Université Paris Sud — Année 2004–2005

Licence MA — Algèbre Générale

Table des matières

Université Paris Sud **Année 2004–2005**

Licence MA — Algèbre Générale

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.

0 . −Introduction

Rappelons que, si $\mathbb{K}$ est un corps, E est un $\mathbb{K}$-espace vectoriel (cf. II.3.13) si
- $(E,+)$ est un groupe abélien (cf. I.1.3) et
- pour tout $(\alpha,\beta)\in\mathbb{K}\times\mathbb{K}$, et tout $(x,y)\in E\times E$,

$$\begin{aligned}\alpha\cdot(x+y) &= \alpha\cdot x+\alpha\cdot y\\ (\alpha+\beta)\cdot x &= \alpha\cdot x+\beta\cdot x\\ (\alpha*\beta)\cdot x &= \alpha\cdot(\beta\cdot x)\\ 1_{\mathbb{K}}\cdot x &= x\,.\end{aligned}$$

Par ailleurs, si A est un anneau, un sous-ensemble I de A est un idéal (cf. II.5.6) si
- $(I,+)$ est un sous-groupe de $(A,+)$ et
- pour tout $\alpha\in A$ et tout $x\in I$, $\alpha*x\in I$.

On constate immédiatement que pour tout $(x,y)\in I\times I$, $\alpha*(x+y)=\alpha*x+\alpha*y$ par le fait que la multiplication dans A est distributive sur l'addition. On vérifierait sans peine que I satisfait également les autres axiomes des espaces vectoriels, à ceci près que A n'est pas nécessairement un corps.

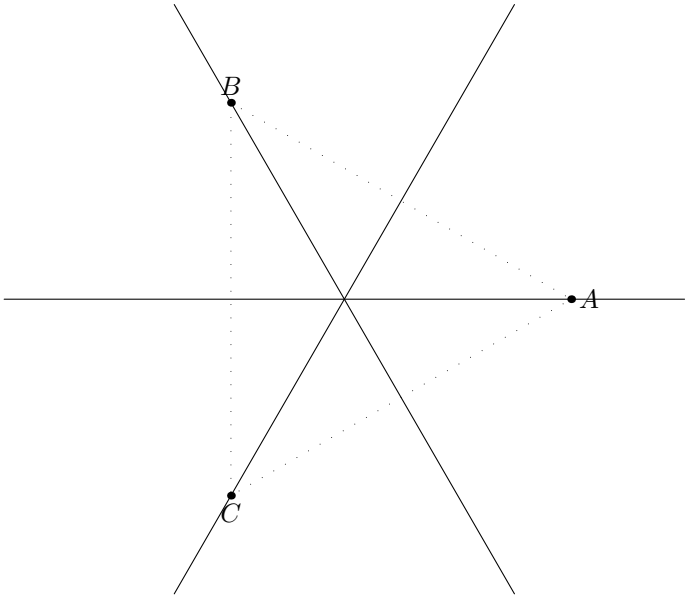
Enfin, si $(G,+)$ est un groupe abélien (commutatif), pour tout $n\in\mathbb{Z}$ et tout $g\in G$, $n\cdot g$ est naturellement défini comme la somme de n termes égaux à g si n est positif et de n termes égaux à $-g$ (l'opposé de g dans $G,$) si n est négatif. Il résulte immédiatement de cette définition que $n\cdot(g+h)=n\cdot g+n\cdot h$, que $(m*n)\cdot g=m\cdot(n\cdot g)$ etc ...

On constate donc qu'une base axiomatique unique permettrait de traiter de la même manière des problèmes communs aux $\mathbb{K}$-espaces vectoriels, aux idéaux d'un anneau A et aux groupes abéliens. Ceci conduira à la définition de A-module (cf. II.3.1.) Les questions d'arithmétique (divisibilité dans $\mathbb{Z}$, primalité, congruences etc ...) nous amèneront à étudier précisément les idéaux et les groupes abéliens.

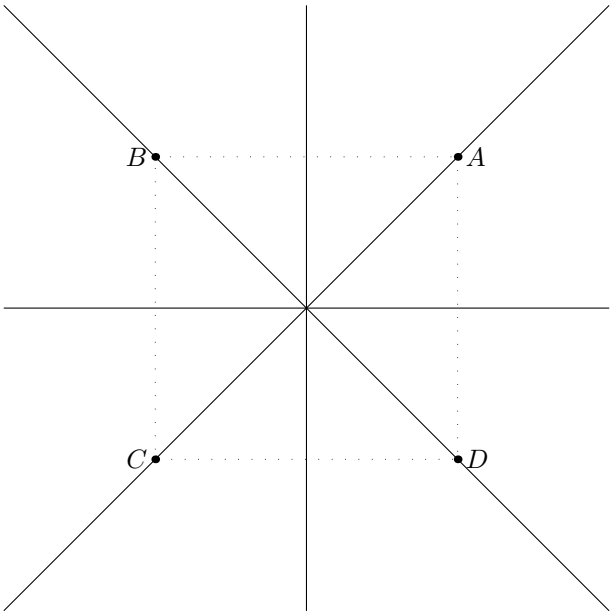
Il est néanmoins bien évident que cette généralisation ne pourra pas rendre compte de toutes les propriétés spécifiques à chacune des structures (espace vectoriel, idéal et groupe abélien) mentionnée ci-dessus.

Enfin le cas des groupes non commutatifs doit être traité séparément; car pour $(G,*)$ un groupe quelconque, on n'a pas nécessairement $n\cdot(g*h)=(n\cdot g)*(n\cdot h)$ plus usuellement connu sous la forme $(gh)^n\neq g^nh^n$. Pensons notamment au cas des groupes linéaires $\mathrm{GL}(E)$ pour un $\mathbb{K}$-espace vectoriel E et à ses sous-groupes de nature plus géométrique comme $\mathcal{O}_{<>}(E)$ et $\mathcal{SO}_{<>}(E)$ qui ne sont pas abéliens en général. Certains de leurs

sous-groupes notamment finis comme les groupes d'isométries du triangle



qui s'identifie au groupe des permutations $\mathcal{S}_3$ (cf. I.4) ou du groupe des isométries du carré



qui s'identifie au sous-groupe D_4 du groupe des permutations $\mathcal{S}_4$.

Bien que la définition des diverses structures mentionnées ci-dessus repose axiomatiquement sur la théorie des ensembles, nous n'entrerons pas dans les détails de cette dernière.

L'étude de ses raffinements et de ses aspects problématiques ne s'avérera en effet pas pertinent ici et il suffira bien souvent de s'en rapporter à l'idée intuitive qu'on en a.

On est couramment amené à identifier des objets, hors même du champ des mathématiques, lequel n'échappe pas à cette volonté de classification. Afin de donner, dans ce cadre, une formulation rigoureuse aux raisonnements qu'on mènera, on est conduit à donner un certain nombre de définitions et à introduire les notions de relation et celle plus précise encore de relation d'équivalence. Rappelons d'abord quelques aspects très élémentaires de la théorie des ensembles :

Définition 0.1 Étant donnés deux ensembles A et B, on dit que B *est inclus dans* A ou encore que B est *une partie de* A ou encore que B est *un sous-ensemble de* A si pour tout x appartenant à B, x appartient à A ; ce qui s'écrit

$$\forall x \in B \ , \ x \in A \ .$$

On notera encore $B \subset A$.

Définition 0.2 Étant donné un ensemble A on note $\mathcal{P}(A)$ l'ensemble des parties de A c'est-à-dire l'ensemble des ensembles B inclus dans A . La théorie des ensembles assure que

$$\mathcal{P}(A) \ := \ \{B \mid B \subset A\}$$

est bien un ensemble.

Définition 0.3 Deux ensembles B et A sont *égaux* s'ils ont les mêmes éléments c'est-à-dire que tout y de B appartient à A et que tout x de A appartient à B ; ce qui peut s'écrire

$$\forall y \in B \ , \ y \in A \text{ et } \forall x \in A \ , \ x \in B \ .$$

Ceci équivaut à dire que B est inclus dans A et que A est inclus dans B :

$$B \subset A \text{ et } A \subset B \ .$$

On notera encore $B = A$.

Définition 0.4 Étant donnés deux ensembles A et B, on appelle *produit cartésien* de A et B l'ensemble

$$A \times B \ := \ \{(x, y) \mid x \in A \, y \in B\} \ ,$$

ensemble des couples dont le premier élément est dans A et le second dans B.

Pour une famille finie $A_{i \ , 1 \leq i \leq n}$ d'ensembles on définit également le produit cartésien des A_i comme l'ensemble des n-uplets $(x_1, \ldots, x_n)$ avec $x_i \in A_i$, pour tout $1 \ \leq \ i \ \leq \ n$.

Définition 0.5 Étant donnés deux ensembles A et B,

i) on peut définir une *application* f de A dans B comme une partie G du produit cartésien $A \times B$ de A et B telle que tout x de A soit la première composante d'un et d'un seul élément de $G \subset A \times B$ c'est-à-dire encore que pour tout $x \in A$, il existe un unique $y \in B$ tel que (x, y) appartienne à G . On note alors usuellement $y := f(x)$ et on l'appelle *image de x par f* . Le sous-ensemble G de $A \times B$ est appelé le *graphe de f* .

Plus généralement, pour toute partie $U \subset A$, on note

$$f(U) := \{f(x) \, , \, x \in U\} \subset B \, ,$$

qu'on appelle *image de U par f* .

ii) Étant donné une application $f : A \to B$, pour toute partie $V \subset B$, on note

$$f^{-1}(V) := \{x \in A \mid f(x) \in V\} \subset A$$

l'ensemble des antécédents des éléments de V par f qu'on appelle *pré-image (ou image réciproque) de V par f* .

Si $V := \{y\} \subset B$ est un singleton, $f^{-1}(\{y\}) = f^{-1}(V)$ souvent abusivement noté $f^{-1}(y)$ (bien que f ne soit pas bijective,) est appelé *pré-image de y par f* ou parfois aussi *fibre de f au-dessus de y* .

iii) Une application $f : A \to B$ est dite *injective* si pour tout couple (x, x') d'éléments de A, $f(x) = f(x')$ implique $x = x'$. Ceci équivaut encore à dire que tout élément de B possède au plus un antécédent par f ou encore que la fibre de f au-dessus d'un élément de B contient au plus un élément.

Si U est une partie d'un ensemble A la partie

$$I := \{(x, x) \, , \, x \in U\} \subset U \times A$$

du produit cartésien de U et A définit une application injective $i : U \hookrightarrow A$. Elle est appelée *injection canonique.*

iv) Une application $f : A \to B$ est dite *surjective* si tout élément de B possède au moins un antécédent dans A ou encore que la fibre de f au dessus d'un élément de B est non vide.

v) Une application $f : A \to B$ est dite *bijective* si tout élément de B possède un et un seul antécédent dans A .

Ceci équivaut à dire que l'équation $f(x) = y$ d'inconnue $x \in A$ et de paramètre $y \in B$ possède une unique solution ou encore que la fibre de f au-dessus d'un élément de B est un singleton.

Cette définition équivaut encore au fait que f est simultanément injective et surjective et finalement encore au fait qu'il existe une application $g : B \to A$ telle que

$$f \circ g = \mathrm{Id}_B \text{ et } g \circ f = \mathrm{Id}_A .$$

On notera usuellement $g = f^{-1}$.

Remarque 0.6 La composition $\circ$ des applications, à laquelle nous avons fait librement référence sans définition préalable car elle ne pose guère de difficulté conceptuelle, introduit une structure supplémentaire qui pourrait, moyennant quelques restrictions, conduire rapidement à la notion de groupe ou tout au moins à celle de monoïde.

Cependant nous allons tout d'abord nous intéresser à une notion complémentaire à celle d'application :

Définition 0.7 Étant donné un ensemble A on appelle *relation binaire* sur A une partie G du produit cartésien $A \times A$ de A avec lui-même. On notera, pour tout $(x, y) \in A \times A$, $x \, R \, y$ si $(x, y) \in G$.

Le sous-ensemble G de $A \times A$ est appelé *graphe de la relation* R .

Remarque 0.8 On remarque immédiatement qu'une application de A dans lui-même est un cas particulier de relation binaire sur A et que les définitions de graphe données jusqu'ici sont cohérentes de ce point de vue.

Sans hypothèse supplémentaire, les relations binaires permettent rarement de "classer" les ensembles de manière satisfaisante ; c'est pourquoi on est amené à préciser la définition ci-dessus :

Définition 0.9 Étant donné un ensemble A et une relation binaire R sur A,

i) on dit que R est *réflexive* si pour tout $x \in A$, $x \, R \, x$.

ii) On dit que R est *symétrique* si pour tout $(x, y) \in A \times A$, $x \, R \, y$ implique $y \, R \, x$.

iii) On dit que R est *antisymétrique* si pour tout couple $(x, y) \in A \times A$, $x \, R \, y$ et $y \, R \, x$ impliquent $x = y$.

iv) On dit que R est *transitive* si pour tout triplet (x, y, z) d'éléments de A, $x \, R \, y$ et $y \, R \, z$ impliquent $x \, R \, z$.

Définition 0.10 Étant donnée une relation R sur un ensemble A,

i) si R est réflexive, antisymétrique et transitive, on dira que R est *une relation d'ordre.*

Exemple i).1 La relation $\leq$ (resp. $\geq$) (inférieur (resp. supérieur) ou égal) est une relation d'ordre sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$.

ii) Si R est réflexive, symétrique et transitive, on dit que R est *une relation d'équivalence.*

Exemple ii).1 La relation d'égalité $x = y$ est une relation d'équivalence sur n'importe quel ensemble sans qu'il y ait certes un grand intérêt à la considérer comme telle. À noter que c'est également une relation d'ordre.

iii) Si R est une relation d'équivalence sur A, pour tout $x \in A$ on appelle *classe de x selon (ou modulo) R* la partie

$$\overline{x} := \{y \mid y\, R\, x\} \subset A$$

de A .

Proposition 0.11 *Étant donnée une relation d'équivalence R sur un ensemble A,*

i) Aucune des classes selon (modulo) R n'est vide.

ii) Les classes selon (modulo) R sont deux à deux disjointes c'est-à-dire que si $\overline{x} \cap \overline{y} \neq \emptyset$, alors $\overline{x} = \overline{y}$.

iii) La réunion des classes selon (modulo) R est égale à A .

***Preuve** : La démonstration de cette proposition est laissée en exercice.*

Définition 0.12 i) On dit que l'ensemble des classes d'équivalence pour une relation d'équivalence R sur un ensemble A forme une *partition de A* .

Remarque i).1 On note que, si l'on se donne une partition de A, c'est-à-dire une partie Q de $\mathcal{P}(A)$ (cf. 0.2) telle que

— $\emptyset \notin Q$,
— les éléments de Q sont deux à deux disjoints,
— A est égal à la réunion des éléments de Q,

il existe une unique relation d'équivalence R dont l'ensemble des classes est égal à Q .

ii) L'ensemble des classes d'équivalences pour une relation d'équivalence R sur un ensemble A est appelé *quotient de A par R* et noté A/R .

On peut définir une application canonique $p : A \to A/R$ qui à tout $x \in A$ associe sa classe $\overline{x}$ selon R .

Remarque ii).1 On remarque que p est surjective et que ses fibres (cf. 0.5.ii)) s'identifient aux classes d'équivalence selon R .

L'application p sera appelée *surjection* (ou *projection) canonique.*

Remarque ii).2 À noter qu'étant donnée une application surjective $p : A \to B$, ses fibres définissent une partition de A et l'on peut donc, par conséquent, définir une unique relation d'équivalence sur A pour laquelle p sera la surjection canonique.

Remarque 0.13 À noter qu'une bonne partie de ce qui va suivre consistera à étudier la compatibilité de certaines relations d'équivalence avec les structures (de groupes, anneaux, modules etc ...) que nous allons définir, ce qui revient en définitive à déterminer quel structure pourra être induite sur les ensembles quotients.

I . −Groupes

I.1 . −Généralités

Définition I.1.1 (Groupe) Un *groupe* est un couple $(G, *)$ (le plus souvent noté G) où G est un ensemble et $*$ une loi de composition interne *i.e.*une application :

$$\begin{aligned} \star : G \times G &\to G ; \\ (x, y) &\mapsto x * y . \end{aligned}$$

La loi $*$ vérifie :

GR$_1$ pour tout triplet (x, y, z) d'éléments de G, on a :

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

($*$ est *associative*) ;

GR$_2$ il existe un élément e_G dans G, appelé *élément neutre* de G, tel que pour tout $x \in G$:

$$x * e_G = e_G * x = x,$$

(on notera simplement e l'élément neutre si aucune confusion n'est à craindre) ;

GR$_3$ pour tout $x \in G$, il existe un élément $x' \in G$ appelé *inverse* de x tel que :

$$x * x' = x' * x = e_G .$$

On appellera, en général *produit* la loi $*$.

On dira indifféremment que $(G, *)$ est un groupe ou que l'ensemble G est *muni par* $*$ *d'une structure de groupe*.

Remarque I.1.2 i) L'existence d'un élément neutre dans un groupe implique qu'un groupe n'est jamais vide.

ii) L'unicité de l'élément neutre n'est pas requise par les axiomes mais en est une conséquence immédiate.

iii) Il en est de même pour l'unicité de l'inverse d'un élément dans un groupe.

Définition I.1.3 Étant donné un groupe $(G, *)$, si
GR_4 pour tout couple (x, y) d'éléments de G, $x * y = y * x$, on dira que la loi de composition interne $*$ est *commutative* ou encore que le groupe G est *commutatif* ou *abélien.*

Remarque I.1.4 Dans le cas d'un groupe abélien G, l'élément neutre est le plus souvent noté 0_G, l'inverse de x $-x$ est appelé *opposé*; par analogie avec "le groupe abélien modèle $(\mathbb{Z}, +)$"

Exemple I.1.5 a) L'ensemble $\mathbb{Z}$, muni de l'addition, est un groupe abélien. En revanche, l'ensemble $\mathbb{N}$ des entiers naturels n'est pas un groupe pour l'addition usuelle.

b) Pour tout entier $n > 1$, $\sim_n$ est la relation de *congruence modulo* n *sur* $\mathbb{Z}$, c'est-à-dire la relation d'équivalence définie par $a \sim_n b$ si $n \backslash b - a$ pour a et b dans $\mathbb{Z}$. Pour $a \in \mathbb{Z}$, on note $\overline{a}$ la classe de a modulo n. La relation $\sim_n$ vérifie la propriété fondamentale suivante : si

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

alors

$$a + a' \sim_n b + b' ,$$

(cf. I.2.12.) Ceci permet de définir une loi de composition interne $+$ sur l'ensemble $\mathbb{Z}/n$ des classes modulo $\sim_n$, par

$$\overline{a} +_{\mathbb{Z}/n} \overline{b} = \overline{a + b} .$$

Le couple $(\mathbb{Z}/n, +_{\mathbb{Z}/n})$ le plus souvent noté $(\mathbb{Z}/n, +)$ où même $\mathbb{Z}/n$ est un groupe abélien.

c)

Définition I.1.6 Pour deux groupes $(G, *_G)$ et $(H, *_H)$, on appellera *morphisme (homomorphisme) de groupes,* (ou simplement *morphisme* si le contexte est clair), de G à valeurs dans H une application f de l'ensemble G à valeurs dans l'ensemble H telle que
GR_5, pour tout $(x, y) \in G \times G$:

$$f(x *_G y) \;=\; f(x) *_H f(y)\,.$$

Proposition I.1.7 *Si $f : G \to H$ et $g : H \to I$ sont deux morphismes de groupes, la composée $g \circ f$ est un morphisme de groupes de G dans I.*

I.1.8 . −Notation

Étant donnés deux groupes G et H on notera $\mathrm{Hom}_{\mathbf{Gr}}(G, H)$ (ou simplement $\mathrm{Hom}(G, H)$ si le contexte est clair) l'ensemble des morphismes de groupes de G à valeurs dans H.

Remarque I.1.9 Pour tout morphisme $f : G \to H$, on a :

i) $f(e_G) = e_H$;

ii) pour tout $x \in G$,

$$f(x^{-1}) \;=\; f(x)^{-1}\,.$$

Exemple I.1.10 a) Pour tout groupe G, on a un morphisme de G dans lui-même appelé *identité de* G, noté Id_G et caractérisé par le fait que pour tout $x \in G$, $\mathrm{Id}_G(x) = x$.

b) Pour tout entier $n > 1$, l'application

$$\begin{array}{rcl} \pi_n : \mathbb{Z} & \to & \mathbb{Z}/n \\ a & \mapsto & \overline{a}\,, \end{array}$$

(cf. I.1.5.b)), est un morphisme de groupes. Cela découle presque totologiquement de la définition de $+$ sur $\mathbb{Z}/n$ puisque

$$\overline{a+b} \;=\; \overline{a} + \overline{b}\,.$$

c) Étant donné un groupe G, tout élément $x \in G$ définit un unique morphisme

$$\begin{array}{rcl} \epsilon_x : \mathbb{Z} & \longrightarrow & G \\ 1 & \longmapsto & x\,. \end{array}$$

On notera x^n l'image de l'entier n. Avec cette notation on aura $x^0 = e_G$ et x^{-1} désignera l'inverse de x.

d) L'application logarithme népérien $\ln : \mathbb{R}^{+,*} \to \mathbb{R}$ est un morphisme du groupe abélien des nombres réels strictement positifs, muni de la multiplication dans le groupe abélien des nombres réels, muni de l'addition.

e) L'exponentielle est un morphisme de groupes abéliens, du groupe des nombres réels muni de l'addition, dans le groupe des nombres réels strictement positifs, muni de la multiplication.

Définition I.1.11 Un morphisme de groupes $f : (G, *_G) \to (H, *_H)$ (cf. I.1.6e)st un *isomorphisme* s'il existe un morphisme $g : (H, *_H) \to (G, *_G)$ tel que :

$$f \circ g = \mathrm{Id}_H \text{ et } g \circ f = \mathrm{Id}_G .$$

Proposition I.1.12 *Un morphisme de groupes $f : (G, *_G) \to (H, *_H)$ est un isomorphisme si et seulement si il est bijectif.*

Preuve *: La démonstration est exactement analogue à celle de la proposition II.3.15.Si f est un morphisme bijectif, il existe une application ensembliste $g : H \to G$ telle que $g \circ f = \mathrm{Id}_G$ et $f \circ g = \mathrm{Id}_H$. Pour tout $(u, v) \in H \times H$, comme f est bijective, il existe un unique couple $(x, y) \in G \times G$ tel que*

$$\begin{array}{rcl} u = f(x) & \Leftrightarrow & x = g(u) \\ v = f(y) & \Leftrightarrow & y = g(v) . \end{array}$$

On a donc

$$\begin{aligned} g(u *_H v) &= g[f(x) *_H f(y)] \\ &= g[f(x *_G y)] \\ &= x *_G y \\ &= g(u) *_G g(v) ; \end{aligned}$$

ce qui prouve que g vérifie GR$_5$ et est donc un morphisme.

Proposition I.1.13 *Étant donnés deux groupes (resp. abéliens) $(G, *_G)$ et $(H, *_H)$, avec $(H, *_H)$ abélien la loi de composition $*_H$ permet de munir l'ensemble $\mathrm{Hom}_{\mathbf{Gr}}(G, H)$ d'une loi de composition interne canonique notée $*_{\mathrm{Hom}_{\mathbf{Gr}}(G,H)}$ (ou simplement $*$). Alors*

$$(\mathrm{Hom}_{\mathbf{Gr}}(G, H), *_{\mathrm{Hom}_{\mathbf{Gr}}(G,H)} \text{ est un groupe. abélien.}$$

Preuve *: Pour f et g deux morphismes de G dans H, on définit $f * g$ en posant, pour tout $x \in G$,*

$$(f * g)(x) := f(x) *_H g(x) .$$

Le reste des vérifications est laissé en exercice.

Remarque I.1.14 Il se pourrait que $\mathrm{Hom}_{\mathbf{Gr}}(G,H)$ soit muni d'autres structures de groupe ; cependant si on ne précise pas quelle structure de groupe on considère sur $\mathrm{Hom}_{\mathbf{Gr}}(G,H)$ il s'agira toujours de celle définie ci-dessus.

Définition I.1.15 (Sous-groupe) Étant donné un groupe $(G,*_G)$, (cf. I.1.1o)n appelle *sous-groupe de* G un groupe $(H,*_H)$ muni d'un morphisme de groupes (cf. I.1.6)

$$i \,:\, (H,*_H) \,\hookrightarrow\, (G,*_G) \ \underline{\text{injectif}} \ .$$

Exemple I.1.16 a) Pour tout groupe G, l'ensemble $\{e\}$ formé de l'élément neutre de G est un sous-groupe de G. Le groupe G lui-même est également un sous-groupe de G.

b) Pour tout couple (H,K) de sous-groupes d'un groupe G, $H\cap K$ est un sous-groupe de G.

c) Pour un couple quelconque (H,K) de sous-groupes de G, $H\cup K$ n'est pas en général un sous-groupe de G. On a même l'énoncé suivant : *$H\cup K$ est un sous-groupe de G si et seulement si $H\subset K$ ou $K\subset H$.*

Exemple I.1.17 a) Si E est un $\mathbb{C}$-espace vectoriel hermitien, (resp. un $\mathbb{R}$-espace vectoriel euclidien,) l'ensemble des endomorphismes unitaires, (resp. orthogonaux,) de E est un sous-groupe de $\mathrm{GL}(E)$.

b) L'image d'un morphisme de groupes $f \,:\, G \,\to\, H$ est un sous-groupe de H.

Remarque I.1.18 i) L'application $i \,:\, H \,\hookrightarrow\, G$ dans la définition I.1.15 induisant un isomorphisme de groupes (cf. I.1.11) souvent, pour $x\in H \ : x \,\in\, G$ au lieu de $i(x)\in G$.

ii) Dans un grand nombre de situations, un sous-groupe H d'un groupe G est une partie ensembliste de G (un sous-ensemble de G) *muni de la structure de groupe induite par celle de G* ; c'est-à-dire que pour tout $(x,y)\in H\times H, x*_H y \,:=\, x*_G y$. Dans ces cas, l'injection $i : H\hookrightarrow G$ est simplement l'inclusion ensembliste canonique et on omet de la noter.

Proposition I.1.19 *Étant donné un groupe $(G,*)$ une partie H de G muni de la loi de composition $*$ est un sous-groupe de G si et seulement si :*

- *H est non vide ;*
- *pour tout $x \,\in\, H$ $x^{-1}\in H$;*
- *pour tout $(x,y)\in H\times H, x*y\in H$.*

Exemple I.1.20 (Sous-groupes de $\mathbb{Z}$) Pour tout sous-groupe H de $(\mathbb{Z},+)$, on remarque que l'intersection $H\cap\mathbb{N}$ de H avec $\mathbb{N}$ est non vide. Si l'on suppose $H\neq\{0\}$, l'intersection $H\cap\mathbb{N}^*$ est non vide. Il s'ensuit qu'il existe un plus petit élément strictement positif d appartenant à H. D'après la proposition I.1.19, l'opposé $-d$ de d appartient à H ainsi que kd (la somme de k éléments égaux à d,) pour tout $k\in\mathbb{N}$. Il s'ensuit que l'ensemble $d\mathbb{Z}:=\{dk\ ,\ k\in\mathbb{Z}\}$, est inclus dans H. Il convient dès maintenant de remarquer que $d\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Pour tout $x\in H$, il existe un unique couple $(q,r)\in\mathbb{Z}\times\mathbb{Z}$ tel que $x=dq+r$ et $0\leq r<d$ puisque $\mathbb{Z}$ est *euclidien* c'est-à-dire qu'il est muni d'une *division euclidienne*. D'après ce qui précède, $dq\in H$ ce qui implique que $r=x-dq\in H$ et par conséquent que $r=0$.

Il en résulte finalement que $H=d\mathbb{Z}$.

Définition I.1.21 On appelle *noyau* d'un morphisme de groupes $f:G\to H$ l'ensemble

$$\mathrm{Ker}\, f:=\{x\in G\mid f(x)=e_H\}\ .$$

Proposition I.1.22 *Le noyau d'un morphisme de groupes $f:G\to H$ est un sous-groupe de G.*

Proposition I.1.23 *Un morphisme de groupes $f:G\to H$ est injectif si et seulement si son noyau $\mathrm{Ker}\, f$ est réduit à l'élément neutre e_G de G.*

Proposition I.1.24 *Soit $(G,*)$ un groupe et $S\subset G$ une partie non vide de G. Notons*

$$S^{g_{\mathfrak{p}}}:=\{s_1^{\epsilon_1}*\ldots*s_n^{\epsilon_n}\ ,\ n\in\mathbb{N}^*\ ,\ s_i\ ,1\leq i\leq n\in S\ ,\ \epsilon_i\ ,1\leq i\leq n\in\{-1;1\}\}\ .$$

Alors :

i) L'ensemble $S^{g_{\mathfrak{p}}}$ muni de la loi $*$ est un sous-groupe de G.

ii) $S^{g_{\mathfrak{p}}}$ est le plus petit (au sens de l'inclusion) sous-groupe de G contenant S i.e.pour tout sous-groupe $H\subset G$ contenant S, $S^{g_{\mathfrak{p}}}\subset H$.

Preuve *: La démonstration est laissée en exercice.*

Définition I.1.25 Avec les notations de la proposition I.1.24, on dit que $S^{g_{\mathfrak{p}}}$ est le *sous-groupe engendré* par S. Si $S^{g_{\mathfrak{p}}}$ est égal à G, on dit que *le groupe G est engendré par S.*

Remarque I.1.26 Avec les notations de la proposition I.1.24, si S est l'ensemble vide, on posera, par convention, $S^{g_{\mathfrak{p}}}:=\{e_G\}$.

I.2 . −Relations d'équivalence (compatibles) sur un groupe, groupe quotient, sous-groupe distingué

I.2.1. − Étant donné un groupe $(G,*)$ et H un sous-groupe on note $\sim_{g,H}$ (resp. $\sim_{d,H}$) la relation binaire sur $G\times G$ définie par

$$x\sim_{g,H} y \text{ si } x^{-1}*y\in H\ , \qquad \text{I.2.1.1}$$

(resp.

$$x\sim_{d,H} y \text{ si } y*x^{-1}\in H.) \qquad \text{I.2.1.2}$$

On notera encore, pour tout $x\in G$,

$$x*H\ :=\ \{x*y\ ,\ y\in H\}\ ,$$

(resp.

$$H*x\ :=\ \{y*x\ ,\ y\in H\}\ .)$$

Proposition I.2.2 *Soient un groupe $(G,*)$ et H un sous-groupe.*

i) Les relations binaires définies en (cf. I.2.1) sont des relations d'équivalence.

ii) L'ensemble $G/\sim_{g,H}$ (resp. $G/\sim_{d,H}$) des classes d'équivalence pour la relation $\sim_{g,H}$ (resp. $\sim_{d,H}$) s'identifie à $\{x*H,\ x\in G\}$, (resp. $\{H*x,\ x\in G\}$.)

iii) Toute classe d'équivalence pour la relation $\sim_{g,H}$ (resp. $\sim_{d,H}$) est en bijection avec H.

iv) Si G est fini on a :

$$\#(G)\ =\ \#(H)\#\big(G/\sim_{d,H}\big)\ =\ \#(H)\#\big(G/\sim_{g,H}\big)\ .$$

***Preuve** :*

i) Montrons que la relation $\sim_{g,H}$ est une relation d'équivalence. Pour tout $x\in G$, $x^{-1}*x=e\in H$ car H est un sous-groupe de G, i.e.$x\sim_{g,H} x$; c'est-à-dire que la relation $\sim_{g,H}$ est réflexive.

Par ailleurs pour tout $(x,y)\in G\times G$,

$$\begin{array}{lrcl} & x & \sim_{g,H} & y \\ \text{(cf. I.2.1.1,)}\Rightarrow & x^{-1}*y & \in & H \\ H \text{ est un groupe}\Rightarrow & y^{-1}*x\ =\ (x^{-1}*y)^{-1} & \in & H \\ \text{(cf. I.2.1.1,)}\Rightarrow & y & \sim_{g,H} & x\ ; \end{array}$$

la relation $\sim_{g,H}$ est donc symétrique.

Enfin, pour tout $(x, y, z) \in G \times G \times G$,

$$\begin{array}{lrcl} & x \sim_{g,H} y & \text{et} & y \sim_{g,H} z \\ \overset{\Rightarrow}{\text{(cf. I.2.1.1,)}} & x^{-1} * y \in H & \text{et} & y^{-1} * z \in H \\ \overset{\Rightarrow}{H \text{ est un groupe}} & x^{-1} * y * y^{-1} * z & \in & H \\ \Rightarrow & x^{-1} * z & \in & H \\ \overset{\Rightarrow}{\text{(cf. I.2.1.1,)}} & x & \sim_{g,H} & z \ ; \end{array}$$

c'est-à-dire que la relation $\sim_{g,H}$ est transitive.

Les arguments valent également pour $\sim_{d,H}$.

ii) Pour tout $x \in G$, un élément y de G appartient à la classe de x modulo $\sim_{g,H}$ si et seulement si $x^{-1} * y \in H$ (cf. I.2.1.1) c'est-à-dire si et seulement si il existe $h \in H$ tel que $x^{-1} * y = h$, i.e.si et seulement si $y \in x * H$ (cf. I.2.1.)

iii) Pour tout $x \in G$, l'application

$$\begin{array}{ccc} G & \to & G \\ g & \mapsto & x * g \end{array}$$

induit par restriction une application $H \to x * H$ dont la bijection réciproque est

$$\begin{array}{ccc} G & \to & G \\ g & \mapsto & x^{-1} * g \ . \end{array}$$

iv) Ce dernier résultat provient de ce que l'union des classes d'équivalence est égale à G et que toutes ces classes ont même cardinal égal à celui de H. Il faut aussi remarquer, pour prouver la deuxième partie de l'égalité, que l'ensemble des classes selon $\sim_{g,H}$ est en bijection avec l'ensemble des classes selon $\sim_{d,H}$.

Définition I.2.3 Étant donnés un groupe $(G, *)$ et H un sous-groupe de $(G, *)$,

i) on appelle *indice de H dans G* le nombre de classes d'équivalences pour la relation $\sim_{d,H}$ (cf. I.2.1,) encore égal au nombre de classes d'équivalences pour la relation $\sim_{g,H}$ (cf. I.2.24).

ii) on appelle ordre de H dans G le nombre d'éléments de H (si celui-ci est fini, sinon on pourra convenir que l'ordre est infini.)

Corollaire I.2.4 *Étant donné un groupe fini $(G, *)$ et H un sous-groupe de $(G, *)$, le cardinal de H divise le cardinnal de G.*

Preuve *: (cf. I.2.2.iv).)*

Définition I.2.5 i) Étant donné un groupe $(G, *)$, on dit que deux éléments x et y de G sont *conjugués* s'il existe un élément $g \in G$ tel que

$$x = g * y * g^{-1} .$$

ii) Étant donnée une partie E de G (pas nécessairement un sous-groupe,) on appelle *conjugué de E par g* et on note

$$g * E * g^{-1} := \{g * x * g^{-1} , \ x \in E\}$$

l'ensemble des conjugués d'éléments de E par g.

Remarque I.2.6 On pourrait également introduire la notion (qui s'est déjà révélée utile) de conjugaison d'un élément x d'un ensemble E par un élément g d'un groupe G alors que x n'appartient pas nécessairement à G mais pour peu que $g * x$ et $x * g^{-1}$ soient néanmoins définis. C'est notamment le cas si E est l'ensemble $\mathrm{End}(V)$ des endomorphismes d'un K-espace vectoriel V et si $g \in \mathrm{GL}(V)$.

Proposition I.2.7 *i) La relation de conjugaison sur les éléments d'un groupe G est une relation d'équivalence sur G.*

ii) La relation de conjugaison sur les parties d'un groupe G est une relation d'équivalence sur l'ensemble $\mathcal{P}(G)$ des parties de G.

Proposition I.2.8 *Si H est un sous-groupe d'un groupe G, tout conjugué $g * H * g^{-1}$ de H par un élément g de G est un sous-groupe de G.*

Proposition I.2.9 *Étant donné un groupe G et H un sous-groupe de G, les assertions suivantes sont équivalentes :*

a) Pour tout $g \in G$, $g * H = H * g$ c'est-à-dire

$$\{g * h, \ h \in H\} = \{h * g, \ h \in H\} .$$

b) Pour tout $g \in G$, $g * H * g^{-1} = H$,

c) Pour tout $g \in G$, $g * H * g^{-1} \subset H$.

Preuve *:*

b) $\Rightarrow$ *c) est immédiat.*

c) $\Rightarrow$ *a) Soit* $g \in G$. *Pour tout* $x \in g * H$, *il existe* $y \in H$, *tel que* $x = g * y$ *i.e.*$x * g^{-1} = g * y * g^{-1}$. *Or, d'après (c),* $g * y * g^{-1} \in H$. *Il existe donc* $z \in H$ *tel que*

$$x * g^{-1} = g * y * g^{-1} = z \, ,$$

d'où $x = z * g$ *c'est-à-dire que* $x \in H * g$. *On vient donc de montrer que (c) implique que* $g * H \subset H * g$.
L'inclusion réciproque s'obtient par le même argument, en appliquant cette fois (c) à l'élément g^{-1}.

a) $\Rightarrow$ *b) Soit* $g \in G$. *Pour tout* $x \in g * H * g^{-1}$, *il existe* $y \in H$ *tel que* $x = g * y * g^{-1}$. *Or* $g * y \in g * H$. *D'après (a),* $g * y \in H * g$. *Il existe donc* $z \in H$ *tel que* $g * y = z * g$ *; c'est-à-dire que*

$$x = g * y * g^{-1} = z * g * g^{-1} = z \in H \, .$$

On vient donc de démontrer que (a) implique que $g * H * g^{-1} \subset H$.
Réciproquement, pour tout $x \in H$, $g^{-1} * x \in g^{-1} * H$. *D'après (a) ,* $g^{-1} * x \in H * g^{-1}$. *Il existe donc* $y \in H$ *tel que* $g^{-1} * x = y * g^{-1}$ *c'est-à-dire*

$$x = g * y * g^{-1} \in g * H * g^{-1} \, .$$

On vient donc de montrer que $H \subset g * H * g^{-1}$ *; ce qui termine la preuve.*

Définition I.2.10 Étant donné un groupe $(G, *)$ un sous-groupe H vérifiant l'une des trois propriétés équivalentes de la proposition I.2.9 est dit *distingué* ou *normal.*

Exemple I.2.11 a) Le noyau $\mathrm{Ker}\, f$ d'un morphisme de groupes $f : G \to H$ est un sous-groupe distingué de G. En particulier, $\{e_G\} = \mathrm{Ker}\, \mathrm{Id}_G$ est distingué.

b) Le groupe G vue comme sous-groupe de lui-même est distingué.

c) Si G est un groupe abélien (cf. I.1.3) tout sous-groupe de G est distingué.

d) Si E est un $\mathbb{R}$-espace vectoriel euclidien, le groupe spécial orthogonal $\mathcal{SO}_{<>}(E)$ est un sous-groupe distingué du groupe orthogonal $\mathcal{O}_{<>}(E)$.

Définition I.2.12 Si $\sim$ est une relation d'équivalence sur un groupe $(G, *)$, on dit que $\sim$ est *compatible à la structure de groupe* si pour tout quadruplet (x, x', y, y') d'éléments de G,

$$x \sim y \text{ et } x' \sim y' \Rightarrow xx' \sim yy'.$$

Proposition I.2.13 *Soit G un groupe.*

i) Une relation d'équivalence $\sim$ sur G est compatible si et seulement si pour tout $(x, y) \in G \times G$,

$$x \sim y \Leftrightarrow x^{-1} * y \sim e\,.$$

ii) La classe $\overline{e}$ de l'élément neutre e est un sous-groupe distingué de G.

iii) Étant donné un sous-groupe distingué H de G, les relations $\sim_{g,H}$ (cf. I.2.1.1) et $\sim_{d,H}$ (cf. I.2.1.2) coïncident c'est-à-dire sont une même relation

$$\sim_H := \sim_{g,H} = \sim_{d,H} \qquad 1$$

qui est compatible.

iv) Étant donné un sous-groupe distingué H de G, la relation $\sim_H$ compatible définie ci-dessus est la seule relation d'équivalence compatible $\sim$ sur G telle que $\overline{e} = H$.

Preuve *:*

i Si $\sim$ est une relation d'équivalence compatible sur G, comme $\sim$ est réflexive, pour tout $x \in G$, $x^{-1} \sim x^{-1}$. Comme $\sim$ est compatible, si $y \sim x$,

$$x^{-1} * y \sim x^{-1} * x = e\,.$$

Réciproquement, si x et y dans G sont tels que $x^{-1} * y \sim e$, comme $x \sim x$ et que $\sim$ est compatible,

$$y = x * x^{-1} * y \sim x * e = x\,.$$

ii Par définition même d'une classe d'équivalence, $e \in \overline{e}$. Si $x \in \overline{e}$, comme $x^{-1} \sim x^{-1}$, (par réflexivité de $\sim$,)

$$e = x^{-1} * x \sim x^{-1} * e = x^{-1}\,,$$

(par compatibilité ;) i.e.$x^{-1} \in \overline{e}$. Enfin si $(x, y) \in \overline{e} \times \overline{e}$,

$$x * y \sim e * e = e\,,$$

(par compatibilité ;) i.e.$x * y \in \overline{e}$. D'après la proposition I.1.19, $\overline{e}$ est donc un sous groupe de G.

Pour tout $x \in \overline{e}$, *et tout* $y \in G$,

$$\begin{array}{rrcl} & x & \sim & e \\ \Rightarrow & y * x & \sim & y \\ \Rightarrow & y * x * y^{-1} & \sim & y * y^{-1} \\ \Rightarrow & y * x * y^{-1} & \sim & e \ ; \end{array}$$

c'est-à-dire que pour tout $y \in G$,

$$y * \overline{e} * y^{-1} \subset \overline{e} \ ;$$

i.e., d'après la proposition I.2.9.c) $\overline{e}$ *est un sous-groupe distingué de* G.

iii En combinant I.2.2.iii) et I.2.9.a), il est clair que les classes selon $\sim_{g,H}$ *sont exactement les classes selon* $\sim_{d,H}$; *c'est-à-dire, de manière presque tautologique, que* $\sim_{g,H} = \sim_{d,H}$ *est une relation d'équivalence que l'on notera* $\sim_H$.
Soient donnés des éléments x, x', y, y' *de* G *tels que :*

$$\begin{array}{lrcl} & x \sim_H x' & \text{et} & y \sim_H y' \\ \Rightarrow & x \sim_{g,H} x' & \text{et} & y \sim_{d,H} y' \\ \overset{\Rightarrow}{\text{(cf. I.2.1.1,)}} & x^{-1} * x' \in H & \text{et} & y^{-1} * y' \in H \\ H \text{ est } \overset{\Rightarrow}{\text{distingué}} & x^{-1} * x' \in H & \text{et} & x^{-1} * (y^{-1} * y') * x \in H \\ H \text{ est un } \overset{\Rightarrow}{\text{groupe}} & (x^{-1} * y^{-1} * y' * x) * (x^{-1} * x') & \in & H \\ \Rightarrow & x^{-1} * y^{-1} * y' * x' & \in & H \\ \Rightarrow & (y * x)^{-1} * (y' * x') & \in & H \\ \overset{\Rightarrow}{\text{(cf. I.2.1.1,)}} & y' * x' & \sim & y * x \ ; \end{array}$$

ce qui prouve que $\sim_H$ *est compatible.*

iv Il est clair que la classe de e *selon* $\sim_H$ *pour tout sous-groupe distingué* H *de* G *s'identifie à* H. *L'unicité de* $\sim_H$ *sous les conditions de (iv) découle alors du lemme plus général :*

Lemme I.2.14 *Étant donné un groupe* G *et deux relations d'équivalence* $\sim_1$ *et* $\sim_2$ *compatibles sur* G, *on note* $\overline{x}_1$ *(resp.* $\overline{x}_2$*) la classe d'un élément* x *de* G *selon* $\sim_1$ *(resp.* $\sim_2$.)
Alors les assertions suivantes sont équivalentes :

a) Les relations $\sim_1$ *et* $\sim_2$ *coïncident c'est-à-dire que pour tout* $(x, y) \in G \times G$,

$$x \sim_1 y \Leftrightarrow x \sim_2 y \ .$$

b) Pour tout $x \in G$

$$\overline{x}_1 = \overline{x}_2 \ .$$

c) Il existe $g \in G$ *tel que*

$$\overline{g}_1 = \overline{g}_2 .$$

d)

$$\overline{e}_1 = \overline{e}_2 .$$

***Preuve** :*

a) $\Leftrightarrow$ *b) est pour ainsi dire tautologique.*

b) $\Rightarrow$ *c) est immédiat.*

c) $\Rightarrow$ *d) Soit donné* $g \in G$*, tel que* $\overline{g}_1 = \overline{g}_2$*. Pour tout*

$$\begin{array}{lll}
 & x \in \overline{e}_1 & \\
\Rightarrow & x \sim_1 e & \\
\overset{\Rightarrow}{\sim_1} \textit{ est compatible etréflexive} & x * g \sim_1 g & \\
\Rightarrow & x * g \in \overline{g}_1 & \\
\overset{\Rightarrow}{c)} & x * g \in \overline{g}_2 & \\
\Rightarrow & x * g \sim_2 g & \\
\overset{\Rightarrow}{\sim_2} \textit{ est réflexiveet compatible} & x * g * g^{-1} \sim_2 g * g^{-1} = e & \\
\Rightarrow & x \sim_2 e . &
\end{array}$$

On vient donc de montrer que $\overline{e}_1 \subset \overline{e}_2$*. Le raisonnement étant parfaitement symétrique, on peut montrer, de la même manière, l'inclusion réciproque.*

d) $\Rightarrow$ *a) Pour tout* $(x, y) \in G$*, si* $x \sim_1 y$*, alors, d'après I.2.13.i)*

$$\begin{array}{lll}
 & x^{-1} * y \sim_1 e & \\
\Rightarrow & x^{-1} * y \in \overline{e}_1 & \\
\overset{\Rightarrow}{d)} & x^{-1} * y \in \overline{e}_2 & \\
\Rightarrow & x \sim_2 y . &
\end{array}$$

Le raisonnement étant évidemment symétrique, on montrerait, exactement de la même manière que si $x \sim_2 y$ *alors* $x \sim_1 y$*; ce qui termine la preuve.*

Proposition I.2.15 *Étant donné un groupe* $(G, *)$*, si* H *est un sous-groupe distingué (cf. I.2.10d)e* $(G, *)$*, il existe une unique structure de groupe sur le quotient* $G/\sim_H$ *(cf. I.2.13ii) telle que la surjection canonique* $G \to G/\sim_H$ *(cf. 0.12.ii))soit un morphisme de groupes.*

***Preuve** :*

Analyse : *S'il existe une structure de groupe $\dagger$ sur l'ensemble $G/\sim_H$ des classes d'équivalence selon $\sim_H$, nécessairement, pour tout quadruplet (x, x', y, y') d'éléments de G tel que*

$$x \sim_H x' \text{ et } y \sim_H y' ,$$

$$\begin{array}{rcl} \pi_H(x*y) & \overset{=}{GR_5} & \pi_H(x) \dagger \pi_H(y) \\ & = & \pi_H(x') \dagger \pi_H(y') \\ & \overset{=}{GR_5} & \pi_H(x'*y') . \end{array}$$

Comme π_H est surjective, la structure $\dagger$ est nécessairement unique.

Synthèse : *Comme $\sim_H$ est compatible à $(G,*)$ (cf. I.2.13.iii),*

$$\begin{array}{rcl} \pi_H(x*y) & = & \overline{x*y} \\ & = & \overline{x'*y'} \\ & = & \pi_H(x'*y') ; \end{array}$$

on peut donc poser, pour tout $(\overline{x}, \overline{y}) \in G/\sim_H \times G/\sim_H$,

$$\overline{x} \dagger \overline{y} := \overline{u*v} ,$$

(cf. I.1.5.b)) pour n'importe quel élément $u \in \overline{x}$ (resp. $v \in \overline{y}$;) ce qui prouve l'existence de la structure $\dagger$.

Définition I.2.16 Étant donné un groupe $(G,*)$ et un sous-groupe distingué H de $(G,*)$, on appelle *groupe quotient* de G par H et l'on note G/H l'ensemble $G/\sim_H$ (cf. I.2.2.3) muni de l'unique structure de groupe déduite de la proposition I.2.15.

Proposition I.2.17 *Étant donné un groupe $(G,*)$, les données suivantes sont équivalentes, au sens où la donnée de l'une d'entre elles permet de construire canoniquement les autres :*

i) Un sous-groupe distingué K de G.

ii) Une relation d'équivalence $\sim$ compatible sur G.

iii) Un morphisme de groupes surjectif $p : G \to I$.

Preuve *:*

- α *On a vu, grâce à la proposition I.2.13, qu'à toute relation compatible $\sim$ on associe canoniquement un sous-groupe distingué $K := \overline{e}$ et que, réciproquement, à tout sous-groupe distingué K on associe une unique relation compatible telle que $\overline{e} = K$.*
- β *On a vu également, grâce à la proposition I.2.15, qu'à tout sous-groupe distingué (ou de manière équivalente à toute relation d'équivalence compatible) on associe une surjection $\pi_K : G \to G/K$ qui est un morphisme de groupes.*
- γ *Réciproquement, à tout morphisme surjectif $p : G \to I$, on peut associer le sous-groupe distingué $K := \mathrm{Ker}\, p$ (cf. I.2.11.a).)*
- *Le lemme suivant établit qu'en fait, les procédés β et γ sont "inverses" l'un de l'autre, en un certain sens.*

Lemme I.2.18 *Étant donné un morphisme surjectif de groupes $p : G \to I$, il existe un unique isomorphisme de groupes $\phi : G/\mathrm{Ker}\, p \to I$ tel que $p = \phi \circ \pi$, où π est la surjection canonique $G \to G/\mathrm{Ker}\, p$.*

Preuve *:*

- *Si ϕ existe, alors nécessairement, pour tout $x \in G$, $\phi[\pi(x)] = p(x)$; ce qui suffit à prouver l'unicité de ϕ puisque π est surjective.*
- *Pour tout $(x, x') \in G \times G$, si $p(x) = p(x')$, $x^{-1} * x' \in \mathrm{Ker}\, p$ c'est-à-dire, d'après I.2.13.iii).1 $x \sim_{\mathrm{Ker}\, p} x'$. Ce qui implique que*

$$\pi(x) = \overline{x} = \overline{x'} = \pi(x') .$$

On définit donc bien ainsi une application $\phi : G/\sim_H \to p(G)$ en posant, pour tout $x \in G$, $\phi[\pi(x)] := p(x)$.

Il est clair que, pour tout $x \in G$, par définition même de ϕ, $\pi(x)$ est un antécédent par ϕ de $p(x)$; ce qui prouve, comme π est surjective, que ϕ l'est aussi.

Pour tout couple $(\xi, \eta) \in G/\mathrm{Ker}\, p \times G/\mathrm{Ker}\, p$, il existe un couple $(x, y) \in G \times G$ tel que $\xi = \pi(x)$ et $\eta = \pi(y)$ puisque π est surjective. Si $\phi(\xi) = \phi(\eta)$ alors

$$\begin{array}{rrcl} & p(x) & = & p(y) \\ \Rightarrow & x & \sim_{\mathrm{Ker}\, p} & y \\ \Rightarrow & x^{-1} * y & \in & \mathrm{Ker}\, p \\ \Rightarrow & \pi(x) & = & \pi(y) \\ \Rightarrow & \xi & = & \eta \, ; \end{array}$$

ce qui prouve que ϕ est injective.

L'application ϕ est donc bijective.

Enfin pour tout couple (ξ, η) et tout couple (x, y) comme précédemment,

$$\begin{aligned}\phi(\xi *_{G/\mathrm{Ker}\, p} \eta) &= \phi[\pi(x) *_{G/\mathrm{Ker}\, p} \pi(y)] \\ &= \phi[\pi(x * y)] \\ &= p(x * y) \\ &= p(x) *_I p(y) \\ &= \phi[\pi(x)] *_I \phi[\pi(y)] \\ &= \phi(\xi) *_I \phi(\eta)\ ;\end{aligned}$$

ce qui prouve que ϕ vérifie l'axiome GR_5 et donc que ϕ est un morphisme de groupes. La proposition I.1.12 prouve finalement que ϕ est un isomorphisme.

Corollaire I.2.19 *Plus généralement, pour tout morphisme de groupes $f : G \to G'$ tel que $f(K) = \{e'_G\}$ (i.e.tel que $K \subset \mathrm{Ker}\, f$) pour K un sous-groupe distingué de G, il existe un unique morphisme $\phi : G/K \to G'$ tel que $f = \phi \circ \pi$ où $\pi : G \to G/K$ est la surjection canonique*

Preuve *: On peut tout d'abord noter $I := \mathrm{Im}\, f$, $p : G \to I$ l'application f elle-même vue à valeurs dans I et $i : I \to G'$ l'injection canonique de I dans G' (cf. 0.5.iii).)*

On a alors $p \circ i = f$ et p est un morphisme surjectif tandis que i est un morphisme injectif. De plus, il est facile de vérifier que $\mathrm{Ker}\, p = \mathrm{Ker}\, f$.

On peut donc, grâce au lemme I.2.18, construire un unique isomorphisme

$$\chi : G/\mathrm{Ker}\, p = G/\mathrm{Ker}\, f \to I$$

tel que $\chi \circ \pi_f = p$, où π_f désigne la surjection canonique $G \to G/\mathrm{Ker}\, f$.

Comme $K \subset \mathrm{Ker}\, f$, pour tout $x \in G$, $x * K \subset x * \mathrm{Ker}\, f$, c'est-à-dire, d'après I.2.2.iii), que toute classe modulo K est incluse dans au moins une classe modulo $\mathrm{Ker}\, f$, mais également dans au plus une classe selon $\mathrm{Ker}\, f$ car ces dernières sont deux à deux disjointes. À toute classe modulo K on peut donc associer une unique classe modulo $\mathrm{Ker}\, f$ la contenant. Ceci permet de définir une application $\mu : G/K \to G/\mathrm{Ker}\, f$.

On laisse le soin au lecteur de prouver que

— μ est un morphisme de groupes,

— $\mu \circ \pi = \pi_f$.

Il résulte de ce qui précède que

$$\begin{aligned} f &= i \circ p \\ &= i \circ \chi \circ \pi_f \\ &= i \circ \chi \circ \mu \circ \pi\ .\end{aligned}$$

En posant $\phi := i \circ \chi \circ \mu$, on prouve son existence.

L'unicité est laissée en exercice et l'on conseille de se reporter au paragraphe II.6 où cette question est traitée dans le détail pour le cas des groupes abéliens, les techniques étant exactement les mêmes.

Remarque I.2.20 Si G est un groupe abélien tout sous-groupe de G est distingué. La définition du groupe quotient donnée en I.2.16 coïncide avec celle d'un $\mathbb{Z}$-module quotient donnée en II.5.5.

Proposition I.2.21 *Pour tout groupe $(G, *)$ et x un élément de G,*

- *l'image $\mathrm{Im}\,\epsilon_x$ du morphisme*

$$\begin{array}{rcl} \epsilon_x : \mathbb{Z} & \to & G \\ 1 & \mapsto & x \end{array}$$

  (cf. I.1.10.b),) est un groupe abélien ;
- *si G est de cardinal fini, l'ordre de $\mathrm{Im}\,\epsilon_x$ est le plus petit entier positif d tel que $\epsilon_x(d) = x^d = e_G$.*

Preuve *:*

- *D'après I.1.17.b), $\mathrm{Im}\,\epsilon_x$ est un sous-groupe de G. Or pour tout $(g, h) \in \mathrm{Im}\,\epsilon_x \times \mathrm{Im}\,\epsilon_x$, il existe $(r, s) \in \mathbb{Z} \times \mathbb{Z}$ tel que*

$$\begin{array}{rcl} \epsilon_x(r) & = & g \\ \epsilon_x(s) & = & h\ . \end{array}$$

  Il s'ensuit que

$$\begin{array}{rcl} g *_G h & = & \epsilon_x(r) *_G \epsilon_x(s) \\ & = & \epsilon_x(r +_{\mathbb{Z}} s) \\ & = & \epsilon_x(s +_{\mathbb{Z}} r) \\ & = & \epsilon_x(s) *_G \epsilon_x(r) \\ & = & h *_G g\ . \end{array}$$

- *Il s'ensuit que ϵ_x induit un morphisme surjectif de groupes abéliens $\mathbb{Z} \to \mathrm{Im}\,\epsilon_x$. Si G est fini ce morphisme ne peut pas être injectif car $\mathbb{Z}$ est infini. Le noyau de ϵ_x est donc un sous-groupe (distingué) de $\mathbb{Z}$. On sait qu'il existe un unique entier $d > 0$ tel qu'un tel sous-groupe soit de la forme $d\mathbb{Z}$. L'entier d est le plus petit entier strictement positif appartenant à $\mathrm{Ker}\,\epsilon_x$ donc le plus petit entier strictement positif tel que $x^d = e_G$.*
  Par ailleurs, le lemme I.2.19 prouve qu'il existe un isomorphisme canonique $\mathbb{Z}/d\mathbb{Z} \cong \mathrm{Im}\,\epsilon_x$ ce qui prouve que $\#(]\mathrm{Im}\,\epsilon_x] = d$.

Définition I.2.22 Étant donné un groupe $(G, *)$ pour tout $x \in G$ on appelle *ordre de* x l'ordre du sous-groupe $\mathrm{Im}\,\epsilon_x$ où ϵ_x est défini comme dans la proposition I.2.21.

Corollaire I.2.23 *Étant donné un groupe fini $(G, *)$ l'ordre d'un élément $x \in G$, divise le cardinal de G.*

Preuve *: C'est une conséquence quasi-immédiate de ce qui précède et de la formule I.2.2.iv).*

Proposition I.2.24 *Dans un groupe G, deux éléments conjugués ont même ordre.*

I.3 . −Quelques résultats sur les groupes finis

Proposition I.3.1 *Si $(G, *)$ est un groupe fini, une partie H de G munie de la loi de composition $*$ est un sous-groupe de G si H est non-vide et pour tout $(x, y) \in H \times H$, $x * y \in H$.*

Proposition I.3.2 *Si G est un groupe fini de cardinal p premier, G est isomorphe (non canoniquement) à $(\mathbb{Z}/p, +)$ et donc commutatif (abélien).*

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

Définition I.3.3 Un groupe fini G de cardinal $n \in \mathbb{N}^*$ est *cyclique* s'il est engendré par un seul élément, c'est-à-dire s'il existe un élément $g \in G$ tel que l'image du morphisme

$$\begin{array}{rccc} \phi_g : & \mathbb{Z} & \to & G \\ & 1 & \mapsto & g \end{array}$$

(cf. I.1.10.c)) soit égale à G (cf. I.1.25.)

Le lemme I.2.19 montre qu'alors $G \cong \mathbb{Z}/n$ et est donc commutatif (*abélien*.)

I.4 . −Groupe symétrique

Définition I.4.1 Étant donné un ensemble fini E on appelle *permutation* ou encore *substitution* de E toute bijection de E sur lui-même.

On note $\mathcal{S}(E)$ l'ensemble des permutations de E.

Proposition I.4.2 *Le couple $(\mathcal{S}(E), \circ)$ est un groupe (cf. I.1.1.)*

Définition I.4.3 Si $E := \{1, 2, \ldots, n\}$ est l'ensemble des n premiers entiers non nuls, le groupe $\mathcal{S}(E)$ est noté $\mathcal{S}_n$ et appelé *groupe symétrique d'ordre* n. Pour tout $s \in \mathcal{S}_n$, on adoptera la notation :

$$s := \begin{array}{cccc} 1 & 2 & \ldots & n \\ s(1) & s(2) & \ldots & s(n)\,. \end{array}$$

Proposition I.4.4 *i) Le cardinal de $\mathcal{S}_n$ c'est-à-dire le nombre d'éléments de $\mathcal{S}_n$ est égal à $n!$.*

ii) Si E est un ensemble fini à n éléments toute bijection $E \to \{1, 2, \ldots, n\}$ définit un isomorphisme de groupes $\mathcal{S}(E) \cong \mathcal{S}_n$ (cf. I.1.11.)

***Preuve** :*

i) Soit

$$\Sigma := \{s \in \mathcal{S}_{n+1} \mid s(n+1) = n+1\} .$$

Il est très facile de vérifier que Σ est un sous-groupe de $\mathcal{S}_{n+1}$ isomorphe à $\mathcal{S}_n$. Le sous-groupe Σ ne sera pas, en général, distingué (cf. I.2.10,) en revanche on peut toujours considérer sur $\mathcal{S}_{n+1}$ la relation d'équivalence $\sim_{g,\Sigma}$ (cf. I.2.1.1i)nduite par Σ. On a alors, pour tout $(s, s') \in \mathcal{S}_{n+1} \times \mathcal{S}_{n+1}$,

$$\begin{array}{rrcl} & s & \sim_{g,\Sigma} & s' \\ \Leftrightarrow & s^{-1} \circ s' & \in & \Sigma \\ \Leftrightarrow & s^{-1} \circ s'(n+1) & = & n+1 \\ \Leftrightarrow & s'(n+1) & = & s(n+1) . \end{array}$$

Autrement dit, la classe de s est l'ensemble des permutations de $\{1; \ldots; n+1\}$ telles que $n+1$ ait pour image $s(n+1)$. On voit donc qu'il y a autant de classes que d'images possibles pour $n+1$ c'est-à-dire $n+1$. Autrement dit,

$$\#(\mathcal{S}_{n+1}/\sim_{g,\Sigma}) = n+1.$$

En appliquant la formule I.2.2.iv), il vient

$$\#(\mathcal{S}_{n+1}) = \#(\Sigma).\#(\mathcal{S}_{n+1}/\sim_{g,\Sigma}) = \#(\Sigma).(n+1) = \#(\mathcal{S}_n).(n+1)$$

ce qui donne une formule de récurrence pour calculer $\#(\mathcal{S}_n)$ et donne bien $\#(\mathcal{S}_n) = n!$ en remarquant que $\#(S_1) = 1$.

ii) Étant donnée une bijection $\theta : E \to \{1; \ldots; n\}$, l'application qui à $s \in \mathcal{S}(E)$ associe $\theta \circ s \circ \theta^{-1}$ définit un isomorphisme de groupes $\mathcal{S}(E) \cong \mathcal{S}_n$, ce qui est très facile à vérifier.

I.4.5 . −Notations

Dans toute la suite, on fixe un entier $n \geq 1$ et on étudiera désormais $\mathcal{S}_n$ pour $n \in \mathbb{N}^*$. Pour tout $s \in \mathcal{S}_n$, et tout $k \in \mathbb{Z}$, on notera s^k l'image de k dans $\mathcal{S}_n$ par l'unique morphisme $\mathbb{Z} \to \mathcal{S}_n$ défini par $1 \mapsto s$ (cf. I.1.10.c).)

Pour tout $s \in \mathcal{S}_n$, on définit la relation binaire R_s sur $[1; n] := \{1; 2; \ldots; n\}$ par : aR_sb s'il existe $k \in \mathbb{Z}$ tel que

$$b = s^k(a). \qquad \text{I.4.5.1}$$

Proposition I.4.6 *Pour tout $s \in \mathcal{S}_n$ la relation R_s, définie ci-dessus, est une relation d'équivalence.*

Définition I.4.7 La classe d'équivalence d'un élément a de $\{1, 2, \ldots, n\}$ est appelée *orbite de a suivant s* et notée $O_s(a)$.

Définition I.4.8 i) On appelle *cycle* une permutation c dont toutes les orbites sont réduites à un seul élément sauf une que l'on note $O_c(a)$.

ii) L'orbite $O_c(a)$ est appelée *support du cycle c.*

iii) Le cardinal de $O_c(a)$ est appelé *longueur du cycle c.*

iv) Un cycle de longueur 2 est appelé *transposition* et on note t_{ij} la transposition telle que : $t_{ij}(i) = j$ et $t_{ij}(j) = i$, pour $1 \leq i \leq n$ et $1 \leq j \leq n$ $i \neq j$.

v) Un cycle de longueur n est appelé *permutation circulaire.*

Remarque I.4.9 L'inverse d'une transposition est elle-même $t_{ij}^{-1} = t_{ij}$. On dit que t_{ij} est *involutive*.

Proposition I.4.10 *Étant donné un cycle $c \in \mathcal{S}_n$, de longueur l, et de support S,*

i) pour tout $a \in S$, l'application

$$\begin{array}{ccc} \mathbb{Z} & \to & S \\ m & \mapsto & c^m(a) \end{array}$$

induit une bijection $\phi_a : \mathbb{Z}/l \to S$, telle que

$$\phi_a(\overline{m}) = c^m(a)\,; \qquad 1$$

(où $\overline{m}$ est la classe de m modulo l.)

ii) L'entier l est l'ordre de c dans $\mathcal{S}_n$ (cf. I.2.22.)

Preuve *:*

i) Soit $a \in S$*. Pour tout* $m \in \mathbb{Z}$, $c^m(a) R_c a$ *par définition de* R_c *(cf. I.4.5.1.) Il s'ensuit donc que* $c^m(a) \in S$*. On définit donc bien une application à valeurs dans* S*. L'ensemble* $[1;n]$ *étant fini,* $S \subset [1;n]$ *est fini ; ce qui implique que* $m \mapsto c^m(a)$ *n'est pas injective ; i.e.il existe au moins deux entiers* $p > q$ *tels que*

$$\begin{array}{rcl} c^p(a) & = & c^q(a) \\ \Leftrightarrow \quad c^{p-q}(a) & = & a\ . \end{array}$$

L'ensemble

$$K := \{m \in \mathbb{Z} \mid c^m(a) = a\}$$

est donc non réduit à $\{0\}$*. Par ailleurs,* $K \neq \mathbb{Z}$*. En effet,* $c(a) \neq a$ *car* $a \in S$ *i.e.*$1 \notin K$*. Enfin pour tout* $(k, k') \in K \times K$,

$$\begin{array}{rcl} c^{k+k'}(a) & = & c^{k'}[c^k(a)] \\ & = & c^{k'}(a) \\ & = & a\ . \end{array}$$

De plus si $c^k(a) = a$, $c^{-k}[c^k(a)] = c^{-k}(a)$ *i.e.*$c^{-k}(a) = a$*. D'après la proposition I.1.19* K *est un sous-groupe de* $\mathbb{Z}$*. Il existe donc, (cf. I.1.20)un entier* $k_0 > 1$ *tel que* $K = k_0\mathbb{Z}$*.*

Pour tout $b \in S$*, il existe* $m \in \mathbb{Z}$ *tel que* $b = c^m(a)$ *puisque* $bR_c a$*. L'application*

$$\begin{array}{rcl} \mathbb{Z} & \to & S \\ m & \mapsto & c^m(a) \end{array}$$

est donc surjective.

Pour tout p, q *tels que* $p = q + mk_0$,

$$\begin{array}{rcl} c^p(a) & = & c^{q+mk_0}(a) \\ & = & c^q(c^{mk_0}(a)) \\ & = & c^q(a)\ . \end{array}$$

On peut donc définir une application $\phi_a : \mathbb{Z}/k_0 \to S$ *par* $\phi_a(\mu) := c^m(a)$ *où* m *est n'importe quel représentant de* μ *modulo* k_0*. L'application* ϕ_a *est clairement surjective.*

Soient $(\mu, \eta) \in \mathbb{Z}/k_0 \times \mathbb{Z}/k_0$, $(p, q) \in \mathbb{Z} \times \mathbb{Z}$ *un couple de représentants de* (μ, η) *tel que*

$$\begin{array}{rcl} \phi_a(\mu) & = & \phi_a(\eta) \\ \Leftrightarrow \quad c^p(a) & = & c^q(a) \\ \Leftrightarrow \quad c^{p-q}(a) & = & a \\ \Leftrightarrow \quad p - q & \in & K \\ \Leftrightarrow \quad \mu & = & \eta\ ; \end{array}$$

c'est-à-dire que ϕ_a est injective.

L'application $\phi_a : \mathbb{Z}/k_0 \to S$ est donc une bijection entre deux ensembles finis. On en déduit que

$$k_0 \;=\; \#(\mathbb{Z}/k_0) \;=\; \#(S) \;=\; l.$$

ii) D'après ce qui précède, k_0 est indépendant de $a \in S$, il s'ensuit que pour tout $a \in S$, $c^{k_0}(a) = a$. Pour $a \notin S$, $c(a) = a$ d'où $c^{k_0}(a) = a$. On en déduit que $c^{k_0} = \mathrm{Id}_{[1;n]}$. L'entier k_0 est, par construction même, le plus petit vérifiant cette propriété ; il s'ensuit que c'est l'ordre de c dans $\mathcal{S}_n$.

Proposition I.4.11 *Soient c_1 et c_2 deux cycles de $\mathcal{S}_n$, de supports respectifs $S_1 := O_{c_1}(a_1)$ et $S_2 := O_{c_2}(a_2)$, tels que*

$$S_1 \;\cap\; S_2 \;=\; \emptyset\,.$$

Alors

$$c_1 \circ c_2 \;=\; c_2 \circ c_1\,.$$

***Preuve** :*

- *Pour tout $a \in S_1$,*

$$\begin{array}{lll} c_1(c_2(a)) & a \overset{=}{\notin} S_2 & c_1(a) \\ & c_1(a) \overset{=}{\notin} S_2 & c_2(c_1(a))\,. \end{array}$$

- *De même pour $a \in S_2$.*
- *Pour tout $a \in [1;n] \setminus (S_1 \cup S_2)$,*

$$\begin{array}{lll} c_1(c_2(a)) & a \overset{=}{\notin} S_2 & c_1(a) \\ & a \overset{=}{\notin} S_1 & a \\ & a \overset{=}{\notin} S_1 & c_1(a) \\ & c_1(a) \;=\; a \overset{=}{\notin} S_2 & c_2(c_1(a))\,. \end{array}$$

Comme $[1;n]$ est l'union disjointe

$$S_1 \;\cup\; S_2 \;\cup\; \big([1;n] \setminus (S_1 \cup S_2)\big)\,,$$

ce qui précède prouve que c_1 et c_2 vérifient sur $[1;n]$ l'identité

$$c_1 \;\circ\; c_2 \;=\; c_2 \;\circ\; c_1\,.$$

Proposition I.4.12 *Toute permutation qui n'est pas l'identité se décompose de manière unique en un produit de cycles dont les supports sont deux à deux disjoints.*

Preuve *: Soit* $s \in \mathcal{S}_n$ *une permutation différente de* $\mathrm{Id}_{[1;n]}$. *La permutation* s *possède au moins une orbite non réduite à un élément. Notons* $O_{i1 \leq i \leq d}$ *les orbites non réduites à un élément de* s. *Ces orbites sont des classes d'équivalence pour la relation* R_s *(cf. I.4.5.1 ;) elles sont donc deux à deux disjointes. Pour tout* $1 \leq i \leq d$ *on définit*

$$\begin{array}{rccc} c_i : & [1;n] & \to & [1;n] \\ & a & \mapsto & s(a) \quad \text{si } a \in O_i \\ & a & \mapsto & a \quad \text{si } a \notin O_i \ . \end{array}$$

Il est clair que la seule orbite non réduite à un élément de c_i *est* O_i *; donc que* c_i *est un cycle de support* O_i, *pour tout* $1 \leq i \leq d$. *Pour tout* $a \in [1;n] \setminus \bigcup_{1 \leq i \leq d} O_i$,

$$\prod_{i=1}^{d} c_i(a) \ = \ a \ = \ s(a)$$

car pour tout $1 \leq i \leq d$ $c_i(a) = a$ *et* $s(a) = a$.

Pour tout $1 \leq i \leq d$ *et tout* $a \in O_i$,

$$\begin{array}{rcl} \prod_{i=1}^{d} c_i(a) & \overset{=}{\text{(cf. I.4.11,)}} & \big(c_i \circ c_1 \circ \ldots \circ c_{i-1} \circ c_{i+1} \circ \ldots \circ c_d\big)(a) \\ & = & c_i(a) \\ & = & s(a) \ . \end{array}$$

Il s'ensuit que

$$s \ = \ \prod_{i=1}^{d} c_i \ .$$

L'unicité de la décomposition est laissée en exercice.

Définition I.4.13 Étant donnée une permutation $s \in \mathcal{S}_n$, on note $(l_1, \ldots, l_d)$ le d-uplet formé des longueurs des cycles qui la décomposent (cf. I.4.12e)n supposant $l_i \leq l_{i+1}$,$1 \leq i \leq d-1$, qu'on appelle *type cyclique* de s.

Proposition I.4.14 *Tout cycle* $c \in \mathcal{S}_n$ *se décompose en un produit de transpositions.*

Preuve : *Notons l la longueur du cycle et fixons un élément $a \in S$. Il définit une bijection $\phi : \mathbb{Z}/l \to S$ telle que $\phi(\eta) = c^m(a)$ pour m un représentant de η dans $\mathbb{Z}$ (cf. I.4.10.i)D)e cette manière on définit une "numérotation" des éléments de S :*

$$\begin{aligned} a_0 &:= a \\ a_1 &:= c(a) \\ \dots &\quad \dots \\ a_{l-1} &:= c^{l-1}(a) \, . \end{aligned}$$

La restriction du cycle c à S est alors "représentée" par la permutation circulaire de $[0; l-1]$:

$$\gamma := \begin{matrix} 0 & 1 & \dots & l-2 & l-1 \\ 1 & 2 & \dots & l-1 & 0 \end{matrix}$$

(cf. I.4.8.v)P)lus précisément on a :

$$c|S = \phi \circ \gamma \circ \phi^{-1} \, .$$

On vérifie aisément que

$$\gamma = \prod_{i=0}^{l-1} t_{\overline{i},\overline{i+1}} \, ,$$

où $\overline{m}$ désigne la classe de m modulo l pour tout $m \in \mathbb{Z}$ et $t_{\mu,\eta}$ $(\mu \neq \eta,)$ la transposition de $\mathbb{Z}/l$ définie par

$$\begin{aligned} t_{\mu,\eta}(\mu) &:= \eta \\ t_{\mu,\eta}(\eta) &:= \mu \, . \end{aligned}$$

Il s'ensuit que

$$\begin{aligned} c|S &= \phi \circ \gamma \circ \phi^{-1} \\ &= \phi \circ (\prod_{i=0}^{l-1} t_{\overline{i},\overline{i+1}}) \circ \phi^{-1} \\ &= \phi \circ (\prod_{i=0}^{l-1} t_{\overline{i},\overline{i+1}} \circ \phi^{-1} \circ \phi) \circ \phi^{-1} \\ &= \text{on développe le produit } \prod_{i=0}^{l-1} \phi \circ t_{\overline{i},\overline{i+1}} \circ \phi^{-1} \, . \end{aligned}$$

Or il est clair que pour tout $0 \leq i \leq l-1$ $\phi \circ t_{\overline{i},\overline{i+1}} \circ \phi^{-1}$ est une transposition de S. Il s'ensuit que $c|S$ est un produit de transpositions.

Par ailleurs $c|([1; n] \setminus S)$ est l'identité et pour tout $0 \leq i \leq l-1$ $(\phi \circ t_{\overline{i},\overline{i+1}} \circ \phi^{-1})$ est prolongée par l'identité sur $[1; n] \setminus S$. Ceci donne le résultat.

Corollaire I.4.15 *Toute permutation se décompose en un produit de transpositions.*

Preuve *: Ce résultat est une conséquence immédiate des propositions I.4.12 et I.4.14.*

Définition I.4.16 i) On appelle *signature* d'une permutation $s \in \mathcal{S}_n$, le nombre $\sigma(s) := (-1)^{n-m_s}$ (où m_s est le nombre d'orbites de la permutation s.)

ii) Une permutation dont la signature est égale à 1 (resp. -1) est dite *paire* (resp. *impaire*.)

Exemple I.4.17 a) La signature d'un cycle de longueur l est $(-1)^{l-1}$.

b) La signature d'une transposition est -1 ; *i.e.*une transposition est toujours impaire.

c) La signature d'une permutation circulaire est $(-1)^{n-1}$.

Proposition I.4.18 *Supposons $n > 1$. Étant donnée une permutation $s \in \mathcal{S}_n$, pour toute transposition*

$$t \in \mathcal{S}_n \ , \ \sigma(t * s) = \sigma(s * t) = -\sigma(s) = \sigma(t) * \sigma(s) \ .$$

Preuve *: Soit t une transposition de $[1;n]$ et $\{a;b\}$ la paire d'éléments distincts de $[1;n]$ tel que $t(a) = b$ et $t(b) = a$. On examinera successivement les deux situations où $O_s(a) = O_s(b)$ et $O_s(a) \neq O_s(b)$.*

- *Supposons que a et b appartiennent à une même orbite $O := O_s(a)$ de s. Notons $l := \#(O_s(a)$.*
  Pour tout $(x,y) \in O \times O$, notons

$$\overrightarrow{xy} := \phi_a^{-1}(y) - \phi_a^{-1}(x) \in \mathbb{Z}/l \qquad \textit{I.4.18.1}$$

(cf. I.4.10.i).) Cette notation peut, à première vue sembler étonnante mais on laisse au lecteur le soin de vérifier le lemme suivant qui confère à la dite notation sa cohérence. O est, en effet, vraiment un espace affine de dimension 1 sous $\mathbb{Z}/l$ si l est premier et un espace homogène principal sous le $\mathbb{Z}/l$-module libre $\mathbb{Z}/l$ dans le cas où $\mathbb{Z}/l$ est juste un anneau.

Lemme I.4.18.2 *i)* ***Relation de Chasles :*** *Pour tout triplet (x,y,z) d'éléments de O,*

$$\overrightarrow{xy} + \overrightarrow{yz} = \overrightarrow{xz} \ .$$

ii) ***Changement d'origine :*** *Pour tout $c \in O$, une origine non nécessairement égale à a, et tout $(x, y) \in O \times O$,*

$$\overrightarrow{xy} \;=\; \phi_c^{-1}(y) - \phi_c^{-1}(x)\;.$$

Enfin une propriété plus directement liée à la situation dans laquelle nous nous trouvons, si l'on note $||\overrightarrow{xy}||$ le représentant de $\overrightarrow{xy}$ dans l'intervalle $[0, l-1]$, est que :

$$\begin{array}{lll} s^{||\overrightarrow{xy}||}(x) & \text{(cf. I.4.18.2.ii),} & s^{||\phi_x^{-1}(y)-\phi_x^{-1}(x)||}(x) \\ & = & s^{||\phi_x^{-1}(y)||}(x) \\ & = & \phi_x[\phi_x^{-1}(y)] \\ & = & y\;. \end{array} \qquad \textit{I.4.18.3}$$

Remarquons, en outre, que l'application $||\cdot||$ vérifie les propriétés suivantes :

Lemme I.4.18.4 *i) Pour tout triplet (x, y, z) d'éléments de O,*

$$||\overrightarrow{xz}|| \;\leq\; ||\overrightarrow{xy}|| \;+\; ||\overrightarrow{yz}||\;.$$

ii) Pour tout $(x, y) \in O \times O$, $||\overrightarrow{xy}|| \;=\; 0$ si et seulement si $x \;=\; y$.

Remarque I.4.18.5 Dans les lemmes I.4.18.2 et I.4.18.4, nous n'avons pas énoncé de propriétés de compatibilité à la multiplication par un scalaire $\lambda \in \mathbb{Z}/l$ qui seraient nécessaires pour satisfaire aux axiomes des *espaces affines* et des *normes* mais dont nous n'aurons pas besoin ici.

On veut maintenant comprendre comment agit $s \circ t$ sur O. Remarquons d'abord que O est stable sous $s \circ t$. On note Ω_a (resp. Ω_b) l'orbite de a (resp. b) sous $s \circ t$ et on établit le lemme suivant :

Lemme I.4.18.6 *i) Les orbites Ω_a et Ω_b sont disjointes et*

$$O \;=\; \Omega_a \;\cup\; \Omega_b\;.$$

ii) Pour tout $x \;\in\; O$, $x \in \Omega_a$ (resp. $x \in \Omega_b$) si et seulement si

$$0 \;<\; ||\overrightarrow{bx}|| \;\leq\; ||\overrightarrow{ba}||\;,$$

(resp.

$$0 \;<\; ||\overrightarrow{ax}|| \;\leq\; ||\overrightarrow{ab}||\;.)$$

Preuve *:*

α *On prouve le sens réciproque de ii) par récurrence sur* $k := ||\overrightarrow{ax}||$, $0 < k < ||\overrightarrow{ba}||$.

† *Pour* $||\overrightarrow{bx}|| = 1$, *d'après I.4.18.3,*

$$x = s(b) = s[t(a)] ,$$

i.e.$x \in \Omega_a$.

† *Supposons* $(\sharp)$: $0 < ||\overrightarrow{bx}|| < ||\overrightarrow{ba}||$ *et* $x \in \Omega_a$. *L'identité* $\sharp$ *implique que :*

$$x \neq a \text{ et } x \neq b ,$$

d'où $t(x) = x$ *d'où* $s \circ t(x) = s(x)$ *i.e.*$s(x) \in \Omega_a$. *Il est facile de voir que*

$$||\overrightarrow{bs(x)}|| = ||\overrightarrow{bx}|| + 1 ,$$

ce qui constitue la clef de l'argument de réccurence.

l'argument relatif à Ω_b *est exactement identique puisque* a *et* b *jouent exactement le même rôle.*

β *Prouvons maintenant que* Ω_a *et* Ω_b *sont disjointes. Ces deux ensembles étant des classes d'équivalence, il suffit de montrer qu'ils sont distincts. Prouvons donc, par l'absurde, que* $b \notin \Omega_a$.
Si $b \in \Omega_a$, *il existe des entiers* $k \in \mathbb{N}$ *tels que* $(s \circ t)^k(a) = b$. *Soit* m *le plus petit d'entre eux. Comme* O *est stable sous* $s \circ t$, *nécessairement* $m \leq l$ *et, comme* $a \neq b$, $m \geq 1$.

$$\begin{array}{rrcl} & (s \circ t)^m(a) & = & b \\ \Leftrightarrow & (s \circ t)^{m-1}[s \circ t(a)] & = & b \\ \Leftrightarrow & (s \circ t)^{m-1}[s(b)] & = & b . \end{array} \qquad \textit{I.4.18.6.1}$$

Lemme I.4.18.6.2 *Or pour tout* $x \in O$ *tel que* $0 < ||\overrightarrow{bx}|| < ||\overrightarrow{ba}||$, *on a* $x \notin \{a; b\}$, *d'où* $t(x) = x$ *d'où* $s \circ t(x) = s(x)$.

Il s'ensuit que l'équation I.4.18.6.1 équivaut à :

$$\begin{array}{rrcl} & (s \circ t)^{m-||\overrightarrow{ba}||}[s^{||\overrightarrow{ba}||}(b)] & = & b \\ \overset{\Leftrightarrow}{\textit{(cf. I.4.18.3,)}} & (s \circ t)^{m-||\overrightarrow{ba}||}(a) & = & b , \end{array} \qquad \textit{I.4.18.6.3}$$

ce qui implique, par minimalité de m, *que*

$$m - ||\overrightarrow{ba}|| \leq 0 . \qquad \textit{I.4.18.6.4}$$

Or, par ailleurs, $m - ||\overrightarrow{ba}|| = 0$ *et l'équation I.4.18.6.3 impliqueraient* $a = b$ *ce qui est contraire aux hypothèses. Il s'ensuit, en appliquant I.4.18.6.2, que l'équation I.4.18.6.1 équivaut à*

$$s^m(b) = b\,.$$

Comme $m \neq 0$, *nécessairement on a :*

$$l = m < ||\overrightarrow{ba}|| \leq l\,;$$

ceci est évidemment contradictoire.

γ *En remarquant finalement que pour tout* $x \in O$, *soit* $||\overrightarrow{ax}|| < ||\overrightarrow{ab}||$, *soit* $||\overrightarrow{bx}|| < ||\overrightarrow{ba}||$ *on obient que*

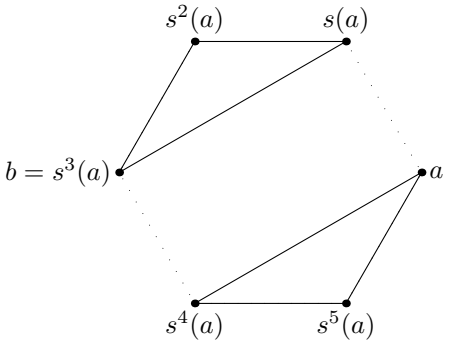
$$O = \{x \mid ||\overrightarrow{ax}|| < ||\overrightarrow{ab}||\} \cup \{x \mid ||\overrightarrow{bx}|| < ||\overrightarrow{ba}||\}\,.$$

Ceci prouve, grâce à la réciproque de ii), que nous avons prouvé en α, *que*

$$O = \Omega_a \cup \Omega_b\,;$$

cette union étant disjointe d'après β, *ce qui achève la preuve de i).*
Le sens direct de ii) découle aisément de ce qui précède.

On a illustré, dans le dessin ci-dessous, la situation dans le cas où $l = 6$ *et* $||\overrightarrow{ab}|| = 3$.



Les orbites de s *différentes de* O *restent des orbites sous* $s \circ t$ *puisque* t *restreinte à ces orbites est l'identité. Seule l'orbite* O *a donc été modifiée et transformée en deux orbites exactement. Il s'ensuit que* $s \circ t$ *a une orbite de plus que* s *et donc que* $\sigma(s \circ t) = -\sigma(s)$.

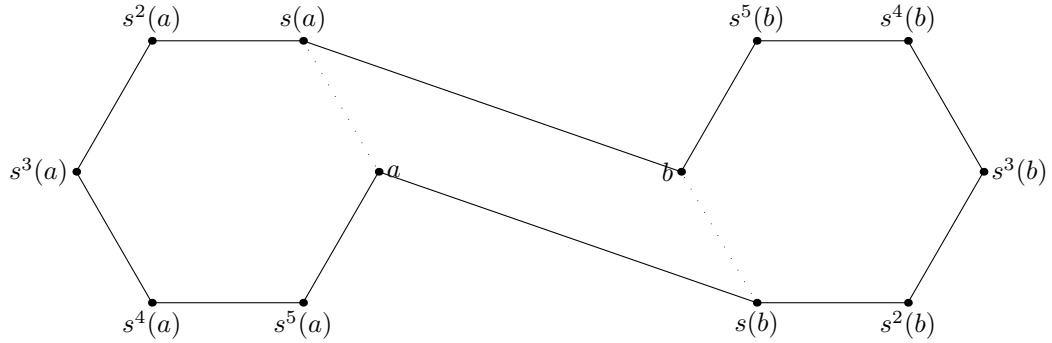
- *Supposons maintenant que a et b appartiennent respectivement à deux orbites distinctes O_a et O_b de s. Pour tout $x \in O_a$ tel que $||\overrightarrow{ax}|| > 0$, (cf. I.4.18.4,) $x \notin \{a; b\}$ d'où $t(x) = x$ d'où $s \circ t(x) = s(x)$. Il en résulte que*

$$\begin{array}{rll} x & \overset{=}{\text{(cf. I.4.18.3,)}} & s^{||\overrightarrow{ax}||}(a) \\ & = & s^{||\overrightarrow{ax}||-1}[s(a)] \\ & = & (s \circ t)^{||\overrightarrow{ax}||-1}[s(a)] \\ & = & (s \circ t)^{||\overrightarrow{ax}||-1}[s \circ t(b)] \\ & = & (s \circ t)^{||\overrightarrow{ax}||}(b)\ . \end{array}$$

On prouve ainsi, que tout $x \in O_a$ tel que $||\overrightarrow{ax}|| > 0$ appartient à la classe de b selon $s \circ t$ et on prouverait, par un raisonnement tout à fait symétrique, que tout $x \in O_b$ tel que $||\overrightarrow{bx}|| > 0$, appartient à la classe de a selon $s \circ t$.
Posons finalement $l_b := \#(O_b)$. On a alors :

$$\begin{array}{rcl} (s \circ t)^{l_b}(a) & = & (s \circ t)^{l_b-1}[s \circ t(a)] \\ & = & (s \circ t)^{l_b-1}[s(b)] \\ & = & s^{l_b}(b) \\ & = & b\ ; \end{array}$$

ceci prouve que b appartient à l'orbite de a selon $s \circ t$.
On déduit alors finalement facilement de ce qui précède, que l'orbite de a selon $s \circ t$ est aussi l'orbite de b selon $s \circ t$ et est égale à $O_a \cup O_b$. On a représenté cette situation sur le dessin ci-dessous.



Comme précédemment, les orbites de s distinctes de O_a et O_b ne sont pas affectées par la composition par t et il en résulte que $s \circ t$ possède une orbite de moins que s et donc que $\sigma(s \circ t) = -\sigma(s)$.

Le cas de $t \circ s$ se ramène à la situation précédente grâce à la remarque suivante :

Remarque I.4.18.7 Pour toute permutation $u \in \mathcal{S}_n$, la relation d'équivalence R_u (cf. I.4.5.1) coïncide avec la relation d'équivalence $R_{u^{-1}}$ d'où $\sigma(u) = \sigma(u^{-1})$.

On applique ce résultat à

$$(t \circ s)^{-1} = s^{-1} \circ t^{-1} \overset{=}{\text{(cf. I.4.9,)}} s^{-1} \circ t \ .$$

Ceci achève finalement la preuve de la proposition I.4.18.

Corollaire I.4.19 *Dans la décomposition d'une permutation en transpositions (cf. I.4.14,) le nombre de transpositions n'est pas uniquement déterminé ; mais sa parité l'est.*

Preuve *: En effet, si*

$$s = \prod_{i=1}^{\mu} t_i \in \mathcal{S}_n,$$

$\sigma(s) = (-1)^{\mu}$ *d'après la proposition I.4.18.*

Proposition I.4.20 *Pour tout couple (s, s') de permutations*

$$\sigma(s \circ s') = \sigma(s) * \sigma(s') \ .$$

On en déduit que σ est un morphisme de groupes :

$$\sigma : \mathcal{S}_n \to \mathbb{Z}^{\times} = (\{-1, 1\}, *) \cong \mathbb{Z}/2 \ .$$

Preuve *: Ceci résulte immédiatement de la proposition I.4.18 et de la proposition I.4.14.*

Corollaire I.4.21 *Deux éléments s et s' de $\mathcal{S}_n$ conjugués (cf. I.2.5o)nt même signature.*

Définition I.4.22 Pour $n \geq 2$, le noyau de σ est un sous-groupe distingué de $\mathcal{S}_n$ (cf. I.2.11.a),) noté $\mathcal{A}_n$ et appelé *groupe alterné d'ordre* n ; de plus $\mathcal{S}_n/\mathcal{A}_n$ s'identifie canoniquement à $\mathbb{Z}/2\mathbb{Z}$ (cf. I.2.19.)

Proposition I.4.23 *Pour $l \leq n$, tous les cycles de longueur l forment une seule classe de conjugaison.*

Preuve *: Soient c et c' deux cycles de longueur l. Soit S, (resp. S' ,) le support de c, (resp. c' ,) avec*

$$l := \#(S) = \#(S') \ .$$

Tout élément $a \in S$ (resp. $a' \in S'$) définit une bijection $\phi : \mathbb{Z}/l \to S$, (resp. $\phi' : \mathbb{Z}/l \to S'$) (cf. I.4.10.i).)

α *Posons*

$$s \ := \ \phi' \circ \phi^{-1} \ .$$

Pour tout $b \ \in \ S$, *il existe un unique* $\mu \in \mathbb{Z}/l$ *tel que* $b \ = \ \phi(\mu) \ = \ c^{\mu}(a)$. *Dès lors*

$$\begin{aligned}
(s^{-1} \circ c' \circ s)(b) &= (s^{-1} \circ c')[\phi'(\phi^{-1}(b))] \\
&= (s^{-1} \circ c')[\phi'(\mu)] \\
&= (s^{-1} \circ c')(c'^{\mu}(a')) \\
&= s^{-1}(c'^{\mu+1}(a') \\
&= \phi[\phi'^{-1}(c'^{\mu+1}(a'))] \\
&= \phi(\mu+1) \\
&= c^{\mu+1}(a) \\
&= c(c^{\mu}(a)) \\
&= c(b) \ .
\end{aligned}$$

β *L'application* s *n'est pour l'instant définie que sur* S. *Or*

$$\#([1;n] \ \setminus S) \ = \ \#([1;n]) \ - \ \#(S) \ = \ \#([1;n]) \ - \ \#(S') \ = \ \#([1;] \ \setminus \ S') \ .$$

Il existe donc une bijection

$$u \ : \ [1;n] \ \setminus \ S \ \to \ [1;n] \ \setminus \ S' \ .$$

On définira donc $\tilde{s}$ *par* s *sur* S *et* u *sur* $[1;n] \ \setminus \ S$. *On vérifiera ensuite que* $\tilde{s}$ *est une bijection de* $[1;n]$ *sur lui-même et que*

$$\tilde{s}^{-1} \ \circ \ c' \ \tilde{s} \ = \ c \ .$$

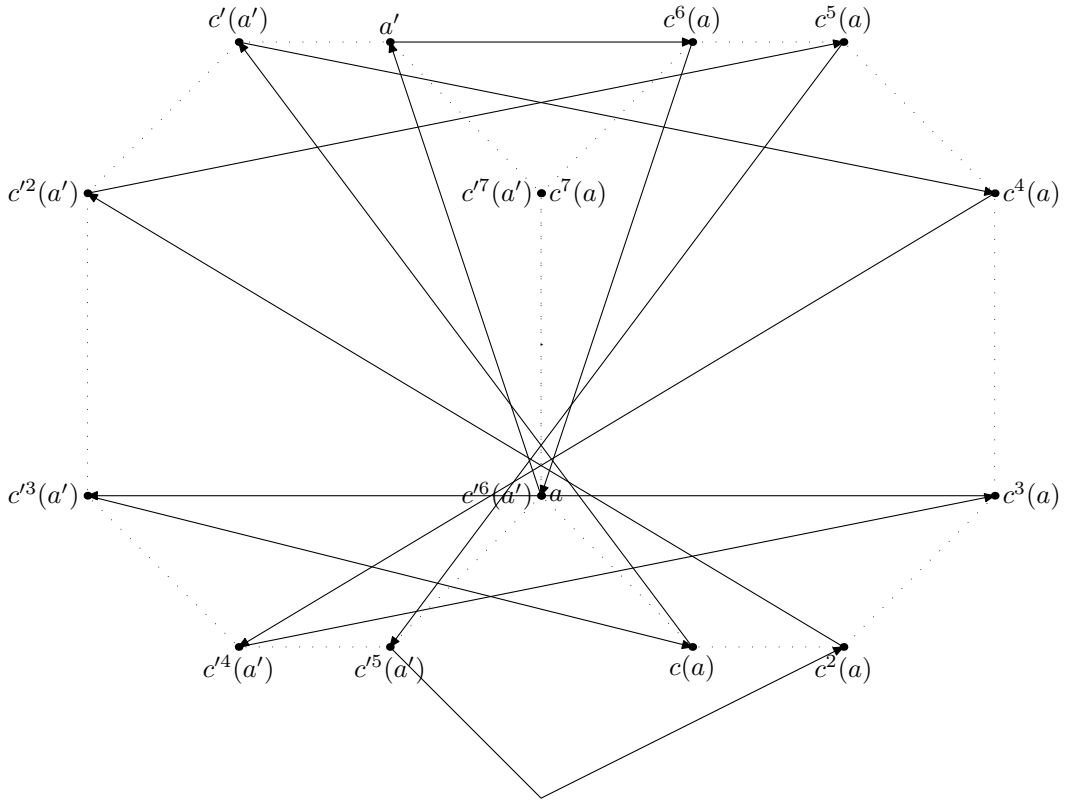
Comme

$$[1;n] \ = \ S \ \cup \ \big([1;n] \setminus (S \cup S')\big) \ \cup \ \big(S' \setminus (S \cap S')\big) \ ,$$

les points α, β *et* γ *permettent de définir* s *sur* $[1;n]$ *vérifiant l'identité*

$$s^{-1} \ \circ \ c' \ \circ \ s \ = \ c \ ;$$

c'est-à-dire que s conjugue c et c'.



Corollaire I.4.24 *Les permutations de même type cyclique (cf. I.4.13f)orment une seule classe de conjugaison.*

Preuve *: (cf. TD n° I, exercice G.)*

II . −Anneaux, algèbres, modules

II.1 . −Premières définitions (rappels : anneaux)

Définition II.1.1 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.

Définition II.1.2 Étant donné un anneau $(A, +, *)$, si ANN$_5$ pour tout couple (x, y) d'éléments de A, $x * y = y * x$ on dira que la loi $*$ est *commutative* ou encore que l'anneau $(A, +, *)$ est un *anneau commutatif.*

Exemple II.1.3 a) La multiplication $*$ sur $\mathbb{Z}$, donne a $(\mathbb{Z}, +, *)$ une structure d'anneau commutatif.

Par ailleurs la relation de *congruence* modulo n (cf. I.1.5.b)) est compatible à la multiplication (cf. I.2.12) *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 $*_{\mathbb{Z}/n}$ sur l'ensemble $\mathbb{Z}/n$ des classes modulo n par :

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

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

b) 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 C des fonctions continues à support compact, muni de l'adition :

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

et de la multiplication :

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

n'est pas un anneau au sens de la définition II.1.1. En effet, C ne possède pas d'élément neutre pour la multiplication $*$ et ne vérifie donc pas l'axiome ANN_3 de la définition II.1.1.

Dans la suite de ce cours, nous n'aurons pas à considérer de tels objets, ce qui nous incite 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.*

II.1.4 . −Notations et conventions

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 $*$ Si A est un anneau (resp. un anneau commutatif) $A^\times$ est un groupe (resp. un groupe abélien.) On appelle parfois également *unité* un élément de $A^\times$.

Exemple II.1.4.1 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 II.1.5 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.* $A^\times = A \setminus \{0_A\}$.

Convention On ne considérera, par la suite, que des corps commutatifs qu'on appelera simplement corps.

Exemple II.1.6 Les ensembles $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de leurs lois usuelles sont des corps commutatifs ainsi que $\mathbb{Z}/p$ pour p premier ; en revanche le corps des *quaternions de* HAMILTON n'est pas commutatif.

Exemple II.1.7 Soit $(G, +)$ un groupe abélien, d'après la proposition I.1.13, la loi $+$ de G induit une loi $+$ sur

$$\mathrm{Hom}_{\mathbf{Gr}}(G,G) \text{ telle que } (\mathrm{Hom}_{\mathbf{Gr}}(G,G), +) \text{ est un groupe abélien.}$$

Par ailleurs, si f et g sont deux éléments de $\mathrm{Hom}_{\mathbf{Gr}}(G,G)$, $f \circ g$ est un élément de $\mathrm{Hom}_{\mathbf{Gr}}(G,G)$ (cf. I.1.7.)

Proposition II.1.8 *Étant donné un groupe abélien* $(G,+)$, $(\mathrm{Hom}_{\mathbf{Gr}}(G,G),+,\circ)$ *est un anneau (non commutatif.)*

Preuve *: Comme* $(\mathrm{Hom}_{\mathbf{Gr}}(G,G),+)$ *est déjà un groupe abélien cette vérification étant laissée en exercice, il suffit de vérifier les axiomes ANN*$_2$*, ANN*$_3$ *et ANN*$_4$ *de la définition II.1.1.*

ANN$_2$ *La loi* $\circ$ *est associative par définition.*

ANN$_3$ *L'élément* $\mathrm{Id}_G \in \mathrm{Hom}_{\mathbf{Gr}}(G,G)$ *(cf. I.1.10.a)) vérifie*

$$f \circ \mathrm{Id}_G \;=\; \mathrm{Id}_G \circ f \;=\; f\ ,$$

pour tout $f \in \mathrm{Hom}_{\mathbf{Gr}}(G,G)$.

ANN$_4$ *Étant donnés trois éléments* f,g,h *de* $\mathrm{Hom}_{\mathbf{Gr}}(G,G)$, *pour tout* $x \in G$,

$$\begin{array}{rcl}
[h\circ(f+_{\mathrm{Hom}_{\mathbf{Gr}}(G,G)}g)](x) & = & h[(f+_{\mathrm{Hom}_{\mathbf{Gr}}(G,G)}g)(x)] \\
& = & h(f(x)+_G g(x)) \\
& = & \\
& \textit{(cf. I.1.6,)} & h(f(x))+_G h(g(x)) \\
& = & (h\circ f)(x)+_G (h\circ g)(x) \\
& = & [(h\circ f)+_{\mathrm{Hom}_{\mathbf{Gr}}(G,G)}(h\circ g)](x)\ ;
\end{array}$$

et

$$\begin{array}{rcl}
[(f+_{\mathrm{Hom}_{\mathbf{Gr}}(G,G)}g)\circ h](x) & = & (f+_{\mathrm{Hom}_{\mathbf{Gr}}(G,G)}g)(h(x)) \\
& = & (f(h(x))+_G f(g(x)) \\
& = & (f\circ h)(x)+_G (f\circ g)(x) \\
& = & \\
& \textit{(cf. I.1.13,)} & [(f\circ h)+_{\mathrm{Hom}_{\mathbf{Gr}}(G,G)}(f\circ g)](x)
\end{array}$$

.

Ce qui prouve que $\circ$ *est distributive sur* $+_{\mathrm{Hom}_{\mathbf{Gr}}(G,G)}$.

Définition II.1.9 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$_6$ $f:(A,+_A)\to(B,+_B)$ est un morphisme de groupes (cf. I.1.6.)

ANN$_7$ $f(1_A)\ =\ 1_B$.

ANN$_8$ Pour tout couple (x, y) d'éléments de A,

$$f(x *_A y) \;=\; f(x) *_B f(y)\,.$$

Remarque II.1.10 i) L'axiome ANN$_7$ a en particulier pour conséquence que l'image d'un élément inversible d'un anneau A par un morphisme $f : A \to B$ est un élément inversible de B et que $f(u)^{-1} = f(u^{-1})$ pour $u \in A^\times$.

ii) On remarquera qu'il est inutile de donner une définition de morphisme de corps puisque axiomatiquement, un corps (cf. II.1.5) est un anneau qui a simplement une propriété supplémentaire.

Proposition II.1.11 *Si $f : A \to B$ et $g : B \to C$ sont des morphismes d'anneaux alors la composée $g \circ f$ est un morphisme d'anneaux de A dans C.*

II.2 . −Algèbres

Définition II.2.1 (A-algèbre) Si $f : A \to B$ est un morphisme d'anneaux (cf. II.1.9) on dit que B ou le couple (B, f) ou même le morphisme f est une *A-algèbre*. Le morphisme f est appelé *morphisme structural*.

Si B est un anneau commutatif on dit de B, (B, f) ou f que c'est une *algèbre commutative*.

Définition II.2.2 Soit A un anneau

$$f : A \to B \text{ et } g : A \to C \text{ deux } A\text{-algèbres}\,.$$

Un morphisme d'anneaux (cf. II.1.9) $u : B \to C$ est un *morphisme de A-algèbres* si $u \circ f = g$.

Proposition II.2.3 *Étant donné un anneau A $u : (B, f) \to (C, g)$ et $v : (C, g) \to (D, h)$ des morphismes de A-algèbres, la composée $v \circ u$ est un morphisme de A-algèbres.*

Preuve *: D'après la proposition II.1.11 $v \circ u$ est un morphisme d'aneaux. Par ailleurs*

$$\begin{aligned} v \circ u \circ f &= v \circ g \\ &= h\,. \end{aligned}$$

II.2.4 . $-$Notation

Étant donnés un anneau A et deux A-algèbres B et C, on notera $\mathrm{Hom}_{A-\mathbf{alg}}(B, C)$ l'ensemble des morphismes de A-algèbres de B à valeurs dans C.

Définition II.2.5 (Sous-algèbre) Étant donées un anneau de base A et deux A-algèbres B et C on dira que B est une *sous-A-algèbre de C* s'il existe un morphisme de A-algèbres injectif $i : B \hookrightarrow C$.

Proposition II.2.6 *Une partie B d'une A-algèbre C est une sous-A-algèbre de C si et seulement si :*

- *pour tout $(x, y) \in B \times B$, $x +_C y \in B$, $-x \in B$, et $0_C \in B$, (i.e.$(B, +_C)$ est un sous-groupe de $(C, +_C)$, (cf. I.1.19 ;)*
- *pour tout $(x, y) \in B \times B$, $x *_C y \in B$;*
- *$1_C \in B$;*
- *le morphisme structural $g : A \to C$ est à valeurs dans B .*

Preuve *: Il suffit décrire que l'inclusion canonique (cf. 0.1e)st un morphisme de A-algèbres.*

Exemple II.2.7 (Exemples de sous-algèbres) L'anneau $\mathbb{Q}$ (resp. $\mathbb{R}$) est une sous-algèbre de $\mathbb{R}$ (resp. $\mathbb{C}$) même si l'injection étant l'inclusion canonique on omet presque toujours de la noter.

Proposition II.2.8 *i) Tout anneau A est canoniquement une $\mathbb{Z}$-algèbre, i.e.*

il existe un unique morphisme de structure $f : \mathbb{Z} \to A$.

ii) Étant donnés deux anneaux A et B, $u : A \to B$ est un morphisme d'anneaux si et seulement si u est un morphisme de $\mathbb{Z}$-algèbres.

Preuve *: Rappelons le fait bien connu que $\mathbb{Z} = (\mathbb{Z}, +, *)$ est un anneau commutatif (cf. II.1.3.a).)*

i) Soit A un anneau. ***Analyse :*** *s'il existe un morphisme $f : \mathbb{Z} \to A$, d'après l'axiomeANN_6 de la définition II.1.9, $f : (\mathbb{Z}, +) \to (A, +_A)$ est un morphisme de groupes, ce qui impose (cf. I.1.9.i)) $f(0) = 0_A$. Par ailleurs pour tout $n \in \mathbb{N}$,*

$$f(n + 1) = f(n) +_A f(1) .$$

De plus pour tout $n \in \mathbb{N}$,

$$f(-n) = -f(n) \text{ (cf. I.1.9.ii) .)}$$

Synthèse : *ainsi, on constate que dès l'instant où $f(1)$ est déterminé f est parfaitement défini par un argument de récurrence. Or d'après l'axiome ANN_7 de la définition II.1.9, nécessairement $f(1) = 1_A$.*

ii) Soient A et B deux anneaux dont on notera f_A et f_B les structures canoniques de $\mathbb{Z}$-algèbres dont l'existence et l'unicité ont été établies en (i).

Soit $u : A \to B$ un morphisme d'anneaux. D'après la proposition II.1.11, $u \circ f_A$ est un morphisme d'anneaux de $\mathbb{Z}$ à valeurs dans B. Or d'après (i), un tel morphisme est unique il s'ensuit que $u \circ f_A = f_B$; ce qui prouve que u est un morphisme de $\mathbb{Z}$-algèbres .

Réciproquement un morphisme $u : A \to B$ de $\mathbb{Z}$-algèbres est par définition , un morphisme d'anneaux.

Exemple II.2.9 a) Pour tout anneau A, l'identité de A donne à A une structure de A-algèbre *i.e.*(A, Id_A) est une A-algèbre

b) Soit K un corps et E un K-espace vectoriel de dimension finie.

Le corps K s'identifie "naturellement" à l'ensemble des homothéties de E, c'est-à-dire qu'à tout $\lambda \in K$, on associe l'endomorphisme de E défini par $x \mapsto \lambda x$ pour tout $x \in E$. On définit ainsi une structure "naturelle" de K-algèbre sur $\mathrm{End}(E)$.

Définition II.2.10 Étant donné un anneau A, un morphisme d'algèbres

$$\begin{array}{ccc} & A & \\ {\scriptstyle f}\big\downarrow & \searrow {\scriptstyle g} & \\ B & \xrightarrow{u} & C \end{array}$$

est un *isomorphisme* s'il existe un morphisme d'algèbre

$$\begin{array}{ccc} & A & \\ {\scriptstyle g}\big\downarrow & \searrow {\scriptstyle f} & \\ C & \xrightarrow{v} & B, \end{array}$$

tel que :

$$u \circ v = \mathrm{Id}_C \text{ et } v \circ u = \mathrm{Id}_B .$$

Remarque II.2.11 On se reportera notamment aux sections II.3 II.6 pour des compléments et notamment à II.3.16, II.3.19 et II.3.18.

II.3 . −Modules

Dans toute cette section, A est un anneau commutatif. (cf. II.1.2.)
Les A-algèbres considérées sont commutatives (cf. II.2.1) (sauf mention du contraire.)

Définition II.3.1 Un *A-module* ou simplement *module* est un triplet $(M, +_M, \cdot_M)$ (le plus souvent noté simplement $M,$) tel que :
Mod$_1$ $(M, +_M)$ est un groupe abélien (cf. I.1.3 ;) $\cdot_M$ est une loi de composition externe $\cdot_M$: $A \times M \to M$ vérifiant, pour tout $(a, b) \in A \times A$, et tout $(x, y) \in M \times M$,

$$\begin{array}{lrcl} \text{Mod}_2 & a \cdot_M (x +_M y) & = & a \cdot_M x +_M a \cdot_M y\ , \\ \text{Mod}_3 & (a +_A b) \cdot_M x & = & a \cdot_M x +_M b \cdot_M x\ , \\ \text{Mod}_4 & 1_A \cdot_M x & = & x\ , \\ \text{Mod}_5 & (a *_A b) \cdot_M x & = & a \cdot_M (b \cdot_M x)\ . \end{array}$$

On dira aussi que les lois $+_M$ et $\cdot_M$ *munissent M d'une structure de module*.

Proposition II.3.2 *i) À tout A-module $(M, +_M, \cdot_M)$ on associe un morphisme d'anneaux (cf. II.1.9,)*

$$\phi_{(M,+_M,\cdot_M)} \text{ de } A \text{ à valeurs dans l'anneau } (\mathrm{Hom}_{\mathbf{Gr}}(M, M), +_{\mathrm{Hom}_{\mathbf{Gr}}(M,M)}, \circ)$$

(où la structure d'anneau sur $\mathrm{Hom}_{\mathbf{Gr}}(M, M)$ est celle définie en II.1.8) en posant, pour tout $a \in A$,

$$\begin{array}{rccc} \phi_{(M,+,\cdot)}(a) : & M & \to & M \\ & x & \mapsto & a \cdot x\ . \end{array}$$

ii) Réciproquement, étant donné un groupe abélien $(M, +)$ muni d'un morphisme

$$\phi\ :\ (A, +, *)\ \to\ (\mathrm{End}_{\mathbf{Gr}}(M), +, \circ),$$

il existe une unique structure de A-module $\cdot_{\phi,M}$ sur M telle que

$$\phi_{(M,+,\cdot_{\phi,M})}\ =\ \phi\ .$$

iii) Si $(M, +, \cdot)$ est un A-module

$$\cdot_{\phi_{(M,+,\cdot)},M}\ =\ \cdot\ .$$

Preuve *:*

i) Posons

$$\phi \;:=\; \phi_{(M,+_M,\cdot_M)} \;:\; A \;\to\; \mathrm{Hom}_{\mathbf{Gr}}(M,M)\;.$$

L'axiome Mod$_2$ de la définition II.3.1 assure que $\phi(a)$ est un morphisme de groupes (cf. I.1.6,) c'est-à-dire que

$$\phi(a) \in \mathrm{Hom}_{\mathbf{Gr}}(M,M)\;.$$

L'application ϕ ainsi définie est donc bien à valeurs dans $\mathrm{Hom}_{\mathbf{Gr}}(M,M)$.

L'axiome Mod$_3$ assure que $\phi : (A,+_A) \to (\mathrm{Hom}_{\mathbf{Gr}}(M,M), +_{\mathrm{Hom}_{\mathbf{Gr}}(M,M)})$ est un morphisme de groupes c'est-à-dire que ϕ satisfait l'axiome ANN$_6$ de la définition II.1.9.

Enfin les axiomes Mod$_4$ et Mod$_5$ assurent que ϕ satisfait aux axiomes ANN$_7$ et ANN$_8$ de la définition II.1.9.

ii) Réciproquement supposons donné un groupe abélien $(M,+_M)$ et un morphisme d'anneaux

$$\phi \;:\; (A,+_A,*_A) \;\to\; (\mathrm{Hom}_{\mathbf{Gr}}(M,M), +_{\mathrm{Hom}_{\mathbf{Gr}}(M,M)}, \circ)\;.$$

Supposons qu'il existe une structure de module $\cdot_M$ sur M telle que

$$\psi \;:=\; \phi_{(M,+_M,\cdot_M)} \;=\; \phi\;.$$

Pour tout $a \in A$, et tout $x \in M$,

$$a \cdot_M x \;=\; \psi(a)(x) \;=\; \phi(a)(x)\;.$$

La structure $\cdot_M$ existe et est donc uniquement déterminée. Reste à prouver qu'elle vérifie bien les axiomes Mod$_2$ à Mod$_5$. On peut dégager de la preuve de (i) le tableau suivant, mettant en correspondance les axiomes :

$\cdot$	ϕ
Mod$_2$	ϕ est à valeurs dans $\mathrm{Hom}_{\mathbf{Gr}}(\cdot,\cdot)$
Mod$_3$	ANN$_6$
Mod$_4$	ANN$_7$
Mod$_5$	ANN$_8$.

iii) Est tout à fait formel en considérant le tableau précédent.

Remarque II.3.3 i) Si M est un A-module, pour tout $x \in M$, on a :

$$0_A \cdot x = 0_M .$$

Grâce à la proposition II.3.2, ceci est immédiat car l'image de 0_A dans $(\mathrm{End}_{\mathbf{Gr}}(M), +)$ est nécessairement l'application nulle (cf. I.1.9.i).)

On peut aussi donner une démonstration directe de ce fait, qui reprend évidemment l'argument utilisé pour prouver I.1.9.i) : On a en effet, pour tout $x \in M$,

$$\begin{aligned} 0_A \cdot x &= (0_A +_A 0_A) \cdot x \\ &= 0_A \cdot x + 0_A \cdot x . \end{aligned}$$

Le fait que l'on puisse "simplifier" l'égalité $0_A \cdot x + 0_A \cdot x = 0_A \cdot x$ par $0_A \cdot x$, vient de ce que $(M, +)$ est un groupe.

ii) De même pour tout $x \in M$,

$$(-1_A) \cdot x = -x ,$$

(où -1_A désigne l'opposé de 1_A dans le groupe $(A, +_A)$ et $-x$ l'opposé de x dans le groupe $(M, +)$.)

iii) Enfin pour tout $a \in A$,

$$a \cdot 0_M = 0_M ;$$

ce qui découle du fait qu'on peut, grâce à la proposition II.3.2, voir a comme une homothétie de M et donc comme un endomorphisme du groupe abélien $(M, +)$.

Exemple II.3.4 Soit $f : A \to B$ une A-algèbre (cf. II.2.1.)

a) Si $(M, +_M, \cdot_M^B)$ est un B-module, M est muni d'une structure naturelle de A-module $\cdot_M^A$ définie pour tout $a \in A$ et tout $x \in M$ par :

$$a \cdot_M^A x := f(a) \cdot_M^B x .$$

Il s'ensuit que pour deux B-modules M et N, munis de leur structure canonique de A-module définie ci-dessus,

$$\mathrm{Hom}_B(M, N) \subset \mathrm{Hom}_A(M, N) .$$

(cf. II.3.7.ii).)

b) L'anneau A lui-même est une A-algèbre par Id_A (cf. II.2.9.a)) et donc un A-module dont la structure $\cdot_A$ est donnée pour tout $(a, x) \in A \times A$ par :

$$a \cdot_A x := a *_A x .$$

c) Pour un entier $n \in \mathbb{N}^*$ l'ensemble

$$A^n = A \times A \times \ldots \times A = \{(a_1, \ldots, a_n)\ ,\ a_i \in A\ ,\ 1 \leq i \leq n\}$$

possède une structure "naturelle" de A-module (cf. II.7.2.) Pour tout $\alpha \in A$ et tout couple de n-uplets d'éléments de A $((a_1, \ldots, a_n), (b_1, \ldots, b_n))$ on posera :

$$\alpha \cdot_{A^n} (a_1, \ldots, a_n) +_{A^n} (b_1, \ldots, b_n) = (\alpha *_A a_1 +_A b_1, \ldots, \alpha *_A a_n +_A b_n)\ .$$

Définition II.3.5 Étant donnés deux A-modules $(M, +_M, \cdot_M)$ et $(N, +_N, \cdot_N)$ on appelle *morphisme (homomorphisme) de A-modules* (ou simplement *morphisme* si le contexte est clair, ou même *application linéaire*) une application $f : M \to N$, telle que :

Mod$_6$ $f : (M, +_M) \to (N, +_N)$ est un morphisme de groupes (cf. I.1.6 ;)

Mod$_7$ pour tout $a \in A$ et tout $x \in M$,

$$f(a \cdot_M x) = a \cdot_N f(x)\ .$$

De manière équivalente, $f : M \to N$ est un morphisme de A-modules si et seulement si pour tout $(a, b) \in A \times A$ et tout $(x, y) \in M \times M$,

$$f(a \cdot_M x +_M b \cdot_M y) = a \cdot_N f(x) +_N b \cdot_N f(y)\ .$$

Exemple II.3.6 Pour tout A-module M l'application identique Id_M est un morphisme de A-modules.

Remarque II.3.7 i) Pour un A-module M, on omettra, le plus souvent, d'écrire le symbole $\cdot_M$ de la loi externe et l'on écrira simplement, pour $a \in A$ et $x \in M$, ax au lieu de $a \cdot_M x$.

ii) Étant donnés deux A-modules M et N on notera $\mathrm{Hom}_A(M, N)$ l'ensemble des morphismes de A-modules de M à valeurs dans N.

Proposition II.3.8

Pour tout morphisme de A-modules $f : M \to N$ et $g : N \to P$,

l'application composée

$g \circ f$ est un morphisme de A-modules de M à valeurs dans P .

Proposition II.3.9 *i) Tout groupe abélien $(G, +_G)$ (cf. I.1.3,) est canoniquement un $\mathbb{Z}$-module, i.e.il existe une unique structure de $\mathbb{Z}$-module $\cdot_G$ sur $(G, +_G)$.*

ii) Étant donnés deux groupes abéliens G et H, une application $f : G \to H$ est un morphisme de groupes (cf. I.1.6) si et seulement si f est un morphisme de $\mathbb{Z}$-modules.

***Preuve** :*

i) La structure de groupe abélien sur G induit une structure d'anneau sur $\mathrm{Hom}_{\mathbf{Gr}}(G,G)$ (cf. II.1.8.) D'après la proposition II.3.2, la donnée d"une structure de A-module sur G équivaut à la donnée d'une structure de A-algèbre sur $(\mathrm{Hom}_{\mathbf{Gr}}(G,G), +_{\mathrm{Hom}_{\mathbf{Gr}}(G,G)}, \circ)$. Or tout anneau étant canoniquement une $\mathbb{Z}$-algèbre (cf. II.2.8,)
$(\mathrm{Hom}_{\mathbf{Gr}}(G,G), +_{\mathrm{Hom}_{\mathbf{Gr}}(G,G)}, \circ)$ a une unique structure de $\mathbb{Z}$-algèbre ; c'est-à-dire que G a une unique structure de $\mathbb{Z}$-module.

ii) Est laissé en exercice.

Remarque II.3.10 On peut donner une démonstration directe (et peut-être plus éclairante) de II.3.9.i). En effet, s'il existe une structure de $\mathbb{Z}$-module $\cdot_G$ sur un groupe abélien G, nécessairement d'après Mod_4, pour tout $g \in G$ $1_{\mathbb{Z}} \cdot_G g = g$. Par ailleurs, pour tout $n > 0$, d'après Mod_2,

$$\begin{aligned}(n+1) \cdot_G g &= n \cdot_G g +_G 1 \cdot_G g \\ &= n \cdot_G g +_G g \,;\end{aligned}$$

ce qui permet de définir $\cdot_G$ par récurrence pour les entiers positifs. La remarque II.3.3.i) permet de montrer que $0 \cdot_G g = 0_G$ et par conséquent que $(-n) \cdot_G g = -(n \cdot_G g)$ ce qui permet de définir $\cdot_G$ pour tous les entiers.

Reste, bien entendu à vérifier que la loi externe ainsi définie satisfait bien aux axiomes Mod_3, et Mod_5 ; ce qui n'est pas difficile. À noter toutefois, que Mod_3 repose fortement sur le fait que G est commutatif (abélien) et ne serait pas satisfait pour un groupe quelconque, ce qui oblige à réserver un traitement particulier aux groupes non commutatifs (cf. I.1q)ui n'entrent pas dans le cadre des $\mathbb{Z}$-modules.

Remarque II.3.11 Pour un entier $n > 1$, l'ensemble $\mathbb{Z} : n$ des classes d'entiers modulo n est muni d'une structure de groupe donnée par $\overline{a} +_{\mathbb{Z}/n} \overline{b} = \overline{a +_{\mathbb{Z}} b}$ (cf. I.1.5.b)).

Nous verrons par la suite, (cf. II.5.4,) que c'est la seule structure de groupe sur $\mathbb{Z}/n$ "compatible avec la surjection ensembliste" $a \mapsto \overline{a}$. Pour tout $(k, \overline{a}) \in \mathbb{Z} \times \mathbb{Z}/n$,

$$\begin{aligned}(k, \overline{a}) &\mapsto \overline{k *_{\mathbb{Z}} a} \\ &\overset{=}{\text{(cf. II.1.3a)}} \ \overline{k} *_{\mathbb{Z}/n} \overline{a} \,,\end{aligned}$$

définit une structure de $\mathbb{Z}$-module sur $\mathbb{Z}/n$ qui est la seule compatible à la structure de groupe d'après la proposition précédente.

Proposition II.3.12 *i) Soit B un anneau commutatif muni d'une loi de composition externe*

$$\cdot_B \ : \ A \times B \ \to \ B$$

telle que $(B, +_B, \cdot_B)$ soit un A-module.

Alors il existe un unique morphisme d'anneaux $f \ : \ A \ \to \ B$ tel que

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

soit aussi un morphisme de A-modules (où A est vu comme A-module à travers l'identité Id_A (cf. II.3.4.)

ii) Une A-algèbre $f \ : \ A \ \to \ B$ a une structure canonique de A-module, donnée, pour tout $(a, b) \in A \times B$, par :

$$a \cdot_B b \ := \ f(a) *_B b \ .$$

Avec cette structure,

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

est un morphisme de A-modules, (où A est vu comme A-module à travers l'identité Id_A. (cf. II.3.4.b)). Ce procédé est inverse de i).

***Preuve** :*

*i) S'il existe un morphisme d'anneau $f \ : \ A \ \to \ B$, (**analyse**,) nécessairement $f(1_A) \ = \ 1_B$. Pour tout $a \ \in \ A$,*

$$\begin{array}{rcl} f(a) & = & f(a *_A 1_A) \\ & \overset{=}{} & \\ & \text{(cf. II.3.4.b))} & f(a \cdot_A 1_A) \\ & \overset{=}{} & \\ & f \text{ est un morphisme de modules} & a \cdot_B f(1_A) \\ & = & a \cdot_B 1_B \end{array}$$

.

Ceci définit bien une unique application $f \ : \ A \ \to \ B$. La vérification que f est bien un morphisme d'anneaux et un morphisme de A-modules est laissée en exercice.

ii) Est laissé en exercice.

Définition II.3.13 Si K est un corps on appelle *K-espace vectoriel* un K-module.
On appelle usuellement *application linéaire* un morphisme de K-modules.

Définition II.3.14 Étant donnés deux A-modules M et N, un morphisme $f : M \to N$ est un isomorphisme s'il existe un morphisme $g : N \to M$, tel que :

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

Proposition II.3.15 *Étant donné un morphisme de A-modules $f : M \to N$, f est un isomorphisme si et seulement si f est une bijection.*

Preuve : *Si f est un isomorphisme, f est évidemment une bijection.*
Réciproquement, supposons que f est une bijection. Il existe alors une bijection ensembliste réciproque $g : N \to M$, i.e. une application telle que

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

Il ne reste qu'à prouver que g est un morphisme. Pour tout $(a, b) \in A \times A$ et $(u, v) \in N \times N$, il existe un unique couple $(x, y) = (g(u), g(v)) \in M \times M$ tel que

$$\begin{aligned} f(x) &= u , \\ f(y) &= v ; \end{aligned}$$

puisque f est bijective d'application réciproque g. Il s'ensuit que :

$$\begin{aligned} g(au + bv) &= g(af(x) + bf(y)) \\ &\overset{f \text{ est un morphisme}}{=} g(f(ax + by)) \\ &= ax + by \\ &= ag(u) + bg(v) . \end{aligned}$$

Ce qui prouve que g est un morphisme (cf. II.3.5.)

Corollaire II.3.16 *Étant donnés deux groupes abéliens G et H, un morphisme de groupes $f : G \to H$ est un isomorphisme si et seulement si f est une bijection.*

Preuve : *Ceci est une conséquence de la proposition II.3.9 et de la proposition II.3.15.*

Remarque II.3.17 Dans le cas des groupes quelconques, le résultat a déjà été établi dans la proposition I.1.12 et le corollaire précédent peut également être vu comme une conséquence de cette dernière.

Corollaire II.3.18 *Étant données deux A-algèbres (cf. II.2.1) B et C, un morphisme de A-algèbres (cf. II.2.2) $f : B \to C$ est un isomorphisme si et seulement si il est bijectif.*

Preuve : *Si f est bijectif, comme $f : (B, +_B) \to (C, +_C)$ est un morphisme de groupes (cf. II.1.91), l'application réciproque g est un morphisme de groupes d'après II.3.16.*

Par ailleurs 1_B est l'unique antécédent de 1_C par f ; c'est-à-dire que $g(1_C) = 1_B$; ce qui assure que g vérifie l'axiome (cf. II.1.92).

De plus, pour tout $(u, v) \in C \times C$, il existe un unique $(x, y) = (g(u), g(v)) \in B \times B$ tel que :

$$\begin{aligned} f(x) &= u\,, \\ f(y) &= v \end{aligned}$$

.

Il s'ensuit que :

$$\begin{array}{lcl} g(uv) & = & g(f(x)f(y)) \\ & \overset{=}{f \text{ est un morphisme}} & g(f(xy)) \\ & = & xy \\ & = & g(u)g(v) \end{array}$$

.

Ce qui assure que g vérifie l'axiome (cf. II.1.93).

On doit enfin vérifier la compatibilité aux morphismes structuraux. Notons $\phi_B : A \to B$ (resp. $\phi_C : A \to C$) le morphisme structural de B (resp. C.) On a alors :

$$\begin{array}{lcl} g \circ \phi_C & \overset{=}{f \text{ est un morphisme}} & g \circ f \circ \phi_B \\ & = & \phi_B \end{array}$$

.

Ceci achève la preuve.

Corollaire II.3.19 *Un morphisme d'anneaux est un isomorphisme si et seulement s'il est bijectif.*

Preuve : *Ceci se déduit de la proposition II.2.8 et du corollaire II.3.18.*

II.4 . −Sous-modules

Dans toute cette section, A est un anneau commutatif. (cf. II.1.2.)
Les A-algèbres considérées sont commutatives (cf. II.2.1) (sauf mention du contraire.)

Définition II.4.1 Étant donné un morphisme de A-modules $f : M \to N$, on appellera *noyau* (resp. *image*) de f

$$\operatorname{Ker} f := \{x \in M \mid f(x) = 0_N\},$$

(resp.

$$\operatorname{Im} f := \{f(x)\,,\ x \in M\}\ .)$$

Remarque II.4.2 Les définitions II.4.1 s'appliquent évidemment aux groupes abéliens grâce à la proposition II.3.9 (et coïncident avec celles données pour les groupes quelconques (cf. I.1.21,)) aux A-algèbres grâce à II.3.4.a), et aux anneaux grâce à la proposition II.2.8.

Définition II.4.3 On appellera *monomorphisme* (resp. *épimorphisme*) de A-modules un morphisme de A-modules injectif (resp. surjectif.)

Définition II.4.4 Étant donné un A-module $(M, +_M, \cdot_M)$ on appelle *sous-A-module* (ou simplement sous-module) de M un sous-ensemble K de M tel que les lois $+_M$ et $\cdot_M$ définissent une structure de A-module sur K.

On appellera aussi sous-module de M tout A-module isomorphe à un sous-A-module au sens précédent.

Exemple II.4.5 a) Étant donné un A-module M, M est un sous-A-module de lui-même ; $\{0_M\}$ est un sous-A-module de M.

b) Un $\mathbb{Z}$-module K est un sous-$\mathbb{Z}$-module de $\mathbb{Z}$ vu comme module sur lui-même (cf. II.3.4.b),) si et seulement si K est isomorphe à $n\mathbb{Z}$ pour $n \in \mathbb{N}$.

Proposition II.4.6 *Étant donné un A-module M et K un ensemble, les conditions suivantes sont équivalentes :*

a) K est un sous-A-module de M.

b) K est un sous-ensemble non vide de M tel que pour tout $(a, b) \in A \times A$ et tout $(x, y) \in K \times K$,

$$a \cdot_M x +_M b \cdot_M y \in K\ .$$

c) Il existe un monomorphisme $i : K \hookrightarrow M$.

Preuve *:*

a) $\Rightarrow$ *b) est, pour ainsi dire tautologique.,*

b) $\Rightarrow$ *a) Pour tout* $(x, y) \in K \times K$*, par hypothèse,* $x +_M y \in K$*. La loi* $+_M$ *se restreint donc en une loi* $+_M : K \times K \to K$*.*
Par ailleurs, pour tout $x \in K$*,* $(-1_A) \cdot_M x = -x$ *(cf. II.3.3.ii)) appartient à* K *et est de manière évidente un opposé pour* x *dans* $(K, +_M)$*.*
De plus, pour tout $x \in K$*,* $0_A \cdot_M x = 0_M$ *(cf. II.3.3.i)) appartient à* K *et est un élément neutre pour* $(K, +_M)$*. Ici intervient l'hypothèse* K *non vide.*
Enfin, par hypothèse même, $\cdot_M$ *se restreint en une loi de composition externe*

$$\cdot_M : A \times K \to K.$$

a) $\Rightarrow$ *c) découle de ce que l'inclusion canonique* $i : K \hookrightarrow M$ *définie pour tout* $x \in K$ *par* $i(x) = x$ *est clairement un monomorphisme.*

c) $\Rightarrow$ *b) est une conséquence de la proposition II.4.9. En effet, si* $i : K \to M$ *est un monomorphisme i.e.un morphisme injectif,* $i : K \to \operatorname{Im} i$ *est également surjectif, donc bijectif. D'après la proposition II.3.15* $i : K \to \operatorname{Im} i$ *est un isomorphisme.*

Remarque II.4.7 On exprimera usuellement la propriété II.4.6.b) en disant que K est *stable par combinaisons linéaires à coefficients dans* A.

Exemple II.4.8 a) Si N est un sous-A-module de M et P un sous-A-module de N alors P est un sous-A-module de M.

b) Si N et P sont deux sous-A-modules d'un module M, $N \cap P$ est un sous-A-module de M. Noter qu'en général, $N \cup P$ n'est pas un sous-A-module de M (cf. I.1.16.b).)

Proposition II.4.9 *Étant donné un morphisme de* A*-modules* $f : M \to N$*, le noyau (resp. l'image) de* f *(cf. II.4.1) est un sous-*A*-module de* M *(resp.* N*.)*

Preuve *:*

Noyau La remarque I.1.9.i) assure que $f(0_M) = 0_N$ *i.e.*$0_M \in \operatorname{Ker} f$*. Le noyau de* f *est donc non-vide. De plus, pour tout* $(a, b) \in A \times A$*, et tout* $(x, y) \in \operatorname{Ker} f \times \operatorname{Ker} f$*,*

$$f(ax + by) = af(x) + bf(y) = a \cdot_N 0 + b \cdot_N 0$$

qui est nul d'après la remarque II.3.3.iii). Grâce à II.4.6.b), on conclut que $\operatorname{Ker} f$ *est un sous-module de* M*.*

Image *Comme* $f(0_M) = 0_N$, $\mathrm{Im}\, f$ *est non vide. Par ailleurs, pour tout* $(a,b) \in A \times A$, *et tout* $(u,v) \in \mathrm{Im}\, f \times \mathrm{Im}\, f$, *il existe* $(x,y) \in M \times M$ *(non nécessairement unique) tel que*

$$\begin{aligned} f(x) &= u \\ f(y) &= v\ . \end{aligned}$$

Il s'ensuit que

$$\begin{aligned} a \cdot_N u +_N b \cdot_N v \quad &= \quad a \cdot_N f(x) +_N b \cdot_N f(y) \\ &\overset{=}{\text{(cf. II.3.5,)}} \quad f(a \cdot_M x +_M b \cdot_M y) \\ &\in \quad \mathrm{Im}\, f\ ; \end{aligned}$$

c'est-à-dire que $\mathrm{Im}\, f$ *est stable par combinaisons linéaires à coefficients dans* A. *D'après II.4.6.b),* $\mathrm{Im}\, f$ *est donc un sous-module de* N.

Proposition II.4.10 *i) Un morphisme de* A*-modules* $f : M \to N$ *est un monomorphisme (resp. épimorphisme) si et seulement si*

$$\mathrm{Ker}\, f = \{0_M\}\ ,$$

(resp.

$$\mathrm{Im}\, f = N\ .)$$

ii) Un morphisme $f : M \to N$ *est un isomorphisme si et seulement si* f *est un monomorphisme et un épimorphisme i.e. si et seulement si*

$$\mathrm{Ker}\, f = \{0_M\} \text{ et } \mathrm{Im}\, f = N\ .$$

Remarque II.4.11 i) Les définitions II.4.1, II.4.3, II.4.4, les propositions II.4.6, II.4.9, et II.4.10 s'appliquent au cas des groupes abéliens grâce à la proposition II.3.9.

ii) Ceci s'applique également aux anneaux et aux A-algèbres mais il faut prendre garde au fait que l'on ne peut pas tirer de la proposition II.4.9 que le noyau d'un morphisme de A-algèbres $f : B \to C$, est une sous-algèbre de B. Ceci est d'ailleurs faux en général (cf. II.5.8.a).)

iii) En revanche, on peut montrer, sans grande difficulté, que l'image de f est une sous-A-algèbre de C.

iv) De même le critère de stabilité II.4.6.b) ne saurait être pertinent dans le contexte des A-algèbres.

II.5 . −Quotients

Dans toute cette section, A est un anneau commutatif. (cf. II.1.2.)
Les A-algèbres considérées sont commutatives (cf. II.2.1) (sauf mention du contraire.)

Définition II.5.1 Soit M un A-module, on dira qu'une relation d'équivalence $\sim$ sur M est *compatible à la structure de A-module* (ou simplement *compatible* si aucune confusion n'est à craindre,) si pour tout $(x, y) \in M \times M$, tout $(x', y') \in M \times M$ et tout $(a, b) \in A \times A$,

$$x \sim x' \text{ et } y \sim y'$$

implique

$$ax + by \sim ax' + by'$$

(cf. I.2.12,) .

Proposition II.5.2 *Soit M un A-module.*

i) Une relation d'équivalence $\sim$ sur M est compatible avec la structure de A-module de M si et seulement si $\overline{0_M}$ est un sous-A-module de M, (où $\overline{0_M}$ est la classe modulo $\sim$ de l'élément neutre 0_M de $(M, +_M)$.)

ii) Étant donné un sous-A-module K de M, il existe une unique relation d'équivalence compatible $\sim_K$ sur M telle que $K = \overline{0_M}$ (où $\overline{0_M}$ est la classe de 0_M modulo $\sim_K$.)

Remarque II.5.2.3 Comparer cette proposition avec la proposition I.2.13.

***Preuve** :*

i) Si $\sim$ est une relation d'équivalence compatible sur M, la classe $\overline{0_M}$ de 0_M modulo $\sim$ est non vide car $0_M \in \overline{0_M}$. Pour tout $(x, y) \in \overline{0_M} \times \overline{0_M}$, i.e.pour tout $(x, y) \in M \times M$ tel que

$$x \sim 0_M \text{ et } y \sim 0_M ,$$

pour tout $(a, b) \in A \times A$,

$$ax + by \sim a0_M + b0_M = 0_M .$$

C'est-à-dire que $\overline{0_M}$ est non vide et stable par combinaisons linéaires à coefficients dans A. D'après II.4.6.b), $\overline{0_M}$ est un sous-A-module de M.

*ii) Étant donné un sous A-module K de M, supposons (**analyse**,) qu'il existe une relation d'équivalence compatible $\sim$ sur M telle que $\overline{0_M} = K$. Pour tout $(x, x') \in M \times M$, si $x \sim x'$, en utilisant la propriété de compatibilité uniquement par rapport à x', on a :*

$$x - x' \sim x - x = 0_M .$$

Il s'ensuit que nécessairement $x - x' \in \overline{0_M} = K$.

*Il suffit donc de montrer (**synthèse**, laissée en exercice,) que l'on définit bien une relation compatible $\sim_K$ sur M en posant*

$$x \sim_K y \text{ si } x - y \in K .$$

Remarque II.5.3 On parlera désormais indifféremment de classes modulo un sous-A-module ou modulo la relation compatible qui lui est canoniquement associée d'après II.5.2.ii).

Proposition II.5.4 *Soit M un A-module. Étant donné un sous-A-module K ou de manière équivalente une relation d'équivalence compatible $\sim_K$ sur M, il existe une unique structure de A-module sur l'ensemble $M/\sim_K$ des classes d'équivalences modulo K (ou modulo $\sim_K$) telle que la surjection canonique $\pi : M \to M/\sim_K$ soit un morphisme de A-modules (cf. II.3.5,) (cf. II.1.3.a).)*

***Preuve** :*

Analyse *Si π est un morphisme, pour tout $(\overline{x}, \overline{y}) \in M/\sim_K \times M/\sim_K$, et pour tous $(x, y) \in M \times M$, $(x', y') \in M \times M$, tels que*

$$\begin{array}{rcl} x \in \overline{x} \text{ i.e. } p(x) & = & \overline{x}, \\ x' \in \overline{x} \text{ i.e. } p(x') & = & \overline{x}, \\ y \in \overline{y} \text{ i.e. } p(y) & = & \overline{y}, \\ y' \in \overline{y} \text{ i.e. } p(y') & = & \overline{y} ; \end{array} \qquad \text{II.5.4.1}$$

pour tout $(a, b) \in A \times A$,

$$\begin{array}{rcl} \pi(a \cdot_M x +_M b \cdot_M y) & = & a \cdot_{M/\sim_K} \pi(x) +_{M/\sim_K} b \cdot_{M/\sim_K} \pi(y) \\ & = & a \cdot_{M/\sim_K} \overline{x} +_{M/\sim_K} b \cdot_{M/\sim_K} \overline{y} \\ & = & a \cdot_{M/\sim_K} \pi(x') +_{M/\sim_K} b \cdot_{M/\sim_K} \pi(y') \\ & = & \pi(a \cdot_M x' +_M b \cdot_M y') . \end{array}$$

Ceci prouve, comme π est surjective, que si cette structure existe, elle est nécessairement unique.

Synthèse *Or précisément, puisque la relation d'équivalence modulo K est compatible (cf. II.5.2.ii),) pour tous $(x, y) \in M \times M$, $(x', y') \in M \times M$ vérifiant les conditions II.5.4.1, et pour tout $(a, b) \in A$, on a :*

$$\begin{array}{rcl} a \cdot_M x +_M b \cdot_M y & \sim_K & a \cdot_M x' +_M b \cdot_M y' \\ \Leftrightarrow \quad \pi(a \cdot_M x +_M b \cdot_M y) & = & \pi(a \cdot_M x' +_M b \cdot_M y') \, . \end{array}$$

On définira donc la structure de A-module sur $M/\sim_K$ en posant, pour tout $(\overline{x}, \overline{y}) \in M/\sim_K \times M/\sim_K$, et tout $(a, b) \in A \times A$,

$$a \cdot_{M/\sim_K} \overline{x} \; +_{M/\sim_K} \; b \cdot_{M/\sim_K} \overline{y} \; := \; \pi(a \cdot_M x +_M b \cdot_M y) \, ; \qquad \textit{II.5.4.2}$$

(où x (resp. y) est n'importe quel représentant de $\overline{x}$ (resp. $\overline{y}$).)

Définition II.5.5 Pour un A-module M et un sous-A-module K, on notera M/K l'ensemble

$M/\sim_K$ muni de la structure de A-module définie par la proposition II.5.4

que l'on appellera *structure quotient*.

On appellera M/K *module quotient.*

Définition II.5.6 Soit B une A-algèbre, on rappel que B et canoniquement un B-module sur lui-même à travers l'identité (cf. II.3.4.b).) On appelle *idéal* tout sous-B-module de B.

On appelle *idéal propre* de B tout sous-B-module différent de B lui-même.

Remarque II.5.7 Nous ne discutons pas ici les propriétés des idéaux qui seront détaillées dans la section II.5.6.

Exemple II.5.8 a) Une conséquence immédiate de la proposition II.4.9 est que le noyau d'un morphisme d'anneaux (cf. II.1.9,) (d'algèbres (cf. II.2.2)) $f : B \to C$ est un idéal propre de B. En effet,

$$f : (B, +_B, \cdot_B) \to (C, +_C, \cdot_C)$$

est un morphisme de B-modules (cf. II.3.12.ii),) où B est muni de sa structure de B-module à travers l'identité Id_B (cf. II.3.4.b)) et C est muni de la structure de B-module induite par f (cf. II.3.4.a).)

De plus, le noyau $\mathrm{Ker}\, f$ de f est un idéal propre de B : si en effet, $\mathrm{Ker}\, f = B$, pour tout $b \in B$, $f(b) = 0_C$ et en particulier,

$$f(1_B) \; = \; 0_C \; \neq \; 1_C$$

ce qui est incompatible avec les axiomes ANN_3 de la définition II.1.1 et ANN_7 de la définition II.1.9.

b) Pour toute A-algèbre B $\{0_B\}$ est un idéal propre de B.

Proposition II.5.9 *Étant donnés une A-algèbre B et un idéal propre J de B, il existe une unique structure de A-algèbre sur le B-module B/J (cf. II.5.4) telle que le morphisme de B-modules canonique $\pi : B \to B/J$ soit un morphisme de A-algèbres.*

Preuve : *Étant donnée la proposition II.5.4, il ne reste à déterminer que la multiplication et le morphisme structural de B/J (cf. II.2.1.)*

*Si π est un morphisme de A-algbres (**analyse**), pour tout $(\overline{x}, \overline{y}) \in B/J \times B/J$, et tous x, x', y, y' satisfaisant II.5.4.1, on aura nécessairement :*

$$\begin{aligned} \pi(x *_B y) &= \pi(x) *_{B/J} \pi(y) \\ &= \overline{x} *_{B/J} \overline{y} \\ &= \pi(x') *_{B/J} \pi(y') \\ &= \pi(x' *_B y') ; \end{aligned}$$

et $1_{B/J} = \pi(1_B)$; ce qui prouve, grâce à la surjectivité de π, que cette structure, si elle existe, est nécessairement unique.

*Or (**synthèse**,) pour tous x, x', y, y' satisfaisant II.5.4.1,*

$$\begin{aligned} x *_B y -_B x' *_B y' &= xy - x'y + x'y - x'y' \\ &= y(x - x') + x'(y - y') \\ &= y \cdot_J (x -_J -x') +_J x' \cdot_J (y -_J y') \\ &\in J ; \end{aligned}$$

car $x - x'$ (resp. $y - y'$) appartient à J par hypothèse et J est stable par combinaisons linéaires à coefficients dans B (cf. II.4.6.b).) On posera donc, pour tout $(\overline{x}, \overline{y}) \in B/J \times B/J$,

$$\overline{x} *_{B/J} \overline{y} := \pi(x *_B y) = \overline{x *_B y} ; \qquad \text{II.5.9.1}$$

(pour n'importe quel représentant x de $\overline{x}$ (resp. y de $\overline{y}$).)

Reste encore à vérifier que

$$1_{B/J} := \pi(1_B) \neq 0_{B/J} = \pi(0_B) .$$

Or

$$\begin{aligned} & 1_{B/J} = 0_{B/J} \\ \Leftrightarrow \quad & 1_B \sim_J 0_B \\ \Leftrightarrow \quad & 1_B \in J . \end{aligned}$$

Or, si $1_B \in J$, pour tout $b \in B$,

$$b = b *_B 1_B \in J ,$$

d'après (cf. II.4.6.b).)

Ceci implique $B \subset J$ i.e.$B = J$; ce qui est en contradiction avec le fait que J est un idéal propre.

La vérification que $p(1_B)$ est bien un élément neutre pour la multiplication $*_{B/J}$ est laissée en exercice.

Enfin si $f_B : A \to B$ est le morphisme structural de B, le seul choix pour le morphisme structural de B/J est $\pi \circ f_B$ (cf. II.2.1.)

Remarque II.5.10 En fait, la surjection canonique $\pi : B \to B/J$ est, sous les hypothèses de la proposition II.5.9, un morphisme de B-algèbres où le morphisme structural de B/J est π lui-même.

Définition II.5.11 Étant donnés une A-algèbre B et un idéal propre J on appellera *algèbre quotient* le A-module B/J muni de la structure d'algèbre définie par la proposition II.5.9.

On dira indifféremment que B/J est *muni de la structure quotient*.

II.6 . −Factorisation canonique des morphismes

Dans toute cette section, A est un anneau commutatif. (cf. II.1.2.)
Les A-algèbres considérées sont commutatives (cf. II.2.1) (sauf mention du contraire.)

Proposition II.6.1 *Soient M un A-module, (resp. B une A-algèbre,) et K un sous-A-module de M, (resp. J un idéal propre de B.) Pour tout morphisme de A-modules, (resp. A-algèbres,)*

$$u : M \to P, \text{ (resp. } B \to C, \text{) tel que } u(K) = \{0_P\}, \text{ (resp. } u(J) = \{0_C\} \text{ ,)}$$

il existe un unique morphisme de A-modules, (resp. de A-algèbres,) $v : M/K \to P$, (resp. $B/J \to C$,) tel que

$$v \circ \pi = u \, ;$$

(où $\pi : M \to M/K$, (resp. $B \to B/J$,) est la surjection canonique.)

Remarque II.6.1.1 Comparer la proposition ci-dessus au lemme I.2.19.

Preuve *:*

i) On traite d'abord le cas d'un morphisme de A-modules

$$u : M \to P \text{ tel que } u(K) = \{0_P\},$$

où K est un sous-A-module de M.

Si $v : M/K \to P$ *tel que* $v \circ \pi = u$ *existe (**analyse**,) pour tout* $\overline{x} \in M/K$ *et tout* $(x, x') \in \overline{x} \times \overline{x}$, *on a :*

$$\begin{aligned} u(x) &= (v \circ \pi)(x) \\ &= v(\overline{x}) \\ &= (v \circ \pi)(x') \\ &= u(x') \ . \end{aligned}$$

Ce qui implique que, comme π *est surjective, s'il existe,* v *est bien déterminé et donc unique.*

*Or, (**synthèse**,) pour tout* $\overline{x} \in M/K$ *et tout* $(x, x') \in \overline{x} \times \overline{x}$, $x - x' \in K$. *Il s'ensuit donc que* $u(x - x') = 0_P$ *par hypothèse et donc* $u(x) = u(x')$. *On devra donc poser, pour tout* $\overline{x} \in M/K$

$$v(\overline{x}) := u(x) \ ; \qquad 1$$

(pour n'importe quel représentant x *de* $\overline{x}$.)

ii) On vérifie que le morphisme v *défini ci-dessus est bien un morphisme de* A*-modules (cf. II.3.5.)*

Pour $(\overline{x}, \overline{y}) \in M/K \times M/K$ *tel que* $x \in \overline{x}$, $y \in \overline{y}$ *et tout* $(a, b) \in A \times A$,

$$\begin{aligned} v(a \cdot_{M/K} \overline{x} +_{M/K} b \cdot_{M/K} \overline{y}) &= u(a \cdot_M x +_M b \cdot_M y) \\ &= a \cdot_P u(x) +_P b \cdot_P u(y) \\ &= a \cdot_P v(\overline{x}) +_P b \cdot_P v(\overline{y}) \ . \end{aligned}$$

iii) Enfin si $B = M$ *est une* A*-algèbre,* $J = K$ *un idéal propre de* B *et* $u : B \to C$ *un morphisme de* A*-algèbres tel que* $u(J) = \{0_C\}$ *il existe, d'après (i) et (ii) un unique morphisme de* A*-modules* $v : B/J \to C$ *tel que* $v \circ p = u$. *Montrons que* v *est un morphisme de* A*-algèbres (cf. II.2.2.)*

On a d'abord :

$$\begin{aligned} v(1_{B/J}) \quad \overset{\text{(cf. II.5.9)}}{=} \quad & v(\overline{1_B}) \\ = \quad & u(1_B) \\ = \quad & 1_C \ . \end{aligned}$$

Ensuite, pour tout $(\overline{x}, \overline{y}) \in B/J \times B/J$ *tel que* $x \in \overline{x}$ *et* $y \in \overline{y}$, *on a :*

$$\begin{aligned} v(\overline{x} *_{B/J} \overline{y}) &= u(x *_B y) \\ &= u(x) *_C u(y) \\ &= v(\overline{x}) *_C v(\overline{y}) \ . \end{aligned}$$

Enfin, si $f_B : A \to B$, *(resp.* $f_C : A \to C$, *) est le morphisme structural de* B, *(resp.* C, *) on rappel (cf. II.5.9) que* $\pi \circ f_B$ *est le morphisme structural de* B/J ; *on a alors :*

$$\begin{aligned} v \circ \pi \circ f_B &= u \circ f_B \\ &= f_C \ . \end{aligned}$$

Proposition II.6.2 *Avec les hypothèses et les notations de la proposition II.6.1*

i) Si u est un morphisme surjectif (épimorphisme,) alors v est surjectif.

ii) Si $\operatorname{Ker} u \ = \ K$, *alors v est injectif (monomorphisme.)*

Preuve *:*

i) Si u est surjectif, pour tout $y \ \in \ P$ (resp. $y \ \in \ C,$) il existe un $x \ \in \ M$ (resp. $x \ \in \ B,$) tel que $y \ = \ u(x)$. On a alors,

$$v(\pi(x)) \ = \ u(x) \ = \ y$$

ce qui prouve que $\pi(x)$ est un antécédent pour y par v et donc que v est surjectif.

ii) Pour tout $(\xi, \xi') \in M/K \times M/K$ (resp. $(\xi, \xi') \in B/J \times B/J,$) il existe $(x, x') \in M \times M$ (resp. $(x, x') \in B \times B,$) tel que

$$\pi(x) \ = \ \xi \text{ et } \pi(x') \ = \ \xi' \ .$$

Alors

$$\begin{array}{rrrcl} & & v(\xi) & = & v(\xi') \\ \Leftrightarrow & & v[\pi(x)] & = & v[\pi(x')] \\ \Leftrightarrow & & u(x) & = & u(x') \\ \Leftrightarrow & & x - x' & \in & \operatorname{Ker} u \\ \operatorname{Ker} u \overset{\Leftrightarrow}{=} & K & x - x' & \in & K \\ \Leftrightarrow & & \pi(x) & = & \pi(x') \\ \Leftrightarrow & & \xi & = & \xi' \end{array}$$

ce qui prouve que v est injectif.

Corollaire II.6.3 *Étant donné un morphisme surjectif de A-modules, (resp. de A-algèbres,)*

$$q \ : \ M \ \to \ Q \ , \ (\textit{resp. } .q \ : \ B \ \to \ Q \ ,)$$

il existe un unique isomorphisme (de A-modules, (resp. de A-algèbres,))

$$\pi \ : \ M/\operatorname{Ker} q \ \cong \ Q \ (\textit{resp. } .\phi \ : \ B/\operatorname{Ker} q \ \cong \ Q \ ,) \ \textit{tel que} \ \phi \circ \pi \ = \ q \ ,$$

$\big($ *où* $\pi \ : \ M \ \to \ M/\operatorname{Ker} q \ , \ (\textit{resp. } .\pi \ : \ B \ \to \ B/\operatorname{Ker} q \ ,)$ *est la surjection canonique.*$\big)$

Preuve *: C'est une conséquence immédiate de la proposition II.6.2 grâce à la proposition II.3.15, (resp. au corollaire II.3.18,)*

Corollaire II.6.4 *Étant donné un morphisme de A-modules, (resp. de A-algèbres,) $u : M \to P$, (resp. $B \to C,$) il existe un unique isomorphisme (de A-modules, (resp. de A-algèbres,)) $\phi : M/\mathrm{Ker}\, u \to \mathrm{Im}\, u$, (resp. $B/\mathrm{Ker}\, u \to \mathrm{Im}\, u,$) tel que :*

$$\phi \circ \pi = u\,,$$

(où π est la surjection canonique.)

Preuve *: C'est une conséquence immédiate du corollaire II.6.3.*

Corollaire II.6.5 *Soit M (resp. $B,$) un A module (resp. une A-algèbre.) Étant donnés des sous-A-modules N et P de M (resp. des idéaux propres I et J de B) tels que $P \subset N$ (resp. $I \subset J,$)*

i) on a un morphisme de A-modules (resp. de A-algèbres) canonique surjectif (épimorphisme) $M/P \to M/N$ (resp. $B/I \to B/J;$)

ii) on a un morphisme canonique injectif (monomorphisme) de A-modules $N/P \hookrightarrow M/P$.

Preuve *: C'est une conséquence facile du corollaire II.6.3, .*

Proposition II.6.6 *Étant donné un A-module M (resp. une A-algèbre $B,$) les données suivantes sont équivalentes au sens où la donnée de l'une d'entre elles permet de construire canoniquement les trois autres :*

i) Un sous-A-module K de M (resp. un idéal propre J de $B.$)

ii) Un monomorphisme (morphisme injectif) $i : K \hookrightarrow M$.

iii) Une relation d'équivalence compatible sur M (resp. $B.$)

iv) Un morphisme surjectif (épimorphisme,) $q : M \to Q$ (resp. $q : B \to Q.$)

Remarque II.6.7 i) Comparer cette proposition à la proposition I.2.17.

ii) Le point II.6.6.ii) est spécifique aux A-modules et ne s'adapte pas de manière satisfaisante au contexte des A-algèbres. En effet si l'on a un monomorphisme de A-algèbres $i : B' \hookrightarrow B$, B' est une sous-A-algèbre de B (cf. II.2.5,) et le quotient n'est pas défini dans ce contexte.

Preuve : Les détails de cette démonstration ne sont pas donnés dans la mesure où elle est très similaire à celle de la proposition I.2.17.

On notera qu'on n'a pas défini, dans ce paragraphe, à proprement parler, la notion de relation d'équivalence compatible à une structure d'algèbre. On laisse le soin au lecteur de vérifier qu'en fait la compatibilité à la structure de module suffit .

Corollaire II.6.1 *Étant donné un A-module M (resp. une A-algèbre $M,$) on peut mettre en correspondance les éléments caractéristiques des trois données équivalentes de la proposition II.6.6, dans le tableau récapitulatif suivant :*

sous-module / idéal K	*relation d'équivalence $\sim$*	*épimorphisme p*
K	$\overline{0}$	$\mathrm{Ker}\, p$
$x + K$	$\overline{x}$	$p^{-1}[p(x)] \;=\; p^{-1}($
M/K	$\{\overline{x}\ ,\ x \in M\}$	$\mathrm{Im}\, p$.

II.6.2. − Dans le cas des A-modules on adoptera usuellement la notation, pour $i : K \hookrightarrow M$ un sous-A-module de M (*i.e.*un monomorphisme de A-modules) (resp. $p \;:\; M \;\to\; Q$ un épimorphisme de A-modules,)

$$0 \to K \xrightarrow{\ i\ } M \xrightarrow{\ \pi\ } M/K \to 0 \qquad \text{II.6.2.1}$$

(resp.

$$0 \to \mathrm{Ker}\, p \xrightarrow{\ i\ } M \xrightarrow{\ p\ } Q \to 0\ ) \qquad \text{II.6.2.2}$$

et on parlera de *suite exacte courte de A-modules.*

Remarque II.6.2.3 La notation serait maladroite dans le contexte des A-algèbres, dans la mesure où, comme nous l'avons déjà fait remarquer en II.6.7.ii) le terme de gauche dans la suite (le noyau qui est un idéal) ne serait pas de même nature que les deux autres termes qui sont des algèbres.

Proposition II.6.3 *Soit M un A-module et K un sous-A-module de M. Notons*

$$\pi \;:\; M \to Q \;:=\; M/K$$

la surjection canonique.

Un sous-ensemble N de Q est un sous-A-module de Q si et seulement si $\pi^{-1}(N)$ est un sous-A-module de M.

On a alors

$$N \;\cong\; \pi^{-1}(N)/(\pi^{-1}(N) \cap K)\ .$$

***Preuve** :*

- *Supposons que N est une partie de Q telle que $\pi^{-1}(N)$ soit un sous-A-module de M. Alors $\pi^{-1}(N)$ n'est pas vide, d'où il découle que N n'est pas vide non plus. Par ailleurs pour tout $(u,v) \in N \times N$, il existe $(x,y) \in M \times M$ tel que*

$$\pi(x) \;=\; u \,\text{et}\, \pi(y) \;=\; v$$

car π est surjective. Il est clair que

$$(x,y) \in \pi^{-1}(N) \times \pi^{-1}(N)\;.$$

Comme $\pi^{-1}(N)$ est un sous-A-module de M, pour tout $(a,b) \in A \times A$, $ax + by \in \pi^{-1}(N)$; i.e.

$$\begin{array}{rcl} a \cdot_Q u +_Q b \cdot_Q v & = & a \cdot_Q \pi(x) +_Q b \cdot_Q \pi(y) \\ & = & \pi(a \cdot_M x +_M b \cdot_M y) \\ & \in & N\;; \end{array}$$

c'est-à-dire que N est non vide et stable par combinaisons linéaires et donc est un sous-A-module de Q d'après II.4.6.b).

- *Réciproquement, soit N un sous-A-module de Q. Comme $\pi(0_M) \;=\; 0_Q \in N$, $\pi^{-1}(N)$ est non vide. La stabilité par combinaisons linéaires est à peu près évidente puisque π est un morphisme et que N est stable.*
- *Soit N un sous-A-module de Q. D'après ce qui précède et II.4.8.b), $K \cap \pi^{-1}(N)$ est un sous-A-module de $\pi^{-1}(N)$. Par ailleurs, $\pi(K \cap \pi^{-1}(N)) \;=\; \{0_Q\}$ puisque $\pi(K) \;=\; \{0_Q\}$. On a même de manière presque évidente $\mathrm{Ker}\,\pi_N \;=\; \pi^{-1}(N) \cap K$. De manière non moins immédiate, π_N est surjective. Ainsi, d'après le corollaire II.6.4 on a un isomorphisme canonique*

$$\pi^{-1}(N)/(K \cap \pi^{-1}(N)) \;=\; \pi^{-1}(N)/\mathrm{Ker}\,\pi_N \;\cong\; \mathrm{Im}\,\pi_N \;=\; N\;.$$

II.7 . −Quelques constructions

Dans toute cette section, A est un anneau commutatif. (cf. II.1.2.)
Les A-algèbres considérées sont commutatives (cf. II.2.1) (sauf mention du contraire.)

Remarque II.7.1 Étant donné un entier $n \in \mathbb{N}^*$, si $E_i\,,_{1\leq i\leq n}$ sont des ensembles, le *produit cartésien*

$$F \;:=\; \prod_{i=1}^{n} E_i \;=\; E_1 \times \ldots \times E_n$$

est l'ensemble des $(x_1, \ldots, x_n)$ $x_i \in E_i$. Le produit cartésien F est canoniquement muni de n projections (surjections ensemblistes)

$$\begin{array}{rccc} \pi_{i\,,\,1 \leq i \leq n}: & F & \longrightarrow & E_i \\ & (x_1, \ldots, x_n) & \longmapsto & x_i\,. \end{array}$$

Proposition II.7.2 (Structure produit) *Étant donnés un entier* $n \in \mathbb{N}^*$,

$$M_{i1 \leq i \leq n}\,,$$

(resp.

$$B_{i1 \leq i \leq n},)$$

des A*-modules (cf. II.3.1,) (resp. des* A*-algèbres (cf. II.2.1,)) il existe une unique structure de* A*-module, (resp. de* A*-algèbre,) sur le produit cartésien* $\prod_{i=1}^{n} M_i$, *(resp.* $\prod_{i=1}^{n} B_i,$*) telle que les projections canoniques (cf. II.7.1) soient des morphismes.*

Preuve *:*

Modules ***Analyse :*** *S'il existe une structure de* A*-module sur* $P := \prod_{i=1}^{n} M_i$, *(i.e.une loi de composition interne* $+_P : P \times P \to P$ *et une loi de composition externe* $\cdot_P : A \times P \to P$ *vérifiant les axiomes* Mod_1 *à* Mod_5 *de la définition II.3.1, telles que pour tout* $1 \leq i \leq n$ p_i *soit un morphisme, alors pour tout*

$$\begin{array}{rcl} X & := & (x_1, \ldots, x_n) \in P\,, \\ Y & := & (y_1, \ldots, y_n) \in P\,, \end{array}$$

tout $(a, b) \in A \times A$ *et tout* $1 \leq i \leq n$

$$\begin{array}{rcl} \pi_i(a \cdot_P X +_P b \cdot_P Y) & = & a \cdot_{M_i} \pi_i(X) +_{M_i} a \cdot_{M_i} \pi_i(Y) \\ & = & a \cdot_{M_i} x_i +_{M_i} b \cdot_{M_i} y_i \end{array}$$

.

C'est-à-dire que pour tout $1 \leq i \leq n$

$$(a \cdot_P X +_P b \cdot_P Y)_i = a \cdot_{M_i} x_i +_{M_i} b \cdot_{M_i} y_i\,;$$

c'est-à-dire

$$a \cdot_P X +_P b \cdot_P Y = (a \cdot_{M_1} x_1 +_{M_1} b \cdot_{M_1} y_1, \ldots, a \cdot_{M_n} x_n +_{M_n} b \cdot_{M_n} y_n)\,. \quad \textit{II.7.2.1}$$

Synthèse : *reste à montrer que la formule II.7.2.1 définit bien une structure de* A*-module sur* P*. Il faut notamment vérifier que l' élément neutre est*

$$0_P = (0_{M_1}, \ldots, 0_{M_n})\,. \quad \textit{II.7.2.2}$$

Algèbres *De la même manière, si $B_{i1 \leq i \leq n}$, sont des A-algèbres la multiplication $*_C$ sur $C := \prod_{i=1}^{n} B_i$ est, nécessairement définie, si l'on veut que chaque π_i soit un morphisme par :*

$$(x_1, \ldots, x_n) *_C (y_1, \ldots, y_n) := (x_1 *_{B_1} y_1, \ldots, x_n *_{B_n} y_n) . \qquad \textit{II.7.2.3}$$

C'est un exercice de vérifier que C muni de cette multiplication $*_C$ dont l' élément neutre est

$$1_C := (1_{B_1}, \ldots, 1_{B_n}) \qquad \textit{II.7.2.4}$$

et de l'addition $+_C$ héritée de sa structure de A-module (cf. (i)) est un anneau (cf. II.1.1.)

Enfin, le morphisme de structure $f_C : A \to C$ s'il existe, vérifie nécessairement, pour tout $1 \leq i \leq n$

$$\pi_i \circ f_C = f_{B_i}$$

(où $f_{B_i} : A \to B_i$ est le morphisme structural de l'algèbre B_i.)

Il s'ensuit dès lors, que pour tout $a \in A$,

$$f_C(a) = (f_{B_1}(a), \ldots, f_{B_n}(a)) . \qquad \textit{II.7.2.5}$$

Reste à vérifier que f_C ainsi défini est bien un morphisme d'anneaux (cf. II.1.9,) ce qui est laissé en exercice. .

Définition II.7.3 Si $M_{i1 \leq i \leq n}$, (resp. $B_{i1 \leq i \leq n}$,) sont des A-modules, (resp. des A-algèbres,) on appelle *structure produit* (de A-module, (resp. de A-algèbre,)) l'unique structure sur le produit cartésien $\prod_{i=1}^{n} M_i$, (resp. $\prod_{i=1}^{n} B_i$,) telle que les projections naturelles soient des morphismes. Cette structure est définie par les formules II.7.2.1, II.7.2.2, II.7.2.3, II.7.2.4, II.7.2.5.

Lorsqu'on notera $\prod_{i=1}^{n} M_i$, (resp. $\prod_{i=1}^{n} B_i$,) sans autre précision, la structure considérée sera la structure produit.

Exemple II.7.4 Étant donnés deux corps K et L, on peut former le produit $K \times L$ au sens des $\mathbb{Z}$-algèbres, qui est encore, d'après ce qui précède, une $\mathbb{Z}$-algèbre. Cependant, $K \times L$ n'est jamais un corps. En effet, pour deux éléments $x \in K$ et $y \in L$ tous deux non nuls, les éléments $(x, 0)$ et $(0, y)$ dans $K \times L$ sont également tous deux non nuls. En revanche leur produit

$$(x, 0) *_{K \times L} (0, y) = (0, 0)$$

est nul. Ceci prouve qu'aucun des deux éléments $(x, 0)$ et $(0, y)$ n'est inversible dans $K \times L$.

On sait bien que $\mathbb{C}$ s'identifie à $\mathbb{R} \times \mathbb{R}$ en tant que $\mathbb{R}$-espace vectoriel par exemple (cf. II.3.13) et que $\mathbb{C}$ est un corps. On remarquera alors que la loi $*$ sur $\mathbb{C}$ n'est pas la loi produit : en effet

$$(a + ib) * (c + id) = ac - bd + i(ad + bc)$$

et non $ac + ibd$.

Proposition II.7.5 *Étant donnés un A-module M et des sous-A-modules $N_{i\ ,\ i\in I}$ (où $I \subset \mathbb{N}$ est un ensemble d'indices,)*

i)

$$\bigcap_{i\in I} N_i$$

est un sous-A-module de M et c'est le plus grand (au sens de l'inclusion) sous-A-module de M contenu dans tous les N_i ;

ii)

$$\sum_{i\in I} N_i \ = \ N_1 +_M \ldots +_M N_i +_M \ldots \ = \ \{\sum_{k=1}^{n} x_{i_k} \ , \ i_k \in I \ , \ x_{i_k} \in N_{i_k}\}$$

est un sous-A-module de M et c'est le plus petit (au sens de l'inclusion) sous-A-module de M contenant tous les N_i .

Preuve *: Ces résultats ont déjà été vus pour les espaces vectoriels et la généralisation aux modules ne pose aucun problème .*

Définition II.7.6 i) Pour une famille $N_{i\ ,1\leq i\leq n}$ de sous-A-modules d'un A-module M, on dit que la somme $N_1+\ldots+N_n$ est *directe* si, pour tout $x \in N_1+\ldots+N_n$ il existe un unique n-uplet

$$(x_1, \ldots, x_n) \in N_1 \times \ldots \times N_n$$

tel que

$$x \ = \ \sum_{i=1}^{n} x_i \ .$$

On notera alors

$$N_1 \ + \ \ldots \ + \ N_n \ = \ N_1 \ \oplus \ \ldots \ \oplus N_n \ .$$

ii) Pour un sous-A-module $N \subset M$ de M on dit qu'un sous-A-module $P \subset M$ de M est un *supplémentaire* de N si $M \ = \ N \ \oplus \ P$ est la somme directe de N et P.

vii) Pour un sous-A-module $N \subset M$ de M, l'existence d'un supplémentaire n'est pas automatiquement assurée. Elle équivaut en fait à l'existence d'une section de la surjection canonique $\pi \ : \ M \ \to \ M/N$.

Proposition II.7.8 *Étant donné un A-module M et des sous-ensembles S et N de M avec $S \neq \emptyset$, les conditions suivantes sont équivalentes :*

a)

$$N \;=\; \{\sum_{i=1}^{n} a_i \cdot_M s_i \;,\; n \in \mathbb{N} \;,\; a_{i1 \,\leq\, i \,\leq\, n} \in A \;,\; s_{i1 \,\leq\, i \,\leq\, n} \in S\} \;;$$

b) N est un sous-A-module de M tel que, pour tout sous-A-module P de M contenant S, $N \subset P$;

c)

$$N \;=\; \bigcap_{P \text{ sous-}A\text{-module de } M \;|\; S \subset P} P \;.$$

***Preuve** : La preuve a déjà été donnée, dans ce cours, pour les groupes (cf. I.1.24,)*

Définition II.7.9 Étant donnés un A-module M et des sous-ensembles S et N de M, avec S non vide, si N et S vérifient l'une des trois conditions équivalentes de la proposition II.7.8, on dira que N *est le sous-A-module de M engendré par S*. On dira que S est un *système générateur de N*.

Si $N \;=\; M$ on dira que le *module M est engendré par S*, ou que S *est un système générateur de M*.

Remarque II.7.10 Si S est l'ensemble vide, on posera, par convention, que le sous-A-module de M engendré par S est $\{0_M\}$ (cf. I.1.26.)

Exemple II.7.11 a) Le $\mathbb{Z}$-module $\mathbb{Z}/n$ (cf. I.1.5.b)) est engendré par $1_{\mathbb{Z}/n} \;=\; \overline{1}$ ou par tout élément inversible de l'anneau $(\mathbb{Z}/n, +, *)$.

b) Tout sous-$\mathbb{Z}$-module de $\mathbb{Z}$, (resp. sous-$K[X]$-module de $K[X]$ (cf. IV.2,)) *i.e.*tout idéal (cf. II.5.6) de $\mathbb{Z}$ (resp. $K[X],$) est engendré par un seul élément .

Définition II.7.12 Étant donné un A-module M,

i) on dit qu'un sous-ensemble $\mathcal{B}$ de M est *libre* si pour tout $n \;\in\; \mathbb{N}$, pour tous $b_{i\;,1 \leq i \leq n} \in \mathcal{B}$, tous $a_{i\;,1 \leq i \leq n} \in A$,

$$\sum_{i=1}^{n} a_i \cdot_M b_i \;=\; 0_M$$

implique $a_i \;=\; 0_A$ pour tout $1 \;\leq\; i \;\leq\; n$;

ii) on dit qu'un sous-ensemble $\mathcal{B}$ de M est une *base* si $\mathcal{B}$ est libre et générateur pour M (cf. II.7.9.)

Définition II.7.13 i) On dira qu'un A-module M est *libre* s'il admet une base.

ii) On dira qu'un A-module M est *de type fini* s'il admet un système générateur fini.

Remarque II.7.14 La nouveauté des modules par rapport aux espaces vectoriels (cf. II.3.13,) est que tous les modules ne sont pas libres !

Par exemple, pour $n \in \mathbb{N}^*$, $\mathbb{Z}/n$ (cf. I.1.5.b)) n'est pas un $\mathbb{Z}$-module libre. Néanmoins, il est de type fini.

Proposition II.7.15 *Pour un A-module M,les conditions suivantes sont équivalentes :*

a) M possède une base de cardinal fini $n \in \mathbb{N}^*$.

b) Il existe un isomorphisme

$$M \cong \mathbb{Z}^n (\textit{resp. } A^n)$$

(cf. II.3.4.c),) (cf. II.7.2.)

c) M est un A-module libre et de type fini.

***Preuve** :*

a) $\Leftrightarrow$ c) résulte des définitions mêmes.

a) $\Rightarrow$ b) Supposons que $\mathcal{B} := \{b_i \ , \ 1 \leq i \leq n\}$ est une base finie de cardinal $n \in \mathbb{N}^*$ de M. On montre qu'il existe un unique morphisme

$$\begin{array}{rccl} \phi : & M & \to & A^n \\ & b_i & \mapsto & (0, 0, \ldots, 1, \ldots, 0, \ldots) \ , \end{array}$$

(où 1 est placé en $i^{\text{ème}}$ position.) On laisse le soin au lecteur de montrer que ϕ ainsi défini est un isomorphisme.

b) $\Rightarrow$ a) Un isomorphisme $\phi : M \to A^n$ étant donné, c'est un exercice facile que de montrer que

$$\{\phi^{-1}(0, 0, \ldots, 1, \ldots, 0, \ldots) \ , \ \textit{avec } 1 \textit{ en } i^{\text{ème}} \textit{ position} \ , \ 1 \leq i \leq n\}$$

est une base de M.

II.8 . −Théorème des restes chinois

Dans cette section, A est un anneau commutatif.

Définition II.8.1 Deux idéaux I et J d'une A-algèbre B sont *comaximaux* si $I+J = B$ (cf. II.7.5.ii),) ce qui équivaut à dire qu'il existe un couple $(x, y) \in I \times J$ tel que $x + y = 1_B$.

Proposition II.8.2 *Étant donnés une A-algèbre B et $I_1, \ldots, I_n$ des idéaux ; si les I_k $1 \leq k \leq n$ sont deux à deux comaximaux, c'est-à-dire que pour tout $1 \leq k < l \leq n$, $B = I_k + I_l$; alors pour tout $1 \leq k \leq n$ I_k et $\bigcap_{1 \leq l \leq n l \neq k} I_l$ sont comaximaux.*

***Preuve** : On peut démontrer ce résultat par récurrence sur le nombre n d'idéaux. Pour $n = 2$, le résultat est tautologique.*

Supposons $n > 2$. Pour tout $1 \leq k \leq n$ fixons $1 \leq m \leq n$ avec $m \neq k$ et notons

$$J := \bigcap_{1 \leq l \leq n l \not= , \, l \neq m} I_l \, .$$

Par hypothèse de récurrence, I_k et J sont comaximaux et, par hypothèse, I_k et I_m sont comaximaux. Il existe donc $(x, y) \in I_k \times J$ (resp. $(z, t) \in I_k \times I_m$) tel que $1_B = x + y$ (resp. $1_B = z + t$.) Il s'ensuit que

$$\begin{aligned} 1_B &= (x + y)(z + t) \\ &= xz + xt + zy + yt \, . \end{aligned}$$

Or $xz + xt + zy \in I_k$ et

$$yt \in I_m \cap J = \bigcap_{1 \leq l \leq n l \neq k} I_l$$

ce qui achève la preuve.

Soit A un anneau commutatif (cf. II.1.2,) $f_B : A \to B$ une A-algèbre commutative (cf. II.2.1e)t $I_1, \ldots, I_n$ une suite d'idéaux propres de B (cf. II.5.6.)

II.8.3 . −Notations

Pour tout $1 \leq k \leq n$ on note

$$\pi_k : B \to B/I_k \qquad \text{II.8.3.1}$$

la surjection canonique (cf. II.5.11.)

On définit une application :

$$\begin{array}{rcl} \pi := \pi_1 \times \ldots \times \pi_n \quad B & \to & \prod_{k=1}^{n} B/I_k \\ b & \mapsto & (\pi_1(b), \ldots, \pi_n(b)) \, , \end{array} \qquad \text{II.8.3.2}$$

(cf. II.7.3.)

Théorème II.8.4 (Théorème des restes chinois) *i) L'application π définie ci-dessus est un morphisme de A-algèbres.*

ii) Le noyau de π est l'idéal

$$\operatorname{Ker} \pi \; = \; \bigcap_{k=1}^{n} I_k \; \subset \; B$$

(cf. II.7.5.i).)

iii) Si les idéaux I_k ,$1 \leq k \leq n$, sont deux à deux comaximaux (cf. II.8.1,) le morphisme π est un épimorphisme (surjectif) ; il existe donc un unique isomorphisme de A-algèbres

$$\phi : B/\bigcap_{k=1}^{n} I_k \; \to \; \prod_{k=1}^{n} B/I_k$$

tel que

$$\phi \circ \psi \; = \; \pi \, ,$$

où $\psi \; : \; B \; \to \; B/\bigcap_{k=1}^{n} I_k$ est la surjection canonique.

Preuve *:*

i) Pour tout $(a, b) \in B \times B$,

$$\begin{array}{lll} \pi(a +_B b) & \overset{=}{\text{(cf. II.8.3.2,)}} & (\pi_1(a +_B b), \ldots, \pi_n(a +_B b)) \\ & \overset{=}{\pi_k \text{ est un morphisme}} & (\pi_1(a) +_{B/I_1} \pi_1(b), \ldots, \pi_n(a) +_{B/I_n} \pi_n(b)) \\ & \overset{=}{\text{(cf. II.7.2.1,)}} & (\pi_1(a), \ldots, \pi_n(a)) +_{\prod_{k=1}^{n} B/I_k} (\pi_1(b), \ldots, \pi_n(b)) \\ & = & \pi(a) +_{\prod_{k=1}^{n} B/I_k} \pi(b) \end{array}$$

ce qui prouve que π satisfait l'axiome ANN$_6$ de la définition II.1.9.

Par ailleurs,

$$\begin{array}{rll} \pi(1_B) & \overset{=}{\text{(cf. II.8.3.2,)}} & (\pi_1(1_B),\dots,\pi_n(1_B)) \\ & \overset{=}{\text{(cf. II.5.11,)}} & (1_{B/I_1},\dots,1_{B/I_n}) \\ & \overset{=}{\text{(cf. II.7.2.4,)}} & 1_{\prod_{k=1}^{n} B/I_k} \end{array}$$

c'est-à-dire que π satisfait l'axiome ANN$_7$ de la définition II.1.9.

De plus, pour tout $(a,b)\in B\times B$,

$$\begin{array}{rll} \pi(a *_B b) & \overset{=}{\text{(cf. II.8.3.2,)}} & (\pi_1(a *_B b),\dots,\pi_n(a *_B b)) \\ & \overset{=}{\pi_k \text{ est un morphisme}} & (\pi_1(a) *_{B/I_1} \pi_1(b),\dots,\pi_n(a) *_{B/I_n} \pi_n(b)) \\ & \overset{=}{\text{(cf. II.7.2.3,)}} & (\pi_1(a),\dots,\pi_n(a)) *_{\prod_{k=1}^{n} B/I_k} (\pi_1(b),\dots,\pi_n(b)) \\ & = & \pi(a) *_{\prod_{k=1}^{n} B/I_k} \pi(b) \end{array}$$

c'est-à-dire que π satisfait l'axiome ANN$_8$ de la définition II.1.9.

À ce point, π est un morphisme d'anneaux. Notons f_k le morphisme structural de B/I_k. Par définition de la structure quotient (cf. II.5.11,) $f_k = \pi_k\circ f_B$. Dès lors, pour tout $a\in A$, on a :

$$\begin{array}{rll} \pi(f_B(a)) & \overset{=}{\text{(cf. II.8.3.2,)}} & (\pi_1(f_B(a)),\dots,\pi_n(f_B(a))) \\ & = & (f_1(a),\dots,f_n(a)) \\ & \overset{=}{\text{(cf. II.7.2.5,)}} & f_{\prod_{k=1}^{n} B/I_k}(a)\,, \end{array}$$

(si $f_{\prod_{k=1}^{n} B/I_k}$ désigne le morphisme structural de $\prod_{k=1}^{n} B/I_k$) c'est-à-dire que

$$\pi \circ f_B = f_{\prod_{k=1}^{n} B/I_k}$$

qui était la dernière vérification à effectuer pour montrer que π est un morphisme de A-algèbres (cf. II.2.2.)

ii) Soit $b \in B$, *tel que*

$$\begin{array}{rrcl} & \pi(b) & = & 0_{\prod_{k=1}^{n} B/I_k} \\ \text{(cf. II.7.2.2,)} \overset{\Leftrightarrow}{} & \pi(b) & = & (0_{B/I_1}, \ldots, 0_{B/I_n}) \\ \text{(cf. II.8.3.2,)} \overset{\Leftrightarrow}{} & \pi_k(b) & = & 0_{B/I_k} \, \forall \, 1 \leq k \leq n \\ \Leftrightarrow & b & \in & I_k \, \forall \, 1 \leq k \leq n \end{array}$$

c'est-à-dire

$$\operatorname{Ker} \pi = \bigcap_{i=1}^{n} I_k \, .$$

iii) Montrons la surjectivité du morphisme π *sous les hypothèses de comaximalité. Pour tout* $1 \leq k \leq n$ *et tout* $1 \leq l \leq n \, k \neq l$, *il existe* $x_l \in I_k$ *et* $y_l \in I_l$ *tels que* $x_l + y_l = 1_B$ *(cf. II.8.1.) En effet, dire que* I_k *et* I_l *sont comaximaux signifie que* $B = I_k + I_l$, *autrement dit que tout élément de* B *s'écrit comme somme d'un élément de* I_k *et d'un élément de* I_l ; *ce qui est en particulier vrai pour* 1_B. *Posons* $e_{kl} := y_l$. *Alors* e_{kl} *est un élément de* B *vérifiant :*

$$\begin{array}{rcl} \pi_k(e_{kl}) & = & 1_{B/I_k} \\ \pi_l(e_{kl}) & = & 0_{B/I_l} \, . \end{array}$$

Posons encore

$$e_k := \prod_{l \neq k} e_{kl} \, ,$$

le produit dans B *de tous les* e_{kl} *pour* $l \neq k$. *Comme* π_j *pour tout* $1 \leq j \leq n$ *est un morphisme d'anneaux (cf. II.5.11,)*

$$\begin{array}{rcl} \pi_k(e_k) & = & \pi_k(\prod_{l \neq k} e_{kl}) \\ & = & \prod_{l \neq k} \pi_k(e_{kl}) \\ & = & 1_{B/I_k} \, ; \end{array}$$

ce qui signifie que e_k *congrue à* 1 *modulo* I_k.

Pour tout $l \neq k$

$$\begin{array}{rcl} \pi_l(e_k) & = & \pi_l(\prod_{j \neq k} e_{kj}) \\ & = & \prod j \neq k \pi_l(e_{kj}) \\ & = & \pi_l(e_{kl}). \prod_{j \neq k, \; j \neq l} \pi_l(e_{kj}) \\ & = & 0_{B/I_l} \, ; \end{array}$$

ce qui signifie que e_k *congrue à* 0 *modulo* I_l *pour tout* $l \neq k$.

Remarque iii).1 On pourrait construire e_k directement, sans la construction intermédiaire de e_{kl} en utilisant la proposition II.8.2.

Étant donné un élément

$$(\beta_1, \ldots, \beta_n) \in \prod_{k=1}^{n} B/I_k \ ,$$

pour tout $1 \leq k \leq n$ *il existe* $b_k \in B$ *tel que* $\pi_k(b_k) = \beta_k$, *puisque* $\pi_k : B \to B/I_k$ *est surjectif. Posons*

$$b := \sum_{k=1}^{n} b_k * e_k \ .$$

Pour tout $1 \leq k \leq n$

$$\begin{aligned} \pi_k(b) &= \pi_k(\sum_{l=1}^{n} b_l *_B e_l) \\ &= \sum_{l=1}^{n} \pi_k(b_l) *_{B/I_k} \pi_k(e_l) \\ &= \pi_k(b_k) *_{B/I_k} \pi_k(e_k) \\ &= \beta_k *_{B/I_k} 1_{B/I_k} \\ &= \beta_k \ . \end{aligned}$$

Par définition de l'application π, *(cf. II.8.3.2,)*

$$\begin{aligned} \pi(b) &= (\pi_1(b), \ldots, \pi_n(b)) \\ &= (\beta_1, \ldots, \beta_n) \ . \end{aligned}$$

Il s'ensuit que l'élément b *de* B *ainsi construit est un antécédent pour* $(\beta_1, \beta_2, \ldots, \beta_n)$ *par* π *et donc que* π *est surjectif.*

L'existence de ϕ *et la formule* $\phi \circ \psi = \pi$ *sont des conséquences immédiates de ce qui précède et du corollaire II.6.4.*

III . −Arithmétique

Dans toute cette section, A est un anneau commutatif. (cf. II.1.2.)
Les A-algèbres considérées sont commutatives (cf. II.2.1) (sauf mention du contraire.)

III.1 . −Idéaux et divisibilité

Remarque III.1.1 Étant donnée une A-algèbre commutative B (cf. II.2.1q)ui n'est pas un corps (cf. II.1.5,) pour deux éléments b et c de B, non nuls, il n'existe pas forcément un élément $x \in B$ tel que $b = c *_B x$ ou $c = b *_B x$. Ceci conduit naturellement à donner une définition lorsqu'on est dans cette situation.

Définition III.1.2 (Divisibilité) Étant donnés deux éléments b et c d'une A-algèbre commutative B, on dit que b *divise* c (ou que b est un *diviseur* de c) (ou encore que c est un *multiple* de b) et l'on note $b|c$ s'il existe un élément $x \in B$ tel que $c = b *_B x$.

Remarque III.1.3 i) On remarque immédiatement que la relation de divisibilité sur une A-algèbre B est une relation binaire (cf. 0.7q)ui vérifie :

— pour tout $b \in B$, $b|b$, en effet, $b = 1_B *_B b$, *réflexivité* ;

— pour tout triplet (b, c, d) d'éléments de B,

$$\begin{array}{rrcl} & b|c & \text{et} & c|d \\ \Rightarrow & \exists (x,y) \in B \times B & | & c = b *_B x \text{ et } d = c *_B y \\ \Rightarrow & d & = & b *_B x *_B y \\ \Rightarrow & b & | & d \, , \end{array}$$

transitivité ;

— pour tout couple (b, c) d'éléments de B,

$$\begin{array}{rrcl} & b|c & \text{et} & c|b \\ \Rightarrow & \exists (x,y) \in B \times B & | & c = b *_B x \text{ et } b = c *_B y \\ \Rightarrow & b *_B (1_B - x *_B y) & = & 0_B \, . \end{array}$$

On ne peut rien conclure de cette dernière identité sans hypothèses sur l'algèbre B et l'on sera rapidement amené à introduire la notion d'algèbre *intègre* (cf. III.2.1.)

ii) On remarque que, un élément $b \in B$ étant fixé, l'ensemble

$$(b) := \{c \in B \mid b|c\}$$

est un sous-B-module de B (cf. II.4.4*i.e.*)(b) est non vide (cf. i)e)t pour tout couple (c, d) d'éléments de (b) et tout couple (γ, δ) d'éléments de B, $\gamma *_B c +_B \delta *_B d \in (b)$, (cf. II.4.6.b),) c'est-à-dire que (b) est l'*idéal* de B engendré par $\{b\}$ (cf. II.5.6,) (cf. II.7.9.)

Définition III.1.4 Étant donnée une A-algèbre commutative B, un idéal (b) engendré par un élément $b \in B$, est dit *principal*. On dit que b est un *générateur* de (b) . On note parfois $b *_B B$
$:= (b)$ ou parfois même $b = (b)$.

Remarque III.1.5 Dans un anneau quelconque, tous les idéaux ne sont en général pas principaux. Par exemple, dans l'anneau $K[X, Y]$ des polynômes à deux indéterminées sur un corps K l'ensemble des polynômes dont le terme constant est nul forme un idéal pour lequel on ne peut trouver un unique générateur. On s'apercevra qu'il est engendré par la paire $\{X; Y\}$. Néanmoins dans nombre des anneaux que nous serons amenés à considérer, les idéaux sont tous principaux. Le défaut de cette propriété n'a été constaté que par les arithméticiens du XIX$^{\text{ième}}$ siècle et son ignorance a pu, auparavant, conduire à des erreurs et selon toute vraisemblance, celle de FERMAT notamment.

Proposition III.1.6 *Étant donné un élément b d'une A-algèbre commutative B, l'idéal principal (b) est égal à B si et seulement si b est inversible (une unité.)*

Preuve *: La démonstration de cette proposition est un exercice très facile.*

Proposition III.1.7 *Étant donné un couple (b, c) d'éléments de B les assertions suivantes sont équivalentes :*

a) *b divise c ;*

b) $c \in (b)$;

c) $(c) \subset (b)$.

Preuve *: La démonstration de cette proposition est laissée en exercice.*

Définition III.1.8 Étant donnée une A-algèbre commutative B,

i) un idéal I de B est *premier* si
— $I \neq B$
— pour tout couple (b, c) d'éléments de B, si $b * c \in I$, alors $b \in I$ ou $c \in I$.

ii) (**Éléments premiers**)
un élément $p \in B$ est *premier* si
— $p \neq 0$
— l'idéal principal (p) (cf. III.1.4e)st premier, ce qui signifie, de manière quasi-immédiate, que pour tout couple (b, c) d'éléments de B, si $p|b * c$ alors $p|b$ ou $p|c$.
On notera usuellement $\mathcal{P}(B)$ l'ensemble des éléments premiers de B .

Définition III.1.9 Dans une A-algèbre commutative B on dit qu'un idéal M est *maximal* s'il est

— différent de B

— et maximal pour la relation d'inclusion, c'est-à-dire que tout idéal contenant strictement M est égal à B .

III.2 . −Algèbres intègres, éléments associés et idéaux principaux

Définition III.2.1 Une A-algèbre commutative B (cf. II.2.1e)st *intègre* si pour tout couple (b, c) d'éléments de B, $b * c = 0_B$ implique $b = 0_B$ ou $c = 0_B$. Ceci revient à dire que l'idéal principal (0_B) (cf. III.1.4e)st premier (cf. III.1.8.i).)

On ne dira cependant pas que 0_B est premier en tant qu'élément (cf. III.1.8.ii)p)uisque, par définition, un élément premier est non nul.

Un anneau est dit intègre si c'est une $\mathbb{Z}$-algèbre intègre (cf. II.2.8.)

Exemple III.2.2 Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont intègres ; plus généralement, un corps (cf. II.1.5e)st un anneau intègre même si bien sûr tous les anneaux intègres ne sont pas des corps ($\mathbb{Z}$ par exemple.)

Remarque III.2.3 Si B est une A-algèbre intègre, on peut préciser le troisième point de la remarque III.1.3.i).

En effet, pour tout couple (b, c) d'éléments de B, tel que $b|c$ et $c|b$, il existe un couple (x, y) d'éléments de B tel que

$$\begin{aligned} c &= b * x \\ b &= c * y \\ b * (1 - x * y) &= 0 . \end{aligned}$$

Si $b = 0$, alors $c = 0$ sinon $1 - x * y = 0$ c'est-à-dire que x et y sont inversibles et inverses l'un de l'autre (cf. II.1.4.)

On constate donc que la relation de divisibilité n'est pas antisymétrique mais que :

Proposition III.2.4 *Pour tout couple d'éléments (b, c) d'une A-algèbre intègre B, $b|c$ et $c|b$ si et seulement s'il existe une unité $u \in B^\times$ telle que $c = b *_B u$.*

Définition III.2.5 Dans la situation de la proposition III.2.4 on dit que les éléments b et c sont *associés*.

Remarque III.2.6 i) La relation "être associés" est une relation d'équivalence sur B . Comme l'égalité est "remplacée" dans l'axiome d'antisymétrie (cf. 0.10.i)p)ar une relation d'équivalence, pour la divisibilité, on dira simplement que c'est un *pré-ordre* sur B .

ii) On constate, grâce à la remarque III.1.3.ii) que l'ensemble des classes d'équivalence pour la relation d'association est en bijection avec l'ensemble des idéaux *principaux* de B et que la relation de divisibilité correspond à l'inclusion sur l'ensemble des idéaux principaux (cf. III.1.7.) Cette dernière est une relation d'ordre (cf. 0.10.i) ;) ce qui illustre un fait plus général à savoir qu'un pré-ordre relativement à une relation d'équivalence induit une relation d'ordre sur le quotient par cette relation d'équivalence.

On peut formaliser ces résultats dans la proposition suivante :

Proposition III.2.7 *Étant donnés un couple (b, c) d'éléments d'une A-algèbre intègre B, les assertions suivantes sont équivalentes :*

a) $b|c$ *et* $c|b$;

b) $c \in (b)$ *et* $b \in (c)$;

c) $(b) = (c)$;

d) b *et* c *sont associés.*

Preuve *: Cette proposition n'est qu'une reformulation des résultats précédents.*

Corollaire III.2.8 *Dans une A-algèbre intègre B, l'ensemble des idéaux principaux est en bijection avec l'ensemble des classes d'association.*

Preuve *: Ce corrolaire n'exprime en fait que l'équivalence entre les points III.2.7.c) et III.2.7.d).*

Remarque III.2.9 Bien que la relation de divisibilité ne soit pas une relation d'ordre, on pourrait toutefois parler de plus petit (resp. de plus grand) élément au sens de la divisibilité d'une partie E d'une A-algèbre B avec le défaut d'unicité qu'implique le défaut d'égalité dans l'antisymétrie.

Si m et m' sont deux plus petits éléments de E, on peut simplement dire que $m|m'$ et que $m'|m$, ce qui implique, d'après la proposition ci-dessus, qu'il existe une unité u de B telle que $m' = u * m$ (m et m' sont associés.)

On se satisfait pourtant de ce défaut d'unicité pour donner les définitions suivantes :

Définition III.2.10 (Pgcd Ppcm) Pour tout couple (b, c) d'éléments d'une A-algèbre B intègre, on appelle *plus grand commun diviseur ou PGCD des éléments b et c* et l'on note $b \wedge c$ (resp.*plus petit commun multiple ou **Ppcm** des éléments b et c* et l'on note $[b, c]$) le plus grand (resp. le plus petit) au sens de la divisibilité parmi les diviseurs (resp. multiples) communs de b et c .

Remarque III.2.11 i) Il faut remarquer qu'avec ce degré de généralité, la définition ci-dessus n'implique absolument pas l'existence de **Ppcm** et de PGCD et encore moins leur unicité. On se rapportera au paragraphe consacré aux anneaux factoriels (cf. III.3p)our des conditions d'existence du **Ppcm** et du PGCD.

ii) L'unicité ne peut en général être assurée que par des conditions ad hoc. Pour les entiers 4 et 6 de $\mathbb{Z}$, les entiers 12 et -12 répondent à la définition de **Ppcm** donnée ci-dessus. On peut privilégier 12 en spécifiant que le **Ppcm** doit être positif. De même il est clair que les éléments $(X-1)$ et $2004*(X-1)$ correspondent à la définition de PGCD des éléments $(X-3)*(X-1)$ et $(X-1)^2$ dans $\mathbb{Q}[X]$ et que l'on peut privilégier $(X-1)$ en spécifiant que le PGCD doit être unitaire dans $\mathbb{Q}[X]$.

En revanche la classe d'association du PGCD (resp. du PPCM) est unique.

iii) Étant donné un couple (b,c) d'éléments d'une A-algèbre intègre B, on pourrait remarquer, grâce à la remarque III.2.6.ii), que le PGCD (resp. le PPCM) de b et c est le générateur du plus petit (resp. plus grand) idéal principal contenant (resp. contenu dans) (b) et (c) . Outre que l'existence de tels idéaux n'est pas établie en toute généralité (dans ce cours), le plus grand (resp. le plus petit) idéal vérifiant une propriété donnée n'est pas nécessairement principal. Cette remarque qui est l'ingrédient essentiel du théorème de BÉZOUT (cf. III.4.14p)rend réellement tout son sens dans le cadre des anneaux *principaux* (cf. III.4.)

Proposition III.2.12 *Étant donnée une A-algèbre B, un idéal propre J de B est premier, (resp. maximal) si et seulement si l'algèbre quotient B/J (cf. II.5.11,) est une A-algèbre intègre (resp. un corps (cf. II.1.5.))*

Preuve : *Notons $\pi : B \to B/J$ la surjection canonique qui est un morphisme d'algèbres, d'après la définition II.5.11.*

- *L'algèbre B/J est intègre si et seulement si pour tout $(\xi,\eta) \in B/J \times B/J$, $\xi *_{B/J} \eta = 0_{B/J}$ implique $\xi = 0_{B/J}$ ou $\eta = 0_{B/J}$*

$$
\begin{array}{lcl}
 & \Leftrightarrow & \\
\forall (x,y) \in \pi^{-1}(\xi)\times\pi^{-1}(\eta),\ \pi(x)*_{B/J}\pi(y) = 0_{B/J} & \Rightarrow & \pi(x) = 0_{B/J} \text{ ou } \pi(y) = 0_{B/J} \\
 & \Leftrightarrow & \\
\forall (x,y) \in \pi^{-1}(\xi)\times\pi^{-1}(\eta),\ \pi(x)*_{B/J}\pi(y) = 0_{B/J} & \Rightarrow & x \in \operatorname{Ker}\pi \text{ ou } y \in \operatorname{Ker}\pi \\
 & \Leftrightarrow & \\
\forall (x,y) \in \pi^{-1}(\xi)\times\pi^{-1}(\eta),\ \pi(x*_B y) = 0_{B/J} & \Rightarrow & x \in \operatorname{Ker}\pi \text{ ou } y \in \operatorname{Ker}\pi \\
 & \Leftrightarrow & \\
 & \pi \text{ est surjective} & \\
\forall (x,y) \in B\times B,\ \pi(x*_B y) = 0_{B/J} & \Rightarrow & x \in \operatorname{Ker}\pi \text{ ou } y \in \operatorname{Ker}\pi \\
 & \Leftrightarrow & \\
 & \text{(cf. II.6.1,)} & \\
\forall (x,y) \in B\times B,\ x*_B y \in J & \Rightarrow & x \in J \text{ ou } y \in J
\end{array}
$$

  c'est-à-dire précisément, que J est un idéal premier.

- *L'algèbre B/J est un corps, si et seulement si pour tout $\xi \in B/J$ et $\xi \neq 0_{B/J}$, il existe $\xi' \in B/J$ tel que $\xi *_{B/J} \xi' = 1_{B/J}$ c'est-à-dire, pour tout $\xi \in B/J \setminus \{0_{B/J}\}$,*

et tout $x \in \pi^{-1}(\xi)$ *il existe* $x' \in B \setminus J$ *tel que* $\pi(x) *_{B/J} \pi(x') = 1_{B/J}$. *Comme* π *est surjective, ceci équivaut à : pour tout* $x \in B \setminus J$, *il existe* $x' \in B \setminus J$ *tel que*

$$\pi(x *_B x') = \pi(x) *_{B/J} \pi(x') = 1_{B/J} .$$

C'est-à-dire, d'après le corollaire II.6.1, pour tout $x \in B \setminus J$, *il existe* $x' \in B \setminus J$ *tel que*

$$x *_B x' \in 1_B + J . \qquad \text{III.2.12.1}$$

- *Soit* K *un idéal de* B *contenant strictement* J. *Supposons que III.2.12.1 est vérifiée. Comme* $K \neq J$, *il existe* $x \in K$, $x \notin J$. *Donc il existe* $x' \in B \setminus J$, *tel que* $x *_B x' \in 1 + J$. *C'est-à-dire qu'il existe* $j \in J$, *tel que* $x *_B x' = 1 + j$ *i.e.*$1 = x * x' - j$. *Or* $x \in K$ *implique* $x' * x \in K$ *car* K *est un idéal.* $j \in J \subset K$ *implique* $j \in K$. *D'où*

$$1_B = x *' x - j \in K .$$

Ce qui implique que $K = B$; *c'est-à-dire que* J *est maximal.*

- *Réciproquement, supposons que* J *est un idéal maximal. Alors pour tout* $x \notin J$ *l'idéal engendré par* $\{x\} \cup J$ *contient* J *est est différent de* J. *Il est donc égal à* B. *C'est-à-dire que* 1_B *appartient à cet idéal ; autrement dit qu'il existe* $(y, z) \in B \times J$, *tel que*

$$1_B = x * y + z ;$$

i.e.

$$x * z = 1_B - y \in 1_B + J ;$$

ce qui permet de conclure que B/J *est un corps d'après III.2.12.1.*

Corollaire III.2.13 *Tout idéal maximal est premier.*

Preuve : *Découle immédiatement de la proposition III.2.12 et de l'exemple III.2.2.*

III.3 . −Éléments irréductibles, anneaux factoriels, lemme de GAUSS

Dans toute cette section, A est un anneau commutatif. (cf. II.1.2.)
Les A-algèbres considérées sont commutatives (cf. II.2.1) (sauf mention du contraire.)

Définition III.3.1 Un élément non inversible b d'une A-algèbre commutative B, (cf. II.1.4,)est *irréductible* si pour tout couple $(c, d) \in B \times B$, tel que $c * d = b$, c est inversible ou d est inversible ; ce qui signifie, de manière équivalente, que tous ses diviseurs sont associés.

Proposition III.3.2 *Soit* B *une* A*-algèbre commutative intègre (cf. III.2.1 :)*

i) Tout élément premier p *(cf. III.1.8.ii)d)e* B *est irréductible.*

ii) Étant donné un élément $q \in B$, si l'idéal principal (q) engendré par q (cf. III.1.4e)st maximal alors q est irréductible.

***Preuve** :*

i) Soit $p \in B$ un élément premier. Pour tout $(a,b) \in B \times B$, tel que $ab = p$, i.e.$p \in (a)$ et $p \in (b)$ i.e.

$$(p) \subset (a) \text{ et } (p) \subset (b)\ . \qquad 1$$

Comme p est premier (cf. III.1.8.i),)

$$\begin{array}{lrcl} & ab & \in & (p) \\ \Rightarrow & a \in (p) & \text{ou} & b \in (p) \\ \overset{\Rightarrow}{\text{(cf. 1,)}} & (a) = (p) & \text{ou} & (b) = (p) \\ \overset{\Rightarrow}{\text{(cf. III.2.7.d),)}} & \exists u \in B^\times & | & p = au \text{ ou } p = bu \\ \Rightarrow & \exists u \in B^\times & | & ab = au \text{ ou } ab = bu \\ \Rightarrow & \exists u \in B^\times & | & a(b-u) = 0 \text{ ou } b(a-u) = 0\ . \end{array} \qquad 2$$

Comme ni a ni b n'est nul, puisque p n'est pas nul, il résulte de 2 et du fait que B est intègre que $a = u$ ou $b = u$.

ii) Soit $q \in B$ tel que (q) soit maximal. Soient b et c des éléments de B tels que $b * c = q$. Il s'ensuit que $b|q$ et $c|q$ ou encore, d'après III.1.7.c), que $(q) \subset (b)$ et $(q) \subset (c)$.

Or (q) est maximal, par hypothèse. Il en résulte donc que (cf. III.1.9,)

i) soit $(b) = (q)$ et dans ce cas, b et q sont associés (cf. III.2.7.d)c)'est-à-dire qu'il existe $u \in B^\times$ tel que $q = b * u$. Il en résulte par intégralité de l'anneau B que $c = u$.

ii) Soit $(b) = B$ et dans ce cas b est inversible d'après III.1.6.

Remarque III.3.3 La réciproque d'aucune des deux assertions de la proposition III.3.2 n'est en général vraie sans hypothèses supplémentaires.

Il existe des éléments irréductibles qui ne sont pas premiers.

Il existe des éléments irréductibles tels que l'idéal principal qu'il engendrent n'est pas maximal. Dans l'anneau $\mathbb{R}[X,Y]$ des polynômes à deux indéterminées sur $\mathbb{R}$, l'idéal (X) est constitué des polynômes qui s'annulent sur l'axe des ordonnées. Il est clair que X est irréductible. Or (X) est contenu dans l'ensemble des polynômes qui s'annulent à l'origine $(0,0)$. Il n'est pas difficile de voir que ce dernier n'est ni (X) ni $\mathbb{R}[X,Y]$ tout entier. On remarque également que c'est l'idéal engendré par la paire $\{X;Y\}$.

Définition III.3.4 Soit B une A-algèbre commutative.

i) Pour un élément $a \in B$ on appelle *décomposition en produit de facteurs premiers (resp. irréductibles) de* a un ensemble p_i ,$1 \leq i \leq n$ d'éléments premiers (cf. III.1.8.ii)) (resp. irréductibles) de B tels qu'il existe un élément $u \in B^\times$ inversible tel que

$$a = u *_B \prod_{i=1}^{n} p_i \, .$$

ii) Pour un élément $a \in B$, on dit que deux décompositions p_i ,$1 \leq i \leq n$ et q_i ,$1 \leq i \leq m$ sont *équivalentes* si

- $n = m$,
- il existe une permutation $\sigma \in S_n$ (cf. I.4.1)
- il existe un n-uplet u_i ,$1 \leq i \leq n$ d'éléments inversibles de B tels que pour tout $1 \leq i \leq n$ $p_i = u_i q_{\sigma(i)}$.

Proposition III.3.5 *Étant donnée une A-algèbre intègre B, les trois assertions suivantes sont équivalentes :*

a) Pour tout élément $a \in B$, il existe une unique classe de décomposition de a en produit de facteurs premiers.

b) Pour tout élément $a \in B$, il existe une unique classe de décomposition de a en produit de facteurs premiers.

c) Pour tout $a \in B$, il existe une unique classe de décomposition de a en produit de facteurs irréductibles.

***Preuve** :*

a) $\Rightarrow$ b) Supposons qu'il existe deux telles classes :

$$a = u_1 * \prod_{i=1}^{n_1} p_{i,1}$$
$$a = u_2 * \prod_{i=1}^{n_2} p_{i,2} \, .$$

On a alors

$$u_1 * \prod_{i=1}^{n_1} p_{i,1} = u_2 * \prod_{i=1}^{n_2} p_{i,2}$$

et du fait que B est intègre, on peut supposer, quitte à changer de notations que

$$\prod_{i=1}^{m_1} p_{i,1} \;=\; u * \prod_{i=1}^{m_2} p_{i,2}\ ,\ u \in B^{\times} \qquad \textit{III.3.5.1}$$

où H : les ensembles $P_1 \;:=\; \{p_{i,1}\ ,1 \leq i \leq m_1\}$ et $P_2 \;:=\; \{p_{i,2}\ ,1 \leq i \leq m_2\}$ sont disjoints. On peut, en effet, "simplifier" par les facteurs communs aux deux décompositions.

Il résulte de l'égalité III.3.5.1 que $p_{1,1}$ divise $u * \prod_{i=1}^{m_2} p_{i,2}$, c'est-à-dire, comme $p_{1,1}$ est premier (cf. III.1.8.i),) que $p_{1,1}$ divise l'un des $p_{i,2}$. Or, chacun des $p_{i,2}$ est premier par hypothèse et donc irréductible d'après le lemme III.3.2.i).

Si donc il existe i_0 tel que $p_{1,1}|p_{i_0,2}$ i.e.s'il existe $q \in B$ tel que $p_{i_0,2} = q * p_{1,1}$, soit q est inversible, soit $p_{1,1}$ est inversible.

Or un élément premier n'est pas inversible (cf. III.1.8.i),) donc nécessairement q est inversible. Ceci signifie, quitte à remplacer l'unité u par $q * u$, que $p_{1,1} \in P_1 \cap P_2$ ce qui contredit l'hypothèse H.

b) $\Rightarrow$ c) Si l'on suppose b), satisfaite, il existe une décomposition unique de a en produit de facteurs premiers. Celle-ci est également une décomposition en produit de facteurs irréductibles d'après le lemme III.3.2.i).

Reste à prouver l'unicité de cette dernière. Or, si l'on suppose l'existence d'une autre décomposition en produit de facteurs irréductibles, on peut mener le même raisonnement qu'au point précédent en remarquant qu'on a utilisé le fait que les éléments de P_1 sont premiers, mais que les éléments de P_2 sont irréductibles.

c) $\Rightarrow$ a) est une conséquence du lemme de GAUSS *(cf. III.3.6.)*

Proposition III.3.6 (Lemme de GAUSS ou théorème fondamental de l'arithmétique) *Si B est une A-algèbre intègre satisfaisant la propriété III.3.5.c), si (a, b, c) est un triplet d'éléments de B vérifiant $a|bc$ et a est irréductible, alors $a|b$ ou $a|c$; autrement dit, un élément irréductible est premier.*

***Preuve** : Supposons que $ab|c$. Il existe donc $d \in B$ tel que $ad = bc$. Par ailleurs, comme B satisfait la propriété III.3.5.c), il existe des éléments irréductibles $b_i\ ,1\leq i\leq n_b$ (resp. $c_i\ ,1\leq i\leq n_c\ ,$) (resp. $d_i\ ,1\leq i\leq n_d\ ,$) et des éléments inversibles u_b (resp. u_c) (resp. u_d) de B tels que*

$$b \;=\; u_b \prod_{i=1}^{n_b} b_i$$

$$(\textit{resp.}\quad c \;=\; u_c \prod_{i=1}^{n_c} c_i,)$$

$$(\textit{resp.}\quad d \;=\; u_d \prod_{i=1}^{n_d} d_i.)$$

Il s'ensuit que

$$\begin{aligned} u_b * \prod_{i=1}^{n_b} b_i * u_c * \prod_{i=1}^{n_c} c_i &= b * c \\ &= a * d \\ &= a * u_d * \prod_{i=1}^{n_d} d_i \ . \end{aligned}$$

Il s'ensuit, du fait que l'élément $ad = bc$ *a une unique classe de décomposition en facteurs irréductibles, qu'il existe* $u \in B^\times$ *tel que* $a = ub_i$ *ou* $a = uc_j$ *pour un certain* $1 \leq i \leq n_b$ *ou* $1 \leq j \leq n_c$.

Définition III.3.7 i) Si B est une A-algèbre intègre satisfaisant l'une des trois propriétés équivalentes de la proposition III.3.5 on dit que B est une A-algèbre *factorielle.*

ii) Un *anneau factoriel* est une $\mathbb{Z}$-algèbre factorielle.

iii) On commettra très souvent l'abus de langage consistant à dire que, dans un anneau factoriel, la décomposition d'un élément en produit de facteurs premiers (ou irréductibles ce qui revient au même,) est *unique*.

Définition III.3.8 Soit B une A-algèbre factorielle. D'après ce qui précède, on a vu que tout élément non nul $b \in B$ possède une unique classe de décomposition en produit de facteurs premiers. On peut donc écrire

$$a = u * \prod_{p \in \mathcal{P}(B)} p^{v_p(a)}$$

avec $u \in B^\times$ et $\mathcal{P}(B)$ l'ensemble des éléments premiers de B (cf. III.1.8.i).)

Les $v_p(a)$ ne dépendent que de p et de a (c'est le sens de l'unicité de la décomposition,) et sont appelés *valuations p-adiques* de a .

Proposition III.3.9 *Si B est une A-algèbre factorielle, tout couple (b, c) d'éléments non nuls de B possède un* ***Ppcm*** *et un PGCD (cf. III.2.10.)*

Preuve *: La démonstration de cette propriété est laissée en exercice.*

Lemme III.3.10 *Étant donnés deux éléments non nuls b et c d'une A-algèbre factorielle B, pour tout PGCD d et tout* ***Ppcm*** *m de b et c, il existe une unité $u \in B^\times$ telle que $b * c = u * d * m$.*

Preuve *: La démonstration de ce lemme est laissée en exercice.*

Proposition III.3.11 *Étant donnée une A-algèbre factorielle B, pour deux éléments non nuls b et c de B, les assertions suivantes sont équivalentes :*

a) La classe d'association de leur PGCD (cf. III.2.11.ii)e)st le groupe des unités $B^\times$.

b) Tout diviseur commun de b et c est une unité.

c) Les décompositions respectives de b et c n'ont aucun élément en commun.

*d) Pour tout **Ppcm** m de b et c, il existe une unité $u \in B^\times$ telle que $b * c = u * m$.*

***Preuve** :*

a) $\Rightarrow$ b) Si δ est un diviseur commun de b et c par unicité de la décomposition en produit de facteurs premiers, les facteurs de la décomposition de δ sont des éléments soit de celle de b soit de celle de c.

b) $\Rightarrow$ c) est immédiat puisque le PGCD est en particulier un diviseur commun à b et c .

c) $\Rightarrow$ d) est une conséquence immédiate du lemme III.3.10.

d) $\Rightarrow$ a) est laissée en exercice.

Définition III.3.12 Dans une A-algèbre factorielle B, on dit que deux éléments a et b sont *premiers entre eux* s'ils vérifient l'une des assertions équivalentes de la proposition III.3.11.

III.4 . −Anneaux principaux, théorème de BÉZOUT

Dans toute cette section, A est un anneau commutatif. (cf. II.1.2.)
Les A-algèbres considérées sont commutatives (cf. II.2.1) (sauf mention du contraire.)

Définition III.4.1 (Anneau principal) Une A-algèbre B intègre (cf. III.2.1e)st *principale* si tous ses idéaux sont principaux (cf. III.1.4.) Un anneau est *principal* si c'est une $\mathbb{Z}$-algèbre principale.

III.4.2 . −Exemples fondamental

L'anneau $\mathbb{Z}$ est principal. En effet, étant donné un idéal I de $\mathbb{Z}$, c'est-à-dire un sous-$\mathbb{Z}$-module de $\mathbb{Z}$ (cf. II.5.6c)'est-à-dire encore grâce aux propositions II.3.9.i) et II.3.9.ii) un sous-groupe de $\mathbb{Z}$, on a vu en I.1.20, que tout sous-groupe de $\mathbb{Z}$ était de la forme $d\mathbb{Z}$ pour $d \in \mathbb{Z}$.

Proposition III.4.3 *Si B est une A-algèbre principale (cf. III.4.1,) toute suite croissante (au sens de l'inclusion) d'idéaux est stationnaire. On dit que B est un anneau noethérien.*

Preuve : *Soit $I_{n\ ,n\in\mathbb{N}} \subset B$ une suite croissante d'idéaux de B c'est-à-dire que pour tout $n \in \mathbb{N}$, $I_n \subset I_{n+1}$.*

Il faut prendre garde au fait qu'en général, une réunion d'idéaux, (et plus généralement de sous-modules) n'est pas un idéal (resp. un sous module.) Cependant, dans le cas d'une suite croissante,

$$I := \bigcup_{n\in\mathbb{N}} I_n$$

est un idéal. En effet, pour tout $(x, y) \in I \times I$ et tout $(a, b) \in B \times B$, il existe des entiers n_x et n_y tels que $x \in I_{n_x}$ et $y \in I_{n_y}$. On peut, sans perte de généralité, supposer que $n_x \leq n_y$ c'est-à-dire que $I_{n_x} \subset I_{n_y}$ et donc x et y appartiennent à I_{n_y}. Ce dernier étant un idéal,

$$ax + by \in I_{n_y} \subset I\ .$$

Il s'ensuit que I est stable par combinaisons linéaires à coefficients dans B et évidemment non vide et donc que I est un idéal d'après la proposition II.4.6.b).

Comme B est principale, il existe $x_0 \in B$ tel que $I = x_0 * B$. Comme $x_0 \in I$, il existe n_0 tel que $x_0 \in I_{n_0}$.

Pour tout $n \geq n_0$, et tout $y \in I_n$, $y \in I$. Il existe donc $y_0 \in B$ tel que $y = x_0 * y_0$, c'est-à-dire que $y \in I_{n_0}$. Il en résulte donc que, pour tout $n \geq n_0$, $I_n \subset I_{n_0}$. Or, par hypothèse, pour tout $n \geq n_0$, $I_{n_0} \subset I_n$, c'est-à-dire, finalement, que pour tout $n \geq n_0$, $I_n = I_{n_0}$.

Corollaire III.4.4 *Si B est une A-algèbre principale, tout idéal de B est contenu dans un idéal maximal.*

Preuve : *Soit I un idéal de B. Si I n'est pas maximal, alors, il existe un idéal $I_1 \neq B$ contenant strictement $I_0 := I$. Par récurrence, on peut supposer construits des idéaux $I_{k\ ,0\leq k\leq n}$ tels que pour tout $0 \leq k \leq n-1$ $I_k \subset I_{k+1}$. Si I_n n'est pas maximal, on peut construire $I_{n+1} \neq B$ tel que I_{n+1} contient strictement I_n. Ainsi, de deux choses l'une : soit il existe $n \in \mathbb{N}$ tel que I_n est maximal et dans ce cas le corollaire est démontré, soit on a construit une suite strictement croissante d'idéaux $I_{n\ ,\ n\in\mathbb{N}}$ dans B. D'après la proposition précédente, cette suite est alors stationnaire ce qui est contradictoire.*

Remarque III.4.5 Ce résultat est en fait vrai dans un plus grand degré de généralité mais il faut, pour l'établir, utiliser le lemme de Zorn. Cependant nous n'appliquerons ce résultat qu'à $\mathbb{Z}$ ou $K[X]$ qui sont principaux.

Proposition III.4.6 *Si B est une A-algèbre principale (cf. III.4.1,) alors tout idéal premier de B différent de $\{0_B\}$ est maximal.*

Preuve : *Soit $\mathfrak{p}$ un idéal premier de B. Il existe, d'après le corollaire III.4.4, un idéal maximal $\mathfrak{m}$ contenant $\mathfrak{p}$. Or, B étant principale, $\mathfrak{m}$ (resp. $\mathfrak{p}$) est engendré par un élément $m \in B$ (resp. $p \in B$.) L'élément p appartient donc à $\mathfrak{m}$; c'est-à-dire qu'il existe $x \in B$ tel que $p = m *_B x$. Par conséquent, $m *_B x \in \mathfrak{p}$. Comme $\mathfrak{p}$ est premier, soit $m \in \mathfrak{p}$ et dans ce cas $\mathfrak{m} = \mathfrak{p}$ et le résultat est établi ; soit $x \in \mathfrak{p}$. Dans ce cas, il existe $y \in B$ tel que*

$$\begin{array}{rrcl} & x & = & p *_B y \\ \Rightarrow & m * x & = & m * p * y \\ \Rightarrow & p & = & m * p * y \\ \Rightarrow & p * (1 - m * y) & = & 0_B \ . \end{array}$$

Ceci implique, comme B est intègre, soit que $p = 0$, ce qui est contraire à l'hypothèse $\mathfrak{p} \neq \{0_B\}$, soit que $1 - my = 0_B$, c'est-à-dire que m est inversible dans B ce qui est alors contradictoire avec le fait que $\mathfrak{m}$ est un idéal maximal.

Remarque III.4.7 La proposition III.4.6 peut être vue comme une réciproque dans le cas des anneaux principaux du corollaire III.2.13.

Proposition III.4.8 *Soit B une A-algèbre principale (cf. III.4.1.) Pour tout élément irréductible $b \in B$, l'idéal principal (b) engendré par b est maximal, ce qui implique que b est premier. Autrement dit, dans une A-algèbre principale, le Lemme de* GAUSS *(cf. III.3.6e)st vérifié.*

Preuve : *L'idéal (b) est contenu dans un idéal maximal principal (m) d'après le corollaire III.4.4. Il s'ensuit donc que $b \in (m)$ i.e.il existe $x \in B$ tel que $b = m *_B x$. Comme b est irréductible (cf. III.3.1,) soit m soit x est inversible. Or m ne peut être inversible puisque (m) est un idéal maximal (cf. III.1.9,) c'est-à-dire que x est inversible ce qui implique, d'après la proposition III.2.7, que $(m) = (b)$.*

On en déduit que (b) est premier d'après le corollaire III.2.13 c'est-à-dire que b est premier.

Remarque III.4.9 La proposition III.3.6 et le fait qu'une A-algèbre principale est un anneau noethérien (cf. III.4.3s)uffiraient en fait à montrer qu'une telle algèbre est factorielle (cf. III.3.7.i)m)ais on va procéder de manière plus directe dans la proposition suivante :

Proposition III.4.10 *Si B est une A-algèbre principale (cf. III.4.1,) B est factorielle.*

Preuve : *Supposons que $a \in B$ ne soit pas premier.*

III.4.10.1. − Il existe un idéal maximal $\mathfrak{m}_1$ contenant (a) d'après le corollaire III.4.4. Comme B est principale, $\mathfrak{m}_1$ est engendré par un élément $m_1 \in B$, lequel est premier, d'après le corollaire III.2.13. Il existe donc $a_1 \in B$ tel que $a = m_1 * a_1$.

Supposons construite une suite de couples $(m_i, a_i)_{,1 \leq i \leq n} \in B \times B$, telle que m_i est premier et $a_{i-1} = m_i * a_i$.

α *Si a_n est également premier, on voit immédiatement que*

$$a \;=\; a_n * \prod_{i=1}^{n} m_i$$

est une décomposition de a en produit de facteurs premiers (cf. III.3.4.i).)

β *Sinon on peut construire un couple (m_{n+1}, a_{n+1}) tel que m_{n+1} soit premier et que $a_n \;=\; m_{n+1} * a_{n+1}$, d'après le procédé III.4.10.1.*
Or, par construction, pour tout i, $a_{i+1}|a_i$ i.e.$(a_i) \subset (a_{i+1})$. On construit donc une suite croissante d'idéaux de B. Grâce à la proposition III.4.3, cette suite est donc stationnaire, donc il existe un entier $n \in \mathbb{N}^*$ tel que $(a_n) \;=\; (a_{n+1})$. Ceci implique, grâce à la proposition III.2.7, qu'il existe une unité $u \in B^\times$ telle que $a_n \;=\; u * a_{n+1}$ c'est-à-dire

$$a_{n+1} * (m_{n+1} - u) \;=\; 0\,.$$

Comme B est intègre et $a_{n+1} \neq 0_B$, il s'ensuit que $m_{n+1} \;=\; u$ ce qui est contradictoire avec le fait que m_{n+1} est premier ; autrement dit, on ne peut pas itérer le procédé III.4.10.1 jusqu'au rang $n+1$, c'est-à-dire que a_n était déjà premier. On conclut donc en se rapportant au point α.

On a donc vérifié le critère III.3.5.a) qui définit une A-algèbre factorielle.

Corollaire III.4.11 *Dans une A-algèbre principale B deux éléments non nuls b et c admettent des PGCD et des PPCM.*

Preuve *: Ceci est une conséquence de la proposition III.3.9.*

Corollaire III.4.12 *Les anneaux $\mathbb{Z}$ et $K[X]$, pour K un corps (cf. IV.2,) sont factoriels.*

Remarque III.4.13 On retrouve, grâce au lemme de GAUSS (cf. III.3.6e)t à la proposition précédente, les deux définitions de *nombre premier* dans $\mathbb{Z}$ à savoir, soit un entier (différent de 1 et -1) uniquement divisible par $1, -1$ et lui-même autrement dit un élément irréductible de $\mathbb{Z}$; soit un entier p non nul qui s'il divise un produit ab divise l'un ou l'autre des deux facteurs c'est-à-dire un entier tel que l'idéal $(p) \;=\; p\mathbb{Z}$ est premier (cf. III.1.8.i).)

Théorème III.4.14 (Théorème de BÉZOUT) *Soient B une A-algèbre principale (cf. III.4.1e)t b et c deux éléments non nuls de B.*

i) Un PGCD de b et c (cf. III.2.10e)st un générateur du plus petit idéal contenant simultanément (b) et (c) égal à $(b) + (c)$ (cf. II.7.5.ii).)

ii) Si d est un PGCD de b et c il existe des éléments u et v de B tels que

$$d \;=\; bu \;+\; cv\,.$$

iii) Un ***Ppcm*** *de b et c (cf. III.2.10e)st un générateur du plus grand idéal simultanément contenu dans (b) et (c) égal à $(b) \cap (c)$ (cf. II.7.5.i).)*

Preuve *: On va en fait interpréter la remarque III.2.11.iii) dans le cas des anneaux principaux.*

i) Notons

$$D := \{d \in B \mid (d) = (b) + (c)\} .$$

Comme B est principale, D est bien entendu non vide et l'on peut remarquer, de plus, que tous ses éléments sont associés.

Pour tout diviseur commun e de b et c,

$$(b) \subset (e) \text{ et } (c) \subset (e)$$

(cf. III.1.7e)t, par conséquent, $(b) + (c) \subset (e)$, c'est-à-dire que, pour tout $d \in D$, $e|d$.

Les éléments de D sont donc tous des PGCD de b et c .

Réciproquement, pour tout PGCD d' de b et c, d' est en particulier un diviseur commun à b et c et divise donc tout élément $d \in D$, i.e.$(b) + (c) \subset (d')$. Par ailleurs, tout idéal I contenant simultanément (b) et (c), est de la forme (e) pour un certain élément $e \in B$ (puisque B est principale), c'est-à-dire que e est un diviseur commun de b et c. Par conséquent, $e|d'$ par maximalité du PGCD et (d') est donc le plus petit idéal contenant simultanément (b) et (c) c'est-à-dire que $d' \in D$.

ii) Il suffit d'écrire qu'un PGCD de b et c est un élément de $(b) + (c)$.

iii) Ce résultat s'obtient par un raisonnement analogue à celui de (i) et le détail est laissé en exercice.

Corollaire III.4.15 *Étant donnés une A-algèbre principale B et deux éléments non nuls b et c de B, les assertions suivantes sont équivalentes :*

a) Les éléments b et c sont premiers entre eux (cf. III.3.12.)

b) Les idéaux (b) et (c) sont comaximaux (cf. II.8.1.)

c) Pour tout unité $u \in B^\times$, il existe un couple (x, y) d'éléments de B tel que $u = bx + cy$.

d) Il existe un couple (x, y) d'éléments de B tel que $1_B = bx + cy$.

Preuve *: La démonstration de ce corollaire est laissée en exercice.*

IV . −Compléments : exemples d'anneaux

IV.1 . −Corps des fractions d'un anneau intègre

Soit A un anneau commutatif (cf. II.1.2i)ntègre (cf. III.2.1.)

IV.1.1. − On note

$$B \ := \ A \times (A \setminus \{0_A\}) \qquad \text{IV.1.1.1}$$

et on définit une relation $\sim$ sur B par

$$(\nu, \delta) \ \sim \ (\nu', \delta') \text{ si } \nu\delta' \ = \ \nu'\delta \ . \qquad \text{IV.1.1.2}$$

Lemme IV.1.2 *La relation $\sim$ est une relation d'équivalence.*

IV.1.3. − On définit des lois internes

$$\begin{array}{rccc} * : & B \times B & \to & B \\ & ((\nu, \delta), (\nu', \delta')) & \mapsto & (\nu\nu', \delta\delta') \end{array} \qquad \text{IV.1.3.1}$$

et

$$\begin{array}{rccc} + : & B \times B & \to & B \\ & ((\nu, \delta), (\nu', \delta)) & \mapsto & (\nu\delta' + \nu'\delta, \delta\delta') \ . \end{array} \qquad \text{IV.1.3.2}$$

Proposition IV.1.4 *i) Les lois $*$ et $+$ définies en IV.1.3.1 et IV.1.3.2 sont compatibles avec la relation d'équivalence $\sim$ (cf. IV.1.1.2s)ur B c'est-à-dire que si*

$$\begin{array}{rcl} (\nu_1, \delta_1) & \sim & (\nu'_1, \delta'_1) \\ & \text{et} & \\ (\nu_2, \delta_2) & \sim & (\nu'_2, \delta'_2) \ , \end{array}$$

alors

$$\begin{array}{rcl} (\nu_1, \delta_1) * (\nu_2, \delta_2) & \sim & (\nu'_1, \delta'_1) * (\nu'_2, \delta'_2) \\ & \text{et} & \\ (\nu_1, \delta_1) + (\nu_2, \delta_2) & \sim & (\nu'_1, \delta'_1) + (\nu'_2, \delta'_2) \ . \end{array}$$

Elle définissent donc des lois internes encore notées $*$ et $+$ sur

$$K \ := \ B/\sim \qquad 1$$

l'ensemble des classes d'équivalence de B selon $\sim$.

ii) Le triplet $(K, +, *)$ est un corps (cf. II.1.5.)

iii) L'application

$$\begin{array}{ccc} A & \to & B \\ a & \mapsto & (a, 1) \end{array}$$

donne une application $i : A \to K$, qui est un morphisme d'anneaux injectif. L'anneau A est donc une sous-A-algèbre de K (cf. II.2.5.)

iv) Le corps K est le plus petit corps contenant A au sens où, pour tout morphisme d'anneaux injectif $j : A \to L$, où L est un corps, il existe un unique morphisme d'anneaux $h : K \to L$ tel que $h \circ i = j$.

Définition IV.1.5 Étant donné un anneau commutatif intègre A, le corps K (cf. IV.1.4.i).1c)onstruit comme dans la proposition précédente, est appelé *corps des fractions de A*.

Usuellement, les éléments de K sont notés ν/δ ou $\frac{\nu}{\delta}$ pour $\nu \in A$, $\delta \in A \setminus \{0_A\}$ et (ν, δ) un représentant d'un élément de K.

Usuellement également, ν est appelé *numérateur* et δ *dénominateur*.

Remarque IV.1.6 Si $A = \mathbb{Z}$, le corps des fractions est le corps des nombres rationnels $\mathbb{Q}$.

IV.2 . −Algèbre des polynômes à une indéterminée

Dans toute cette section, A est un anneau commutatif (cf. II.1.2.)

Définition IV.2.1 i) On rappelle qu'une *suite à valeurs dans A* est une application $\mathbb{N} \to A$. On note le plus souvent $\alpha_n \in A$ et on appelle *$n^{ième}$ terme général* l'image d'un entier $n \in \mathbb{N}$ par la suite α.

ii) On dira qu'une suite à valeurs dans A de terme général α_n est *presque nulle* s'il existe un entier n_0 tel que pour tout $n > n_0$, $\alpha_n = 0$.

Proposition IV.2.2 *i) La structure canonique de A-module de A (cf. II.3.4.b)) induit une structure de A-module (cf. II.3.1) sur l'ensemble $A^{\mathbb{N}}$ des suites à valeurs dans A donnée pour tout $(\alpha, \beta) \in A^{\mathbb{N}} \times A^{\mathbb{N}}$ et tout $(a, b) \in A \times A$ par :*

$$(a \cdot \alpha +_{A^{\mathbb{N}}} b \cdot \beta)_n := a * \alpha_n + b * \beta_n \ . \qquad 1$$

ii) La structure de A-module définie ci-dessus s'induit sur l'ensemble ${A^{\mathbb{N}}}_0$ des suites presque nulles à valeurs dans A de sorte que ${A^{\mathbb{N}}}_0$ est un sous-A-module de $A^{\mathbb{N}}$ (cf. II.4.4.)

Preuve : *La vérification est immédiate et laissée en exercice.*

IV.2.3. – On définit une multiplication sur $A^{\mathbb{N}}$ de la manière suivante. Pour tout $(\alpha, \beta) \in A^{\mathbb{N}} \times A^{\mathbb{N}}$, de terme général (α_n, β_n) on posera $\alpha *_{A^{\mathbb{N}}} \beta$ la suite de terme général

$$(\alpha *_{A^{\mathbb{N}}} \beta)_n := \sum_{k+l=n} \alpha_k *_A \beta_l \ . \qquad \text{IV.2.3.1}$$

Proposition IV.2.4 *i) La multiplication définie en IV.2.3.1 donne au A-module $A^{\mathbb{N}}$, une structure de A-algèbre (cf. II.2.1) dont l'élément unité est*

$$1_{A^{\mathbb{N}}} := 1, 0, 0, \ldots, 0, \ldots \qquad 1$$

et le morphisme structural est donné par

$$\begin{array}{ccc} A & \to & A^{\mathbb{N}} \\ a & \mapsto & a, 0, 0, \ldots, 0, \ldots \ . \end{array}$$

ii) La structure définie ci-dessus s'induit sur ${A^{\mathbb{N}}}_0$ de sorte que ${A^{\mathbb{N}}}_0$ devient une sous-A-algèbre de $A^{\mathbb{N}}$ (cf. II.2.5.)

Preuve : *Les vérifications sont sans difficulté. Il convient toutefois de bien vérifier que la multiplication définie par IV.2.3.1 est bien interne sur ${A^{\mathbb{N}}}_0$; autrement dit, que le produit, en ce sens, de deux suites presque nulles est encore une suite presque nulle. On remarquera qu'on peut même trouver une borne explicite, même si elle n'est pas optimale. En effet, si pour tout $n \geq n_0$, $\alpha_n = 0$ et pour tout $m \geq m_0$, $\beta_m = 0$, il n'est pas difficile de constater que pour tout $p \geq n_0 + m_0$, $(\alpha *_{A^{\mathbb{N}}} \beta)_p = 0$.*

Remarque IV.2.5 i) Il faut remarquer que le morphisme structural $A \hookrightarrow {A^{\mathbb{N}}}_0$ est injectif.

ii) La structure de A-algèbre définie ci-dessus sur ${A^{\mathbb{N}}}_0$ est la structure d'algèbre compatible à la structure de A-module définie en IV.2.2 au sens de la remarque II.3.4.a).

Définition IV.2.6 i) On appelle *polynôme à coefficients dans A et à une indéterminée* un élément de la A-algèbre ${A^{\mathbb{N}}}_0$.

ii) On appelle *degré* (resp. *valuation*) d'un polynôme $P := \alpha_0, \ldots, \alpha_n, \ldots$ et l'on note $\deg(P)$, (resp. $\mathrm{val}(P)$) le plus petit (resp. le plus grand) entier k tel que pour tout $n > k$ (resp. $n < k$) $\alpha_n = 0$. Pour que la proposition (cf. IV.2.9) ait un sens, en toute généralité, on posera, par convention

$$\begin{aligned} \deg(0_{A^{\mathbb{N}}{}_0}) &= -\infty\,, \\ \mathrm{val}(0_{A^{\mathbb{N}}{}_0}) &= +\infty\,. \end{aligned}$$

Proposition IV.2.7 *i) Les éléments*

$$\begin{aligned} e_0 &:= 1, 0, 0, \ldots, 0, \ldots \\ e_1 &:= 0, 1, 0, \ldots, 0, \ldots \\ e_2 &:= 0, 0, 1, \ldots, 0, \ldots \\ \ldots &\quad \ldots \end{aligned}$$

forment une base de $A_0^{\mathbb{N}}$ (cf. II.7.12.ii).) Le module $A^{\mathbb{N}}{}_0$ est, par conséquent, un A-module libre (cf. II.7.13.i).)

ii) Pour tout $(i, j) \in \mathbb{N} \times \mathbb{N}$,

$$e_i *_{A^{\mathbb{N}}{}_0} e_j = e_{i+j} \qquad 1$$

***Preuve** : Ces vérifications sont des calculs faciles.*

IV.2.8. – Si l'on note $X := e_1$, et que l'on pose, par convention

$$X^0 := e_0 = 1_{A^{\mathbb{N}}{}_0} = 1, 0, 0, \ldots\,,$$

on constate que

$$X^i = X *_{A^{\mathbb{N}}{}_0} X *_{A^{\mathbb{N}}{}_0} \ldots *_{A^{\mathbb{N}}{}_0} X\,,\ i \in \mathbb{N}$$

(un produit de i termes égaux à $X,$) est une base de $A^{\mathbb{N}}{}_0$, d'après la proposition IV.2.7. C'est pourquoi, on note usuellement $A[X]$ l'algèbre des polynômes à une indéterminée à coefficients dans A et

$$P := \sum_{i=0}^{\deg(P)} \alpha_i X^i$$

un élément de $A[X]$.

Proposition IV.2.9 *i) Pour tout $(P, Q) \in A[X] \times A[X]$, on a :*

$$\deg(P + Q) \leq \max(\deg(P), \deg(Q))\,; \qquad 1$$

$$\deg(P * Q) \ \leq \ \deg(P) + \deg(Q) \ ; \qquad 2$$

$$\mathrm{val}(P + Q) \ \geq \ \min(\mathrm{val}(P), \mathrm{val}(Q)) \ ; \qquad 3$$

$$\mathrm{val}(P * Q) \ \geq \ \mathrm{val}(P) + \mathrm{val}(Q) \ . \qquad 4$$

ii) Si A est intègre (cf. III.2.1,) on a égalité dans les formules i).2 et i).4.

Preuve *: La démonstration de ces formules est sans mystère.*

IV.2.10. — L'ensemble des fonctions $f \ : \ A \ \to \ A$ définies sur A à valeurs dans A est canoniquement muni de deux lois $+$ et $*$ définies respectivement par

$$(f + g)(a) \ := \ f(a) +_A g(a) \ , \qquad \text{IV.2.10.1}$$

et

$$(f * g)(a) \ := \ f(a) *_A g(a) \ , \qquad \text{IV.2.10.2}$$

pour tout couple (f, g) de fonctions définies sur A à valeurs dans A.

Proposition IV.2.11 *i) L'ensemble des fonctions définies sur A à valeurs dans A muni des lois*

$$+ \text{ (cf. IV.2.10.1,) et } * \text{ (cf. IV.2.10.2,)}$$

est un anneau (commutatif si A est commutatif).

ii) L'application de A dans l'anneau des fonctions définies sur A à valeurs dans A qui à tout élément $a \ \in \ A$, associe la fonction constante de valeurs a, i.e.la fonction $c_a \ : \ A \ \to \ A$ définie pour tout $b \ \in \ A$ par $c_a(b) \ = \ a$, donne à l'ensemble des fonctions définies sur A à valeurs dans A une structure de A-algèbre.

IV.2.12. — À tout polynôme

$$P \ := \ \sum_{i=0}^{\deg(P)} \alpha_i X^i \ \in \ A[X]$$

on associe une *fonction polynôme* encore notée P *i.e.*une fonction à valeurs dans A, définie sur A par

$$P(a) \ := \ \sum_{i=0}^{\deg(P)} \alpha_i a^i \qquad \text{IV.2.12.1}$$

pour tout $a \in A$.

Proposition IV.2.13 *L'application qui à un polynôme $P \in A[X]$ associe sa fonction polynôme (cf. IV.2.12.1) est un morphisme de A-algèbres de $A[X]$ dans l'algèbre des fonctions définies sur A à valeurs dans A (cf. IV.2.11.)*

Remarque IV.2.14 Le morphisme défini en IV.2.12.1 n'est pas injectif en général, y compris si A est un corps. Par exemple pour $p \in \mathbb{Z}$ premier, pour tout $\xi \in \mathbb{Z}/p\, \xi^p - \xi = 0$ (cf. TD n° III, exercice E, question 4).) Ceci signifie que la fonction polynôme associée au polynôme $X^p - X \in \mathbb{Z}/p[X]$ est la fonction nulle alors que ce polynôme n'est pas l'élément $0_{\mathbb{Z}/p[X]}$.

Proposition IV.2.15 (Propriété universelle de l'anneau des polynômes) *Étant donnée une*

$$A - \text{algèbre } f_B : A \to B \text{ (cf. II.2.1 ,)}$$

pour tout $b \in B$, il existe un unique morphisme de A-algèbres (cf. II.2.2) $\phi_b : A[X] \to B$ tel que $\phi_b(X) = b$.

Preuve *: Un élément $b \in B$ étant fixé, s'il existe un morphisme $\phi_b : A[X] \to B$ tel que $\phi_b(X) = b$, nécessairement, pour tout élément*

$$P := \sum_{i=0}^{\deg(P)} \alpha_i X^i \in A[X]\,,$$

$$\phi_b(P) = \sum_{i=0}^{\deg(P)} f_B(\alpha_i) *_B b^i \,! \qquad \text{IV.2.15.1}$$

On vérifie facilement que ϕ_b ainsi défini est un morphisme de A-algèbres.

Corollaire IV.2.16 (Fonctorialité de l'algèbre des polynômes) *En particulier si B est une A-algèbre il existe un unique morphisme de A-algèbres $A[X] \to B[X]$ caractérisé par : $X \mapsto X$.*

Définition IV.2.17 On dit qu'un polynôme $P \in A[X]$ est *irréductible* si c'est un élément irréductible de l'anneau $A[X]$ au sens de la définition III.3.1.

Proposition IV.2.18 *i) Un élément $P := \sum_{i=0}^{\deg(P)} \alpha_i X^i \in A[X]$ est inversible, si et seulement si $P \in A^\times$, c'est-à-dire si et seulement si $\deg(P) = 0$ et $\alpha_0 \in A^\times$.*

ii) Un polynôme $P \in A[X]$ est irréductible s'il n'existe pas de polynômes Q et R dans $A[X]$ avec $\deg(Q) > 0$ et $\deg(R) > 0$ tels que $P = Q *_{A[X]} R$.

Proposition IV.2.19 *Si A est un corps alors $A[X]$ est un anneau euclidien donc principal (cf. III.4.1.)*

Remarque IV.2.20 L'anneau $A[X]$ n'est pas principal en général. Par exemple, pour K un corps, $K[X,Y] := K[X][Y]$ n'est pas principal : l'idéal engendré par $\{X;Y\}$ n'est en effet pas principal.

Définition IV.2.21 Pour tout polynôme $P \in A[X]$ on appelle *racine de P dans A* un élément $a \in A$ tel que : $P(a) = 0_A$.

Proposition IV.2.22 *Si K est un corps, et $P \in K[X]$, $a \in K$ est une racine de P si et seulement si il existe $Q \in K[X]$ tel que*

$$P = (X-a) *_{K[X]} Q \, .$$

Preuve *: Supposons que a est une racine de P. D'après la proposition IV.2.15, il existe un unique morphisme de K-algèbres $\phi_a : K[X] \to K$ tel que $\phi_a(X) = a$, (où K est considéré comme algèbre sur lui-même via Id_K.)*

Notons que ce morphisme associe à tout polynôme $R \in K[X]$, "sa valeur en a $R(a)$;" c'est-à-dire l'image de a par la fonction polynôme associée à R (cf. IV.2.12.1.)

Un élément $a \in K$ est racine de P si et seulement si $P \in \mathrm{Ker}\,\phi_a$. Or $\mathrm{Ker}\,\phi_a$ est un idéal de $K[X]$ (cf. II.5.8.a)) non égal à $K[X]$. En effet, un corps contient au moins deux éléments distincts, il existe donc $b \in K$ $b \neq a$, ce qui implique que $X - b \notin \mathrm{Ker}\,\phi_a$.

Comme $K[X]$ est principal $\mathrm{Ker}\,\phi_a$ est engendré par un élément M. Comme $\mathrm{Ker}\,\phi_a \neq K[X]$, $\deg(M) > 0$. Or $X - a \in \mathrm{Ker}\,\phi_a$, ce qui implique que M divise $X - a$ (cf. III.1.2.) Un corps étant un anneau intègre (cf. III.2.1,) il s'ensuit que $\deg(M) \leq 1$ d'après la formule IV.2.9.i).2 et la proposition IV.2.9.ii).

Il en résulte que $X - a$ est un générateur de $\mathrm{Ker}\,\phi_a$ donc qu'il existe $Q \in K[X]$ tel que

$$P = (X-a) *_{K[X]} Q \, .$$

Réciproquement si $P = (X-a) *_{K[X]} Q$ il est clair que $P(a) = 0$.

Corollaire IV.2.23 *Étant donnés un anneau intègre A et $P \in A[X]$, $a \in A$ est une racine de P si et seulement si il existe $Q \in A[X]$ tel que*

$$P = (X-a) *_{A[X]} Q \, .$$

Preuve : *Notons K le corps des fractions de A (cf. IV.1.5.) L'injection canonique*

$$\begin{array}{rccl} i: & A & \hookrightarrow & K \\ & a & \mapsto & (a, 1_A) \;=\; \frac{a}{1_A} \;=\; a \end{array}$$

(cf. IV.1.4.iii)) induit un unique morphisme de A-algèbres $i[X] : A[X] \to K[X]$ tel que $i[X](X) = X$ (cf. IV.2.16.) Pour tout

$$P \;=\; \sum_{k=0}^{\deg(P)} \alpha_k X^k \;\in\; A[X]\,,$$

$$i[X](P) \;=\; \sum_{k=0}^{\deg(P)} i(\alpha_k) X^k\,.$$

Il n'est pas difficile de voir que $i[X]$ est injectif.
Supposons que a est une racine de

$$P \;:=\; \sum_{k=0}^{\deg(P)} \alpha_k X^k\,.$$

$$\begin{array}{lrcl} & P(a) & = & 0_A \\ i \text{ est un } \overset{\Leftrightarrow}{\text{injectif}} & i(P(a)) & = & 0_K \\ \Leftrightarrow & i(\sum_{k=0}^{\deg(P)} \alpha_k a^k) & = & 0_K \\ i \text{ est un } \overset{\Leftrightarrow}{\text{morphisme}} & \sum_{k=0}^{\deg(P)} i(\alpha_k) i(a)^k & = & 0_K \\ \Leftrightarrow & i[X](P)(i(a)) & = & 0_K \end{array}$$

c'est-à-dire que $i(a)$ est une racine de $i[X](P)$ lequel est un élément de $K[X]$. D'après la proposition IV.2.22, il existe donc

$$\Xi \;:=\; \sum_{k=0}^{\deg(\Xi)} \xi_k X^k \;\in\; K[X]$$

tel que

$$i[X](P) \;=\; (X - i(a)) *_{K[X]} \Xi \;=\; i[X](X - a) *_{K[X]} \Xi\,. \qquad \textit{IV.2.23.1}$$

Ceci implique que $\deg(\Xi) = \deg(P) - 1$ et $\xi_{\deg(\Xi)} = i(\alpha_{\deg(P)})$. Il s'ensuit que $\xi_{\deg(\Xi)} \in A$.

Supposons que pour tout $k \geq j$, $\xi_k = i(\beta_k)$ *i.e.*$\xi_k \in A$. *On a l'identité :*

$$\begin{array}{lrcl} & i(\alpha_j) & = & \xi_{j-1} -_K i(a) *_K \xi_j \\ \Leftrightarrow & \xi_{j-1} & = & i(\alpha_j) +_K i(a) *_K \xi_j \\ \overset{\Leftrightarrow}{\text{hypothèse de récurrence}} & \xi_{j-1} & = & i(\alpha_j) +_K i(a) *_K i(\beta_j) \\ \overset{\Leftrightarrow}{i \text{ est un morphisme}} & \xi_{j-1} & = & i(\alpha_j +_A a *_A \beta_j) \, . \end{array}$$

Posons alors $\beta_{j-1} := \alpha_j +_A a *_A \beta_j$. *Il s'ensuit que pour tout* $0 \leq k \leq \deg(\Xi)$ *il existe* $\beta_k \in A$ *tel que* $\xi_k = i(\beta_k)$. *Par conséquent :*

$$\begin{aligned} \Xi &= \sum_{k=0}^{\deg(\Xi)} \xi_k X^k \\ &= \sum_{k=0}^{\deg(\Xi)} i(\beta_k) X^k \\ &= i[X](\sum_{k=0}^{\deg(\Xi)} \beta_k X^k) \\ &= i[X](Q) \, ; \end{aligned}$$

avec

$$Q := \sum_{k=0}^{\deg(\Xi)} \beta_k X^k \in A[X] \, .$$

L'identité IV.2.23.1 se réécrit donc :

$$\begin{array}{rcl} i[X](P) & = & i[X](X-a) *_{K[X]} i[X](Q) \\ & \overset{=}{i[X] \text{ est un morphisme}} & i[X]\big((X-a) *_{A[X]} Q\big) \, ; \end{array}$$

ce qui implique

$$P = (X-a) *_{A[X]} Q$$

car $i[X]$ *est injectif.*

Définition IV.2.24 Étant donné un polynôme $P \in A[X]$, où A est un anneau intègre, si $a \in A$ est une racine de P, on appelle *ordre de multiplicité de la racine* a le plus grand entier n tel que $P = (X-a)^n * Q$ avec $Q \in A[X]$.

Proposition IV.2.25 *Si* A *est un anneau intègre, pour tout polynôme* $P \in A[X]$, *la somme des ordres de multiplicité des racines de* P *est inférieure ou égale au degré de* P.

IV.3 . −Anneaux de caractéristique p

Dans cette section les anneaux sont commutatifs (cf. II.1.2.)

Proposition IV.3.1 *Étant donné un anneau intègre (cf. III.2.1,) A, le morphisme canonique $\phi : \mathbb{Z} \to A$ (cf. II.2.8.i)e)st soit injectif, soit son noyau (cf. II.5.8.a)e)st un idéal premier (cf. III.1.8.i)d)e $\mathbb{Z}$.*

***Preuve** : Si $\phi : \mathbb{Z} \to A$ n'est pas injective, son noyau n'est pas réduit à $\{0_{\mathbb{Z}}\}$ et c'est un idéal de $\mathbb{Z}$ également différent de $\mathbb{Z}$ tout entier puisque le morphisme nul n'est pas un morphisme d'anneau (cf. l'axiome ANN$_7$ de la définition II.1.9.)*

Par conséquent, $\mathrm{Ker}\,\phi = n\mathbb{Z}$ pour $n \neq 1$.

D'après le corollaire II.6.4, ϕ induit un isomorphisme

$$\gamma : \mathbb{Z}/\mathrm{Ker}\,\phi = \mathbb{Z}/n\mathbb{Z} \cong B := \mathrm{Im}\,\phi .$$

Par conséquent B est une sous-$\mathbb{Z}$-algèbre de A (cf. II.4.11.iii).)

Comme A est intègre, B est également intègre et, par conséquent, $\mathbb{Z}/n$ qui lui est isomorphe est intègre. Il s'ensuit, d'après la proposition III.2.12 que $n\mathbb{Z}$ est premier, c'est-à-dire que n est premier (cf. III.1.8.ii).)

Définition IV.3.2 Si dans la proposition IV.3.1 le morphisme ϕ est injectif on dit que *A est de caractéristique* 0 sinon on dit que *A est de caractéristique p* où p est un générateur de $\mathrm{Ker}\,\phi$.

Corollaire IV.3.3 *La caractéristique d'un anneau intègre est soit 0 soit un nombre premier p. Dans ce derniers cas $\mathbb{Z}/\mathrm{Ker}\,\phi = \mathbb{Z}/p\mathbb{Z}$ est d'ailleurs un corps .*

Exemple IV.3.4 a) Un certain nombre d'exemples d'anneaux de caractéristique 0 est bien connu ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}[X]$, $\mathbb{Q}[X, Y]$ etc ...)

b) Nous ne nous intéresserons, dans cette section, qu'à des anneaux de caractéristique non nulle.

Notons tout d'abord que de tels anneaux existent. En effet, étant donné un nombre premier p, l'anneau $\mathbb{Z}/p$ est intègre (cf. III.2.12e)t il est, à l'évidence, de caractéristique p.

À noter que $\mathbb{Z}$ étant un anneau principal, l'idéal premier (p) est également maximal (cf. III.4.6,) c'est-à-dire que $\mathbb{Z}/p$ est en fait un corps (cf. II.1.5.)

Définition IV.3.5 Pour un nombre premier $p \in \mathbb{Z}$ on appellera *corps premier* et on notera $\mathbb{F}_p$ l'anneau $\mathbb{Z}/p$ (où la structure d'anneau considérée sur $\mathbb{Z}/p$ est la structure canonique *i.e.*la structure quotient (cf. II.5.11.))

Exemple IV.3.6 Dans $\mathbb{Z}$, un idéal premier étant nécessairement maximal, un quotient $\mathbb{Z}/n$ $n \in \mathbb{Z}$ est soit un corps, soit un anneau non intègre. Cependant, il existe des anneaux de caractéristique p (p premier dans $\mathbb{Z}$,) qui ne sont pas des corps : par exemple $\mathbb{F}_p[X]$ l'anneau des polynômes à une indéterminée et à coefficients dans le corps premier $\mathbb{F}_p$.

Proposition IV.3.7 *Un nombre entier p étant fixé,*

i) un anneau A de caractéristique p est canoniquement une $\mathbb{F}_p$-algèbre ;

ii) pour deux anneaux A et B de caractéristique p, $u : A \to B$ est un morphisme d'anneaux si et seulement si u est un morphisme de $\mathbb{F}_p$-algèbres.

Preuve *:*

i Par définition, si A est de caractéristique p (cf. IV.3.2,) le morphisme canonique $f_A : \mathbb{Z} \to A$ (cf. II.2.8a) pour noyau l'idéal premier $(p) = p\mathbb{Z}$.

D'après la proposition II.6.2.ii), le morphisme structural canonique f_A se factorise à travers $\mathbb{F}_p = \mathbb{Z}/p$ en un morphisme injectif $\phi_A : \mathbb{F}_p \to A$ tel que $\phi_A \circ \pi_p = f_A$ (où $\pi_p : \mathbb{Z} \to \mathbb{F}_p$ est la surjection canonique.)

Supposons donnés deux morphismes d'anneaux g et $h : \mathbb{F}_p \to A$ i.e.deux structures de $\mathbb{F}_p$-algèbre sur A.

Les morphismes $g \circ \pi_p$ et $h \circ \pi_p$ sont alors des structures de $\mathbb{Z}$-algèbre sur A. Par la proposition II.2.8.i),

$$g \circ \pi_p = f_A = h \circ \pi_p .$$

Par conséquent, pour tout $x \in \mathbb{Z}$, $g[\pi_p(x)] = h[\pi_p(x)]$. Comme π_p est surjectif, pour tout $\xi \in \mathbb{F}_p$, $g(\xi) = h(\xi)$ c'est-à-dire que g et h coïncident, d'où l'unicité de la structure de $\mathbb{F}_p$-algèbre sur A.

ii Ce point résulte de (i) suivant un raisonnement tout à fait analogue à celui de la démonstration de II.2.8.ii).

Lemme IV.3.8 *i) Si $\pi : \mathbb{F}_p[X] \to A$ est un morphisme d'anneaux (cf. II.1.9s)urjectif et si A est intègre, alors A est un anneau de caractéristique p.*

ii) L'anneau A est un corps si et seulement si $\operatorname{Ker}\pi$ est un idéal maximal de $\mathbb{F}_p[X]$ si et seulement si $\operatorname{Ker}\pi$ est engendré par un polynôme irréductible (cf. IV.2.17,) (cf. III.3.1,) dans $\mathbb{F}_p[X]$.

Preuve *:*

i On rappelle qu'il existe un unique morphisme de structure de $\mathbb{Z}$-algèbre $f_A : \mathbb{Z} \to A$ (cf. II.2.8.i)e)t que, par conséquent, $f_A = \pi \circ \phi$ où ϕ est le morphisme de structure de $\mathbb{F}_p[X]$ comme $\mathbb{Z}$-algèbre. Toujours d'après l'unicité du morphisme structural (cf. loc. cit.) $\phi = i \circ \pi_p$ où i est l'inclusion canonique $\mathbb{F}_p \to \mathbb{F}_p[X]$ (cf. IV.2.5.i)e)t $\pi_p : \mathbb{Z} \to \mathbb{F}_p = \mathbb{Z}/p$ la surjection canonique.

Il s'ensuit que

$$f_A = \pi \circ i \circ \pi_p$$

est un morphisme d'algèbres qui n'est pas injectif puisque π_p ne l'est pas et que $\operatorname{Ker} \pi_p \subset \operatorname{Ker} f_A$. Or, $\operatorname{Im} f_A$ étant une sous-$\mathbb{Z}$-algèbre de A (cf. II.4.11.iii)i)somorphe à $\mathbb{Z}/\operatorname{Ker} f_A$ est intègre puisque A est intègre. Il s'ensuit que $\operatorname{Ker} f_A$ est un idéal premier de $\mathbb{Z}$ contenant (p). Par maximalité des idéaux premiers dans $\mathbb{Z}$ (cf. III.4.6,) $\operatorname{Ker} f_A = (p)$ ce qui prouve que A est de caractéristique p (cf. IV.3.2.)

ii La proposition III.2.12 entraîne que A est un corps si et seulement si $\operatorname{Ker} \pi$ est un idéal maximal dans $\mathbb{F}_p[X]$. Comme $\mathbb{F}_p[X]$ est principal (euclidien), le corollaire III.2.13 et la proposition III.4.6 entraînent que A est un corps si et seulement si $\operatorname{Ker} \pi$ est un idéal premier non nul.

Or comme $\mathbb{F}_p[X]$ est principal, il existe un élément $P \in \mathbb{F}_p[X]$ tel que $\operatorname{Ker} \pi = P\mathbb{F}_p[X]$. Il s'ensuit que A est un corps si et seulement si P est non nul et est un élément premier de $\mathbb{F}_p[X]$.

En combinant finalement le lemme III.3.2 et le lemme de GAUSS *(cf. III.3.6o)n conclut que A est un corps si et seulement si P est irréductible.*

Remarque IV.3.9 Le lemme précédent permet de construire un grand nombre d'anneaux de caractéristique p dont certains sont des corps comme nous venons de le voir.

Proposition IV.3.10 *Pour tout anneau A de caractéristique p, l'application*

$$\begin{array}{rccc} \mathcal{F}_A : & A & \to & A \\ & a & \mapsto & a^p \end{array}$$

est un morphisme de $\mathbb{F}_p$-algèbres appelé morphisme de Frobenius de A.

Preuve *:*

- *Il faut, tout d'abord, montrer que $\mathcal{F}_A$ est un morphisme de groupes (voir l'axiome ANN_6 de la définition II.1.9.)*

  Ceci est traité dans la TD n° III, exercice E, question 2) de l'exercice TD n° III, exercice E du TD TD n° III.

- *Les axiomes ANN_7 et ANN_8 de la définition II.1.9 se vérifient immédiatement.*

- *Enfin, la compatibilité au morphisme structural $\mathbb{F}_p \to A$ (cf. II.2.2r)ésulte du fait que, pour tout $\lambda \in \mathbb{F}_p$, $\lambda^p = \lambda$ (voir TD n° III, exercice E, question 3) de l'exercice TD n° III, exercice E du TD TD n° III.)*

Proposition IV.3.11 *i) Soit p un nombre premier et P un polynôme irréductible (cf. IV.2.17d)e degré d dans $\mathbb{F}_p[X]$. Alors le quotient $k := \mathbb{F}_p[X]/P$ est un corps fini, c'est-à-dire possédant un nombre fini q d'éléments avec $q = p^d$.*

Preuve *:*

- *Si $P \in \mathbb{F}_p[X]$ est irréductible c'est un élément premier (cf. III.3.6p)uisque $\mathbb{F}_p[X]$ est principal (euclidien.) Par conséquent (P) est maximal d'après la proposition III.4.6 et $k := \mathbb{F}_p[X]/P$ est donc un corps d'après la proposition III.2.12.*
- *Notons $e_0, e_1, \ldots, e_{d-1}$ les images respectives de $1_{\mathbb{F}_p}, X, \ldots, X^{d-1}$ par la surjection canonique $\pi : \mathbb{F}_p[X] \to \mathbb{F}_p[X]/P$ où $d = \deg(P)$.*
- *Pour tout d-uplet $(\lambda_0, \ldots, \lambda_{d-1})$ d'éléments de $\mathbb{F}_p$,*

$$\begin{aligned}
& \sum_{k=0}^{d-1} \lambda_k e_k = 0_k \\
\Leftrightarrow \quad & \sum_{k=0}^{d-1} \lambda_k \pi(X^k) = 0_k \\
\Leftrightarrow \quad & \pi[\sum_{k=0}^{d-1} \lambda_k X^k] = 0_k \\
\Leftrightarrow \quad & \sum_{k=0}^{d-1} \lambda_k X^k \in \operatorname{Ker}\pi = P\mathbb{F}_p[X] \\
\Leftrightarrow \quad & P \mid Q := \sum_{k=0}^{d-1} \lambda_k X^k .
\end{aligned}$$

Or Q est de degré $d-1$ et P est de degré d par conséquent, $P|Q$ implique que $Q = 0_{\mathbb{F}_p[X]}$, c'est-à-dire que, pour tout $0 \leq k \leq d-1$ $\lambda_k = 0_{\mathbb{F}_p}$. Ceci prouve que $e_0, e_1, \ldots, e_{d-1}$ est un système libre dans k.

- *Pour tout élément $\xi \in k$, il existe un élément $Q \in \mathbb{F}_p[X]$ tel que $\pi(Q) = \xi$. Or, $\mathbb{F}_p[X]$ étant un anneau euclidien, le reste de la division de Q par P est un polynôme R de degré strictement inférieur à d, congru à Q modulo P, c'est-à-dire vérifiant*

$\pi(R) = \xi$. *Posons* $R := \sum_{k=0}^{e} \lambda_k X^k$ *avec* $e \leq d-1$. *Il s'ensuit que*

$$\begin{aligned} \xi &= \pi[\sum_{k=0}^{e} \lambda_k X^k] \\ &= \sum_{k=0}^{e} \lambda_k \pi(X^k) \\ &= \sum_{k=0}^{e} \lambda_k e_k \ , \end{aligned}$$

ce qui prouve que $e_0, e_1, \ldots, e_{d-1}$ *est un système générateur de* k.
C'est donc une base de k *et, par conséquent,* k *est un* $\mathbb{F}_p$*-espace vectoriel de dimension* d. *Il est très élémentaire de constater qu'alors* k *possède* p^d *éléments.*

Remarque IV.3.11.1 On aurait pu d'abord montrer que k est une $\mathbb{F}_p$-algèbre de dimension finie, puis, grâce au fait que P est irréductible, que k est intègre ce qui entraîne que K est un corps (cf. TD n° II, exercice E, question 1), e).)

Université Paris Sud — Année 2004–2005

Licence MA — Algèbre Générale

TD n° I

Exercice A : (**Un exemple de représentation linéaire de** $(\mathbb{R}, +)$)

Pour un entier $n \in \mathbb{N}$ **fixé, on note** $\mathbb{R}[X]_n$ **le** $\mathbb{R}$**-espace vectoriel des polynômes à coefficients réels et de degré inférieur ou égal à** n .

On note

$$\mathcal{B}_0 := (1, X, \ldots, X^n)$$

sa base canonique et pour tout $a \in \mathbb{R}$, **on pose**

$$\mathcal{B}_a := (1, (X-a), \ldots, (X-a)^n) .$$

1) Montrer que, pour tout $a \in \mathbb{R}$, $\mathcal{B}_a$ est une base de $\mathbb{R}[X]_n$ et donner la matrice de passage P_a de la base $\mathcal{B}_0$ à la base $\mathcal{B}_a$.

2) **a)** Montrer que, pour tout couple (a, b) de nombres réels, $P_{a+b} := P_a P_b$.

b) En déduire que l'application

$$\begin{array}{rccc} \phi : & \mathbb{R} & \to & \mathrm{GL}_n(\mathbb{R}) \\ & a & \mapsto & P_a \end{array}$$

est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathrm{GL}_n(\mathbb{R}), *)$.

c) Donner (sans calcul) pour tout a réel, P_a^{-1} .

d) L'image de ϕ est-elle un groupe abélien ?

Exercice B : (**Relations binaires**)

Étant donné un ensemble E, **on appelle** $\mathcal{R}$ **l'ensemble des relations d'équivalence sur** E .

1) R_1 **et** R_2 **étant deux éléments de** $\mathcal{R}$, **on considère la relation** $R :=$ **"**R_1 **et** R_2**" appelée intersection de** R_1 **et** R_2.

a) Démontrer que R est une relation d'équivalence.

b) Quel est son graphe ?

c) Démontrer que toute classe modulo R est l'intersection d'une classe modulo R_1 et d'une classe modulo R_2.

d) Étudier les exemples suivants :

$\alpha)$ $E = \mathbb{Z}$, d_1 et d_2 sont deux entiers strictement positifs, R_i est la congruence modulo d_i. (On rappelle que deux entiers m et n sont *dits congrus modulo* d s'il existe $q \in \mathbb{Z}$ tel que $m - n = qd$.)

$\beta)$ E est le plan et D_1 et D_2 sont deux droites. La relation R_i est "(MM') est parallèle à D_i".

2) Avec les mêmes notations que ci-dessus, la relation "R_1 ou R_2" est elle une relation d'équivalence ? Quel est son graphe ?

3) Étant donnés deux éléments R et R' de $\mathcal{R}$, on dit que R est *plus fine que* R' lorsque

$$\forall (x, y) \in E \times E \ , \ R(x, y) \ \Rightarrow \ R'(x, y)$$

et on note $R \leq R'$.

a) Comparer les graphes de R et R' lorsque $R \leq R'$.

b) Montrer que $\leq$ est une relation d'ordre sur $\mathcal{R}$.

c) Est-ce une relation d'ordre totale ?

d) Y a-t-il un plus petit et un plus grand élément dans $\mathcal{R}$ muni de $\leq$?

e) Montrer que R est plus fine que R' $(R \leq R')$ si et seulement si toute classe modulo R' est réunion de classes modulo R.

f) $E = \mathbb{Z}$, déterminer toutes les congruences modulo un entier strictement positif qui sont plus fines que la congruence modulo d.

Exercice C : $(\mathbb{Z}/n\mathbb{Z})$

Soit $n \in \mathbb{N}$ un entier. Pour tout couple $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, on écrira $a \equiv b \, [n]$ si $n \mid b - a$ et on dira que a est congru à b modulo n.

1) Pour a, b, c des éléments de $\mathbb{Z}$, vérifier que :

i) (**Réflexivité**)

$$a \equiv a \, [n] \ ;$$

ii) (**Symétrie**)

$$a \equiv b \, [n] \ \Rightarrow \ b \equiv a \, [n] \ ;$$

iii) (**Transitivité**)

$$\big(a \equiv b \, [n] \text{ et } b \equiv c \, [n]\big) \ \Rightarrow \ a \equiv c \, [n] \ .$$

On dit alors que la relation de congruence est une *relation d'équivalence*. Pour tout $a \in \mathbb{Z}$, on notera

$$\overline{a} := \{b \in \mathbb{Z} \ / \ b \equiv a \, [n]\} \ .$$

2) Montrer que :

a) Pour tout

$$a \in \mathbb{Z}, \ a \in \overline{a} \ .$$

b) Pour tous a et b éléments de $\mathbb{Z}$,

$$\left(\overline{a} \cap \overline{b} \neq \emptyset \right) \Rightarrow \overline{a} = \overline{b} .$$

c)

$$\mathbb{Z} = \bigcup_{a \in \mathbb{Z}} \overline{a} .$$

Dans la suite on note

$$\mathbb{Z}/n\mathbb{Z} := \{\overline{a} , \ a \in \mathbb{Z}\} .$$

3) Quel est le nombre d'éléments de $\mathbb{Z}/n\mathbb{Z}$?

4) Soient a, b, c, d des éléments de $\mathbb{Z}$.

a) Montrer que

$$\left(a \equiv c \, [n] \text{ et } b \equiv d \, [n] \right) \Rightarrow \left(a+b \equiv c+d \, [n] \text{ et } ab \equiv cd \, [n] \right) .$$

b) En déduire qu'en posant

$$\overline{a} + \overline{b} := \overline{a+b} \text{ et } \overline{a} \times \overline{b} := \overline{a \times b},$$

on définit bien des lois $+$ et $*$ sur $\mathbb{Z}/n\mathbb{Z}$ qui donnent à ce dernier une structure d'anneau commutatif.

c) Quels sont les élément neutre et élément unité pour la structure ci-dessus ?

d) Donner les tables d'addition et de multiplication de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ pour $n = 2, 3, 4, 5$.

e) À quelle condition nécessaire et suffisante sur n $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est-il un corps ?

Exercice D : (Étude de quelques groupes finis)

Soit $n \in \mathbb{N}^*$, un entier non nul et $(G, *)$ un groupe (qui n'est pas supposé, a priori, commutatif) à n éléments.

1) On suppose, dans cette question, que n est premier.

a) Montrer que G possède au moins un élément g d'ordre n.

b) Montrer qu'il existe un unique morphisme de groupes

$$\begin{array}{rcl} \phi : (\mathbb{Z}/n, +) & \to & (G, *) \\ 1_{\mathbb{Z}/n} & \mapsto & g . \end{array}$$

c) Montrer que ϕ est un isomorphisme et en déduire que *tout groupe fini d'ordre n premier est isomorphe à $\mathbb{Z}/n$ et commutatif.*

On suppose, dans les questions question 2), question 3) et question 4) que $n = 4$. On pourra, pour fixer les idées, noter

$$G := \{\epsilon; a; b; c\}$$

où ϵ est l'élément neutre de G pour la loi de composition qu'on notera $*$.

2) Montrer que les éléments a, b, c de G sont nécessairement d'ordre 2 ou 4.

3) On suppose, dans cette question, que tous les éléments de G sont d'ordre 2.

a) Montrer qu'on a alors :

$$\begin{array}{rcccl} a*b & = & c & = & b*a \\ b*c & = & a & = & c*b \\ c*a & = & b & = & a*c\,. \end{array}$$

b) En déduire la table de la loi de composition $*$ pour le groupe G puis que G est abélien.

c) Montrer qu'il existe un unique morphisme de groupes

$$\begin{array}{rcl} \psi : \mathbb{Z}/2 \times \mathbb{Z}/2 & \to & G \\ (1,0) & \mapsto & a \\ (0,1) & \mapsto & b \end{array}$$

puis vérifier que ψ est un isomorphisme.

4) On suppose, dans cette question, que G possède au moins un élément d'ordre 4. On pourra supposer que $a \in G$ est d'ordre 4.
En vous inspirant de la méthode de la question 1) montrer que G est isomorphe à $\mathbb{Z}/4$.

5) Le groupe S_3 des permutations d'un ensemble à trois éléments est-il commutatif ?

a) Combien le groupe S_3 possède-t-il d'éléments ?

6) Rassembler les résultats de l'exercice pour expliquer pourquoi un groupe non commutatif possède au moins 6 éléments.

Exercice E : Soit G un groupe fini contenant 8 éléments.

1) Montrer que les éléments de G sont d'ordre $2, 4$ ou 8.

2) **a)** Montrer que s'il existe $g \in G$, d'ordre 8, il existe un unique morphisme de groupes

$$\begin{array}{rcl} \phi : \quad \mathbb{Z} & \to & G \\ 1_{\mathbb{Z}} & \mapsto & g\,. \end{array}$$

b) Montrer que ϕ est surjective.

c) Déterminer le noyau de ϕ et en déduire que

$$G \;\cong\; \mathbb{Z}/8\,;$$

et que, par conséquent, G est abélien.

On suppose désormais, que G ne contient pas d'élément d'ordre 8. Supposons, en revanche, qu'il existe un élément $g \in G$ d'ordre 4 et notons

$$\Delta(G) \;:=\; (\{e_G, g, g^2, g^3\}, *_G)$$

le sous-groupe de G engendré par g.

3) **a)** Montrer que $\Delta(G)$ est abélien (on pourra rappeler brièvement, en le généralisant, l'argument de la question question 2).)

b) Montrer qu'il existe un élément $x \in G$ tel que $x\Delta(G) \neq \Delta(G)$.

c) Montrer qu'alors $\Delta(G)x \neq \Delta(G)$.

d) En déduire que $\Delta(G)$ est distingué dans G. (On pourrait tirer de l'argument, l'énoncé : *Tout sous-groupe d'indice* 2 *est distingué.*)

e) Déterminer le quotient $G/\Delta(G)$.

f) En déduire que si $\pi : G \to G/\Delta(G)$ est la surjection canonique, pour tout $y \in x\Delta(G)$, $\pi(y^2) = e_{G/\Delta(G)}$ et par conséquent que $y^2 \in \Delta(G)$.

g) Montrer que, pour tout $y \in x\Delta(G)$, $y^2 = h$ ou $y^2 = h^3$ est contradictoire avec le fait que G ne possède pas d'élément d'ordre 8.

4) Avec les notations de la question précédente, on suppose dans cette question que $x^2 = e_G$.

a) Montrer qu'alors, soit pour tout $y \in x\Delta(G)$ $y^2 = e_G$ soit G est abélien.

b) Montrer que si G est abélien, l'application

$$\begin{aligned} x &\mapsto 1_{\mathbb{Z}/2} \\ h &\mapsto 1_{\mathbb{Z}/4} \end{aligned}$$

définit un isomorphisme

$$G \cong \mathbb{Z}/2 \times \mathbb{Z}/4 \,.$$

c) Montrer que, si G n'est pas abélien, $x \mapsto S_2$ $h \mapsto R$ définit un isomorphisme de groupes

$$G \cong D_4 \,,$$

5) On suppose dans cette question, avec les notations de la question question 3), que $x^2 = h^2$. Montrer qu'alors, pour tout $y \in x\Delta(G)$, $y^2 = h^2$. (On pourra utiliser les résultats de la question question 4) en montrant que n'importe quel élément $y \in x\Delta(G)$ "joue le même rôle que x," en excluant, évidemment ici encore, le cas où G est abélien déjà traité en question 4), b).)

On note Q le sous-groupe de $\mathrm{GL}_2(\mathbb{C})$ engendré par les éléments

$$A := \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \text{ et } B := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

(*groupe des quaternions de Hamilton*.)

6) **a)** Montrer que Q possède 8 éléments (on pourra penser à introduire l'éléments $C := AB$.)

b) Déterminer un sous-groupe $\Delta(Q)$ de Q.

c) Déterminer les éléments d'ordre 4 dans Q.

d) En déduire qu'il n'existe pas d'isomorphisme de groupes de D_4 dans Q.

e) Montrer que

$$A^2 \;=\; B^2 \;=\; C^2 \;=\; ABAB \;=\; -\mathrm{Id}_{\mathbb{C}^2}\,.$$

f) Montrer que dans le cas de la question question 5), $x \mapsto B\ h \mapsto A$ définit un isomorphisme de groupes

$$G \;\cong\; Q\,.$$

On suppose finalement, que G n'a pas d'élément d'ordre 4 c'est-à-dire que tous les éléments de G sont d'ordre 2.

7) Montrer que, pour $(x, y) \in G \times G$, $x^2 = e_G$, $y^2 = e_G$ et $x * y * x * y = e_G$ implique $x * y = y * x$ et en déduire que G est abélien. On pourrait dégager l'énoncé suivant : *Un groupe dont tous les éléments sont d'ordre 2 est abélien.*

8) Récapituler les résultats du problème pour déterminer quel sont, à isomorphisme près, tous les groupes à 8 éléments.

Exercice F : (Introduction au groupe symétrique)

Dans tout cet exercice, E est un ensemble.

1) Montrer que l'ensemble $\mathcal{S}(E)$ des bijections de E sur lui-même, muni de la loi $\circ$ de composition des applications est un groupe.

a) Est-il commutatif ?

On suppose désormais que E est fini c'est-à-dire qu'il existe une bijection $\iota : E \to [1; n]$ où

$$[1; n] \;:=\; \{1; 2; \ldots; n\}$$

est l'ensemble des n premiers entiers naturels, $n \in \mathbb{N}^*$.

2) Montrer que l'application

$$\begin{array}{rccl} \phi : & \mathcal{S}(E) & \to & \mathcal{S}_n \;:=\; \mathcal{S}([1; n]) \\ & u & \mapsto & \iota \circ u \circ \iota^{-1} \end{array}$$

est un isomorphisme de groupes.

3) Quel est le cardinal de $\mathcal{S}_2$?

Fixons un entier $n \geq 2$, et $a \in [1; n+1]$ un entier compris entre 1 et $n+1$. On définit sur $\mathcal{S}_{n+1}$ la relation binaire R_a par

$$s\ R_a\ s' \text{ si } s(a) \;=\; s'(a)\,.$$

a) Montrer que R_a ainsi définie est une relation d'équivalence.

b) Montrer que pour tout $s \in \mathcal{S}_{n+1}$ il existe une bijection entre la classe $\overline{s}$ de s selon R_a et $\mathcal{S}_n$.

c) À quelle condition (nécessaire et suffisante) la classe $\overline{s}$ d'un élément de $\mathcal{S}_{n+1}$ est-elle un sous-groupe de $\mathcal{S}_{n+1}$?

d) Donner en fonction de n le nombre de classes selon R_a.

e) Déduire de ce qui précède une relation entre les cardinaux de $\mathcal{S}_n$ et $\mathcal{S}_{n+1}$; puis le cardinal de $\mathcal{S}_n$ en fonction de n.

4) Soit V un K-espace vectoriel de dimension n (où K est un corps) muni d'une base $(v_1, \ldots, v_n)$.

a) Montrer que pour tout $s \in \mathcal{S}_n$, il existe un unique endomorphisme $\phi(s)$ de V défini par

$$\phi(s)(v_i) := v_{s(i)} \text{ , } \forall 1 \leq i \leq n, \text{ .}$$

b) Montrer que pour tout $s \in \mathcal{S}_n$, $\phi(s)$ est inversible et que ϕ est un morphisme de groupes de $\mathcal{S}_n$ dans $\mathrm{GL}(V)$.

c) Le morphisme ϕ est-il injectif ? surjectif ?

Exercice G : (Type cyclique)

1) Décomposer les permutations

$$s := \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 4 & 5 & 7 & 6 \end{matrix} \text{ et } s' := \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 3 & 6 & 5 & 4 & 1 \end{matrix}$$

de l'ensemble $[1; 7] \subset \mathbb{N}$ en produit de cycles à supports deux à deux disjoints.

a) Calculer le nombre de différentes classes de conjugaison dans $\mathcal{S}_5$ et donner un représentant de chacune d'entre elles.

b) Montrer que tous les 3-cycles de $\mathcal{A}_5$ forment une unique classe de conjugaison.

Un entier $n > 1$ étant fixé dans tout l'exercice, on note $\mathcal{S}_n$ le groupe symétrique d'ordre n *i.e.*le groupe des bijections de l'ensemble $[1, n] \subset \mathbb{N}$.

2) Soient

$$s := \prod_{i=1}^{d} c_i \text{ et}$$
$$s' := \prod_{i=1}^{d} c'_i$$

deux éléments de $\mathcal{S}_n$, tels que pour tout $1 \leq i \leq d$ c_i et c'_i sont deux cycles de même longueur l_i et les $c_{i\,,1 \leq i \leq d}$ (resp. $c'_{i\,,1 \leq i \leq d}$) sont de support deux à deux disjoints.

a) Rappeler, en citant le résultat du cours, que, pour tout $1 \leq i \leq d$ il existe $u_i \in \mathcal{S}_n$, tel que

$$c'_i = u_i \circ c_i \circ u_i^{-1} \text{ .}$$

b) Montrer que pour tout $1 \leq i \leq d$ et tout $a \in [1, n]$, $a \in S_i$ si et seulement si $u_i(a) \in S'_i$ où S_i (resp. S'_i) est le support de c_i (resp. c'_i.)

c) Montrer que l'application u définie sur $\bigcup_{i=1}^{d} S_i$ par $u|S_i := u_i|S_i$ est une bijection de $\bigcup_{i=1}^{d} S_i$ sur $\bigcup_{i=1}^{d} S'_i$.

d) Montrer que l'on peut prolonger u en une bijection $\tilde{u}$ de $[1, n]$ sur lui-même et calculer $\tilde{u} \circ s \circ \tilde{u}^{-1}$.

e) En déduire que s et s' sont conjugués dans $\mathcal{S}_n$.

3) Donner explicitement une permutation $u \in S_7$ conjuguant les éléments s et s' donnés dans la question 1).

Exercice H : Dans tout cet exercice, pour $A := \{a_1, \ldots, a_n\}$ un sous-ensemble fini d'un ensemble E on notera $(a_1, \ldots, a_n)$ la permutation circulaire sur A telle que

$$a_i \mapsto a_{i+1} \, \forall lleq1in-1 \text{ et } a_n \mapsto a_1 \, .$$

Ainsi (a, b) désigne la transposition de support $\{a; b\} \subset E$, pour $a \neq b$.

Les questions question 1) à question 4) constituent un ensemble conduisant à démontrer que *le groupe $\mathcal{A}_4$ ne contient pas de sous-groupe d'ordre* 6.

La question 5) consiste à déterminer un ensemble de générateurs du groupe $\mathcal{A}_4$ et est indépendante de ce qui précède.

La question 6) consiste à étudier un sous-groupe normal particulier d'un groupe G et est tout à fait indépendante des questions précédentes.

La question 7) consiste à particulariser l'étude précédente au cas de $\mathcal{S}_n$ et peut faire appel à des résultats de tout l'exercice.

1) Soient $(G, *)$ un groupe fini à $2k$ éléments, $k \in \mathbb{N}^*$, et H un sous-groupe de G à k éléments.

a) Pourquoi le groupe quotient G/H existe-t-il ? Quel est ce groupe ?

b) En déduire que, pour tout $g \in G$, $g * g \in H$.

2) a) Rappelez la définition du groupe alterné $\mathcal{A}_4$.

b) Quel est le cardinal de $\mathcal{A}_4$?

3) a) Montrer que, pour tout $n \geq 3$, un cycle de longueur 3 est une permutation paire (*i.e.*un élément de $\mathcal{A}_n$.)

b) Combien de parties de $\{1; 2; 3; 4\}$ sont des supports de cycles de longueur 3 dans $\mathcal{A}_4$?

c) Combien de cycles de longueur 3 peuvent avoir le même support ?

d) En déduire quel est le nombre de cycles de longueur 3 dans $\mathcal{A}_4$.

4) Soient a, b, c trois éléments de $[1; 4]$ distincts deux à deux.

a) Calculer $((a, b) \circ (b, c))^2$.

b) En déduire que pour tout cycle $c \in \mathcal{A}_4$ de longueur 3, il existe un élément $d \in \mathcal{A}_4$ tel que $d^2 = c$.

c) Déduire de la question précédente et de la question 1), b) que si H est un sous-groupe d'ordre 6 de $\mathcal{A}_4$, il contient tous les cycles d'ordre 3 .

d) Déduire finalement de la question précédente et de la question 3), d) que $\mathcal{A}_4$ ne possède pas de sous-groupe d'ordre 6.

5) **a)** Montrer qu'un élément de $\mathcal{A}_4$ est soit l'identité, soit un produit de deux transpositions à supports disjoints, soit un cycle d'ordre 3.

b) Pour a, b, c, d des éléments de $[1; 4]$ distincts deux à deux, calculer $(a, b, c) \circ (b, c, d)$.

c) Déduire des deux questions précédentes que $\mathcal{A}_4$ est engendré par les cycles de longueur 3.

Pour $(G, *)$ un groupe, on note $D(G)$ le sous-groupe de G engendré par les éléments de la forme $[g, h] := g * h * g^{-1} * h^{-1}$, g et h des éléments de G.

6) **a)** Que vaut $D(G)$ si G est abélien (commutatif ?)

b) Pour tout couple (g, k) d'éléments de G, on note g^k le conjugué de g par k . Comparer $[g, h]^k$ et $[g^k, h^k]$ pour tout triplet (g, h, k) d'éléments de G. En déduire que $D(G)$ est distingué dans G.

7) **Soit $n \geq 2$ un entier.**

a) Montrer que, pour tout $s \in \mathcal{S}_n$, s et son inverse ont même signature.

b) En déduire que, pour tout $n \geq 2$, $D(\mathcal{S}_n) \subset \mathcal{A}_n$.

c) Montrer finalement que $\mathcal{A}_4 = D(\mathcal{S}_4)$. (on pourra utiliser le calcul de la question 4), a).)

Université Paris Sud — Année 2004–2005

Licence MA — Algèbre Générale

TD n° II

Exercice A : (**Idéaux de $\mathbb{Z}$ et $\mathbb{K}[X]$**)

1) Montrer qu'une partie $I \subset \mathbb{Z}$ de $\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ si et seulement si I est un idéal de $(\mathbb{Z}, +, *)$.

2) Montrer qu'un idéal $I \subset \mathbb{Z}$ de $\mathbb{Z}$, possède un plus petit élément $d \in \mathbb{N}^*$; puis que

$$I = d\mathbb{Z} = \{dz\ ,\ z \in \mathbb{Z}\}\ .$$

3) **a)** Vérifier que l'ensemble $K[X]$ des polynômes à une indéterminée sur un corps K est un anneau (on pourra donner explicitement la somme et le produit de deux polynômes en fonction de leurs coefficients.)

b) Tout sous-groupe de $K[X]$ est-il un idéal de $K[X]$?

c) Déterminer les idéaux de $K[X]$.

d) Les sous-ensembles suivants de $K[X]$ sont-ils des idéaux :

—

$$E_0 := \{P \in K[X] | P(0) = 0\}$$

—

$$E_a := \{P \in K[X] | P(0) = a\}$$

pour tout $a \in K, a \neq 0$.

—

$$E'_0 := \{P \in K[X] | P'(0) = 0\}\ ?$$

Exercice B : (**Introduction à $\mathbb{Z}/n\mathbb{Z}$**)

1) **a)** Montrer que tout entier relatif divise 0 tandis que 0 ne divise que lui-même.

Pour tout entier naturel n on définit la *relation de congruence modulo* n sur $\mathbb{Z}$ par a congrue à b modulo n si n divise $b - a$ et l'on écrit

$$a \equiv b\ [n]\ .$$

b) Montrer que la relation de congruence modulo n est une relation d'équivalence.

On notera $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence pour la relation de congruence modulo n, qu'on abrègera en *Classes de congruence modulo* n.

Pour tout $a \in \mathbb{Z}$, on notera $\pi_n(a)$ ou $\overline{a}$ la classe de a modulo n .

c) **a)** Montrer que $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est une application surjective. On 'lappelle usuellement *surjection canonique*.

b) Est-elle injective ?

d) Donner le cardinal de $\mathbb{Z}/n\mathbb{Z}$.

e) Un entier naturel n étant fixé, montrer que, pour tout quadruplet (a, b, a', b') d'entiers relatifs,

$$a \equiv a' [n] \text{ et } b \equiv b' [n] \Rightarrow a + b \equiv a' + b' [n] .$$

f) Sous les mêmes hypothèses qu'à la question précédente, montrer que

$$a \equiv a' [n] \text{ et } b \equiv b' [n] \Rightarrow ab \equiv a' * b' [n] .$$

2) (L'addition sur $\mathbb{Z}/n\mathbb{Z}$)
Pour tout entier $n \geq 2$, on note

$\mathbb{Z}/n\mathbb{Z}$ **l'ensemble des classes de congruence modulo** n
et $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ **la surjection canonique (cf. question 1).)**

a) Montrer que l'on définit bien une loi interne

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

en posant, pour tout couple (α, β) d'éléments de $\mathbb{Z}/n\mathbb{Z}$,

$$\alpha + \beta := \overline{a + b}$$

où

$\overline{a + b}$ est la classe de congruence modulo n de la somme $a + b$

pour a (resp. $b,$) n'importe quel représentant de α (resp. β .)

b) Montrer que $+$ ainsi définie sur $\mathbb{Z}/n\mathbb{Z}$ est associative, possède un élément neutre qu'on déterminera, que tout élément possède un opposé et que $+$ est commutative.

c) Montrer que la loi $+$ ainsi définie sur $\mathbb{Z}/n\mathbb{Z}$ est la seule telle que π_n soit un morphisme de groupes.

3) (La multiplication sur $\mathbb{Z}/n\mathbb{Z}$)
Pour tout entier $n \geq 2$, on note

$\mathbb{Z}/n\mathbb{Z}$ **l'ensemble des classes de congruence modulo** n
et $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ **la surjection canonique (cf. question 1).)**

a) Même question qu'en question 2) pour la multiplication $*$.

b) Montrer que la multiplication $*$ sur $\mathbb{Z}/n\mathbb{Z}$ est associative, possède un élément neutre que l'on déterminera et que $*$ est commutative.

c) Montrer que $*$ est distributive sur $+$. On dira que $(\mathbb{Z}/n\mathbb{Z}, +, *)$ a une structure d'*anneau commutatif*. Connaissez-vous d'autres anneaux commutatifs ?

d) Tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ ont-ils un inverse pour $*$?

e) Donner un analogue au question 2), c) pour $*$.

f) Montrer que $\pi_n \,:\, \mathbb{Z} \,\to\, \mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneaux et que c'est le seul.

4) **a)** Montrer que les lois $+_n$ et $*_n$ définies à l'question 1) donnent à $\mathbb{Z}/n$ une structure d'anneau.

b) Cette structure est-elle "raisonnablement" unique ?

c) L'anneau $(\mathbb{Z}/n, +_n, *_n)$ est-il commutatif ?

Exercice C : (Polynômes)

En dépit de ce que pourait laisser penser le titre de cet exercice, aucune connaissance concernant les polynômes n'est nécessaire.

Soit $(A, +, *)$ **un anneau commutatif dont on note** 0 **l'élément neutre pour** $+$ **et** 1 **l'élément neutre pour** $*$. **On note** $A^{\mathbb{N}}$ **l'ensemble des suites à valeurs dans** A **ou encore de manière équivalente l'ensemble des applications de** $\mathbb{N}$ **dans** A. **Pour tout** $a \,\in\, A^{\mathbb{N}}$, **on note** a_n **le** $n^{\text{ième}}$ **terme de** a ***i.e.*** **la valeur de** a **en** $n \,\in\, \mathbb{N}$.

1) (**Addition**)

Pour tout $(a, b) \,\in\, A^{\mathbb{N}} \times A^{\mathbb{N}}$, **on définit l'élément** $a +_{A^{\mathbb{N}}} b \in A^{\mathbb{N}}$ **par** $(a +_{A^{\mathbb{N}}} b)_n \,:=\, a_n + b_n$.

Montrer que $(A^{\mathbb{N}},\, +_{A^{\mathbb{N}}})$ ainsi construit est un groupe abélien dont on précisera l'élément neutre z.

Dorénavant on notera simplement $+$ **pour** $+_{A^{\mathbb{N}}}$ **si aucune confusion n'est à craindre.**

2) (**Multiplication**)

Pour tout $(a, b) \in A^{\mathbb{N}} \times A^{\mathbb{N}}$, **on définit** $a *_{A^{\mathbb{N}}} b$ **par**

$$(a *_{A^{\mathbb{N}}} b)_n \,:=\, \sum_{k=0}^{n} a_k * b_{n-k}\ .$$

Montrer que :

a) l'élément $v \in A^{\mathbb{N}}$ défini par

$$v_0 \,:=\, 1 \text{ et } \forall n \in \mathbb{N},\ n \geq 1 \,\Rightarrow\, v_n \,:=\, 0,$$

est un élément neutre pour $*_{A^{\mathbb{N}}}$;

b)

$$\forall (a, b) \in A^{\mathbb{N}} \times A^{\mathbb{N}},\ a *_{A^{\mathbb{N}}} b \,=\, b *_{A^{\mathbb{N}}} a\ ;$$

c)

$$\forall (a, b, c) \in A^{\mathbb{N}} \times A^{\mathbb{N}} \times A^{\mathbb{N}},\ a *_{A^{\mathbb{N}}} (b +_{A^{\mathbb{N}}} c) \,=\, a *_{A^{\mathbb{N}}} b +_{A^{\mathbb{N}}} a *_{A^{\mathbb{N}}} c\ .$$

De même on notera $*$ **au lieu de** $*_{A^{\mathbb{N}}}$ **si aucune confusion n'est à craindre.**

3) (**Anneau**)

Énoncer sans démonstration les propriétés de $+_{A^{\mathbb{N}}}$ et $*_{A^{\mathbb{N}}}$ qui font de

$$(A^{\mathbb{N}},\, +_{A^{\mathbb{N}}}\,,\, *_{A^{\mathbb{N}}}) \text{ un anneau commutatif .}$$

On admettra dans la suite celles de ces propriétés qui n'auraient pas été démontrées auparavant.

4) (**Valuation**)

a) Rappeler ce que signifie que l'anneau A est intègre.

On suppose, dans toute la suite de la question 4) que $(A, +, *)$ est intègre.

b) Pour tout $a \in A^{\mathbb{N}}$, $a \neq \zeta$, montrer qu'il existe un plus petit entier $v \in \mathbb{N}$ tel que $a_v \neq 0$.

On notera désormais $\mathrm{val}(a)$ **l'entier** v **qu'on appellera la *valuation* de** a **et on adoptera les conventions suivantes :** $\mathrm{val}(\zeta) = (+\infty)$, $(+\infty) \leq (+\infty)$, $(+\infty) + (+\infty) = (+\infty)$

$$\forall n \in \mathbb{N},\ n + (+\infty) = (+\infty) \text{ et } n < (+\infty)\ .$$

c) Montrer que

$$\forall (a, b) \in A^{\mathbb{N}} \times A^{\mathbb{N}},\ \mathrm{val}(a *_{A^{\mathbb{N}}} b) = \mathrm{val}(a) + \mathrm{val}(b)\ ;$$

d) En déduire que $(A^{\mathbb{N}}, +_{A^{\mathbb{N}}}, *_{A^{\mathbb{N}}})$ est un anneau intègre.

e) Montrer que

$$\forall (a, b) \in A^{\mathbb{N}} \times A^{\mathbb{N}},\ \mathrm{val}(a +_{A^{\mathbb{N}}} b) \geq \min(\mathrm{val}(a), \mathrm{val}(b))$$

avec égalité si $\mathrm{val}(a) \neq \mathrm{val}(b)$.

f) Montrer que

$$\mathfrak{m} := \{a \in A^{\mathbb{N}}\ ;\ \mathrm{val}(a) > 0\}$$

est un idéal de $A^{\mathbb{N}}$ dont on donnera une autre caractérisation.

5) (**Morphisme structural**)

Pour tout $a \in A$, **on définit l'élément** $i(a)$ **de** $A^{\mathbb{N}}$ **par**

$$i(a)_0 := a \text{ et } \forall n \in \mathbb{N},\ n > 0 \Rightarrow i(a)_n = 0\ .$$

Montrer que l'application $i : A \to A^{\mathbb{N}}$ ainsi définie est un morphisme injectif d'anneaux.

On note désormais

$$\mathcal{P} := \{a \in A^{\mathbb{N}}\ ;\ \exists n \in \mathbb{N},\ \forall p \in \mathbb{N},\ p \geq n \Rightarrow a_p = 0\}$$

le sous-ensemble de $A^{\mathbb{N}}$ **des suites « presque nulles » autrement dit dont le terme est nul à partir d'un certain rang.**

6) (**degré**)

On suppose encore dans cette question que A **est un anneau intègre.**

a) Montrer que, pour tout $a \in \mathcal{P}$, $a \neq \zeta$, il existe un entier $d \in \mathbb{N}$ tel que

$$a_d \neq 0 \text{ et } \forall n \in \mathbb{N},\ n > d \Rightarrow a_n = 0\ .$$

On notera désormais $\deg(a)$ **l'entier** d **qu'on appellera le *degré* de** a **et on adoptera les conventions suivantes :** $\deg(\zeta) = (-\infty)$, $(-\infty) \leq (-\infty)$, $(-\infty) + (-\infty) = (-\infty)$

$$\forall n \in \mathbb{N},\ n + (-\infty) = (-\infty) \text{ et } n > (-\infty)\ .$$

b) Montrer que

$$\forall (a, b) \in \mathcal{P} \times \mathcal{P},\ \deg(a *_{A^{\mathbb{N}}} b) = \deg(a) + \deg(b)\ .$$

c) Montrer que

$$\forall (a,b) \in \mathcal{P} \times \mathcal{P},\ \deg(a +_{A^{\mathbb{N}}} b) \ \leq\ \max(\deg(a), \deg(b))$$

avec égalité si $\deg(a) \neq \deg(b)$.

d) En déduire que $(\mathcal{P},\ +_{A^{\mathbb{N}}}\ ,\ *_{A^{\mathbb{N}}}\ )$ est un anneau commutatif intègre.

e) Montrer que

$$\mathfrak{m}_0\ :=\ \mathcal{P} \cap \mathfrak{m}$$

est un idéal de $\mathcal{P}$ (où $\mathfrak{m}$ est l'idéal de $A^{\mathbb{N}}$ défini à la question 4), f).)

f) Montrer que pour tout $(a,b)\ \in\ \mathcal{P}\ \times\ \mathcal{P}$, si b divise a et $a \neq \zeta$, $\deg(b)\ \leq\ \deg(a)$

g) Montrer que l'image du morphisme i défini à la question 5), est contenue dans $\mathcal{P}$ et que i est donc un morphisme injectif d'anneaux de A dans $\mathcal{P}$. Caractériser les éléments de $\mathrm{Im}\, i$ par leur degré.

h) Montrer que la restriction $i^{\times}\ :=\ i_{|A^{\times}}$ de i à l'ensemble $A^{\times}$ des éléments inversibles de A est un morphisme bijectif de groupes de $(A^{\times}, *)$ dans $(\mathcal{P}^{\times},\ *_{A^{\mathbb{N}}}\ )$
Indication : *on pourra penser à caractériser les éléments de $\mathcal{P}^{\times}$ en termes de degré.*

7) (**Division euclidienne**)

a) Rappeler ce que signifie l'assertion : A est un corps.

On suppose, jusqu'à la fin de question 7) que A est un corps.
Soit $b\ \in\ \mathcal{P}, b\ \neq\ \zeta$.

b) Montrer que pour tout $a\ \in\ \mathcal{P}$, si $\deg(a) < \deg(b)$, il existe $(q,r)\ \in\ \mathcal{P}\ \times\ \mathcal{P}$ tel que

$$a\ =\ b\ *_{A^{\mathbb{N}}} q\ +_{A^{\mathbb{N}}}\ r \text{ et } \deg(r)\ <\ \deg(b)\ .$$

c) Montrer que pour tout $a\ \in\ \mathcal{P}$, si $\deg(a)\ \geq\ \deg(b)$, il existe $(s,c)\ \in\ \mathcal{P}\ \times\ \mathcal{P}$ tel que

$$a\ =\ b\ *_{A^{\mathbb{N}}} s\ +_{A^{\mathbb{N}}}\ c \text{ et } \deg(c)\ <\ \deg(a)\ .$$

d) Montrer finalement que, pour tout $a\ \in\ \mathcal{P}$ il existe un unique $(q,r)\ \in\ \mathcal{P}\ \times\ \mathcal{P}$ tel que :

$$a\ =\ b *_{A^{\mathbb{N}}} q\ +_{A^{\mathbb{N}}} r \text{ et } \deg(r)\ <\ \deg(b)\ .$$

Exercice D : (**Anneau des entiers de GAUSS**)
Soit $\mathbb{Z}[i]$ **le sous-ensemble de** $\mathbb{C}$ **défini par**

$$\mathbb{Z}[i]\ :=\ \{a + ib\ ,\ a \in \mathbb{Z}\ ,\ b \in \mathbb{Z}\}\ \subset\ \mathbb{C}\ .$$

Il est muni des lois de multiplication $*$ **et d'addition** $+$ **déduites de celles du corps des complexes** $\mathbb{C}$.
On note $||z||$ **le module d'un nombre complexe** z **et** N **l'application** $z \mapsto ||z||^2$.

1) Montrer que $(\mathbb{Z}[i], +, *)$ est bien un anneau que l'on appellera *anneau des entiers de* GAUSS.

2) Déterminer les éléments inversibles de $\mathbb{Z}[i]$.

3) Soit β un nombre réel strictement positif et α un nombre complexe.

i Montrer que $||\alpha - \beta|| \geq ||\alpha||$si et seulement si $\mathrm{Re}(()\alpha) \leq \dfrac{\beta}{2}$ et de même que

$$\begin{aligned} ||\alpha - i\beta|| &\geq ||\alpha|| \Leftrightarrow \mathrm{Im}(()\alpha) \leq \frac{\beta}{2} \\ ||\alpha + \beta|| &\geq ||\alpha|| \Leftrightarrow \mathrm{Re}(()\alpha) \geq -\frac{\beta}{2} \\ ||\alpha + i\beta|| &\geq ||\alpha|| \Leftrightarrow \mathrm{Im}(()\alpha) \geq -\frac{\beta}{2} . \end{aligned}$$

ii En déduire que, si l'on suppose$||\alpha|| \geq \beta$, il existe k entier dans $[0, 3]$ tel que

$$||\alpha - i^k\beta|| < ||\alpha|| .$$

4) **a)** Soit deux éléments a et b de $\mathbb{Z}[i]$ avec$b$ non nul. Montrer que s'il existe des éléments q et r dans $\mathbb{Z}[i]$ vérifiant

$$a = bq + r \text{ et } ||r|| < ||b|| ,$$

alors

$$\mathcal{M} : ||q|| < \frac{||a||}{||b||} + 1 .$$

b) Montrer que l'ensemble $\mathcal{Q}$ des éléments$q \in \mathbb{Z}[i]$ vérifiant $\mathcal{M}$ est fini et non vide. On notera $q_0 \in \mathcal{Q}$ l'élément tel que $||a - bq||$ soit minimal.

c) Montrer qu'alors $||a - bq_0|| < ||b||$.

5) Déterminer les idéaux de $\mathbb{Z}[i]$.

Macros locales

Exercice E : (**Nombres algébriques**)

1) Soient K un corps et $f : K \to A$ une K-algèbre commutative.

a) Montrer que f munit A d'une structure de K-espace vectoriel.
Pour tout $a \in A$, **on note** m_a **la multiplication par** a **dans** A (***i.e.*pour tout** $b \in A$, $m_a(b) := ab$.)

b) Montrer que m_a est un endomorphisme de K-espace vectoriel pour la structure définie par f.

c) Montrer que si A est intègre m_a est injective pour tout $a \in A \setminus \{0_A\}$.

d) En déduire que si A est intègre et de dimension finie comme K-espace vectoriel, pour tout $a \in A$, m_a est un isomorphisme.

e) En déduire que si A est intègre et de dimension finie, A est un corps.

Pour tout sous-corps K **de** $\mathbb{C}$ **(c'est-à-dire toute sous-algèbre de** $\mathbb{C}$ **qui est un corps) et tout** $a \in \mathbb{C}$ **on notera**

$$K[a] := \{\sum_{k=0}^{r} x_k a^k \mid x_k \in K \; r \in \mathbb{N}\} .$$

Dans la suite, K **désigne un sous-corps quelconque de** $\mathbb{C}$.

2) Montrer que pour tout sous-corps K de $\mathbb{C}$ et tout $a \in \mathbb{C}$, $K[a]$ est une sous-K-algèbre de $\mathbb{C}$.

Pour $a \in \mathbb{C}$, **on dit que** a **est** K***-algébrique*** **s'il existe un polynôme** $P_a \in K[X]$, **tel que** $P_a(a) = 0$.

3) **a)** Que dire de l'ensemble

$$I_a := \{P \in K[X] \mid P(a) = 0\} \subset K[X] \,?$$

b) En déduire qu'il existe un unique $\mathfrak{I}rr_a \in K[X]$ unitaire tel que $\mathfrak{I}rr_a(a) = 0$ et pour tout $P \in K[X]$, $P(a) = 0$ si et seulement si il existe $R \in K[X]$, tel que $P = R * \mathfrak{I}rr_a$.

4) Montrer que $a \in \mathbb{C}$ est K-algébrique si et seulement si $K[a]$ est un K-espace vectoriel de dimension finie.

a) En déduire que $a \in \mathbb{C}$ est K-algébrique si et seulement si $K[a]$ est un corps.

5) Un nombre K-algébrique $a \in \mathbb{C}$ étant fixé, soit σ un automorphisme de K-algèbres de $K[a]$.

a) Montrer que σ est une application K-linéaire de $K[a]$ dans lui-même.

b) Montrer que σ est entièrement déterminé par l'image $\sigma(a)$ de a.

c) Montrer que nécessairement si α est une racine de $\mathfrak{I}rr_a$, il en est de même pour $\sigma(\alpha)$.

6) Un élément a de $\mathbb{C}$ étant fixé, montrer que s'il existe un sous-K-espace vectoriel de dimension finie E de $\mathbb{C}$, contenant $K[a]$ alors a est K-algébrique.

Soit (a, b) **un couple de nombres complexes** K**-algébriques :**

7) Montrer que b est $K[a]$-algébrique.

a) En déduire que $K[a][b]$ est un $K[a]$-espace vectoriel de dimension finie ; puis un K-espace vectoriel de dimension finie.

8) Déduire de la question précédente que $a + b$ et ab sont K-algébriques.

9) Conclure que l'ensemble des nombres complexes K-algébriques est un corps.

Université Paris Sud **Année 2004–2005**

Licence MA **Algèbre Générale**

TD n° III

Exercice A : **Soit** $(A, +, *)$ **un anneau commutatif et** I **un idéal de** A .

1) Montrer que A/I est un anneau intègre (resp. un corps) si et seulement si I est un idéal premier (resp. maximal.)

2) En déduire qu'un idéal maximal est premier. La réciproque est-elle vraie ?

Exercice B : **1)** Rappeler, en citant le résultat du cours, pourquoi on a un isomorphisme de $\mathbb{Z}$-algèbres

$$\phi \ := \ (\phi_3 \times \phi_5) \ : \ \mathbb{Z}/15 \ \to \ \mathbb{Z}/3 \ \times \ \mathbb{Z}/5 \, .$$

2) Montrer que l'équation $x^{15} \ = \ x$ d'inconnue $x \ \in \ \mathbb{Z}/15$ équivaut au système

$$S \ : \ \left(\begin{array}{ccc} y^{15} & = & y \\ z^{15} & = & z \end{array} \right)$$

d'inconnue $(y, z) \in \mathbb{Z}/3 \times \mathbb{Z}/5$ équivalant lui-même au système

$$S' \ : \ \left(\begin{array}{ccc} y^{3} & = & y \\ z^{3} & = & z \, . \end{array} \right)$$

a) Résoudre S' et donner les solutions de $x^{15} \ = \ x$ dans $\mathbb{Z}/15$.

Exercice C : **Soit** p **un nombre premier. On note** $\mathbb{F}_p \ := \ (\mathbb{Z}/p\mathbb{Z}, +, *)$ **le corps à** p **éléments dont on notera** 0 **et** 1 **l'élément neutre pour l'addition et la multiplication respectivement.**

1) Rappeler pourquoi $\mathbb{F}_p$ est un corps et ce que cela signifie.

2) **On suppose** $p \neq 2$; **et qu'il existe** $\alpha \in \mathbb{F}_p$ **tel que**

$$\alpha^2 + 1 \ = \ 0 \, .$$

a) Montrer que le sous-groupe multiplicatif de $({\mathbb{F}_p}^{\times}, *)$ engendré par α est de cardinal 4.

b) En déduire que $p \ \equiv \ 1 \ [4]$.

c) En déduire que les seules racines du polynôme $X^4 - 1$ dans $\mathbb{Z}/11\mathbb{Z}$ sont 1 et -1.

3) Donner les racines différentes de 1 du polynôme $X^4 - 1$ dans $\mathbb{Z}/5\mathbb{Z}$.

4) Résoudre dans $\mathbb{Z}/55\mathbb{Z}$ l'équation $x^3 + x^2 + x + 1 = 0$.

Exercice D : (Algorithme d'EUCLIDE et théorème de BÉZOUT)

Soient a et b des éléments de $\mathbb{Z}$. On note d leur Pgcd (ou encore $d = a \wedge b$.) On définit les deux suites à valeurs entières $\left(a_n\right)_{,n\in\mathbb{N}}$ et $\left(b_n\right)_{,n\in\mathbb{N}}$ par :

$$\begin{aligned} a_0 &= a, \\ b_0 &= b\,, \end{aligned}$$

et pour tout $n \in \mathbb{N}$, $a_{n+1} = b_n$ et b_{n+1} est le reste de la division euclidienne de a_n par b_n.

1) Montrer que pour tout $n \in \mathbb{N}$,

$$a_n \wedge b_n = a_{n+1} \wedge b_{n+1}.$$

2) Montrer que les suites a_n et b_n convergent vers le **Pgcd** d.

3) Déduire de ce qui précède un "algorithme" de calcul d'un couple d'entiers (u, v) tel que $d = au+bv$.

4) Montrer que deux entiers a et b sont premiers entre eux c'est-à-dire n'ont pas de diviseur commun (autre que 1 (cf. cours III.3.12)) si et seulement si les idéaux qu'ils engendrent sont comaximaux (cf. cours II.8.1).

5) a) Déterminer $(\mathbb{Z}/n)^\times$ pour un entier $n \geq 2$ ainsi que l'ensemble des générateurs du groupe ($\mathbb{Z}$-module) $(\mathbb{Z}/n, +)$ et faire une remarque.

b) Donner une condition nécessaire et suffisante sur l'entier n pour que l'anneau $(\mathbb{Z}/n, +, *)$ soit un corps.

Quel est alors le cardinal du groupe $((\mathbb{Z}/n)^\times, *)$?

Exercice E : (Automorphisme de FROBENIUS et petit théorème de FERMAT)

Soit p un nombre premier.

1) Montrer que le coefficient binomial $\binom{p}{k}$ est toujours divisible par p pour $0 < k < p$.

2) a) En déduire que l'application

$$\begin{array}{rccc} \phi : & \mathbb{F}_p & \to & \mathbb{F}_p \\ & a & \mapsto & a^p \end{array}$$

est un morphisme de groupes (où $\mathbb{F}_p$ est le corps premier $\mathbb{Z}/p$.)

b) Montrer que ϕ est un morphisme d'anneaux.

c) Montrer que ϕ est injectif.

d) En déduire que ϕ est un automorphisme.

3) Montrer que pour tout $a \in \mathbb{F}_p$, $\phi(a) = a$.

4) Déduire de la question précédente que tout $a \in \mathbb{F}_p$ est racine du polynôme $X^p - X \in \mathbb{F}_p[X]$ puis finalement que :

$$X^p - X = \prod_{a_i \in \mathbb{F}_p} (X - a_i)$$

dans $\mathbb{F}_p[X]$.

5) En déduire le **petit théorème de FERMAT :** *pour tout entier a non nul et tout nombre premier p, a^{p-1} congrue à 1 modulo p.*

Exercice F : (Critère D'eisenstein)

Soit P un polynôme unitaire à coefficients dans $\mathbb{Z}$, noté

$$P := \sum_{i=0}^{d-1} p_i X^i + X^d .$$

On suppose qu'il existe un nombre premier p tel que pour tout $0 \leq i \leq d-1$ p divise p_i ; et tel que p^2 ne divise pas $P(0)$.

On conviendra de noter, pour tout entier $n \in \mathbb{Z}$, $\overline{n}$ sa classe modulo p.

1) On suppose qu'il existe des polynômes de $\mathbb{Z}[X]$ dont les degrés respectifs d_Q et d_R sont supérieurs ou égaux à 1 :

$$Q := \sum_{i=0}^{d_Q} q_i X^i \text{ et } R := \sum_{i=0}^{d_R} r_i X^i$$

tels que $Q * R = P$.

a) Montrer que $\overline{q_{d_Q}}$ et $\overline{r_{d_R}}$ sont inversibles dans $\mathbb{Z}/p\mathbb{Z}$.

b) Montrer que si K est un corps les seuls diviseurs non inversibles du polynôme $X^d \in K[X]$ sont les polynômes λX^k avec $1 \leq k \leq d$ et $\lambda \in K^\times$.

c) En étudiant le produit $Q * R = P$, dans l'anneau $\mathbb{Z}/p\mathbb{Z}[X]$, montrer que $\overline{q_0} = \overline{r_0} = 0_{\mathbb{Z}/p\mathbb{Z}}$.

2) En déduire qu'alors finalement p^2 divise p_0 ce qui contredit l'hypothèse.

3) Déduire finalement de ce qui précède, que sous les hypothèses du début de l'exercice, P est irréductible.

Exercice G : (L'algorithme R.S.A.)

Pour un entier $n \geq 2$, on utilisera les notations suivantes :

— $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ **est la surjection canonique ;**

— $\phi(n)$ **est le nombre d'entiers inférieurs ou égaux à n et premiers avec n .**

On suppose dans la suite, que $n = pq$ et de plus que p et q sont deux nombres premiers impairs distincts. On posera $m := \phi(n) = (p-1)(q-1)$ et l'on choisira un nombre entier $2 < e < m$ premier à m .

1) a) Pour tout entier r premier à n calculer r^m modulo n . (Les résultats de théorie des groupes qu'on pourrait être amené à utiliser pour prouver ce résultat ne sont pas à redémontrer.)

b) Montrer (en citant un résultat du cours qu'on ne cherchera pas à démontrer,) qu'il existe un couple d'entiers $(d, k) \in \mathbb{N} \times \mathbb{Z}$ tel que $de \ + \ mk \ = \ 1$.

c) Déduire de la a) et de la b) que pour tout entier r premier à n,

$$r^{de} \ \equiv \ r \ [n] \ .$$

,

2) Les entiers $n = pq$, e et d sont comme à la question précédente. On note

$$E \ := \ \{k \ \in \ \mathbb{N} \, ; \ k < n \ , \ (n \wedge k) \ = \ 1\} \ ,$$

(où $n \wedge k$ désigne le Pgcd de n et k .)

a) Pour deux entiers a et b premiers à n montrer que ab est premier à n ; puis en déduire que pour tout r premier à n et tout entier k, r^k est premier à n et enfin que le reste de la division euclidienne de r^k par n est premier à n.

b) Montrer que l'application $\mathcal{C}$ qui à tout entier r associe le représentant compris (au sens large) entre 0 et $n - 1$, de la classe de r^e modulo n définit une application de E dans lui-même.

c) Montrer qu'il en est de même de l'application $\mathcal{D}$ qui à tout entier s associe le représentant compris (au sens large) entre 0 et $n - 1$, de la classe de s^d modulo n et que $\mathcal{D}$ est l'application réciproque de $\mathcal{C}$ sur E .

Université Paris Sud — Année 2004–2005

Licence MA — Algèbre Générale

Corrigé I

Exercice H de la feuille n° I

1) Si G est un groupe de cardinal $2k$ et $H \subset G$ un sous-groupe de cardinal k, H est d'indice 2 (cf. cours I.2.3.i)) et il est par conséquent distingué.

On peut donc former le quotient de G par H qui possède une structure de groupe canonique. G/H est un groupe à 2 éléments et par conséquent canoniquement isomorphe à $\mathbb{Z}/2$.

a) On a donc un morphisme de groupes surjectif canonique

$$\pi \ : \ G \ \to \ G/H \ = \ \mathbb{Z}/2$$

dont le noyau $\mathrm{Ker}\,\pi$ est précisément H . Pour tout $g \in G$,

$$\begin{aligned} \pi(g * g) &= \pi(g) +_{\mathbb{Z}/2} \pi(g) \\ &= 0_{\mathbb{Z}/2} \end{aligned}$$

c'est-à-dire que $g * g \in \mathrm{Ker}\,\pi \ = \ H$.

2) (cf. cours I.4.22.)

a) On sait qu'en général, pour $n \geq 2$,

$$\#(\mathcal{A}_n) \ = \ \frac{\#(\mathcal{S}_n)}{2} \ = \ \frac{n!}{2} \, .$$

Ici on a donc $\#(\mathcal{A}_4) \ = \ 12$.

3) Soit $n \geq 3$ un entier. Un cycle c de longueur 3 dans $\mathcal{S}_n$, a $\nu_c \ = \ n - 3 + 1 \ = \ n - 2$ orbites. Par conséquent

$$\sigma(c) \ \text{(cf. I.4.16,)} \ (-1)^{n-\nu_c} \ = \ (-1)^2 \ = \ 1$$

c'est-à-dire que $c \ \in \ \mathcal{A}_n$.

a) Toute partie à 3 éléments dans $\{1;2;3;4\}$ est le support d'au moins un cycle de longueur 3 . Ces parties sont au nombre de 4 .

b) Étant donnée une partie $\{a;b;c\} \ \subset \ \{1;2;3;4\}$, Les deux cycles suivants sont les seuls dont $\{a;b;c\}$ est le support :

$$c_1 \ = \ \begin{matrix} a & b & c \\ c & a & b \end{matrix}$$

$$c_2 \ = \ \begin{matrix} a & b & c \\ b & c & a \end{matrix}$$

c) On déduit des deux questions précédentes qu'il y a $4 * 2 \ = \ 8$ cycles de longueur 3 dans $\mathcal{A}_4$.

4) Étant donné $\{a;b;c\} \subset [1;4]$, on a :

$$\begin{aligned}((a,b)\circ(b,c))^2(a) &= ((a,b)\circ(b,c)\circ(a,b))(a)\\ &= ((a,b)\circ(b,c))(b)\\ &= (a,b)(c)\\ &= c\\ ((a,b)\circ(b,c))^2(b) &= a\\ ((a,b)\circ(b,c))^2(c) &= b\,.\end{aligned}$$

Il est clair que, pour tout $x \in [1;4]$, $x \notin \{a;b;c\}$ $((a,b)\circ(b,c)^2(x) = x$ d'où l'on déduit que

$$((a,b)\circ(b,c))^2 = \begin{matrix}a & b & c\\ c & a & b\end{matrix} = (a,b,c)\,.$$

a) D'après la question 3), b), tout 3-cycle c dans $\mathcal{A}_4$ de support $\{a;b;c\} \subset [1;4]$, est :
— soit $(a,b,c) = ((a,b)\circ(b,c))^2$
— soit $(a,b,c)^2 = (((a,b)\circ(b,c))^2)^2$
d'après la question précédente.

b) On a vu à la question 1), a) que, si H est un sous-groupe d'indice 2 de $\mathcal{A}_4$, il contient tous les carrés d'éléments de $\mathcal{A}_4$. Par conséquent, d'après la question précédente, il contient tous les 3-cycles.

c) Si $\mathcal{A}_4$ possédait un sous-groupe d'ordre 6, celui-ci serait d'indice 2 (cf. question 2), a)) et, d'après la question précédente, contiendrait donc tous les 3-cycles de $\mathcal{A}_4$. Or d'après la question 3), c), ces derniers sont au nombre de 8 ce qui est contradictoire.

Le groupe alterné $\mathcal{A}_4$ n'a donc pas de sous-groupe d'ordre 6 .

5) Tout élément de $\mathcal{S}_4$ différent de l'identité se décompose de manière unique en un produit de cycles à supports deux à deux disjoints (cf. cours I.4.12) ce qui permet de définir le type cyclique d'un élément. La signature d'un élément se calculant en fonction du nombre d'orbites, est clairement une fonction du type cyclique. On donne, dans le tableau suivant, les différents types cycliques possibles pour les éléments de $\mathcal{S}_4$ et s'ils correspondent ou non à des éléments de $\mathcal{A}_4$:

$$\begin{aligned}(2) &\notin \mathcal{A}_4\\ (2,2) &\in \mathcal{A}_4\\ (3) &\in \mathcal{A}_4\,.\end{aligned}$$

Ceci répond à la question.

a) Pour $\{a;b;c;d\} = [1;4]$, on a :

$$\begin{aligned}(a,b,c)\circ(b,c,d)(a) &= b\\ (a,b,c)\circ(b,c,d)(b) &= a\\ (a,b,c)\circ(b,c,d)(c) &= d\\ (a,b,c)\circ(b,c,d)(d) &= c\,;\end{aligned}$$

c'est-à-dire que

$$(a,b,c)\circ(b,c,d) = (a,b)\circ(c,d)\,.$$

b) Pour tout 3-cycle c, $c^3 = \mathrm{Id}$. Tout élément de $\mathcal{A}_4$ différent de Id étant, d'après la question 5), soit de type cyclique (3) donc un 3-cycle soit de type cyclique $(2,2)$ donc produit de 2 3-cycles d'après la a), on en déduit que $\mathcal{A}_4$ est engendré par les 3-cycles.

6) Si $(G,*)$ est un groupe abélien, pour tout couple (g,h) d'éléments de G,

$$\begin{aligned}[g,h] &= g*h*g^{-1}*h^{-1}\\ &= g*h*h^{-1}*g^{-1}\\ &= e_G\ .\end{aligned}$$

Il en résulte que, si G est abélien, $D(G) = \{e_G\}$.

a) — Pour $k \in G$ fixé, il suffit de remarquer que l'application $g \mapsto g^k$ pour $g \in G$, est un endomorphisme du groupe c'est-à-dire que $(g*h)^k = g^k * h^k$ pour tout couple (g,h) d'éléments de G . Il en résulte que, pour tout $g \in G$ $(g^{-1})^k = (g^k)^{-1}$ puis finalement, par un calcul très élémentaire que

$$\dagger\ :\ [g,h]^k = [g^k,h^k]\ \forall\,(g,h,k) \in G\times G\times G\ .$$

— Pour tout $x \in D(G)$, il existe $g_{i\ ,1\le i\le d} \in G$ et $h_{i\ ,1\le i\le d} \in G$ tels que

$$x = \prod_{i=1}^{d}[g_i,h_i]\ .$$

Du fait que $g \mapsto g^k$ est un endomorphisme de G et du résultat $\dagger$, on déduit que

$$x^k = \prod_{i=1}^{d}[g_i^k,h_i^k] \in D(G)\ ;$$

ce qui prouve que $D(G)$ est normal.

7) Pour tout entier $n \ge 2$, la signature $\sigma : \mathcal{S}_n \to \{-1;1\}$ est un morphisme de groupes (cf. cours I.4.20.) Or dans $(\{-1;1\},*)$ tout élément étant son propre inverse, on a

$$\sigma(s^{-1}) = \sigma(s)^{-1} = \sigma(s)\ .$$

On pourrait aussi remarquer que s et s^{-1} ont exactement les mêmes orbites donc la même signature.

a) Pour tout $n \ge 2$ et tout couple (s_1,s_2) d'éléments de $\mathcal{S}_n$, comme σ est un morphisme de groupes,

$$\sigma([s_1,s_2]) = [\sigma(s_1),\sigma(s_2)] \in (\{-1;1\},*) = (\mathbb{Z}/2,+)\ .$$

Ce dernier groupe étant abélien, d'après question 6), $[\sigma(s_1),\sigma(s_2)] = 1$; ce qui prouve que $D(\mathcal{S}_n) \subset \mathcal{A}_n$.

b) Il faut donc finalement montrer que tout élément de $\mathcal{A}_4$ s'écrit comme un produit de $[s_i,s_i']$ pour s_i et s_i' dans $\mathcal{S}_4$.

Or on a vu, à la question 5), b), que $\mathcal{A}_4$ est engendré par les 3-cycles. Par ailleurs on a vu à la question 4) que, pour toute partie $\{a;b;c\} \subset [1;4]$,

$$\begin{aligned}(a,b,c) &= (a,c,b)^2\\ &= (((a,b)\circ(b,c))^2)^2\\ &= [(a,b),(b,c)]^2\ ;\end{aligned}$$

ce qui prouve le résultat demandé.

Université Paris Sud **Année 2004–2005**

Licence MA **Algèbre Générale**

Problème n° II

5 janvier 2005

Soit A un anneau commutatif, K, M, Q des A-modules de type fini (c'est-à-dire engendrés par un nombre fini d'éléments,) $i : K \to M$ et $p : M \to Q$ des morphismes de A-modules. On suppose de plus :

$\mathcal{H}_1$ **Le morphisme i est injectif ;**

$\mathcal{H}_2$ **le morphisme p est surjectif ;**

$\mathcal{H}_3$ $\operatorname{Im} i = \operatorname{Ker} p$ **que l'on notera I .**

On note $\pi : M \to M/I$ la surjection canonique.

1) Montrer qu'il existe un unique isomorphisme de A-modules $u : M/I \to Q$ tel que

$$u \circ \pi = p .$$

2) Supposons $\mathcal{H}_4$: Il existe un morphisme de A-modules $s : Q \to M$ tel que $p \circ s = \mathrm{Id}_Q$. On note alors $J := \operatorname{Im} s$.

a) À quelle condition sur I a-t-on $s \circ p = \mathrm{Id}_M$?

b) Calculer $I \cap J$.

c) Vérifier que, pour tout $x \in M$, $x = x - s[p(x)] + s[p(x)]$ et en déduire que

$$M = I \oplus J .$$

d) Montrer que s est injectif et construire un isomorphisme de A-modules de $M/I \times K$ dans M .

3) On suppose dans cette question, que A est un corps.

a) Que dire de K, M, Q et I sous cette hypothèse ?

b) Montrer qu'alors l'hypothèse $\mathcal{H}_4$ est toujours satisfaite. (On pourra penser à justifier l'existence d'un sous-A-module J de M tel que $I \oplus J = M$ et à en déduire une construction de s .)

4) Étant donné un isomorphisme de groupes $f : G \to H$, montrer que pour tout $x \in G$, x et $f(x)$ ont même ordre.

5) Construire un morphisme de $\mathbb{Z}$-modules injectif $i : \mathbb{Z}/2 \to \mathbb{Z}/4$ dont on notera I l'image.

6) Que vaut le quotient $Q := (\mathbb{Z}/4)/I$?

7) Calculer l'ordre des éléments de $\mathbb{Z}/4$ et de $\mathbb{Z}/2 \times Q$ puis en déduire que $\mathcal{H}_4$ ne peut être vérifiée.

Université Paris Sud — Année 2004–2005

Licence MA — Algèbre Générale

Corrigé II

1) (cf. cours II.6.2.)

2) **a)** Comme l'on suppose déjà $\mathcal{H}_4$ *i.e.*$p \circ s = \mathrm{Id}_Q$, si l'on suppose de plus que $s \circ p = \mathrm{Id}_M$, p et s sont, par définition (cf. cours II.3.14,) des isomorphismes. Or p étant supposé surjectif, d'après l'hypothèse $\mathcal{H}_2$, p est un isomorphisme si et seulement s'il est injectif ce qui équivaut à ce que son noyau I soit le singleton $\{0\}$.

b) Pour tout $x \in M$, $x \in I \cap J$ si et seulement s'il existe $y \in Q$ tel que $x = s(y)$ et $p(x) = 0$. Ceci implique en particulier que $p[s(y)] = 0$. Or, d'après $\mathcal{H}_4$, $p[s(y)] = y$ d'où $y = 0$; ce qui implique, par linéarité de s que

$$x = s(y) = 0 \, ;$$

c'est-à-dire finalement

$$I \cap J = \{0\} \, .$$

c) Il est clair que, pour tout $x \in M$, $x = x - s[p(x)] + s[p(x)]$ avec $s[p(x)] \in \operatorname{Im} s = J$ et

$$\begin{array}{rcl} p[x - s[p(x)]] & = & p(x) - p[s[p(x)]] \\ & \overset{=}{\mathcal{H}_4} & p(x) - p(x) \\ & = & 0 \, ; \end{array}$$

c'est-à-dire que $x - s[p(x)] \in \operatorname{Ker} p = I$.

Cette décomposition est unique, d'après la question précédente.

d) — Pour tout $x \in Q$,

$$\begin{array}{rcl} s(x) & = & 0 \\ \Rightarrow \quad p[s(x)] & = & 0 \\ \overset{\Rightarrow}{\mathcal{H}_4} \qquad x & = & 0 \, ; \end{array}$$

c'est-à-dire que s est injectif.

—

— En utilisant la proposition II.6.2, on obtient un isomorphisme $v : M/I \to Q$.
Définissons

$$\begin{array}{rccl} w : & M/I \times K & \to & M \\ & (x, y) & \mapsto & s[v(x)] + i(y) \, . \end{array}$$

Vérifions :

— Pour tout (x, y) et tout (x', y') éléments de $M/I \times K$, et tout couple (a, a') d'éléments de A,

$$\begin{array}{lll} w(a(x,y) + a'(x',y')) & \overset{=}{\text{(cf. II.7.3,)}} & w(ax + a'x', ay + a'y') \\ & = & s[v(ax + a'x')] + i(ay + a'y') \\ & \overset{=}{s, v, i \text{ sont des morphismes}} & a\big(s[v(x)] + i(y)\big) + a'\big(s[v(x')] + i(y')\big) \\ & = & aw((x,y)) + a'w((x',y')) \, ; \end{array}$$

c'est-à-dire que w est linéaire.

— Pour tout $x \in M$, l'équation d'inconnue $(\xi, \eta) \in M/I \times K$,

$$\mathcal{E} \ : \ w((\xi,\eta)) \ = \ x$$

équivaut, par définition de w, à

$$s[v(\xi)] \ + \ i(\eta) \ = \ x \ .$$

Or $i(\eta) \in I$ et $s[v(\xi)] \in \operatorname{Im} s \ = \ J$ et d'après la c), il existe un unique couple $(y, z) \in I \times J$ tel que $x \ = \ y + z$.
Par conséquent, l'équation $\mathcal{E}$ équivaut au système

$$\mathcal{S} \ : \ \left(\begin{array}{rcl} i(\eta) & = & y \\ s[v(\xi)] & = & z \end{array} \right) .$$

D'après les hypothèses $\mathcal{H}_1$ et $\mathcal{H}_3$, i est un isomorphisme de K sur I et la première équation de $\mathcal{S}$ a, par conséquent, une unique solution.
Par définition même de $J \ = \ \operatorname{Im} s$ et du fait que s est injectif, s définit un isomorphisme de Q sur J . Comme v est un isomorphisme, la deuxième équation de $\mathcal{S}$ a également une unique solution ; c'est-à-dire que $\mathcal{S}$ a une unique solution ; autrement dit w est bijectif donc un isomorphisme de A-modules.

3) Si A est un corps, K, M, Q et I sont des A-espaces vectoriels de dimension finie (cf. cours II.3.13.) De plus I est un sous-espace vectoriel de M .

a) S'il existe s vérifiant $\mathcal{H}_4$, on a vu (cf. question 2), c)) que $M \ = \ I \ \oplus \ \operatorname{Im} s$. Ainsi la donnée de s détermine un supplémentaire de I . Or si M est un A-espace vectoriel de dimension finie et I un sous-espace de M, I admet des supplémentaires dans M . Le cas le plus favorable serait que chacun d'entre eux permette de construire un morphisme s vérifiant $\mathcal{H}_4$. Sans indication supplémentaire, on peut toujours chercher à construire s pour un supplémentaire arbitraire J de I .

Supposons donc donnés $J \ \subset \ M$ et $s \ : \ Q \ \to \ M$ tels que :

i $M \ = \ J \ \oplus \ I$;

ii $\operatorname{Im} s \ = \ J$;

iii $p \ \circ \ s \ = \ \operatorname{Id}_Q$.

Pour tout $x \ \in \ Q$, la condition (iii) implique que $p[s(x)] \ = \ x$ *i.e.*$s(x) \in F_x \ := \ p^{-1}(\{x\})$.

Le cas le plus favorable serait donc celui où, pour tout $x \ \in \ Q$, $J \cap F_x$ serait un singleton. Dans ce cas en effet, s serait entièrement déterminé et il ne resterait plus à vérifier que c'est un morphisme.

Étudions $F_x \cap J$.

— Étant donnés deux éléments ξ et η de $F_x \cap J$, $\xi - \eta \in J$ car J est un sous-espace de M . Or

$$\begin{array}{rcl} p(\xi - \eta) & = & p(\xi) - p(\eta) \\ & = & x - x \\ & = & 0 \ . \end{array}$$

Par conséquent $\xi - \eta \in \operatorname{Ker} p \ = \ I$ d'après $\mathcal{H}_3$. Or $I \cap J \ = \ \{0\}$ d'où finalement $\xi \ = \ \eta$. Il en résulte que $F_x \cap J$ contient au plus un élément.

— Par ailleurs, p est surjectif c'est-à-dire que F_x est non vide pour tout $x \in Q$. Soit donc $\xi \in F_x$. Comme $M \ = \ I \ \oplus \ J$ et $\xi \in M$, il existe un unique $(y, z) \in I \times J$, tel que $\xi \ = \ y + z$. Or

$$\begin{array}{rcl} p(z) & = & p(\xi - y) \\ & \underset{y \in I}{=} & p(\xi) \\ & = & x \ ; \end{array}$$

c'est-à-dire que $z \in F_x$; d'où $z \in F_x \cap J$; c'est-à-dire que $F_x \cap J$ contient au moins un élément.

On a donc montré que pour tout supplémentaire J de I et tout élément $x \in Q$, $F_x \cap J$ contient un unique élément. Si donc s existe, $\{s(x)\} = F_x \cap J$. Il est tautologique qu'alors, $p[s(x)] = x$. En revanche, rien ne prouve que s soit un morphisme.

Soit donc (x, y) un couple d'éléments de Q et (a, b) un couple d'éléments de A .

Soit $\xi := s(x)$ et $\eta = s(y)$. On a :

$$\begin{array}{lll} p(a\xi + b\eta) & \overset{=}{p \text{ est un morphisme}} & ap(\xi) + bp(\eta) \\ & = & ap[s(x)] + bp[s(y)] \\ & = & ax + by \ ; \end{array}$$

c'est-à-dire que $a\xi + b\eta \in F_{ax+by}$. Par ailleurs $\xi \in J$ et $\eta \in J$. Or J étant un sous-espace de M, $a\xi + b\eta \in J$. D'où $a\xi + b\eta \in F_{ax+by} \cap J$ c'est-à-dire, par définition même de s,

$$\begin{array}{rcl} a\xi + b\eta & = & s(ax + by) \\ \Leftrightarrow \quad as(x) + bs(y) & = & s(ax + by) \ ; \end{array}$$

c'est-à-dire que s est un morphisme.

On constate donc, a posteriori, qu'il n'y a aucun choix à faire sur le supplémentaire J de I et que, celui-ci une fois choisi, s est entièrement déterminé et vérifie $\mathcal{H}_4$.

Remarquons que, sans tenir compte de l'indication de l'énoncé, on pouvait remarquer que le A-espace vectoriel Q étant de dimension finie, possède une base $(q_1, \ldots, q_d)$. Le morphisme p étant surjectif, il existe, pour tout $1 \leq i \leq d$ un élément $m_i \in p^{-1}(\{q_i\})$.

L'unique morphisme $s : Q \to M$ défini par $s(q_i) = m_i$ satisfait $\mathcal{H}_4$.

4) Pour $f : G \to H$ un isomorphisme de groupes, tout $x \in G$ et tout $n \in \mathbb{Z}$,

$$\begin{array}{lll} & x^n & = e_G \\ f \overset{\Leftrightarrow}{\text{injectif}} & f(x^n) & = f(e_G) \\ f \overset{\Leftrightarrow}{\text{est un morphisme}} & f(x)^n & = e_H \ ; \end{array}$$

ce qui prouve que x et $f(x)$ ont même ordre.

On remarque que le fait que f soit bijectif n'est pas utilisé ici mais seulement le fait qu'il est injectif.

5) S'il existe un morphisme de groupes $i : \mathbb{Z}/2 \to \mathbb{Z}/4$ nécessairement $i(0) = 0$ (cf. cours I.1.9.i).) Par ailleurs, on a remarqué à la question 4) qu'un morphisme injectif conserve l'ordre des éléments. Or $1_{\mathbb{Z}/2}$ est d'ordre 2 . Dans $\mathbb{Z}/4$, 1 et 3 sont d'ordre 4 tandis que 2 est d'ordre 2 . On aura donc nécessairement $i(1_{\mathbb{Z}/2}) = 2_{\mathbb{Z}/4}$; c'est-à-dire que

$$I := \operatorname{Im} i = \{0; 2\} \ .$$

a) Le sous-$\mathbb{Z}$-module I de $\mathbb{Z}/4$ est, en particulier un sous-groupe normal de $\mathbb{Z}/4$ et, par conséquent, d'après la proposition I.2.2.iv) le quotient $Q := (\mathbb{Z}/4)/I$ est un groupe abélien de cardinal 2 et par conséquent canoniquement isomorphe à $\mathbb{Z}/2$.

b) L'ordre des éléments de $\mathbb{Z}/4$ a été donné à la question 5). Par ailleurs

$$\mathbb{Z}/2 \times Q = \mathbb{Z}/2 \times \mathbb{Z}/2$$

d'après la question précédente. Dans ce dernier groupe tous les éléments différents de 0 sont d'ordre 2 .

Si donc $\mathcal{H}_4$ était vérifiée avec :

$$\begin{array}{rcl} K & = & \mathbb{Z}/2 \\ Q & = & M/I = \mathbb{Z}/2 \end{array}$$

on pourrait, d'après la question 2), d), construire un isomorphisme de $\mathbb{Z}$-modules *i.e.*de groupes)

$$\mathbb{Z}/2 \times \mathbb{Z}/2 \cong \mathbb{Z}/4$$

ce qui serait en contradiction avec le résultat établi en question 4).

L'intérêt de ce problème consiste bien évidemment à comparer les résultats obtenus en question 5), b) et question 3), a) pour comprendre quel genre de propriétés les espaces vectoriels peuvent avoir que n'ont pas des modules de type plus général.

Université Paris Sud **Année 2004–2005**

Licence MA **Algèbre Générale**

Problème n° IV

13 janvier 2005

Indicatrice d'EULER

Soit $n \in \mathbb{N}^*$ un entier naturel. On note $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la surjection canonique.

1) Pour $a \in \mathbb{Z}$, un entier relatif, montrer que les trois assertions suivantes sont équivalentes :

i) a est premier à n.

ii) $\pi_n(a) \in \mathbb{Z}/n\mathbb{Z}^\times$.

iii) $\pi_n(a)$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

Pour tout entier $n \in \mathbb{N}^*$, on notera désormais $\phi(n)$ qu'on appelle l'*indicatrice d'Euler* de n, le nombre d'entiers naturels inférieurs ou égaux à n premiers à n, ou, ce qui revient au même, le nombre de générateurs du groupe abélien $(\mathbb{Z}/n\mathbb{Z}, +)$, ou encore le cardinal de $\mathbb{Z}/n\mathbb{Z}^\times$.

2) Pour trois entiers relatifs a, b, c montrer que a est premier à bc si et seulement si a est premier à b et a est premier à c.

3) Soit p un nombre premier, et $\alpha \in \mathbb{N}^*$; déterminer le nombre $\phi(p^\alpha)$ des entiers naturels inférieurs ou égaux à p^α et premiers avec p^α.

On note

$$n = \prod_{i=1}^{i=d} p_i^{\alpha_i}$$

(où les p_i ,$1 \leq i \leq d$ sont des nombres premiers deux à deux distincts, et les α_i ,$1 \leq i \leq d$ sont des entiers supérieurs ou égaux à $1,$) la *décomposition en produit de facteurs premiers* de n.

4) Montrer qu'un entier relatif a est inversible modulo n si et seulement s'il est inversible modulo $p_i^{\alpha_i}$ pour tout $1 \leq i \leq d$.

5) En déduire que

$$\phi(n) = \prod_{i=1}^{d} \phi(p_i^{\alpha_i}) \, .$$

6) Donner tous les entiers n dont l'indicattrice d'Euler $\phi(n)$ est égal à 12 et donner l'indicatrice d'Euler de 480.

7) Soit H un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$.

a) Montrer qu'il existe un entier $d \in \mathbb{N}$ tel que $\pi_n^{-1}(H) = d\mathbb{Z}$ et $d|n$.

b) En déduire que π_n induit un isomorphisme de groupes $\mathbb{Z}/d\mathbb{Z}' \cong H$ avec $dd' = n$.

c) En déduire que pour tout d tel que $d|n$, $(\mathbb{Z}/n\mathbb{Z}, +)$ contient un et un seul sous-groupe de cardinal d et que celui-ci est cyclique isomorphe à $\mathbb{Z}/d\mathbb{Z}$.

8) a) On note A_d l'ensemble des éléments d'ordre d dans $(\mathbb{Z}/n\mathbb{Z}, +)$. Montrer que

$$\mathbb{Z}/n\mathbb{Z} = \bigcup_{d|n} A_d \, .$$

b) En déduire que

$$n = \sum_{d|n} \phi(d) \, .$$

Université Paris Sud — Année 2004–2005

Licence MA — Algèbre Générale

Corrigé III

Pour un entier $n \in \mathbb{Z}$ non nul, on notera $\pi_n : \mathbb{Z} \to \mathbb{Z}/n$ la surjection canonique (cf. cours II.5.) Soit $n \in \mathbb{Z}$ non nul. Un entier $m \in \mathbb{Z}$ est le représentant d'un générateur du groupe $(\mathbb{Z}/n, +)$ c'est-à-dire du $\mathbb{Z}$-module $\mathbb{Z}/n$ si et seulement si, pour tout $k \in \mathbb{Z}$, il existe un entier $l \in \mathbb{Z}$ tel que

$$\begin{array}{rrcl} & l \cdot_{\mathbb{Z}/n} \pi_n(m) & = & \pi_n(k) \\ \Leftrightarrow & \pi_n(l) *_{\mathbb{Z}/n} \pi_n(m) & = & \pi_n(k) \\ \Leftrightarrow & \pi_n(l * m) & = & \pi_n(k) \\ \Leftrightarrow & \pi_n(l * m - k) & = & 0_{\mathbb{Z}/n} \\ \Leftrightarrow & l * m - k & \in & \operatorname{Ker} \pi_n \ = \ n\mathbb{Z} \, . \end{array}$$

Ceci implique, en particulier, pour $k = 1$, qu'il existe un couple $(l, l') \in \mathbb{Z} \times \mathbb{Z}$ tel que $l * m - 1 = l' * n$, c'est-à-dire que $(m) := m\mathbb{Z}$ et $(n) := n\mathbb{Z}$ sont comaximaux ou encore que m et n sont premiers entre eux ou encore, que $\pi_n(m)$ et $\pi_n(l)$ sont inverses l'un de l'autre dans $\mathbb{Z}/n$.

Réciproquement, si m est premier avec n *i.e.*si $\pi_n(m)$ est inversible dans $\mathbb{Z}/n$, il existe $l \in \mathbb{Z}$ tel que

$$\begin{array}{rrcl} & \pi_n(l) *_{\mathbb{Z}/n} \pi_n(m) & = & 1_{\mathbb{Z}/n} \\ \Leftrightarrow & 1_{\mathbb{Z}/n} & = & \pi_n(l * m) \\ \Rightarrow & \forall k \in \mathbb{Z} \; k \cdot_{\mathbb{Z}/n} 1_{\mathbb{Z}/n} & = & k \cdot_{\mathbb{Z}/n} \pi_n(l * m) \\ \Rightarrow & \pi_n(k) & = & (k * l) \cdot_{\mathbb{Z}/n} \pi_n(m) \, , \end{array}$$

c'est-à-dire que $\pi_n(m)$ est un générateur de $\mathbb{Z}/n$.

On dégage donc l'énoncé : un entier n non nul étant fixé, $m \in \mathbb{Z}$ est premier avec n si et seulement si $\pi_n(m)$ est un générateur du groupe abélien $(\mathbb{Z}/n, +)$ si et seulement si $\pi_n(m)$ est inversible dans l'anneau $(\mathbb{Z}/n, +, *)$. Un nombre premier p et un entier α étant fixés, il est plus facile de déterminer le nombre d'entiers inférieurs ou égaux à p^α qui ne sont pas premiers à p^α puisque ce sont en fait les multiples m de p compris entre $0 \leq m < p^\alpha$. Il est facile de les dénombrer et de constater qu'il sont au nombre de $p^{\alpha-1}$. Les nombres $0 \leq q < p^\alpha$ premiers à p^α sont donc tous les autres au nombre de $p^\alpha - p^{\alpha-1}$, ce qui donne la formule

$$E_p \ : \ \phi(p^\alpha) \ = \ p^{\alpha-1}(p-1) \, .$$

À noter que, pour $\alpha = 1$, cette formule correspond au fait que dans l'anneau $\mathbb{Z}/p$, il y a $p-1$ éléments inversibles, autrement dit que tous les éléments sauf 0 sont inversibles, autrement dit que $\mathbb{Z}/p$ est un corps.

L'anneau $\mathbb{Z}$ étant principal et p et q deux nombres premiers distincts, pour tout couple $(k, l) \in \mathbb{N}^* \times \mathbb{N}^*$, (p^k) et (q^l) sont comaximaux. Un générateur d de $(p^k) + (q^l)$ *i.e.*un PGCD de p^k et q^l se décompose en effet de manière unique en un produit de facteurs premiers $d = \prod_{i=1}^{r} s_i$. Par conséquent, pour tout $1 \leq i \leq r$ $s_i | d | p^k$. Comme s_i est premier, $s_i | p$. Comme p est irréductible s_i est inversible ou égal à p. Or comme s_i est irréductible $s_i = p$. De même, on montre que $s_i = q$, ce qui contredit le fait que p et q sont distincts. Il s'ensuit que d est inversible et par conséquent que $(p^k) + (q^l) = \mathbb{Z}$.

Fixons $n \in \mathbb{Z}$ non nul et notons

$$n \ = \ \prod_{i=1}^{d} p_i^{\alpha_i}$$

une décomposition de n en produit de facteurs premiers où l'on suppose les p_i distincts deux à deux.

Les $(p_i^{\alpha_i})$ sont donc deux à deux comaximaux et l'isomorphisme de $\mathbb{Z}$-algèbres

$$\omega \ : \ \mathbb{Z}/n \ \rightarrow \ \mathbb{Z}/p_1^{\alpha_1} \times \ldots \times \mathbb{Z}/p_d^{\alpha_d}$$

résulte alors d'une application directe du théorème des restes chinois (cf. cours II.8.4.) Soit $n \in \mathbb{Z}$ non nul fixé et décomposé en produit de facteurs premiers comme dans la Corrigé III . Un entier $0 \leq m < n$ est premier à n si et seulement si, d'après la Corrigé III ,

$$\begin{array}{rcl} & \pi_n(m) & \in \ (\mathbb{Z}/n)^\times \\ \omega \text{ est un morphisme d'algèbres} \overset{\Leftrightarrow}{} & \omega[\pi_n(m)] & \in \ [\prod_{i=1}^{d} \mathbb{Z}/p_i^{\alpha_i}]^\times \\ \text{(cf. cours II.8.4)} \overset{\Leftrightarrow}{} & \forall 1 \leq i \leq d, \ pi_i(m) & \in \ (\mathbb{Z}/p_i^{\alpha_i})^\times \ , \end{array}$$

ce qui résulte de la structure d'algèbre produit (cf. cours II.7.3) (où les $\pi_{i \ , \ 1 \leq i \leq d}$ sont les surjections canoniques $\mathbb{Z} \rightarrow \mathbb{Z}/p_i^{\alpha_i}$.)

Il y a donc autant d'éléments inversibles dans $\mathbb{Z}/n$ qu'il y a de d-uplets

$$(\xi_1, \ldots, \xi_d) \ \in \ \prod_{i=1}^{d} (\mathbb{Z}/p_i^{\alpha_i})^\times \ .$$

Il est dès lors clair que

$$\phi(n) \ = \ \prod_{i=1}^{d} \phi(p_i^{\alpha_i}) \ .$$

On déduit, par conséquent, de la formule E_p une formule

$$E_n \ : \ \phi(n) \ = \ \prod_{i=1}^{d} p_i^{\alpha_i - 1}(p_i - 1) \ .$$

Remarquons tout d'abord, que pour un nombre premier p, et un entier $\alpha \in \mathbb{N}^*$, $\phi(p) \geq p - 1$ (cf. E_p.) Ainsi, si n est un entier tel que $\phi(n) \ = \ 12$, les nombres premiers intervenant dans la décomposition en facteurs premiers de n sont nécessairement inférieurs ou égaux à 13. On dresse le tableau suivant donnant les indicateurs d'Euler de puissances de nombres premiers inférieurs ou égaux à 13, susceptibles d'intervenir dans la décomposition en produit de facteurs premiers d'un nombre n tel que $\phi(n) \ = \ 12$.

$$\begin{array}{cccccccccccc} & 2 & 2^2 & 2^3 & 2^4 & 3 & 3^2 & 5 & 7 & 11 & 13 \\ \phi & 1 & 2 & 4 & 8 & 2 & 6 & 4 & 6 & 10 & 12 \ . \end{array}$$

Les entiers n tels que $\phi(n) \ = \ 12$ sont donc

$$13 \ , \ 21 \ , \ 26 \ , \ 28 \ , \ 36 \text{ et } 42 \ .$$

On remarque que $9216 \ = \ 2^{10} * 3^2$. D'après la formule E_n, on a donc

$$\phi(9216) \ = \ 2^9 * 3 * 2 \ = \ 2^{10} * 3 \ = \ 3072 \ .$$

Université Paris Sud — Année 2004–2005

Licence MA — Algèbre Générale

Examen du jeudi 27 janvier 2005
Durée 3 heures

La qualité de la rédaction entrera pour une grande part dans la notation. Les calculatrices, téléphones mobiles, objets connectés et documents ne sont pas autorisés.

Il sera tenu compte de la clarté des raisonnements et de la rédaction dans la notation. Toute réponse doit être justifiée par un résultat du cours, ceux-ci ne devant pas être redémontrés.

Code :

Exercice A : () **(Le groupe de Klein dans $\mathcal{S}_4$)**
Soit X l'ensemble des produits de deux transpositions disjointes dans $\mathcal{S}_4$.

1) () Quel est le cardinal de X ?

2) () Montrer que X engendre un sous-groupe V de $\mathcal{S}_4$ distinct de $\mathcal{S}_4$. Quel est le cardinal de V ?

3) () **a)** () Pour tout $s \in \mathcal{S}_4$ et tout $x \in X$, montrer que le conjugué de x par s est dans X .

b) () En déduire un homomorphisme de groupes $\phi : \mathcal{S}_4 \to \mathcal{S}(X)$.

c) () Identifier le noyau de ϕ et son image.

d) () Quelle est l'image par ϕ du groupe alterné $\mathcal{A}_4$?

Exercice B : () **Soit $(G, +)$ un groupe <u>abélien</u> dont l'élément neutre est noté 0 , α et β des éléments de G d'ordre respectif a et b où a et b sont des entiers premiers entre eux. On note A (resp. B) le sous-groupe de G engendré par α (resp. par β,) c'est-à-dire**

$$A := \{n\alpha \, , \, n \in \mathbb{Z}\} \, , \text{ (resp. } B := \{n\beta \, , \, n \in \mathbb{Z}\} \, .)$$

On note

$$A + B := \{\xi + \eta \, , \, \xi \in A \, , \, \eta \in B\} \, .$$

1) () Montrer que $A + B$ est un sous-groupe de G .

2) () Montrer que $A \cap B = \{0\}$.

3) () Montrer que le morphisme de groupes

$$\phi_\alpha \ : \ \mathbb{Z} \ \to \ G \ , \ 1 \ \mapsto \ \alpha \ ; \ (\text{resp. } \phi_\beta \ : \ \mathbb{Z} \ \to \ G \ , \ 1 \ \mapsto \ \beta \ )$$

définit un isomorphisme de groupes

$$\xi_\alpha \ : \ \mathbb{Z}/a \ \cong \ A \ , \ (\text{resp. } \xi_\beta \ : \ \mathbb{Z}/b \ \cong \ B \ ;)$$

puis que l'on définit bien un morphisme de groupes

$$\begin{array}{rccl} \xi : & \mathbb{Z}/a \times \mathbb{Z}/b & \to & A + B \\ & (\lambda, \mu) & \mapsto & \phi_\alpha(l) + \phi_\beta(m) \ , \ \forall l \in \lambda \text{ et } \forall m \in \mu \ . \end{array}$$

4) () Montrer que ξ est un morphisme injectif ; puis que ξ est un isomorphisme de groupes ; puis finalement qu'il existe un isomorphisme de groupes

$$\mathbb{Z}/(ab) \ \cong \ A + B \ .$$

Exercice C : () **Soit** $a \ := \ i\sqrt{5} \ \in \ \mathbb{C}$. **On définit le sous-ensemble** A **de** $\mathbb{C}$ **par :**

$$A \ := \ \{x + ya \ , \ (x, y) \ \in \ \mathbb{Z} \times \mathbb{Z}\} \ \subset \ \mathbb{C} \ .$$

Pour tout nombre complexe $z \ := \ x + yi$, **on notera** $|z| \ := \ \sqrt{x^2 + y^2}$ **le module de** z .

1) () Montrer que A est un anneau pour les lois $+$ et $*$ du corps des complexes $\mathbb{C}$.

2) () **a)** () Donner un minorant du module d'un élément α non nul de A .

b) () En déduire que, si un élément α de A est inversible, alors $|\alpha| \ = \ 1$.

c) () Déterminer l'ensemble $A^\times$ des éléments inversibles de A .

3) () Calculer $(1 + a) * (1 - a)$ et en déduire que 2 n'est pas premier dans A .

4) () **a)** () Donner un majorant du module d'un diviseur de 2 dans A .

b) () Donner l'ensemble des diviseurs de 2 dans A et en déduire que 2 est irréductible dans A .

c) () L'anneau A est-il factoriel ?

Exercice D : () **Dans cet exercice, on note** $\mathbb{F}_2 \ := \ (\mathbb{Z}/2, +, *)$ **le corps fini à** 2 **éléments et** $V \ := \ \mathbb{F}_2 \ \times \ \mathbb{F}_2$ **un espace vectoriel de dimension** 2 **sur** $\mathbb{F}_2$ **dont la base canonique est** $\mathcal{B} \ := \ ((1, 0), (0, 1))$.

1) () Donner le cardinal n de l'ensemble $\tilde{V}$ des éléments non nuls de V .

Soit ϕ **un endomorphisme inversible de** V .

2) () Montrer que deux vecteurs non nuls de V sont colinéaires si et seulement s'ils sont égaux.

3) () Donner toutes les images possibles de $\mathcal{B}$ par ϕ et en déduire le cardinal du groupe $\mathrm{GL}_2(\mathbb{F}_2)$ des endomorphismes inversibles de V .

4) () Montrer que pour tout $x \ \in \ \tilde{V}, \phi(x) \ \in \ \tilde{V}$ puis que ϕ définit une bijection $\tilde{\phi}$ de $\tilde{V}$ sur lui-même.

5) () Montrer que l'application $\phi \mapsto \tilde{\phi}$ définit un morphisme de groupes injectif $u \ : \ \mathrm{GL}_2(\mathbb{F}_2) \ \to \ \mathcal{S}_n$.

6) () Montrer finalement que u est un isomorphisme. Le groupe $\mathrm{GL}_2(\mathbb{F}_2)$ est-il abélien ?

Université Paris Sud — Année 2004–2005

Licence MA — Algèbre Générale

Corrigé de l'examen du 27 janvier 2005

Exercice A : () **1)** () — Pour tout $x \in \mathcal{S}_4$ fixé, et tout couple y, z d'éléments de $\mathcal{S}_4$,

$$\begin{aligned}(yz)^x &= x^{-1}(yz)x \\ &= x^{-1}yxx^{-1}zx \\ &= y^x * z^x \ ;\end{aligned}$$

ce qui prouve que $y \mapsto y^x$ est un endomorphisme de $\mathcal{S}_4$.

— Pour tout triplet (x, y, z) d'éléments de $\mathcal{S}_4$,

$$\begin{aligned}x^{yz} &= (yz)^{-1}xyz \\ &= z^{-1}y^{-1}xyz \\ &= z^{-1}x^y z \\ &= (x^y)^z \ .\end{aligned}$$

a) () Pour tous x et y éléments de $\mathcal{S}_4$ et tout $a \in [1;4]$ a est un point fixe pour y si et seulement si :

$$\begin{array}{lrcl} & y(a) & = & a \\ x \text{ est bijective} \overset{\Leftrightarrow}{} & x^{-1}[y(a)] & = & x^{-1}(a) \\ \Leftrightarrow & x^{-1}[y[x(x^{-1}(a))]] & = & x^{-1}(a) \\ \Leftrightarrow & y^x[x^{-1}(a)] & = & x^{-1}(a) \ . \end{array}$$

b) () Il suffit de faire un passage au complémentaire avec le résultat de la question précédente.

c) () On sait que la conjuguée d'une transposition est une transposition (ce résultat pouvant d'ailleurs se déduire de la question précédente.) Pour calculer les conjuguées de t par les puissances de c il suffit donc de trouver les images réciproques du support de t par les puissances de c puisque une transposition est entièrement caractérisée par son support. Il s'ensuit immédiatement que

$$\begin{aligned}t^c &= (1,4) \\ t^{c^2} &= (3,4) \\ t^{c^3} &= (2,3) \ .\end{aligned}$$

Reste à remarquer que pour tous i, j et k dans $[1;4]$

$$(i,j)^{(j,k)} = (i,k) \ .$$

On montre ainsi que l'ensemble des transpositions de $\mathcal{S}_4$ est engendré par c et t ce qui suffit pour prouver que c et t engendrent $\mathcal{S}_4$.

2) () Remarquons que v_1 comme v_2 sont des produits de transpositions à supports disjoints et qui par conséquent commutent. Comme par ailleurs une transposition est d'ordre 2, on en déduit facilement que

$$v_1^2 \ = \ v_2^2 \ = \ \mathrm{Id} \ .$$

Par ailleurs on remarque que

$$v_1 v_2 \ = \ v_2 v_1 \ = \ \begin{matrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{matrix} \ .$$

Notons v_3 ce dernier élément. Remarquons que pour les mêmes raisons que pour v_1 et v_2, on a $v_3^2 \ = \ \mathrm{Id}$. Par ailleurs :

$$\begin{aligned} v_3 v_1 \ = \ v_1 v_3 \ &= \ v_2 \\ v_3 v_2 \ = \ v_2 v_3 \ &= \ v_1 \ ; \end{aligned}$$

ceci permet d'établir que

$$V \ = \ \{\mathrm{Id}, v_1, v_2, v_3\} \ .$$

On compare ensuite sa table à celle de $\mathbb{Z}/2 \times \mathbb{Z}/2$ pour constater qu'elles sont identiques.

a) () Pour montrer que V est normal dans $\mathcal{S}_4$, il suffit, comme c et t engendrent $\mathcal{S}_4$ et v_1 et v_2 engendrent V, de calculer :

$$\begin{aligned} v_1^t \ &= \ v_1 \ \in \ V \\ v_1^c \ &= \ v_3 \ \in \ V \\ v_2^t \ &= \ v_3 \ \in \ V \\ v_2^c \ &= \ v_2 \ \in \ V \ . \end{aligned}$$

b) () Comme V est normal dans $\mathcal{S}_4$, pour tout $v \ \in \ V$ et tout $x \ \in \ \mathcal{S}_4$, $v^x \in V$. Comme $\mathcal{A}_4$ est un sous-groupe de $\mathcal{S}_4$, en particulier, pour tout $y \ \in \ \mathcal{A}_4$, $v^y \in V$.

On rappelle que $\#(\mathcal{A}_4) \ = \ 12$. Comme $\#(V) \ = \ 4$, le cardinal du groupe quotient $\mathcal{A}_4/V$ est 3 . Un groupe de cardinal 3 est isomorphe à $\mathbb{Z}/3$.

Exercice B : () **1)** () Pour tout $\xi \ := \ x\alpha + y\beta$ et tout $\xi' \ := \ x'\alpha + y'\beta$ des éléments de $A + B$,

— $$\xi + \xi' \ = \ x\alpha + y\beta + x'\alpha + y'\beta \ = \ (x +_{\mathbb{Z}} x')\alpha + (y +_{\mathbb{Z}} y')\beta$$
puisque G est un $\mathbb{Z}$-module. Par conséquent $+$ est interne sur $A + B$.

— Par ailleurs
$$0 \ = \ 0_{\mathbb{Z}}\alpha + 0_{\mathbb{Z}}\beta \ \in \ A + B$$
est un élément neutre pour $+$ dans $A + B$.

— Enfin $-x\alpha \in A$ et $-y\beta \in B$ et il est clair que $-x\alpha - y\beta$ est un opposé pour ξ dans $A + B$.

2) () Comme A et B sont des sous-groupes de G, $0 \in A$ et $0 \in B$.

Par ailleurs si $\xi \in G$ et $\xi \in A \cap B$, il existe des entiers r et s tels que

$$\xi \ = \ r\alpha \text{ et } \xi \ = \ s\beta \ .$$

Il en résulte que

$$\begin{aligned} a\xi \ &= \ ar\alpha \\ &= \ 0 \\ &\text{et} \\ b\xi \ &= \ bs\beta \\ &= \ 0 \ ; \end{aligned}$$

c'est-à-dire que l'ordre de ξ dans G divise simultanément a et b . Or ces derniers étant supposés premiers entre eux, l'ordre de ξ est nécessairement 1 c'est-à-dire que $\xi \ = \ 0$ d'où $A \cap B \ = \ \{0\}$.

3) () Par définition même de l'ordre de l'élément α dans G, $A \;=\; \mathrm{Im}\,\phi_\alpha$ et

$$\mathrm{Ker}\,\phi_\alpha \;=\; (a) \;=\; a\mathbb{Z}\,.$$

En appliquant le théorème de factorisation des morphismes de groupes (ou $\mathbb{Z}$-modules dans le cas présent,) on obtient un isomorphisme de groupes

$$\xi_\alpha \;:\; \mathbb{Z}/a \;\cong\; \mathrm{Im}\,\phi_\alpha \;=\; A\,.$$

Pour tous

$$\begin{array}{rcl}(\lambda,\mu) & \in & \mathbb{Z}/a \times \mathbb{Z}/b \\ (l,l') & \in & \lambda \times \lambda \\ (m,m') & \in & \mu \times \mu\,,\end{array}$$

il existe des entiers relatifs r et s tels que $l' = l + ra$ et $m' = m + sb$. Il en résulte que :

$$\begin{array}{rcl}\phi_\alpha(l') + \phi_\beta(m') & = & l'\alpha + m'\beta \\ & = & (l+ra)\alpha + (m+sb)\beta \\ & = & l\alpha + m\beta \\ & = & \phi_\alpha(l) + \phi_\beta(m)\end{array}$$

c'est-à-dire que ξ est bien défini.

4) () Pour tous

$$\begin{array}{rcl}(\lambda,\mu) & \in & \mathbb{Z}/a \times \mathbb{Z}/b \\ (\lambda',\mu') & \in & \mathbb{Z}/a \times \mathbb{Z}/b \\ (l,m) & \in & \lambda \times \mu \\ (l',m') & \in & \lambda' \times \mu'\,,\end{array}$$

—

$$\begin{array}{rcl}\xi((\lambda,\mu)+(\lambda',\mu')) & = & \xi((\lambda+\lambda'),(\mu+\mu')) \\ & = & \phi_\alpha(l+l') + \phi_\beta(m+m') \\ & = & \phi_\alpha(l) + \phi_\beta(m) + \phi_\alpha(l') + \phi_\beta(m') \\ & = & \xi(\lambda,\mu) + \xi(\lambda',\mu')\,;\end{array}$$

c'est-à-dire que ξ est un morphisme de groupes.

— De plus

$$\begin{array}{lrcl} & \xi(\lambda,\mu) & = & 0 \\ \Leftrightarrow & \phi_\alpha(l) + \phi_\beta(m) & = & 0 \\ \Leftrightarrow & \phi_\alpha(l) & = & -\phi_\beta(m) \\ \Rightarrow & \phi_\alpha(m) \in B & \text{et} & \phi_\beta(m) \in A \\ \overset{\Rightarrow}{\text{(cf. question 2),}} & \phi_\alpha(l) \;=\; \phi_\beta(m) & = & 0 \\ \Rightarrow & l \in (a) & \text{et} & m \in (b) \\ \Rightarrow & \lambda \;=\; 0 & \text{et} & \mu \;=\; 0\,;\end{array}$$

c'est-à-dire que ξ est un morphisme injectif.

— Pour tout élément $\gamma \in A + B$, il existe l et m dans $\mathbb{Z}$ tels que

$$\begin{array}{rcl}\gamma & = & l\alpha + m\beta \\ & = & \phi_\alpha(l) + \phi_\beta(m) \\ & = & \xi(\overline{l},\overline{m})\,;\end{array}$$

c'est-à-dire que ξ est surjectif donc, d'après ce qui précède, un isomorphisme.

— Enfin les entiers a et b étant premiers entre eux, le théorème des restes chinois donne un isomorphisme d'anneaux

$$(\mathbb{Z}/(ab),+,*) \;\cong\; (\mathbb{Z}/a,+,*) \;\times\; (\mathbb{Z}/b,+,*)\;;$$

mais comme "qui peut le plus peut le moins" c'est aussi un isomorphisme des groupes additifs.

Exercice C : () **1)** () Pour tout $\xi \;:=\; x+ya$ et tout $\xi' \;:=\; x'+y'a$ éléments de A,

—

$$\begin{aligned}\xi+\xi' &= (x+ya)+(x'+y'a)\\ &= (x+x')+(y+y')a\\ &\in A\,,\end{aligned}$$

car $x+x'$ et $y+y'$ sont des éléments de $\mathbb{Z}$. On en déduit que la loi $+$ est interne sur A .

— Il est clair que $+$ est associative sur A puisqu'elle l'est sur $\mathbb{C}$.

— L'élément $0_{\mathbb{C}} \;=\; 0+0*a$ appartient à A et est un élément neutre pour $+$ sur A .

— On a

$$(x+y*a)+(-x+(-y)*a) \;=\; 0$$

c'est-à-dire que $-x-y*a$ est un opposé pour $x+y*a$.

— Enfin $+$ est commutative sur A puisqu'elle l'est sur $\mathbb{C}$ c'est-à-dire finalement que $(A,+)$ est un groupe abélien.

—

$$\begin{aligned}\xi*\xi' &= (x+ya)*(x'+y'a)\\ &= x*x'+y*y'*a^2+(x*y'+x'*y)a\\ &= x*x'-5*y*y'+(x*y'+y*x')a\\ &\in A\,,\end{aligned}$$

puisque $x*x'-5*y*y'$ et $x*y'+y*x'$ sont des éléments de $\mathbb{Z}$ puisque celui-ci est un anneau. La loi $*$ est donc interne sur A .

— L'élément $1_{\mathbb{C}} \;=\; 1+0*a$ appartient à A et est un élément neutre pour $*$.

— Enfin $*$ est distributive par rapport à $+$ puisque ceci est déjà vrai dans $\mathbb{C}$.

— Le sous-ensemble A de $\mathbb{C}$ est donc un anneau pour les lois induites.

2) () Pour tout $\alpha \;:=\; x+y*a \;\in\; A, \alpha\neq 0, |\alpha| \;=\; \sqrt{x^2+5*y^2}$. Or si $x\neq 0$ ou $y\neq 0$, il est clair que $|\alpha|\geq 1$.

a) () Un élément $\alpha\in A$ est inversible si et seulement si $\alpha\neq 0$ et il existe $\beta\neq 0$ tel que

$$\begin{aligned}&\alpha*\beta &&= 1\\ \Rightarrow\quad &|\alpha|*|\beta| &&= 1\\ \Rightarrow\quad &|\alpha| &&= \frac{1}{|\beta|}\\ \overset{\Rightarrow}{\text{(cf. question 2),)}}\quad &|\alpha| &&\leq 1\,.\end{aligned}$$

Cette dernière majoration combinée avec la minoration de la question 2) implique que $|\alpha| \;=\; 1$.

b) () Si $\alpha \;:=\; x+y*a \;\in\; A$ vérifie

$$\begin{aligned}&|\alpha| &&= 1\\ \Leftrightarrow\quad &|\alpha|^2 &&= 1\\ \Leftrightarrow\quad &x^2+5y^2 &&= 1\,,\end{aligned}$$

on a nécessairement $y=0$ d'où $x^2=1$ c'est-à-dire $x=1$ ou $x=-1$. Les éléments -1 et 1 sont bien des éléments de A qui sont par ailleurs leur propre inverse d'où

$$A^{\times} \;=\; \{-1;1\}\,.$$

3) () On a

$$(1+a)*(1-a) \;=\; 1-a^2 \;=\; 1+5 \;=\; 6\,.$$

Or $6 \;=\; 2*3$ avec 2 et 3 des éléments de A c'est-à-dire que $2(|1+a)*(1-a)$. Si 2 était premier dans A, il devrait diviser l'un des deux facteurs. Or supposons par exemple qu'il existe $\alpha \;=\; x+y*a$ tel que

$$\begin{array}{rrcl} & 2*(x+y*a) & = & 1+a \\ \Leftrightarrow & 2*x+2*y*\sqrt{5}*i & = & 1+\sqrt{5}*i \end{array}$$

ce qui équivaut, puisque $(1,i)$ est une base de $\mathbb{C}$ comme $\mathbb{R}$-espace vectoriel, à

$$2*x \;=\; 1 \text{ et } 2*y \;=\; 1\,.$$

Or 2 n'est pas inversible dans $\mathbb{Z}$ et par conséquent la première égalité ne peut pas être satisfaite.
Un raisonnement exactement analogue montre que 2 ne divise pas $1-a$.
On en déduit que 2 n'est pas premier dans A .

a) () Si $\alpha \in A$ est un diviseur de 2, il existe $\beta \neq 0$ dans A tel que

$$\begin{array}{rrcl} & \alpha*\beta & = & 2 \\ \Rightarrow & |\alpha|*|\beta| & = & 2 \\ \Rightarrow & |\alpha| & = & \dfrac{2}{|\beta|} \\ \overset{\Rightarrow}{\text{(cf. question 2),)}} & |\alpha| & \leq & 2\,. \end{array}$$

b) () D'après ce qui précède si $\alpha \;:=\; x+y*a$ est un diviseur de 2 dans A,

$$\begin{array}{rrcl} & |\alpha| & \leq & 2 \\ \Leftrightarrow & |\alpha|^2 & \leq & 4 \\ \Leftrightarrow & x^2+5*y^2 & \leq & 4\,; \end{array}$$

ce qui implique clairement que $y=0$. Les diviseurs possibles de 2 sont donc $-2,-1,1,2$ et l'on voit que les seuls produits possibles sont

$$\begin{array}{rcl} 2 & = & 2*1 \\ 2 & = & (-1)*(-2)\,, \end{array}$$

d'où l'on déduit, grâce à la question 2), b), que 2 est irréductible dans A .

c) () Dans l'anneau A, l'élément 2 est irréductible sans être premier; c'est-à-dire que l'anneau A ne vérifie pas la propriété de GAUSS et n'est donc pas factoriel.

Exercice D : () **1)** () Les éléments de V sont des combinaisons linéaires des vecteurs $(1,0)$ et $(0,1)$ à coefficients dans $\mathbb{F}_2$. Ce dernier comportant 2 éléments il est clair qu'on peut former 4 telles combinaisons linéaires. L'une d'entre elles seulement est l'élément neutre de V et par conséquent :

$$n \;:=\; \#(\tilde{v}) \;=\; 3\,.$$

2) () Soient v et w deux vecteurs non nuls dans V . Ils sont colinéaires si et seulement s'il existe α et β des éléments non tous nuls de $\mathbb{F}_2$ tels que $\alpha v+\beta w \;=\; 0$. On peut supposer $\alpha \neq 0$ et il vient alors : $v \;=\; \alpha^{-1}\beta w$. Le fait que $v \neq 0$ implique $\beta \neq 0$ et par conséquent

$$\alpha \;=\; \beta \;=\; 1\,.$$

Il vient alors $v \;=\; -w$. Comme dans $\mathbb{F}_2$ $-1=1$ il vient finalement $v=w$.

3) () L'endomorphisme ϕ est inversible si et seulement si l'image de $\mathcal{B}$ par ϕ est une base de V . Réciproquement l'image de $\mathcal{B}$ détermine entièrement un endomorphisme de V .

La question revient donc à dénombrer les bases dans V . Une base est formée de deux vecteurs non colinéaires. Or d'après la question précédente, deux vecteurs sont indépendants si et seulement s'ils sont non nuls et différents. Il faut donc finalement trouver les couples d'éléments différents de $\tilde{V}$ qui sont au nombre de 6 d'où :

$$\#(\mathrm{GL}_2(\mathbb{F}_2)) \;=\; 6\,.$$

4) () Comme ϕ est un isomorphisme il est clair que $\phi(x) \;=\; 0$ si et seulement si $x \;=\; 0$. Ceci prouve que ϕ définit bien une bijection $\tilde{\phi}$ de $\tilde{V}$ sur lui-même.

5) () Le fait que $\phi \mapsto \tilde{\phi}$ est un morphisme résulte simplement du fait que la restriction et la composition des applications sont deux opérations qui commutent. Supposons que ϕ est tel que $\tilde{\phi} \;=\; \mathrm{Id}_{\tilde{V}}$. Cela a en particulier pour conséquence que les vecteurs de la base $\mathcal{B}$ qui sont des éléments de $\tilde{V}$ sont fixes par ϕ ce qui implique que $\phi \;=\; \mathrm{Id}_V$. Le morphisme

$$\begin{array}{rccc} u: & \mathrm{GL}_2(\mathbb{F}_2) & \to & \mathcal{S}_3 \\ & \phi & \mapsto & \tilde{\phi} \end{array}$$

est donc injectif.

6) () Il suffit de remarquer que

$$\#(\mathrm{GL}_2(\mathbb{F}_2)) \;=\; 6 \;=\; \#(\mathcal{S}_3)$$

et que u est injectif pour en déduire que u est un isomorphisme. Le groupe $\mathcal{S}_3$ n'étant pas abélien, $\mathrm{GL}_2(\mathbb{F}_2)$ non plus.

Université Paris Sud **Année 2004–2005**

Licence MA **Algèbre Générale**

Examen du mardi 6 septembre 2005
Durée 2 heures

La qualité de la rédaction entrera pour une grande part dans la notation. Les calculatrices, téléphones mobiles, objets connectés et documents ne sont pas autorisés.

Il sera tenu compte de la clarté des raisonnements et de la rédaction dans la notation. Toute réponse doit être justifiée par un résultat du cours, ceux-ci ne devant pas être redémontrés.
Rédiger sur une nouvelle copie.

Exercice A : () Déterminer tous les entiers x vérifiant

$$x^{12} \equiv x\,[12]\,.$$

Exercice B : () **1)** () Pour un entier naturel $n > 1$, déterminer l'ordre du produit $s_1 s_2$ en fonction des ordres respectifs de s_1 et s_2 pour deux éléments s_1 et s_2 du groupe symétrique $\mathcal{S}_n$ dont les supports sont disjoints.

a) () Généraliser, pour un entier $p > 2$ quelconque, le résultat précédent au produit de p éléments s_i ,$1 \leq i \leq p$ du groupe symétrique $\mathcal{S}_n$ de supports deux à deux disjoints

2) () Pour

$$s := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 11 & 8 & 10 & 4 & 6 & 5 & 3 & 1 & 7 & 9 & 2 \end{pmatrix} \in \mathcal{S}_{11},$$

calculer s^{2006}.

Exercice C : () **On note** $\mathrm{GL}_2(\mathbb{Z})$ **l'ensemble des matrices carrées** 2×2 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ **à coefficients entiers relatifs dont le déterminant vaut** 1 **ou** -1.

1) () Montrer que $\mathrm{GL}_2(\mathbb{Z})$ muni de la multiplication des matrices est un groupe.

a) () Pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$, que peut-on dire des couples d'entiers (a, d) et (b, c) ?

b) () En admettant que l'ensemble des nombres premiers est infini, montrer que $\mathrm{GL}_2(\mathbb{Z})$ est infini.

Pour tout entier $n \in \mathbb{N}^*$, **on note** $\Gamma_0(n)$ **(resp.** $\Gamma_1(n)$**) l'ensemble des matrices** $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ **de déterminant** 1 **telles que** $c \equiv 0[n]$ **(resp.** $c \equiv 0[n], a \equiv 1[n]$ **et** $d \equiv 1[n]$).

2) () Montrer que $\Gamma_0(n)$ (resp. $\Gamma_1(n)$) est un sous-groupe de $\mathrm{GL}_2(\mathbb{Z})$.

Exercice D : () **1)** () Soit k un corps. Montrer que le polynôme $X^2-1 \in k[X]$ possède au plus deux racines distinctes. Dans quel cas ces deux racines sont-elles confondues ?

2) () **Soit $n > 1$ un entier.**

a) () À quelle condition nécessaire et suffisante sur n, l'anneau $\mathbb{Z}/n$ est-il un corps ?

b) () Dans ce cas, quels éléments de $(\mathbb{Z}/n)^\times$ sont leur propre inverse ?

c) () En déduire la valeur du produit

$$\prod_{a \in (\mathbb{Z}/n)^\times} a \ .$$

d) () En déduire finalement, que si n est premier,

$$(n-1)! \ \equiv \ -1 \ [n] \ .$$

3) () Établir la réciproque de l'assertion de la question 2), d).

Université Paris Sud — Année 2004–2005

Licence MA — Algèbre Générale

Corrigé de l'examen du 6 septembre 2005

Exercice A : () Déterminer les entiers $x \in \mathbb{Z}$ tels que $E : x^{12} \equiv x\ [12]$ équivaut à déterminer tous les entiers $x \in \mathbb{Z}$ dont la classe ξ dans $\mathbb{Z}/12$ vérifie $\xi^{12} = \xi$. Les entiers 3 et 4 étant premiers entre eux, il existe un isomorphisme d'anneaux (théorème des restes chinois,)

$$\begin{array}{rccc} f: & \mathbb{Z}/12 & \to & \mathbb{Z}/3 \times \mathbb{Z}/4 \\ & \xi & \mapsto & (\eta, \zeta)\,. \end{array}$$

Comme f est un isomorphisme d'anneaux, l'équation E équivaut à $f(\xi)^{12} = f(\xi)$. Cette dernière équivaut encore au système

$$S : \left(\begin{array}{rcl} \eta^{12} & = & \eta \in \mathbb{Z}/3 \\ \zeta^{12} & = & \zeta \in \mathbb{Z}/4 \end{array} \right).$$

Or 3 étant premier, on sait, d'après le petit théorème de FERMAT par exemple, que pour tout $\eta \in \mathbb{Z}/3$, $\eta^3 = \eta$. La première équation du système S équivaut donc à $\eta^4 = \eta$ et encore à $\eta^2 = \eta$ qui équivaut finalement à $\eta(\eta - 1) = 0$ c'est-à-dire, comme $\mathbb{Z}/3$ est un corps et partant un anneau intègre, à $\eta = 0$ ou $\eta = 1$.

L'entier 4 n'étant pas premier, on ne peut faire un raisonnement analogue pour la deuxième équation. Cependant on constate que :

— $0^{12} = 0$ donc 0 est solution ;
— $1^{12} = 1$ donc 1 est solution ;
— $2^2 = 0$ et par conséquent $2^{12} = 0 \neq 2$ donc 2 n'est pas solution ;
— $3^2 = (-1)^2 = 1$ et par conséquent, $3^{12} = 1 \neq 3$ donc 3 n'est pas solution.

Les couples (η, ζ) solutions du système S sont donc $(0,0), (1,0), (0,1), (1,1)$. Chacun a un unique antécédent par f dans $\mathbb{Z}/12$ respectivement $0, 4, 9, 1$.

Finalement l'ensemble des solutions de E est

$$\{12kk \in \mathbb{Z}\} \cup \{1 + 12kk \in \mathbb{Z}\} \cup \{4 + 12kk \in \mathbb{Z}\} \cup \{9 + 12kk \in \mathbb{Z}\}\,.$$

Exercice B : () **1)** () On rappelle que l'ordre de l'élément a est le plus petit entier naturel α tel que $a^\alpha = e$ si e désigne l'élément neutre de G. C'est aussi le plus petit au sens de la relation de divisibilité ou ce qui revient au même, le générateur positif de l'idéal $N_a := \{x \in \mathbb{Z} \,|a^x = e\}$. Ceci signiifie encore que pour $x \in \mathbb{Z}\ a^x = e$ si et seulement si $\alpha | x$.

Pour tout couple (s_1, s_2) d'éléments de $\mathcal{S}_n$, et tout x si s_1 et s_2 sont à supports disjoints, $s_1 s_2 = s_2 s_1$ et par conséquent, $(s_1 s_2)^x = s_1^x s_2^x$. Il en résulte que si $o_1 | x$ et $o_2 | x$, (où o_i est l'ordre de s_i dans $\mathcal{S}_n$ pour $i = 1$ ou $2,$) $(s_1 s_2)^x = e$. Par définition même du **Ppcm** de deux entiers, il en résulte que l'ordre de $s_1 s_2$ divise le **Ppcm** $[o_1, o_2]$ de o_1 et o_2.

Notons ω l'ordre de $s_1 s_2$, et S_i le support de de s_i $i = 1$ ou 2.

On a $(s_1 s_2)^\omega = e$ c'est-à-dire que pour tout $u \in [1; n]$, $(s_1 s_2)\omega(u) = u$.

Si $u \in S_1$, $u \notin S_2$ puisque les supports sont disjoints. Par conséquent $s_2(u) = u$ et pour tout entier k, $s_2^k(u) = u$. Il en résulte que $(s_1 s_2)^\omega(u) = s_1^\omega(u) = u$. Il en résulte que la restriction de s_1^ω àS_1 est e. Comme la restriction de s_1 au complémentaire de S_1 est l'identité, il en résulte que $s_1^\omega = e$. Ceci signifie que $o_1 | \omega$.

On montre par un raisonnement exactement angloque que $o_2 | \omega$. D'où il résulte que $[o_1, o_2] - \omega$.

On en conclut finalement que $\omega = [o_1, o_2]$.

a) () On va montrer que l'ordre du produit de p permutations à supports deux à deux disjoints, est le **Ppcm** des ordres de chacune d'entre elles.

Le résultat a été établi pour $p = 2$ à la question précédente. Si le résultat est établi pour un produit de p permutations à supports deux à deux disjoints, considérons $p+1$ permutations $s_{i\ ,1\leq i\leq p+1}$ à supports deux à deux disjoints. Si l'on note

$$s \ := \ \prod_{i=1}^{p} s_i,$$

s et s_{p+1} sont encore à supports disjoints puisque le support de s est la réunion des supports des $s_{i\ ,1\leq i\leq p}$. On peut donc appliquer le résultat pour $p = 2$ à s et s_{p+1} c'est-à-dire que l'ordre du produit

$$v \ := \ \prod_{i=1}^{p+1} s_i \ = \ ss_{p+1}$$

est le **Ppcm** de l'ordre de s et de l'ordre de s_{p+1}. Le résultat découle ensuite de l'associativité du ppcm.

2) () La permutation s s'écrit comme le produit :

$$s \ = \ (5,6)(1,11,2,8)(3,10,9,7)$$

c'est-à-dire comme le produit d'une transposisiton et de deux 4-cycles à supports deux à deux disjoints. La permutation s est donc d'ordre $4 \ = \ [2,4,4]$.

On remarque ensuite que $2006 \ \equiv \ 2[4]$ et par conséquent,

$$s^{2006} \ = \ s^2 \ = \ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 2 & 1 & 9 & 4 & 5 & 6 & 10 & 11 & 3 & 7 & 8 \end{pmatrix} .$$

Exercice C : () **1)** () — Pour deux matrices

$$A \ := \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ et } E \ := \ \begin{pmatrix} e & f \\ g & h \end{pmatrix},$$

$$A * E \ = \ \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} \ \in \ \mathrm{GL}_2(\mathbb{Z}) .$$

En effet les coefficients sont bien des entiers relatifs et comme $\det(()A * E) \ = \ \det(()A)\det(()E)$ il vaut bien 1 ou -1. La multiplication est donc une loi interne sur $\mathrm{GL}_2(\mathbb{Z})$.

— La multiplication est associative puisque ce résultat est bien connu pour la multiplication des matrices en général.

— La matrice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est bien entendu un élément de $\mathrm{GL}_2(\mathbb{Z})$ et est un élément neutre pour la multiplication.

— Enfin, pour tout élément $A \ := \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ \in \ \mathrm{GL}_2(\mathbb{Z})$, il est clair que $A' \ := \ \dfrac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ appartient à $\mathrm{GL}_2(\mathbb{Z})$ et que

$$AA' \ = \ A'A \ = \ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} .$$

Tout élément de $\mathrm{GL}_2(\mathbb{Z})$ a donc un inverse dans $\mathrm{GL}_2(\mathbb{Z})$.

a) () Pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \ \in \ \mathrm{GL}_2(\mathbb{Z})$, on a $ad - bc = 1$ ou -1, ce qui signifie qu'on a l'identité de BÉZOUT pour les couples (a,d) et (b,c) respectivmeents c'est-à-dire que a et d respectivement b et c sont premiers entre eux.

b) () Si l'ensemble des nombres premier est infini, l'ensemble des couples de nombres premiers distincts est également infini. À tout tel couple (p, q) on associe un couple (u, v) de coefficients de BÉZOUT tel que $pu - qv = 1$. À tout couple de nombres premiers distincts (p, q) on peut donc associer la matrice

$$\begin{pmatrix} p & q \\ v & u \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}) .$$

2) () Avec les notations de la question 1), si A et E sont des éléments de $\Gamma_0(n)$, $c \equiv 0[n]$ et $g \equiv 0[n]$. Il en résulte que $ce + dg \equiv 0[n]$. Par ailleurs si $\det(()A) = \det(()E) = 1$, $\det(()AE) = 1$. Il en résulte que $\Gamma_0(n)$ est stable par multiplication. Par ailleurs, si $c \equiv 0[n]$, $-c \equiv 0[n]$ ce qui assure que l'inverse de A est bien dans $\Gamma_0(n)$.

Il n'est pas plus difficile de montrer que $\Gamma_1(n)$ est un sous-groupe de $\Gamma_0(n)$.

Université Paris Sud — Année 2004–2005

Licence MA — Algèbre Générale

Index