendré) Avec les notations du corollaire IV.4.1, le sous-module (resp. la sous-algèbre) $< S >$ s'appelle le *sous-module engendré*, (resp. la *sous-algèbre engendrée*,) par S. On dit que S est une *partie génératrice* de $< S >$.

Exemple IV.4.3 a) $< \emptyset > = \{0\}$.

b) Pour tout sous-module N de M,

$$< N > = N .$$

c) Tout sous-$\mathbb{Z}$-module de $\mathbb{Z}$, (resp. sous-$\mathbb{K}[X]$-module de $\mathbb{K}[X]$ (cf. I.4.4,)) *i.e.* tout idéal de $\mathbb{Z}$ (resp. $\mathbb{K}[X]$,) est engendré par un seul élément *i.e.* est *principal*.

d) Si $\mathbb{K}$ est un corps et E un $\mathbb{K}$-espace vectoriel, pour tout $S \subset E$, $< S >$ n'est autre que le sous-espace vectoriel engendré par S usuellement noté $\mathrm{Vect}\{S\}$ dans le cadre de l'algèbre linéaire.

Il se peut également que pour un A-module M avec A un anneau qu'i n'est pas nécessairement un corps, et $S \subset M$, on note $\mathrm{Vect}\{S\} := < S >$.

Lemme IV.4.4 (descriptions du sous-module engendré) *Étant donné un A-module M, pour tout $X \subset M$, tout $x \in M$, $x \in < X >$ si et seulement s'il existe $r \in \mathbb{N}$, $x_{i\,,1 \leq i \leq r} \in X$, et $a_{i\,,1 \leq i \leq r} \in A$ tels que*

$$x = \sum_{i=1}^{r} a_i \cdot x_i . \qquad \text{IV.4.4.1}$$

Lemme IV.4.5 (Somme) *Étant donné un A-module M et $\mathcal{X}$ un ensemble de sous-modules de M,*

$$< \bigcup_{X \in \mathcal{X}} X > = \left\{ r \in \mathbb{N} ; \sum_i 1rs_i \ , \forall 1 \leq i \leq r, \ \exists X \in \mathcal{X}, \ s_i \in X \right\} . \qquad IV.4.5.1$$

Autrement dit :

$$\forall x \in M, \ x \in < \bigcup_{X \in \mathcal{X}} X > \Leftrightarrow \exists r \in \mathbb{N}, \ \forall 1 \leq i \leq r, \ \exists X_i \in \mathcal{X}, \ \exists x_i \in X_i, \ x = \sum_{i=1}^{r} x_i \ . \qquad IV.4.5.2$$

Définition IV.4.6 (Somme) Avec les notations du lemme IV.4.5 :

i) (**Somme**)
$(\bigcup_{X \in \mathcal{X}} Y)$ s'appelle la *somme* des X pour X appartenant à $\mathcal{X}$ qu'on notera $\sum_{X \in \mathcal{X}} X$.

ii) (**Somme directe**)
On dit qu'on a une *somme directe* si dans la décomposition IV.4.5.2 l'entier r, les X_i et les $x_i \neq 0$, sont uniques. On notera alors

$$\bigoplus_{X \in \mathcal{X}} X := < \bigcup_{X \in \mathcal{X}} > .$$

iii) (**Supplémentaires**)
Pour un A-module M et deux sous-modules N et P, si $M = N \oplus P$, on dit que N et P sont *supplémentaires* l'un de l'autre.

Remarque IV.4.7 Soient M un A-module et $\mathcal{N}$ un ensemble (quelconque en particulier pas nécessairement fini) de sous$-A$-modules de M.

i) (**Somme directe externe**)
On peut comme pour les groupe abéliens (cf. MAG*303 Algèbre 1* 4.1,) on peut définir la *somme directe externe* des éléments de $\mathcal{N}$

$$\bigoplus_{N \in \mathcal{N}} N \subset \prod_{N \in \mathcal{N}} N \text{ (cf. IV.1.2 ,)}$$

constitué des *éléments presque nuls*, ou encore *à support fini i.e.* les éléments $f \in \prod_{N \in \mathcal{N}} N$ tel que l'ensemble $\{N \in \mathcal{N} \ ; \ f(n) \neq 0_N\}$ est fini.

ii) À noter qu'une telle construction n'est possible que parce que chaque $N \in \mathcal{N}$ contient un élément 0_N ; ce qui était déjà le cas pour les groupes abéliens.

iii) Pour peu qu'on se convainque qu'un groupe abélien n'est rien d'autres qu'un $\mathbb{Z}$-module, la construction ci-dessus généralise la construction faite pour les groupes abéliens et en a toutes les propriétés :

a) si $\mathcal{N}$ est fini

$$\bigoplus_{N \in \mathcal{N}} N = \prod_{N \in \mathcal{N}} N \ ;$$

ce que nous avons en fait détaillé en IV.1.8 et qui fait que parfois les deux constructions ne sont pas forcément faciles à distinguer (cf. TD n° VIII, exercice C ;)

b) $\bigoplus_{N \in \mathcal{N}} N$ est un sous-A-module de $\prod_{N \in \mathcal{N}} N$;

c) pour tout $N \in \mathcal{N}$, l'application $N \to \prod_{N \in \mathcal{N}} N$, $x \mapsto P \mapsto \delta_{N,P}x$ est un morphisme injectif de A-modules qui permet d'identifier N à un sous-A-module de $\prod_{N \in \mathcal{N}} N$;

d) $\bigoplus_{N \in \mathcal{N}} N$ est alors la somme directe des sous module $N \in \mathcal{N}$ au sens de IV.4.6.ii).

Notons

$$\phi : \bigoplus_{N \in \mathcal{N}} N \to M , f \mapsto \sum_{N \in \mathcal{N}} f(N)$$

(la dernière somme ayant précisément un sens puisque f est presque nulle ou à support fini) alors :

e) L'application ϕ est un morphisme de A-modules ;

f) l'image $\operatorname{Im} \phi$ de ϕ est la somme des $N \in \mathcal{N}$ au sens de IV.4.6.i) ;

g) la somme est directe si et seulement si ϕ est injectif.

Proposition IV.4.8 (Propriété universelle des sommes directes) *Étant donnée un a-module M et $\mathcal{N}$ une famille de sous-modules telle que la somme $\sum_{N \in \mathcal{N}} N = \bigoplus_{N \in \mathcal{N}} N$ est directte, pour tout ensemble de morphismes*

$$\{f_N : N \to P\}_{,N \in \mathcal{N}} ,$$

où P est un A-module, il existe un unique morphisme

$$f : \bigoplus_{N \in \mathcal{N}} N \to P \text{ tel que } \forall N \in \mathcal{N},\ f_{|N} = f_N .$$

Remarque IV.4.9 i) De même que dans le cas des groupes abéliens, pour M un A-module, N et P des sous-modules,N et P sont en somme directe ou encore supplémentaires l'un de l'autre si et seulement si

$$M = N + P \text{ et } N \cap P = \{0\} .$$

ii) Pour deux sous-modules N et P de M, le sous-module $N + P$ engendré par $N \cup P$ est l'ensemble des $x + y$ avec $x \in N$ et $y \in P$.

iii) Plus généralement, pour $N_{i\ ,1 \leq i \leq r}$ ($r \in \mathbb{N}^*$) un r-uplet de sous-modules de M, Notons

$$S := \sum_{i=1}^{r} N_i = N_1 + \ldots + N_r .$$

Alors pour tout $x \in M$, $x \in S$ si et seulement s'il existe un r-uplet

$$x_{i\ ,1 \leq i \leq r} ,\ \forall 1 \leq i \leq r,\ x_i \in N_i \text{ tel que } x = \sum_{i=1}^{r} x_i .$$

iv) Étant donné un A-module M et $\mathcal{N}$ un ensemble de sous-modules de M, on note $S := \sum_{N \in \mathcal{N}} N$. Alors pour tout $x \in M$, $x \in S$ si et seulement s'il existe un entier $r \in \mathbb{N}$, un r-uplet $N_{i\ ,1 \leq i \leq r} \in \mathcal{N}$ de sous-modules appartenant à $\mathcal{N}$, un r-uplet

$$x_{i\ ,1 \leq i \leq r}\ ,\ \forall 1 \leq i \leq r,\ x_i \in N_i \text{ tel que } x = \sum_{i=1}^{r} x_i\ .$$

Il convient de bien remarquer que, même si l'ensemble $\mathcal{N}$ n'est pas fini, la somme $\sum_{N \in \mathcal{N}} N$ est l'ensemble des sommes finies d'éléments des $N \in \mathcal{N}$.

Ainsi, par exemple la famille $X^n{}_{,n \in \mathbb{N}}$ est génératrice pour l'anneau $\mathbb{K}[X]$ vu comme $\mathbb{K}$-module (cf. I.2,) mais ne l'est pas pour l'anneau $\mathbb{K}[[X]]$ des séries formelles, toujours vu comme $\mathbb{K}$-module (cf. I.1.)

v) Ici encore l'existence d'un supplémentaire pour un sous-module N d'un A-module M n'est pas assurée en général ; puisqu'en particulier elle n'est déjà pas assurée dans le cas des $\mathbb{Z}$-modules . Ici encore le théorème IV.3.15 établit l'équivalence entre existence d'un supplémentaire de N et d'une section de la surjection canonique $M \to M/N$.

vi) (**Espaces vectoriels**)

Bien entendu, on sait que dans le cas où A est un corps un A-module M est un espace vectoriel. Dans le cas où M est de dimension finie, on connaît bien le théorème de la base incomplète qui assure en particulier que tout sous-espace vectoriel de M admet un supplémentaire.

Remarque IV.4.10 i) Si $(A, +)$ est un groupe abélien et $S \subset A$ une partie de A, le sous-groupe de A engendré par S (cf. MAG*303 Algèbre 1* 1.4.6,) est exactement le sous-$\mathbb{Z}$-module de A engendré par S au sens de la définition IV.4.2.

ii) De même si $(A, +, *)$ est un anneau commutatif et $S \subset A$ une partie de A, l'idéal engendré par S (cf. II.2.13,) est exactement le sous-A-module de A engendré par S au sens de la définition IV.4.2.

iii) La *somme* (resp. *somme directe*) d'un ensemble de sous-$\mathbb{Z}$-modules définie en IV.4.6 est exactement la somme (resp. la somme directe) définie pour les sous-groupes en (cf. MAG*303 Algèbre 1* 4.1.)