Université Paris Sud **Année 2019–2020**

L3/S6 M305 Algèbre II

Responsable Pierre Lorenzon
Bureau 2I3
IMO Bat. 307 91405 Orsay cedex
Tel. : +33 1 69 15 60 26
Courriel : lorenzon@math.u-psud.fr
http://www.math.u-psud.fr/∼lorenzon

Pour une impression papier de ce texte, adressez-vous au secrétariat du L3. Cependant il n'est pas exclu que des modifications qui seront sans doute mineures soient apportées à cette version électronique. À ce propos, toute suggestion, est la bienvenue. Signalez-moi toute erreur.

Avant-propos

On montre, au chapitre II, que les groupes abéliens sont essentiellement du genre $\mathbb{Z}^r$ ou $\mathbb{Z}/n\mathbb{Z}$ ou bien des produits de ce type d'objets. On verra, au chapitre IV, qu'une matrice à coefficients dans un corps, dans les cas les plus favorables, est semblable à une matrice composée de blocs de JORDAN :

$$\begin{pmatrix}
\lambda_1 & 0 & 0 & \dots & 0 & 0 & & & & & & & & & & \\
1 & \lambda_1 & 0 & \dots & 0 & 0 & & & & & & & & & & \\
0 & 1 & \lambda_1 & \dots & 0 & 0 & & & 0 & & & \dots & & & 0 & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & & & & & & & & & \\
0 & 0 & 0 & \dots & 1 & \lambda_1 & & & & & & & & & & \\
& & & & & & \lambda_2 & 0 & 0 & \dots & 0 & 0 & & & & & \\
& & & & & & 1 & \lambda_2 & 0 & \dots & 0 & 0 & & & & & \\
& & 0 & & & & 0 & 1 & \lambda_2 & \dots & 0 & 0 & \dots & & 0 & & \\
& & & & & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & & & & \\
& & & & & & 0 & 0 & 0 & \dots & 1 & \lambda_2 & & & & & \\
& & \vdots & & & & & & \vdots & & & & \vdots & & \vdots & & \\
& & & & & & & & & & & & \lambda_n & 0 & 0 & \dots & 0 & 0 \\
& & & & & & & & & & & & 1 & \lambda_n & 0 & \dots & 0 & 0 \\
& & 0 & & & & & & 0 & & & \dots & 0 & 1 & \lambda_n & \dots & 0 & 0 \\
& & & & & & & & & & & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
& & & & & & & & & & & & 0 & 0 & 0 & \dots & 1 & \lambda_n
\end{pmatrix}.$$

Même s'il n'est pas toujours possible d'obtenir une telle réduite de JORDAN, une matrice quelconque sera, en revanche, toujours semblable à une matrice diagonale par blocs, dont les blocs diagonaux sont des matrices compagnons :

$$\begin{pmatrix}
SMCa_{1,}d_1 & & & & 0 & & & \dots & & & 0 & & \\
& 0 & 0 & \dots & 0 & 0 & -a_{2,0} & & & & & & \\
& 1 & 0 & \dots & 0 & 0 & -a_{2,1} & & & & & & \\
0 & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \dots & & & 0 & & \\
& 0 & 0 & \dots & 1 & 0 & -a_{2,d_2-2} & & & & & & \\
& 0 & 0 & \dots & 0 & 1 & -a_{2,d_2-1} & & & & & & \\
\vdots & & & & \vdots & & & \vdots & & & \vdots & & \\
& & & & & & & & 0 & 0 & \dots & 0 & 0 & -a_{r,0} \\
& & & & & & & & 1 & 0 & \dots & 0 & 0 & -a_{r,1} \\
0 & & & & 0 & & & \dots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
& & & & & & & & 0 & 0 & \dots & 1 & 0 & -a_{r,d_r-2} \\
& & & & & & & & 0 & 0 & \dots & 0 & 1 & -a_{r,d_r-1}
\end{pmatrix}.$$

On constate que, même si les questions paraissent, au premier abord tout du moins, assez dissemblables, dans l'un et l'autre cas, celui des groupes abéliens et celui des matrices, on cherche à « décomposer« l'objet de départ en objets élémentaires puis à assurer que deux objets possédant la même décomposition sont en fait « identiques ».

Il conviendra bien évidemment de préciser ce que sont ces « décompositions » et ce que signifie être « identique« qui peut être précisé en « isomorphe« mais ne sera tout à fait précis que lorsqu'on aura bien spécifié de quel isomorphisme on veut parler.

La ressemblance entre les deux démarches évoquées ci-dessus n'est ni fortuite ni complètement formelle. Nous verrons en effet que les résultats les plus précis qu'on peut obtenir concernant les groupes abéliens sont en fait conséquences du théorème de structure (théorème II.10.5 ;) tandis que ceux concernant les matrices proviennent du théorème de réduction de FROBENIUS (théorème IV.11.5.) On pourra alors se convaincre que ces deux résultats sont des avatars du théorème B.6.13, de structure des modules de torsion sur un anneau principal.

On pourait donc tout à fait introduire le formalisme général, à savoir celui des A-modules et faire découler les résultats qu'on veut obtenir de résultats généraux sur ces objets. Cependant on préfère laisser découvrir de telles formulations générales après avoir étudié en détail les cas particuliers ; sans compter que les preuves des résultats généraux, exposés au paragraphe B.6 par exemple, nécéssitent l'usage d'outils plus techniques que dans les cas particuliers des paragraphes II.10 et IV.11. Le formalisme des A-modules cependant développé à l'appendice A, n'est en aucun cas un prérequis à la compréhension des résultats de ce cours, mais doit davantage apparaître comme une synthèse des énoncés précédents. En particulier il est recommandé d'étudier l'appendice A après avoir compris comment les constructions données dans les paragraphes I.6 et IV.1 se formalisent dans le cadre plus général de la théorie des A-modules.

Dans cette perspective, on trouvera nombre de titres de paragraphes prenant, par exemple, la forme :

« I.1 Structures de groupe, d'anneau … (cf. A.1) »

signifiant que le paragraphe A.1 peut être lu en parallèle avec le paragraphe I.1.

De la même manière :

« Théorème II.10.5 (cf. IV.11.5, B.6.13) »

signifie que ces trois énoncés sont de même nature.

I . −Groupes, anneaux, quelques constructions

I.0 . −Introduction

Ce chapitre (I,) pourra sembler être essentiellement constitué de révisions, ce qui est d'ailleurs le cas. on recommande néanmoins de porter une attention particulière aux paragraphes I.7, I.8 et I.9 qui introduisent à un formalisme dont il est très utile de disposer dans la suite. les notions de quotients et leur propriétés universelles en particulier sont indispensables à nombre de constructions ultérieures.

on a placé ci-après (I.0.1, I.0.2) les définitions de *magma* et de leur morphismes à seule fin de pouvoir y référer librement dans la suite, sans que ces objets n'aient un véritable intérêt en eux-mêmes eu égard au peu de résultats qu'on peut obtenir avec aussi peu de structure. Bien entendu les structures algébriques qui seront étudiées en détails au long de ce cours sont celles de groupes et d'anneaux exposées dans le paragraphe I.1 et suivants.

Les notations données en I.0.3 sont autant de conventions commodes utilisées dans tout ce texte.

I.0.1 . −Magma

Définition I.0.1.1 (Loi de composition) Pour un ensemble M on appelle *loi de composition* (ou *loi de composition interne* ou *loi interne*) $*$ sur M une application

$$* \,:\, M \times M \,\to\, M\,.$$

Le couple $(M, *)$ est appelé *magma*.

Définition I.0.1.2 (Associativité) On dit qu'une loi de composition $*$ sur un ensemble M est *associative* si

$$\forall x \in M,\ \forall y \in M,\ \forall z \in M,\ ((x * y) * z \,=\, x * (y * z))\,.$$

On peut alors parler pour $(M, *)$ de *magma associatif*.

Définition I.0.1.3 (Éléments particuliers) Soit $(M, *)$ un ensemble muni d'une loi de composition associative (magma associatif)

i) (**Élément neutre**)
Un *élément neutre* pour $(M, *)$ est un élément $\epsilon \,\in\, M$ tel que

$$\forall x \in M,\ (x * \epsilon \,=\, \epsilon * x \,=\, x)\,.$$

ii) (**Symétrique**)
Si M possède un élément neutre ϵ on dit qu'un élément $x \,\in\, M$ possède un symétrique pour la loi $*$ s'il existe $y \,\in\, M$ tel que

$$x * y \,=\, y * x \,=\, \epsilon\,.$$

Remarque I.0.1.4 Dans la suite on ne considérera que des magmas associatifs dans la mesure où ce seront les seuls que nous rencontrerons. Il se peut que certains énoncés puissent être formulés sans cette hypothèse mais nous ne cherchons pas le plus grand degré de généralité possible mais une présentation que nous espérons la plus claire et la plus lisible ainsi que la moins répétitive.

Proposition I.0.1.5 (Propriétés) *Soient $(M, *)$ un magma associatif.*

i) Si ϵ et ϵ' sont des éléments neutres de $(M, *)$ alors $\epsilon \,=\, \epsilon'$.

ii) Si $(M,*)$ possède un élément neutre et si y et z éléments de M sont des symétriques pour $x \in M$, $y = z$.

Remarque I.0.1.6 On pourra donc parler de L'élément neutre d'un magma lorsqu'il en possède un et du symétrique d'un élément lorsqu'il en possède un.

Exemple I.0.1.7 Si X est un ensemble l'ensemble M des applications de X dans lui-même est un magma associatif pour la loi $\circ$ de composition des applications. Il possède un élément neutre Id_X. En revanche un élément $f : X \to X$ de M n'a pas de symétrique en général puisque f n'est pas bijective en général. La loi $\circ$ n'est en général pas commutative non plus.

Définition I.0.1.8 (Commutativité) On dit qu'une loi de composition $*$ sur un ensemble M est *commutative* si

$$\forall x \in M,\ \forall y \in M,\ (x * y = y * x)\ .$$

I.0.2 . $-$morphisme

Définition I.0.2.1 (Morphisme homomorphisme) Étant donnés deux magmas

$$(M,*) \text{ et } (N,\cdot)$$

on dit qu'une application $f : M \to N$ est un *morphisme* ou *homomorphisme* de $(M,*)$ dans $(N,\cdot)$ si

$$\forall x \in M,\ \forall y \in M,\ (f(x*y) = f(x) \cdot f(y))\ .$$

Lemme I.0.2.2 *i) Pour tout magma $(M,*)$ l'identité Id_M est un morphisme du magma M dans lui-même.*

ii) Pour $(M,*_M)$, $(N,*_N)$ et $(P,*_P)$ des magmas, $f : M \to N$ et $g : N \to P$ des morphismes, le composé $g \circ f$ est un morphisme.

Définition I.0.2.3 Étant donnés deux magmas $(M,*)$ et $(N,\cdot)$, un morphisme $f : M \to N$ est un *isomorphisme* s'il existe un morphisme $g : N \to M$ tel que

$$g \circ f = \mathrm{Id}_M \text{ et } f \circ g = \mathrm{Id}_N\ .$$

On notera $\mathrm{Isom}(M,N)$ l'ensemble des isomorphismes de $(M,*)$ dans $(N,\cdot)$.

Proposition I.0.2.4 *Étant donnés deux magmas $(M,*)$ et $(N,\cdot)$, une application $f : M \to N$ est un isomorphisme si et seulement si c'est un morphisme bijectif.*

Preuve *: Si f est un isomorphisme, c'est par définition un morphisme qui est bijectif puisque possédant une application réciproque.*

Réciproquement si $f : M \to N$ est une application bijective, il existe une application

$$g : N \to M \text{ telle que } g \circ f = \mathrm{Id}_M \text{ et } f \circ g = \mathrm{Id}_N\ .$$

Alors :

$$\begin{array}{rcl} \forall (u,v) \in N \times N,\quad g(u \cdot v) & = & g\big[f[g(u)] \cdot f[g(v)]\big] \\ & = & g\big[f[g(u) * g(v)]\big] \\ & = & g(u) * g(v)\ . \end{array}$$

Définition I.0.2.5 Soit $(M, *)$ un magma.

i) (**Enndomorphismes**)
Un morphisme $f : M \to M$ de M dans lui-même est appelé *endomorphisme*. On note $\mathrm{End}(M)$ l'ensemble des endomorphismes de M.

ii) (**Automorphisme**)
Un morphisme $f : M \to M$ est un *automorphisme* si c'est à la fois un isomorphisme et un endomorphisme. Il revient au même, grâce à la proposition I.0.2.4, de dire que f est un endomorphisme bijectif. On note $\mathrm{Aut}(M)$ l'ensemble des automorphismes de M.

Exemple I.0.2.6 Pour un magma M, l'identité Id_M est un automorphisme de M.

Proposition I.0.2.7 *Soient $(M, *)$ un magma, E un ensemble et M^E l'ensemble des applications de E dans M. Pour tout $(f, g) \in M^E \times M^E$, on définit $f *_{M^E} g \in M^E$ de la manière suivante : Pour tout $x \in E$,*

$$f *_{M^E} g(x) := f(x) * g(x) .$$

i) $(M^E, *_{M^E})$ est un magma c'est-à-dire que $*_{M^E}$ est une loi de composition interne sur M^E.

ii) La loi $*_{M^E}$ est la seule loi sur l'ensemble M^E telle que, pour tout $x \in E$, l'application

$$M^E \to M , f \mapsto f(x)$$

soit un morphisme.

iii) Le magma $(M^E, *_{M^E})$ est associatif dès que $(M, *)$ l'est.

iv) Le magma $(M^E, *_{M^E})$ est commutatif dès que $(M, *)$ l'est.

v) Si $(M, *)$ possède un élément neutre ϵ, l'application

$$\epsilon_{M^E} : E \to M , x \mapsto \epsilon$$

est l'élément neutre de M^E.

Notation I.0.3 i) (**Triangle/carré commutatif**)
On dit que

$$\begin{array}{ccc} X & & \\ {\scriptstyle f}\downarrow & \searrow {\scriptstyle g} & \\ Y & \xrightarrow{h} & Z \end{array} \qquad \left(\text{resp.} \begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ Z & \xrightarrow{i} & T \end{array} \right)$$

est un triangle (resp ; un carré) *commutatif* si X, Y, Z et T sont des ensembles f, g, h, i des applications dont la sources et le but sont évidemment donnés par le sens des flèches et que

$$g = h \circ f \% (\text{resp. } i \circ g = h \circ f .)$$

ii) (**Diagramme commutatif**)

Un diagramme plus élaboré sera dit *commutatif* si tous les triangles et carrés le constituant le sont. Par exemple, dire que le diagramme

$$\begin{array}{ccccc} X & \xrightarrow{f} & X & & \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} & \searrow{\scriptstyle i} & \\ Z & \xrightarrow{j} & T & \xrightarrow{k} & U \end{array}$$

est commutatif signifie que

$$k \circ h = i\,,\ h \circ f = j \circ g$$

ce qui entraîne en particulier que

$$i \circ f = k \circ j \circ g\,.$$

Autrement dit encore, en termes de graphes, si deux parcours sont possibles d'un sommet à un autre, il sont équivalents au sens ou les composées des applications que l'ont trouve le long de l'un et l'autre parcours sont les mêmes.

iii) Bien entendu les ensembles en jeu peuvent bénéficier de structures supplémentaires (groupes I.1.1, anneaux I.1.6, modules A.1.1 ...) auquel cas les applications en jeu sont des morphismes (de groupes I.2.1, anneaux I.2.4, modules A.2.1 ....)

I.1 . –Structures de groupe, d'anneau ... (cf. A.1)

Définition I.1.1 (Groupe) Un *groupe* est un couple $(G, *)$ (le plus souvent simplement noté $G,$) où G est un ensemble et $* : G \times G \to G$ est une application appelée *loi de composition* vérifiant :

Gr_1) Pour tout triplet (x, y, z) d'éléments de G,

$$(x * y) * z = x * (y * z)\,,$$

on dit que la loi interne $*$ est *associative*.

Gr_2) Il existe un élément $e \in G$ appelé *élément neutre* de G tel que, pour tout $x \in G$, $x * e = e * x = x$.

Gr_3) Pour tout élément $x \in G$, il existe un élément $x' \in G$ appelé *symétrique* de x et tel que $x*x' = x'*x = e$.

Il revient au même de dire que $(G, *)$ est un magma associatif possédant un élément neutre et dans lequel tout élément possède un symétrique au sens des définitions du paragraphe I.0.1.

Les formulations « $(G, *)$ est un groupe » ou « $*$ munit G d'une *structure de groupe* » sont synonymes.

Exemple I.1.2 a) L'axiome I.1.1.Gr_2) entraîne qu'il n'existe aucune structure de groupe sur l'ensemble vide $\emptyset$. Un groupe est donc un ensemble possédant au moins 1 élément.

b) On peut définir une unique loi de composition qui donne à l'ensemble $\{\emptyset\}$ à un élément une structure de groupe :

$$\emptyset * \emptyset := \emptyset\,.$$

c) (**Le groupe** $\mathcal{S}(X)$)

Un des premiers groupes qu'on peut introduire, au sens où sa définition ne nécessite guère plus que les premiers axiomes de la théorie des ensembles, est le groupe $\mathcal{S}(E)$ des bijections d'un ensemble E muni de la loi $\circ$. C'est une partie du magma considéré dans l'exemple I.0.1.7, et précisément celle constituée des éléments qui ont un symétrique. Pour ne nécessiter que très peu de matériel pour être défini, ce groupe n'est cependant pas le plus aisé à étudier.

d) Si $\mathbb{K}$ est un corps et E un $\mathbb{K}$-espace vectoriel, l'ensemble $\mathrm{GL}(E)$ des applications linéaires bijectives de E dans lui-même (endomorphismes) est un groupe pour la loi de composition $\circ$. Si E est de dimension finie n, une base de E étant fixée, cette dernière définit un isomorphisme de $\mathbb{K}$-espace vectoriel $E \cong \mathbb{K}^n$ qui définit lui-même un isomorphisme de $\mathrm{GL}(E)$ sur le groupe $\mathrm{GL}_n(\mathbb{K})$ des matrices carrées $n \times n$ inversibles à coefficients dans $\mathbb{K}$.

Définition I.1.3 Étant donné un groupe $(G, *)$, si pour tout couple (x, y) d'éléments de G, $x * y = y * x$, on dira que G est *abélien* ou *commutatif*.

Dans ce cas on notera usuellement $+$ la loi interne et 0 l'élément neutre en référence au groupe abélien $(\mathbb{Z}, +)$.

Un groupe n'étant rien de plus (ni de moins d'ailleurs) qu'un magma associatif possédant un élément neutre et dans lequel tout élément possède un symétrique, la proposition I.0.1.5 vaut encore ici mutatis mutandis.

Proposition I.1.4 (Propriétés) *Soient $(G, *)$ un grouepe.*

i) Si ϵ et ϵ' sont des éléments neutres de $(G, *)$ alors $\epsilon = \epsilon'$.

ii) Si y et z éléments de E sont des symétriques pour $x \in E$, $y = z$.

Remarque I.1.5 On pourra donc parler de L'élément neutre d'un groupe et du symétrique d'un élément dans un groupe.

L'élément neutre est souvent noté 1 et même 0 dans le cas des groupes abéliens par analogie avec le groupe $(\mathbb{Z}, +)$. Le symétrique d'un élément x est usuellement noté x^{-1} et appelé *inverse* de x, voire $-x$ dans le cas d'un groupe abélien et appelé alors *opposé* de x.

Définition I.1.6 (Anneau) Un *anneau* est un triplet $(A, +, *)$ (le plus souvent noté $A,)$ tel que :

Ann$_1$) $(A, +)$ est un groupe abélien (cf. I.1.3 ;)
et la loi $* : A \times A \to A$ vérifie :

Ann$_2$) pour tout triplet (x, y, z) d'éléments de A,

$$x * (y * z) = (x * y) * z \, ,$$

(la loi $*$ est *associative*) ;

Ann$_3$) il existe un élément 1_A de A, appelé *élément neutre de* $(A, *)$, (souvent noté 1 lorsque le contexte est clair) tel que, pour tout $x \in A$,

$$1_A * x = x * 1_A = x \, ;$$

(on supposera toujours que $1_A \neq 0_A$ où 0_A est l'élément neutre pour la loi $+$;)

Ann$_4$) pour tout triplet (x, y, z) d'éléments de A,

$$x * (y + z) = x * y + x * z, \text{ et } (x + y) * z = x * z + y * z \, ,$$

(la loi $*$ est *distributive* par rapport à la loi $+$.)

On dira aussi que les lois $+$ et $*$ *donnent à l'ensemble A une structure d'anneau*.

La loi $+$ est usuellement appelée *addition* et la loi $*$ *multiplication*, par analogie avec l'anneau "modèle" $(\mathbb{Z}, +, *)$. Pour tout couple (x, y) d'éléments de A, on appellera $x + y$ et $x * y$ respectivement *somme* et *produit* de x et y.

On remarque que pour tout $x \in A$,

$$0_A * x \; = \; x * 0_A \; = \; 0_A \, .$$

On dit que 0_A est un *élément absorbant*.

Il est usuel de désigner le groupe abélien $(A, +)$ sous le terme de *groupe abélien sous-jacent* à l'anneau A.

Remarque I.1.7 On aurait pu formuler les axiomes I.1.6.Ann$_2$) et I.1.6.Ann$_3$) en disant que $(A, *)$ est un magma associatif possédant un élément neutre (cf. I.0.1.)

Définition I.1.8 (Anneau commutatif) Étant donné un anneau $(A, +, *)$, si

$$\forall (x, y) \in A \times A, \; x * y \; = \; y * x$$

on dira que la loi $*$ est *commutative* ou encore que l'anneau $(A, +, *)$ est un *anneau commutatif.*

Exemple I.1.9 a) L'ensemble $\mathbb{Z}$ des entiers relatifs muni de ses opérations $+$ et $*$ est un anneau commutatif.

b) La relation $\sim_n$ de *congruence* modulo n est compatible à la multiplication *i.e.* pour tout $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, et $(a', b') \in \mathbb{Z} \times \mathbb{Z}$, si

$$a \; \sim_n \; a' \text{ et } b \; \sim_n \; b' \, ,$$

alors

$$ab \; \sim_n \; a'b' \, .$$

Ce qui permet de définir une multiplication $*_{\mathbb{Z}/n\mathbb{Z}}$ sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes modulo n par :

$$\overline{a} *_{\mathbb{Z}/n\mathbb{Z}} \overline{b} \; = \; \overline{a * b} \, .$$

Le triplet $(\mathbb{Z}/n\mathbb{Z}, +_{\mathbb{Z}/n\mathbb{Z}}, *_{\mathbb{Z}/n\mathbb{Z}})$, le plus souvent noté $\mathbb{Z}/n\mathbb{Z}$, est un anneau commutatif.

$(\mathbb{Z}/n\mathbb{Z}, *)$ n'est jamais un groupe.

c) On dira qu'une fonction $f : \mathbb{R} \to \mathbb{R}$ est *à support compact*, s'il existe un intervalle $[a; b] \subset \mathbb{R}$ (*i.e.*un sous ensemble compact de $\mathbb{R}$,) tel que pour tout $x \notin [a; b]$, $f(x) = 0$. L'ensemble $\mathcal{C}$ des fonctions continues à support compact, muni de l'addition :

$$\begin{array}{rccl} + : & \mathcal{C} \times \mathcal{C} & \to & \mathcal{C} \\ & (f, g) & \mapsto & f + g \mid (f + g)(x) \; := \; f(x) + g(x) \, \forall x \in \mathbb{R}, \; ; \end{array}$$

et de la multiplication :

$$\begin{array}{rccl} * : & \mathcal{C} \times \mathcal{C} & \to & \mathcal{C} \\ & (f, g) & \mapsto & f * g \mid (f * g)(x) \; := \; f(x) * g(x) \, \forall x \in \mathbb{R}, \; ; \end{array}$$

n'est pas un anneau au sens de la définition I.1.6. En effet, $\mathcal{C}$ ne possède pas d'élément neutre pour la multiplication $*$ et ne vérifie donc pas l'axiome I.1.6.Ann$_3$).

Dans la suite de ce cours, nous n'aurons pas à considérer de tels objets, ce qui nous a incité à donner une définition d'anneau plus restrictive à laquelle satisferont tous les objets de notre étude. Les anneaux que nous considérerons sont parfois appelés *anneaux unifères*.

Les propositions I.0.1.5 et I.1.4 s'étendent encore au cas des anneaux. On peut en effet remarquer qu'un anneau est un magma à la fois pour sa loi d'addition $+$ ainsi que pour sa loi de multiplication $*$ si bien que :

Proposition I.1.10 (Propriétés) *Soient $(A, +, *)$ un Anneau. Le couple $(A, +)$ est en particulier un groupe abélien si bien que :*

i) L'élément neutre 0_A pour la loi $+$ est unique.

ii) Tout élément de A possède un unique opposé pour la loi $+$.

iii) L'élément neutre 1_A pour la loi $*$ est unique.

iv) Un élément de A possède au plus un symétrique pour la loi $*$ qu'on appellera inverse.

Définition I.1.11 (Élément inversible) Tous les éléments d'un anneau A différents de 0_A ne possédant pas nécessairement un inverse pour la loi $*$, on notera $A^\times$ l'ensemble des éléments de A *inversibles* pour $*$ *i.e.* ceux qui possèdent un inverse. On appelle parfois également *unité* un élément de $A^\times$.

Proposition I.1.12 *Si A est un anneau (resp. un anneau commutatif) $(A^\times, *)$ est un groupe (resp. un groupe abélien.)*

Exemple I.1.13 a) Le groupe $(\mathbb{Z}^\times, *)$ des inversibles de $\mathbb{Z}$ est $(\{-1, 1\}, *)$ qui est isomorphe au groupe abélien $\mathbb{Z}/2\mathbb{Z}$.

b) Pour un $\mathbb{K}$-espace vectoriel V l'ensemble $\mathrm{End}(V)$ des endomorphismes de V est un anneau dont le groupe des inversibles $\mathrm{End}(V)^\times$ est le *groupe linéaire* $\mathrm{GL}(V)$.

Définition I.1.14 (Anneau intègre) Si $(A, +, *)$ est un anneau tel que

$$\forall x \in A,\ \forall y \in A,\ (x * y = 0 \Rightarrow x = 0 \vee y = 0),$$

on dit que A est un anneau *intègre*.

Exemple I.1.15 Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ (cf. III.2.5.i),) sont intègres.

Définition I.1.16 (Corps) Un anneau commutatif $(A, +, *)$ est un *corps* si tous les éléments de A différents de 0_A possèdent un inverse pour la loi $*$; *i.e.* $A^\times = A \setminus \{0_A\}$.

Remarque I.1.17 Un corps est un anneau intègre mais la réciproque est fausse. En effet l'anneau $(\mathbb{Z}, +, *)$ est intègre mais n'est pas un corps.

Exemple I.1.18 Les ensembles $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de leurs lois usuelles sont des corps commutatifs ainsi que $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ pour p premier ; en revanche le corps des *quaternions de Hamilton* n'est pas commutatif.

I.2 . −Morphismes (cf. A.2)

Définition I.2.1 (Morphisme de groupes) Étant donnés des groupes

$$(G, *) \text{ et } (H, \cdot),$$

un *morphisme de groupes* (ou *homomorphisme de groupes*) est une application $f : G \to H$ telle que pour tout couple (x, y) d'éléments de G,

$$f(x * y) = f(x) \cdot f(y) .$$

On notera $\mathrm{Hom}_{\mathbf{Gr}}(G, H)$ (ou simplement $\mathrm{Hom}(G, H)$ si le contexte ne prête pas à confusion) l'ensemble des morphismes de G dans H. On verra également au paragraphe I.6 que la notation $\mathrm{Hom}_{\mathbb{Z}}(G, H)$ est tout à fait naturelle.

Remarque I.2.2 On constate que dans la définition ci-dessus aucune condition supplémentaire n'est exigée par rapport à un morphisme de magma (cf. I.0.2.1.)

Proposition I.2.3 (Propriétés des morphismes) *de groupes Étant donné un morphisme de groupe*

$$f : (G, *) \to (H, \cdot) \text{ avec } e_G(\text{resp. } e_H) \text{ l'élément neutre de } G(\text{resp. } H :)$$

i) $f(e_G) = e_H$;

ii) pour tout $x \in G$, *si* $y \in G$ *est son symétrique,* $f(y)$ *est le symétrique de* $f(x)$ *dans* H.

Définition I.2.4 (Morphisme d'anneaux) Une application

$$f : (A, +_A, *_A) \to (B, +_B, *_B)$$

est un *morphisme (homomorphisme) d'anneaux* (ou simplement *morphisme* si le contexte ne prête pas à confusion,) si :

Ann$_5$) $f : (A, +_A) \to (B, +_B)$ est un morphisme de groupes (cf. I.2.1.)

Ann$_6$) Pour tout couple (x, y) d'éléments de A,

$$f(x *_A y) = f(x) *_B f(y) .$$

Ann$_7$) $f(1_A) = 1_B$.

Cela revient à dire que f est un morphisme à la fois pour les magma $(A, +)$ et $(B, +)$ (cf. Ann$_5$),) ainsi que pour les magma $(A, *)$ et $(B, *)$ (cf. Ann$_6$).) Néanmoins on ajoute la condition Ann$_7$) dont on verra l'importance dans la suite.

On parlera, ici encore, du *morphisme de groupe sous-jacent* à f.

Lemme I.2.5 ((cf. A.2.3)) *i) Étant donné un ensemble* X, *si* $(X, +)$ *est un groupe (resp.* $(X+, *)$ *un anneau) l'identité* Id_X *de* X *et un morphisme de groupes (resp. d'anneaux.)*

ii) Soient

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

des applications (où X, Y et Z sont des ensembles) si $(X,+)$, $(Y,+)$ et $(Z,+)$ sont des groupes, f et g des morphismes de groupes (resp. $(X,+,*)$ $(Y,+,*)$ et $(Z,+,*)$ sont des anneaux, f et g des morphismes d'anneaux,) $g \circ f$ est un morphisme de groupes (resp. d'anneaux.)

Définition I.2.6 (Isomorphisme (cf. A.2.4)) Soit $f : X \to Y$ une application (où X et Y sont des ensembles,) si $(X,+)$ et $(Y,+)$ sont des groupes (resp. $(X,+,*)$ et $(Y,+,*)$ des anneaux,) f est un *isomorphisme* de groupes (resp. d'anneaux,) s'il existe un morphisme de groupes (resp. d'anneaux,)

$$g : Y \to X \text{ tel que } g \circ f = \mathrm{Id}_X \text{ et } f \circ g = \mathrm{Id}_Y .$$

On notera

$$\mathrm{Isom}_{\mathbf{Gr}}(X,Y) \text{(resp. } \mathrm{Isom}_{\mathbf{Ann}}(X,Y) \text{) ou simplement } \mathrm{Isom}(X,Y)$$

si le contexte ne prête pas à confusion, l'ensemble des isomorphismes de groupes (resp. d'anneaux) de X dans Y.

Proposition I.2.7 (Morphisme bijectif (cf. A.2.5)) *Étant donnée une application*

$$f : X \to Y \text{ (où } X \text{ et } Y \text{ sont des ensembles,)}$$

si $(X,+)$ et $(Y,+)$ sont des groupes (resp. $(X,+,*)$ et $(Y,+,*)$ des anneaux,) f est un isomorphisme de groupes (resp. d'anneaux,) si et seulement si f est un morphisme de groupe (resp. d'anneaux,) bijectif.

***Preuve** : Si f est un isomorphisme c'est une application bijective puisque possédant une application réciproque.*

Réciproquement si f est un morphisme bijectif (de groupes (resp. d'anneaux,)) c'est en particulier un morphisme du magma $(X,+)$ dans le magma $(Y,+)$ (resp. et du magma $(X,*)$ dans le magma $(Y,*)$.) Il découle alors de la proposition I.0.2.4 qu'il existe une application réciproque

$$\begin{array}{ll} g : Y \to X \text{ telle que} & \\ \forall (u,v) \in Y \times Y, & g(u+v) = g(u) + g(v) \\ \text{(resp.} & g(u+v) = g(u) + g(v) \quad \text{et} \quad g(u*v) = g(u) * g(v) \text{ .)} \end{array}$$

Dans le cas où $f : (X,+,*) \to (Y,+,*)$ est un morphisme d'anneaux reste uniquement à vérifier que g satisfait bien à l'axiome I.2.4.Ann$_7$) à savoir $g(1_Y) = 1_X$. Or f est un morphisme d'anneaux et g son application réciproque, si bien que $f(1_X) = 1_Y$ et $g \circ f = \mathrm{Id}_X$. Il s'ensuit que

$$1_X = g(f(1_X)) = g(1_Y) .$$

Définition I.2.8 (Endomorphisme/Automorphisme (cf. A.2.6)) Étant donné

$$\text{un groupe } (X,+) \ (mathresp \text{ un anneau } (X,+,*), \ )$$

i) On appelle *endomorphisme* de X un morphisme de groupes (resp. d'anneaux) de $(X,+)$ (resp. $(X,+,*)$) dans lui-même et on note

$$\mathrm{End}_{\mathbf{Gr}}(X) \text{ (resp. .End}_{\mathbf{Ann}}(X) \text{) ou simplement } \mathrm{End}(X) \text{ si le contexte ne prête pas à confusion}$$

l'ensemble des endomorphismes de X.

ii) On appelle *automorphisme* de X un isomorphisme de groupes (resp. d'anneaux) de $(X,+)$ (resp. $(X,+,*)$) dans lui-même et on note

$$\mathrm{Aut}_{\mathbf{Gr}}(X) \text{ (resp. .}\mathrm{Aut}_{\mathbf{Ann}}(X)\text{) ou simplement } \mathrm{Aut}(X)\text{si le contexte ne prête pas à confusion}$$

l'ensemble des automorphismes de X. Un automorphisme est donc un morphisme qui est à la fois un endomorphisme et un isomorphisme. À noter qu'en vertu de la proposition I.2.7, une application $f : X \to X$ est un automorphisme de groupe (resp. d'anneau) si et seulement si c'est un endomorphisme de groupe (resp. d'anneau) bijectif.

Exemple I.2.9 a) Pour $(X,+)$ un groupe (resp. $(X,+,*)$) un anneau, Id_X est un automorphisme.

b) On a construit, pour tout $n \in \mathbb{N}$, $n > 1$, un isomorphisme de groupes

$$\mathrm{Aut}_{\mathbf{Gr}}((\mathbb{Z}/n\mathbb{Z},+)) \cong (\mathbb{Z}/n\mathbb{Z},+,*)^\times \text{ donné par : } \tau \mapsto \tau(1)\ .$$

Lemme I.2.10 *i) Pour tout morphisme d'anneaux $Morf AB$, la restriction $f^\times := f_{|A^\times}$ de f à $A^\times$ est un morphisme de groupes à valeurs dans $B^\times$.*

ii) Pour tout anneau A,

$$\mathrm{Id}_A{}^\times = \mathrm{Id}_{A^\times}\ .$$

iii) Pour tous morphismes d'anneaux $f : A \to B$ et $g : B \to C$,

$$(g \circ f)^\times = g^\times \circ f^\times\ .$$

iv) Pour tout isomorphisme d'anneaux $f : A \to B$ d'isomorphisme réciproque $g : B \to A$,

$$f^\times : (A^\times,*) \to (B^\times,*)$$

est un isomorphisme de groupes d'isomorphisme réciproque $g^\times$.

I.3 . −Sous-groupes, sous-anneaux, idéaux (cf. A.3)

Définition I.3.1 (Sous-groupe) Une partie H d'un groupe $(G, *)$ est un *sous-groupe* si la restriction de $*$ à $H \times H$ donne à H une structure de groupe.

Exemple I.3.2 Étant donné un groupe $(G, *)$ d'élément neutre ϵ, les ensembles $\{\epsilon\}$ et G lui-même sont des sous-groupes de G.

Définition I.3.3 (Sous-annau) Étant donné un anneau $(A, +, *)$ un *sous-anneau* de A est une partie B de A telle que $1_A \in B$ et les restrictions respectives des lois $+$ et $*$ à B donnent à B une structure d'anneau.

En particulier $(B, +)$ est alors un sous-groupe de $(A, +)$.

Remarque I.3.4 i) Notons que l'axiome I.1.6.Ann$_1$) a en particulier pour conséquence que $(B, +)$ est un sous-groupe de $(A, +)$; ce qui entraîne, en particulier, que l'élément neutre 0_A de $(A, +)$ est aussi l'élément neutre de $(B, +)$ et que l'opposé d'un élément $x \in B$ est son opposé dans A.

ii) Notons que la condition $1_A \in B$, entraîne que 1_A est l'élément neutre pour la loi $*$ sur B et que tout inversible dans B est inversible dans A et que son inverse dans B est encore son inverse dans A. Il s'ensuit que $(B^\times, *)$ est alors un sous-groupe de $(A^\times, *)$.

iii) La condition $1_A \in B$ est automatiquement satisfaite dans le cas où A est intègre. En revanche si l'on considère un anneau R quelconque (même intègre) et $A := R \times R$ muni des lois

$$(x, y) +_A (z, t) := (x +_R z, y +_R t) \text{ et } (x, y) *_A (z, t) := (x *_R z, y *_R t),$$

(ce qu'on appelle la structure produit,) La partie

$$B := \{(x, 0), x \in R\}$$

est une partie qui est un sous-groupe pour la loi $+_A$ un sous-magma pour la loi $*_A$. B est même un anneau isomorphe à R dont l'élément neutre est $1_B = (1_R, 0)$ différent de lélément neutre $1_A = (1_R, 1_R)$ de A. On ne dira pas dans ce cas que B est un sous-anneau de A.

La condition $1_A \in B$ est à rapprocher de la condition I.2.4.Ann$_7$) et donne sa cohérence à un énoncé comme la proposition I.3.10.c).

Définition I.3.5 (Idéal) Étant donné un anneau commutatif $(A, +, *)$, une partie $\mathfrak{I} \subset A$ de A est un *idéal* si $\mathfrak{I}$ est un sous-groupe de $(A, +)$ tel que

$$\forall (a, x) \in A \times \mathfrak{I},\ a * x \in \mathfrak{I}\,.$$

Exemple I.3.6 a) Les sous-ensembles $\{0\}$, et A de A sont des idéaux de A. Ce sont les seuls idéaux de A si A est un corps.

b) Pour tout $a \in A$, le sous-ensemble

$$aA := \{a * b\,,\ b \in A\}$$

est un idéal de A.

c) Les idéaux de l'anneau $(\mathbb{Z}, +, *)$ sont exactement les sous-groupes du groupe $(\mathbb{Z}, +)$ c'est-à-dire les sous-ensemble de $\mathbb{Z}$ de la forme $d\mathbb{Z}$ avec $d \in \mathbb{Z}$.

Définition I.3.7 (Idéal stricte/propre) Un idéal $\mathfrak{I} \subset A$, est un *idéal strict* ou un *idéal propre* si $\mathfrak{I} \neq A$.

Définition I.3.8 Un idéal $\mathfrak{p} \subset A$ est *premier* si $\mathfrak{p} \neq A$ (*i.e.* $\mathfrak{p}$ est un idéal propre) et

$$\forall (a,b) \in A \times A,\ a * b \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \vee b \in \mathfrak{p}\ .$$

Proposition I.3.9 (Caractérisation des sous-groupes (cf. A.3.6)) *Étant donnés un groupe $(G,*)$ et $H \subset G$ une partie de G, les assertions suivantes sont équivalentes :*

a) H est un sous-groupe au sens de la définition I.3.1.

b) H est non vide et pour tout couple (x,y) d'éléments de H, $x * y^{-1} \in H$.

c) H est non vide, pour tout couple (x,y) d'éléments de H, $x * y \in H$ et pour tout $x \in H$, $x^{-1} \in H$.

d) La restriction

$$\mathrm{Id}_{G|H} : H \to G$$

de l'identité Id_G à H est un morphisme de groupes. Ceci signifie implicitement que H possède une structure de groupe.

Proposition I.3.10 (Caractérisation des sous-anneaux) *Étant donnés un anneau*

$$(A,+,*) \text{ et } B \subset A$$

une partie de A, les assertions suivantes sont équivalentes :

a) B est un sous-anneau au sens de la définition I.3.3.

b) B est non vide, $1_A \in B$, et pour tout couple (x,y) d'éléments de B,

$$y - x \in B \text{ et } x * y \in B\ .$$

c) La restriction

$$\mathrm{Id}_{A|B} : B \to A$$

de l'identité Id_A à B est un morphisme d'anneaux. Ceci signifie implicitement que B possède une structure d'anneau.

Proposition I.3.11 (Caractérisation des idéaux) *Une partie $\mathfrak{I}$ d'un anneau commutatif $(A,+,*)$ est un idéal de a si et seulement si $\mathfrak{I} \neq \emptyset$ et*

$$\forall (x,y) \in \mathfrak{I} \times \mathfrak{I},\ \forall (a,b) \in A \times A,\ a * x + b * y \in \mathfrak{I}\ .$$

Proposition I.3.12 (Le « treillis » des sous-groupes (resp. idéaux) (cf. A.3.9)) *Soit*

$$(X,+) \text{ un groupe } (\text{resp. } (X,+,*) \text{ un anneau },)(\text{resp. } (X,+,*) \text{ un anneau commutatif }.)$$

*i) (**Intersection**)*

Pour tout ensemble $\mathcal{Y}$ de sous-groupes (resp. de sous-anneaux) (resp. d'idéaux) de X, $\bigcap_{\mathcal{Y}} Y$ est un sous-groupe (resp. un idéal de X.)

*ii) (**Réunion**)*

Pour Y et Z deux sous-groupes (resp. deux sous-anneaux) (resp. deux idéaux) de X, $Y \cup Z$ est un sous-groupe (resp. un sous-anneau) (resp. un idéal) si et seulement si

$$Y \subset Z \text{ ou } Z \subset Y .$$

*iii) (**Union filtrante**)*

Étant donnée une suite $\left(Y_n\right)_{,n\in\mathbb{N}}$ de sous-groupes (resp. de sous-anneaux) (resp. d'idéaux) de X, telle que

$$\forall (p,q) \in \mathbb{N}\times\mathbb{N},\ \exists r \in \mathbb{N},\ Y_p \subset Y_r \text{ et } Y_q \subset Y_r$$

alors $\bigcap_{n\in\mathbb{N}} Y_n$ est un sous-groupe ((resp. un sous-anneau) (resp. un idéal) de X. C'est en particulier le cas si la suite $\left(Y_n\right)_{,n\in\mathbb{N}}$, est croissante pour l'inclusion.

I.4 . –Intersection, somme, engendrement (cf. A.4)

Corollaire I.4.1 (de la proposition I.3.12 (cf. A.4.1)) *Étant donné*

$$\begin{array}{rcl} & \textit{un groupe} & (X,+), \\ (\textit{resp.} & \textit{un anneau} & (X,+,*),\ ) \\ (\textit{resp.} & \textit{un anneau commutatif} & (X,+,*),\ ) \end{array}$$

et une partie $S \subset X$, *l'ensemble* $\mathcal{Y}$

$$\begin{array}{rcl} & \textit{des sous-ghroupes de} & X, \\ (\textit{resp.} & \textit{des sous-anneaux de} & X,\ ) \\ (\textit{resp.} & \textit{des idéaux de} & X,\ ) \end{array}$$

contenant S *possède un plus petit élément*

$$(S) \ = \ \bigcap_{Y \ \in \ \mathcal{Y}} Y \ .$$

Définition I.4.2 (Sous-groupe (resp. idéal,) engendré (cf. A.4.2)) Avec les notations du corollaire I.4.1, le sous-groupe (resp. sous-anneau) (resp. idéal) (S) s'appelle le *sous-groupe engendré*, (resp. le *sous-anneau engendré*,) (resp. l'*idéal engendré*,) par S. On dit que S est une *partie génératrice* de (S).

Exemple I.4.3 ((cf. A.4.3)) a) $< \emptyset > \ = \ \{0\}$ est le groupe à un élément ; l'idéal $(\emptyset)$ est l'idéal nul $\{0\}$.

b) Pour tout sous-groupe (resp. idéal) Y, $< Y > \ = \ Y$.

c) Le groupe abélien $(\mathbb{Z}/n\mathbb{Z},+)$ est engendré par $1_{\mathbb{Z}/n} \ = \ \overline{1}$ ou par tout élément inversible de l'anneau $(\mathbb{Z}/n\mathbb{Z},+,*)$.

Notation I.4.4 Si $a \ \in \ A$, l'idéal $(\{a\})$ engendré par le singleton $\{a\}$, est usuellement noté aA ou (a), et l'on a :

$$(\{a\}) \ = \ (a) \ = \ aA \ = \ \{a * b \ , \ b \ \in \ A\} \ .$$

un tel idéal est dit *principal* (cf. I.12.)

Lemme I.4.5 *Étant donné un idéal* $\mathfrak{I}$ *de* A, *les assertion suivantes sont équivalentes :*

a) $\mathfrak{I} \ = \ A$;

b) $\mathfrak{I} \cap A^{\times} \ \neq \ \emptyset$;

c) $\exists u \ \in \ A^{\times}, \ \mathfrak{I} \ = \ uA$.

d) $1 \ \in \ \mathfrak{I}$;

On peut donner une description explicite du sous-groupe (resp. de l'idéal) engendré. Ce serait aussi théoriquement possible pour le sous-anneau engendré mais ne présente pas de réel intérêt, dans le cadre de ce cours au moins.

Lemme I.4.6 ((cf. A.4.4)) *Si $(X,+)$ est un groupe le sous-groupe engendré par une partie $S \subset X$ est :*

$$< S >= \left\{ r \in \mathbb{N} \, ; \, \sum_{i=1}^{r} s_i \, , \, \forall 1 \leq i \leq r, \, s_i \in S \text{ ou } s_i^{-1} \in S \right\} . \qquad \textit{I.4.6.1}$$

Si $(X,+,*)$ est un anneau commutatif l'idéal engendré par une partie $S \subset X$ est :

$$(S) = \left\{ r \in \mathbb{N} \, ; \, \sum_{i=1}^{r} a_i * s_i \, , \, \forall 1 \leq i \leq r, \, s_i \in S \text{ et } a_i \in X \right\} . \qquad \textit{I.4.6.2}$$

Lemme I.4.7 (Somme (cf. A.4.5)) *Soit $(A,+)$ un groupe abélien, (resp. $(A,+,*)$) un anneau commutatif et $\mathcal{X}$ un ensemble de sous-groupes (resp. d'idéaux) de A.*

$$(\bigcup_{X \in \mathcal{X}} X) = \left\{ r \in \mathbb{N} \, ; \, \sum_{i} 1 r s_i \, , \, \forall 1 \leq i \leq r, \, \exists X \in \mathcal{X}, \, s_i \in X \right\} . \qquad \textit{I.4.7.1}$$

Autrement dit :

$$\forall x \in A, \, x \in (\bigcup_{X \in \mathcal{X}} X) \Leftrightarrow \exists r \in \mathbb{N}, \, \forall 1 \leq i \leq r, \, \exists X_i \in \mathcal{X}, \, \exists x_i \in X_i, \, x = \sum_{i=1}^{r} x_i \, . \qquad \textit{I.4.7.2}$$

Définition I.4.8 (Somme (cf. A.4.6)) Avec les notations du lemme I.4.7 :

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 I.4.7.2 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 groupe abélien A et deux sous-groupes B et C de A, si $A = B \oplus C$, on dit que B et C sont *supplémentaires* l'un de l'autre.

iv) (**Idéaux étrangers/comaximaux**)
Pour un anneau commutatif A et des idéaux $\mathfrak{I}$ et $\mathfrak{J}$ de A, on dit que $\mathfrak{I}$ et $\mathfrak{J}$ sont *comaximaux* ou *étrangers* si $A = \mathfrak{I} + \mathfrak{J}$.

Proposition I.4.9 (Propriété universelle des sommes directes (cf. A.4.7)) *Étant donnés*

$$\text{un groupe abélien } (A,+) \text{ et } \mathcal{X} \text{ une famille de sous-groupes}$$

telle que la somme

$$\sum_{X\,\in\,\mathcal{X}} X \;=\; \bigoplus_{X\,\in\,\mathcal{X}} X$$

est directte, pour tout ensemble de morphismes

$$\{f_X \,:\, X \;\to\; B\}\,,_{X\,\in\,\mathcal{X}}\,,$$

où B est un groupe abélien, il existe un unique morphisme

$$f \,:\, \bigoplus_{X\,\in\,\mathcal{X}} X \;\to\; B \text{ tel que } \forall X \in \mathcal{X},\; f_{|X} \;=\; f_X\;.$$

Preuve *: Ce résultat est en définitive plus long à énoncer qu'à démontrer.*

Remarque I.4.10 ((cf. A.4.8)) i) Il est bien sûr immédiat de vérifier que deux sous-groupes B et C d'un groupe abélien A sont supplémentaires l'un de l'autre si et seulement si

$$A \;=\; B \;+\; C \text{ et } B \,\cap\, C \;=\; \{0\}\;.$$

ii) La définition de supplémentaire donnée en I.4.8.iii) ne doit pas pour autant laisser penser que, pour un groupe abélien A quelconque et B un sous-groupe, un suplémentaire existe toujours. On se reportera au théorème I.9.15 qui assure que l'existence d'un supplémentaire pour B équivaut à l'existence d'une section pour la surjection canonique $A \;\to\; A/B$.

I.5 . −Images directes, images réciproques, noyaux (cf. A.5)

Proposition I.5.1 (Image réciproque/directe (cf. A.5.1)) *Soient X et Y des groupes (resp. des anneaux commutatifs) et $f : X \to Y$ un morphisme de groupes (resp. d'anneaux.)*

*i) (**Image réciproque**)*
Pour tout sous-groupe $Z \subset Y$ (resp. tout idéal $Z \subset Y$,) l'image réciproque $f^{-1}(Z)$ de Z par f, est un sous-groupe (distingué si Z l'est) (resp. un idéal) de X.
En particulier le noyau $\operatorname{Ker} f = f^{-1}(\{0\})$ est un sous-groupe distingué (resp. un idéal) de X.

*ii) (**Image directe**)*
Pour tout sous-groupe (resp. sous-anneau) $Z \subset X$ de X, l'image directe $f(Z)$ de Z par f, est un sous-groupe (resp. un sous-anneau) de Y.
En particulier l'image $\operatorname{Im} f = f(X)$ de f est un sous-groupe (resp. un sous-anneau de Y.)

Définition I.5.2 (Noyau/Image (cf. A.5.2)) Étant donné un morphisme de groupes $f : G \to H$, (resp. un morphisme d'anneaux $f : A \to B$,) ϵ_H étant l'élément neutre de H, (resp. 0 l'élément neutre de B, cette notation étant plus usuelle puisque $(B, +)$ est un groupe abélien,) on appelle

i) (**Noyau**)
noyau de f le sous-ensemble

$$\operatorname{Ker} f := f^{-1}(\{\epsilon\}_H) = \{x \in G\,;\, f(x) = \epsilon_H\} \text{ (resp. } .f^{-1}\{0\}\text{)},$$

ii) (**Image**)
image de f l'ensemble

$$\operatorname{Im} f := f(G) = \{y \in H\,;\, \exists x \in G,\ ,\ y = f(x)\} \text{ (resp. } f(A)\text{)}\,.$$

Remarque I.5.3 (Noyau/Image (cf. A.5.3)) Le noyau (resp. l'image) d'un morphisme d'anneaux est encore le noyau (resp. l'image) du morphisme de groupes sous-jacent.

Proposition I.5.4 (Injectivité/surjectivité (cf. A.5.5)) *Soit*

$$f : X \to Y \text{ un morphisme de groupes (resp. d'anneaux.)}$$

i) Le morphisme f est injectif si et seulement si $\operatorname{Ker} f = \{0\}$.

ii) Le morphisme f est surjectif si et seulement si $\operatorname{Im} f = Y$.

I.6 . −Compléments sur les groupes abéliens

Proposition I.6.1 *i) Étant donnés un groupe $(G, *)$ et un ensemble E, l'ensemble G^E des applications de E dans G muni de la loi induite (cf. I.0.2.7,) est un groupe (abélien si G l'est.) C'est la seule loi sur G^E telle que pour tout $x \in E$, l'évaluation en x,*

$$G^E \to G\ ,\ f \mapsto f(x)$$

soit un morphisme de groupes.

ii) Étant donnés un anneau $(A, +, *)$ et un ensemble E, l'ensemble A^E des applications de E dans A muni des lois induites (cf. I.0.2.7,) est un anneau (commutatif si A l'est.) Ce sont les seules lois sur A^E telles que pour tout $x \in E$, l'évaluation en x,

$$A^E \to G\ ,\ f \mapsto f(x)$$

soit un morphisme d'anneaux.

Preuve *: (cf. I.14.1.question 5).)*

Proposition I.6.2 *Pour deux groupes abéliens A et B, $\mathrm{Hom}_{\mathbf{Gr}}(A, B)$ est un sous-groupe commutatif du groupe B^A considéré en I.6.1.i).*

Preuve *: (cf. TD n° I, exercice B, question 1).)*

Proposition I.6.3 *Soit $(G, +)$ un groupe abélien (cf. I.1.3.)*

i) L'ensemble $\mathrm{End}_{\mathbf{Gr}}(G) = \mathrm{Hom}_{\mathbf{Gr}}(G, G)$ est un sous-groupe du groupe G^G (cf. I.6.1.i).)

Preuve *: (cf. A.2.12.)*

ii) Le triplet $(\mathrm{End}_{\mathbf{Gr}}(G), +, \circ)$ est un anneau.

Proposition I.6.4 *Pour tout groupe $(G, *)$ et tout élément $x \in G$, il existe un unique morphisme de groupes $\epsilon_x : (\mathbb{Z}, +) \to (G, *)$ tel que $\epsilon_x(1) = x$.*

Notation I.6.5 On note usuellement $x^n := \epsilon_x(n)$ pour tout $n \in \mathbb{Z}$.
Comme $\epsilon_x(-1)$ est l'inverse de $\epsilon_x(1) = x$, on notera x^{-1} l'inverse de x dans G.
Si G est abélien et sa loi interne notée $+$, on notera $n \cdot x := \epsilon_x(n)$.
Notons qu'ici, $\cdot$ n'est pas une loi interne et que par conséquent, les propriétés qui suivent ne sont pas tautologiques et demandent une démonstration, même si cette dernière est très élémentaire :

Proposition I.6.6

Étant donné un groupe abélien $(A, +)$,

il existe une unique loi externe $\cdot : \mathbb{Z} \times A \to A$ telle que pour tout couple d'entiers relatifs (p, q) et tout couple (x, y) d'éléments de A,

$$p \cdot (x +_A y) = p \cdot x +_A p \cdot y\ . \qquad \textit{I.6.6.1}$$

$$(p +_{\mathbb{Z}} q) \cdot x = p \cdot x +_A q \cdot x\ ; \qquad \textit{I.6.6.2}$$

$$(p *_{\mathbb{Z}} q) \cdot x \;=\; p \cdot (q \cdot x)\,; \qquad \textit{I.6.6.3}$$

$$1 \cdot x \;=\; x\,; \qquad \textit{I.6.6.4}$$

Il est nécessaire de faire l'hypothèse que $(A,+)$ est abélien, pour obtenir la propriété I.6.6.1.

***Preuve** : (cf. I.14.1.question 6).)*

Corollaire I.6.7 (de la proposition I.6.6) *Les propriétés énoncées dans la proposition I.6.6 ont, entre autres, pour conséquences, que pour tout $n \in \mathbb{Z}$ et tout $x \in A$,*

$$\begin{array}{rcl} n \cdot 0_A & = & 0_A \\ 0_{\mathbb{Z}} \cdot x & = & 0_A \\ (-n) \cdot x & = & -(n \cdot x) \;=\; n \cdot (-x)\,. \end{array} \qquad \textit{I.6.7.1}$$

Corollaire I.6.8 (de la proposition I.6.6) *Soit $(A,+)$ un groupe abélien.*

i) Pour tout $n \in \mathbb{Z}$, on note

$$\phi(n) \;:\; A \;\to\; A\,,\; x \;\mapsto\; n \cdot x\,.$$

On définit ainsi un morphisme d'anneaux

$$\phi \;:\; \mathbb{Z} \;\to\; \mathrm{End}_{\mathbf{Gr}}(A)\,.$$

***Preuve** : La propriété I.6.6.1 assure que $\phi(n)$ est bien un morphisme de groupes i.e. un élément de $\mathrm{End}_{\mathbf{Gr}}(A)$. La propriété I.6.6.2 assure alors que ϕ est un morphisme de groupes si bien que l'axiome I.2.4.Ann$_5$) est satisfait.*

Enfin les propriétés I.6.6.3 et I.6.6.4 correspondent respectivement aux axiomes I.2.4.Ann$_6$) et I.2.4.Ann$_7$).

ii) Réciproquement si $\phi \;:\; \mathbb{Z} \;\to\; \mathrm{End}_{\mathbf{Gr}}(A)$ est un morphisme d'anneaux, la loi externe

$$\cdot \;:\; \mathbb{Z} \times A \;\to\; A\,,\; (n,x) \;\mapsto\; \phi(n)(x)$$

vérifie les propriétés I.6.6.1 à I.6.6.4.

Remarque I.6.9 L'énoncé d'unicité dans la proposition I.6.6 permettrait d'établir l'unicité d'un morphisme $\phi \;:\; \mathbb{Z} \;\to\; EndoGrA$ pour peu qu'on établisse rigoureusement (ce qui n'est en réalité pas très difficile) que les procédés I.6.8.i) et I.6.8.ii) sont inverses l'un de l'autre. Cependant un résultat d'unicité plus général est établi à la proposition I.6.11.

Proposition I.6.10 *Pour deux groupes abéliens A et B, une application $f \;:\; A \;\to\; B$ est un morphisme de groupes si et seulement si*

$$\forall (x,y) \in A \times A,\; \forall (p,q) \in \mathbb{Z} \times \mathbb{Z},\; f(p \cdot x + q \cdot y) \;=\; p \cdot f(x) + q \cdot f(y)\,.$$

Proposition I.6.11 *Pour tout anneau $(A,+,*)$ (pas nécessairement commutatif) il existe un unique morphisme d'anneau $\mathbb{Z} \;\to\; A$ appelé morphisme structural de A.*

Preuve *:*

i) ***(Existence)***
— *Puisque* $(A,+,*)$ *est un anneau* $(A,+)$ *est en particulier un groupe abélien. Il s'ensuit, en vertu de la proposition I.6.6 qu'on dispose d'une loi externe* $\cdot\ :\ \mathbb{Z}\times A\ \to\ A$*. Il s'ensuit que*

$$\phi\ :\ \mathbb{Z}\ \to\ A\ ,\ n\ \mapsto\ n\cdot 1_A$$

est une application de $\mathbb{Z}$ *dans* A*.*
— *De plus la propriété I.6.6.2 assure que*

$$\forall (p,q)\in\mathbb{Z}\times\mathbb{Z},\ \phi(p+q)\ =\ (p+q)\cdot 1_A\ =\ p\cdot 1_A\ +_A\ q\cdot 1_A\ =\ \phi(p=\ +_A\phi(q)$$

si bien que ϕ *satisfait l'axiome I.2.4.Ann*$_5$*).*
— *La propriété I.6.6.4 assure que*

$$\phi(1)\ =\ 1\cdot 1_A\ =\ 1_A$$

si bien que l'axiome I.2.4.Ann$_7$*) est satisfait.*
— *On laisse le soin au lecteur de vérifier que l'axiome I.2.4.Ann*$_6$*) est satisfait.*

ii) ***(Unicité)***
Un morphisme d'anneaux $\phi\ :\ \mathbb{Z}\ \to\ A$ *est en particulier un morphisme de groupes et vérifie* $\phi(1)\ =\ 1_A$ *ce qui le détermine complètement.*

Remarque I.6.12 On aurait pu établir a priori l'unicité du morphisme structural (cf. I.6.11) et en déduire l'unicité de la loi externe sur un groupe abélien (cf. I.6.6) grâce à la correspondance établie au corollaire I.6.8.

Remarque I.6.13 Soit $(A,+,*)$ un anneau.
— On dispose du morphisme structural $\phi\ :\ \mathbb{Z}\ \to\ A$ grâce à la proposition I.6.11.
— De plus, en vertu du corollaire I.6.8.i), puisque $(A,+)$ est un groupe abélien, on dispose d'un morphisme d'anneaux $\psi\ :\ \mathbb{Z}\ \to\ \mathrm{End}_{\mathbf{Gr}}(A)$.
— Enfin pour tout $a\ \in\ A$, lapplication

$$\mu(a)\ :\ A\ \to\ A\ ,\ x\ \mapsto\ a*x$$

est un endomorphisme du groupe $(A,+)$ (cf. I.1.6.Ann$_4$).)
Le même axiome assure que

$$\mu\ :\ A\ \to\ \mathrm{End}_{\mathbf{Gr}}(A)$$

est un morphisme de groupes. Les axiomes I.1.6.Ann$_2$) et I.1.6.Ann$_3$) assurent que μ est un morphisme d'anneaux.
— Le composé

$$\mu\circ\phi\ :\ \mathbb{Z}\ \to\ \mathrm{End}_{\mathbf{Gr}}(A)$$

est alors un morphisme d'anneau qui ne peut-être que le morphisme structural ψ de $\mathrm{End}_{\mathbf{Gr}}(A)$ en vertu de la proposition I.6.11. On a alors le diagramme commutatif de morphismes d'anneaux :

$$\begin{array}{ccc}\mathbb{Z} & \xrightarrow{\ \phi\ } & A\\ & \searrow\psi & \big\downarrow\mu\\ & & \mathrm{End}_{\mathbf{Gr}}(A)\ .\end{array}\qquad\text{I.6.13.1}$$

Remarque I.6.14 Étant donné un idéal $\mathfrak{I}$ d'un anneau A, on peut définir une loi externe

$$\cdot \,:\, A \times \mathfrak{I} \,\to\, \mathfrak{I}\,,\ (a,x) \,\mapsto\, a\cdot x \,:=\, a * x$$

sur $\mathfrak{I}$. On remarque alors que, pour tout $(x,y) \,\in\, \mathfrak{I} \,\times\, \mathfrak{I}$, et tout $(a,b) \,\in\, A \,\times\, A$,

$$a\cdot(x+y) \,=\, a\cdot x \,+\, a\cdot y\,; \tag{I.6.14.1}$$

$$(a+b)\cdot x \,=\, a\cdot x \,+\, b\cdot x\,; \tag{I.6.14.2}$$

$$(a * b)\cdot x \,=\, a\cdot(b\cdot x)\,; \tag{I.6.14.3}$$

$$1\cdot x \,=\, x\,. \tag{I.6.14.4}$$

On avait déjà mis en évidence des propriétés très analogues à la proposition I.6.6, auxquelles on donnera un cadre général et formel avec la définition A.1.1.

On pourra alors constater qu'un idéal de A n'est, ni plus ni moins, qu'un sous-A-module de A (cf. A.3.1.)

I.7 . –Produits

La construction du *produit* est d'abord une construction ensembliste comme expliqué en I.7.0. À ce stade déjà le produit possède une *propriété universelle* I.7.0.iii) qui ne peut être formulée sans le secours des projections introduites en I.7.0.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 I.7.0 *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

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

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.*

Notation I.7.1 Dans tout le paragraphe I.7, on garde les notations de la proposition I.7.0, 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. I.0.1.1 ;)

i) (**groupe**)
$(E_k, *_k)$ est un *groupe* (éventuellement abélien) (cf. I.1.1) d'élément neutre ε_k ;

ii) (**anneau**)
$(E_k, +_k, *_k, 0_k, 1_k)$ est un anneau (éventuellement commutatif) (cf. I.1.6 ;)

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

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

Proposition I.7.2 (Existence de produits) *Si pour tout $1 \leq k \leq n$, E_k est muni de l'une des structures algébrique I.7.1.0) à I.7.1.iv) 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. I.0.2.1,) (resp. de groupes (cf. I.2.1,)) (resp. d'anneaux (cf. I.2.4,)) (resp. de A-modules (cf. A.2.1,)) (resp. de A-algèbres (cf. A.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 :

$$\begin{array}{c} \forall\big((x_1,\dots,x_n),(y_1,\dots,x_n)\big) \in P\times P, \\ (x_1,\dots,x_n)\ \dagger\ (y_1,\dots,y_n)\ =\ (x_1\dagger_1 y_1,\dots,x_n\dagger_n y_n)\,; \end{array} \qquad \text{I.7.2.1}$$

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

$$(\varepsilon_1,\dots,\varepsilon_n) \text{ est un l'élément neutre pour } \dagger\,; \qquad \text{I.7.2.2}$$

si

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

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

$$(y_1,\dots,y_n) \text{ est le symétrique de } (x_1,\dots,x_n) \text{ pour } \dagger\,; \qquad \text{I.7.2.3}$$

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 :

$$\begin{array}{c} \forall (x_1,\dots,x_n)\in P,\ \forall a\in a,\ A \\ a\cdot(x_1,\dots,x_n)\ =\ (a\cdot_1 x_1,\dots,a\cdot_n x_n)\,. \end{array} \qquad \text{I.7.2.4}$$

***Preuve** :*

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

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

est un morphisme, alors :

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

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 I.7.2.1. 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 I.7.2.2 et I.7.2.3 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

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

Il est en outre immédiat de vérifier, en utilisant par exemple l'expression I.7.2.1 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) (A**-modules**)*
Si

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

$(E_k, +_k)$ 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 I.7.2.4 ce qui est sans difficulté.

*iv) (A**-algèbres**)*
Si

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

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 $s \ : \ A \ \to \ P$ il faut disposer du résultat de la proposition I.7.4 pour les anneaux. En dépit du fait que celui-ci est présenté immédiatement après, aucun défaut de logique n'est cependant à déplorer.

Définition I.7.3 (Structure produit) Avec les notations I.7.1, 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 *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 I.7.4 (Propriété universelle du produit) *Pour tout ensemble F et tout*

$$n-\textit{uplet de morphismes, } f_k \,:\, F \,\to\, E_k \textit{ pour l'une des structures I.7.1.0) à I.7.1.iv)}$$

il existe un unique morphisme

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

Remarque I.7.4.1 i) Dès l'instant où l'on fait l'hypothèse que $\forall 1 \leq k \leq n,\ f_k \,:\, F \,\to\, E_k$ est un morphisme c'est qu'on suppose implicitement que F et E_k sont munis de la structure algébrique (I.7.1.0) à I.7.1.iv)) correspondante.

ii) Le résultat de cette proposition est, bien entendu, une particularisation au cas des morphismes de l'énoncé I.7.0.iii) ; ce dernier constituant d'ailleurs l'ingrédient principal de la preuve qui suit.

***Preuve* (*de la proposition I.7.4*)**: *Les $f_{k\ ,1\leq k\leq n}$ étant en particulier des applications il résulte de I.7.0.iii) qu'il existe une unique application*

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

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 I.7.4.1 (Le cas des A-algèbrs) On peut alors compléter le point I.7.2.iv) de la preuve de la proposition I.7.2 tout en justifiant aussi la proposition I.7.4 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 I.7.2.ii) une unique structure d'anneau telle que les $p_{k\ ,1\leq k\leq n}$ sont des morphismes. Les morphismes structuraux $s_k \,:\, A \,\to\, E_k$ étant, par définition, des morphismes d'anneaux, la proposition I.7.4 appliquée au cas des anneaux assure qu'il existe un unique morphisme d'anneaux

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

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 I.7.4 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 I.7.5 *Dans le cas où il existe E tel que*

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

définie par la proposition I.7.0.iv) est un isomorphisme pour l'une des structure I.7.1.0) à à I.7.1.iv), pour peu que $E^{[1;n]}$ soit muni de la structure considérée en I.0.2.7, (resp. I.6.1.i),) (resp. I.6.1.ii),) (resp. A.1.2.d) . . . .)

Proposition I.7.6 *Supposons que* $\forall 1 \leq k \leq n,\ (E_k, +_k)$ *(resp.* $(E_k, +_k, \cdot_k)$*) est un groupe (abélien) (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*

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

i) Pour tout $1 \leq k \leq n$ i_k *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. A*-module,)* P *est la somme directe (cf. I.4.8.ii),) (resp. (cf. A.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 *induit un isomorphisme* $E_k \cong \mathrm{Im}\, i_k$*,*

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

Remarque I.7.7 (Attention !) Dans la proposition I.7.6, ci-dessus on a uniquement considéré le cas des groupes et des A-modules mais on n'a pas de résultat analogue pour les anneaux ou les A-algèbnres (cf. I.14.4.)

Remarque I.7.8 Si l'on considère avec attention les propriétés universelles énoncées d'une part en I.7.4 et d'autre part en I.4.9 (resp. A.4.7,) 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 I.7.6 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. I.7.1.0)à I.7.1.iv)) 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.

I.8 . –Quotients

De même que pour le produit traité au paragraphe I.7, 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 I.8.0 (sur les relations d'équivalence) On rappelle que si E est un ensemble muni d'une relation d'équivalence $\sim$, 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 I.8.0.1 (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 I.8.0.2 *En particulier si $p : E \to F$ est une application surjective et que l'on définit la relation $\sim$ sur E, par :*

$$forallset(x,y)E \times Ex \sim y \Leftrightarrow p(x) = p(y), \qquad \text{I.8.0.2.1}$$

on a un unique diagramme commutatif :

$$\begin{array}{ccc} & & E \\ & \overset{\pi}{\swarrow} & \searrow p \\ E/\sim & \xrightarrow{g} & F \end{array} \qquad \text{I.8.0.2.2}$$

où g est bijective.

Lemme I.8.0.3 *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 I.8.0.2.1.*

Lemme I.8.0.4 *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 I.8.0.5 Les lemmes I.8.0.3 et I.8.0.4 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 I.8.0.2.1

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. I.1.1,) anneau (cf. I.1.6,) A-module (cf. A.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 I.8.0.1 mais mettant cette fois en jeu des morphismes pour la structure considérée.

On est alors amené à donner la définition suivante :

Définition I.8.1 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 I.8.2 De même si A est un anneau et M est muni dune loi externe $\cdot : A \times M \to M$, une relation d'équivalence $\sim$ sur M sera dite *compatible* à $\cdot$ si

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

Lemme I.8.3

Soit $(X, +)$ *un groupe abélien,*
(resp. $(X, +, *)$ *un anneau commutatif,)*
(resp. $(X, +, \cdot)$ *un A-module pour A un anneau commutatif fixé.)*

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 de $(X, +)$ (resp. un idéal de $(X, +, *)$) (resp un sous-A-module de $(X, +, \cdot)$,) 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-module) de X 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*

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

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

Par ailleurs :

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

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 A*-module en utilisant par exemple la caractérisation des sous-modules donnée en A.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 A*-module est laissé encore en exercice mais consiste en réalité formellement à remplacer* $*$ *par* $\cdot$ *dans la formule ci-dessus.*

Lemme I.8.4 *Étant donnés $(X,+)$ un groupe abélien, (resp. $(X,+,*)$ un anneau commutatif,) (resp. $(X,+,\cdot)$ un A-module pour A un anneau commutatif fixé) et Y $subset$ X un sous-groupe (resp. un idéal,) (resp. un sous-A-module,) 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*

$$\forall (x,y) \in X \times X,\ x \sim y \Leftrightarrow y - x \in \overline{0_X}\ . \qquad \text{I.8.4.1}$$

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 I.8.4.1. L'unicité est ainsi assurée et la formule I.8.4.1 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-module) entraînera que $\sim$ est compatible à $*$ (resp. $\cdot$.)

Définition I.8.5 Si $(X,+)$ est un groupe abélien (resp. $(X,+,*)$, un anneau commutatif,) (resp. $(X,+,\cdot)$ un A-module,) on dira simplement qu'une relation d'équivalence $\sim$ sur X est *compatible* à la structur de groupe (resp. d'anneau) (resp. de A-module) 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 I.8.3 et I.8.4 assurent que $^\sim$ est alors la relation d'équivalence donnée par un sous-groupe (resp. un idéal,) (resp. un sous-module) Y de X et la formule I.8.4.1.

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

Remarque I.8.6 Le caractère un peu disparate de la définition ci-dessus ainsi que des constructions dans les lemmes I.8.3 et I.8.4, tiens au fait qu'on n'a pas formulé ces énoncé dans le langage des A-module.

Si en effet on considère un groupe abélien $(X,+)$ muni de sa structure naturelle de $\mathbb{Z}$-module (cf. A.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. A.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. A.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. A.3.2.b).)

Remarque I.8.7 Dans les énoncés I.8.3 à I.8.6, 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.

Proposition I.8.8 (existence de quotients) *Soient $(X,+)$ un groupe abélien (resp. $(X,+,*)$ un anneau commutatif,) (resp. $(X,+,\cdot)$ un A-module,.) (resp. $(X,+,*,s : A \to X)$ une A-algèbre (cf. A.1.6.)) Étant donné un sous-groupe de $(X,+)$ (resp. un idéal de $(X,+,*)$) (resp. un sous-A-module de $(X,+,\cdot)$,) (resp. un idéal de $(X,+,*,s : A \to X)$,) Y ou, de manière équivalente (cf. I.8.3,) une relation d'équivalence compatible $\sim$ sur X, il existe une unique structure de groupe (resp. d'anneau,) (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. I.2.1,) (resp. d'anneaux (cf. I.2.4,)) (resp. de A-modules (cf. A.2.1,)) (resp. de A-algèbres (cf. A.2.2.))*

On a alors :

$$Y = \overline{0_X} = \operatorname{Ker} \pi\ l \qquad \text{I.8.8.1}$$

et

$$\forall (x,y) \in X \times X,\ x \sim y \Leftrightarrow y - x \in Y\ . \qquad \text{I.8.8.2}$$

Preuve *:*

Lemme I.8.8.1 *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 I.8.8.1, on peut munir $X/\sim$ d'une unique structure de groupe (resp. d'anneau.) Le cas des A-modules consiste à faire des vérifications analogues à celles du lemme I.8.8.1 dans le cas d'une loi externe ce qui est tout à fait formel et laissé en exercice.

Définition I.8.9 (Structure quotient) Pour un groupe abélien $(X, +)$ (resp. un anneau commutatif $(X, +, *)$,) (resp. un A-module $(X, +, \cdot)$,) (resp. une A-algèbre $(X, +, *, s : A \to X)$,) et Y un sous-groupe (resp. un idéal) (resp. un sous-A-module,) (resp. un idéal ;) on notera X/Y l'ensemble $X/\sim$ muni de la structure de groupe (resp. d'anneau,) (resp. de A-module,) (resp. de A-algèbre,) définie par la proposition I.8.8 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. *module quotient*) (resp. *algèbre quotient*.)

Remarque I.8.10 Dans la définition ci-dessus il s'agit en fait dans tous les cas de modules quotient, qui peuvent éventuellement disposer d'autres structures.

La proposition qui suit assure que les quotients au sens où on les a construits par la proposition I.8.8 l'on été de manière à « prolonger » la propriété universelle dont on disposait dans le cadre ensembliste (cf. I.8.0.1.) Il s'agit en quelque sorte de « remplacer » les applications par des morphismes pour la structure algébrique à laquelle on a affaire :

Proposition I.8.11 (Propriété universelle des quotients)

Soit	$(X, +)$	*un groupe abélien,*
(resp.	$(X, +, *)$	*un anneau commutatif,*)
(resp.	$(X, +, \cdot)$	*un A-module,*)
(resp.	$(X, +, *, s : A \to X)$	*une A-algèbre.*)

Pour tout morphisme $f : X \to Y$ (de groupes (cf. I.2.1,)) (d'anneaux (cf. I.2.4,)) (resp. de A-modules (cf. A.2.1,)) (resp. de A-algèbres (cf. A.2.2,)) et tout sous-groupe (resp. idéal,) (resp. sous- A-module,) (resp. idéal,) $Z \subset X$, notons

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

Alors les assertions suivantes sont équivalentes :

a)

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

b)

$$f(Z) \;=\; \{0_Y\} \textit{ i.e. } Z \;\subset\; \operatorname{Ker} f\ .$$

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

$$g \;:\; X/Z \;\to\; Y \textit{ tel que } f \;=\; g \circ \pi \;\textit{ où }\pi \;:\; X \;\to\; X/Z$$

est la surjection canonique.

De plus le morphisme g est injectif si et seulement si $Z \;=\; \operatorname{Ker} f$, 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 de la proposition I.8.3.

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

*iii) (**b)** $\Rightarrow$ **c**))*
On est alors dans la situation de l'implication I.8.0.1.a) entraîne I.8.0.1.b) si bien qu'il

$$\textit{existe une unique application } g \;:\; X/Z \;\to\; Y \textit{ tel que } f \;=\; g \circ \pi\ .$$

Reste donc uniquement à prouver que g est un morphisme :

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

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

f est π étant des morphismes.

*†) (**de groupes**)*
Cela découle immédiatement de $*$).

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

$$g(1_{X/Z}) \;=\; g[\pi(1_X)] \;=\; f(1_X) \;=\; 1_Y$$

puisque f et π sont des morphismes d'anneaux.

*§) (A-**modules**)*
D'après †), g est déjà un morphisme de groupes. De plus

$$\begin{array}{lrcl} \forall (a,u) \in A \times X/Z,\ \exists x \in X,\ u & = & \pi(x) & \\ \text{d'où} \qquad g(a \cdot_{X/Z} u) & = & g[a \cdot_{X/Z} \pi(x)] & \\ & = & g[\pi(a \cdot_X x)] & \\ & = & f(a \cdot_X x) & \\ & = & a \cdot_Y f(x) & \\ & = & a \cdot_Y g[\pi(x)] & \\ & = & a \cdot_Y g(u) & \end{array}$$

f et π étant des morphismes.

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

$$g \circ s_{X/Z} = g \circ \pi \circ s_X = f \circ s_X = s_Y .$$

*iv) (**Injectivité/surjectivité**)*
Sont des questions purement ensemblistes déjà établies en I.8.0.1.

Notation I.8.12 On dit souvent, dans la situation de la proposition I.8.11, que *f se factorise à travers X/Z* ou encore à travers π.

Corollaire I.8.13 *Étant donné un morphisme surjectif de groupes, (resp. d'anneaux,) (resp. de A-modules,) (resp. de A-algèbres,) $q : X \to Y$ il existe un unique isomorphisme de groupes (resp. anneaux,) (resp. A-modules,) (resp. A-algèbres,)*

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

Corollaire I.8.14 (Factorisation canonique des morphismes)

Étant donné un morphisme $f : X \to Y$ de groupes (resp. d'anneaux,) (resp. de A-modules,) (resp. de A-algèbres,)

il existe un unique isomorphisme de groupes (resp. d'anneaux,) (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 I.8.15 *Soient $(X,+)$ un groupe abélien (resp. $(X,+,\cdot)$ un A-module,) Y et Z des sous-groupes (resp. sous-A-modules de X.)*

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 :

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

ii) Si $Z \subset Y$, 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 :

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

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 :

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

Corollaire I.8.16 *Soient $(X, +)$ un groupe abélien (resp. $(X, +, *)$ un anneau commutatif,) (resp. $(X, +, \cdot)$ un A-module,) (resp. $(X, +, *, s : A \to X)$ une A-algèbre,) et $Y \subset X$ un sous-groupe (resp. un idéal,) (resp. un sous- A-module,) (resp. un idéal.)*

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

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

On a alors

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

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

Remarque I.8.17 Étant donné un groupe abélien (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- 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-A-module.)

L'équivalence a) $\Leftrightarrow$ c) a été établie dans la proposition I.8.3.

Le reste des vérifications est laissé au lecteur.

Remarque I.8.18 (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.

I.9 . –Suites exactes

Dans toute cette section (I.9,) A désigne un anneau commutatif (cf. I.1.8.)

Définition I.9.1 (Suite exacte courte) La notation

$$0 \to N \xrightarrow{i} X \xrightarrow{p} Q \to 0 \qquad \text{I.9.1.1}$$

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)

$$\mathrm{Im}\, i = \mathrm{Ker}\, p\,.$$

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 I.9.1.1 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 I.9.2 La donnée d'une suite exacte courte de groupes abéliens (resp. de A-modules,) équivaut à l'une des données équivalentes de la remarque I.8.17.

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

$$X/\mathrm{Ker}\, p = X/\mathrm{Im}\, i = X/N \cong Q \text{ (cf. I.8.14 .)}$$

Remarque I.9.3 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 I.9.4 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 I.3 (resp. A.3.)

Remarque I.9.5 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 I.9.6 a) Dans la proposition I.7.6 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 I.9.9 et I.9.10.

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 quotient 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'il n'existe pas de morphisme de groupes injectif de $\mathbb{Z}/d\mathbb{Z}$ dans $\mathbb{Z}$. Ainsi $\mathbb{Z}/d\mathbb{Z}$ ne peut en aucun cas se réaliser comme (ous-groupe (sous-$\mathbb{Z}$-module) de $\mathbb{Z}$. Il résulte de a) ou plus exactement de la proposition I.7.6 qu'on ne peut pas écrire $\mathbb{Z} = d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$.

Définition I.9.7 (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 I.9.8 (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 I.9.9 *Soient*

$$0 \to N \xrightarrow{i} X \xrightarrow{p} Q \to 0, \qquad \text{I.9.9.1}$$

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

$$s : Q \to X \text{ tel que } p \circ s = \mathrm{Id}_Q . \qquad \text{I.9.9.2}$$

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 I.9.8. 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 I.9.9.1 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 I.9.8. Or p étant surjectif, $\mathrm{Im}\, s \circ p = \mathrm{Im}\, s$.

v) Il résulte de ce qui précède que

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

est une suite exacte courte.

Proposition I.9.10 *Soient*

$$0 \to N \xrightarrow{i} X \xrightarrow{p} Q \to 0, \qquad \text{I.9.10.1}$$

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

$$r : X \to N \text{ tel que } r \circ i = \mathrm{Id}_N . \qquad \text{I.9.10.2}$$

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 I.9.8. 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 I.9.10.1 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 I.9.8,*

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

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 I.9.11 i) (**Section**)
Un morphisme $s : Q \to M$ comme en I.9.9.2 est usuellement appelée une *section* de p ou un *scindage de la suite exacte* et l'on di que la suite exacte courte I.9.9.1 est *scindée* ;

ii) (**Rétraction**)
On dit qu'un morphisme $r : M \to N$ come en I.9.10.2 est une *rétraction* de i et l'on dit que la suite exacte courte I.9.10.1 est *rétractée*.

En fait les proposition I.9.9 et I.9.10 montrent qu'une suite exacte courte de groupes abéliens (resp. A-modules,) est scindée si et seulement si elle est rétractée ;

Exemple I.9.12 a) Bien entendu les situations envisagées en I.7.6 fournissent des exemples de suites exactes courtes scindées (ou de manière équivalente rétractée.) Nous allons en fait voir à la proposition I.9.13, 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 $(u_1, \ldots, u_n)$ de F se complète en une base $(u_1, \ldots, u_m)$ 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 I.9.6.a) :

Proposition I.9.13 *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. I.9.9.2 ,)

(resp. une rétraction $r : M \to N$ de i (cf. I.9.10.2 ,)

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 :*

$$\begin{array}{rcl} \forall x \in M, \quad g[f(x)] & = & g[r(x), p(x)] \\ & = & i[r(x)] + p[p(x)] \\ & = & x \text{ (cf. I.9.9.iii) ou I.9.10.iii))} . \end{array}$$

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 I.9.14 La proposition I.9.13 ci-dessus est en fait un énoncé réciproque de la proposition I.7.6. En effet, avec les notations de la proposition I.7.6, les points I.7.6.i) à I.7.6.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 I.9.15 *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 I.9.16 (Facteur direct) Dans le cas où X et Y sont des groupes abéliens (resp. A-modules,) vérifiant les conditions équivalentes du théorème I.9.15, on dit que Y est un *facteur direct* de X. Ceci signifie que Y est <u>à la fois</u> un quotient et un sous-groupe (resp. sous- A-module,) de X.

Corollaire I.9.17 *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 I.9.18 *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

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

Le théorème qui suit permetra notamment de donner une preuve moins technique que dans le cas général du théorème II.10.5 dans le cas des groupes abéliens et des $\mathbb{K}[X]$-modules (E, u).

Théorème I.9.19 (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

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

I.10 . –Divisibilité et idéaux

Supposons donc dans cette section (I.10) que $(A, +, *)$ est un anneau commutatif (cf. I.1.8.)

Définition I.10.1 (Divisibilité) Pour tout couple $(a, b) \in A \times A$, on dit que a *divise* b ou que a est un *diviseur* de b ou encore que b est un *multiple* de a et l'on note $a|b$, s'il existe $c \in A$ tel que $a * c = b$.

Lemme I.10.2

$$\forall (a, b) \in A \times A,\ a|b \Leftrightarrow bA \subset aA \Leftrightarrow b \in aA$$

(où aA est l'idéal principal engendré par a .)

Remarque I.10.3 On sait que dans un anneau A, pour tout $a \in A$, $0 * a = 0$. Il en résulte que pour tout $a \in A$, $a|0$.

Par ailleurs

$$\forall a \in A,\ \forall b \in A,\ \forall c \in A,\ \big(a|b \text{ et } a|c \Rightarrow a|b + c\big) .$$

Remarque I.10.4 On remarque que la notion de divisibilité « correspond » à l'inclusion sur les idéaux laquelle est une relation d'ordre partielle. La réflexivité et la transitivité ne posent aucune difficulté pour la relation de divisibilité mais il n'est pas clair qu'elle soit antisymétrique : $a|b$ et $b|a$ n'implique pas forcément que $a = b$. Même dans $\mathbb{Z}$ $5| - 5$ et $-5|5$.

On verra comment on peut affiner cette notion de manière intéressante dans le paragraphe concernant les anneaux intègres (cf. I.11.)

Définition I.10.5 (Élément premier) Un élément $a \in A$ est dit *premier* si l'idéal principal engendré par a aA est premier (cf. I.3.8 ;) ce qui équivaut à dire que $a \notin A^\times$ (cf. I.4.5,) et

$$\forall (b, c) \in A \times A,\ a|b * c \Rightarrow a|b \vee a|c .$$

Définition I.10.6 (Élément irréductible) Un élément $a \in A$ est irréductible si $a \notin A^\times$ (a n'est pas inversible) et

$$\forall (b, c) \in A \times A,\ a = b * c \Rightarrow b \in A^\times \vee c \in A^\times .$$

Remarque I.10.7 Les définitions I.10.6 et I.10.5 sont présentées ici de manière tout à fait indépendantes l'une de l'autre contrairement à l'habitude qu'on peut en avoir en travaillant dans les anneaux usuels $\mathbb{Z}$ ou $\mathbb{K}[X]$. Ces deux notions n'entretiennent en effet de rapports étroit que si on fait des hypothèses sur l'anneau A. Un premier résultat sera obtenu dans la proposition I.11.1 en supposant que A est intègre. Finalement dans le cas des anneaux principaux le lemme de GAUSS et son corollaire le lemme d'EUCLIDE (cf. I.13.2.6,) permettra de « presque » confondre les deux notions d'irréductibilité et de primalité et de retrouver la définition usuelle de *nombre premier*

Notation I.10.8 On notera

$$\forall X \subset A\ ,\ \mathcal{D}(X) := \{y \in A\ ;\ \forall x \in X,\ y|x\} \text{ (resp. } \mathcal{M}(X) := \{y \in A\ ;\ \forall x \in X,\ x|y\} \text{)}$$

l'ensemble des diviseurs (resp. multiples) communs à tous les éléments de X.

De manière un peu abusive, on notera encore

$$\mathcal{D}(x, y) := \mathcal{D}(\{x, y\}) \text{ (resp. } \mathcal{M}(x, y) := \mathcal{M}(\{x, y\}) .)$$

Proposition I.10.9 *Pour tout* $X \subset A$,

$$d \in \mathcal{D}(X) \Leftrightarrow (X) \subset dA,$$

(où (X) *est l'idéal engendré par* X *défini en (cf. I.4.2.)*

Corollaire I.10.10 *Pour tout* $X \subset A$, $A^\times \subset \mathcal{D}(X)$.

Définition I.10.11 Pour $X \subset A$, si $\mathcal{D}(X) = A^\times$ on dit que les éléments de X sont *premiers entre eux (dans leur ensemble)*.

Remarque I.10.12 Cependant la situation que nous aurons souvent à considérer par la suite est celle où deux éléments x et y de A sont premiers entre eux *i.e.*où $\mathcal{D}(\{x,y\}) = A^\times$ ou vien où $X \subset A$ est constitué d'éléments *deux à deux premiers entre eux* c'est-à-dire

$$\forall (x,y) \in X \times X,\ \mathcal{D}(\{x,y\}) = A^\times .$$

Bien sûr que cette situation entraîne que les éléments de X sont premiers entre eux dans leur ensemble mais le fait que les éléments de X sont deux à deux premiers entre eux est une hypothèse plus forte. Les éléments 2, 5, 6 de $\mathbb{Z}$ sont premiers entre eux dans leur ensemble mais pas deux à deux premiers entre eux.

Définition I.10.13 (PGCD PPCM) Étant donné un ensemble $X \subset A$, on appelle *plus grand commun diviseur* ou *PGCD* (resp. *plus petit commun multiple* ou *PPCM*)

$$\text{un plus grand élément de } \mathcal{D}(X) (\text{resp. un plus petit élément de } \mathcal{M}(X),\ )$$

au sens de la relation $|$ bien entendu, autrement dit, un élément $d \in \mathcal{D}(X)$ (resp. $m \in \mathcal{M}(X)$) tel que :

$$\forall a \in X,\ d|a \text{ et } \forall b \in \mathcal{D}(X),\ b|d \text{ (resp. } \forall a \in X,\ a|m \text{ et } \forall b \in \mathcal{M}(X),\ m|b\ .) \qquad \text{I.10.13.1}$$

Remarque I.10.14 La définition I.10.13 peut sembler un peu abusive au sens où nous n'avons parlé de *plus grand élément* ou de *plus petit élément* que pour une relation d'ordre. Nous verrons en outre que la relation $\cdot|\cdot$ n'est pas « vraiment » une relation d'ordre (cf. I.11.6,) met en particulier en défaut le fait que de tels éléments, s'ils existent, (ce que nous n'avons pas encore établi mais qui le sera pour les anneaux principaux (cf. I.13.1.3 et I.13.1.6) est unique.

Lemme I.10.15 *Étant donné une partie* $X \subset A$, *tous les PGCD (resp. PPCM) de* X *s'ils existent engendrent un même idéal (cf. I.4.4.)*

Notation I.10.16 Le lemme ci-dessus peux motiver les notations suivantes : Pour $X \subset A$ d (resp. m) un PGCD (resp. PPCM) de X, on notera :

$$\bigwedge X := dA \text{ et } \mathrm{PPCM}(X) := mA\ . \qquad \text{I.10.16.1}$$

Pour tout $(x,y) \in A \times A$, on notera :

$$x \wedge y := \bigwedge \{x,y\} \text{ et } \mathrm{PPCM}(x,y) = \mathrm{PPCM}(\{x,y\})\ . \qquad \text{I.10.16.2}$$

I.11 . –Éléments remarquables d'un anneau intègre

Dans cette section (I.11,) $(A, +, *)$ est un anneau commutatif intègre (cf. I.1.8, I.1.14.)

Proposition I.11.1 *Dans un anneau commutatif intègre A, tout élément premier (cf. I.10.5,) non nul est irréductible (cf. I.10.6.)*

Définition I.11.2 (Éléments associés) Pour $(a, b) \in A \times A$, on dit que b est *associé* à a s'il existe un élément inversible $u \in A^\times$, tel que $b = u * a$.

Lemme I.11.3 *La relation d'association est une relation déquivalence.*

Lemme I.11.4 *Pour tout $(a, b) \in A \times A$, les assertions suivantes sont équivalentes :*

a) $a|b$ et $b|a$;

b) $aA = bA$;

c) $\exists u \in A^\times,\ b = a * u$;

d) $\exists u \in A^\times,\ a = b * u$;

e) a *et* b *sont associés.*

Remarque I.11.5 L'équivalence entre I.11.4.b) et I.11.4.e) peut se reformuler en disant qu'on a une bijection naturelle entre les classes d'équivalences pour la relation d'association et les idéaux principaux de A.

Remarque I.11.6 Bien qu'elle soit réflexive et transitive, la relation $|$ (divise) n'est pas « vraiment » *antisymétrique*, fait qu'on ne peut pas dire que $|$ est une relation d'ordre.

Cependant la relation d'association est une *relation d'équivalence*. On dira dans ce cas que $|$ est une relation de *pré-ordre*. Ce pré-ordre n'est pas total, en effet on ne peut pas toujours comparer deux éléments de $\mathbb{Z}$ du point de vue de la divisibilité. Par exemple, on n'a ni $3|5$ ni $5|3$.

Lemme I.11.7 *L'élément neutre pour $+$ 0 est le plus grand élément pour $|$ tandis que tout élément $u \in A^\times$ est un plus petit élément pour $|$.*

Remarque I.11.7.1 On constate d'ores et déjà que $|$ ne se comporte pas tout à fait comme une relation d'ordre puisqu'il n'y a pas unicité d'un plus petit élément.

Lemme I.11.8 *Pour tout $X \subset A$, les PGCD de X (resp. PPCM de X) forment une classe d'équivalence pour la relation d'association.*

Remarque I.11.9 On n'a pas parlé jusqu'ici du PGCD ni du PPCM mais d'un PGCD ou d'un PPCM à cause du défaut d'unicité constaté dans le lemme ci-dessus. Ce dernier énoncé montre en outre que de toute évidence, le « bon objet » à considérer n'est pas un PGCD ou un PPCM mais la classe d'association des PGCD (resp PPCM) qui, pour le coup, et d'après le lemme I.11.8 est unique. Cette classe d'association elle-même ne semble pourtant pas être un objet très utilisable sauf à remarquer qu'on peut la représenter par un objet tout à fait maniable à savoir un idéal. Grâce au lemme I.11.4 on sait en effet que tous les PGCD (resp. PPCM) engendrent le même idéal.

Le défaut majeur de ces notions, dans ce cadre trop général, est de ne pas jouir d'un résultat d'existence. Un cadre confortable pour s'y intéresser est celui des anneaux principaux (cf. I.13,) à moins qu'on introduise la notion d'anneau factoriel, ce qui ne sera pas fait dans le cadre de ce cours.

I.12 . −Anneaux principaux

Définition I.12.1 (Idéal principal) Un idéal aA pour $a \in A$ comme dans l'exemple I.3.6.b), est dit *principal*. On dit que l'idéal aA est *engendré* par a ou encore que a est un *générateur* de l'idéal aA.

Définition I.12.2 (Anneau principal) Un anneau commutatif A est *principal* s'il est intègre (cf. I.1.14,) et si tout idéal de A est principal.

Exemple I.12.3 a) Un corps est un anneau principal, puisqu'on a déjà remarqué (cf. I.3.6.a),) que ses seuls idéaux sont $\{0\}$ et lui-même qui sont évidemment principaux. Néanmoins cet exemple ne présente qu'un intérêt très limité du point de vue de l'arithmétique.

b) La proposition I.13.6.4 nous permettra de donner un certain nombre d'exemple d'anneaux principaux qui ne sont pas des corps à savoir les anneaux euclidiens :

Exemple I.12.4 D'autres exemples d'anneaux principaux sont donnés par :

a) (**L'anneau des entiers relatifs**)
l'anneau $\mathbb{Z}$. des entiers relatifs ;

b) (**Les anneaux de polynômes**)
les anneaux de polynômes $\mathbb{K}[X]$ (cf. III.4.4,) où κ est un corps ;

c) (**Les entiers de GAUSS**)
l'anneau des entiers de GAUSS ;

d) (**Les entiers d'Eisenstein**)
et l'anneau des entiers d'Eisenstein.

I.13 . −Arithmétique des anneaux principaux

I.13.1 . −Existence de PGCD et de PPCM dans les anneaux principaux

Dans la suite, c'est-à-dire dans les paragraphes I.13.1 à I.13.5 A est un anneau principal.

Lemme I.13.1.1 *Pour tout $X \subset A$, il existe $d \in A$, tel que $(X) = dA$.*

Lemme I.13.1.2 *Pour $X \subset A$, si d est un générateur de (X), i.e.si $(X) = dA$, il existe $n \in \mathbb{N}$, $a_{i\ ,1\leq i\leq n} \in A$ et $x_{i\ ,1\leq i\leq n} \in X$ tels que*

$$d = \sum_{i=1}^{n} a_i * x_i \ .$$

Proposition I.13.1.3 (PGCD) *Soit $X \subset A$ une partie de A (qui peut être finie ou non.)*

i) X admet un PGCD (cf. I.10.13 ;)

ii) $d \in A$ est un PGCD de X si et seulement si $(X) = dA$;

iii) pour tout PGCD d de X :

$$\exists n \in \mathbb{N},\ \forall 1 \leq i \leq n,\ \left(\exists x_i \in X,\ \exists a_i \in A,\ \right),\ d = \sum_{i=1}^{n} a_i * x_i \ . \qquad 1$$

Définition I.13.1.4 (Identité de BÉZOUT) La formule I.13.1.3.iii).1 est appelée *identité de Bézout* et les éléments $a_{i\ ,1\leq i\leq n} \in A$ *coefficients de Bézout*.

Remarque I.13.1.5 La proposition I.13.1.3 montre en particulier que, dans le cas où A est un anneau principal et $X \subset A$, les notations (X) introduite en I.4.1 et $\bigwedge X$ introduite en I.10.16.1, sont redondantes au sens où elles désignent le même objet, à savoir l'idéal engendré par X. Cependant dans le cas où A est principal, cet idéal est aussi celui engendré par n'importe quel PGCD des éléments de X.

On pourrait aussi sans grande difficulté constater que les éléments de X eux-mêmes sont bien moins déterminants que les idéaux qu'ils engendrent. En effet, si on remplace les éléments de X par des éléments qui leurs sont associés, l'idéal (X) n'est pas changé et partant l'ensemble des PGCD non plus.

Proposition I.13.1.6 (PPCM) *Pour tout $X \subset A$, X admet un PPCM et les PPCM de X sont les générateurs de l'idéal*

$$\cap(X) := \bigcap x \in XxA \ .$$

I.13.2 . −Théorème de BÉZOUT,

lemme de GAUSS,
lemme d'EUCLIDE

On insiste que dans cettte section (I.13.2) l'anneau A est principal. Certains résultats comme le lemme de GAUSS (cf. I.13.2.3,) le lemme d'EUCLIDE (cf. I.13.2.6,) pourrraient être obtenus dans un cadre plus général, à savoir celui des anneaux factoriels, mais l'hypothèse A principal est indispensable pour disposer du théorème de BÉZOUT I.13.2.1. Dans la mesure où, dans ce paragraphe les résultas qui suivent sont des corollaires de ce premier théorème, il est évident que la stratégie de démonstration devra être tout à fait différente pour les obtenir dans un autre cadre que celui des anneaux principaux.

Théorème I.13.2.1 (de BÉZOUT) *Pour tout $X \subset A$, les assertions suivantes sont équivalentes :*

a) $\mathcal{D}(X) = A^\times$ *c'est-à-dire que les éléments de X sont premiers entre eux dans leur ensemble (cf. I.10.11.)*

b)

$$(X) = \bigwedge X = A\,.$$

c) L'élément 1 *de A est un PGCD pour X.*

d) Il existe un entiers $n \in \mathbb{N}$, un n-uplet $a_{i\ ,1\leq i\leq n} \in A$, un n-uplet $x_{i\ ,1\leq i\leq n} \in X$ tels que

$$\sum_{i=1}^{n} a_i * x_i = 1\,.$$

Corollaire I.13.2.2 (Idéaux comaximau) *Deux idéaux $\mathfrak{I}$ et $\mathfrak{J}$ de A sont comaximaux (cf. I.4.8.iv),) si et seulement si pour tout couple $(x, y) \in A \times A$ tel que $\mathfrak{I} = xA$ et $\mathfrak{J} = yA$ x et y sont premiers entre eux.*

Théorème I.13.2.3 (Lemme de GAUSS) *Pour tout $(a, b, c) \in A \times A \times A$, si a et b sont premiers entre eux, et $a|bc$ alors $a|c$.*

Remarque I.13.2.4 Il se peut que dans la littérature, le lemme de GAUSSne soit pas habituellement déduit du théorème de BÉZOUT mais plutôt du théorème fondamental de l'arithmétique (théorème I.13.5.3.) Il pourrait alors sembler surprenant de procéder comme on l'a fait. Pour expliquer cette différence d'approche, il faudrait mentionner qu'il existe des anneaux dans lesquels le théorème I.13.5.3 est satisfait mais dans lesquels le théorème de BÉZOUT I.13.2.1 ne l'est pas. Dans de tels anneaux dits *factoriels* le lemme de GAUSSest encore vérifié mais ne peut alors se déduire du théorème de BÉZOUT. Pour donner une quelconque pertinence aux considérations qui précède il faudrait encore montrer qu'il existe vraiment des anneaux factoriels qui n'ont pas la propriété de BÉZOUT, ce qui est effectivement le cas.

Lemme I.13.2.5 *Pour tout $p \in A$ irréductible et tout $a \in A$, si p ne divise pas a, a et p sont premiers entre eux.*

Théorème I.13.2.6 (Lemme d'EUCLIDE) *Dans un anneau principal A, tout éléments irréductibles (cf. I.10.6,) est premier (cf. I.10.5.)*

Remarque I.13.2.7 Comme on a supposé dans cette section que A est intègre, tout élément premier non nul de A est irréductible (cf. I.11.1,). Le lemme d'EUCLIDE ci-dessus montre donc que les notions de premiers et d'irréductibles coïncident peu ou prou, et correspondent à l'idée que l'on a depuis longtemps des nombres premiers.

Proposition I.13.2.8 *Étant donné un anneau principal A qui n'est pas un corps, pour tout élément $p \in A$, le quotient A/pA est un corps si et seulement si p est irréductible (cf. I.10.6.)*

I.13.3 . −Arithmétique modulaire

Proposition I.13.3.1 *Étant donné un anneau principal A et $p \in A$, si p est irréductible l'anneau quotient A/Ap est un corps. La réciproque est vraie, pour peu que A ne soit pas déjà lui-même un corps.*

I.13.4 . −Le théorème chinois des restes

Notation I.13.4.1 i) Pour tout idéal I de A, on notera $\pi_I : A \to A/I$ la surjection canonique

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

ii)
$$\forall 1 \leq k \leq n,\ p_k\ :\ \prod_j 1nA/I_j\ \to\ A/I_k$$

la projection du produit sur le $k^{\text{ième}}$ facteur (cf. I.7.1,)

iii) Il existe alors un unique morphisme d'anneaux

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

caractérisé par le fait que
$$\forall 1 \leq k \leq n,\ p_k\ \circ\ \pi_{\mathcal{I}}\ =\ \pi_{I_k}$$

Plus explicitement, pour tout $x \in A$,

$$\pi_{\mathcal{I}}(x)\ =\ \big(\pi_{I_1}(x), \ldots, \pi_{I_n}(x)\big)\ .$$

iv) On simplifiera autant que possible la notation π_{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
$$\psi_{\mathcal{I}} \text{ ou simplement } \psi\ :\ A\ \to\ A/\big(\bigcap_{1\leq j\leq n} A/I_j\big)$$

la surjection canonique.

On peut synthétiser ces notations dans le diagramme suivant :

$$\begin{array}{ccc} A & \xrightarrow{\pi_{\mathcal{I}}} & \prod_j 1nA/I_j \\ {\scriptstyle \psi_{\mathcal{I}}}\big\downarrow & \searrow \pi_{I_k} & \big\downarrow {\scriptstyle p_k} \\ A/\big(\bigcap_{1\leq j\leq n} A/I_j\big) & & A/I_k\ . \end{array} \qquad \text{I.13.4.1.1}$$

Proposition I.13.4.2 *Soient $n \in \mathbb{N}, \mathcal{I} := I_{1\ ,k\leq 1\leq n}$ un n-uplet d'idéaux de A.*

i) Il existe un unique morphisme injectif d'anneaux

$$\gamma\ :\ A/\big(\bigcap_{1\leq j\leq n} A/I_j\big)\ \to\ \prod_j 1nA/I_j\ \textit{ tel que }\ \gamma\ \circ\ \psi\ =\ \pi\ .$$

ii) Si les idéaux $I_{k\ ,1\leq k\leq n}$ sont deux à deux comaximaux (cf. I.4.8.iv),) π est surjective et partant γ est surjective et donc un isomorphisme.

Remarque I.13.4.3 Une lecture attentive montrera que dans la preuve de la proposition I.13.4.2 il n'a jamais été fait usage du fait que A est un anneau principal ni d'aucun des résultats que nous avons établis pour ce type d'anneau (cf. TD n° II, exercice B.)

La particularité du cas des anneaux principaux va consister à traduire en termes de PGCD l'hypothèse que les idéaux sont deux à deux comaximaux grâce au corollaire I.13.2.2, et conduira à la forme suivante (théorème I.13.4.4,) plus usuelle, du théorème chinois des restes. Des formulations plus particulières encores dans le cas de l'anneau $\mathbb{Z}$ (resp. de l'anneau $\mathbb{K}[X]$) pourront être données .

Théorème I.13.4.4 *Soient $n \in \mathbb{N}$, $a_{k\ ,1\leq k\leq n}$ des éléments de A et m un PPcM (cf. I.13.1.6,) des $a_{k\ ,1\leq k\leq n}$.*

Pour tout $1 \leq k \leq n$, on note $\pi_k : A \to A/a_kA$ (qui correspond à la notation donnée en I.13.4.1.iv) pour peu qu'on définisse l'idéal I_k par $I_k := a_kA$. Il s'en déduit comme en I.13.4.1.iii) un morphisme d'anneaux

$$\pi : A \to \prod_{j=1}^{n} A/a_jA = \prod_{j} 1nA/I_j .$$

Notons encore $\psi : A \to A/mA$ la surjection canonique (qui n'est autre que le morphisme ψ défini en I.13.4.1.v) dans la mesure où

$$mA = \bigcap_{1\leq j\leq n} a_jA$$

(cf. I.13.1.6.))

Alors :

i) Il existe un unique morphisme injectif d'anneaux

$$\gamma : A/mA \to \prod_{j=1}^{n} A/a_jA \text{ tel que } \gamma \circ \psi = \pi .$$

ii) Si les $a_{k\ ,1\leq k\leq n}$ sont <u>deux à deux</u> premiers entre eux (cf. I.10.11,) le morphisme π est surjectif ce qui entraîne que γ est surjectif et donc un isomorphisme.

I.13.5 . –Théorème fondamental de l'arithmétique

La preuve des résultats de cette section peut être assez appréciablement simplifiée dans le cas de $\mathbb{Z}$ ou $\mathbb{K}[X]$ en utilisant la valeur absolue ou le degré. Il peut cependant être instructif de savoir que ces énoncés sont valables dans un cadre plus général.

Lemme I.13.5.1 *Tout élément $a \in A \setminus A^\times$ possède un diviseur irréductible.*

***Preuve** : Construisons des suites $(a_n)_{,n\in\mathbb{N}}$ et $(b_n)_{,n\in\mathbb{N}}$ à valeurs dans A de la manière suivante. On pose $a_0 := a$, et $b_0 := 1$.*

— Si a_n n'est pas irréductible, il existe a_{n+1} et b_{n+1} tous deux non inversibles tels que $a_n = a_{n+1} * b_{n+1}$.

— Sinon on pose $a_{n+1} := a_n$ et $b_{n+1} := 1$.

Les suites $(a_n)_{,n\in\mathbb{N}}$ et $(b_n)_{,n\in\mathbb{N}}$ sont bien définies par récurrence.

Notons $\mathfrak{I}_n := a_nA$, l'idéal engendré par a_n. Puisque $a_{n+1}|a_n$, la suite $(\mathfrak{I}_n)_{,n\in\mathbb{N}}$ est croissante. Il résulte alors de la proposition I.3.12.iii), que $\mathfrak{I} := \bigcup_{n\in\mathbb{N}} \mathfrak{I}_n$ est un idéal de A.

Puisque A est principal, il existe $c \in A$ tel que $\mathfrak{I} = cA$. Or $c \in \mathfrak{I}$, donc $c \in \bigcup_{nn\in\mathbb{N}} \mathfrak{I}_n$; donc il existe $p \in \mathbb{N}$ tel que $c \in \mathfrak{I}_p$. Il en résulte que $\mathfrak{I} \subset \mathfrak{I}_p$. Comme $\mathfrak{I}_p \subset \mathfrak{I}$ par construction, $\mathfrak{I} = \mathfrak{I}_p$. Comme

$$\forall q \in \mathbb{N},\ q \geq p \ \Rightarrow\ \mathfrak{I}_p \subset \mathfrak{I}_q,$$

On a

$$\mathfrak{I}_p \subset \mathfrak{I}_q \subset \mathfrak{I} = \mathfrak{I}_p$$

si bien que

$$\forall q \in \mathbb{N},\ q \geq p \ \Rightarrow\ \mathfrak{I}_q = \mathfrak{I}_p\ .$$

En particulier $\mathfrak{I}_{p+1} = \mathfrak{I}_p$. Ceci entraîne que $a_{p+1} \in \mathfrak{I}_p$ i.e. $a_p | a_{P+1}$. Comme, par hypothèse, $a_{p+1} | a_p$, a_{p+1} et a_p sont associés. Il existe donc $u \in A^\times$ tel que $a_{p+1} * u = a_p$. Par construction on a $a_p = a_{p+1} * b_{p+1}$, il en résulte que $b_{p+1} = u$. Ceci entraîne par construction des suites $\left(a_n\right)_{,n\in\mathbb{N}}$ et $\left(b_n\right)_{,n\in\mathbb{N}}$, que a_p est irréductible. Or $a_p | a$, si bien qu'on a mis en évidence un diviseur irréductible de a.

Remarque I.13.5.2 En considérant attentivement la preuve du lemme I.13.5.1, on constate qu'on a montré que dans un anneau principal toute suite croissante d'idéaux est stationnaire à partir d'un certain rang. Un anneau possédant cette propriété est dit *noethérien*.

Théorème I.13.5.3 (fondamental de l'arithmétique) *i) Pour tout élément $a \in A, a \neq 0$, il exist un entier $n \in \mathbb{N}$ des éléments irréductibles $p_i\,,_{1\leq i\leq n}$ deux à deux non associés, des entiers naturels $\alpha_i\,,_{1\leq i\leq n} \in \mathbb{N}$, et un élément inversible u tels que :*

$$a = u * \prod_{i=1}^{n} p_i^{\alpha_i}\ . \qquad 1$$

ii) La décomposition ci-dessus d'un élément $a \in A, a \neq 0$, est unique au sens où si

$$a = u * \prod_{i=1}^{d} p_i^{\alpha_i} = v * \prod_{i=1}^{e} q_i^{\beta_i}, \qquad 1$$

$m = n$ et il existe une bijection $\sigma : [1; d] \to [1; d]$ tel que

$$\forall 1 \leq i \leq n,\ \alpha_i = \beta_{\sigma(i)}\ ,\ p_i et\ q_{\beta(i)}\ \text{sont associés}\ .$$

Remarque I.13.5.4 On pourra être surpris de voir ici que la décomposition en produit de facteurs premiers (irréductibles) apparaît comme une conséquence du lemme de GAUSS (cf. I.13.2.3,) ou du lemme d'Euclide (cf. I.13.2.6,) alors que souvent l'on présente ces deux résultats comme conséquence de la décomposition en produit de facteurs premiers. On pourrrait montrer qu'en fait ces propriétés sont équivalentes pour un anneau et qu'en particulier un anneau dans lequel le théorème de BÉZOUT est vérifié, les possède.

Définition I.13.5.5 (Valuation p-adique) Le théorème I.13.5.3.ii) assure que pour tout

$$a = u * \prod_{i=1}^{n} p_i^{\alpha_i} \in A \setminus \{0\},$$

l'entier naturel α_i est bien défini. On le notera $v_{p_i}(a)$ qu'on appellera *valuation p_i-adique* de a.

I.13.6 . −Algorithme d'Euclide

Il ne suffit pas que l'anneau A soit principal pour qu'on puisse mettre en œuvre l'algorithme d'Euclide, celui-ci s'appuyant en effet sur la *division euclidienne*. Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ (cf. III.4.2,) disposent néanmoins de cette propriété. Nous allons introduire la notion d'anneau euclidien à seule fin de donner une dénommination commune à ces situations et remarquer que les anneaux euclidiens sont principaux de manière à pouvoir utiliser toutes les ressources dévloppées dans le paragraphe I.13, à propos des anneaux principaux.

Définition I.13.6.1 Étant donné un anneau commutatif intègre A, un *stathme euclidien* sur A est une application

$$\mathbf{v} \,:\, A \setminus \{0\} \,\to\, \mathbb{N}$$

vérifiant :

$$\forall (a,b) \in A \,\times\, (A \setminus \{0\}),\, \exists (q,)r \,\in\, A \,\times\, A,\, a \,=\, b*q \,+\, r \,\text{et}\, \big(r \,=\, 0 \,\text{ou}\, \mathbf{v}(r) \,<\, \mathbf{v}(b)\,\big), \quad \text{I.13.6.1.1}$$

$$\forall (a,b) \in (A \setminus \{0\}) \,\times\, (A \setminus \{0\}),\, \mathbf{v}(b) \,\leq\, \mathbf{v}(a*b)\,. \quad \text{I.13.6.1.2}$$

Un anneau commutatif intègre muni d'un stathme euclidien $\mathbf{v}$ est appelé *anneau euclidien* et on parle de *division euclidienne* suivant le stathme $\mathbf{v}$.

On adopte en général la terminologie usuelle suivante : a est le *dividende* b le *diviseur* q un *quotient* et r un *reste*.

Exemple I.13.6.2 a) $((\mathbb{Z}, |\cdot|))$

L'anneau $\mathbb{Z}$ muni de la valeur absolue est un anneau euclidien .

b) $((\mathbb{K}[X], \deg(\cdot)))$

L'anneau $\mathbb{K}[X]$ muni du degré $\deg(\cdot)$ est un anneau euclidien (cf. III.4.)

c) $((\mathbb{K}[X], \mathrm{val}(\cdot)))$

L'anneau $\mathbb{K}[X]$ peut également être muni du stathme euclidien donné par la valuation $\mathrm{val}(\cdot)$ donnant lieu à la notion de *division suivant les puissances croissantes*.

d) (**Entiers de GAUSS**)

Remarque I.13.6.3 On constate que dans la définition I.13.6.1 aucun énoncé d'unicité du couple (q,r) n'est donné contrairement à ce qui est le cas dans le cas de l'anneau $\mathbb{Z}$ ou même pour l'anneau $\mathbb{K}[X]$ (cf. III.4.2.) Dans ces deux cas, le stathme euclidien considéré possède une propriété supplémentaire de « compatibilité » à l'addition $|a+b| \,\leq\, |a| \,+\, |b|$, $\deg(P+Q) \,\leq\, \max(\deg(P), \deg(Q))$ qui n'est pas exigé par les axiomes I.13.6.1.1 et I.13.6.1.2. On constatera que l'anneau des entiers de GAUSS n'a pas de telle propriété et que néanmoins une arithmétique similaire à celle des anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ peut y être développée.

En particulier l'absence d'énoncé d'unicité dans la division euclidienne n'interdit pas de montrer que l'anneau est principal comme nous allons le voir dans la proposition I.13.6.4 qui peut servir de point de départ à toute l'arithmétique de ces anneaux.

Proposition I.13.6.4 *Un anneau euclidien $(A, \mathbf{v})$ (où A est un anneau commutatif intègre et $\mathbf{v}$ un stathme euclidien) est principal.*

Proposition I.13.6.5 (Algorithme d'Euclide) *Soit $(A, \mathbf{v})$ un anneau euclidien (cf. I.13.6.1.) Étant donnés deux éléments a_0 et a_1 de A, l'algorithme d'Euclide consiste en la donnée des suites*

$$\left(a_n\right)_{,n\in\mathbb{N}}\ ,\ \left(u_n\right)_{,n\in\mathbb{N}}\ ,\ \left(v_n\right)_{,n\in\mathbb{N}} \text{ et } \left(q_n\right)_{,n\in\mathbb{N}}$$

définies par récurrence de la manière suivante :

$$\begin{array}{rcl} u_0 & := & 1 \\ u_1 & := & 0 \\ v_0 & := & 0 \\ v_1 & := & 1\,; \end{array} \qquad \text{I.13.6.5.1}$$

pour tout $n \in \mathbb{N}$, si $a_{n+1} = 0$,

$$a_{n+2} \ = \ u_{n+2} \ = \ v_{n+2} \ = \ q_n \ = \ 0\,;$$

sinon, q_n est un quotient de la division euclidienne de a_n par a_{n+1} et $a_{n+2} \ := \ a_n - q_n * a_{n+1}$ un reste. On pose alors :

$$\begin{array}{rcl} u_{n+2} & := & u_n - q_n * u_{n+1} \\ v_{n+2} & := & v_n - q_n * v_{n+1}\,. \end{array} \qquad \text{I.13.6.5.2}$$

Alors :

i) Soit

$$\forall n \in \mathbb{N},\ a_n \ = \ 0,$$

et on pose $m \ := \ 0$, soit

$$\exists m \in \mathbb{N},\ ((a_m \ \neq \ 0) \text{ et } (\forall q > m\ ,\ a_q \ = \ 0))\,.$$

ii)

$$\forall n \in \mathbb{N},\ \left(n \leq m-2 \ \Rightarrow \ \mathcal{D}(a_n, a_{n+1}) \ = \ \mathcal{D}(a_{n+1}, a_{n+2})\right)\,;$$

d'où il résulte que d est un PGCD de a_n et a_{n+1} si et seulement si d est un PGCD de a_{n+1} et a_{n+2}.

iii)

$$\forall n \in \mathbb{N},\ a_n \ = \ a_0 * u_n \ + \ a_1 * v_n\,.$$

iv) L'élément $a_{m\,\in\,A}$ est un PGCD pour a_0 et a_1, u_m et v_m des coefficients de BÉZOUT *(cf. I.13.1.4.)*

Exemple I.13.6.6 On peut [1] mettre en oeuvre l'algorithme d'Euclide de la manière suivante :

q_n	a_n	u_n	v_n
	179	1	0
	11	0	1
16	3	1	-16
3	2	-3	49
1	1	4	-65

d'où il résulte que

$$179 \wedge 11 \ = \ 1 \text{ et } 4 * 179 \ - \ 65 * 11 \ = \ 1\,.$$

1. On n'a jamais dit « on doit »

Remarque I.13.6.7 En considérant attentivement la proposition I.13.6.5, on constaterait qu'il n'est nul besoin de savoir a priori qu'il existe un PGcD dans l'anneau A. En particulier nul besoin de savoir si l'anneau A est principal ou non. l'algorithme d'Euclide établit directement l'existence du pGCD à partir de la division euclidienne. Comme il donne également les coefficients de BÉZOUT il permet de démontrer le théorème de BÉZOUT sans recours au formalisme des idéaux. Reformuler le théorème chinois des restes dans ce contexte commencerait peut-être à devenir moins séduisant moins encore si on s'avisait d'en donner une formulation pour l'anneau $\mathbb{K}[X]$.

I.14 . −Exercices

Exercice I.14.1 [Loi de composition, (Magma)]

Cet exercice a été traité dans le premier TD d'algèbre I (M303).

Dans tout cet exercice A est un ensemble muni d'une loi de composition associative (*i.e.* un magma associatif (cf. I.0.1.2.)) Pour tout $(x, y) \in A \times A$, on note simplement xy leur composé qu'on appellera également produit.

1) a) Soit n un entier ≥ 2, et soient $a_1, \ldots, a_n$ des éléments de A. Pour calculer dans A le produit $a_1 a_2 \ldots a_n$, il faut mettre des parenthèses de façon à ne calculer, aux étapes successives, que des produits de deux éléments de A. Montrer que le résultat ne dépend pas du choix d'un tel parenthésage ; on le note $a_1 a_2 \ldots a_n$.

Indication : *On pourra procéder par une récurrence sur n, et comparer deux tels parenthésages, l'un où le dernier produit effectué regroupe les k premiers termes : $(a_1 \ldots a_k)(a_{k+1} \ldots a_n)$, l'autre où le dernier produit regroupe les $(k+1)$ premiers termes $(1 \leq k \leq n)$.*

b) Pour $a \in A$ et p entier ≥ 1, on note a^p le produit $a_1 \ldots a_p$ où $a_1 = a_2 = \ldots = a_p = a$. Montrer qu'on a

$$a^p a^q = a^{p+q} \text{ et } (a^p)^q = a^{pq} \text{ pour } p, q \text{ entiers } \geq 1 .$$

2) a) Supposons que A possède un élément neutre, c'est-à-dire un élément e tel que $ea = ae = a$ pour tout $a \in A$. Montrer qu'un tel élément est unique ; on le note souvent 1 et on pose $a^0 = 1$ pour tout $a \in A$.

b) Étendre aux entiers p et $q \geq 0$ les règles établies en question 1), b).

c) Soient a,b,c des éléments de A tels que $ab = bc = 1$; montrer qu'alors $a = c$. En déduire que si a possède un inverse b, cet inverse est unique ; on le note a^{-1}.

d) Prouver que si des éléments $a_1, \ldots, a_n$ de A ont chacun un inverse, alors $a_1 \ldots a_n$ est inversible aussi, et calculer son inverse.

e) Prouver que l'ensemble des éléments inversibles de A est un groupe pour la loi $(a, b) \mapsto ab$.

f) Si a est un élément inversible de A, on pose $a^{-p} := (a^{-1})^p$ pour p entier ≥ 1. Étendre les règles établies en question 1), b) à tous les entiers $p, q \in \mathbb{Z}$.

3) a) Soient x et y deux éléments de A qui commutent : $xy = yx$. Prouver que, quels que soient les entiers p et $q \geq 1$, x^p et y^q commutent aussi, et qu'on a $(xy)^p = x^p y^p$.

b) Étendre ces résultats aux entiers p et $q \geq 0$ si A a un élément neutre 1, et à tous les entiers p et q si x et y sont inversibles.

c) Si on prend pour A un groupe abélien avec une loi noté additivement $(a, b) \mapsto a + b$, on écrit 0 (plutôt que 1) pour l'élément neutre et on note nx au lieu de x^n (en particulier l'opposé de x, c'est-à-dire l'inverse pour la loi $+$, est noté $-x$.)

a) Écrire dans ces notations les résultats obtenus en question 1), question 2), question 3).

b) Pour x, y dans A on pose alors $x - y = x + (-y)$; prouver que c'est le seul élément z de A tel que $x = z + y$; calculer $-(x-y)$, $(x-y)+(x'-y')$, $(x-y)-(x'-y')$.

4) Pour $n \in \mathbb{N}^*$ et tout n-uplet $a_{i\ ,1\leq i\leq n}$ d'éléments de A, on définit le *produit des* $a_{i\ ,1\leq i\leq n}$ qu'on note $a_1 \times \ldots \times a_n$ par *récurrence* : Si $n = 1$, le produit de l'élément a est a lui-même et pour tout $n+1$-uplet $a_{i\ ,1\leq i\leq n+1}$,

$$(a_1 \times \ldots \times a_{n+1}) \ := \ (a_1 \times \ldots \times a_n) \times a_{n+1} \ .$$

a) Soit n un entier ≥ 1, et $(a_i)_{i\ \in\ I}$ une famille à n éléments de A, ces éléments commutent l'un à l'autre. Montrer que, quelle que soit la numérotation $i_1, \ldots, i_n$ qu'on mette sur I (*i.e.*quelle que soit la bijection $n \mapsto i_n$ de $\{1, \ldots, n\}$ sur I ,) le produit $a_{i_1} \times \ldots \times a_{i_n}$ est toujours le même ; on le note $\prod_{i\ \in\ I} a_i$ [on pourra procéder par récurrence sur n et comparer deux tels produits, tout d'abord dans le cas où un élément b de A se trouve en dernière position, puis dans le cas où un élément b de A se trouve en $k^{\text{ième}}$ position dans le premier produit, et en $(k+1)^{\text{ième}}$ position dans le second, $1 \leq k < n$.]

b) Soit $I = \bigcup_{k\ \in\ K} J_k$ une partition de I (en sous-ensembles deux à deux disjoints non vides.) Montrer qu'on a :

$$\prod_{i\ \in\ I} a_i \ = \ \prod_{k\ \in\ K} \ (\prod_{j \in J_k} a_j) \ .$$

Pour m entier ≥ 1, on a

$$(\prod_{i\ \in\ I} a_i)^m \ = \ \prod_{i\ \in\ I} a_i^m \ .$$

c) Supposons que A ait en outre un élément neutre 1 ; on pose alors $\prod_{i\ \in\ I} a_i = 1$ si I est vide ; étendre les règles précédentes aux cas où I, ou l'un des J_k est vide.

d) Supposons que A soit un groupe abélien noté additivement ; on écrit alors $\sum_{i\ \in\ I} a_i$; traduire dans ces notations les résultats précédents.

5) Soit X un ensemble. On munit l'ensemble A^X des applications de X dans A de la loi $(f, f') \mapsto ff'$ où $ff'(x) = f(x)f'(x)$ pour tout $x \ \in \ X$.

a) Montrer que la loi définie ci-dessus est la seule pour laquelle, pour tout $x \ \in \ XX$, $f \ \mapsto \ f(x)$ est un morphisme.

b) Montrer que cette loi sur A^X est associative et que A^X est un groupe pour cette loi si A est un groupe, un groupe abélien si A est un groupe abélien.

c) Si A est un groupe, et X un autre groupe, montrer que l'ensemble $\mathrm{Hom}(X, A)$ des homomorphismes de groupes de X dans A est un sous-groupe de A^X, pourvu que A soit abélien.

6) (**Groupe abélien**)

On suppose que A est un groupe abélien et pour tout $p \in \mathbb{Z}$, et tout $a \in A$, on note $p \cdot a := a^p$ avec les notations de question 2), f) et question 1), b).

Réécrire dans ce formalisme les résultats de question 1), b) et question 2), f).

Exercice I.14.2 Quelle différence y-a-til entre I.5.1.i) et I.5.1.ii) du point de vue des anneaux et de celui des groupes. Comparer à la proposition A.5.1.

Exercice I.14.3 Avec les notations I.7.1, montrer que pour tout F muni d'une des structures algébriques I.7.1.i) ou I.7.1.iii), l'application

$$\mathrm{Hom}(F,P) \to \prod_{k=1}^{n} \mathrm{Hom}(F,E_k)\ ,\ f \mapsto \big(p_1 \circ f, \ldots, p_n \circ f\big)$$

est un isomorphisme pour la structure algébrique considérée.

Exercice I.14.4 Avec les notations I.7.1, si $\forall 1 \leq k \leq n$, E_k est un anneau, (resp. une A-algèbre,)

1) les applications i_k de la proposition I.7.6 sont-elles des morphismes d'anneaux (resp. de A-algèbres ?)

2) Que peut-on dire de $\mathrm{Im}\, i_k$?

Exercice I.14.5 Démontrer le théorème I.9.19.

Exercice I.14.6 Soit

$$0 \to B \xrightarrow{\ i\ } A \xrightarrow{\ p\ } C \to 0$$

une suite exacte courte de groupes abéliens finis. On suppose que $\#(B)$ et $\#(C)$ sont des entiers premiers entre eux. Montrer qu'alors la suite exacte courte est scindée.

Exercice I.14.7

Exercice I.14.8