Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

Table des matières

Université Paris Sud **Année 2018–2019**

L3/S5 M313 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

À défaut de chercher à justifier l'intérêt que pourrait avoir en soi l'étude des structures algébrique (groupes, anneaux, corps ...) on est tenté de présenter deux questions pour la résolution desquelles l'algèbre est en mesure de fournir des outils d'une grande efficacité. Ces questions relèvent de deux des plus anciens champs d'études de la mathématique que sont la géométrie et l'arithmétique.

En premier lieu, au paragraphe 0.2, nous expliquerons comment l'étude des groupes (chapitre III) et plus précisément l'étude des actions de groupes (chapitre V,) permet d'apporter une solution complète au problème de la classification des polyèdres régulier dans l'espace de dimension 3. Après avoir en effet ramené le problème à celui de déterminer les sous-groupes finis du *groupe spécial orthogonal* $\mathcal{SO}_3(\mathbb{R})$, de $\mathbb{R}^3$, la théorie des actions de groupes permet d'écrire une formule numérique dite *équation caractéristique* (cf. 0.2.2.6,) qui contraint à tel point certains invariants liés au groupe que ceux-ci sont finalement très peu nombreux.

En second lieu nous exposerons, au paragraphe 0.3, la solution proposée par GAUSS au problème de FERMAT dans le cas de l'exposant $n = 3$. Nous espérons que ce résulta et sa preuve motiverons l'étude des anneaux principaux (chapitre IX,) sans s'en tenir exclusivement aux cas de l'ensemble $\mathbb{Z}$ des entiers relatifs (néanmoins étudié au chapitre IV,) ou à celui de l'anneau $\mathbb{K}[X]$ des polynômes à une indéterminée à coefficients dans un corps (dont l'étude sera cependant détaillée au chapitre VIII.) Les anneaux d'entiers de GAUSS (cf. IX.1.4.c),) et d'Eisenstein (cf. IX.1.4.d),) sont en effet amenés à jouer un rôle déterminant dans ces questions d'arithmétique.

Nous ne donerons évidemment aux paragraphes 0.2 et 0.3 qu'une esquisse de la stratégie des preuves, en espérant bien qu'à la fin de ce cours nous serons en mesure d'en faire tous les détails.

Nous reviendrons dans ce cours sur un certain nombre de notions fondamentales notttament dans le domaine de la téhorie des ensembles sans toutefois consacrer une étude systématique à ce sujet qui excéderait le cadre de ce cours.

Il est usuel de construire l'ensemble $\mathbb{N}$ des entiers naturel, comme nous le ferons au chapitre II,à partir d'un système de PEANO dont on rappelle la définition :

Définition 0.1 (Système de Peano) On appelle *Système de* PEANO la donnée d'un ensemble $\mathbb{N}$, contenant au moins un élément 0, et de trois appplications :

$$\begin{array}{rrcl} \mathfrak{s}: & \mathbb{N} & \to & \mathbb{N} \\ +: & \mathbb{N}\times\mathbb{N} & \to & \mathbb{N} \\ *: & \mathbb{N}\times\mathbb{N} & \to & \mathbb{N} \end{array} \qquad 0.1.1$$

satisfaisant les axiomes suivants :

PA$_1$) (**Succ**$_1$)

$$\forall p \in \mathbb{N},\ \big(p \neq 0 \Leftrightarrow \exists q \in \mathbb{N},\ (p = \mathfrak{s}(q))\big)\ .$$

PA$_2$) (**Succ**$_2$)

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \big(\mathfrak{s}(p) = \mathfrak{s}(q) \Rightarrow p = q\big)\ .$$

PA$_3$) (**Ind**)

$$\forall A \subset \mathbb{N},\ \big(0 \in A \wedge \forall p(p \in A \Rightarrow \mathfrak{s}(p) \in A) \Rightarrow A = \mathbb{N}\big)\ .$$

PA$_4$) (**Add**$_1$)

$$\forall p \in \mathbb{N},\ (0 + p = p)\ .$$

PA$_5$) (**Add**$_2$)

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \big(\mathfrak{s}(p) + q = \mathfrak{s}(p+q)\big)\ .$$

PA$_6$) (**Mult**$_1$)

$$\forall p \in \mathbb{N},\ (0 * p = 0)\ .$$

PA$_7$) (**Mult**$_2$)

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \big(\mathfrak{s}(p) * q = (p * q) + q\big)\ .$$

On constate cependant sur cette définition qu'elle fait librement appel aux notions d'*ensemble*, d'*application*, de *loi de composition* etc... On pourrait s'en tenir à l'idée intuitive qu'on a de ces notions et c'est à peu près ce que nous ferons dans la pratique, mais cela ne peut être ni suffisant ni satisfaisant si l'on s'interrroge sur ce qui fonde ces notions. D'autant qu'elles seront de nouveau utilisée dans le chapitre VI.Il semble, à ce point, à tout le moins raisonnable de se demander si on parle de la même chose, ou encore s'il existe un cadre dans lequel envisager simultanément ces différentes notions.

On ne peut affirmer a priori qu'une *théorie des ensembles* et celle en particulier que nous allons survoler dans les paragraphes I.1 à I.4, soit « le bon cadre » cherché, ce que nous n'affirmerons pas, mais même un « cadre acceptable ». Cependant un résultat comme la proposition I.3.10 affirmant qu'il existe une « représentation des entiers » dans le système **ZF** est de nature à conforter la démarche consistant à chercher à « faire des mathématiques » en prenant pour base le système **ZF**. La construction de l'ensemble des entiers relatifs $\mathbb{Z}$

exposée au paragraphe IVpeut se faire à partir de $\mathbb{N}$ par des « opérations ensemblistes » si bien qu'on ne sort toujours pas du cadre. Le même procédé permet de construire l'ensemble des nombres rationnels $\mathbb{Q}$ à partir de $\mathbb{Z}$. Si la construction de l'ensemble des nombres réels $\mathbb{R}$ à partir de $\mathbb{Q}$ est un peu plus sophistiquée, elle n'échappe toujours pas au cadre de la téhorie des ensembles. Ainsi en va-t-il encore de celle des nombres complexes $\mathbb{C}$ à partir de $\mathbb{R}$ [1]

Tout ceci n'a certainement pas pour but de modifier la manière que nous avons de « faire des mathématiques » [2] c'est-à-dire de démontrer logiquement des propositions. Cependant en fournissant un cadre axiomatique aussi restreint que possible dans lequel « existent » les objets mathématiques usuels la théorie **ZFC** permet de poser de manière claire la question de la cohérence de l'édifice mathématique. Notons finalement que le succès de telles théories est dû en grande partie à la possibilité qu'elles offrent de formaliser de manière satisfaisante les questions relatives à la « taille des ensembles » dont la plus célèbre est l'*hypothèse du continu*, consistant à savoir s'il existe un « infini de taille intermédiaire entre $\mathbb{N}$ et $\mathbb{R}$. Outre que cette question n'a pour l'instant reçu aucune réponse définitive, elle dépasse absoluement le cadre de ce cours dans lequel il serait même bien surprenant qu'il soit question de l'ensemble $\mathbb{R}$.

Indépendamment de la cohérence qu'une théorie des ensembles peut apporter à l'édifice mathématique, dont nous avons esquissé une présentation ci-dessus, un point de vue plus pragmatique peut consister à constater que la plupart des textes mathématiques contemporains font référence à des collections d'objets partageant une même propriété, ou même définies a priori, et considérées indépendamments de leurs constituants, comme de nouveaux objets mathématiques. On pourrait très bien considérer qu'il n'y a pas de raison de faire reposer l'édifice sur ces objets, mais considérer que les entiers, les fonctions, les suites, les réels ou que sais-je encore sont premiers. En tout état de cause il faut quand-même savoir de quoi l'on parle lorsque l'on parle d'ensemble de ci ou çà et une fois encore l'axiomatique **ZFC** se révèle particulièrement efficace sans modifier substantiellement la manière qu'on a d'écrire des mathématiques simplement sans doute parce qu'elle l'a inspirée de manière plus ou moins explicite au moins pour ce qui concerne les textes contemporains.

0.2 . −Les solides platoniciens

Il s'agit d'expliquer pourquoi il n'y a qu'un nombre fini (5 en fait) de type de polyèdres convexes réguliers dans l'espace euclidien de dimension 3 usuel. En attachant à un telle polyèdre Π un certain groupe (cf. III.1.1,) G, ce que nous ferons en 0.2.1, on est amené à déterminer quels peuvent être les groupes ainsi associés à des polyèdre convexes réguliers. Nous verrons en 0.2.2 que les contraintes pesant sur de tels groupes sont à ce point importantes, qu'il n'y a en fait que très peu de tels groupes. En réalité la manière dont ces groupes déplacent ou permutent certains objets (*opèrent*, *agissent*, sur un certain ensemble) (cf.

1. Cette dernière étant d'ailleurs plus simple que la précédente tant qu'on ne cherche pas à démontrer le théorème de D'ALEMBERT–GAUSS affirmant que $\mathbb{C}$ est algébriquement clos.

2. pour peu qu'elle soit « « bonne » »

V,) les contraint considérablement. Il en résulte donc finalement qu'il n'y a que très peu de tels groupes et partant que très peu de polyèdres convexes réguliers.

Plus précisément :

0.2.1. – Étant donné un polyèdre Π, certaines isométries de l'espace $\mathbb{R}^3$ euclidien le laissent invariant. Autrement dit il s'agit des éléments $f \in \mathcal{O}_3(\mathbb{R})$ tels que $f(\Pi) = \Pi$. On espère qu'il reste encore au lecteur quelques souvenirs de ce que sont les groupes $\mathcal{O}_3(\mathbb{R})$ (resp. $\mathcal{SO}_3(\mathbb{R})$) des isométries de l'espace $\mathbb{R}^3$, (resp. des déplacements de l'espace $\mathbb{R}^3$.) On associera, en effet, au polyèdre Π l'ensemble

$$G := \{g \in \mathcal{SO}_3(\mathbb{R}) \; ; \; g(\Pi) = \Pi\} \; . \qquad 0.2.1.1$$

On établira d'abord, ce qui est un exercice sur les définitions, que G est un sous-groupe (cf. III.3.1,) de $\mathcal{SO}_3(\mathbb{R})$ (cf. TD n° III, exercice J.)

Nous nous abstenons ici de donner une définition absoluement rigoureuse de ce que sont les sommets, les arêtes et les faces d'un polyèdre (et même ce qu'est un polyèdre) car l'idée que chacun à pu s'en faire au cours de ses études est amplement suffisante pour cette présentation. Or si s est un sommet de Π et (a_1, a_2, a_3) un triplet d'arêtes adjacentes en s, (a_1, a_2, a_3) est une famille libre (donc une base) de $\mathbb{R}^3$. On ne justifie pas ici que cette situation se produise toujours, même si c'est effectivement le cas. Il se trouve alors que pour $f \in G$, $\big(f(a_1), f(a_2,), f(a_3)\big)$ est encore un triplet d'arêtes adjacentes en $f(s)$ et donc encore une base de $\mathbb{R}^3$. La donnée de $\big(f(a_1), f(a_2), f(a_3)\big)$ détermine alors complètement f. Or il y a un nombre fini de triplets d'arêtes adjacentes dans Π si bien que le nombre de déplacements laissant Π invariant est donc fini. Autrement dit, le groupe G est un groupe fini.

0.2.2. – Reste donc à comprendre, au moins dans les grandes lignes, puisque précisément la suite de ce cours prétend fournir les outils nécessaires à la compréhension des détails, ce qui empêche qu'il existe beaucoup de sous-groupes finis de $\mathcal{SO}_3(\mathbb{R})$. La raison en est, qu'un certain nombre d'invariants numériques associés à ces groupes vérifient une équation dite *équation caractéristique* (cf. 0.2.2.6,) dont il est pour le coup très élémentaire d'établir qu'elle a très peu de solution. Les éléments les plus avancés de théorie des groupes que nous étudierons dans ce cours, notamment au chapitre V, sont nécessaire pour définir les grandeurs intervenant dans l'équation caractéristique ainsi que les relations entre ces grandeurs.

En premier lieu, on rappelle que, pour tout élément $f \in \mathcal{SO}_3(\mathbb{R})$ différent de l"identité il existe un unique couple $(p_1, p_2) \in \mathbb{R}^3 \times \mathbb{R}^3$ tel que p_1 et p_2 sont de norme 1 et fixes par f, *i.e.*

$$f(p_1) = p_1 \text{ et } f(p_2) = p_2 \; .$$

Il se trouve d'ailleurs qu'alors $p_1 = -p_2$. Les vecteurs p_1 et p_2 sont appelés *pôles* de f.

Étant donné un sous-groupe $G \subset \mathcal{SO}_3(\mathbb{R})$, on note

$$G^* := G \setminus \{\mathrm{Id}\}$$

et P l'ensemble des pôles des éléments de G^*. On note encore

$$\mathcal{F} \ := \ \{(g,p) \ \in \ G^* \times P \ ; \ g(p) \ = \ p\} \ . \qquad 0.2.2.1$$

On suppose désormais que G est fini à n éléments si bien que G^* possède $n-1$ éléments. Chaque élément de G^* ayant exactement 2 pôles P contient au plus $2(n-1)$ éléments, deux éléments de G^* pouvant partager la même paire de pôles. L'équation caractéristique du groupe G résulte du fait que l'on peut compter les éléments de $\mathcal{F}$ de deux manières différentes. L'ensemble $\mathcal{F}$ étant un sous-ensemble du produit cartésien $G^* \times P$, on pourrait le représenter sur un graphique en portant les éléments de G en abscisse et les éléments de P en ordonnée. On peut donc dénombrer les éléments de $\mathcal{F}$ soit en faisant la somme sur les colonnes soit sur les lignes.

La somme sur les colonnes est très élémentaire. En effet pour un élément $g \ \in \ G^*$ fixé, les couples (g,p) tels que $g(p) \ = \ p$, sont exactement les couples (g,p) tels que p soit un pôle de g. Or on a dit plus haut qu'un élément de G^* a exactement 2 pôles. Il en résulte que :

$$\#(\mathcal{F}) \ = \ 2(n-1) \ . \qquad 0.2.2.2$$

Dénombrer les éléments de $\mathcal{F}$ suivant les lignes fait précisément intervenir un certain nombre d'arguments de théorie des groupes.

Tout d'abord si p est un pôle, il existe $h \ \in \ G$, tel que $h(p) \ = \ p$, ce qui entraîne que

$$g * h * g^{-1}\big(g(p)\big) \ = \ g(p)$$

donc que $g(p)$ est un pôle de $g * h * g^{-1} \ \in \ G^*$ (cf. V.3.) Ces constructions seront détaillées et précisées au TD n° V, exercice B et au TD n° V, exercice C. On constate cependant d'ores et déjà que G transforme élément de P en éléments de P et l'on dit que G *agit* ou *opère* sur P (cf. V.1.1.)

Pour un pôle p fixé,

$$\mathrm{Stab}_G(p) \ := \ \{g \ \in \ G \ ; \ g(p) \ = \ p\}$$

est un sous-groupe de G appelé *stabilisateur* de p (cf. V.1.15.) Puisque $\mathrm{Id} \ \in \ \mathrm{Stab}_G(p)$,

$$\#\big(\mathrm{Stab}_G(p) \cap G^*\big) \ = \ \#(\mathrm{Stab}_G(p)) - 1 \ .$$

On pourrait alors écrire une formule :

$$\#(\mathcal{F}) \ = \ \sum_{p \in P} \#(\mathrm{Stab}_G(p)) - 1 \ . \qquad 0.2.2.3$$

Outre que cette formule n'est pas très exploitable en soi, on peut encore aller plus loin graçe à d'autres arguments de théorie des groupes.

On va donc regrouper les éléments de P en sous-ensembles de pôles pouvant se déduire les uns des autres par l'action de G. Autrement dit, pour un pôle donné p son *orbite* (cf. V.1.9.i),) $O(p)$ est définie par

$$O(p) \ := \ \{g(p) \ , \ g \ \in \ G\} \ .$$

Les orbites forment une partition (cf. I.5.3,) de P. L'ensemble P étant fini il y a donc un nombre fini r d'orbites $(O_1, \ldots, O_r)$, chacune d'entre elle étant elle-même un ensemble fini. La formule 0.2.2.3 se réécrit donc :

$$\#(\mathcal{F}) \ = \ \sum_{i=1}^{r} \sum_{p \in O_i} \#(\mathrm{Stab}_G(p)) - 1 \ . \qquad 0.2.2.4$$

La proposition V.1.18 permet encore de faire une réduction assez considérable dans la formule si dessus. En effet, même si deux éléments p et q de la même orbite O_i n'ont pas nécessairement le même stabilisateur, $\#(\mathrm{Stab}_G(p)) \ = \ \#(\mathrm{Stab}_G(q))$. En notant

$$s_i \ := \ \#(\mathrm{Stab}_G(p)) \, {}_{,p \in O_i \ , lleq1ir} \ ,$$

la formule 0.2.2.4 devient :

$$\#(\mathcal{F}) \ = \ \sum_{i=1}^{r} \#(O_i)(s_i - 1) \ . \qquad 0.2.2.5$$

Le corollaire V.1.17 à la proposition V.1.16, qui est un résultat clef de la théorie des actions de groupes, permet de réécrire 0.2.2.5 $\#(\mathcal{F}) \ = \ \sum_{i=1}^{r} n - \#(O_i)$. Il en résulte, grâce à 0.2.2.2,

$$2(n-1) \ = \ \sum_{i=1}^{r} n - \#(O_i)$$

qui donne l'*équation caractéristique* du groupe G :

$$2 - \frac{2}{n} \ = \ \sum_{i=1}^{r} 1 - \frac{1}{s_i} \ . \qquad 0.2.2.6$$

Un jeu d'inégalité sur cette équation, 0.2.2.6 permet d'abord d'éxclure le cas $r \ = \ 1$, puis de montrer que $r < 4$.

Théorème 0.2.2.7 *Les solutions de l'équation caractéristique sont :*

1)

$$r \ = \ 2 \ , \ s_1 \ = \ s_2 \ = \ n \ ;$$

2) $r = 3$ *et alors :*

i) $(2, 2, \frac{n}{2})$ *et donc* n *est pair ;*

ii)

$$(2, 3, 3) \text{ et } n = 12 ;$$

iii)

$$(2, 3, 4) \text{ et } n = 24 ;$$

iv)

$$(2, 3, 5) \text{ et } n = 60 .$$

Ce théorème a en particulier pour conséquence que le nombre de sous-groupes finis de $\mathcal{SO}_3(\mathbb{R})$ qui peuvent être des groupes de transformations de polyèdres réguliers est fini. On peut ensuite en déduire qu'il y a un nombre fini de classes de polyèdres convexes réguliers. En affinant encore l'étude on montrerai qu'il y a en fait :

— le tétraèdre,
— le cube,
— l'octaèdre,
— le dodécaèdre,
— l'icosaèdre.

0.3 . −la preuve par GAUSS du cas $n = 3$ de la conjecture de FERMAT

On rappelle, s'il en était besoin, que FERMAT avait assuré que pour un entiers $n \geq 3$, il n'existait aucun triplet (a, b, c) d'entiers, tous non nuls, tel que

$$a^n + b^n = c^n .$$

On doute que, contrairement à ce quil afirmait, FERMAT ait jamais connu une preuve de ce résultat. La démonstration du cas général est évidemment hors de portée de ce cours et même la spectaculaire avancée obtenue par Kummer au XIXe siècle nécessiterait de mettre en œuvre des outils dont nous ne disposerons pas.

En revanche la stratégie utilisée par GAUSS pour résoudre le cas $n = 3$, pourrait être exposée en détail avec le matériel dont nous disposerons à la fin de ce cours. Montrer qu'il n'y a pas de solutions à l'équation de FERMAT dans un ensemble plus vaste que les entiers relatifs pourrait constituer la première surprise de cette démarche. Et pourtant, la méthode esquissée ci-après consiste à chercher à résoudre l'équation de FERMAT non dans l'ensemble $\mathbb{Z}$ des entiers relatifs mais dans l'ensemble $\mathbb{Z}[j]$ des entiers d'Eisenstein (cf.

IX.1.4.d).)En effet l'ensemble $\mathbb{Z}[j]$ est un anneau (cf. VII.1.1,) et même un *anneau principal* (cf. IX.1.2,) auquel on peut donc appliquer toute la machinerie dévelopée au chapitre IX.Cet anneau contient $\mathbb{Z}$ si bien que l'absence de solution dans $\mathbb{Z}[j]$ entraînera immédiatement l'absence de solutions dans $\mathbb{Z}$. Avant de tenter de faire comprendre avec les quelques idées qui suivent, pourquoi en « agrandissant » l'ensemble où chercher de potentielles solutions, on simplifie les arguments, il convient de remarquer que la méthode utilisée ici ne se généraliserait pas aux cas d'exposants n grands dans l'équation de FERMAT, précisément parce que les aneaux qui seraient alors impliqués dans la construction ne seraient en particulier pas principaux. Certains historiens pensent que ce serait précisément ce point qui aurait échappé à FERMAT ...

On rappelle que j désigne un nombre complexe vérifiant

$$j^3 \;=\; 1 \text{ et } j \;\neq\; 1 \text{ si bien que } 1 \;+\; j \;+\; j^2 \;=\; 0\,. \tag{0.3.1}$$

On note $\pi \;:=\; 1 - j$, qui est un élément premier (cf. VII.5.4,) de $\mathbb{Z}[j]$. On note v la valuation qui lui est associée (cf. IX.6.5.)La méthode dite de *descente infinie* consiste à montrer que si l'on dispose d'un triplet $(a, b, c) \;\in\; \mathbb{Z}[j]^3$, solution de l'équation de FERMAT $a^3 + b^3 \;=\; c^3$, il en existe une autre $(a', b', c',)$ telle que $v(abc) > v(a'b'c')$. Or v étant une application à valeurs dans $\mathbb{N}$, on aboutit à une contradiction. Les étapes de la constructions sont essentiellement celles qui suivent :

Soit $(a, b, c) \;\in\; \mathbb{Z}[j]^3$ deux à deux premiers entre eux (cf. VII.5.9,) (ce qu'on peut supposer au terme d'un argument très élémentaire) et vérifiant $a^3 + b^3 \;=\; c^3$ ou encore, quitte à changer c en $-c$:

$$a^3 \;+\; b^3 \;+\; c^3 \;=\; 0\,. \tag{0.3.2}$$

Ce qui a pour conséquence immédiate que :

$$(a + b + c)^3 \;=\; 3(a + b)(b + c)(c + a)\,. \tag{0.3.3}$$

Par ailleurs on calcul immédiatement que

$$\pi^2 \;=\; (1 - j)^2 \;=\; 1 - 2j + j^2 \;=\; -3j,$$

d'où $-j^2\pi^2 \;=\; 3$, d'où il résulte, que

$$\pi^2 | (a + b + c)^3\,.$$

Comme π est premier le lemme de GAUSS (cf. IX.3.3,)entraîne que :

$$\pi | (a + b + c) \tag{0.3.4}$$

donc $\pi^3|(a+b+c)^3$ c'est-à-dire que $\pi^3|-j^2\pi^2(a+b)(b+c)(c+a)$ d'où finalement :

$$\pi|(a+b)(b+c)(c+a)\,. \tag{0.3.5}$$

En appliquant une fois encore le lemme de GAUSS on montre que π divise l'un des trois facteurs $(a+b)$, $(b+c)$ ou $(c+a)$. Supposons que $\pi|a+b$. Comme d'après 0.3.4, $\pi|a+b+c$:

$$\pi|c \;\Leftrightarrow\; v(c) \;>\; 0\,. \tag{0.3.6}$$

Quitte à étudier l'anneau $\mathbb{Z}[j]/\pi\mathbb{Z}[j]$ (cf. IX.4,)on peut déduire de ce qi précède que :

$$a \;\equiv\; 1\,[\pi] \text{ et } b \;\equiv\; -1\,[\pi] \text{ d'où } v(a) \;=\; v(b) \;=\; 0 \text{ et } v(abc) \;=\; (vc) \;>0\,. \tag{0.3.7}$$

Une étude un peu plus approfondie de l'anneau quotient $\mathbb{Z}[j]/\pi^2\mathbb{Z}[j]$ permettrait d'établir que, quitte à multiplier a (resp. b) par j ou j^2, on peut même supposer qu'on a un triplet :

$$\begin{array}{rcl} (a,b,c) \;\in\; \mathbb{Z}[j]^3 \text{ tel que} \quad a^3+b^3+c^3 &=& 0 \\ c &\equiv& 0\,[\pi] \\ a &\equiv& 1\,[\pi^2] \\ b &\equiv& -1\,[\pi^2]\,. \end{array} \tag{0.3.8}$$

Les trois entiers d'Eisenstein

$$\begin{array}{rcl} A := \quad (a+bj)/\pi &=& \frac{1}{\pi}(a+b-b\pi) \\ B := \quad (aj+b)/\pi &=& \frac{1}{\pi}(a+b-a\pi) \\ C := \quad j^2(a+b)/\pi & & \end{array} \tag{0.3.9}$$

sont
— premiers entre eux
— de somme nulle :

$$\pi(A+B+C) \;=\; (1+j+j^2)(a+b) \;=\; 0\,; \tag{0.3.10}$$

— congrus respectivement à 1, -1 et 0 mod π ;
— et leur produit est un cube non nul :

$$\begin{array}{rcl} \pi^3 ABC & = & (a+bj)(a+bj^2)(a+b) \\ & = & a^3+b^3 \\ & = & -c^3\ . \end{array} \qquad 0.3.11$$

Il existe donc $\theta \in \mathbb{Z}[j]$ tel que :

$$ABC \ = \ \theta^3 \text{ pour } \theta \ := \ -\frac{c}{\pi}\ ; \qquad 0.3.12$$

On peut alors montrer qu'il existe $(a', b', c') \in \mathbb{Z}[j]^3$ tel que :

$$\begin{array}{rcl} A & = & a'^{,3}, \\ B & = & b'^{,3}, \\ C & = & c'^{,3} \\ c' & := & \theta/(a'b'))\ . \end{array} \qquad 0.3.13$$

L'identité 0.3.10 combinée à 0.3.13 montre alors que (a', b', c') est une solution de l'équation de FERMAT. En utilisant 0.3.12 il vient :

$$(a'b'c')^3\pi^3 \ = \ ABC\pi^3 \ = \ (\theta\pi)^3 \ = \ -c^3\ . \qquad 0.3.14$$

D'où il résult $3v(a'b'c') \ + \ 3 \ = \ 3v(c)$ c'est-à-dire

$$v(a'b'c') \ = \ v(c) - 1$$

et finalement en utilisant 0.3.6 :

$$v(a'b'c') \ = \ v(abc) \ - \ 1\ . \qquad 0.3.15$$

I . −un bref survol de téhorie des ensembles

I.1 . −Le système de ZERMELO fini

Faute de pouvoir « définir » les ensembles (à partir de quoi d'ailleurs) on est amené à proposer une axiomatique des ensembles. Une fois encore la pertinence de ce point de vue, qui pourrait paraître dogmatique, ne se révèlera que dans le fait que l'on puisse écrire les mathématiques de manière convenable dans ce cadre et en particulier que l'arithmétique dont

nous avons l'habitude (appuyée sur les axiomes de PEANO (cf. 0.1,)) puisse se faire au sein de cette théorie grâce en particulier à des résultats comme la proposition I.3.10.

Les axiomes de la théorie **ZFC** sécrivent avec les symboles de la logique dont nous rappelons la signification, mais pour lesquels nous ne rappelons pas ici les règles qui font qu'un enchaînement de tels symboles constitue ou non une proposition correcte :

Notation I.1.1 i) $\forall$: pour tout (quantificateur universel ;)

ii) $\exists$: il existe ;

iii) et ou $\wedge$: et (conjonction ;)

iv) ou ou $\vee$: disjonction ;

v) non ou $\not$ négation ;

vi) $\Rightarrow$: implication.

Le système de ZERMELO *fini* $\mathbf{Z}_{\text{fini}}$ explicité ci-après fournit un premier point de départ à la théorie **ZFC** donnée en I.4.2. Il consiste en un certain nombre d'axiomes qui sont des propositions écrites avec les symboles de la logiques rappelés ci-dessus et dont les seules variables sont des ensembles. Il comportent en outre et principalement le symbole $\in$ dont en quelque sorte, il fixe la « grammaire ». On pourait à juste titre s'étonner une fois encore ici que les axiomes de $\mathbf{Z}_{\text{fini}}$ (et ceux de **ZFC** ne feront pas mieux d'ailleurs) ne « construisent un monde où il n'y a que des ensembles » alors que l'intuition semble suggérer qu'il « existe » des objets mathématiques de « nature » multiple et diverse. Une fois encore le « miracle » tient à des énoncés du genre de la proposition I.3.10 qui assurent que ce « monde » des ensembles est assez vaste pour représenter une partie substantiellle des mathématiques. En outre l'homogénéité de ce système est d'une grande lisibilité pour les questions relatives à la cohérence de l'édifice mathématique.

Notation I.1.2 ($\Leftrightarrow$) Nous utiliseront librement dans la suite, pour deux proposition P et Q $P \Leftrightarrow Q$ qui ne signifie rien de plus (mais rien de moins d'ailleurs), que

$$P \Rightarrow Q \wedge Q \Rightarrow P .$$

Définition I.1.3 (Le système $\mathbf{Z}_{\text{fini}}$) $\mathbf{Z}_{\text{fini}1}$) (Ext)

$$\forall a, b \, (\forall x \, (x \in a \Leftrightarrow x \in b) \Rightarrow a = b) ,$$

$\mathbf{Z}_{\text{fini}\,2}$) (Paire)

$$\forall a, b\, \exists c\, (a \in c \text{ et } b \in c)\ ,$$

$\mathbf{Z}_{\text{fini}\,3}$) (Un)

$$\forall a\, \exists b\, \forall x\, (\exists y\, (x \in y \text{ et } y \in a)\ \Rightarrow\ x \in b)\ ,$$

$\mathbf{Z}_{\text{fini}\,4}$) (Par)

$$\forall a\, \exists b\, \forall x\, (\forall y\, (y \in x\ \Rightarrow\ y \in a)\ \Rightarrow\ x \in b)\ ,$$

et pour chaque formule ensembliste $F(x, c)$ où a et b n'apparaissent pas comme variables libres,

$\mathbf{Z}_{\text{fini}\,5}$) ($\mathbf{Sep}_F$)

$$\forall a\, \forall c\, \exists b\, \forall x\, (x \in b\ \Leftrightarrow (x \in a \text{ et } F(x, c)))\ .$$

Les axiomes ci-dessus permettent d'introduire de nouveaux symboles :

Définition I.1.4 (Symboles du langage ensembliste) i) ($\subset$:)

$$\forall a,\ \forall b,\ (a\ \subset\ b\ \Leftrightarrow\ (\forall x(x \in a \Rightarrow x \in b))\ .$$

ii) ($\mathcal{P}(\cdot)$:)
L'ensemble b introduit dans l'axiome I.1.3.$\mathbf{Z}_{\text{fini}\,4}$) sera noté $\mathcal{P}(a)$.

iii) ($\bigcup$:)
L'ensemble b introduit dans l'axiome de l'union I.1.3.$\mathbf{Z}_{\text{fini}\,3}$) peut être noté

$$\bigcup_{x \in a} x\ .$$

iv) ($\cup$:)
Pour deux ensembles a et b l'axiome de la paire I.1.3.$\mathbf{Z}_{\text{fini}\,2}$) assure que $c\ :=\ \{a, b\}$ est bien un ensemble et l'on peut dès lors grâce au point précédent, noter

$$a\ \cup\ b\ :=\ \bigcup_{x \in c} x\ =\ \bigcup_{x \in \{a,b\}} x\ .$$

v) ($\cap$:)

$$\forall a,\ \forall b,\ \forall x, (x \in\ a\ \cap\ b\ \Leftrightarrow\ x \in a\ \wedge\ x \in b)\ .$$

vi) ($\emptyset$:)

$$\forall x(x\ =\ \emptyset\ \Leftrightarrow\ \forall y(y \notin x))\ .$$

Définition I.1.5 i) (**Formules ensemblistes**)

On appelle *formule ensembliste* une formule comportant des variables, les symboles de la logique (cf. I.1.1) et le symbole $\in$.

ii) (**Formules ensemblistes étendues**)

On appelle *formule ensembliste étendue* une formule comportant des variables, les symboles de la logique et les symboles supplémentaires définis en I.1.4.

Remarque I.1.6 Il faut noter que toute formule ensembliste étendue peut se reformuler à l'aide de formule ensemblistes et que par conséquent, on pourra les utiliser dans la suite sans sortir du cadre des axiomes I.1.3 y compris pour formuler de nouveaux axiomes. Un bon exercice consiste à réécrire avec les symboles de I.1.4 ceux des axiomes de I.1.3 qui peuvent l'être leur donnant alors une forme plus lisible et plus usuelle.

I.2 . −Représentation des objets mathématique

On peut désormais constater qu'un certain nombre de constructions très usuelles peuvent être faite dans le cadre de la théorie des ensembles :

Définition I.2.1 i) (**Couples**)

Au regard des axiomes de I.1.3, seules les paires existent. Or dans une paire il est impossible de parler de l'ordre des éléments : $\{x, y\}\ =\ \{y, x\}$. On peut représenter le *couple* (x, y) par $\big\{\{x, y\}, \{x\}\big\}$. C'est alors un bon exercice sur les manipulations des axiomes de I.1.3 de montrer que $(x, y)\ \neq\ (y, x)$.

ii) (**Produit cartésien**)

Dès l'instant où l'on dispose de couples on peut définir le *produit cartésien* de deux ensembles a et b noté $a \times b$ par :

$$a \times b\ :=\ \{(x, y)\ ;\ x \in a,\ y \in b\}\ .$$

iii) (**Relation**)
une *relation* (ou *relation binaire*) sur un ensemble a est alors une partie R du produit cartésien $a \times a$. À la notation naturellement issue du formalisme développé jusqu'ici $(x, y) \in R$, on préférera bien sûr, celle tout à fait usuelle et connue de $x\ R\ y$.

iv) (**Fonction**)
Une *fonction* f d'un ensemble a dans un ensemble b est une partie du produit cartésien $a \times b$ [3] telle que

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

Autrement dit un élément de a possède au plus une image par f. Ici encore on continuera à écrire (comme on l'a toujours fait) $y = f(x)$ pour $(x, y) \in f$.

On rappelle maintenant quelques définitions espérons-le bien connues concernant les relations et les fonctions :

Définition I.2.2 (Relations) Soit a un ensemble et R une relation sur a :

i) (**Réflexivité**)
On dit que R est *réflexive* si

$$\forall x \in a,\ x\ R\ x\ .$$

ii) (**Symétrie**)
On dit que R est *symétrique* si

$$\forall x \in a,\ \forall y \in a,\ (x\ R\ y\ \Rightarrow\ y\ R\ x)\ .$$

iii) (**Antisymétrie**)
On dit que R est *antisymétrique* si

$$\forall x \in a,\ \forall y \in a,\ (x\ R\ y\ \wedge\ y\ R\ x\ \Rightarrow x = y)\ .$$

iv) (**Transitivité**)
On dit que R est *transitive* si

$$\forall x \in a,\ \forall y \in a,\ \forall z \in a,\ (x\ R\ y\ \wedge\ yRZ\ \Rightarrow x\ R\ z)\ .$$

v) (**Relation d'équivalence**)
On dit que R est une *relation d'équivalence* si elle est réflexive symétrique et transitive.

3. Autrement dit on représente une fonction par son *graphe*.

vi) (**Relation d'ordre**)

On dit que R est une *relation d'ordre* si elle est réflexive antisymétrique et transitive. On dit alors que le couple (a, R) est un *ensemble ordonné*. On dit que R est une *relation d'ordre totale* si

$$\forall x \in a,\ \forall y \in a,\ (x\ R\ y\ \vee\ y\ R\ x)\ ;$$

dans ce cas on dit que le couple (a, R) est un *ensemble totalement ordonné*.

vii) (**Majorant/minorant** . . .)

Si $(a, \leq)$ est un ensemble ordonnée et b
$subseta$ une partie de a : Un *majorant* (resp. *minorant*) pour b (dans a,) est un élément $x \in a$ vérifiant

$$\forall y \in b,\ (y \leq x) \text{ resp. } (\forall y \in b,\ (x \leq y))\ .$$

Si b possède un majorant (resp. un minorant) on dit que b est *majoré* (resp. *minoré*.)

Un *plus grand élément* (resp. *plus petit élément*) pour b est un majorant (resp. minorant) de b appartenant à b.

Lemme I.2.3 *Si une partie $b \subset a$ d'un ensemble ordonné $(a, \leq)$ possède un plut petit (resp. plus grand) élément, celui-ci est unique.*

Preuve *: C'est une conséquence immédiate de l'antisymétrie des relations d'ordre.*

Définition I.2.4 (Fonctions) Soit f une fonction de a dans b

$$\text{ce que nous noterons } f\ :\ a\ \to\ b\ :$$

i) (**Domaine**)

On appelle *domaine* de f et on note

$$\mathrm{Dom}\, f\ :=\ \{x\ \in\ a\ ;\ \exists y \in b\ ;\ (x, y) \in f\}\ =\ \{x\ \in\ a\ ;\ \exists y \in b\ ;\ f(x)\ =\ y\}$$

le sous-ensemble de a formé des éléments qui ont une image par f.

ii) (**Image**)

On appelle *image* de f et on note

$$\mathrm{Im}\, f\ :=\ \{y\ \in\ b\ ;\ \exists x \in a\ ;\ (x, y) \in f\}\ =\ \{y\ \in\ b\ ;\ \exists x \in a\ ;\ f(x)\ =\ y\}$$

le sous-ensemble de b formé des éléments qui ont un antécédent dans a.

iii) (**Application**)
On dit que f est une *application* si $\mathrm{Dom}\, f = a$.

Notation I.2.5 Pour deux ensembles a et b on peut montrer que les applications de a dans b qui sont des parties de $a \times b$ *i.e.* des éléments de $\mathcal{P}(a \times b)$ forment un ensemble qu'on notera b^a.

Exemple I.2.6 a) (**Identité**)
Pour tout ensemble A (y compris $A = \emptyset$) l'ensemble A^A contient toujours au moins un élément noté Id_A appelé *identité de* A et caractérisé par

$$\forall x \in A,\ \mathrm{Id}_A(x) = x\ .$$

b) ($A^\emptyset$)
Il existe une unique application $\emptyset \to A$ si bien que $A^\emptyset$ est un singleton.

c) ($\emptyset^A$)
Si A n'est pas vide il n'existe aucune application de A dans $\emptyset$ $\emptyset^A$ est donc vide. En revanche $\emptyset^\emptyset$ est un singleton.

Définition I.2.7 (Applications) Soit $f : a \to b$ une application.

i) (**Injectivité**)
On dit que f est *injective* si

$$\forall x \in a,\ \forall y \in a,\ (f(x) = f(y) \Rightarrow x = y)\ .$$

ii) (**Surjectivité**)
On dit que f est *surjective* si

$$\forall y \in b,\ \exists x \in a (f(x) = y)\ .$$

iii) (**Bijectivité**)
On dit que f est *bijective* si elle est simultanément injective et surjective.

Définition I.2.8 (Restriction) Soient a et b des ensembles. Pour tout $c \subset a$, il est immédiat de vérifier que

$$(c \times b) \subset (a \times b)\ .$$

Pour toute fonction (resp. application) $f : a \to b$[4] il n'est pas difficile de constater non plus que $f \cap (c \times b)$ est une fonction (resp une application) de c dans b, qu'on appellera *restriction* de f à c et qu'on notera $f_{|c}$.

Lemme I.2.9 (Propriétés de la restriction) *i) Si $f : a \to b$ est une fonction $f_{|\mathrm{Dom}\, f}$ est une application.*

4. définie rappelons-le par son graphe (cf. I.2.1.iv),)

ii) Si $f : a \to b$ est une application injective, pour tout $c \subset a$, $f_{|c}$ est encore une application injective.

***Preuve** : Laissée en exercice.*

Définition I.2.10 (Applications et ordre) Si

$$f : (a, \leq) \to (b, \leq)$$

est une application d'un ensemble ordonné $(a, \leq)$ dans un ensemble ordonné $(b, \leq)$ on dit que f est *croissante* (resp. *décroissante*) si

$$\forall x \in a,\ \forall y \in a,\ \big(x \leq y \ \Rightarrow\ f(x) \leq f(y) (\text{resp. } f(y) \leq f(x))\big) .$$

On dit que f est *strictement croissante* (resp. *strictement décroissante* si

$$\forall x \in a,\ \forall y \in a,\ \big(x < y \ \Rightarrow\ f(x) < f(y) (\text{resp. } f(y) < f(x))\big) .$$

Lemme I.2.11 *Une application strictement croissante (resp. strictement décroissante) entre ensembles ordonnés est injective.*

Définition I.2.12 (Image directe/réciproque d'une partie)

Étant donnée une fonction $f : a \to b$,

i) (**Image directe**)
Pour toute partie $c \in a$ de a, on appelle *image directe* (ou simplement *image*) de c par f et on note $f(c)$ l'ensemble

$$f(c) := \{y \in b\,;\, \exists x \in a,\ y = f(x)\} .$$

C'est aussi l'image $\mathrm{Im}\, f_{|c}$ de la restriction de f à c.

ii) (**Image réciproque**)
Pour toute partie $d \in b$ de b, on appelle *image réciproque* de d par f l'ensemble noté

$$f^{-1}(d) := \{x \in a\,;\, f(x) \in d\} .$$

Remarque I.2.13 (ATTENTION) La notation $f^{-1}(d)$ ci-dessus ne signifie pas qu'il existe une fonction f^{-1} et que $f^{-1}(d)$ soit l'image directe de d par cette fonction.

Dans le cas où f est bijective, il existe effectivement une bijection réciproque $g : b \to a$ vérifiant

$$f \circ g = \mathrm{Id}_b \text{ et } g \circ f = \mathrm{Id}_a .$$

Alors pour toute partie $d \in b$ de b, c'est un exercice (qu'il convient de faire si on ne l'a jamais fait auparavant) de montrer que

$$f^{-1}(d) = g(d) .$$

Proposition I.2.14 (Produit) *Étant donnés deux ensembles a et b, on définit les applications*

$$p : a \times b \to a , (x, y) \mapsto x \text{ et } q : a \times b \to b , (x, y) \mapsto y .$$

Alors :

i) Les applications p et q sont surjectives.

ii) Pour tout ensemble c et tout couple d'applications

$$\big(f : c \to a, g : c \to b\big),$$

il existe une unique application

$$h : c \to a \times b \text{ telle que } p \circ h = f \text{ et } q \circ h = g .$$

Définition I.2.15 Avec les notations de la proposition ci-dessus, l'application p (resp. q,) est appelée *première projection* (resp. *deuxième projection*) ou encore *projection sur le premier facteur* (resp. *projection sur le deuxième facteur*.)

I.3 . −Représentation des entiers

On vient de voir qu'un certain nombre de construction usuelles peuvent se faire dans le cadre des axiomes de ZERMELO finis I.1.3. On va expliquer sommairement maintenant comment ils permettent presque de représenter les entiers ou tout au moins une classe d'objet satisfaisant les axiomes de PEANO 0.1. On s'apercevra cependant que les axiomes de I.1.3 ne sont pas tout à fait suffisants et la possibilité de faire de larithmétique motivera suffisaemment, espérons-le, du moins, l'introduction de l'axiome de l"infini I.3.4.

Remarque I.3.1 Les axiomes I.1.3.$\mathbf{Z}_{\text{fini}\,4}$) et I.1.3.$\mathbf{Z}_{\text{fini}\,5}$) permettent de définir pour tout ensemble a le singleton

$$\{a\} := \{b \in \mathcal{P}(a) ; a\, b = a\} .$$

L'union de deux ensembles construite en I.1.4.iv) permet ensuite de définir $\mathfrak{s}(a) := a \cup \{a\}$.

Exemple I.3.2 Rien dans l'axiomatique I.1.3 n'assure jusqu'ici que l'ensemble vide $\emptyset$ défini en I.1.4.vi) existe ni même qu'il existe aucun ensemble. Cependant on pourrait s'interroger sur le bien fondé d'une théorie sans objets. De toute façon l'axiome de l'infini I.3.4 remediera à cette lacune. Même si nous en donnerons une formulation impliquant le symbole $\emptyset$ il faut se persuader qu'on pourrait en donner une formulation purement ensembliste au sens de la définition I.1.5.i) et qu'alors l'existence de l'ensemble vide s'en déduit grâce aux axiomes de séparation I.1.3.$\mathbf{Z}_{\text{fini}\,5}$).

À ce point, si on suppose cependant que $\emptyset$ existe on a :

$$\begin{array}{rcl} \mathfrak{s}(\emptyset) & = & \emptyset \cup \{\emptyset\} \\ & = & \{\emptyset\}, \\ \mathfrak{s}(\mathfrak{s}(\emptyset)) & = & \{\emptyset\} \cup \{\{\emptyset\}\} \\ & = & \big\{\emptyset, \{\emptyset\}\big\} \\ \mathfrak{s}(\mathfrak{s}(\mathfrak{s}(\emptyset))) & = & \big\{\emptyset, \{\emptyset\}\big\} \cup \big\{\big\{\emptyset, \{\emptyset\}\big\}\big\} \\ \big\{\emptyset, \{\emptyset\}, \big\{\emptyset, \{\emptyset\}\big\}\big\} & \ldots & \end{array} \qquad \text{I.3.2.1}$$

On s'aperçoit qu'à chaque opération $\mathfrak{s}$, le « nombre d'éléments » augmente d'un et que les ensembles ainsi construits pourraient être de bons candidats pour représenter les entiers, pour peu qu'on puisse les « équiper » de suffisamment de « structure algébrique » *i.e.*$+, \cdot, \ldots$

On va donc préciser un peu ce qui précède sans toutefois entrer trop dans les détails.

Définition I.3.3 (Ensembles récurrent) On dit qu'un ensemble a est *récurrent* si

$$\emptyset \in a \text{ et } \forall x \in a,\ (\mathfrak{s}(x) \in a)\ .$$

On a dès lors le sentiement qu'un ensemble représentant les entiers naturels c'est-à-dire satisfaisant aux axiomes de PEANO (cf. 0.1,)devrait être un ensemble récurrent pour satisfaire notamment l'axiome
0.1.PA_3).

Cependant à ce point il ne semble pas possible d'établir l'existence même de telles ensembles uniquement à partir des axiomes du système de ZERMELO fini I.1.3. Dans ce cas on a recours à l'introduction d'un nouvel axiome, lequel d'ailleurs ne choque pas la raison :

Définition I.3.4 (Axiome de l'infini) On appelle *axiome de l'infini* la formule :

$$\exists a(\emptyset \in a \text{ et } \forall x \in a,\ (\mathfrak{s}(x) \in a))\ .$$

Définition I.3.5 (Système de ZERMELO Z) On appelle *système de* ZERMELO le système d'axiomes constitué des axiomes de ZERMELO fini I.1.3 auquel on adjoint l'axiome de l'infini.

Autrement dit il existe au moins un ensemble récurrent. Cependant parmi les ensembles récurrents reste à déterminer le bon candidat pour représenter les entiers naturels, c'est-à-dire, moralement, celui qui contiendrait les entiers naturels ; rien de plus rien de moins. Moyennant de vérifier le lemme :

Lemme I.3.6 *L'intersection de deux ensembles récurrents est un ensemble récurrent.*

On peut introduire l'ensemble ω défini comme suit :

Définition I.3.7 On notera ω le plus petit ensemble récurrent.

On se convainc assez facielement à ce point que le couple $(\omega, \mathfrak{s})$ doit satisfaire les axiomes 0.1.PA$_1$), 0.1.PA$_2$) et 0.1.PA$_3$) mais reste la questions des axiomes
0.1.PA$_4$) à 0.1.PA$_7$).

Notation I.3.8 Pour deux ensembles a et b les axiomes de I.1.3 assurent que pour deux ensembles distincts x et y :

$$a \ + \ b \ := \ (a \times \{x\}) \ \cup \ (b \times \{y\}) \qquad \text{I.3.8.1}$$

et

$$a \ \cdot \ b \ := \ a \ \times \ b \qquad \text{I.3.8.2}$$

sont des ensembles et que le premier (resp. le second) possède un nombre d'élément égal à la somme (resp. au produit) du nombre d'éléments de a et du nombre d'éléments de b.

Ce qui en revanche est nettement moins évident et fait l'objet du lemme suivant est que si a et b sont des éléments de ω il en est de même de leur produit et de leur somme. Un tel résultat peux s'appuyer sur la théorie des bons ordres dont le développement dépasserait largement le cadre de cette déjà longue introduction.

Lemme I.3.9 *Pour tout* $a \in \omega$, *tout* $b \in \omega$,

$$a \ + \ b \ \in \ \omega \, \text{et} \, a \ \cdot \ b \ \in \ \omega \, .$$

La proposition qui suit, et dont nous ne pouvons avec les éléments dont nous disposons, donner une preuve, bien qu'une telle preuve soit possible à partir du système de ZERMELO, assure finalement qu'un modèle de l'arithmétique existe dans la théorie **Z** :

Proposition I.3.10 *Le quintuplet* $(\omega, \emptyset, \mathfrak{s}, +, \cdot)$ *vérifie les axiome de* PEANO *0.1*

I.4 . −Le système de ZERMELO–FRAENKEL

On présente les derniers axiomes qu'il faut adjoindre au système de ZERMELO I.3.5 pour arriver au système de ZERMELO–FRAENKEL **ZF** (cf. I.4.1,) puis finalement au système **ZFC** (cf. I.4.2.) On ne mentionnera ces axiomes que pour mémoire et parce que le système **ZF** voire **ZFC** est couramment utilisé par une large partie de la communauté mathématique :

Définition I.4.1 (Le système de ZERMELO–FRAENKEL ZF) Le *système de* ZERMELO–FRAENKEL est obtenu en adjoignant au système de ZERMELO les axiomes : Pour $F(x, y, c)$ formule ensembliste où a et b n'apparaissent pas comme variables libres, on appelle axiome de remplacement pour F :

ZF$_7$) (Remp$_F$)

$$\begin{array}{lll} \forall a \forall c & \big((\forall x, y, z((F(x, y, c) & \text{et} \& F(x, z, c)) \Rightarrow y = z\big) \\ \Rightarrow & \exists b \forall y \big(\exists x \in a(F(x, y, c)) & \Rightarrow \qquad\qquad y \in b)\big) \big) . \end{array}$$

ZF$_8$) (Fondation)

$$\forall a(a \neq \emptyset \Rightarrow \exists b \in a(b \cap a = \emptyset)) .$$

On réserve ordinairement une place à part à l'axiome du choix sans doute parce qu'un certain nombre de matthématiciens ne l'utilisent qu'avec une extrême circonspection tandis que certains autres le refusent tout bonnement. Le point de vue le plus pragmatique consiste à clairement désigner les résultats dont une preuve utilise l'axiome du choix.

Les deux résultats marquants de GÖDEL (1938) *s'il est cohérent, le système **ZF**ne réfute pas l'axiome du choix, c'est-à-dire qu'il n'existe pas de preuve de la négation de l'axiome du choix à partir des axiomes du système **ZF*** et COHEN (1963) *s'il est cohérent, le système **ZF**ne démontre pas l'axiome du choix, c'est-à-dire qu'il n'existe pas de preuve de l'axiome du choix à partir des axiomes du système **ZF*** ne permettent de choisir ni en sa faveur ni en sa défaveur.

Définition I.4.2 (ZFC) i) **(fonction de choix)**

Soit a un ensemble. On appelle *fonction de choix* sur a une application $f : a \setminus \{\emptyset\} \to a$ vérifiant $f(x) \in x$ pour tout x non vide dans a.

ii) **(Axiome du choix)**

On appelle *axiome du choix* l'énoncé : Tout ensemble possède une fonction de choix.

iii) (**Le système ZFC**)

On appelle *système* ***ZFC*** la famille d'axiomes constituée des axiomes de **ZF**
et de l'axiome du choix ci-dessus, c'est-à-dire constituée des axiomes de ZERMELO fini I.1.3
de l'axiome de l'infini I.3.4 des axiomes de remplacement I.4.1.$\mathbf{ZF}_7$)
de l'axiome de fondation I.4.1.$\mathbf{ZF}_8$)
et de l'axiome du choix.

I.5 . −Relations d'équivalence

Les relations d'équivalence, dont nous avons rappelé la définition en I.2.2.v), étant amenées à jouer un rôle majeur dans la plupart des constructions que nou développerons dans ce cours, il ne nous a pas paru vain de leur consacrer quelques lignes afin de rappler certaines de leur propriétés que nous espérons bien connues, ainsi que d'exposer quelques résultats moins habituels. Ainsi l'ensemble $\mathbb{Z}$ des entiers relatifs est construit au paragraphe IV.1

comme un ensemble de classes d'équivalences. On pourrait d'ailleurs s'interroger sur le bienfondé de cette méthode par opposition à une description de $\mathbb{Z}$ (que nous ne manquerons d'ailleurs pas de donner (cf. IV.2.5.ii),))

comme réunion d'entiers positifs et d'entiers négatif. L'expérience montrera cependant que la réunion ensembliste est une opération qui fait assez mauvais ménage avec les structures algébriques.

On va voir immédiatement que les relations d'équivalences constituent une sorte de description alternative aux applications surjectives. Bien mieux encore, nombre de relations que nous pourrons définir s'avérerons *compatible*s aux structures algébriques et fournirons dès lors non seulement des applications surjectives mais encore des *morphisme*s surjectifs (cf. I.6.17,) (cf. V.4, V.5,) (cf. VII.7.)

Définition I.5.1 (Classes (d'équivalence)) Étant donnée une relation binaire (cf. I.2.1.iii),) (pas nécessairement une relation d'équivalence,) $\sim$ sur un ensemble E, pour tout $x \in E$, on appelle *classe* de x selon $\sim$ (ou pour $\sim \dots$) le sous-ensemble $\overline{x} := \{y \in E\,;\, y \sim x\} \subset E$ de E.

Si $\sim$ est une relation d'équivalence, (ce qui est le cas qu'on rencontrera le plus souvent,) on parlera de *classe d'équivalence*.

Le lemme technique suivant permet d'établir bon nombre de résultats concernant les relations d'équivalence :

Lemme I.5.2 *Soit E un ensemble muni d'une relation d'équivalence $\sim$. Pour tout $(x, y) \in E \times E$, les assertions suivantes sont équivalentes :*

a)

$$x \sim y\,;$$

b)

$$\overline{x} \cap \overline{y} \neq \emptyset\,;$$

c)

$$\overline{x} \subset \overline{y}\,;$$

d)

$$\overline{x} = \overline{y}\,.$$

Preuve : *Voir l'exercice I.8.6.*

Nous allons maintenant comparer les relations d'équivalence à d'autres objets mathématique dont on va s'apercevoir qu'ils ne sont en fait que des descriptions alternatives de la même réalité. En premier lieu les partitions d'un ensemble :

Définition I.5.3 (Partition d'un ensemble) Soit E un ensemble. On rappelle qu'une *partition* de E est une partie B de l'ensemble $\mathcal{P}(E)$ des parties de E (ou encore un élément de $\mathcal{P}\big(\mathcal{P}(E)\big)$) vérifiant :

Part$_1$) $\emptyset \notin B$;

Part$_2$)

$$\forall X \in B,\ \forall Y \in B,\ \big(X \cap Y \neq \emptyset \Rightarrow X = Y\big)\,;$$

Part$_3$)

$$\bigcup_{X \in B} X = E\,.$$

Proposition I.5.4 *Étant donné un ensemble E,*

i) pour toute relation d'équivalence $\sim$ sur E, l'ensemble des classes selon $\sim$ est une partition de E ;

ii) réciproquement, étant donnée une partition P de E, il existe une unique relation d'équivalence sur E dont l'ensemble des classes est égal à P.

On définit ainsi une bijection entre l'ensemble des relations d'équivalence sur E et l'ensemble des partitions de E.

Preuve : *Voir l'exercice I.8.7.*

On compare maintenant les relations d'équivalence sur un ensemble E et les applications surjectives dont E est l'ensemble de départ :

Notation I.5.5 Pour un ensemble E muni d'une relation d'équivalence $\sim$, on note $E/\sim$ l'ensemble des classes d'équivalence selon $\sim$.

Proposition I.5.6 *Soit E un ensemble,*

i) pour toute relation d'équivalence $\sim$ sur E, l'application

$$\pi \,:\, E \,\to\, E/\sim\,,\; x \,\mapsto\, \overline{x}$$

est surjecctive ;

ii) réciproquement pour toute application surjective $\rho \,:\, E \,\to\, F$, il existe une unique relation d'équivalence $\sim$ sur E telle que l'application $E/\sim \,\to\, F, \overline{x} \mapsto \rho(x)$ soit une bijection bien définie. La relation $\sim$ est alors caractérisée par

$$x \,\sim\, y \,\Leftrightarrow\, \rho(x) \,=\, \rho(y)\,.$$

On définit ainsi une bijection de l'ensemble des relations déquivalences sur E dans l'ensemble des applications surjectives de E dans un ensemble F.

Preuve *: Voir l'exercice I.8.8.*

Définition I.5.7 Étant donné un ensemble E et une relation d'équivalence $\sim$, on appel

i) *ensemble quotient* l'ensemble $E/\sim$ et

ii) *surjection canonique* (et parfois même *projection canonique*) l'application

$$\pi \,:\, E \,\to\, E/\sim\,,\; x \,\mapsto\, \overline{x}\,.$$

I.6 . −Magma

Définition I.6.1 (Loi de composition) Pour un ensemble M on appelle *loi de composition* (ou *loi de composition interne* ou *loi interne*) $*$ sur M une application (cf. I.2.4.iii),)

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

Évidemment à la notation $((x,y),z) \in *$ qui découle de l'axiomatique présentée précédemment on préférera toujours celle $x * y \,=\, z$.

Le couple $(M,*)$ est appelé *magma*.

Définition I.6.2 (Morphisme homomorphisme) Étant donnés deux magmas

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

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

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

Lemme I.6.3 *i) Pour tout magma $(M, *)$ l'identité Id_M est un morphisme du magma M dans lui-même.*

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

Définition I.6.4 Étant donnés deux magmas $(M, *)$ et $(N, \cdot)$, un morphisme $f : M \to N$ est un *isomorphisme* s'il existe un morphisme $g : N \to M$ tel que

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

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

Proposition I.6.5 *Étant donnés deux magmas $(M, *)$ et $(N, \cdot)$, une application $f : M \to N$ est un isomorphisme si et seulement si c'est un morphisme bijectif.*

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

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

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

Alors :

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

Définition I.6.6 Soit $(M, *)$ un magma.

i) (**Enndomorphismes**)

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

ii) (**Automorphisme**)

Un morphisme $f : M \to M$ est un *automorphisme* si c'est à la fois un isomorphisme et un endomorphisme. Il revient au même, grâce à la proposition I.6.5, de dire que f est un endomorphisme bijectif. On note $\mathrm{Aut}(M)$ l'ensemble des automorphismes de M.

Exemple I.6.7 Pour un magma M, l'identité Id_M est un automorphisme de M.

Définition I.6.8 (Associativité) On dit qu'une loi de composition $*$ sur un ensemble M est *associative* si

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

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

Définition I.6.9 (Commutativité) On dit qu'une loi de composition $*$ sur un ensemble M est *commutative* si

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

Définition I.6.10 (Éléments particuliers) Soit $(M, *)$ un ensemble muni d'une loi de composition associative (magma associatif)

i) (**Élément neutre**)

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

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

ii) (**Symétrique**)

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

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

Remarque I.6.11 Dans la suite on ne considérera que des magmas associatifs dans la mesure où ce seront les seuls que nous rencontrerons. Il se peut que certains énoncés puissent être formulés sans cette hypothèse mais nous ne cherchons pas le plus grand degré de généralité possible mais une présentation que nous espérons la plus claire et la plus lisible ainsi que la moins répétitive.

Exemple I.6.12 Si X est un ensemble l'ensemble M des applications de X dans lui-même est un magma associatif pour la loi $\circ$ de composition des applications. Il possède un élément neutre Id_X. En revanche un élément $f : X \to X$ de M n'a pas de symétrique en général puisque f n'est pas bijective en général. La loi $\circ$ n'est en général pas commutative non plus.

Proposition I.6.13 (Propriétés) *Soient $(M, *)$ un magma associatif.*

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

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

Remarque I.6.14 On pourra donc parler de L'élément neutre d'un magma lorsqu'il en possède un et du symétrique d'un élément lorsqu'il en possède un.

Pour un magma $(M, *)$ et une partie N de M, $N \times N$ est une partie de $M \times M$. La restriction $*_{|N\times N}$ de $*$ à $N \times N$ est une application $*_{|N\times N} : N \times N \to N$. Il se peut cependant que :

Définition I.6.15 (Sous-magma) Que $*_{|N\times N}$ soit à valeurs dans N. On dit dans se cas que la loi $*$ se restreint en une loi interne (usuellement encore notée $*$) sur N.

On pourra alors dire que $(N, *)$ est un sous-magma de $(M, *)$

La définition ci-dessus ne présente pas un grand intérêt en soi, hormis celui de pouvoir énoncer confortablement la proposition I.6.16. Cette dernière n'étant d'ailleurs elle-même qu'un moyen commode de ne pas réécrire de nombreuses fois le même argument.

Proposition I.6.16 *Soit $(M, *)$ un magma.*

i) Le magma $(M, *)$ est toujours un sous-magma de lui-même. Si M possède un élément neutre ϵ, $(\{\epsilon\}, *)$ est un sous-magma de $(M, *)$.

ii) Soit $(N, *)$ un sous-magma de $(M, *)$. Si $(M, *)$ est associatif (resp. commutatif) $(N, *)$ l'est aussi.

Soit $f : (M, *) \to (N, \cdot)$ un morphisme de magmas.

iii) Pour tout sous-magma M' de M, $f(M')$ est un sous-magma de N.

iv) Pour tout sous-magma N' de N, $f^{-1}(N')$ est un sous-magma de M.

Définition I.6.17 Étant donné un magma associatif $(M, *)$, on dit qu'une relation d'équivalence $\sim$ sur l'ensemble M est *compatible à la loi* $*$ ou simplement compatible si

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

Lemme I.6.18 *Si $(M, *)$ est un magma associatif, et $\sim$ une relation d'équivalence compatible,*

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

***Preuve** : (cf. I.8.10.question 1).)*

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

***Preuve** : (cf. I.8.10.question 2).)*

Définition I.6.19 (Magma quotient) Avec les notations du lemme I.6.18, le magma $M/\sim$ est appelé *magma quotient* ou bien on dit que l'ensemble $M/\sim$ est muni de la *structure quotient*.

Proposition I.6.20 *Soient $(M,*)$ un magma, E un ensemble et M^E l'ensemble des applications de E dans M. Pour tout $(f,g) \in M^E \times M^E$, on définit $f *_{M^E} g \in M^E$ de la manière suivante : Pour tout $x \in E$,*

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

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

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

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

soit un morphisme.

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

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

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

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

est l'élément neutre de M^E.

Définition I.6.21 Étant donnés un magma $(M, *)$ et un ensemble E, on appellera *loi induite* par celle de M sur M^E, la loi $*_{M^E}$ construite à la proposition I.6.20. On la notera bien sûr simplement $*$ en général.

Exemple I.6.22 On est habitué depuis longtemps à écrire $f + g$ pour f et g des applications de $\mathbb{R}$ dans lui-même par exemple, ainsi que $f * g$ en utilisant les lois de compositions $+$ et $*$ dont on dispose sur l'ensemble $\mathbb{R}$ des nombres réels.

Proposition I.6.23 *Étant donnés deux magmas $(M, *)$ et $(N, \cdot)$,*

i) la loi $\dagger$ définie sur le produit cartésien $M \times N$ par

$$(x, y) \ \dagger \ (z, t) \ := \ (x * z, y \cdot t)$$

est l'unique loi telle que les projections

$$p \ : \ M \times N \ \to \ M \ , \ (x, y) \ \mapsto \ x \text{ et } q \ : \ M \times N \ \to \ N \ , \ (x, y) \ \mapsto \ y$$

(cf. I.2.15,)soient des morphismes ;

ii) Pour tout magma $(P, \sharp)$, et tout couple de morphismes

$$\big(f \ : \ (P, \sharp) \ \to \ (M, *) \ , \ g \ : \ (P, \sharp) \ \to \ (N, \cdot)\big)$$

il existe un unique morphisme

$$h \ : \ (P, \sharp) \ \to \ (M \times N, \dagger) \text{ tel que } p \circ h \ = \ f \text{ et } q \circ h \ = \ g \ .$$

Preuve *: Voir l'exercice I.8.18.*

Définition I.6.24 (Groupe) i) Un *groupe* est un magma associatif possédant un élément neutre et dans lequel tout élément possède un symétrique (appelé *inverse* ou *opposé* selon les cas.) Le groupe est de plus dit *abélien* ou *commutatif* si la loi de composition est commutative.

ii) Un *morphisme de groupes* ou de manière exactement synonyme un *homomorphisme de groupes* est une application qui préserve les lois de compositions ou encore un morphisme de magma.

iii) Un *isomorphisme de groupes* est un morphisme possédant une application réciproque, cette dernière étant elle-même un morphisme.

Ces notions seront développées en détail aux chapitres III et V.

Définition I.6.25 (Anneau) i) Un anneau est un ensemble A muni de deux lois de compositions $+$ et $*$ tels que $(A,+)$ soit un groupe abélien et $(A,*)$ un magma associatif possédant un élément neutre 1. Par ailleurs la loi $*$ est distributive sur $+$, à savoir que

$$\forall (x,y,z) \in A\times A\times A,\ x*(y+z) \ =\ x*y+x*z \text{ et } (x+y)*z \ =\ x*z+y*z\ .$$

ii) Un *morphisme d'anneaux* (*homomorphisme*) est un morphisme de groupe qui est simultanément un morphisme de magma pour la loi $*$. De plus on exige que l'image de l'élément neutre 1 pour la loi $*$ soit l'élément neutre pour la loi $*$.

iii) Un *isomorphisme d'anneaux* est un morphisme possédant une application réciproque, cette dernière étant elle-même un morphisme.
Ces notions seront développées en détail au chapitre VII.

I.7 . −Ce qu'il faut retenir

La plupart des développements de ce chapitre I constituent des considérations historiques ou de motivation.

Cependant il est indispensable de pouvoir utiliser correctement les symboles $\in$, $\subset$, $\cap$ et $\cup$ du langage ensembliste.

Il est également nécessaire d'être familier avec les définitions concernants les relations binaires et les fonctions I.2.1.iii) à I.2.13 ainsi qu'avec les dévelopements du paragraphe I.5.

Enfin le paragraphe I.6 servira de base aux chapitres III et VII.

I.8 . −Exercices

Exercice I.8.1 [Fonctions caractéristiques] Soit A une partie de E, on appelle fonction caractéristique de A l'application f de E dans l'ensemble à deux éléments $\{0,1\}$, telle que :

$$f(x)=\begin{cases}0 & \text{si } x\notin A\\ 1 & \text{si } x\in A\end{cases}$$

Soit A et B deux parties de E, f et g leurs fonctions caractéristiques. Montrer que les fonctions suivantes sont les fonctions caractéristiques d'ensembles que l'on déterminera :

$$1-f\ ,\ fg.\ ,\ \ ,\ f+g-fg\ .$$

Exercice I.8.2 [Injection] Étant donée une application $f\ :\ A\ \to\ B$, démontrer que les propositions suivantes sont équivalentes

i) f est injective.

ii) il existe une application g de B dans A telle que $g \circ f = \mathrm{Id}_A$.

On dit alors que g est une *rétraction* de f.

Une telle rétraction est elle unique ? Étudier le cas de $A = B = \mathbb{N},\ f(n) = 2n$.

Exercice I.8.3 [Surjection] Étant donnée une application $f : A \to B$, démontrer que les propositions suivantes sont équivalentes

i) f est surjective.

ii) il existe une application g de B dans A telle que $f \circ g = \mathrm{Id}_B$.

On dit alors que g est une *section* de f.

Une telle section est elle unique ? Démontrer que si deux sections ont même image elles coïncident.

Exercice I.8.4 [Propriétés des applications]

Soit $f : E \to F$ une application.

1) () **a)** () Montrer que

$$\forall A \in \mathcal{P}(F),\ f(f^{-1}(A)) \subset A\,.$$

b) () Montrer que f est surjective si et seulement si

$$\forall A \in \mathcal{P}(F),\ A = f(f^{-1}(A))\,.$$

2) () (**Injectivité (facultatif)**)

a) () Montrer que

$$\forall A \in \mathcal{P}(E),\ A \subset f^{-1}(f(A))\,.$$

b) () Montrer que f est injective si et seulement si

$$\forall A \in \mathcal{P}(E),\ A = f^{-1}(f(A))\,.$$

Exercice I.8.5 [] Faire la preuve de la proposition I.2.14.

Exercice I.8.6 [] Faire la preuve du lemme I.5.2.

Exercice I.8.7 [] Donner la preuve de la proposition I.5.4.

Exercice I.8.8 [] Faire la preuve de la proposition I.5.6.

Exercice I.8.9 []

Soit E un ensemble.

1) () **On suppose que E est muni d'une relation d'équivalence R. On note $\pi : E \to E/R$ la surjection canonique.**

Montrer que si F est un ensemble et $f : E \to F$ une application constante sur les classes de R c'est-à-dire que

$$\forall x \in E,\ \forall y \in E,\ \big((xRy) \Leftrightarrow (f(x) = f(y))\big)$$

Il existe une unique application $\overline{f} : E/R \to F$ vérifiant $f = \overline{f} \circ \pi$.

2) () **Soit $p : E \to E'$ une application surjective et $f : E \to F$ une application constante sur les fibres de p, c'est-à-dire que**

$$\forall x \in E,\ \forall y \in E,\ \big((p(x) = p(y)) \Leftrightarrow (f(x) = f(y))\big)\,.$$

Montrer qu'alors il existe une unique application $\overline{f} : E' \to F$ telle que $f = \overline{f} \circ p$.

Exercice I.8.10 []

On suppose que E est munie d'une relation d'équivalence R et d'une loi

$$\cdot : E \times E \to E\,.$$

On suppose que $\cdot$ et R sont *compatibles* c'est-à-dire que

$$\forall x, y, z, t \in E,\ \big(xRy \wedge zRt \Rightarrow x \cdot z\ R\ y \cdot t\big)\,.$$

On note $\pi : E \to E/R$ la surjection canonique.

1) () Montrer qu'il existe une unique loi $\dagger : F \times F \to F$ tel que π soit un morphisme c'est-à-dire que

$$\forall x, y \in E?\ \big(\pi(x \cdot y) = \pi(x) \dagger \pi(y)\big)\,.$$

On parle alors de *structure quotient*.

2) () Montrer que si $\cdot$ est associative, (resp. possède un élément neutre) (resp. est commutative) il en est de même de $\dagger$. Montrer que si $x \in E$ possède un symétrique y pour $\cdot$ alors $\pi(y)$ est le symétrique de $\pi(x)$ pour $\dagger$.

3) () Montrer que si E est muni d'une autre loi $\times$ également compatible à R, qui induit une loi $\sharp$ sur F et si $\times$ est distributive sur $\cdot$ alors $\sharp$ est distributive sur $\dagger$.

4) () Donner des exemples déjà connus des constructions précédentes.

Exercice I.8.11 [Produit cartésien et applications] Soient A, B, C trois ensembles. Étant donnée une application $f : A \times B \to C$, pour tout $x \in A$, on définit $g(x) \in C^B$ une application de B dans C par

$$g(x)(y) := f\big((x,y)\big) .$$

Montrer que l'application

$$\phi : C^{A\times B} \to (C^B)^A , \ f \mapsto g$$

est une bijection,
Indication : *on pourra donner sa bijection réciproque.*

Exercice I.8.12 [] Faire les détails de la preuve de la proposition I.6.13.

Exercice I.8.13 [] Étant doné un morphisme $f : M \to N$, (de magmas associatifs,) montrer que :

1) () si ϵ est l'élément neutre de M son image $f(\epsilon)$ n'est pas nécessairement l'élément neutre de N ;

2) () si y est le symétrique de x dans M, $f(y)$ n'est pas nécessairement le symétrique de $f(x)$ dans N.

Exercice I.8.14 [] Donner la preuve de la proposition I.6.20.

Exercice I.8.15 []

1) () Compléter la preuve de la proposition I.6.16.

2) () Si ϵ est un élément neutre de M est-il encore un élément neutre d'un sous-magma N ?
Si N possède un élément neutre η celui-ci est-il nécessairement celui de M ?
Si $x \in N$ possède un symétrique dans M celui-ci est-il aussi son symétrique dans N ?
Si $x \in N$ possède un symétrique dans N est-il aussi son symétrique dans M ?

Exercice I.8.16 [] Soit $(M, *)$ un magma associatif, d'élément neutre ϵ et N un sous-magma tel que $\epsilon \in N$. Montrer que :

1) () ϵ est l'élément neutre de N.

2) () si $x \in N$ a un inverse y dans N, c'est aussi son inverse dans M.

Exercice I.8.17 [] Faire la preuve du lemme I.6.18.

Exercice I.8.18 [] Faire la preuve de la proposition I.6.23.

II . −L'ensemble $\mathbb{N}$ des entiers naturels

II.0 . −Introduction

On choisit, dans ce cours, de définir l'ensemble $\mathbb{N}$ à partir des axiomes de Peano : Il existe un ensemble $\mathbb{N}$ contenant un élément noté 0 et muni d'une application $\mathfrak{s} : \mathbb{N} \to \mathbb{N}$ vérifiant :

PA$_1$) (**Succ**$_1$)

$$\forall p \in \mathbb{N},\ \big(p \neq 0 \Leftrightarrow \exists q \in \mathbb{N},\ (p = \mathfrak{s}(q))\big)\ .$$

PA$_2$) (**Succ**$_2$)

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \big(\mathfrak{s}(p) = \mathfrak{s}(q) \Rightarrow p = q\big)\ .$$

PA$_3$) (**Ind**)

$$\forall A \subset \mathbb{N},\ \big(0 \in A \wedge \forall p(p \in A \Rightarrow \mathfrak{s}(p) \in A) \Rightarrow A = \mathbb{N}\big)\ .$$

Remarque II.0.4 On constate qu'ici on ne suppose pas donné l'ensemble de ce qu'on avait appelé *système de Peano* en 0 mais seulement les axiomes 0.1.PA$_1$) à 0.1.PA$_3$).

On avait constaté que l'ensemble ω construit dans le système de Zermelo **Z** en I.3.7, satisfaisait ces trois axiomes. On avait mentionné aussi alors que la construction d'une addition $+$ et d'une multiplication $*$ demandaient des arguments supplémentaires qu'on s'était contenté d'esquisser. Une approche un peu différente sera développée dans les paragraphes II.1 et II.3.

Définition II.0.5 (Entiers naturels) On appellera *entiers naturels* les éléments de $\mathbb{N}$ et $\mathbb{N}$ l'*ensemble des entiers naturels*.

Nous allons, à partir des axiomes de Peano PA_1) à PA_3)
— Construire l'addition sur $\mathbb{N}$ (cf. II.1) et la multiplication sur $\mathbb{N}$ (cf. II.3 ;)
— établir les propriétés algébriques (d'ailleurs bien connues) de $\mathbb{N}$ c'est-à-dire les propriétés des opérations $+$ et $*$;
— définir une relation d'ordre $\leq$ sur $\mathbb{N}$ au paragraphe II.2 et montrer notamment le résultat clef que *toute partie non vide de* $\mathbb{N}$ *possède un plus petit élément* (cf. II.2.9 ;)
— introduire la notion d'ensemble fini en II.4 et donner quelques propriétés.

Définition II.0.6 (suite) Pour tout ensemble E, on appellera *suite à valeurs dans* E une application

$$u \ : \ \mathbb{N} \ \to \ E \, .$$

On notera, en général, $u \ := \ \big(u_n\big)_{,n\in\mathbb{N}}$ et pour tout entier naturel n, $u_n \ := \ u(n)$ l'image de l'entier naturel n par u qu'on appellera $n^{\text{ième}}$ terme de la suite u.

La notation $E^{\mathbb{N}}$ pour désigner l'ensemble des suites à valeurs dans E est un cas particulier de la notation introduite en I.2.5.

II.1 . −L'addition +

Proposition II.1.1 (Existence) *Il existe une application*

$$+ \ : \ \mathbb{N} \times \mathbb{N} \ \to \ \mathbb{N}$$

satisfaisant les axiomes :

*PA_4) (**Add**$_1$)*

$$\forall p \in \mathbb{N}, \ (0 + p \ = \ p) \, .$$

*PA_5) (**Add**$_2$)*

$$\forall p \in \mathbb{N}, \ \forall q \in \mathbb{N}, \ \big(\mathfrak{s}(p) \ + \ q \ = \ \mathfrak{s}(p+q)\big) \, .$$

***Preuve** : (cf. II.6.1.question 1).)*

Lemme II.1.2 *On a :*

$$\forall p \in \mathbb{N}, \ \forall q \in \mathbb{N}, \ \mathfrak{s}(p) + q \ = \ \mathfrak{s}(p+q) \ = \ p + \mathfrak{s}(q) \, .$$

***Preuve** : Voir l'exercice II.6.1.question 2).*

Remarque II.1.3 La formule ci-dessus n'a l'air de rien et semble tout à fait superflue dès l'instant où on aurait établi la commutativité de l'addition. Elle est cependant d'une grande utilité technique, précisément pour établir les propriétés algébriques de l'addition.

Notation II.1.4 On notera :

$$1 \ := \ \mathfrak{s}(0) \ . \qquad \text{II.1.4.1}$$

En prenant $q \ = \ 0$ dans l'axiome 0.1.PA$_5$) et en utilisant 0.1.PA$_4$), il vient alors :

$$\mathfrak{s}(p) \ = \ \mathfrak{s}(p+0) \ = \ p \ + \ \mathfrak{s}(0) \ = \ p \ + \ 1 \ . \qquad \text{II.1.4.2}$$

Plutôt que $\mathfrak{s}(p)$ on utilisera $p+1$ qui est plus habituel ; ce qui donne à l'axiome de récurrence II.0.PA$_3$) la forme plus familière : Si $A \subset \mathbb{N}$ contient 0 et contient $p+1$ pour tout $p \ \in \ A$, alors $A \ = \ \mathbb{N}$. Si P est une propriété portant sur des entiers, et si $A \ := \ \{p \in \mathbb{N} \ < \ P(p)\}$ (autrement dit A est l'ensemble des entiers vérifiant P,) alors o a :

$$(0 \in A \ \wedge \ (p \in A \Rightarrow p+1 \in A)) \ \Leftrightarrow \ (P(0) \ \wedge \ P(p) \ \Rightarrow \ P(p+1))$$

par aillleurs

$$A \ = \ \mathbb{N} \ \Leftrightarrow \ P(p) \forall p \in \mathbb{N} \ .$$

Si bien que l'axiome de récurrence peut se reformuler, lorsque A est défini par une propriété P en :

$$(P(0) \ \wedge \ (P(p) \Rightarrow P(p+1))) \ \Rightarrow \ (\forall p \in \mathbb{N}, \ (P(p))) \ .$$

Proposition II.1.5 (Propriétés algébriques de la loi $+$) *La loi $+$ sur $\mathbb{N}$ a les propriétés suivantes :*

*i) (**Associativité**)*
Elle est associative (cf. I.6.8 ;)

***Preuve** : (cf. II.6.1.question 3).)*

*ii) (**Élément neutre**)*
0 est un élément neutre (cf. I.6.10.i) ;)

***Preuve** : (cf. II.6.1.question 4).)*

*iii) (**Commutativité**)*
elle est commutative (cf. I.6.9.)

***Preuve** : (cf. II.6.1.question 5).)*

Définition II.1.6 On dit que les propriétés ci-dessus donnent à $(\mathbb{N}, +)$ une structure de *monoïde commutatif*.

Proposition II.1.7 (Régularité) *Tout élément de* $\mathbb{N}$ *est régulier c'est-à-dire que*

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ \big((p+r\ =\ q+r\ \Rightarrow\ p\ =\ q)\ \wedge\ (r+p\ =\ r+q\ \Rightarrow\ p\ =\ q)\big)\,.$$

Remarque II.1.8 Si on pouvait d'ores et déjà considérer $\mathbb{N}$ comme un sous-monoïde de $\mathbb{Z}$, la justification de la propriété ci-dessus serait immédiate. Cependant dans le point de vue axiomatique que nous avons adopté, la construction de $\mathbb{Z}$ vient après celle de $\mathbb{N}$. La propriété de régularité des éléments de $\mathbb{N}$ s'avère alors déterminante dans la construction de $\mathbb{Z}$ et est à la source de nombres des propriétés algébriques les plus importantes de $\mathbb{Z}$ (cf. IV.)

Proposition II.1.9 *On a :*

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ (p+q\ =\ 0\ \Rightarrow\ p\ =\ 0\ \wedge\ q\ =\ 0)\,.$$

Preuve *: La démonstration de cette proposition se fait par contraposée : Si en effet,* p *ou* q *est différent de* 0*, supposons, par exemple que ce soit* p*, alors* p *est le successeur d'un élément* r *c'est-à-dire qu'il existe un entier naturel* r *tel que* $p = \mathfrak{s}(r)$ *(cf. II.0.PA*$_1$*).) Il en résulte que* $\mathfrak{s}(r)\ +\ q\ =\ 0$ *c'est-à-dire, d'après II.1.1.PA*$_5$*), que* $\mathfrak{s}(r+q)\ =\ 0$ *ce qui contredit l'axiome II.0.PA*$_1$*).*

II.2 . −La relation d'ordre $\leq$

On définit maintnant une relation d'ordre sur $\mathbb{N}$ (cf. I.2.2.vi),) dont on va montrer qu'elle satisfait de « bonnes propriétés » relativement à l'addition $+$ et la multiplication $*$.

Définition II.2.1 ($\leq$) On définit la relation $\leq$ sur $\mathbb{N}$, par la formule :

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \big(p\ \leq\ q\ \Leftrightarrow\ \exists r \in \mathbb{N},\ (q\ =\ p+r)\big)\,. \qquad \text{II.2.1.1}$$

Pour tout couple (p, q) d'entiers, si $p \leq q$, on dira que p est *inférieur ou égal à* q.

Proposition II.2.2 ($\leq$) *La relation* $\leq$ *définie ci-dessus est une relation d'ordre sur* $\mathbb{N}$ *(cf. I.2.2.vi).)*

Preuve *:*

i) ***(Réflexivité)***
Comme, $\forall p \in \mathbb{N},\ p+0\ =\ p$ *(cf. II.1.5.ii),)* $p \leq p$ *i.e.*$\leq$ *est réflexive.*

*ii) (**Antisymétrie**)*

Pour deux entiers naturels p et q, si $p \leq q$ et $q \leq p$, il existe des entiers naturels u et v tels que

$$p + u \;=\; q \,\text{et}\, q + v \;=\; p\,.$$

Il en résulte que $p + u + v \;=\; q + v \;=\; p$ c'est-à-dire, comme p est régulier (cf. II.1.7,) que $u + v = 0$. Il découle alors du point II.1.9 que $u \;=\; v \;=\; 0$ d'où il résulte finalement que $p = q$. La relation $\leq$ est donc antisymétrique.

*iii) (**Transitivité**)*

Enfin pour tout triplet (p, q, r) d'entiers naturels, si $p \leq q$ et $q \leq r$, il existe des entiers naturels u et v tels que $q = p + u$ et $r = q + v$. Il en résulte que $r \;=\; p + u + v$ et, par conséquent, la relation $\leq$ est transitive.

Il résulte des trois points ci-dessus que $\leq$ est une relation d'ordre.

Définition II.2.3 On peut définir de manière exactement analogue une relation $\geq$ (*supérieur ou égal*) par $p \geq q$ s'il existe r tel que $p = q + r$ ce qui est exactement équivalent à $q \leq p$.

On peut aussi définir une relation $<$ *strictement inférieur à* (resp. $>$ *strictement supérieur à*,) par $p < q$ (resp. $p > q$) si $p \leq q$ (resp. $p \geq q$) et $p \neq q$. Les relations $<$ et $>$ ne sont pas des relations d'ordre, puisqu'elles ne sont pas antisymétriques.

Notation II.2.4 On notera $\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ :$

$$\begin{array}{rcl} [p;q] & := & \{r \in \mathbb{N}\,;\, p \leq r \leq q\} \\ [p;q[& := & \{r \in \mathbb{N}\,;\, p \leq r < q\} \\ ]p;q] & := & \{r \in \mathbb{N}\,;\, p < r \leq q\} \\ ]p;q[& := & \{r \in \mathbb{N}\,;\, p < r < q\} \\ [p;+\infty[& := & \{r \in \mathbb{N}\,;\, p \leq r\} \\ ]p;+\infty[& := & \{r \in \mathbb{N}\,;\, p < r\}\,. \end{array} \qquad \text{II.2.4.1}$$

Proposition II.2.5 (Ordre total) *La relation $\leq$ est une relation d'ordre totale sur $\mathbb{N}$ (cf. I.2.2.vi).)*

***Preuve** : Ceci équivaut encore au fait que, pour tout couple d'entiers naturels (p, q) il existe $r \in \mathbb{N}$ tel que, soit $q = p + r$, soit $p = q + r$. Cet énoncé équivaut encore, avec les notations II.2.4, à :*

$$\forall p \in \mathbb{N},\ \big(\mathbb{N} \;=\; [0;p] \;\cup\; [p;+\infty[\big)\,. \qquad \textit{II.2.5.1}$$

On va démontrer que pour tout $p \in \mathbb{N}$, l'ensemble $[0;p] \cup [p;+\infty[$ satisfait l'axiome de récurrence II.0.PA$_3$) et est donc égal à $\mathbb{N}$ ce qui établit II.2.5.1 :

ii) Tout d'abord

$$0 \in [0;p] \;\subset\; [0;P] \;\cup\; [p;+\infty[\,.$$

iii) Si $q \in [0;p] \cup [p;+\infty[$, *deux cas sont possibles :*

a) Soit $q \in [p;+\infty[$ *c'est-à-dire qu'il existe* $r \in \mathbb{N}$ *tel que* $q = p + r$ *ce qui entraîne que* $q + 1 = p + r + 1$ *et donc que* $q + 1 \in [p;+\infty[$.

b) Soit $q \in [0;p]$ *c'est-à-dire qu'il existe* $r \in \mathbb{N}$ *tel que* $p = q + r$. *Si* $r = 0$ $p = q$ *donc* $q + 1 = p + 1 \in [p;+\infty[$. *Si* $r \neq 0$, *il existe (cf. II.0.PA*$_1$*),)* $t \in \mathbb{N}$ *tel que* $r = t + 1$ *d'où il découle que* $p = q + t + 1 = q + 1 + t$ *c'est-à-dire que* $q + 1 \in [0;p]$.

iv) Dans tous les cas, on a démontré que $[0;p] \cup [p;+\infty[$ *satisfait au principe de récurrence et donc*

$$[0;p] \cup [p;+\infty[= \mathbb{N}\,.$$

Proposition II.2.6 (Addition)

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ \big(p \leq q \Leftrightarrow p + r \leq q + r \Leftrightarrow \mathfrak{s}(p) \leq \mathfrak{s}(q)\big)\,.$$

Preuve *:* *Si* $p \leq q$, *il existe* $u \in \mathbb{N}$ *tel que* $q = p + u$. *Il s'ensuit que pour tout* r, $q + r = p + u + r$. *Il s'ensuit également que* $\mathfrak{s}(q) = \mathfrak{s}(p + u) = \mathfrak{s}(p) + u$.

Réciproquement si $p + r \leq q + r$, *il existe* $u \in \mathbb{N}$ *tel que* $q + r = p + r + u$ *ce qui entraîne, puisque* r *est régulier (cf. II.1.7,)* $q = p + u$. *si* $\mathfrak{s}(p) \leq \mathfrak{s}(q)$, *on pourrait, grâce à ce qu'on a établi auparavant, conclure en prenant* $r = 1$, *dans ce qui précède. On peut aussi écrire qu'il existe* $u \in \mathbb{N}$, *tel que* $\mathfrak{s}(q) = \mathfrak{s}(p) + u = \mathfrak{s}(p + u)$. *Puisque* $\mathfrak{s}$ *est injective, il en résulte que* $q = p + u$.

Corollaire II.2.7 *L'application* $\mathfrak{s} : \mathbb{N} \to \mathbb{N}$ *est strictement croissante.*

Remarque II.2.8 Pour tout $p \in \mathbb{N}$, $p = 0 + p$ (cf. II.1.5.ii),) c'est-à-dire que $0 \leq p$. 0 est donc un plus petit élément pour $\mathbb{N}$ lui-même.

Proposition II.2.9 (Plus petit élément) *Toute partie non vide de* $\mathbb{N}$ *possède un plus petit élément*
(cf. I.2.2.vii).)

Preuve *:*

i) On déduit de la remarque II.2.8, que toute partie P *de* $\mathbb{N}$ *contenant* 0 *possède* 0 *comme plus petit élément c'est-à-dire que l'ensemble* A *des entiers* p *tels que toute partie de* $\mathbb{N}$ *contenant* p *possède un plus petit élément, contient* 0.

ii) Supposons que $p \in A$, c'est-à-dire que toute partie contenant p possède un plus petit élément. Soit P une partie de $\mathbb{N}$ contenant $\mathfrak{s}(p)$.

si $0 \in P$ d'après ce qui précède, 0 est le plus petit élément de P P contient donc un plus petit élément.

si $0 \notin p$ Notons $Q := \mathfrak{s}^{-1}(P)$. Puisque $0 \notin P$, il découle de l'axiome II.0.PA$_1$) que la restriction de $\mathfrak{s}_{|Q}$ est surjective. Comme d'après l'axiome II.0.PA$_2$), $\mathfrak{s}$ est injective, sa restriction $\mathfrak{s}_{|Q}$ reste injective.

Intuitivement ce qui précède signifie simplement que, comme P ne contient pas 0, pour tout $q \in P$, $q-1$ (pour peu qu'on puisse donner un sens à cette écriture,) reste un entier.

Puisque $\mathfrak{s}(p) \in P$, $p \in Q$. Par hypothèse de récurrence, Q possède donc un plus petit élément q. Il s'ensuit que $\forall r \in Q,\ q \leq r$. Il s'ensuit que $\forall r \in Q,\ \mathfrak{s}(r) \leq \mathfrak{s}(q)$ d'après la proposition II.2.6. Il s'ensuit que $\forall r \in \mathfrak{s}(Q),\ \mathfrak{s}(q) \leq r$, ce qui signifie exactement, puisque $\mathfrak{s} : Q \to P$ est une bijection que $\forall r \in P,\ \mathfrak{s}(q) \leq r$. Or $q \in Q$ donc $\mathfrak{s}(q) \in P$ si bien que $\mathfrak{s}(q)$ est le plus petit élément de P.

Remarque ii).1 On aurait pu établir, au rang des propriétés des applications croissantes, que si f est une application croissante, que a possède un plus petit élément x alors $f(x)$ est le plus petit élément de $f(a)$. On aurait ensuite appliqué ce résultat à $\mathfrak{s} : Q \to P$ grâce au corollaire II.2.7.

iii) On vient donc de montrer que l'ensemble A satisfait au principe de récurrence autrement dit que $A = \mathbb{N}$ ce qui achève la preuve de l'existence d'un plus petit élément.

Proposition II.2.10 (Plus grand élément) *Une partie non vide P de $\mathbb{N}$ est majorée (cf. I.2.2.vii),) si et seulement si elle possède un plus grand élément. Celui-ci est alors le plus petit de ses majorants.*

Preuve *: Si P possède un plus grand éléments, celui-ci est un majorant par définition. Et P est évidemment non vide.*

Réciproquement si P est majorée l'ensemble M de ses majorants est non vide. Il résulte de II.2.9 que M possède un plus petit élément m. Comme $\forall p \in P,\ ,\ p \leq m$,

$$m \notin P \Rightarrow \forall p \in P,\ ,\ p \leq m \wedge p \neq m$$

c'est-à-dire

$$\forall p \in P,\ ,\ p < m\,. \qquad \text{II.2.10.1}$$

Il s'ensuit alors que

$$m = 0 \Rightarrow P = \emptyset\,.$$

Donc

$$p \neq \emptyset \Rightarrow m \neq 0 .$$

Il existe donc (cf. II.0.PA$_1$),) $n \in \mathbb{N}$ *tel que* $m = n + 1$. *II.2.10.1 entrraîne alors que*

$$\forall p \in P,\ p < n+1 \Rightarrow \forall p \in P,\ p \leq n \Rightarrow n \in M .$$

Mais $n < m$ m *étant le plus petit élément de* M.

On en déduit donc que $m \in P$ *c'est-à-dire que* m *est le plus grand élément de* P.

II.3 . −La multiplication

Les propriétés algébriques de la multiplication (associativité élément neutre, distributivité sur l'addition et commutativité) sont énoncées dans la proposition II.3.3 dans l'ordre où on les énonce en général dans le cadre des structures algébriques. Il s'agira d'en déduire des propriétés similaires pour l'anneaux $\mathbb{Z}$ étudié au paragraphe IV.3.

La preuve de ces propriétés est cependant donnée dans un ordre différent dans le lemme II.3.2 (comme d'ans le TD n° II, exercice A. Cet ordre correspond à celui dans lequel on peut raisonablement déduire ces propriétés les unes des autres. On constate en particulier que l'associativité (cf. II.3.2.iv),) qui ne concerne pourtant que la seule loi $*$, est établie postérieurement à la distributivité à droite qui pourtant met en jeu les deux lois $+$ et $*$. Il faut juste remarquer que l'axiome II.3.1.PA$_7$) comporte un signe $+$ dans son énoncé. Autrement dit, comme on s'y attendrait et comme on le sait d'ailleurs naïvement depuis fort longtemps, la multiplication des entiers est définie par une itération de sommes. Le but de ce qui suit n'a pour seul but que de rendre formelle (mais pas trop espérons-le) et rigoureuse cette intuition.

Proposition II.3.1 (Existence) *Il existe une application*

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

satisfaisant les axiomes :

*PA$_6$) (**Mult**$_1$)*

$$\forall p \in \mathbb{N},\ (0 * p = 0) .$$

*PA$_7$) (**Mult**$_2$)*

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \big(\mathfrak{s}(p) * q = (p * q) + q\big) .$$

Preuve : *Montrons d'abord le lemme suivant :*

Lemme II.3.1.1 *Il existe un unique élément*

$$\pi \in (\mathbb{N}^{\mathbb{N}})^{\mathbb{N}}$$

tel que :

i) $\pi(0) := 0$ *i.e.*

$$\forall n \in \mathbb{N},\ \pi(0)(n) = 0\ ;$$

ii)

$$\forall n \in \mathbb{N},\ \pi(\mathfrak{s}(n)) = \pi(n) + \mathrm{Id}_{\mathbb{N}}\ ,\ \textit{i.e.}\ \forall n \in \mathbb{N},\ \forall p \in \mathbb{N},\ \pi(\mathfrak{s}(n))(p) = \pi(n)(p) + p\ .$$

Preuve : *Montrons que π est bien définie c'est-à-dire que le domaine de définition D de π est égal à $\mathbb{N}$. La condition i) assure que $\pi(0)$ est bien un élément de $\mathbb{N}^{\mathbb{N}}$ i.e.une application de $\mathbb{N}$ dans lui-même. On en conclut que $0 \in D$.*

Si $n \in \mathbb{N}$ appartient à D, cela signifie que $\pi(n)$ est une application bien définie de $\mathbb{N}$ deans lui même. Alors $\pi(n) + \mathrm{Id}_{\mathbb{N}}$ est encore une application de $\mathbb{N}$ dans lui-même et l'on peut donc définir $\pi(\mathfrak{s}(n))$ par $\pi(n) + \mathrm{Id}_{\mathbb{N}}$ entraînant que $\mathfrak{s}(n) \in D$.

L'ensemble D satisfait donc au principe de récurrence II.0.PA$_3$) si bien que $D = \mathbb{N}$.

On a bien constaté dans ce qui précède que la condition ii) impose que π se prolonge de manière unique, ce qui assure l'unicité de π.

Posons alors désormais

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ p * q := \pi(p)(q)$$

et l'on constate que la condition II.3.1.1.i) (resp. II.3.1.1.ii)) entraîne précisément que l'axiome PA$_6$) (resp. PA$_7$)) est satisfait.

Lemme II.3.2

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},$$

i) ***(Élément neutre)***
$1 * p = p * 1 = p\ ;$

ii) ***(Élément absorbant)***
$0 * p = p * 0 = 0\ ;$

iii) ***(Distributivité à droite)***
$(p+q) * r = p*r + q*r$;

iv) ***(Associativité)***
$p * (q*r) = (p*q) * r$;

v) ***(Distributivité partielle à gauche)***
$p * (q+1) = p*q + p$;

vi) ***(Commutativité)***
$p * q = q * p$;

vii) ***(Distributivité à gauche)***
$p * (q+r) = p*q + p*r$.

Preuve *:*

i) ***(Élément neutre)***
Le fait que

$$\forall p \in \mathbb{N},\ 1 * p = p, \qquad 1$$

est une conséquence de II.3.1.PA$_6$), II.3.1.PA$_7$), II.1.1.PA$_4$) et II.1.1.PA$_5$) sans qu'il soit nécessaire de recourir à un raisonement par récurrence.

Considérons désormais $A := \{p \in \mathbb{N} ;\ p*1 = p\}$. *Il résulte de l'axiome II.3.1.PA$_6$) que* $0*1 = 0$ *i.e.*$0 \in A$.

Par ailleurs d'après II.3.1.PA$_7$),

$$\forall p \in \mathbb{N},\ (p+1)*1 = p*1 + 1*1 .$$

Si on suppose que $p \in A$, *il vient*

$$(p+1)*1 = p*1 + 1*1 = p + 1*1$$

et en appliquant 1, il vient finalement $(p+1)*1 = p+1$ *i.e.*$p+1 \in A$ *si bien que* $A = \mathbb{N}$.

ii) ***(Élément absorbant)***
Il découle immédiatement de II.3.1.PA$_6$) que

$$0 \in A := \{p \in \mathbb{N} ;\ p*0 = 0\} .$$

De plus $\forall p \in \mathbb{N},\ (p+1)*0 = p*0 + 0$ *en vertu de II.3.1.PA$_7$). Si en supposant que* $p \in A$, *il vient, en vertu également de II.1.1.PA$_4$),*

$$(p+1)*0 = p*0 + 0 = 0 + 0 = 0$$

c'est-à-dire que $p+1 \in A$ *et donc finalement que* $A = \mathbb{N}$.

*iii) (**Distributivité à droite**)*
D'après l'axiome II.3.1.PA$_6$), $\forall r \in \mathbb{N},\ 0 * r \ = \ 0$ ce qui, combiné à II.1.5.ii), entraîne que

$$\forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ 0 * r + q * r \ = \ (0 + q) * r$$

c'est à dire que

$$0 \in A \ := \ \{p \ \in \ \mathbb{N}\ ;\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ (p + q) * r \ = \ p * r \ + q * r\}\ .$$

De plus,

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ (p + 1 + q) * r \ = \ ((p + q) + 1) * r \ = \ (p + q) * r + r$$

la dernière égalité résultant de l'axiome II.3.1.PA$_7$) et l'avant dernière de II.1.1.PA$_5$).
Si on suppose $p \in A$, on a

$$(p+1+q)*r \ = \ (p+q)*r+r \ = \ p*r+q*r+r \ = \ p*r+r+q*r \ = \ (p+1)*r+q*r$$

en utilisant II.3.1.PA$_7$) et II.1.5.iii). Il s'ensuit que $p + 1 \in A$ et donc que $A \ = \ \mathbb{N}$.

*iv) (**Associativité**)*
L'axiome II.3.1.PA$_6$) entraîne que

$$\forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ 0 * (q * r) \ = \ 0\, 0 * r \ = \ (0 * q) * r$$

si bien que

$$0 \ \in \ A \ := \ \{p \ \in \ \mathbb{N}\ ;\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ p * (q * r) \ = \ (p * q) * r\}\ .$$

En outre

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ (p + 1) * (q * r) \ = \ p * (q * r) + q * r$$

en appliquant l'axiome II.3.1.PA$_7$). Il en résulte, si $p \in A$, que

$$(p+1)*(q*r) \ = \ p*(q*r)+q*r \ = \ (p*q)*r+q*r \ = \ (p*q+q)*r \ = \ ((p+1)*q)*r$$

l'avant dernière égalité résultant de iii) et la dernière de l'axiome II.3.1.PA$_7$). On an déduit finalement que $p + 1 \in A$ et donc que $A \ = \ \mathbb{N}$.

v) ***(Distributivité partielle à gauche)***
On a bien entendu, $\forall q \in \mathbb{N},\ 0*(q+1) \ = \ 0 \ = \ 0*q \ + \ 0*1$ *en utilisant ii), si bien que*

$$0 \ \in \ A \ := \ \{p \ \in \ \mathbb{N} \, ; \ \forall q \in \mathbb{N},\ p*(q+1) \ = \ p*q+p\} \, .$$

En outre

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ (p+1)*(q+1) \ = \ p*(q+1) \ + \ q \ + \ 1$$

en vertu de II.3.1.PA$_7$*). Si* $p \in A$*, on a*

$$(p+1)*(q+1) \ = \ p*(q+1)+q+1 \ = \ p*q+p+q+1 \, .$$

Comme l'addition $+$ *est commutative (cf. II.1.5.iii),) il vient*

$$(p+1)*(q+1) \ = \ p*q+p+q+1 \ = \ p*q+q+p+1 \ = \ (p+1)*q \ + \ (p+1)$$

en utilisant II.3.1.PA$_7$*). Ce qui précède assure que* $p+1 \in A$ *et donc que* $A \ = \ \mathbb{N}$.

vi) ***(Commutativité)***
Il résulte de ii) que

$$0 \ \in \ A \ := \ \{p \ \in \ \mathbb{N} \, ; \ \forall q \in \mathbb{N},\ p*q \ = \ q*p\} \, .$$

Par ailleurs

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ (p+1)*q \ = \ p*q \ + \ q$$

en vertu de II.3.1.PA$_7$*). Si on suppose de plus que* $p \in A$*, on a :*

$$(p+1)*q \ = \ p*q+q \ = \ q*p+q \ = \ q*(p+1)$$

en utilisant v). Il en résulte que $p+1 \in A$ *i.e.*$A \ = \ \mathbb{N}$.

vii) ***(Distributivité à gauche)***
C'est une conséquence immédiate de iii) et vi).

Proposition II.3.3 (Propriétés de la loi $*$) *La loi $*$ sur $\mathbb{N}$ possède les propriétés suivantes : Elle est associative (cf. II.3.2.iv),) possède un élément neutre 1 (cf. II.3.2.i),) est distributive à gauche et à droite sur l'addition (cf. II.3.2.vii) et II.3.2.iii),) est commutative (cf. II.3.2.vi),) 0 est un élément absorbant (cf. II.3.2.ii).)*

Proposition II.3.4 (Intégrité)

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \big(p * q \ = \ 0 \Leftrightarrow \ p \ = \ 0 \ \vee \ q \ = \ 0\big)\ .$$

Preuve *: Bien sûr si $p \ = \ 0 \ \vee \ q \ = \ 0, p * q \ = \ 0$ en vertu de II.3.2.ii).*

Réciproquement si $p \ \neq \ 0$ et $q \ \neq \ 0$, il existe u et v tels que $p = u + 1$ et $q = v + 1$ en vertu de l'axiome II.0.PA$_1$). On a alors en utilisant la proposition II.3.3 :

$$p * q \ = \ (u + 1) * (v + 1) \ = \ u * v + u + v + 1 \ = \ \mathfrak{s}(u * v + u + v) \ \neq \ 0$$

en appliquant l'axiome II.0.PA$_1$).

Proposition II.3.5

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ \big((p \ \neq \ 0 \wedge p * q \ = \ p * r) \ \Leftrightarrow \ (q \ = \ r)\big)\ .$$

Preuve *: Notons*

$$A \ := \ \{q \ \in \ \mathbb{N}\ ;\ \forall p \in \mathbb{N},\ \forall r \in \mathbb{N},\ \big((p \ \neq \ 0 \wedge p * q \ = \ p * r) \ \Leftrightarrow \ (q \ = \ r)\big)\}\ .$$

Si $q \ = \ 0$,

$$\forall p \in \mathbb{N},\ \forall r \in \mathbb{N},\ \big((p \neq 0 \ \wedge \ p * q \ = \ p * r) \ \Leftrightarrow \ (p * r \ = \ 0)\big)$$

ce qui entraîne que $r \ = \ 0$, en vertu de la proposition II.3.4. On vient donc de constater que $0 \in A$.

Pour tout $(p, q, r,) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$,

$$\big((p * \mathfrak{s}(q) \ = \ p * r) \ \Leftrightarrow \ (p * q + p \ = \ p * r)\big)\ .$$

Or

$$p \ \neq \ 0 \ \Rightarrow \ p * q + p \ \neq \ 0 \ \Rightarrow \ p * r \ \neq \ 0 \ \Rightarrow \ r \ \neq \ 0\ .$$

Il s'ensuit qu'il existe $u \ \in \ \mathbb{N}$ tel que $r \ = \ \mathfrak{s}(u)$. On a donc

$$p * \mathfrak{s}(q) \ = \ p * r \ \Leftrightarrow \ p * q + p \ = \ p * \mathfrak{s}(u) \ \Leftrightarrow \ p * q + p \ = \ p * u + p \ \Leftrightarrow \ p * q \ = \ p * u$$

la dernière égalité résultant de la proposition II.1.7. si $q \in A$,

$$pq \ = \ p * u \ \Rightarrow \ q \ = \ u \ \Rightarrow \ \mathfrak{s}(q) \ = \ \mathfrak{s}(u) \ = \ r$$

ce qui prouve que $\mathfrak{s}(q) \in A$ et assure que A satisfait au principe de récurrence II.0.PA$_3$). On a donc $A \ = \ \mathbb{N}$ ce qui achève la preuve.

Proposition II.3.6

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ \big(q \leq r\ \Rightarrow\ p * q \leq p * r\big)$$

la réciproque étant vraie si $p \neq 0$.

Preuve *:*

i) ***(Sens direct)***
Pour tout $q, r \in \mathbb{N}$,

$$\big(q \leq r\ \Rightarrow\ \exists u \in \mathbb{N},\ (r\ =\ q + u)\big)\ .$$

Ceci entraîne

$$\forall p \in \mathbb{N},\ p * r\ =\ p * q\ +\ p * u$$

ce qui entraîne

$$p * q\ \leq\ p * r\ .$$

ii) ***(Réciproque)***
Il découle du sens direct et de la proposition II.3.5, que

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ \big((p\ \neq\ 0\ \wedge\ q\ <\ r)\ \Leftrightarrow\ (p * q\ <\ p * r)\big)\ .$$

En utilisant que la négation de $q \leq r$ *est* $r < q$*, on établit le résultat par contraposée.*

Proposition II.3.7 *Pour tout couple d'entiers naturels* (p, q), $p * q\ =\ 1$ *si et seulement si* $p = q = 1$.

Preuve *: Pour tout* $p, q \in \mathbb{N}$, $p * q\ =\ 1$, *entraîne par II.3.4*

$$p\ \neq 0\ \wedge\ q\ \neq\ 0\ .$$

Il s'ensuit en particulier que $1 \leq q$*, ce qui entraîne, en vertu de II.3.6*

$$p\ \leq\ p * q\ =\ 1$$

c'est-à-dire $p\ \leq\ 1$. *Un raisonnement symétrique sur* q *donne*

$$1\ \leq\ p\ \wedge\ q\ \leq\ 1$$

d'où il résulte finalement

$$p\ =\ q\ =\ 1\ .$$

Remarque II.3.8 Pour tout couple d'entiers naturels (p, q) on définit p^q par : $p^0 = 1$ et $p^{q+1} = p^q * p$.

On remarque, q'avec cette définition :

$0^0 = 1$ ce qui correspond à $\#(\emptyset^\emptyset)$,

$0^p = 0$ pour $p \neq 0$, ce qui correspond au fait qu'il n'existe aucune application d'un ensemble non vide dans l'ensemble vide,

$p^0 = 1$ pour tout p correspondant à l'unique application de $\emptyset$ dans un ensemble quelconque.

La définition de p^q donnez ici est donc en accord avec la notation A^B
(cf. I.2.5, II.4.11.iv).)

II.4 . −Ensembles finis

Définition II.4.1 (Ensemble fini) On dira qu'un ensemble A est *fini* s'il existe $p \in \mathbb{N}$ et une application injective $i : A \to [1; p]$.

Proposition II.4.2 (Conséquences de la définition II.4.1) *i) Si A est un ensemble fini, et*

$$B \to A$$

une application injective, B est un ensemble fini.

ii) Si A est un ensemble fini, pour toute partie $B \in \mathcal{P}(A)$, B est un ensemble fini.

iii) Si $A \in \mathcal{P}(E)$ et $B \in \mathcal{P}(E)$, sont des ensembles finis, il en est de même de $A \cap B$ et $A \cup B$.

iv) Si A et B sont des ensembles finis, il en est de même de $A \times B$ (cf. I.2.1.ii),) et A^B (cf. I.2.5.)

***Preuve** : (cf. II.6.2.)*

Exemple II.4.3 Par définition pour tout $p \in \mathbb{N}$, $[1; p]$ est fini puisque $\mathrm{Id}_{[1;p]}$ fournit évidemment une application injective $[1; p] \hookrightarrow [1; p]$.

En particulier $\emptyset = [1; 0]$ est un ensemble fini.

Lemme II.4.4 *Pour tout $(p, q) \in \mathbb{N} \times \mathbb{N}$, les assertions suivantes sont équivalentes :*

a) Il existe une application injective $i : [1; p] \to [1; q]$.

b)

$$p \leq q\,.$$

Preuve *:*

i) ***(a)*** $\Rightarrow$ ***b))***

On a $[1;0] = \emptyset$ *or pour tout* $q \in \mathbb{N}$*, l'unique application* $\emptyset \to [1;q]$ *est injective. L'assertion* $\mathcal{H}_p$ *: Pour tout* $q \in \mathbb{N}$*, s'il existe une injection* $[1;p] \hookrightarrow [1;q]$ *alors* $p \leq q$ *est vraie pour* $p = 0$*.*

Pour tout $p \in \mathbb{N}$*,* $\mathfrak{s}(p) \neq 0$ *donc* $1 \in [1;\mathfrak{s}(p)] \neq \emptyset$*. s'il existe donc une application injective* $i : [1;\mathfrak{s}(p)] \to [1;q]$*,* $[1;q] \neq \emptyset \Rightarrow q \neq 0$*. Il existe donc, en vertu de l'axiome II.0.PA*$_1$*) un entier* $r \in \mathbb{N}$ *tel que* $q = \mathfrak{s}(r)$*. Notons* $x := i(\mathfrak{s}(p)) \in [1;q]$ *et* $t : [1;q] \to [1;q]$ *définie par*

$$t(x) := q\,,\ t(q) := x\,,\ t(y) := y \forall y \in [1;q],\ y \neq x, y \neq q\,.$$

L'application t *ainsi définie est bien entendu une bijection de* $[1;q]$ *sur lui-même et l'application* $t \circ i$ *est donc encore une application injective ainsi que sa restriction* $j := t \circ i_{|[1;p]}$ *à l'intervalle* $[1;p]$*. Or* j *est à valeurs dans* $[1;r]$*. On a donc une application injective* $j : [1;p] \hookrightarrow [1;r]$*. Si on suppose donc* $\mathcal{H}_p$ *vérifiée, il s'ensuit que* $p \leq r$*. Il en résulte, en vertu de la proposition II.2.6 que*

$$\mathfrak{s}(p) \leq \mathfrak{s}(r) \Leftrightarrow \mathfrak{s}(p) \leq q$$

c'est-à-dire que $\mathcal{H}_{\mathfrak{s}(p)}$ *est satisfaite si bien qu'on a démontré le résultat par récurrence sur* p*.*

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

si $p \leq q$*,*

$$\forall r \in [1;p],\ 1 \leq r \leq p \Rightarrow r \in [1;q]$$

donc $[1;p] \subset [1;q]$ *l'inclusion naturelle fournit donc*

$$\text{une application injective } [1;p] \hookrightarrow [1;q]\,.$$

Corollaire II.4.5 *L'ensemble* $\mathbb{N}$ *des entiers naturels lui-même n'est pas un ensemble fini.*

Preuve *: En effet, pour tout entier* p *et toute application* $i : \mathbb{N} \to [1;p]$*, on peut considérer sa restriction*

$$i_{|[1;p+1]} : [1;p+1] \to [1;p]\,.$$

Si i *est injective,* $i_{|[1;p+1]}$ *l'est encore, ce qui, en vertu du lemme II.4.4 entraîne* $p+1 \leq p$*.*

Définition II.4.6 (Ensemble dénombrable) On dit qu'un ensemble A est *dénombrable* s'il existe une bijection $A \cong \mathbb{N}$.

Exemple II.4.7 (Ensembles dénombrables) Les ensembles

$$\mathbb{N},\ \mathbb{Z},\ \mathbb{Q}$$

sont dénombrables mais $\mathcal{P}(\mathbb{N})$ ne l'est pas non plus que $\mathbb{R}$.

Proposition II.4.8 *Pour tout ensemble fini A, le plus petit entier p tel qu'il existe une application injective $i : A \to [1;p]$ est l'unique entier p tel qu'il existe une bijection $A \cong [1;p]$.*

***Preuve** :*

*i) (**Existence de l'entier** p)*

Tout d'abord par définition (cf. II.4.1,) l'ensemble $I \subset \mathbb{N}$ des entier q tel qu'il existe une application injective $A \hookrightarrow [1;q]$ est non vide. D'après la proposition II.2.9, I possède donc un plus petit élément noté p.

Si $p = 0$, $A = \emptyset$ et l'unique application $\emptyset \to \emptyset$ est bijective.

Si $p \neq 0$, il existe, par définition une application injective $i : A \hookrightarrow [1;p]$. si i n'est pas surjective, il existe $x \in [1;p]$ qi n'a pas d'antécédent. Notons alors $t : [1;p] \to [1;p]$ définie par

$$t(x) := p\ ,\ t(p) := x\ ,\ t(y) := y\ \forall y \in [1;p],\ y \neq x, y \neq p\ .$$

Comme $p \neq 0$, il existe, d'après l'axiome II.0.PA$_1$), un entier $r \in \mathbb{N}$ tel que $p = \mathfrak{s}(r)$. Puisque t est bijective, $t \circ i$ reste injective et à valeurs dans $[1;r]$. Comme $r < p$, ceci contredit le fait que p soit le plus petit élément de I. L'application i est donc surjective et donc bijective puisque injective par hypothèse.

On a ainsi démontrer l'existence d'un entier p et d'une bijection $A \cong [1;p]$.

*ii) (**Unicité de l'entier** p)*

S'il existe une bijection $\beta : A \cong [1;p]$ et une bijection $\gamma : A \cong [1;q]$

$$\beta \circ \gamma^{-1} : [1;q] \to [1;p] \text{ et } \gamma \circ \beta^{-1} : [1;p] \to [1;q]$$

sont des bijections et donc en particulier des applications injectives. Il découle alors du lemme II.4.4 que

$$q \leq p \text{ et } p \leq q$$

donc $p = q$.

Définition II.4.9 (Cardinal) Pour un ensemble fini A l'unique entier p tel qu'il existe une bijection $A \cong [1;p]$ est appelé *cardinal de* A ou *nombre d'éléments de* A on le notera $\#(A)$.

Exemple II.4.10 On a déjà remarqué que $[1;0] = \emptyset$ d'où il résulte que

$$\#(\emptyset) = 0 .$$

L'application

$$\{x\} \to [1;1] , \ x \mapsto 1$$

est manifestement une bijection d'où il résulte que

$$\#(\{x\}) = 1 = \mathfrak{s}(0) .$$

Proposition II.4.11 *Étant donnés deux ensembles finis A et B :*

i) Pour tout $x \notin A$,

$$\#(A \cup \{x\}) = \#(A) + 1 .$$

ii)

$$\#(A) + \#(B) = \#(A \cup B) + \#(A \cap B) ;$$

iii)

$$\#(A \times B) = \#(A) * \#(B) .$$

iv)

$$\#(A^B) = \#(A)^{\#(B)} .$$

***Preuve** : On notera*

$$p := \#(A) , \ q := \#(B) , \ \alpha : A \to [1;p] \text{ et } \beta : B \to [1;q]$$

des bijections définies par la proposition II.4.8.

i) Pour $x \notin A$, l'application $\gamma : A \cup \{x\} \to [1;p+1]$ définie par $\gamma(x) := p+1$, et $\gamma_{|A} := \alpha$, est une bijection.

ii) Si $B = \emptyset$,

$$\#(A)+\#(B) = \#(A) = \#(A\cup B) = \#(A\cup B)+\#(\emptyset) = \#(A\cup B)+\#(A\cap B)\,.$$

Il s'ensuit que l'ensemble E *des entiers* q *tels que pour tout* A *et tout ensemble* B *de cardinal* q*, la formule* $\#(A)+\#(B) = \#(A\cup B)+\#(A\cap B)$ *est satisfaite, contient* 0.

Pour $q \in \mathbb{N}$ *soit* B *un ensemble tel que* $\#(B) = \mathfrak{s}(q)$. *Alors*

$$\#(B) \neq 0 \Rightarrow B \neq \emptyset\,.$$

Soit donc $x \in B$*, et notons* $B = C \cup \{x\}$*.Il résulte alors du point i) que* $\#(C) = q$ *ou encore*

$$\#(B) = \#(C)+1\,.$$

On considère alors les deux cas suivants :

$x \in A$ *On a alors*

$$A\cup B = A\cup C \text{ et } A\cap B = (A\cap C)\cup\{x\}$$

d'où il résult, d'après le point i), que

$$\#(A\cup B)+\#(A\cap B) = \#(A\cup C)+\#(A\cap C)+1\,.$$

Si $q \in E$*, on a :*

$$\begin{aligned}\#(A\cup B)+\#(A\cap B) &= \#(A\cup C)+\#(A\cap C)+1\\ &= \#(A)+\#(C)+1 = \#(A)+\#(B)\,.\end{aligned}$$

On a ainsi montré que

$$\big((q\in E \wedge x\in A) \Leftrightarrow (\mathfrak{s}(q)\in E)\big)\,.$$

$x \notin A$ *On a alors*

$$A\cup B = A\cup C\cup\{x\} \text{ et } A\cap B = A\cap C$$

d'où il résult, d'après le point i), que

$$\#(A\cup B)+\#(A\cap B) = \#(A\cup C)+\#(A\cap C)+1\,.$$

Si $q \in E$*, on a :*

$$\begin{aligned}\#(A\cup B)+\#(A\cap B) &= \#(A\cup C)+\#(A\cap C)+1\\ &= \#(A)+\#(C)+1 = \#(A)+\#(B)\,.\end{aligned}$$

On a ainsi montré que

$$\big((q\in E \wedge x\notin A) \Leftrightarrow (\mathfrak{s}(q)\in E)\big)\,.$$

On a donc montré que dans tous les cas, l'ensemble E *satisfait au principe de récurrence II.0.PA*$_3$*) et donc que* $E = \mathbb{N}$ *ce qui achève la preuve.*

iii) Pour $B = \emptyset$ $A \times B = \emptyset$, *ce qui entraîne que* $\#(A \times B) = \#(A) * \#(B)$.
Pour $q \in \mathbb{N}$ *et* $\#(B) = \mathfrak{s}(q)$, $B \neq \emptyset$. *Écrivons alors* $B = C \cup \{x\}$. *On a alors*

$$A \times B = (A \times C) \cup (A \times \{x\})$$

ce qui permet de terminer la preuve par récurrence sur le cardinal de B *en utilisant le point ii).*

iv) Pour $B = \emptyset$ A^B *désigne l'ensemble des application* $\emptyset \to A$ *qui est toujours un singleton quel que soit* A. *Il s'ensuit que*

$$\#(A^B) = 1 = \#(A)^0 \text{ (cf. II.3.8.)}$$

Pour $q \in \mathbb{N}$, *et* B *tel que* $\#(B) = \mathfrak{s}(q)$, *notons* $C := B \cup \{x\}$. *On laisse alors le soin au lecteur de définir une bijection*

$$A^B \cong A^C \times A$$

qui permmetra de terminer la preuve par récurrence grâce au point iii).

Proposition II.4.12 *Soient* A *et* B *deux ensembles finis. Si* $\#(B) \leq \#(A)$:

i) toute application $i : A \to B$ *injective, est bijective ;*

ii) toute application surjective $p : B \to A$ *est bijective.*

Preuve : *On notera*

$$p := \#(A)\ ,\ q := \#(B)\ ,\ \alpha : A \to [1;p] \text{ et } \beta : B \to [1;q]$$

des bijections définies par la proposition II.4.8.

i) L'application

$$\beta \circ i \circ \alpha^{-1} : [1;p] \to [1;q]$$

est injective ce qui entraîne, en vertu du lemme II.4.4 que $p \leq q$. *Comme par hypothèse* $q \leq p$, *on a* $p = q$.

Corollaire II.4.13 (de la proposition II.4.8) *Soient* A *et* B *deux ensembles finis. Les assertions suivantes sont équivalentes :*

a) Il existe une bijection $A \cong B$.

b) Il existe une injection $A \hookrightarrow B$ *et une injection* $B \hookrightarrow A$.

c)

$$\#(A) = \#(B) .$$

***Preuve** :*

i) ***(a) $\Rightarrow$ b))***
Est immédiat dans la mesure où la bijection $A \cong B$ *(resp. sa réciproque* $B \cong A$*) fournit l'injection demandée* $A \hookrightarrow B$ *(resp.* $B \hookrightarrow A$*.)*

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

$$i : A \to B \text{ et } j : B \to A$$

des applications injectives. Puisque A *et* B *sont des ensembles finis, il existe, d'après la proposition II.4.8, entiers* p *et* q *et des bijections*

$$\alpha : A \cong [1; p] \text{ et } \beta : B \cong [1; q] .$$

Il s'ensuit que

$$\beta \circ i \circ \alpha^{-1} : [1; p] \to [1; q] \text{ et } \alpha \circ j \circ \beta^{-1} : [1; q] \to [1; p]$$

sont des applications injectives. Il résulte alors due lemme II.4.4 que

$$p = q .$$

iii) ***(c) $\Rightarrow$ a))***
Notons $p := \#(A) = \#(B)$. *D'après la proposition II.4.8 il existe des bijections*

$$\alpha : A \cong [1; p] \text{ et } \beta : B \cong [1; p] .$$

Il s(s'ensuit que

$$\beta^{-1} \circ \alpha : A \cong B$$

remplit la condition a).

Proposition II.4.14 (Parties finies de $\mathbb{N}$) *Étant donnée une partie* $P \subset \mathbb{N}$, *les conditions suivantes sont équivalentes :*

a) La partie P *est non vide et finie.*

b) La partie P est non vide et majorée.

c) La partie P possède un plus grand élément.

d) Il existe un unique $m \in \mathbb{N}$ tel qu'il existe une bijection $[1; m] \cong P$.

***Preuve** : Cette proposition n'est qu'une sunthèse de résultats déjà établis et nous laissons au lecteur le soin de les rassembler.*

Proposition II.4.15 *Une partie $P \subset \mathbb{N}$ de $\mathbb{N}$ est soit finie soit dénombrable.*

***Preuve** : Pour toute partie P de $\mathbb{N}$, on peut définir les suites*

$$\left(P_n\right)_{,n\in\mathbb{N}} \text{ et } \left(Q_n\right)_{,n\in\mathbb{N}}$$

de la manière suivante :

$$\begin{array}{rrcl} & P_0 & := & P \\ & Q_0 & := & \emptyset \\ \forall n \in \mathbb{N} & P_{n+1} & := & P_n \setminus \{\min(P_n)\} \text{ si } P_n \neq \emptyset \\ & & := & \emptyset \text{ sinon} \\ \forall n \in \mathbb{N} & Q_{n+1} & := & Q_n \cup \{\min(P_n)\} \text{ si } P_n \neq \emptyset \\ & & := & Q_n \text{ sinon } . \end{array} \qquad \text{II.4.15.1}$$

Il n'est pas difficile d'établir par récurrence que :

$$\forall P \subset \mathbb{N}\ ,\ \forall n \in \mathbb{N},\ P = P_n \cup Q_n \text{ et } Q_n \text{ est finie } . \qquad \text{II.4.15.2}$$

Il s'ensuit que si P n'est pas finie, pour tout n P_n n'est pas finie et en particulier,

$$\forall n \in \mathbb{N},\ P_n \neq \emptyset\ .$$

Posons donc

$$\forall n \in \mathbb{N},\ f(n) := \min(P_n)\ .$$

On définit ainsi une application $f : \mathbb{N} \to P$. Ce peut être un très bon exercice de montrer qu'elle est bijective.

II.5 . −Suites, produits finis

la proposition qui suit (II.5.1) généralise la proposition I.2.14 qui en est un cas particulier pour $n = 2$, mais doit cependant être établie préalablement pour pouvoir raisonner par récurrence.

Proposition II.5.1 *Soient $n \in \mathbb{N}^*$, et $E_{k\ ,1\leq k\leq n}$, des ensembles.*

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

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

sachant que le produit cartésien de deux ensembles a été défini en I.2.1.ii).

ii) On définit également des projections

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

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

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

Ce qu'on peut écrire

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

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

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

iv) Dans le cas où il existe un ensemble E tel que $\forall 1 \ \leq \ k \ \leq \ n, \ E_k \ = \ E$, on rappelle que $E^{[1;n]}$ désigne l'ensemble des applications de $[1; n]$ à valeurs dans E (cf. I.2.5.) Pour tout $1 \ \leq \ k \ \leq \ n$, on définit

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

En vertu de iii), il existe une unique application

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

L'application ϕ est alors une bijection ;

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

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

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

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

Remarque II.5.2 La construction faite en II.5.1.iv) consiste en fait à considérer une application de $[1;n]$ dans E à travers son graphe qui est un n-uplet de couples

$$((1, f(1), \ldots, (n, f(n))$$

qu'on identifie à

$$(f(1), \ldots, f(n))$$

qui est un élément de $\prod_{k=1}^{n} E$.

Notation II.5.3 Dans le cas de II.5.1.iv) ou de la remarque II.5.2, pour tout $n \in \mathbb{N}^*$, et tout ensemble E, on notera

$$E^n = \prod_{k=1}^{n} E \cong E^{[1;n]}\,.$$

La proposition quie suit (II.5.4) généralise la proposition II.5.1 au cas des magmas ou bien encore la proposition I.6.23 au cas de plus de deux facteurs :

Proposition II.5.4 *Étant donnés un entier* $n \in \mathbb{N}^*$, $(M_k, *_k)_{,1 \leq k \leq n}$ *des magmas (cf. I.6.1,) notons*

$$\forall 1 \leq k \leq n,\ p_k : \prod_{i=1}^{n} M_i \to M_k \text{ les projections}\ .$$

Alors :

i) Il existe une unique loi de composition $*$ *sur* $\prod_{k=1}^{n} M_k$ *telle que pour tout* $1 \leq k \leq n$ p_k *soit un morphisme ; la loi* $*$ *est donnée par*

$$\forall \big((x_1, \ldots, x_n), (y_1, \ldots, x_n)\big) \in \prod_{k=1}^{n} M_k \times \prod_{k=1}^{n} M_K,$$
$$(x_1, \ldots, x_n) * (y_1, \ldots, y_n) = (x_1 *_1 y_1, \ldots, x_n *_n y_n)\,.$$

ii) La loi $*$ *étant définie sur* $\prod_{k=1}^{n} M_k$ *comme ci-dessus, si*

a) pour tout $1 \leq k \leq n$ $*_k$ *est associative,* $*$ *l'est aussi ;*

b) pour tout $1 \leq k \leq n$ $*_k$ *est commutative,* $*$ *l'est aussi ;*

c) pour tout $1 \leq k \leq n$ $*_k$ *possède un élément neutre* e_k, $(e_1, \ldots, e_n)$ *est un élément neutre pour* $*$;

d) $x \in \prod_{k=1}^{n} M_k$ *est tel que pour tout* $1 \leq k \leq n$ $p_k(x)$ *possède un symétrique* y_k *dans* M_k,

alors $(y_1, \ldots, y_n)$ *est un symétrique pour* x *dans* $\prod_{k=1}^{n} M_k$.

iii) Pour tout n*-uplet de morphismes*

$$f_k \ : \ N \ \to \ M_k \ , 1 \leq k \leq n \ ,$$

il existe un unique morphisme

$$f \ : \ N \ \to \ \prod_{k=1}^{n} M_k \text{ tel que } \forall 1 \leq k \leq n, \ f_k \ = \ p_k \ \circ \ f \ .$$

iv) Dans le cas où il existe M *tel que* $\forall 1 \leq k \leq n, \ M_k \ = \ M$, *la bijection* $\phi \ : \ M^{[1;n]} \ \cong \ \prod_{k=1}^{n} M$

définie par la proposition II.5.1.iv) est un isomorphisme, pour peu que $M^{[1;n]}$ *soit muni de la structure définie par la proposition I.6.20.*

Définition II.5.5 (Structure produit) Avec les notations de la proposition II.5.4 la loi $*$ définie sur $\prod_{k=1}^{n} M_k$ comme en II.5.4.i) est appelée *structure produit* ou *loi produit*.

II.6 . −Exercices

Exercice II.6.1 [L'addition dans $\mathbb{N}$]

1) () **(L'addition dans** $\mathbb{N}$**)**

On suppose donné, dans cet exercice, un ensemble $\mathbb{N}$ **contenant un élément** 0, **muni d'une application** $\mathfrak{s} \ : \ \mathbb{N} \ \to \ \mathbb{N}$ **satisfaisant les axiomes :**

PA$_1$) (Succ$_1$)

$$\forall p \in \mathbb{N}, \ \big(p \ \neq \ 0 \ \Leftrightarrow \ \exists q \in \mathbb{N}, \ (p \ = \ \mathfrak{s}(q))\big) \ .$$

PA$_2$) (Succ$_2$)

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \big(\mathfrak{s}(p) \ = \ \mathfrak{s}(q) \ \Rightarrow \ p \ = \ q\big)\ .$$

PA$_3$) (Ind)

$$\forall A \subset \mathbb{N},\ \big(0 \in A \ \wedge \ \forall p(p \in A \ \Rightarrow \ \mathfrak{s}(p) \in A) \ \Rightarrow \ A \ = \ \mathbb{N}\big)\ .$$

On veut définir l'addition $+ \ : \ \mathbb{N} \times \mathbb{N} \ \to \ \mathbb{N}$ **satisfaisant les axiomes :**

PA$_4$) (Add$_1$)

$$\forall p \in \mathbb{N},\ (0 + p \ = \ p)\ .$$

PA$_5$) (Add$_2$)

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \big(\mathfrak{s}(p) \ + \ q \ = \ \mathfrak{s}(p+q)\big)\ .$$

ainsi qu'un certain nombre d'autres propriétés.

On cherche à définir une application $\sigma \ : \ \mathbb{N} \ \to \ \mathbb{N}^{\mathbb{N}}$ ou encore un élément de $(\mathbb{N}^{\mathbb{N}})^{\mathbb{N}}$ de la manière suivante :

i) $\sigma(0) \ := \ \mathrm{Id}_{\mathbb{N}}$,

ii)
$$\forall n \in \mathbb{N},\ \sigma(\mathfrak{s}(n)) \ = \ \mathfrak{s} \ \circ \ \sigma(n)\ .$$

a) () Montrer que σ est bien définie c'est-à-dire que le domaine de définition D de σ est égal à $\mathbb{N}$.

b) () Montrer que
$$\forall n \in \mathbb{N},\ \mathfrak{s} \circ \sigma(n) \ = \ \sigma(n) \circ \mathfrak{s}\ .$$

Dans la suite, on notera

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ p \ + \ q \ := \ \sigma(p)(q) \ \in \ \mathbb{N}\ .$$

Il découle immédiatement des hypothèses i) et ii) respectivement que les axiomes 0.1.PA$_4$) et 0.1.PA$_5$) sont satisfaits.

2) () Montrer que

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \mathfrak{s}(p) + q \ = \ \mathfrak{s}(p+q) \ = \ p + \mathfrak{s}(q)\ .$$

3) () (**Associativité de l'addition**)
Montrer que

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ (p+q)+r \ = \ p+(q+r)\ ;$$

4) () (**Élément neutre**)
Montrer que

$$\forall p \in \mathbb{N},\ 0+p \ = \ p+0 \ = \ p\ .$$

5) () (**Commutativité**)

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ p+q \ = \ q+p\ .$$

Exercice II.6.2 [] Faire le preuve de la proposition II.4.2.

III . −Groupes, morphismes, sous-groupes

III.1 . −Groupe

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

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

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

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

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

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

Il revient au même de dire que $(G,*)$ est un magma associatif possédant un élément neutre et dans lequel tout élément possède un symétrique au sens des définitions du paragraphe I.6.

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

Exemple III.1.2 i) Il n'existe pas de loi de composition $*$ sur $\emptyset$ fasse de $(\emptyset,*)$ un groupe. L'axiome III.1.1.Gr_2) entraîne, en effet, qu'un groupe possède toujours au moins un élément c'est-à-dire n'est jamais vide.

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

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

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

Un des premiers groupes qu'on peut introduire, au sens où sa définition ne nécessite guère plus que les premiers axiomes de la théorie des ensembles(cf. I,) est le groupe $\mathcal{S}(E)$ des bijections d'un ensemble E muni de la loi $\circ$. C'est une partie du magma considéré dans l'exemple I.6.12, et précisément celle constituée des éléments qui ont un symétrique. Pour ne nécessiter que très peu de matériel pour être défini, ce groupe n'est cependant pas le plus aisé à étudier comme le montre le chapitre VI qui lui est entièrement consacré et encore seulement dans le cas où E est un ensemble fini. Pour tout ensemble E, l'ensemble $\mathcal{S}(E)$ des bijections de E dans lui-même muni de la loi $\circ$ de composition des applications est un groupe. En effet :

- si $f \text{et } g \ : \ E \ \to \ E$ sont des bijections de E dans lui-même la composée $f \circ g$ est encore une bijection de E dans lui même, assurant que $\circ$ est bien une loi de composition (cf. I.6.1.)
- L'application identité de E (cf. I.2.6.a),) usuellement notée Id_E est un élément neutre pour $\circ$.
- Enfin pour toute bijection $f \ : \ E \ \to \ E$ son application réciproque f^{-1} est précisément un symétrique pour la composition $\circ$.

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

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

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

Un groupe n'étant rien de plus (ni de moins d'ailleurs) qu'un magma associatif possédant un élément neutre et dans lequel tout élément possède un symétrique, la proposition I.6.13 vaut encore ici mutatis mutandis.

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

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

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

***Preuve** : (cf. III.5.1.)*

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

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

De même la proposition I.6.20 a son pendant pour les groupes :

Proposition III.1.6 *Étant donnés un groupe $(G, *)$ et un ensemble E, l'ensemble G^E des applications de E dans G muni de la loi induite (cf. I.6.20,) est un groupe (abélien si G l'est.)*

III.2 . −Morphisme

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

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

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

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

On notera $\mathrm{Hom}_{\mathbf{Gr}}(G, H)$ (ou simplement $\mathrm{Hom}(G, H)$ si le contexte ne prête pas à confusion) l'ensemble des morphismes de G dans H.

Remarque III.2.2 On constate que dans la définition ci-dessus aucune condition supplémentaire n'est exigée par rapport à un morphisme de magma (cf. I.6.2.)

On a l'exact analogue du lemme I.6.3 :

Lemme III.2.3 *i) Pour tout groupe $(G, *)$ l'identité Id_G est un morphisme du groupe G dans lui-même.*

ii) Pour $(G, *_G)$, $(H, *_H)$ et $(K, *_K)$ des groupes, $f : G \to H$ et $g : H \to K$ des morphismes, le composé $g \circ f$ est un morphisme.

On peut donc donner une définition analogue à la définition I.6.4 :

Définition III.2.4 Étant donnés deux groupes $(G, *)$ et $(H, \cdot)$, un morphisme $f : G \to H$ est un *isomorphisme* s'il existe un morphisme $g : H \to G$ tel que

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

On notera $\mathrm{Isom}_{\mathbf{Gr}}(G, H)$ (ou simplement $\mathrm{Isom}(G, h)$ si le contexte est clair) l'ensemble des isomorphismes de $(G, *)$ dans $(H, \cdot)$.

On a encore, san surprise puisqu'en fait l'axiomatique n'est pas vraiement différente, un analogue de la proposition I.6.5 :

Proposition III.2.5 *Étant donnés deux groupes $(G, *)$ et $(H, \cdot)$, une application $f : G \to H$ est un isomorphisme si et seulement si c'est un morphisme bijectif.*

Preuve *: Il n'y a rien de plus à montrer que dans la preuve de la proposition I.6.5.*

Exemple III.2.6 Soit E et F deux ensembles. On rappelle (cf. III.1.2.c),) que

$$(\mathcal{S}(E), \circ) \text{ (resp. } (\mathcal{S}(F), \circ) \text{)}$$

est le groupe des bijections de E (resp. F,) dans lui-même.

Soit $u : E \to F$ une bijection de E dans F. L'application

$$\mathcal{S}(u) : \mathcal{S}(E) \to \mathcal{S}(F) , \ f \mapsto u \circ f \circ u^{-1}$$

est un isomorphisme de groupes.

Des définitions analogues à I.6.6 peuvent donc être données :

Définition III.2.7 Soit $(G, *)$ un groupe.

i) (**Endomorphismes**)

Un morphisme $f : G \to G$ de G dans lui-même est appelé *endomorphisme*. On note $\mathrm{End}_{\mathbf{Gr}}(G)$ (ou simplement $\mathrm{End}(G)$,) l'ensemble des endomorphismes de G.

ii) (**Automorphisme**)

Un morphisme $f : G \to G$ est un *automorphisme* si c'est à la fois un isomorphisme et un endomorphisme. Il revient au même, grâce à la proposition III.2.5, de dire que f est un endomorphisme bijectif. On note $\mathrm{Aut}_{\mathbf{Gr}}(G)$ (ou simplement $\mathrm{Aut}(G)$) l'ensemble des automorphismes de G.

Exemple III.2.8 Pour un groupe G, l'identité Id_G est un automorphisme.

Proposition III.2.9 (Propriétés des morphismes) *Étant donné un morphisme de groupe*

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

i) $f(e_G) = e_H$;

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

Preuve *:*

i) (cf. III.5.3.question 1).)

ii) (cf. III.5.3.question 2).)

III.3 . −Sous-groupe

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

Remarque III.3.2 i) Il ne suffit pas pour que H soit un sous-groupe de G que H soit un sous-magma de G comme le montre l'exercice I.8.15.question 2). Il faut en effet exiger en plus que H possède un élément neutre (cf. III.1.1.Gr_2)e)t que tout élément de H possède un symétrique (cf. III.1.1.Gr_3).)

ii) La définition de sous-groupe donnée ci-dessus n'est peut-être pas celle qu'on a été habitué à rencontrer qui est parfois plutôt la caractérisation donnée à la proposition III.3.4.b). On ne peut cependant se contenter de cette dernière en l'état puisqu'aux termes stricts de cet énoncé on ne saurait même pas qu'un sous-groupe est lui-même un groupe, ce qui avouons-le devra à tout le moins être établi, si l'on veut bénéficier d'une théorie utilisable. L'énoncé clef est en fait l'équivalence entre III.3.4.a) et III.3.4.b).

Le lemme technique suivant est un ingrédient permettant d'établir l'équivalence entre les diverses caractérisations des sous-groupes.

Lemme III.3.3 *Soit $(G, *)$ un groupe d'élément neutre ϵ_G et H un sous-groupe de G au sens de la définition III.3.1. Notons $*_H$ la restriction de $*$ à $H \times H$.*

i) L'élément neutre ϵ_H de H est l'élément neutre ϵ_G de G.

***Preuve** : Si ϵ_H est l'élément neutre de H, pour tout $x \in H$, $x *_H \epsilon_H = x$. Cependant, x et ϵ_H étant en particulier des éléments de G, on peut encore écrire, $x * \epsilon_H = x$. D'autre part, $x * \epsilon_G = x$. Notons x^{-1} le symétrique de x dans G. On a alors :*

$$x * \epsilon_H = x * \epsilon_G \Rightarrow x^{-1} * x * \epsilon_H = x^{-1} * x * \epsilon_G \Rightarrow \epsilon_H = \epsilon_G$$

c'est-à-dire que l'élément neutre de H est celui de G.

ii) Pour tout $x \in H$, l'inverse ${x^{-1}}_H$ de x dans H est aussi son inverse dans G.

***Preuve** : Tout $x \in H$ possède un inverse ${x^{-1}}_H$ tel que*

$$x *_H {x^{-1}}_H = {x^{-1}}_H *_H x = \epsilon_H = \epsilon_G$$

en utilisant le point i). Or x et ${x^{-1}}_H$ étant en particulier des éléments de G, on peut encore écrire,

$$x * {x^{-1}}_H = {x^{-1}}_H * x = \epsilon_G$$

c'est-à-dire que ${x^{-1}}_H$ est l'inverse x^{-1} de x dans G puisque ce dernier est unique (cf. III.1.4.i).)

Proposition III.3.4 (Sous-Groupe) *Étant donnés un groupe $(G, *)$ et $H \subset G$ une partie de G, les assertions suivantes sont équivalentes :*

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

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

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

d) La restriction

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

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

Preuve *:*

i) ***(a)*** $\Rightarrow$ ***b))***

Si H est un sous-groupe de G, en particulier H est un groupe et il est donc non vide (cf. III.1.2.i).)

Pour tout couple (x, y) d'éléments de H, x et y^{-1} sont encore des éléments de H (cf. III.3.3.ii).) Dire que la restriction $*_H$ de $*$ à $H \times H$ donne à H une structure de groupe signifie, en particulier, qu'elle est à valeurs dans H, ce qui prouve que

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

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

Réciproquement, supposons donnée une partie non vide H de G telle que pour tout couple (x, y) d'éléments de H, $x * y^{-1} \in H$.

Si H est non vide il existe en particulier un élément $x \in H$, et, dès lors, $\epsilon_G = x * x^{-1} \in H$. Il est clair que ϵ_G est alors un élément neutre pour H.

De plus, pour tout $x \in H$, puisque $\epsilon_G \in H$, $\epsilon_G * x^{-1} = x^{-1} \in H$ c'est-à-dire que tout élément de H possède un inverse dans H.

Enfin, pour tout couple (x, y) d'éléments de H, $y^{-1} \in H$ et

$$x * y \;=\; x * (y^{-1})^{-1} \;\in\; H$$

c'est-à-dire que la restriction de $*$ à $H \times H$ est bien à valeurs dans H.

La partie H de G est donc bien un sous-groupe.

Exemple III.3.5 Étant donné un groupe $(G, *)$ d'élément neutre ϵ, les ensembles $\{\epsilon\}$ et G lui-même sont des sous-groupes de G.

Proposition III.3.6 *Soient G un groupe, H et K des sous-groupes de G.*

i) $H \cap K$ est un sous-groupe de G.

Preuve *: (cf. TD n° III, exercice D.)*

ii) Plus généralement, pour $\mathcal{H}$ un ensemble non vide de sous-groupes de G, $\bigcap_{H\in\mathcal{H}} H$ est un sous-groupe de G.

Preuve *: Voir l'exercice III.5.6.*

iii) $H \cup K$ *est un sous-groupe de* G *si et seulement si*

$$H \subset K \text{ ou } K \subset H .$$

Preuve *: (cf. TD n° III, exercice E.)*

iv) Si $\left(H_n\right)_{,n\in\mathbb{N}}$ *est une suite de sous-groupes de* G *telle que*

$$\forall (p,q) \in \mathbb{N}\times\mathbb{N},\ \exists r \in \mathbb{N},\ H_p \subset H_r \text{ et } H_q \subset H_r,$$

alors $\bigcup_{n\in\mathbb{N}} H$ *est un sous-groupe de* G.

Preuve *: (cf. III.5.7.)*

Proposition III.3.7 (Image directe/réciproque) *Soit* $f : G \to H$ *un morphisme de groupes.*

i) (***Image directe***)
Pour tout sous-groupe G' *de* G, *l'image directe de* G'

$$f(G') = \{y \in H\ ;\ \exists x \in G',\ ,\ y = f(x)\}$$

est un sous-groupe de H.

ii) (***Image réciproque***)
Pour tout sous-groupe H' *de* H, *l'image réciproque*

$$f^{-1}(H') = \{x \in G\ ;\ f(x) \in H'\}$$

est un sous-groupe de G.

Définition III.3.8 (Noyau/image) Étant donné un morphisme de groupes $f : G \to H$, ϵ_H étant l'élément neutre de H, on appelle

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

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

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

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

Corollaire III.3.9 *Pour un morphisme de groupes $f \ : \ G \ \to \ H$, le noyau (resp. l'image) de f est un sous-groupe de G (resp. H.)*

Proposition III.3.10 *Un morphisme de groupes $f \ : \ G \ \to \ H$ est injectif (resp. surjectif) si et seulement si* $\mathrm{Ker}\, f \ = \ \{\epsilon_G\}$ *(resp.* $\mathrm{Im}\, f \ = \ H$.)

Définition III.3.11 Si $i \ : \ H \ \to \ G$ est un morphisme de groupes injectif, il induit un isomorphisme $H \ \cong \ \mathrm{Im}\, i$; si bien que H est isomorphe à un sous-groupe de G. On dira parfois même par abus de langage que H est lui-même un sous-groupe de G.

III.4 . −Partie génératrice

Dans tout ce paragraphe (III.4,) $(G, *)$ **est un groupe dont lélément neutre est noté** e **et dans lequel l'inverse (symétrique) de toute élément** x **est noté** x^{-1}.

Lemme III.4.1 *Étant donnée une partie $S \ \subset \ G$, notons $\mathcal{G}_S$ l'ensemble des sous-groupes de G contenant S. Alors*

$$< S > := \bigcap K \in \mathcal{G}_S K$$

est le plus petit élément (pour l'inclusion) de $\mathcal{G}_S$.

Preuve *: On remarque d'abord que $\mathcal{G}_S$ est non vide puisque $G \ \in \ \mathcal{G}_S$. Or pour tout $K \ \in \ \mathcal{G}_S$, $S \ \subset \ K$, donc*

$$S \ \subset < S > .$$

Il s'ensuit en particulier que

$$< S > \neq \ \emptyset \, .$$

Pour tout $(x, y) \ \in < S > \times < S >$, par définition,

$$\forall K \in \mathcal{G}_S, \ x \ \in \ K \ \text{et} \ y \ \in \ K$$

il s'ensuit (cf. III.3.4,) que

$$\forall K \in \mathcal{G}_S, \ x * y^{-1} \ \in \ K$$

ce qui entraîne que $x * y^{-1} \ \in < S >$ ce qui combiné au fait que $< S >$ est non vide assure que $< S >$ est un sous-groupe de G.

Puisque, de plus $S \ \subset < S >$,

$$< S > \in \ \mathcal{G}_S \, .$$

Il est immédiat de montrer, et ce du fait même de la définition de $< S >$*, que*

$$\forall k \in \mathcal{G}_S,\ < S > \subset\ K$$

c'est-à-dire que $< S >$ *est un minorant de* $\mathcal{G}_S$ *qui, étant de plus élément de* $\mathcal{G}_S$ *est son plus petit élément.*

Définition III.4.2 Étant donné un groupe G et $S\ \subset\ G$ une partie de G :

i) (**sous-groupe engendré**)
le sous-groupe $< S >$ de G défini par le lemme III.4.1 s'appelle le *sous-groupe de* G *engendré par* S ;

ii) (**partie génératrice**)
si $G\ =< S >$, on dit que G est *engendré* par S ou que S est une *partie génératrice* de G.

Exemple III.4.3 a) Pour tout groupe G d'élément neutre e,

$$< \emptyset >=\ \{e\}\ .$$

b) Pour tout groupe G, $G\ =< G >$.

Définition III.4.4 (Groupe monogène) Pour un groupe G et $x\ \in\ G$, si $< \{x\} >=\ G$ on dit que G est *monogène*.

Notation III.4.5 Pour deux sous-groupes H et K d'un groupe G, on note

$$HK\ := < (H \cup K) >$$

qui est le plus petit sous-groupe contenant à la fois H et K. Si G est abélien la notation

$$H + K\ := < (H \cup K) >$$

sera plutôt utilisée.

Remarque III.4.6 On a vu en III.3.6.iii) que $H \cup K$ n'est pas en général un sous-groupe de G et c'est HK qui « joue alors le rôle » de $H \cup K$. Si le lecteur a quelques souvenirs de son cours d'algèbre linéaire il remarquera que c'est précisément la situation rencontrée pour les espaces vectoriels, ce qui n'a d'ailleurs rien d'étonnant, ces derniers étant en particuliers des groupes abéliens.

Proposition III.4.7 *Étant donnés un groupe G et une partie S de G, on note (comme au lemme III.4.1,) $\mathcal{G}_S$ l'ensemble des sous-groupes de G qui contiennent S. Alors pour toute partie H G, les assertions suivantes sont équivalentes :*

a) L'ensemble H est l'intersection de tous les sous-groupes de G contenant S :

$$H \;=\; \bigcap_{K \,\in\, \mathcal{G}_S} K \;;$$

b)

$$H \;\in\; \mathcal{G}_S \text{ et } \forall K \in \mathcal{G}_S,\; H \;\subset\; K$$

autrement dit H est le plus petit élément de $\mathcal{G}_S$;

c) H est constitué des éléments $t_1 t_2 \dots t_r$ avec $r \geq 1$ où un élément t_i est dans S ou a son inverse dans S.

***Preuve** : Voir le TD n° III, exercice G.*

III.5 . −Exercices

Exercice III.5.1 [Unicité des éléments remarquables] Soit $(E, *)$ un ensemble muni d'une loi associative.

1) () (**Élément neutre**)
Montrer que si $(E, *)$ possède un élément neutre ϵ celui-ci est unique.

2) () (**Symétrique**)
Montrer que si $(E, *)$ possède un élément neutre ϵ, tout élément $x \in E$ possède au plus un symétrique.

Exercice III.5.2 [] Faire la preuve de la proposition III.1.6.

Exercice III.5.3 [Morphismes de groupes] Soit

$$f \;:\; (G, *, \epsilon_G) \;\to\; (H, \bullet, \epsilon_H)$$

un morphisme de groupes.

1) () (**Élément neutre**)
Montrer que $f(\epsilon_G) \;=\; \epsilon_H$.

2) () (**Symétrique**)
Montrer que pour tout $x \in G$, si y est son symétrique, $f(y)$ est le symétrique de $f(x)$.

3) () (**Image**)
Montrer que $\mathrm{Im}\, f$ est un sous-groupe de $(H, \bullet)$.

4) () (**Noyau**)
Montrer que $\mathrm{Ker}\, f$ est un sous-groupe de $(G, *)$.

5) () (**Isomorphisme**)
Montrer que si f est bijective et que g est son applications réciproque, alors g est un morphisme de groupe.

Exercice III.5.4 [] Faire la preuve de la proposition III.2.9 et comparer à la situation des magmas envisagée dans l'exercice I.8.13.

Exercice III.5.5 [] Compléter la preuve de la proposition III.3.4.

Exercice III.5.6 [] Faire la preuve de la proposition III.3.6.ii).

Exercice III.5.7 [] Faire la preuve de la proposition III.3.6.iv).

Exercice III.5.8 [] Faire la preuve de la proposition III.3.7.

Exercice III.5.9 []

1) () Étant donnés un groupe G et deux parties S et T de G, montrer que

$$< S \cup T > = < S > \ + \ < T > \ .$$

2) () Étant donné un groupe $(G, *)$ pour une partie $S \subset G$ $< S >$ est l'ensemble des éléments $x \in G$ tels que :

$$\exists d \in \mathbb{N}^*, \ \exists s_i \, , 1 \leq i \leq d \in S, \ \exists \alpha_i \, , 1 \leq i \leq d \in \mathbb{Z}, \ x = \prod_{i=1}^{d} s_i^{\alpha_i} \ , \qquad 1$$

en prenant garde que, dans le produit ci-dessus, l'ordre des facteurs n'est pas indifférent, dans la mesure où l'on ne suppose pas que G est abélien. Pour ne pas exclure le cas où $S = \emptyset$, on conviendra que, dans ce cas, le produit ci-dessus vaut e.

IV . −L'ensemble $\mathbb{Z}$ des entiers relatifs

IV.0 . −Introduction

Même si, dans ce chapitre, nous allons montrer au paragraphe IV.3 que l'ensemble $\mathbb{Z}$ possède une structure d'anneau et même au paragraphe IV.5, une structure d'anneau euclidien nous ne considérerons dans les chapitres IV, V et VI la structure de groupe abélien de $(\mathbb{Z}, +)$. Les propriétés arithmétiques de l'anneau $\mathbb{Z}$ seront étudiées en détail au chapitre IX et plus précisément dans les paragraphes IX.2, IX.3, IX.4, IX.5, IX.6 et IX.7.

IV.1 . −Construction de l'ensemble $\mathbb{Z}$ des entiers relatifs

On cherche à définir $\mathbb{Z}$ comme l'ensemble des « différences » d'entiers naturels c'est-à-dire que, pour deux entiers p et q, il existe un entier naturel r tel que soit $q = p + r$ soit $p = q + r$ (cf. II.2.5.) Dans le dernier cas, on voudrait écrire $p - q = r$ et dans le premier cas, $p - q = -r$.

En procédant ainsi il faudra bien évidemment tenir compte du fait que plusieurs couples peuvent donner la même différence, et prendre ce dernier point en compte dans la définition des opérations sur $\mathbb{Z}$: (cf. IV.3.)

Ce point de vue risque d'être source d'une grande quantité de disjonctions pénibles à manier et l'on sait bien que dès qu'il s'agit d'« identifier » on doit pouvoir recourir au formalisme des relations d'équivalences (cf. I.2.2.v)).

On évite ces inconvénients en procédant comme suit, et l'on retrouvera l'idée initiale après avoir construit l'addition sur $\mathbb{Z}$ (cf. IV.3.9.ii) :)

Notation IV.1.1 On note :

$$Z := \mathbb{N} \times \mathbb{N} \qquad \text{IV.1.1.1}$$

l'ensemble des couples d'entiers naturels à ne pas confondre avec $\mathbb{Z}$ que nous allons définir dans cette section.

Sur l'ensemble Z, on considère la relation binaire (cf. I.2.1.iii) :) $\sim$ définie par :

$$\forall (p,q) \in Z,\ \forall (r,s) \in Z,\ (p,q) \sim (r,s) \Leftrightarrow p + s = q + r\ . \qquad \text{IV.1.1.2}$$

Ceci pourrait se réécrire, pour peu qu'on ait introduit la notation $p - q = r - s$ et correspond donc bien à l'idée qu'on se fait que l'on identifie deux couples qui donnent la même « différence ».

Proposition IV.1.2 *La relation $\sim$ est une relation d'équivalence (cf. I.2.2.v).) Pour tout*

$$(p,q) \in Z \text{ on notera } \overline{(p,q)} := \left\{(r,s) \in Z\ ;\ (r,s) \sim (p,q)\right\}$$

la classe du couple (p,q).

Preuve *: . (cf. IV.6.1.)*

IV.2 . −Entiers relatifs

Définition IV.2.1 (Entiers relatifs) On appelle *ensemble des entiers relatifs* l'ensemble des classes de Z selon $\sim$ encore appelé ensemble *quotient* $Z/\sim$ et finalement noté $\mathbb{Z}$. Un élément de $\mathbb{Z}$ est un *entier relatif*.

Notation IV.2.2 On notera :

$$\begin{array}{rccc} \pi : & Z & \to & \mathbb{Z} \,=\, Z/\sim \\ & (p,q) & \mapsto & \overline{(p,q)} \end{array} \qquad \text{IV.2.2.1}$$

la *surjection canonique* (cf. I.5.7.ii).)

Proposition IV.2.3 *Pour toute classe $\overline{(p,q)} \in \mathbb{Z}$, il existe un unique entier naturel r, tel que*

$$\overline{(p,q)} \;=\; \overline{(r,0)} \text{ ou } \overline{(0,r)}\,.$$

La disjonction précédente n'étant pas exclusive.

Preuve : *Pour tout couple d'entiers naturels (p,q), il existe, (cf. II.2.5) un entier naturel r tel que*

$$p+r \;=\; q \;\Leftrightarrow\; (p,q)\sim(0,r) \text{ ou } q+r \;=\; p \;\Leftrightarrow\; (p,q)\sim(r,0)$$

ce qui prouve l'<u>existence</u>

Si maintenant, r et r' sont deux entiers naturels tels que, par exemple,

$$\overline{(p,q)} \;=\; \overline{(r,0)} \;=\; \overline{(r',0)}\,,$$

$(r,0)\sim(r',0)$ c'est-à-dire (cf. IV.1.1.2) $r+0 \;=\; r'+0$ c'est-à-dire $r \;=\; r'$ ce qui assure l'<u>unicité</u>.

Proposition IV.2.4 *Les applications*

$$\begin{array}{rccc} i_+ : & \mathbb{N} & \longrightarrow & \mathbb{Z} \\ & p & \longmapsto & \overline{(p,0)} \end{array} \qquad \textit{IV.2.4.1}$$

et

$$\begin{array}{rccc} i_- : & \mathbb{N} & \longrightarrow & \mathbb{Z} \\ & p & \longmapsto & \overline{(0,p)} \end{array} \qquad \textit{IV.2.4.2}$$

sont injectives. (cf. I.2.7.i).)

Preuve : *Pour $\overline{(p,q)} \in \mathbb{Z}$, si r et r' sont deux entiers naturels tels que $i_+(r) = i_+(r')$, alors*

$$\overline{(p,q)} \;=\; \overline{(r,0)} \;=\; \overline{(r',0)}$$

ce qui, nous l'avons déjà vu dans la démonstration de la proposition IV.2.3 implique que $r = r'$.

La vérification pour i_- est tout à fait identique.

Corollaire IV.2.5 *Les propositions IV.2.3 et IV.2.4 ont pour conséquence que :*

i) $i_+(\mathbb{N})$ *est une partie de* $\mathbb{Z}$ *en bijection (cf. I.2.7.iii)) avec* $\mathbb{N}$. *On identifiera dans la suite* $\mathbb{N}$ *à* $i_+(\mathbb{N})$ *et pour tout entier naturel* $p \in \mathbb{N}$, *on écrira aussi* $p \in \mathbb{Z}$ *pour* $\overline{(p,0)} \in \mathbb{Z}$.

ii) L'ensemble $\mathbb{Z}$ *est la réunion de* $i_+(\mathbb{N})$ *et* $i_-(\mathbb{N})$.
On notera souvent

$$\mathbb{Z}^+ := i_+(\mathbb{N}) \text{ et } \mathbb{Z}^- := i_-(\mathbb{N})$$

et l'on écrira, également $\mathbb{N} = \mathbb{Z}^+$.

iii) L'intersection de $i_+(\mathbb{N})$ *et* $i_-(\mathbb{N})$ *est la classe* $\overline{(0,0)}$ *que nous ne tarderons pas à noter simplement* 0.

Définition IV.2.6 (Entiers positifs/négatifs) On appellera $\mathbb{Z}^+$ l'ensemble des *entiers relatifs positifs* et $\mathbb{Z}^-$ l'ensemble des *entiers relatifs négatifs*.

IV.3 . −L'anneau $(\mathbb{Z}, +, *)$

Dans ce paragraphe (IV.3) l'ensemble noté Z est celui introduit en IV.1.1.1.

Notation IV.3.1 On définit une loi de composition $+_Z$ sur Z par :

$$\forall (p,q) \in Z\ ,\ \forall (r,s) \in Z\ ,\ (p,q)\ +_Z\ (r,s)\ :=\ (p +_{\mathbb{N}} r, q +_{\mathbb{N}} s) \qquad \text{IV.3.1.1}$$

cette écriture ayant un sens puisque l'addition sur $\mathbb{N}$ est bien définie (cf. II.1.5.)

Une chose est de comprendre quelle peut être la formule qui définit la multiplication, une autre de justifier qu'elle définit bien l'opération que l'on souhaite.

Néanmoins, si l'on supposait la multiplication complètement construite, et possédant toutes les propriétés usuelles, on pourrait tout d'abord écrire tout couple d'entiers relatifs

$$(\alpha, \beta)\ =\ (\overline{(p,q)}, \overline{(r,s)})\ .$$

Avec les notations introduites en IV.3.9.i), on aurait encore $\alpha = p - q$ et $\beta = r - s$. On écrirait alors très naturellement

$$\alpha * \beta\ =\ (p-q) * (r-s)\ =\ (pr+qs) - (qr+ps)$$

qui est la classe $\overline{(pr+qs, ps+qr)}$. Cette démarche nous montre qu'on doit pouvoir définir la multiplication dans $\mathbb{Z}$ à partir de la multiplication dans $\mathbb{N}$ et passage aux classes.

On définit donc une loi de composition $*_Z$ sur Z (pas encore sur $\mathbb{Z}$,) par :

$$\forall (p,q) \in Z\ ,\ \forall (r,s) \in Z\ ,\ (p,q)\ *_Z\ (r,s)\ :=\ (p*r+q*s, p*s+q*r) \qquad \text{IV.3.1.2}$$

en utilisant les opérations $+$ et $*$ de $\mathbb{N}$ qui sont bien définies.

Lemme IV.3.2 *Les lois $+_Z$ et $*_Z$ définie ci-dessus sur Z sont compatibles à la relation d'équivalence $\sim$ définie en IV.1.1.2 au sens où*

$$\begin{array}{l}\forall x \in Z,\\ \forall y \in Z,\\ \forall x' \in Z,\\ \forall y' \in Z,\ \Big(\quad x \sim x' \ \wedge\ y \sim y' \quad \Rightarrow \quad x +_Z y \sim x' +_Z y' \text{ et } x *_Z y \sim x' *_Z y'\Big)\ .\end{array}$$

Preuve *:*

i) $(+)$
On a, par définition (cf. IV.3.1.1,)

$$(p,q) +_Z (r,s) \ = \ (p+r, q+s) \text{ et } (p',q') +_Z (r',s') \ = \ (p'+r', q'+s')\ .$$

Par ailleurs (cf. IV.1.1.2,) $p + q' \ = \ p' + q$ *et* $r + s' \ = \ r' + s$ *ce qui implique que* $p + q' + r + s' \ = \ p' + q + r' + s$ *ce qui s'écrit encore*

$$(p+r) \ + \ (q'+s') \ = \ (p'+r') \ + \ (q+s)$$

c'est-à-dire que

$$(p+r, q+s) \ \sim \ (p'+r', q'+s')$$

et prouve le résultat.

ii) $(*)$
On a donc : $p + q' \ = \ p' + q$ *et* $r + s' \ = \ r' + s$*. Il en résulte que*

$$\begin{array}{rcl} p*r + q*s + p'*s + q'*r & = & (p+q')*r + (q+p')*s \\ & = & (p'+q)*r + (p+q')*s \\ & = & p'*r + q's + p*s + q*r\ ; \end{array}$$

c'est-à-dire que

$$(p,q) *_Z (r,s) \ \sim \ (p',q') *_Z (r,s)\ .$$

En appliquant une fois encore ce raisonnement on obtient :

$$(p',q') *_Z (r,s) \ \sim \ (p',q') *_Z (r',s')$$

ce qui achève la preuve par transitivité de $\sim$ *.*

Proposition IV.3.3 *Il existe un unique couple de lois $(+, *)$ sur $\mathbb{Z}$ tel que la surjection canonique π définie en IV.2.2.1 soit simultanément un morphisme de $(Z, +_Z)$ dans $(\mathbb{Z}, +)$ et de $(Z, *_Z)$ dans $(\mathbb{Z}, *)$.*

***Preuve** : La compatibilité des lois $+_Z$ et $*_Z$ sur Z avec la relation déquivalence $\sim$ ayant été établie au lemme IV.3.2, le résultat découle du lemme I.6.18.*

Proposition IV.3.4 (Le groupe $(\mathbb{Z}, +)$) *Le couple $(\mathbb{Z}, +)$ est un groupe abélien (cf. III.1.1.)*

***Preuve** :*

*i) (**Associativité**)*
Il faut vérifier que la loi $+$ est associative, mais en vertu du lemme I.6.18,il suffit de vérifier que $+_Z$ est associative. Or

$$\begin{aligned}\big((p,q)+_Z(r,s)\big)+_Z(t,u) &= (p+r,q+s)+_Z(t,u)\\ &= ((p+r)+t,(q+s)+u)\\ &= (p+(r+t),q+(s+u))\\ &= (p,q)*_Z\big((r,s)+_Z(t,u)\big)\end{aligned}$$

en utilisant l'associativité de $+$ dans $\mathbb{N}$ (cf. II.1.5.i).)

*ii) (**Élément neutre**)*
On constate que

$$\forall (p,q)\in Z,\ ((p,q)+_Z(0,0)\ =\ (0,0)+_Z(p,q)\ =\ (p,q))$$

c'est-à-dire que $(0,0)$ est un élément neutre pour $+_Z$. En utilisant encore le lemme I.6.18,il s'ensuit que $\overline{(0,0)}$ est un élément neutre pour $(\mathbb{Z}, +)$.

*iii) (**Symétrique**)*
Pour tout $\overline{(p,q)}\ \in \mathbb{Z}$,

$$\overline{(p,q)}\ +\ \overline{(q,p)}\ =\ \overline{(p+q,p+q)}\ =\ \overline{(0,0)}\,;$$

c'est-à-dire que $\overline{(q,p)}$ est un opposé à droite pour $\overline{(p,q)}$ mais l'identité ci-dessus étant vraie $\forall p, \forall q$, c'est aussi un opposé à gauche.

*iv) (**Commutativité**)*
Il est encore immédiat de constater que

$$\forall (p,q)\in Z,\ \forall (r,s)\in Z,\ \big((p,q)+_Z(r,s)\ =\ (p+r,q+s)\ =\ (r+p,s+q)\ =\ (r,s)+_Z(p,q)\big)$$

en utilisant la commutativité de $+_{\mathbb{N}}$ dans $\mathbb{N}$ (cf. II.1.5.iii).) On conclut ensuite à la commutativité de $(\mathbb{Z}, +)$ une fois encore graçe au lemme I.6.18.

Les propriétés établies ci-dessus font de $(\mathbb{Z}, +)$ un groupe abélien.

Remarque IV.3.4.5 (L'opposé dans $\mathbb{Z}$) Il convient de s'arrêter un instant sur le fait que, parmi les quatre propriétés établies dans la démonstration de la proposition IV.3.4 la seule qui ne s'obtienne pas grâce à une propriété analogue de $(\mathbb{N}, +_{\mathbb{N}})$ est l'existence du symétrique (oppposé.) Rien de surprenant à cela, puisque précisément c'est le manque de symétrique dans $\mathbb{N}$ qui conduit à construire $\mathbb{Z}$ rien d'étonnant encore qu'on ne le trouve pas avant (même dans Z) sans quoi on ne se serait peut-être pas donné le mal de construire $\mathbb{Z}$.

Proposition IV.3.5 *Pour tout groupe $(G, *)$ et tout élément $x \in G$, il existe un unique morphisme de groupes $\epsilon_x : (\mathbb{Z}, +) \to (G, *)$ tel que $\epsilon_x(1) = x$.*

***Preuve** : (cf. Problème n° III, exercice A.)*

Notation IV.3.6 Avec les notations de la proposition IV.3.5, on notera usuellement

$$x^n := \epsilon_x(n) \text{ ou même } nx := \epsilon_x(n) \text{ si } G \text{ est abélien .}$$

Proposition IV.3.7 (L'anneau $(\mathbb{Z}, +, *)$) *Le triplet $(\mathbb{Z}, +, *)$ est un anneau commutatif (cf. VII.1.1.)*

***Preuve** :*

*i) (**Associativité de** $*$)*

$$\forall (p, q) \in Z,\ \forall (r, s) \in Z,\ \forall (t, u) \in Z,$$

on a :

$$\begin{aligned}
\big((p, q) *_Z (r, s)\big) *_Z (t, u) &= (pr + qs, ps + qr) *_Z (t, u) \\
&= (prt + qst + psu + qru, pst + qrt + pru + qsu) \\
&= (p(rt + su) + q(st + ru), p(st + ru) + q(rt + su) \\
&= (p, q) *_Z \big((r, s) *_Z (t, u)\big) .
\end{aligned}$$

Il suffit ensuite d'utiliser le lemme I.6.18pour assurer l'associativité de $*$ sur $\mathbb{Z}$.

ii) La démonstration des autres propriétés (élément neutre, commutativité et distributivité sur $+$) est facile et laissée en exercice. Elle se fait sur le même modèle.

Proposition IV.3.8 *Pour tout couple (p, q) d'entiers naturels,*

$$i_+(p+q) \;=\; i_+(p) \;+\; i_+(q) \quad , \quad i_-(p+q) \;=\; i_-(p) \;+\; i_-(q),$$
$$i_+(p*q) \;=\; i_+(p)*i_+(q) \quad \text{et} \quad i_-(p*q) \;=\; i_-(p)*i_+(q) \;=\; i_+(p)*i_-(q)\,.$$

Remarque IV.3.8.1 On dit que i_+ est un *morphisme* (cf. I.6.2,) pour les lois $+$ et $*$.
C'est également le cas pour i_- vis-à-vis de $+$ mais pas tout à fait pour $*$.

Preuve *: (cf. IV.6.2.)*

Notation IV.3.9 i) (**Opposé**)
On sait (cf. IV.2.5.ii)) que pour tout entier relatif α il existe un entier naturel p, tel que $\alpha = i_+(p)$ ou $i_-(p)$ c'est-à-dire que $\alpha = \overline{(p,0)}$ ou $\alpha = \overline{(0,p)}$. On a déjà convenu, (cf. IV.2.5.i),) de noter simplement p la classe $\overline{(p,0)}$. Nous venons de plus de constater (cf. IV.3.4) que $\overline{(0,p)}$ est l'opposé de $\overline{(p,0)}$ pour la loi de composition $+$ que nous venons de définir. Traditionnellement on note $-p$ l'opposé de p, et l'on retrouve ainsi la notation usuelle.
Pour résumer, pour tout entier relatif α, il existe un unique entier naturel p tel que $\alpha = p$ ou α est l'opposé dans $\mathbb{Z}$ de p vu comme entier relatif qu'on note $-p$.

ii) Même si cette opération est définie grâce à la loi $+$ et à l'opposé dans $\mathbb{Z}$ il est commode de définir une loi de *soustraction* noté $-$ sur $\mathbb{Z}$ et définie comme la *somme* avec l'opposé c'est-à-dire que pour tout couple (p, q) d'entiers relatifs,

$$p - q \;:=\; p + (-q)\,.$$

On remarque qu'alors, pour des entiers naturels p et q,

$$p - q \;=\; \overline{(p,q)}\,.$$

Proposition IV.3.10 (Règles de calcul) *On a les propriétés suivantes :*

i) Pour tout $p \in \mathbb{Z}$, $-(-p) = p$.

ii) Pour tout $p \in \mathbb{Z}$, $p \in \mathbb{Z}^+$ si et seulement si $-p \in \mathbb{Z}^-$ (cf. IV.2.5.ii).)

iii) Pour tout couple (p, q) d'entiers relatifs,

$$-(p-q) \;=\; q - p\,.$$

On établit de manière analogue les règles usuelles :

iv)
$$(-p) * q \ = \ p * (-q) \ = \ -(p * q)$$
que l'on notera simplement $-p * q$.

v)
$$(-p) * (-q) \ = \ p * q \ .$$

vi) $(-1) * p \ = \ -p$.

Preuve *: Les démonstrations de ces propriétés sont faciles et essentiellement basées sur l'unicité de l'opposé (cf. IV.6.3.)*

Proposition IV.3.11 (Intégrité) *Pour tout couple d'entiers relatifs* (p, q) $p * q \ = \ 0$ *si et seulement si* $p \ = \ 0$ *ou* $q \ = \ 0$ *c'est-à-dire que* $(\mathbb{Z}, +, *)$ *est un anneau intègre* [5]

Preuve *: On laisse le soin au lecteur de déduire cet énoncé de la proposition II.3.4.*

Corollaire IV.3.12 *Pour tout triplet* (p, q, r) *d'entiers relatifs,* $p * r \ = \ q * r$ *si et seulement si* $r = 0$ *ou* $p = q$.

Proposition IV.3.13 *Pour tout couple d'entiers relatifs* (p, q) $p * q \ = \ 1$ *si et seulement si* $(p, q) \ = \ (1, 1)$ *ou* $(p, q) \ = \ (-1, -1)$.

Preuve *:*

i) Si p *et* q *sont positifs (cf. IV.2.6,) on a* $(p, q) \ = \ (1, 1)$ *d'après la proposition II.3.7.*

ii) Si p *et* q *sont négatifs,* $-p$ *et* $-q$ *sont positifs (cf. IV.3.10.ii).) De plus,* $p*q = (-p)*(-q)$ *(cf. IV.3.8.)*

Il en résulte que $(-p, -q) \ = \ (1, 1)$ *d'après le point précédent et par conséquent que* $(p, q) \ = \ (-1, -1)$.

iii) Si p *est négatif et* q *positif,* $-p$ *est positif et* $p * q \ = \ -(-p) * q$ *est négatif d'après les propositions IV.3.8 et IV.3.10.ii). Cette situation n'est donc pas possible puisque* $1 \ = \ \overline{(1, 0)} \ \in \ \mathbb{Z}^+$.

5. Cette notion sera étudiée en plus grands détails au chapitre VII.

Définition IV.3.14 (Éléments inversibles) Les seuls éléments de $\mathbb{Z}$ qui ont un *inverse* sont donc 1 et -1. On dira que ce sont des éléments *inversibles* de $\mathbb{Z}$. On notera $\mathbb{Z}^\times := \{-1, 1\}$ l'ensemble des éléments inversibles de $\mathbb{Z}$.

Remarque IV.3.15 De manière analogue à ce qu'on a fait dans la remarque II.3.8, pour tout $p \in \mathbb{Z}$, on pose $p^0 := 1$ et

$$\forall n \in \mathbb{N},\ p^{n+1} := p * p^n\ .$$

On définit ainsi la *puissance* $n^{\text{ième}}$ de l'entier relatif p. Dans l'écriture ci-dessus, l'entier n s'appelle l'*exposant*.

Il n'est pas difficile d'établir, par récurrence sur l'exposant bien entendu (cf. II.0.PA$_3$),) que pour tout couple (n, m) d'entiers naturels,

$$p^{n+m} = p^n * p^m\ .$$

IV.4 . −Ordre sur $\mathbb{Z}$

On définit maintnant une relation d'ordre sur $\mathbb{Z}$ (cf. I.2.2.vi),) dont on va montrer qu'elle satisfait de « bonnes propriétés » relativement à l'addition $+$, la multiplication $*$ et les injection i_+ et i_-.

Définition IV.4.1 ($\leq$) On définit la relation $\leq$ sur $\mathbb{Z}$, par la formule :

$$\forall p \in \mathbb{Z},\ \forall q \in \mathbb{Z},\ \big(p \leq q \Leftrightarrow \exists r \in \mathbb{N},\ (q = p + r)\big)\ . \qquad \text{IV.4.1.1}$$

Pour tout couple (p, q) d'entiers relatifs, si $p \leq q$, on dira que p est *inférieur ou égal à* q.

Proposition IV.4.2 (Ordre) *La relation $\leq$ définie ci-dessus est une relation d'ordre totale sur $\mathbb{Z}$ (cf. I.2.2.vi).)*

***Preuve** : Le fait que $\leq$ soit réflexive et transitive procède d'arguments semblables à ceux utilisés pour les propriétés analogues de la relation $\leq$ sur $\mathbb{N}$ (cf. II.2.2.)*

Pour tout couple (p, q) d'entiers relatifs, si $p \leq q$, et $q \leq p$, on a : $q - p \in \mathbb{Z}^+$ et $p - q \in \mathbb{Z}^+$. Or $p - q \in \mathbb{Z}^+$ équivaut (cf. IV.3.10.ii)) à $q - p \in \mathbb{Z}^-$. On a donc

$$q - p \in \mathbb{Z}^+ \cap \mathbb{Z}^-$$

ce qui implique (cf. IV.2.5.iii)) que $q - p = 0$ c'est-à-dire que $p = q$. La relation $\leq$ est donc antisymétrique et c'est donc une relation d'ordre.

Le fait qu'elle est totale c'est-à-dire qu'on puisse toujours comparer deux éléments, est une conséquence de IV.2.5.ii).

Remarque IV.4.3 On peut définir une relation $\geq$ de manière évidente sur $\mathbb{Z}$ qui est aussi une relation d'ordre ainsi que des relations $<$ et $>$ qui ne sont pas des relations d'ordre (cf. II.2.3.)

Proposition IV.4.4 *Pour tout couple d'entiers naturels (p, q), $p \leq_{\mathbb{N}} q$ au sens de la relation d'ordre sur $\mathbb{N}$ si et seulement si $i_+(p) \leq_{\mathbb{Z}} i_+(q)$ (cf. IV.2.4.1) que l'on écrira bien entendu $p \leq q$ au sens de la relation d'ordre sur $\mathbb{Z}$. Autrement dit, i_+ est un morphisme pour les relations d'ordre $\leq$ sur $\mathbb{N}$ et $\mathbb{Z}$ c'est-à-dire encore une application croissante (cf. I.2.10.)*

On pourrait encore dire que la relation d'ordre sur $\mathbb{Z}$ « prolonge » la relation d'ordre sur $\mathbb{N}$.

Proposition IV.4.5 (Propriétés de $\leq$) *i) **(Cône positif)***
Pour tout $p \in \mathbb{Z}^-$ et tout $q \in \mathbb{Z}^+$, $p \leq q$.

*ii) **(Addition et ordre)***
Pour tout quadruplet d'entiers relatifs (p, q, r, s) $p \leq q$ et $r \leq s$, implique $p + r \leq q + s$.

*iii) **(Multiplication et ordre)***
Pour tout triplet (p, q, r) d'entiers relatifs, si $p \leq q$ et $r \geq 0$, alors $r * p \leq r * q$.

Remarque IV.4.6 On laisse le soin au lecteur d'établir toutes les variantes usuelles de l'énoncé ci-dessus.

Proposition IV.4.7 *Toute partie non vide majorée (resp. minorée) de $\mathbb{Z}$ possède un plus grand élément (resp. un plus petit élément.)*

Le plus grand élément est le plus petit des majorants, tandis que le plus petit élément est le plus grand des minorants. Ceci implique, en particulier, l'unicité du plus grand (resp. du plus petit élément.)

***Preuve** : On ne démontre que partiellement cette proposition, le reste de l'argument ayant la même forme.*

Étant donnée une partie non vide et majorée P de $\mathbb{Z}$,

i) si $Q := P \cap \mathbb{Z}^+ \neq \emptyset$, Q est une partie non vide majorée de $\mathbb{N}$ et possède donc un plus grand élément (cf. II.2.10.) Il est facile de voir que ce plus grand élément est encore un plus grand élément pour P.

ii) Si $P \cap \mathbb{Z}^+ = \emptyset$, il découle de la proposition IV.3.10.ii) que $P' := \{-p\ ,\ p \in P\}$, est une partie de $\mathbb{Z}^+ = \mathbb{N}$. Elle possède donc un plus petit élément ℓ d'après la proposition II.2.9. Reste à vérifier, ce qui est élémentaire, que $-\ell$ est un plus grand élément pour P.

Proposition IV.4.8 (Parties finies) *i) Une partie de $\mathbb{Z}$ est soit finie (cf. II.4.1,) soit dénombrable (cf. II.4.6.)*

ii) Une partie non vide de $\mathbb{Z}$ est finie si et seulement si elle est à la fois majorée et minorée, si et seulement si elle admet simultanément un plus grand et un plus petit élément.

Définition IV.4.9 (Valeur absolue) La proposition IV.3.10.ii) permet de définir la *valeur absolue*
d'un entier relatif de la manière suivante :

i) si $p \in \mathbb{Z}^+$, on appelle valeur absolue de p et on note $|p|$ l'entier relatif p lui-même ;

ii) si $p \in \mathbb{Z}^-$, la valeur absolue $|p|$ de p est l'entier $-p \in \mathbb{Z}^+$.

De manière équivalente, on peut dire que la valeur absolue d'un entier relatif p est le plus grand des deux nombres p et $-p$:

$$|p| = \max(p, -p) .$$

La valeur absolue est donc une application de $\mathbb{Z}$ dans $\mathbb{N}$.

Proposition IV.4.10 (Propriétés de la valeur absolue) *La valeur absolue sur $\mathbb{Z}$ a les propriétés suivantes :*

i) $|0| = 0$;

ii)
$$\forall p \in \mathbb{Z},\ p \leq |p| ;$$

iii)
$$\forall p \in \mathbb{Z},\ \forall q \in \mathbb{Z},\ |p * q| = |p| * |q| ;$$

iv)
$$\forall p \in \mathbb{Z},\ |-p| = |p| ;$$

v)
$$\forall p \in \mathbb{Z},\ \forall q \in \mathbb{Z},\ ||p| - |q|| \leq |p+q| \leq |p| + |q| .$$

IV.5 . −Le théorème de la division euclidienne

Proposition IV.5.1

$$\forall p \in \mathbb{Z},\ \forall q \in \mathbb{Z},\ \big(p|q \text{ et } q \neq 0 \ \Rightarrow\ |p| \leq |q|\big)\ .$$

Preuve *:*

$$\begin{array}{lr} \forall p \in \mathbb{Z},\ \forall q \in \mathbb{Z}, & p|q \ \text{ et } \ q \neq 0 \\ \Rightarrow & \exists r \in \mathbb{Z},\ q = p * r \ \text{ et } \ r \neq 0 \\ \Rightarrow & \exists r \in \mathbb{Z},\ |r| * |p| = |q| \ \text{ et } \ r \neq 0 \end{array}$$

Or

$$r \neq 0 \ \Rightarrow\ |r| \neq 0 \ \Rightarrow\ 1 \leq |r| \ \Rightarrow\ |p| * 1 \ \leq\ |p| * |r| \ =\ |q|$$

en utilisant la proposition II.3.6.

Théorème IV.5.2 (de la division euclidienne) *Pour tout couple d'entiers relatifs* (a, b), $b \neq 0$, *il existe un unique couple d'entiers relatifs* (q, r) *tel que :*

$$a \ =\ b * q \ +\ r \text{ et } 0 \ \leq\ r \ <\ |b|\ . \qquad \textit{IV.5.2.1}$$

Preuve *:*

i) ***(Existence)***
Montrons d'abord l'existence du couple (q, r). *Considérons pour cela l'ensemble*

$$K \ :=\ \{a - b * k\ ,\ k \in \mathbb{Z}\}\ .$$

Lemme i).1

$$K \ \cap\ \mathbb{Z}^+ \ \neq\ \emptyset\ .$$

Preuve *: Remarquons que* K *n'est pas vide puisque* $a \ =\ a - b * 0 \ \in\ K$. *Si* $K \cap \mathbb{Z}^+$ *était vide, d'après la proposition IV.2.5.ii), pour tout* $m \ \in\ K$, $m \leq 0$. *L'ensemble* K *serait donc une partie non vide majorée de* $\mathbb{Z}$ *et posséderait donc, d'après la proposition IV.4.7, un plus grand élément* $a - b * k_0$.

Cependant, si $b > 0$,

$$a - b * (k_0 - 1) \ =\ a - b * k_0 + b \ >\ a - b * k_0$$

ce qui est contradictoire.

Si $b < 0$,

$$a - b * (k_0 + 1) \ =\ a - b * k_0 - b \ >\ a - b * k_0$$

ce qui est encore contradictoire.

Il en résulte donc que $K \cap \mathbb{Z}^+$ possède, d'après la proposition II.2.9, un plus petit élément $a - b * q$.

Reste finalement à montrer que $a - b * q < |b|$. Or $a - b * q \geq |b|$ entraîne :

— si $b > 0$, $|b| = b$ et $a - b * q \geq b$ implique $a - b * (q + 1) \geq 0$. Par ailleurs, $a - b * (q + 1) < a - b * q$ ce qui contredit la minimalité de $a - b * q$ dans $K \cap \mathbb{Z}^+$.

— Le cas $b < 0$ est laissé en exercice.

*ii) (**Unicité**)*

Supposons maintenant qu'il existe deux couples (q, r) et (q', r') satisfaisant aux conditions IV.5.2.1 du théorème. On a alors $b * q + r = b * q' + r'$ ce qui implique

$$r' - r = b * (q - q')$$

c'est-à-dire que b divise $r' - r$ (cf. VII.5.1.) Par ailleurs, on a $0 \leq r < |b|$ et $0 \leq r' < |b|$ ce qui implique que $-|b| < r' - r < |b|$. Ceci équivaut à $|r' - r| < |b|$. On en déduit, en appliquant le résultat IV.5.1 que $r' - r = 0$. Il s'ensuit que $b * (q - q') = 0$ mais comme $b \neq 0$, d'après la proposition IV.3.11, $q - q' = 0$ ce qui achève de prouver l'unicité du couple (q, r).

Définition IV.5.3 Avec les notations du théorème IV.5.2, on adopte en général la terminologie usuelle suivante : a est le *dividende* b le *diviseur* q un *quotient* et r un *reste*.

Remarque IV.5.4 a) On peut constater que l'énoncé IV.5.2.1 est plus précis que celui correspondant IX.7.1.1 définissant un stathme euclidien. Cet énoncé conduit à l'unicité du couple (q, r) qui n'est pas exigée dans la définition IX.7.1. Nous constaterons cependant, qu'un tel énoncé d'unicité n'est pas requis pour établir la proposition IX.7.4 dont le corollaire IV.5.5 est l'équivalent pour l'anneau $\mathbb{Z}$.

b) On laisse le soin au lecteur de justifier que, si dans la division euclidienne de a par b, a et b sont *positifs* q l'est aussi.

Corollaire IV.5.5 (Sous-groupes de $(\mathbb{Z}, +)$) *Pour toute partie $H \subset \mathbb{Z}$, H est un sous-groupe (cf. III.3.1,) si et seulement s'il existe $d \in \mathbb{Z}$ tel que*

$$H = d\mathbb{Z} := \{d * k \,;\, k \in \mathbb{Z}\} .$$

***Preuve** : (cf. TD n° IV, exercice A.)*

— Si $H = \{0\}$,

$$H = 0\mathbb{Z} = \{0z \,,\, z \in \mathbb{Z}\} .$$

— *Si $H \neq \{0\}$ il existe un entier relatif $x \neq 0$ appartenant à H. Soit $x \in \mathbb{N}^*$ soit $-x$ qui appartient également à H puisque H est un sous-groupe de $\mathbb{Z}$, appartient à $\mathbb{N}^*$ c'est-à-dire que*

$$H \cap \mathbb{N}^* \neq \emptyset .$$

Notons d le plus petit élément de $H \cap \mathbb{N}^*$ qui existe en vertu de la proposition II.2.9.

— *Remarquons tout d'abord que*

$$d\mathbb{Z} = \{dz , z \in \mathbb{Z}\} \subset H .$$

En effet, $d * 0 = 0 \in H$. Pour tout entier naturel n, si $dn \in H$, $d * (n+1) = d * n + d \in H$. Il en résulte (cf. II.0.PA$_3$),) que $d\mathbb{N}^* \in H$. Par ailleurs, pour tout entier relatif n, $dn \in H$ si et seulement si

$$-dn = d * (-n) \in H .$$

Ceci, combiné avec ce qui précède montre que

$$d\mathbb{Z} \subset H .$$

— *Enfin, pour tout $n \in H$, effectuons la division euclidienne (cf. IX.7.1,) de n par $d > 0$. Il existe donc des entiers q et r tels que*

$$n = dq + r \text{ et } 0 \leq r < d .$$

Or $dq \in H$ d'après le point précédent et $n \in H$ par hypothèse, ce qui implique, H étant un sous-groupe, que

$$r = n - dq \in H .$$

L'encadrement de r et la minimalité de d, impliquent que $r = 0$ c'est-à-dire que $n = dq$. On en conclut que

$$H \subset d\mathbb{Z} .$$

Il peut être utile de ne s'intéresser à $\mathbb{Z}$ qu'en tant que groupe abélien, *i.e.*d'oublier la loi $*$ pour ne considérer que les propriétés de la loi $+$. Le théorème IX.7.4 donne d'utiles informations dans ce contexte, grace au fait (voir le lemme IV.5.6) qu'un idéal de l'anneau $(\mathbb{Z}, +, *)$ est exactement un sous-groupe du groupe abélien $(\mathbb{Z}, +)$ ce qui permet de donner le corollaire IV.5.5 :

Lemme IV.5.6 *Une partie $H \subset \mathbb{Z}$ est un sous-groupe du groupe $(\mathbb{Z}, +)$ si et seulement si c'est un idéal de l'anneau $(\mathbb{Z}, +, *)$.*

Preuve *: On peut utiliser la caractérisation des sous-groupes (cf. III.3.4 :) si H est un sous-groupe de $\mathbb{Z}$, H est non vide. Il est presqu'immédiat, en outre, de montrer que pour tout $(x, y) \in H \times H$ et tout $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ $m * x + n * y \in H$. La réciproque est encore plus immédiate et laissée en exercice.*

Corollaire IV.5.7 (Structure des sous-groupes de $(\mathbb{Z},+)$) *Pour toute partie $H \subset \mathbb{Z}$, H est un sous-groupe (cf. III.3.1,) si et seulement si H est un idéal de $\mathbb{Z}$ (cf. VII.4.1,) si et seulement si il existe $d \in \mathbb{Z}$ tel que*

$$H = d\mathbb{Z} := \{d * k \,;\, k \in \mathbb{Z}\} .$$

Corollaire IV.5.8 (Notation de position) *Un entier naturel $b > 1$ étant fixé, pour tout entier relatif $a \neq 0$, il existe un unique entier naturel d un unique élément $\epsilon \in \mathbb{Z}^\times = \{-1;1\}$ et un unique $d+1$-uplet $r_{i\ ,0\leq i\leq d}$ tel que*

$$a = \epsilon \sum_{i=0}^{d} r_i b^i \,; \qquad \textit{IV.5.8.1}$$

$$\forall 0 \leq i \leq d,\ 0 \leq r_i \leq b \,; \qquad \textit{IV.5.8.2}$$

$$r_d \neq 0 . \qquad \textit{IV.5.8.3}$$

Preuve *: (cf. TD n° IV, exercice D.)*

*i) (**Existence**)*

On va tout d'abord chercher à prouver l'existence des entiers d et $r_{i\ ,0\leq i\leq d}$.

a) ($a \geq 0$)

Supposons d'abord que $a > 0$. Notons A l'ensemble des entiers naturels $p > 0$ tels que pour tout $q \leq p$, il existe un entiers d_q et des entiers $r_{q,i\ ,0\,\leq\, i\,\leq\, d_q}$ tels que

$$q = \sum_{i=0}^{d_q} r_{q,i} b^i \text{ avec } 0 \leq r_{q,i} < b \text{ et } r_{q,d_q} \neq 0 .$$

L'entier 1 appartient à A puisque $1 = 1 + 0 * b$.

Pour $p \in A$, l'ensemble

$$B_p := \{b^k \,,\ k \in \mathbb{N} \,;\, b^k \leq p+1\}$$

est non vide puisque $b^0 = 1 \leq p+1$ et clairement majoré par $p+1$. Il admet donc un plus grand élément (cf. IV.4.7,) b^d. Comme $b > 1$, $b^{d+1} = b * b^d > b^d$ et par maximalité de b^d on a donc

$$b^d \leq p+1 < b^{d+1} .$$

Notons r_d le quotient de la division euclidienne de $p+1$ par b^d et ρ son reste. On a donc,

$$0 \leq \rho < b^d .$$

Ceci implique, en particulier, que $r_d b^d \ \leq\ p+1 \ <\ b^{d+1}$ *ce qui implique que* $r_d < b$. *Par ailleurs, en vertu de la remarque IV.5.4.b), on a également* $r_d \geq 0$. *Cependant,* $r_d = 0$ *signifierait que* $\rho \ =\ p+1 \ \geq b^d$ *ce qui est contradictoire. Il en résulte que*

$$0 \ <\ r_d \ <\ b\,.$$

Finalement $\rho < b^d$, *implique que* $\rho < p+1$ *c'est-à-dire que* $\rho \leq p$. *Grâce à l'hypothèse de récurrence faite sur* p, *on sait qu'il existe un entier* d' *et des entiers* $r'_{i\ ,0\ \leq\ i\ \leq\ d'}$ *tels que*

$$\rho \ =\ \sum_{i=0}^{d'} r'_i b^i$$

avec $r'_{d'} \neq 0$. *Ce dernier point a en particulier pour conséquence, comme* $\rho < b^d$, *que* $d' < d$. *On a donc finalement que*

$$p+1 \ =\ r_d b^d \ +\ \sum_{i=0}^{d'} r'_i b^i$$

c'est-à-dire, sous l'hypothèse que p *appartient à* A, $p+1$ *appartient à* A. *Autrement dit* A *satisfait au principe de récurrence II.0.PA*$_3$*) et par conséquent,* A *est l'ensemble* $[1, +\infty[$ *des entiers supérieurs ou égaux à* 1.

b) ($a \leq 0$)

Si a *est négatif, on peut appliquer le résultat précédent à* $-a$ *et l'on prendra* $\epsilon = -1$.

ii) (***Unicité***)

On va maintenant montrer l'unicité de l'écriture précédente. Supposons que pour un entier relatif $a \ \neq\ 0$, *il existe*

$$\epsilon\ ,\ \epsilon'\ ,\ d\ ,\ d'\ ,\ r_{i\ ,0\leq i\leq d}\ \text{et}\ r'_{i\ ,0\ \leq\ i\ \leq\ d'}$$

tels que

$$a \ =\ \epsilon \sum_{i=0}^{d} r_i b^i \ =\ \epsilon' \sum_{i=0}^{d'} r'_i b^i\ .$$

a) Il est tout d'abord clair que ceci implique que $\epsilon \ =\ \epsilon'$.

b) Si $d \neq d'$, *on peut par exemple supposer que* $d > d'$. *Or on montrera en exercice que*

$$\sum_{i=0}^{d'} r'_i b^i < b^{d'+1} .$$

Or $d > d'$ *implique que* $d \geq d' + 1$ *ce qui implique encore, comme* $r_d \neq 0$ *par hypothèse, que*

$$r_d b^d \geq b^{d'+1} > \sum_{i=0}^{d'} r'_i b^i$$

ce qui est contradictoire. On a donc $d = d'$.

c) On a par conséquent,

$$\sum_{i=0}^{d} r_i b^i = \sum_{i=0}^{d} r'_i b^i$$

ce qui implique que

$$\begin{aligned} r_0 - r'_0 &= \sum_{i=1}^{d} (r'_i - r_i) b^i \\ &= b * \sum_{i=1}^{d} (r'_i - r_i) b^{i-1} \end{aligned}$$

c'est-à-dire que $b | r_0 - r'_0$. *Ceci implique, par un argument déjà donné dans la preuve du théorème IV.5.2 que* $r_0 = r'_0$. *On commence ainsi un raisonnement par récurrence sur* i *compris entre* 0 *et* d, *permettant de montrer que* $r_i = r'_i$ *pour tout* $0 \leq i \leq d$. *On laisse le lecteur terminer cette preuve.*

Remarque IV.5.9 Ce corollaire justifie la notation de position c'est-à-dire qu'on peut écrire tout entier relatif en base b (usuellement en base 10 ou $2,$) comme somme de puissances de b avec des coefficients compris entre 0 et b et en utilisant également un signe $+$ ou $-$.

IV.6 . −Exercices

Exercice IV.6.1 [] Faire la preuve de la proposition IV.1.2.

Exercice IV.6.2 [] Faire la preuve de la proposition IV.3.8.

Exercice IV.6.3 [] Faire la preuve de la proposition IV.3.10.

V . −Actions de groupes, groupes quotients

V.1 . −Actions de groupe

Pour tout ensemble E, on rappelle qu'on note $\mathcal{S}(E)$ le groupe des bijections de E défini en III.1.2.c) et pour toute bijection $f : E \to F$,

$$\mathcal{S}(f) : \mathcal{S}(E) \to \mathcal{S}(F)$$

l'isomorphisme de groupes qui s'en déduit (cf. III.2.6.)

Dans toute cette section (V,) $(G, *)$ est un groupe dont on notera e l'élément neutre.

Définition V.1.1 (Action de groupe) Étant donné un ensemble E et un groupe $(G, *)$ on dit que G *agit sur* (ou *opère sur*) E ou que E est muni d'une *action* de G, s'il existe un morphisme de groupe (cf. III.2.1,)

$$\phi : (G, *) \to (\mathcal{S}(E), \circ) .$$

On dira aussi que E est un G-*ensemble*.

Remarque V.1.2 Si l'on a une action $\phi : (G, *) \to (\mathcal{S}(E), \circ)$, cela signifie que

$$\forall g \in G, \forall h \in G, \phi(g * h) = \phi(g) \circ \phi(h)$$

et cela a pour conséquences que $\phi(e_G) = \mathrm{Id}_E$ (cf. III.2.9.i) ;) et $\forall g \in G, \phi(g^{-1}) = \phi(g)^{-1}$ (cf. III.2.9.ii).)

Notation V.1.3 Étant donnés un groupe G agissant sur un ensemble E il est usuel de noter

$$\forall g \in G, \forall x \in E, g \cdot x := \phi(g)(x) .$$

On a alors

$$\forall x \in E, e_G \cdot x = x \text{ et } \forall g \in G, \forall h \in G, (g * h) \cdot x = g \cdot (h \cdot x) .$$

Exemple V.1.4 a) Pour tout ensemble E, le groupe $\mathcal{S}(E)$ agit évidemment sur E, dans la mesure où $\mathrm{Id}_{\mathcal{S}(E)} : \mathcal{S}(E) \to \mathcal{S}(E)$ est un morphisme de groupes.

b) Étant donnés un groupe G agissant sur un ensemble E par $\phi : G \to \mathcal{S}(E)$ tout morphisme $f : H \to G$ définit une action $\phi \circ f$ de H sur E. En particulier si G agit sur E, tout sous-groupe H de G agit naturellement sur E à travers l'injection naturelle $H \hookrightarrow G$.

c) Si $f : E \to F$ est une bijection d'un ensemble E sur un ensemble F, l'isomorphisme

$$\mathcal{S}(f) : \mathcal{S}(E) \to \mathcal{S}(F)$$

défini en III.2.6, associe à toute action $\phi : G \to \mathcal{S}(E)$ d'un groupe G sur E, une action

$$\mathcal{S}(f) \circ \phi : G \to \mathcal{S}(F)$$

et l'on a de manière évidente :

$$\forall (g, x) \in G \times E,\ f(g \cdot x) = g \cdot f(x)\ .$$

Les exemples ci-dessus sont en quelque sorte tautologiques et ne mettent pas en évidence daction de groupes arbitraires (autre que le groupe $\mathcal{S}(E)$.) Or un des intérêts de la notion d'action de groupe est précisément de permettre l'étude d(d'un certain nombre de propriétés de groupes arbitraires à travers la manière dont ils peuvent agir. Donnons donc quelques exemples plus concrets qui sont cependant très loins d'épuiser la question :

Exemple V.1.5 a) Pour un $\mathbb{K}$-espace vectoriel V, le groupe linéaire $\mathrm{GL}(V)$ *i.e.* le groupe des applications linéaires bijectives de V dans lui-même agit sur V, puisque $\mathrm{GL}(V)$ est un sous-groupe de $\mathcal{S}(V)$.

Le groupe $\mathbb{K}^\times$ des éléments inversibles de $\mathbb{K}$ muni de la multiplication s'identifie au sous-groupe de $\mathrm{GL}(V)$ formé des homothéties bijectives et agit donc également sur V.

b) Dans le cas où V est un $\mathbb{K}$-espace vectoriel muni d'une structure euclidienne, il résulte de a) que les sous-groupes $\mathcal{O}(V)$ et $\mathcal{SO}(V)$ de $\mathrm{GL}(V)$ agissent également sur V. Il peut être plus intéressant encore de constater qu'ils agissent sur des parties remarquables de V (voir TD n° V, exercice B.)

c) Étant donné un $\mathbb{K}$-espace affine A, le groupe des translations, (resp. le groupe des isométries si A est euclidien) agit sur A [6].

Définition V.1.6 (Applications invariantes/G-morphismes) Étant donnés un groupe G et deux ensembles E et F munis d'actions

$$\phi_E(\text{resp. } \phi_F) : G \to \mathcal{S}(E)(\text{resp. } \mathcal{S}(F))$$

de G, on dit qu'une application $f : E \to F$ de E dans F est *invariante* si

$$\forall g \in G,\ f \circ \phi_E(g) = \phi_F(g) \circ f$$

ce qui s'écrit encore

$$\forall (g, x) \in G \times E,\ f(g \cdot_E x) = g \cdot_F f(x)\ .$$

Le terme de *morphisme de G-ensembles* est synonyme d'application invariante.

6. On conseille de reconsidérer cet exemple à la lumière du cours de géométrie.

Exemple V.1.7 On a vu un exemple d'application invariante en V.1.4.c) mais c'est loin d'être le plus intéressant.

Toute application linéaire $V_1 \to V_2$ est invariante pour l'action par homothétie (cf. V.1.5.a).)

Proposition V.1.8 *Étant donnés un groupe G agissant sur un ensemble E, la relation $\sim$ définie sur E par*

$$\forall x \in E,\ \forall y \in E,\ x \sim y \Leftrightarrow \exists g \in G,\ y = g \cdot x$$

est une relation d'équivalence (cf. I.2.2.v),) sur E.

Preuve *: (cf. V.7.1.)*

Définition V.1.9 (Orbite) Étant donnés un groupe G agissant sur un ensemble E, *i.e.* un G-ensemble E :

i) (**orbite**)

Les classes déquivalence pour la relation définie par la proposition V.1.8 sont appelées *orbites*. Plus précisément pour tout $x \in E$, la classe de x est appelée *orbite de x sous l'action* de G. On la note usuellement $O_G(x)$ (ou simplement $O(x)$ s'il n'en résulte aucune ambiguîté) et l'on a :

$$O(x) = \{g \cdot x\ ,\ g \in G\}\ .$$

ii) (**point fixe**)

Pour $x \in E$, de manière équivalente, $O(x) = \{x\}$, $O(x)$ est un singleton, $\forall g \in G,\ g \cdot x = x$. On dit alors que x est un *point fixe pour l'action* de G sur E. On dit aussi que l'orbite de x est *triviale*.

Exemple V.1.10 Pour laction de $\mathbb{K}^\times$ sur V par homothétie (cf. V.1.5.a),) les orbites sont, d'une part l'origine 0_V de V et d'autre part les droites de V privées de l'origine.

Lemme V.1.11 *Étant donné un G-ensemble E, les assertions suivantes sont équivalentes :*

a) Il y a une seule orbite sous l'action de G.

b)

$$\forall x \in E,\ O_G(x) = E\ .$$

c)

$$\forall (x, y) \in E \times E,\ \exists g \in G,\ y = g \cdot x\ .$$

Preuve *: Voir l'exercice V.7.2.*

Définition V.1.12 (Action transitive) Si un G-ensemble E vérifie les assertions équivalentes du lemme V.1.11, on dit que l'action de G sur E est *transitive* ou encore que G agit/opère *transitivement* sur E.

Exemple V.1.13 Si E est un G-ensemble, pour tout $x \in E$, G agit transitivement sur l'orbite $O(x)$ de x.

Proposition V.1.14 (Stabilisateur d'un élément) *Étant donnée une action d'un groupe G sur un ensemble E, pour tout $x \in E$, l'ensemble :*

$$\mathrm{Stab}_G(x) := \{g \in G \,;\, g \cdot x = x\} \qquad \text{V.1.14.1}$$

est un sous-groupe de G.

***Preuve** : C'est un exercice(cf. V.7.3 et TD n° V, exercice E, question 3), a) dans le cas particulier de l'action par conjugaison.)*

Définition V.1.15 (Stabilisateur) Étant donnée une action d'un groupe G sur un ensemble E, pour tout $x \in E$, le sous-groupe $\mathrm{Stab}_G(x)$ défini en V.1.14.1 est appelé *stabilisateur* de x.

Proposition V.1.16 *Étant donné un G-ensemble E, pour tout $x \in E$, notons $\mathrm{Stab}_G(x)$ le stabilisateur de x pour l'action de G, et*

$$p : G \to O(x) \,,\; g \mapsto g \cdot x \,.$$

Alors :

i) L'ensemble des $p^{-1}(\{y\})$ pour $y \in O(x)$, forme une partition de G.

***Preuve** : Voir l'exercice V.7.4.*

ii) Pour tout $g \in G$,

$$p^{-1}(\{g \cdot x\}) = g * \mathrm{Stab}_G(x) = \{g * h \,,\; h \in \mathrm{Stab}_G(x)\} \,.$$

***Preuve** : Pour tout $g \in G$ et tout $h \in p^{-1}(\{g \cdot x\})$ si et seulement si $p(h) = g \cdot x$ i.e.*

$$h \cdot x = g \cdot x \Leftrightarrow (g^{-1} * h) \cdot x = x \Leftrightarrow g^{-1} * h \in \mathrm{Stab}_G(x) \Leftrightarrow h \in g * \mathrm{Stab}_G(x) \,.$$

Corollaire V.1.17 *Sous les hypothèses de la proposition V.1.16, si l'on suppose de plus que G est un groupe fini alors :*

$$\forall x \in E,\ \#(G) \ = \ \#(\mathrm{Stab}_G(x)) \cdot \#(O(x)) \ .$$

Preuve *: C'est une conséquence immédiate de la proposition V.1.16.*

Proposition V.1.18 *Soit E un G-ensemble. Pour tout $x \in E$ et tout $g \in G$,*

$$\mathrm{Stab}_G(g \cdot x) \ = \ g \ * \ \mathrm{Stab}_G(X) \ * \ g^{-1} \ := \ \{g * h * g^{-1} \ , \ h \ \in \ \mathrm{Stab}_G(x)\} \ .$$

Preuve *: (cf. V.7.5.)*

Pour tout $(x, g, h) \in E \times G \times G$, $h \in \mathrm{Stab}_G(g \cdot x)$ si et seulement si $h \cdot (g \cdot x) = g \cdot x$ si et seulement si

$$g^{-1} \cdot (h \cdot (g \cdot x)) \ = \ x \ \Leftrightarrow \ (g^{-1} * h * g) \ \cdot x \ = \ x \ \Leftrightarrow \ g^{-1} * h * g \ \in \ \mathrm{Stab}_G(x)$$

c'est-à-dire qu'il existe $k \in \mathrm{Stab}_G(x)$ tel que $g^{-1} * h * g = k$ i.e. $h = g * k * g^{-1}$ c'est-à-dire finalement que

$$h \ \in \ g * \mathrm{Stab}_G(x) * g^{-1} \ .$$

Les définitions qui suivent sont données pour compléter la présentation des actions de groupe mais il est probable qu'on n'en fera assez peu usage.

Définition V.1.19 Soit E un G-ensemble.

i) (**Action libre**)

On dit que l'action de G sur E est *libre* (ou encore que G agit/opère *librement*) si pour tout $x \in E$,

$$\mathrm{Stab}_G(x) \ = \ \{e\} \ .$$

ii) (**Action fidèle**)

On dit que l'action de G sur E est *fidèle* (ou encore que G agit/opère *fidèlement*) si l'intersection de touts les stabilisateurs des éléments de E est $\{e\}$ ce qui équivaut à dire que le morphisme $G \to \mathcal{S}(E)$ définissant l'action est injectif.

iii) (**ACtion simplement transitive**)

Laction est *simplement transitive* si elle est libre et transitive (cf. V.1.12.)

V.2 . −Action par translation à gauche

Dans ce paragraphe $(G, *)$ est un groupe (noté seulement G si aucune confusion n'en résulte) et l'on note e son élément neutre.

Lemme V.2.1 *Soit $(G, *)$ un groupe. L'application de $G \times G$ dans G définie par $g \cdot x := g * x$ est une action de G sur lui-même.*

Preuve *: On constate d'abord que pour tout $g \in G$, l'application de G dans lui-même donée par $x \mapsto g * x$ est bien une bijection de G dans lui-même (i.e. un élément de $\mathcal{S}(G)$,) de bijection réciproque $x \mapsto g^{-1} * x$.*

En outre

$$\forall (g, h) \in G \times G,\ (g * h) \cdot x = (g * h) * x = g * (h * x) = g \cdot (h * x) = g \cdot (h \cdot x)$$

ce qui assure qu'on a bien une action.

Définition V.2.2 (Translation à gauche) Étant donné un groupe G, l'action de G sur lui-même définie par le lemme V.2.1 est appelée *action par translation à gauche*.

Il résulte de V.1.4.b) que tout sous-groupe H de G agit encore sur G à travers l'action de G sur lui-même par translation à gauche. Cette action de H sur G est encore appelée *action par translation à gauche de H sur G*.

Remarque V.2.3 Si $P \subset G$, est une partie de G (*i.e.*

$$P \in \mathcal{P}(G) \text{ pas nécessairement un sous-groupe },\ )$$

notons

$$\forall g \in G,\ g * P := \{g * x\ ,\ x \in P\}\ .$$

Alors l'application $G \times \mathcal{P}(G) \to \mathcal{P}(G)$ définie par $(g, P) \mapsto g \cdot P := g * P$ est une action de G sur l'ensemble de ses parties, qu'on apellera encore action par translation à gauche. Elle induit encore une action par translation à gauche de tout sous-groupe H de G sur $\mathcal{P}(G)$.

Notation V.2.4 On a vu en V.1.8 que, dès que E est un G-ensemble, l'action de G sur E induit une relation d'équivalence $\sim$. Dans le cas de l'action de H sur G par translation à gauche on notera parfois $\sim_{H,g}$ cette relation. Elle prend une forme suffisamment particulière dans ce cas pour qu'on l'explicite :

$$\begin{array}{lrcl}
\forall (x, y) \in G \times G, & x & \sim_{H,g} & y \\
\Leftrightarrow & \exists h \in H,\ y & = & h \cdot x \\
\Leftrightarrow & y & = & h * x \\
\Leftrightarrow & y * x^{-1} & \in & H \\
\Leftrightarrow & x * y^{-1} & \in & H\ .
\end{array}$$

Remarque V.2.5 Soit $(G, *)$ un groupe.

i) L'application de $G \times G$ dans G définie par $g \cdot x \ := \ x * g$ est une *action à droite* de G sur lui-même. Elle est appelée *action par translation à droite*.

La notion d'action à droite ne sera pass développée ni utilisée dans ce qui suit. Disons simplement que la formule

$$(g * h) \cdot x \ = \ g \cdot (h \cdot x)$$

qui caractérise les actions à gauches est remplacée par

$$(g * h) \cdot x \ = \ h \cdot (g \cdot x) \ .$$

ii) Il résulte de V.1.4.b) que tout sous-groupe H de G agit encore sur G à travers l'action de G sur lui-même par translation à droite. Cette action de H sur G est encore appelée *action par translation à droite de H sur G*.

iii) Si $P \ \subset \ G$, est une partie de G (*i.e.* $P \ \in \ \mathcal{P}(G)$ pas nécessairement un sous-groupe,) notons

$$\forall g \in G, \ P * g \ := \ \{x * g \ , \ x \ \in \ P\} \ .$$

Alors l'application $G \times \mathcal{P}(G) \ \to \ \mathcal{P}(G)$ définie par $(g, P) \ \mapsto \ g \cdot P \ := \ P * g$ est une action à droite de G sur l'ensemble de ses parties, qu'on apellera encore action par translation à droite. Elle induit encore une action par translation à droite de tout sous-groupe H de G sur $\mathcal{P}(G)$.

iv) On a vu en V.1.8 que, dès que E est un G-ensemble, l'action de G sur E induit une relation d'équivalence $\sim$. Dans le cas de l'action de H sur G par translation à droite on notera parfois $\sim_{H,d}$ cette relation. Elle prend une forme suffisamment particulière dans ce cas pour qu'on l'explicite :

$$\begin{array}{lrcl}
\forall (x, y) \in G \times G, & x & \sim_{H,d} & y \\
\Leftrightarrow & \exists h \ \in \ H, \ y & = & h \cdot x \\
\Leftrightarrow & y & = & x * h \\
\Leftrightarrow & x^{-1} * y & \in & H \\
\Leftrightarrow & y^{-1} * x & \in & H \ .
\end{array}$$

Définition V.2.6 (Classes à gauche/droite) Étant donnés un groupe G et un sous-groupe H de G, les classes d'équivalence pour la relation $\sim_{H,g}$, (cf. V.2.4,) qui sont aussi les orbites (cf. V.1.9.i),) pour l'action par translation à gauche, sont appelées *classes à gauche*. L'ensemble de ses classes est noté $G/\sim_{H,g}$.

On a une définition analogue de *classes à droite* en utilisant la relation $\sim_{H,d}$ (cf. V.2.5.iv),) dont l'ensemble est noté $G/\sim_{H,d}$.

Proposition V.2.7 *Soit G un groupe et H un sous-groupe de g. On considère l'action de H sur G par translation à gauche. Alors :*

i) Dans le cas où G est abélien, la relations d'équivalence $\sim_{H,g}$ associée à l'action de H est la même qe celle définie en VII.7.3.

Preuve *: Est une vérification immédiate.*

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

$$p : H \to O(x) , g \mapsto g \cdot x$$

définie comme dans la proposition V.1.16 est bijective.

Preuve *: Pour tout $x \in G$, considérons l'application*

$$p : H \to O(x) , g \mapsto g \cdot x$$

comme à la proposition V.1.16. Il résulte alors de V.1.16.ii) que

$$\forall y \in O(x),\ p^{-1}(\{y\}) \cong \mathrm{Stab}_H(x) .$$

Or $g \in \mathrm{Stab}_H(x)$ si et seulement si $g \cdot x = x$, si et seulement si $g * x = x$ si et seulement si $g = e$. Le sous-groupe $\mathrm{Stab}_H(x)$ de H est donc un singleton. Ainsi en va-t-il donc aussi de $p^{-1}(\{y\})$ c'est-à-dire que $p : H \to O(x)$ est bijective.

iii) H est l'orbite de l'élément neutre e et la seule qui soit un sous-groupe de G.

Preuve *: En effet*

$$O(e) = \{h \cdot e , h \in H\} = \{h * e , h \in H\} = \{h \in H\} = H .$$

Pour $x \in G$, si $O(x)$ est un sous-groupe $e \in O(x)$ et par conséquent $O(x) = O(e)$.

iv) Il existe une bijection entre l'ensemble $G/\sim_{H,g}$ des classes à gauche et l'ensemble $G/\sim_{H,d}$ des classes à droite.

Preuve *: V.4.3.*

Remarque V.2.8 Le point V.2.7.ii) pourrait se reformuler en disant que l'action par translation à gauche (resp. à droite) est libre (cf. V.1.19.i).)

Définition V.2.9 (Indice d'un sous-groupe) Étant donnés un groupe G et un sous-groupe H de G, si l'ensemble $G/\sim_{H,g}$, est fini (cf. II.4.1,) son cardinal, qui est aussi celui de $G/\sim_{H,d}$, est appelé *indice de H dans G*.

V.3 . −Action par conjugaison

Dans cette section $(G,*)$ (le plus souvent abrégé en G) est un groupe dont on note e l'élément neutre.

Lemme V.3.1 *Étant donné un groupe G, pour tout $g \in G$, l'application $x \mapsto g*x*g^{-1}$ est un automorphisme de groupe de G (cf. III.2.7.ii).)*

***Preuve** : Tout d'abord*

$$\forall (g,x,y) \in G\times G\times G,\ g*x*y*g^{-1} = g*x*g^{-1} * g*y*g^{-1}$$

si bien que $x \mapsto g*x*g^{-1}$ est bien un morphisme de G dans luie-même (on pourrait dire un endomorphisme de G.)

Par ailleurs,

$$\forall (g,x) \in G\times G,\ (g^{-1})*g*x*g^{-1}*(g^{-1})^{-1} = x$$

si bien que $x \mapsto (g^{-1})*x*(g^{-1})^{-1}$ est l'application réciproque de $x \mapsto g*x*g^{-1}$ cette dernière étant donc bijective donc un isomorphisme et finalement un automorphisme (isomorphisme et endomorphisme.)

Lemme V.3.2 *L'application de $G\times G$ dans G donnée par $(g,x) \mapsto g\cdot x := g*x*g^{-1}$ définit une action de G sur lui-même.*

***Preuve** : On a vu au lemme V.3.1 que $x \mapsto g*x*g^{-1}$ est un automorphisme de G donc en particulier une bijection de G sur lui-même i.e. un élément de $\mathcal{S}(G)$ (cf. III.1.2.c).)*

De plus

$$\begin{array}{rcl} \forall (g,h,x) \in G\times G\times G,\quad (g*h)\cdot x &=& g*h*x*g*h^{-1} \\ &=& g*h*x*h^{-1}*g^{-1} \\ &=& g\cdot(h*x*h^{-1}) \\ &=& g\cdot(h\cdot x) \end{array}$$

ce qui prouve qu'on a bien défini une action.

Définition V.3.3 (Action par conjugaison) Soit G un groupe :

i) L'action de G sur lui-même définie par le lemme V.3.2 s'appelle *action par conjugaison* de G sur lui-même.

ii) Les orbites (cf. V.1.9.i),) pour l'action par conjugaison sont usuellement appelées *classes de conjugaison*.

iii) Deux élément appartenant à la même orbite, ou de manière équivalente, en relation par la relation $\sim$ (cf. V.1.8,) sont dits *conjugués*. Ainsi explicitement, $(x, y) \in G \times G$ sont conjugués s'il existe z (appartenant à G ou à un sous-groupe selon l'action considérée,) tel que $y = z * x * z^{-1}$.

iv) Il résulte de V.1.4.b) que tout sous-groupe H de G agit encore sur G à travers l'action de G sur lui-même par conjugaison. Cette action de H sur G est encore appelée *action par conjugaison de H sur G*.

Remarque V.3.4 Si $P \subset G$, est une partie de G,
(*i.e.* $P \in \mathcal{P}(G)$, pas nécessairement un sous-groupe,) notons

$$\forall g \in G,\ g * P * g^{-1} := \{g * x * g^{-1}\ ,\ x \in P\}\ .$$

Alors l'application $G \times \mathcal{P}(G) \to \mathcal{P}(G)$ définie par $(g, P) \mapsto g \cdot P := g * P * g^{-1}$ est une action de G sur l'ensemble de ses parties, qu'on apellera encore action par conjugaison. Elle induit encore une action par conjugaison de tout sous-groupe H de G sur $\mathcal{P}(G)$.

Proposition V.3.5 *Étant donné un groupe $(G, *)$ on note $\mathcal{G}$ l'ensemble de ses sous-groupes. Pour tout $g \in G$, et $H \in \mathcal{G}$ on note :*

$$g * H * g^{-1} := \{g * x * g^{-1}\ ,\ x \in H\}\ . \qquad \textit{V.3.5.1}$$

Alors :

i) Pour tout $H \in \mathcal{G}$ $g * H * g^{-1}$ est un sous-groupe de G i.e. un élément de $\mathcal{G}$.

***Preuve** : Étant donné un sous-groupe H de G et $g \in G$, $g * H * g^{-1}$ n'est autre que l'image de H par l'application $x \mapsto g * x * g^{-1}$ dont on a montré au lemme V.3.1 que c'est un morphisme de groupe. L'ensemble $g * H * g^{-1}$ est donc un groupe.*

ii) L'application

$$G \times \mathcal{G} \to \mathcal{G}\ ,\ (g,H) \mapsto g * H * g^{-1}$$

est une action de G sur $\mathcal{G}$ qui sera encore apppelée action par conjugaison.

Preuve *: Voir l'exercice V.7.8.*

V.4 . −Sous-groupes normaux

On pourrait tout à fait se passer, pour rédiger cette section (V.4,) des résultats des section V, V.3 et V.2 c'est-à-dire de tout ce qui concerne les actions de groupes. Un certain nombre de vérification devront alors être faites. Dans toute cette section (V.4,) $(G,*)$ **est un groupe d'élément neutre** e.

Notation V.4.1 Pour tout sous-groupe H de G, on définit comme en V.2.4 $\sim_{H,g}$ (resp. comme en V.2.5.iv) $\sim_{H,d}$) la relation binaire sur $G \times G$ par :

$$\begin{array}{c} \forall x \in G,\ \forall y \in G,\ \left(x \sim_{H,d} y \ \Leftrightarrow x^{-1} * y \ \in \ H\right) \\ \left(\text{resp.} \quad \forall x \in G,\ \forall y \in G,\ \left(x \sim_{H,g} y \ \Leftrightarrow \ y * x^{-1} \in H\right) \quad \right)\ . \end{array} \qquad \text{V.4.1.1}$$

On notera encore, :

$$\forall x \in G,\ x * H \ := \ \{x * y\ ;\ y \in H\}\ \left(\text{resp. } H * x \ := \ \{y * x\ ;\ y \in H\}\ .\right) \qquad \text{V.4.1.2}$$

On écrira parfois simplement xH (resp. Hx) pour $x * H$ (resp. $H * x$.)

Remarque V.4.2 La relation $\sim_{H,g}$, (resp. $\sim_{H,d}$,) est la relation d'équivalence induite par l'action de H sur G par translation à gauche (resp. par translation à droite) C'est donc une relation d'équivalence dont les classes sont les orbites de l'action (cf. V.1.9.i).)

Si toutefois on ne veut pas tenir compte de ces résultas on peut montrer directement la proposition suivante :

Proposition V.4.3 *i) Les relations binaires définies en V.4.1.1 sont des relations d'équivalence.*

Preuve *: Montrons que la relation $\sim_{H,d}$ 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. $x \sim_{H,d} x$ c'est-à-dire que la relation $\sim_{H,d}$ est réflexive.*

Par ailleurs :

$$\begin{array}{lrcl}
\forall x \in G,\ \forall y \in G,\ \big(& x & \sim_{H,d} & y \\
\Rightarrow & x^{-1} * y & \in & H \\
\Rightarrow & y^{-1} * x \ = \ (x^{-1} * y)^{-1} & \in & H \\
\Rightarrow & y & \sim_{H,d} & x \big)
\end{array}$$

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

Enfin :

$$\begin{array}{lrcl}
\forall x \in G,\ \forall y \in G,\ \forall z \in G,\ \big(& x \sim_{H,d} y & \text{et} & y \sim_{H,d} z \\
\Rightarrow & x^{-1} * y \in H & \text{et} & y^{-1} * z \in H \\
\Rightarrow & x^{-1} * y * y^{-1} * z & \in & H \\
\Rightarrow & x^{-1} * z & \in & H \\
\Rightarrow & x & \sim_{H,d} & z \big)
\end{array}$$

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

Un argument analogue vaut également pour $\sim_{H,g}$.

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. $\{H * x\ ;\ x \in G\}$.)

Plus précisément :

$$\forall x \in G,\ \mathrm{cl}_g(x) \ = \ \{y \ \in \ G\,;\, x \sim_{g,H} y\} \ = \ x{*}H \ \big(\textsf{resp.}\ \mathrm{cl}_d(x) \ = \ \{y \ \in \ G\,;\, x \sim_{d,H} y\} \ = \ H{*}x\,.\big)$$

1

***Preuve** : Pour tout $x \in G$, un élément y de G appartient à la classe de x modulo $\sim_{H,d}$ si et seulement si*

$$\big((x^{-1} * y \in H) \ \Leftrightarrow \ (\exists z \in H,\ (x^{-1} * y \ = \ z) \ \Leftrightarrow \ y \ \in \ x * H)\big)\,.$$

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

***Preuve** : Pour tout $x \in G$, l'application*

$$G \ \to \ G\,,\ z \ \mapsto \ x * z$$

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

$$G \ \to \ G\,,\ z \ \mapsto \ x^{-1} * z\,.$$

iv) L'application $x * H \mapsto H * x$ *pour* $x \in G$, *induit une bijection de l'ensemble* $G/\sim_{H,d}$ *des classes selon* $\sim_{H,d}$ *dans l'ensemble* $G/\sim_{H,g}$ *des classes selon* $\sim_{H,g}$.

Proposition V.4.4 (Sous-groupe normal) *Pour tout sous-groupe* $H \subset G$, *les assertions suivantes sont équivalentes :*

a) *La relations* $\sim_{H,d}$ *est compatible à la loi de groupe (cf. I.6.17,) i.e.*

$$\forall (x,y,z,t) \in G \times G \times G \times G,\ \big(x \sim_{H,d} z \text{ et } y \sim_{H,d} t\big) \Rightarrow\ x * y \sim_{H,d} z * t\ .$$

b) *La relations* $\sim_{H,g}$ *est compatible à la loi de groupe.*

c) *Les relations* $\sim_{H,g}$ *et* $\sim_{H,d}$ *sont égales.*

d)
$$\forall x \in G,\ \big(x * H * x^{-1} \subset H\big)\ .$$

e)
$$\forall x \in G,\ \big(x * H = H * x\big)\ .$$

f)
$$\forall x \in G,\ \big(H = x * H * x^{-1}\big)\ .$$

Preuve *: On montre l'équivalence d)* $\Leftrightarrow$ *b) :*

Remarquons que, pour tout $y \in H$, $y \sim_{H,g} e$, *et que, pour tout* $x \in G$, $x \sim_{H,g} x$. *Il en résulte donc, si l'on suppose l'assertion a) vérifiée, que pour tout* $y \in H$ *et tout* $x \in G$, $x*y \sim_{H,g} x$ *c'est-à-dire précisément* $x*y*x^{-1} \in H$. *L'assertion b) entraîne donc l'assertion d).*

Réciproquement, étant donné un quadruplet (x,z,y,t) *d'éléments de* G, *si* $y \sim_{H,g} t$, $y * t^{-1} \in H$. *Si l'on suppose l'assertion d) vérifiée,* $x * y * t^{-1} * x^{-1} \in H$. *Mais* $x \sim_{H,g} z$ *entraîne que* $x * z^{-1} \in H$ *; ce qui entraîne, puisque* H *est un sous-groupe de* G, *que*

$$x * y * (z * t)^{-1} = x * y * t^{-1} * z^{-1} = x * y * t^{-1} * x^{-1} * x * z^{-1} \in H$$

c'est-à-dire que $x * y \sim_{H,g} z * t$. *On a donc montré que l'assertion d) entraîne l'assertion b).*

Définition V.4.5 (Sous-groupes normaux/distingués) Un sous-groupe H de G est dit *normal* ou *distingué*, s'il vérifie l'une des conditions équivalentes de la proposition V.4.4.

Remarque V.4.6 On peut reformuler la définition ci-dessus en termes d'actions par conjugaison (cf. V.3,) un sous-groupe distingué n'étant rien d'autre qu'un point fixe pour l'action de G par conjugaison sur ses sous-groupes (cf. V.3.5.) On dira donc parfois que H est *invariant par conjugaison* ou même simplement *invariant*.

Notation V.4.7 Le point V.4.4.c) autorise à noter, pour un sous-groupe distingué H de G, simplement $\sim_H$ indifféremment $\sim_{H,g}$ et $\sim_{H,d}$ qui sont égales. De plus il résulte de V.4.4.b) (ou indifféremment de V.4.4.a)) que $\sim_H$ est compatible à la loi de groupe sur G (cf. I.6.17.) L'ensemble quotient

$$G/\sim_H \;=\; G/\sim_{H,d} \;=\; G/\sim_{H,g},$$

sera usuellement noté G/H et bénéficie de propriétés tout à fait intéressantes qui seront étudiées en détail dans la section V.5.

Définition V.4.8 Pour tout sous-groupe distingué H de G, on appellera *classes modulo* H ou *classes selon* H les classes d'équivalences pour la relation $\sim_H$. Cette dernière étant compatible, pour tout couple (α, β) de classes, tout x, x' dans α tout y, y' dans β, on a $x * y \;\sim_H\; x' * y'$ c'est-à-dire que $x * y$ et $x' * y'$ définissent la même classe selon H. On peut donc poser

$$\alpha * \beta \;=\; \overline{x} * \overline{y} \;:=\; \overline{x * y} \qquad \text{V.4.8.1}$$

la classe de $x * y$ pour n'importe quel représentant x de α et n'importe quel représentant y de β.

On note désormais G/H, l'ensemble des classes selon H muni de la loi de composition définie ci-dessus.

Exemple V.4.9 a) Les sous-groupes $\{e\}$ et G de G sont toujours distingués dans G.

b) Si G est un groupe abélien ($(\mathbb{Z}, +)$ par exemple,) tout sous-groupe est distingué.

c) Pour $n \in \mathbb{N}$, si $\mathcal{S}_n$ est le groupe symétrique, le groupe alterné $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$ (cf. VI.4).

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 $\mathcal{O}(E)$.

Proposition V.4.10 *Pour tout morphisme de groupes $f : G \to H$ (cf. III.2.1,) l'image réciproque $f^{-1}(H')$ de tout sous-groupe distingué H' de H est un sous-groupe distingué de G.*

En particulier, $\mathrm{Ker}\, f = f^{-1}(\{e_H\})$ est un sous-groupe distingué de G.

En revanche, il n'est pas vrai en général que l'image $f(G')$ d'un sous-groupe distingué G' de G est un sous-groupe distingué de H. C'est cependant le cas si f est surjectif.

***Preuve** : (cf. V.7.10.)*

Proposition V.4.11 (Relations d'équivalences compatibles) *i) Une relation d'équivalence $\sim$ sur G est compatible si et seulement si pour tout $(x, y) \in G \times G$,*

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

***Preuve** : 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) La classe $\overline{e}$ de l'élément neutre e pour une relation d'équivalence compatible est un sous-groupe distingué de G.

***Preuve** : 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 III.3.4, $\overline{e}$ 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 caractérisation V.4.4.d), des sous-groupes distingués, $\overline{e}$ *est un sous-groupe distingué de* G.

iii) 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 *: 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* $\sim_H$ *découle alors du lemme plus général :*

Lemme V.4.12 *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* $\sim_2$ *sont égale 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 *:*

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

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

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

$$\begin{array}{rrcl} & x & \in & \overline{e}_1 \\ \Rightarrow & x & \sim_1 & e \\ \Rightarrow & x * g & \sim_1 & g \\ \Rightarrow & x * g & \in & \overline{g}_1 \\ \Rightarrow & x * g & \in & \overline{g}_2 \\ \Rightarrow & x * g & \sim_2 & g \\ \Rightarrow & x * g * g^{-1} & \sim_2 & g * g^{-1} = e \\ \Rightarrow & x & \sim_2 & e\ . \end{array}$$

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.*

iv) ***(d)*** $\Rightarrow$ ***a))***
Pour tout $(x, y) \in G$, *si* $x \sim_1 y$, *alors, d'après V.4.11.i)*

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

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.*

V.5 . −Groupe quotient, factorisation des morphismes

Dans toute cette section (V.5,) $(G, *)$ **est un groupe d'élément neutre** e.

Proposition V.5.1 *Pour* $(G, *)$ *un groupe et* H *un sous-groupe distingué, la relation* $\sim_H$ *est compatible à la loi* $*$ *si bien qu'il existe une unique structyure de groupe sur l'ensemble* G/H *des classes pour la relation* $\sim_H$ *telle que la surjection canonique* $\pi : G \to G/H$ *soit un morphisme de groupe. Alors l'élément neutre de* G/H *est* $\overline{e} = H$ *et l'inverse de tout élément* $\overline{x}$ *est* $\overline{x^{-1}}$.

Preuve *:*

i) S'il existe une structure de groupe † *sur l'ensemble* $G/\sim_H$ *des classes d'équivalence selon* $\sim_H$, *telle que* π *est un morphisme, alors nécessairement, pour tout quadruplet* (x, x', y, y') *d'éléments de* G *tel que*

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

$$\begin{aligned}\pi(x*y) &= \pi(x)\dagger\pi(y)\\ &= \pi(x')\dagger\pi(y')\\ &= \pi(x'*y')\ .\end{aligned}$$

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

ii) Comme $\sim_H$ est compatible à $(G,*)$ (cf. V.4.4,)

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

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

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

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

Définition V.5.2 (Groupe quotient) Le groupe

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

est appelé *groupe quotient*. On dit encore que l'ensemble $G/\sim_H$ est muni de la *structure quotient*.

Exemple V.5.3 Nous avons remarqué (cf. V.4.9.b),) que dans un groupe abélien, et en particulier dans $(\mathbb{Z},+)$, tout sous-groupe est distingué. Nous avons aussi établi (cf. IV.5.5,) qu'une partie H de $\mathbb{Z}$ est un sous-groupe si et seulement s'il existe un entier $d\geq 0$ tel que $H=d\mathbb{Z}$.

On constate alors, que pour deux entiers x et y, $x\sim_H y$ si $y-x\in H$, c'est-à-dire si et seulement si $d|y-x$. La relation $\sim_H$ n'est autre, dans ce cas, que la relation de congruence modulo d.

Nous retrouvons dans ce cas particulier, grâce aux résultats de cette section, que la relation de congruence est compatible, fait que nous avions déjà établi dans le TD n° IV, exercice B. L'ensemble des classes modulo d que nous avions noté $\mathbb{Z}/d\mathbb{Z}$ s'identifie en tant que groupe, au groupe quotient $\mathbb{Z}/H=\mathbb{Z}/d\mathbb{Z}$.

Proposition V.5.4 (Factorisation des morphismes) *Pour tout morphisme de groupes*

$$f\ :\ G\ \to\ K \text{ et tout sous-groupe distingué } H\ \subset\ G,$$

les assertions suivantes sont équivalentes :

a) $H\ \subset\ \mathrm{Ker}\, f$.

b) Il existe un unique morphisme $\overline{f} : G/H \to K$ *tel que* $\overline{f} \circ \pi = f$.
De plus, $\overline{f}$ *est injectif (resp. surjectif) si et seulement si* $H = \operatorname{Ker} f$, *(rsp.* f *est surjectif.)*

Preuve *:*

i) Le fait même qu'on demande que, pour tout $x \in G$,

$$\overline{f}(\overline{x}) = f(x) ,$$

assure tautologiquement l'unicité de $\overline{f}$.

ii) Pour tout x, x' *dans* G, *si* $x \sim_H x'$, $x * x'^{-1} \in H$ *ce qui implique que* $x * x'^{-1} \in \operatorname{Ker} f$ *si l'on suppose que* $H \subset \operatorname{Ker} f$, *c'est-à-dire que* $f(x * x'^{-1}) = e_H$ *ou encore que* $f(x) = f(x')$. *On peut donc définir* $\overline{f}(\overline{x})$ *par* $f(x)$ *pour n'importe quel représentant* x *de* $\overline{x}$. *Ceci assure donc l'existence de* $\overline{f}$.

iii) Pour tout couple (α, β) *d'éléments de* G/H, *tout* $x \in \alpha$, *tout* $y \in \beta$, *étant donné la définition de la loi de composition sur* G/H *(cf. V.4.8.1,)*

$$\begin{aligned} \overline{f}(\alpha * \beta) &= \overline{f}(\overline{x * y}) \\ &= f(x * y) \\ &= f(x) *_H f(y) \\ &= \overline{f}(\alpha) *_H \overline{f}(\beta) \end{aligned}$$

c'est-à-dire que $\overline{f}$ *est un morphisme de groupes.*

iv) Un élément $u \in H$ *appartient à* $\operatorname{Im} \overline{f}$ *si et seulement s'il existe un élément* $\overline{x} \in G/H$ *tel que* $\overline{f}(\overline{x}) = u$ *c'est-à-dire si et seulement s'il existe* $x \in G$ *tel que* $u = f(x)$. *Autrement dit,*

$$\operatorname{Im} \overline{f} = \operatorname{Im} f$$

ce qui établit (cf. III.3.10,) que f *est surjectif si et seulement si* $\overline{f}$ *l'est.*

v) Enfin, $\overline{f}$ *est injective si et seulement si*

$$\operatorname{Ker} \overline{f} = e_{G/H} = H$$

(cf. III.3.10.) Ceci signifie exactement que $\overline{f}(\overline{x}) = e_H$ *si et seulement si* $\overline{x} = H$, *ou encore* $f(x) = e_H$ *si et seulement si* $x \in H$ *c'est-à-dire si et seulement si*

$$H = \operatorname{Ker} f .$$

Corollaire V.5.5 *Étant donné un morphisme de groupes $f : G \to K$ il existe un unique isomorphisme de groupes*

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

où $\pi : G \to G/\mathrm{Ker}\, f$ est la surjection canonique. En particulier si f est surjectif

$$\overline{f} : G/\mathrm{Ker}\, f \cong K$$

est un isomorphisme.

Preuve *: Il suffit d'appliquer la proposition V.5.4 à $H := \mathrm{Ker}\, f$.*

Corollaire V.5.6 *Étant donné un morphisme surjectif de groupes $p : G \to Q$, il existe un unique isomorphisme de groupes*

$\phi : G/\mathrm{Ker}\, p \to Q$ tel que $p = \phi \circ \pi$ où $\pi : G \to G/\mathrm{Ker}\, p$ est la surjection canonique.

Preuve *: C'est une conséquence immédiate du corollaire V.5.5 puisque $\mathrm{Im}\, p = Q$.*

Proposition V.5.7 *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 :*

a) Un sous-groupe distingué K de G.

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

c) Un morphisme de groupes surjectif $p : G \to Q$.

Preuve *:*

i) On a vu, grâce à la proposition V.4.11, qu'à toute relation compatible $\sim$ on associe canoniquement un sous-groupe distingué $H := \overline{e}$ et que, réciproquement, à tout sous-groupe distingué H on associe une unique relation compatible telle que $\overline{e} = H$.

ii) On a vu également, grâce à la proposition V.5.1, qu'à tout sous-groupe distingué (ou de manière équivalente à toute relation d'équivalence compatible) on associe une surjection $\pi : G \to G/H$ qui est un morphisme de groupes.

iii) Réciproquement, à tout morphisme surjectif $p : G \to Q$, on peut associer le sous-groupe distingué $H := \mathrm{Ker}\, p$ (cf. V.4.10.)

Le corollaire V.5.6 établit qu'en fait, les procédés ii) et iii) "inverses" l'un de l'autre, en un certain sens.

La proposition suivante V.5.8 étend au cas des groupes les constructions donées dans la proposition II.5.4.

Proposition V.5.8 *Étant donnés un entier* $n \in \mathbb{N}^*$, $(G_k, *_k)_{,1 \leq k \leq n}$ *des groupes*

$$\forall 1 \leq k \leq n,\ p_k \ :\ \prod_{i=1}^{n} G_i \ \to\ G_k \text{ les projections}$$

(cf. II.5.1.ii),) Alors :

i) Il existe une unique loi de composition $*$ *sur* $\prod_{k=1}^{n} G_k$ *telle que pour tout* $1 \leq k \leq n$ p_k *soit un morphisme de groupes ; la loi* $*$ *est donnée par*

$$\forall\big((x_1,\dots,x_n),(y_1,\dots,x_n)\big) \in \prod_{k=1}^{n} G_k \times \prod_{k=1}^{n} G_K,$$
$$(x_1,\dots,x_n)\ *\ (y_1,\dots,y_n)\ =\ (x_1 *_1 y_1,\dots,x_n *_n y_n)\,.$$

ii) La loi $*$ *étant définie sur* $\prod_{k=1}^{n} G_K$ *comme ci-dessus, si*

a) pour tout $1 \leq k \leq n$ e_k *est l'élément neutre de* G_k, $(e_1,\dots,e_n)$ *est l'élément neutre pour* $*$;

b) $x \in \prod_{k=1}^{n} G_k$ *est tel que pour tout* $1 \leq k \leq n$ $y_k \in G_k$ *est le symétrique de* $p_k(x)$, *alors* $(y_1,\dots,y_n)$ *est le symétrique de* x *dans* $\prod_{k=1}^{n} G_k$.

iii) Si pour tout $1 \leq k \leq n$ $(G_k, *_k)$ *est un groupe abélien,* $\big(\prod_{k=1}^{n} G_k, *\big)$ *est un groupe abélien.*

iv) Pour tout n-uplet de morphismes de groupes

$$f_k \ : \ H \ \to \ G_k \, , 1 \leq k \leq n \, ,$$

il existe un unique morphisme de groupe

$$f \ : \ H \ \to \ \prod_{k=1}^{n} G_k \text{ tel que } \forall 1 \leq k \leq n, \ f_k \ = \ p_k \ \circ \ f \ .$$

v) Dans le cas où il existe G tel que $\forall 1 \leq k \leq n, \ G_k \ = \ G$, la bijection $\phi \ : \ G^{[1;n]} \ \cong \ \prod_{k=1}^{n} G$ définie par la proposition II.5.1.iv) est un isomorphisme, pour peu que $G^{[1;n]}$ soit muni de la structure définie par la proposition I.6.20.

vi) Pour $(G_1, *_1)$, $(G_2, *_2)$ des groupes d'élément neutre respectif ϵ_1 et ϵ_2, on définit les applications

$$i_1 \ : \ G_1 \ \to \ G_1 \times G_2 \ , \ x \ \mapsto \ (x, \epsilon_2) \text{ et } i_2 \ : \ G_2 \ \to \ G_1 \times G_2 \ , \ x \ \mapsto \ (\epsilon_1, x) \ .$$

Alors :

a) les applications i_1 et i_2 sont des morphismes injectifs de groupes ;

b)

$$p_1 \ \circ \ i_1 \ = \ \mathrm{Id}_{G_1} \text{ et } p_2 \ \circ \ i_2 \ = \ \mathrm{Id}_{G_2} \ ;$$

c)

$$\mathrm{Ker}\, p_1 \ = \ \mathrm{Im}\, i_2 \text{ et } \mathrm{Ker}\, p_2 \ = \ \mathrm{Im}\, i_1 \ .$$

***Preuve** : (cf. Examen partiel du 24 octobre 2018 , exercice B.)*

Définition V.5.9 (Groupe produit) Avec les notations de la proposition V.5.8, la loi $*$ définie sur $\prod_{k=1}^{n} G_k$ comme en V.5.8.i) est appelée *loi produit* et le couple

$$(\prod_{k=1}^{n} G_k, *)$$

groupe produit.

V.6 . −Groupes finis : théorème de Lagrange

Définition V.6.1 (Groupe fini) Un groupe $(G, *)$ est un *groupe fini* si G est un ensemble fini au sens de la définition II.4.1.

Exemple V.6.2 Pour $n \in \mathbb{N}^*$, le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe fini (cf. TD n° IV, exercice B.)

D'autres exemples de groupes finis seront étudiés dans le chapitre VI.

Proposition V.6.3 *Si $(G, *)$ est un groupe fini, une partie H de G munie de la loi de composition $*$ est un sous-groupe de G si et seulement si H est non-vide et pour tout $(x, y) \in H \times H$, $x * y \in H$.*

Preuve *: Voir le TD n° V, exercice A.*

Proposition V.6.4 *Si G est un groupe fini et H un sous-groupe de G, la relation d'équivalence $\sim_{H,g}$ (resp. $\sim_{H,d}$) étant définie comme en V.2.4, (resp. V.2.5.iv),)*

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

d'où il résulte en particulier que

$$\#(H) | \#(G)\ .$$

Preuve *: Puisque les orbites sous l'action de H (aussibien à gauche qu'à droite,) sont des classes d'équivalence, elles réalisent une partition de G. Si G est fini, les orbites sont donc toutes des sous-ensembles finis ($H \;=\; O(e)$ (cf. V.2.7.iii),) en particulier) et en nombre fini i.e. $G/\sim$ est aussi un ensemble fini (où $\sim$ désigne aussibien $\sim_{H,g}$, que $\sim_{H,d}$.)*

En posant $\#(G/\sim) \;=\; k \in \mathbb{N}$, choisissons $x_{i\ ,1\leq i\leq k}$ des éléments de G tels que

$$\forall (i,j) \in [1;k] \times [1;k],\ i \neq j \;\Rightarrow\; O(x_i) \cap O(x_j) \;=\; \emptyset$$

autrement dit un représentant par orbite. On a alors :

$$G \;=\; \bigcap_{1\,\leq\, i\,\leq\, k} O(x_i)$$

ce qui entraîne

$$\#(G) \;=\; \sum_{i=1}^{k} \#(O(x_i))\ .$$

Or il découle de V.2.7.ii) que $\forall 1 \leq i \leq k,\ \#(O(x_i)) \;=\; \#(H)$ d'où il résulte finalement que

$$\#(G) \;=\; k * \#(H) \;=\; \#(G/\sim) \;*\; \#(H)\ .$$

Corollaire V.6.5 *Si G est un groupe fini et H un sous-groupe, le cardinal de G est le produit de l'indice de H dans G (cf. V.2.9p)ar le cardinal de H.*

Corollaire V.6.6 (théorème de LAGRANGE) *Si G est un groupe fini pour tout sous-groupe H de G, le cardinal de H divise le cardinal de G.*

Corollaire V.6.7 *Le corollaire V.6.5 ci-dessus et le corollaire V.5.5 on pour conséquence que, pour tout morphisme de groupes $f : G \to H$, avec G groupe fini,*

$$\#(G) = \#\big(\mathrm{Ker}\, f\big) * \#\big(\mathrm{Im}\, f\big) .$$

Proposition V.6.8 *Étant donné un groupe $(G, *)$ pour tout $x \in G$:*

i) Le sous-groupe $< \{x\} >$ engendré par $\{x\}$ (cf. III.4.2,) de G est l'image du morphisme

$$\epsilon_x : \mathbb{Z} \to G , \; n \mapsto x^n$$

(cf. Problème n° III, exercice A.)

Preuve *: Voir l'exercice V.7.12.*

ii) a) Soit le noyau de ϵ_x est réduit à $\{0\}$ au quel cas

$$< \{x\} > \cong \mathbb{Z} ;$$

b) Soit il existe $d \in \mathbb{N}^*$ tel que $\mathrm{Ker}\, \epsilon_X = d\mathbb{Z}$ et

$$< \{x\} > \cong \mathbb{Z}/\mathrm{Ker}\, \epsilon_x \cong \mathbb{Z}/d\mathbb{Z} .$$

Preuve *: Le noyau du morphisme ϵ_x est un sous-groupe de $\mathbb{Z}$ il existe donc $d \in \mathbb{N}$ tel que $\mathrm{Ker}\, \epsilon_x = d\mathbb{Z}$ (cf. IV.5.5.) Or $d = 0$ si et seulement si ϵ_x est un morphisme injectif si et seulement si*

$$\mathbb{Z} \cong \mathrm{Im}\, \epsilon_x \cong < \{x\} >$$

ce qui correspond à la situation du point a).

Si $d \neq 0$, Il existe un unique isomorphisme

$$\overline{\epsilon}_x : \mathbb{Z}/\mathrm{Ker}\, \epsilon_x = \mathbb{Z}/d\mathbb{Z} \to \mathrm{Im}\, \epsilon_x = < \{x\} > .$$

On peut en effet appliquer les résultats du paragraphe V.5 et en particulier la proposition V.5.4.

Définition V.6.9 (Ordre d'un élément) Pour $(G, *)$ un groupe et $x \in G$, avec les notations de la proposition V.6.8, si $< \{x\} > \cong \mathbb{Z}$, on dit que x est d'*ordre infini* sinon on dit que x est d'*ordre* d où d est l'entier défini de manière équivalente dans la proposition V.6.8.ii).b) par $\mathrm{Ker}\, \epsilon_x = d\mathbb{Z}$ ou $d = \#(\mathrm{Im}\, \epsilon_x)$.

Remarque V.6.10 Il est immédiat de vérifier que pour tout élément x d'un groupe G, l'ordre de x défini comme en V.6.9, est le plus petit (aussibien au sens de la relation d'ordre que de la relation de divisibilité sur $\mathbb{Z}$) entier $n \in \mathbb{N}^*$ tel que $x^n = e$.

Proposition V.6.11 (Propriétés de l'ordre d'un éléments) *i) Soit $f : G \to h$ un morphisme de groupes et $x \in G$. Si x est d'ordre fini, $f(x)$ l'est aussi et l'ordre de $f(x)$ divise l'ordre de x.*

ii) Avec les notations du point i), si f est injectif, x et $f(x)$ ont même ordre.

iii) Dans un groupe g deux éléments conjugués (cf. V.3.3.iii),) ont même ordre.

Théorème V.6.12 (de Lagrange) *Pour G un groupe fini, l'ordre de tout élément x de G divise le cardinal de G.*

Preuve *: Remarquons d'abord que si G est fini, on ne peut se trouver dans la situation de V.6.8.ii).a) si bien que l"ordre d de x est bien un entier naturel. Or il résulte de V.6.8.ii).b) que*

$$d = \#(\mathrm{Im}\, \epsilon_x) = \#(< \{x\} >) .$$

Puisque $< \{x\} >$ est un sous-ghroupe de G, il suffit d'appliquer le corollaire V.6.6.

Définition V.6.13 Avec les notations de la proposition V.6.8,

i) si le morphisme ϵ_x est surjectif, autrement dit si

$$G = \mathrm{Im}\, \epsilon_x = < \tilde{s}x >,$$

on dit que G est *monogène* ;

ii) si de plus on est dans la situation de V.6.8.ii).b), auqel cas $G \cong \mathbb{Z}/d\mathbb{Z}$, on dit que G est *cyclique*.

Corollaire V.6.14 *Un groupe est cyclique si et seulement s'il est monogène et fini.*

Corollaire V.6.15 *Si G est un groupe fini de cardinal p premier, G est isomorphe (non canoniquement) à $(\mathbb{Z}/p, +)$ et donc commutatif (abélien).*

V.7 . −Exercices

Exercice V.7.1 [] Faire la preuve de la proposition V.4.3.

Exercice V.7.2 [] Faire la preuve du lemme V.1.11

Exercice V.7.3 [] Faire la preuve de la proposition V.1.14.

Exercice V.7.4 [] Faire la preuve de la proposition V.1.16.i).

Exercice V.7.5 [Stabilisateur]

Soit $(G, *)$ un groupe et E un ensemble muni d'une action de G notée $g \cdot x$ pour tout $(g, x) \in G \times E$.

Montrer que pour tout $(x, g) \in E \times G$,

$$\mathrm{Stab}_G(g \cdot x) = g * \mathrm{Stab}_G(x) * g^{-1} .$$

Exercice V.7.6 []

Considérons l'action par translation à gauche sur les parties de G définie en V.2.3.

1) () Montrer que cette action ne se restreint pas en général en une action de G sur l'ensemble de ses sous-groupes.

2) () Montrer que l'orbite $O(P)$ d'une partie $P \in \mathcal{P}(G)$ contient au plus un sous-groupe.

Exercice V.7.7 [] Faire les détails de la construction esquissée dans la remarque V.2.5.

Exercice V.7.8 [] Faire la preuve de la proposition V.3.5.ii).

Exercice V.7.9 [] Compléter la preuve de la proposition V.4.4.

Exercice V.7.10 [] Faire la preuve de la proposition V.4.10.

Exercice V.7.11 [] Faire la preuve de la proposition V.5.1.

Exercice V.7.12 [] Faire la preuve de la proposition V.6.8.i).

VI . −Groupe symétrique et groupe alterné

VI.0 . −Introduction

Si E est un ensemble fini (cf. II.4.1,) on dispose, par définition, d'une bijection $\gamma \ : \ E \ \cong \ [1; n]$. Ainsi, en vertu de III.2.6, on dispose d'un isomorphisme de groupes

$$\mathcal{S}(\gamma) \ : \ (\mathcal{S}(E), \circ) \ \to \ (\mathcal{S}([1; n]), \circ) \ .$$

L'étude des bijection d'un ensemble fini dans lui-même se ramène donc à l'étude du groupe

$$\mathcal{S}_n \ := \ \mathcal{S}([1; n])$$

qu'on appellera le *groupe symétrique*.

VI.1 . −Groupe symétrique, permutations

Définition VI.1.1 (Groupe symétrique) i) (**Groupe symétrique**)
Pour tout $n \ \in \ \mathbb{N}$, le groupe

$$\mathcal{S}_n \ := \ \big(\mathcal{S}([1; n]), \circ\big)$$

est appelé *groupe symétrique* sur n éléments.

ii) (**Permutation/Substitution**)
Un élément $s \ \in \ \mathcal{S}_n$ est appelé *permutation* ou *substitution*.

iii) Pour toute permutation $s \ \in \ \mathcal{S}_n$, on notera

$$s \ = \ \begin{pmatrix} 1 & 2 & \dots & n \\ s(1) & s(2) & \dots & s(n) \end{pmatrix} \ .$$

Exemple VI.1.2 i) Le groupe $\mathcal{S}_1$ est le groupe à un élément.

ii) Le groupe $\mathcal{S}_2$ a pour éléments l'identité et l'application définie par $1 \mapsto 2$ et $2 \mapsto 1$. C'est donc un groupe à deux éléments canoniquement isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

Proposition VI.1.3 *Pour tout* $(p, q) \ \in \ \mathbb{N}^* \times \mathbb{N}^*, p \ \leq \ q,$

$$S \ := \ \{s \ \in \ \mathcal{S}_q \ ; \ \forall x \in [p + 1; q], \ s(x) \ = \ x\}$$

est un sous-groupe de $\mathcal{S}_q$ *et* S *est isomorphe à* $\mathcal{S}_p$.

Preuve *: (cf. VI.5.2.)*

Remarque VI.1.4 i) On peut donc, grâce à la proposition VI.1.3 ci-dessus, écrire $\mathcal{S}_p \subset \mathcal{S}_q$ pour $p \leq q$ et identifier $\mathcal{S}_p$ à un sous-groupe de $\mathcal{S}_q$.

ii) On étudiera d'autres relations entre les groupes symétrique notamment au TD n° VI, exercice G.

Lemme VI.1.5 *Pour $n \in \mathbb{N}$, la relation $\sim$ définie sur le groupe $\mathcal{S}_{n+1}$ par*

$$s \sim t \Leftrightarrow s^{-1}(n+1) = t^{-1}(n+1)$$

est la relation d'équivalence déterminée par l'action de $\mathcal{S}_n$ (cf. V.4.3,) par translation à gauche sur $\mathcal{S}_{n+1}$ (cf. V.2.2.)

Preuve : *Pour tout $(s,t) \in \mathcal{S}_{n+1} \times \mathcal{S}_{n+1}$,*

$$s \sim t \Leftrightarrow s^{-1}(n+1) = t^{-1}(n+1) \Leftrightarrow s \circ t^{-1}(n+1) = n+1 \Leftrightarrow t \circ s^{-1}(n+1) = n+1 .$$

Ceci équivaut encore, en vertu de la proposition VI.1.3 et de la remarque VI.1.4.i) ci-dessus, à

$$s \circ t^{-1} \in \mathcal{S}_n \text{ et } t \circ s^{-1} \in \mathcal{S}_n$$

c'est-à-dire qu'il existe $(u,v) \in \mathcal{S}_n \times \mathcal{S}_n$ tel que

$$s = u \circ t \text{ et } t = v \circ s$$

ce qui signifie que l'orbite (cf. V.1.9.i),) de s est égale à l'orbite de t sous l'action à gauche de $\mathcal{S}_n$. (Voir aussi l'exercice VI.5.1.question 4).)

Corollaire VI.1.6 *Avec les notations du lemme VI.1.5, chaque classe d'équivalence pour $\sim$ ou de manière équivalente chaque orbite pour l'action à gauche de $\mathcal{S}_n$ est en bijection avec $\mathcal{S}_n$.*

Preuve : *C'est une conséquence du lemme VI.1.5 ci-dessus et de la proposition V.2.7.ii).*

Lemme VI.1.7 *Pour $n \in \mathbb{N}$:*

i) L'application

$$\nu : \mathcal{S}_{n+1} \to [1; n+1] , \ s \mapsto s(n+1) .$$

est surjective.

Preuve : *Pour tout $k \in [1; n+1]$, considérons l'application :*

$$\begin{array}{rccl} t : & [1;n+1] & \to & [1;n+1] \\ & k & \mapsto & n+1 \\ & n+1 & \mapsto & k \\ & \ell & \mapsto & \ell \ \forall 1 \leq \ell \leq n, \ , \ \ell \neq k . \end{array}$$

D'une part on vérifie très facilement que t est bijective, et donc que $t \in \mathcal{S}_{n+1}$ et de manière tautologique que $\nu(t) = k$.

ii) Il existe une bijection

$$\overline{\nu} \,:\, \mathcal{S}_{n+1}/R \,\to\, [1;n+1] \text{ telle que } \forall s \in \mathcal{S}_{n+1},\ \nu(s) \,=\, \overline{\nu}(\overline{s})\ .$$

Preuve *: Par définition, pour tout* $s \,\in\, \mathcal{S}_{n+1}$ *tout* $(t,u) \,\in\, \overline{s} \times \overline{s}$, $t(n+1) \,=\, u(n+1)$ *i.e.* $\nu(t) \,=\, \nu(u)$. *On posera donc*

$$\overline{\nu}(\overline{s}) \,:=\, \nu(t)$$

pour n'importe quel élément $t \,\in\, \overline{s}$. *L'application* $\overline{\nu}$ *est bien définie puisque tous les éléments de* $\overline{s}$ *ont même image par* ν.

Par ailleurs, pourr tout $k \,\in\, [1;n+1]$, *il existe, en vertu de VI.5.1.question 8),* $s \,\in\, \mathcal{S}_{n+1}$ *telle que* $\nu(s) \,=\, k$. *Il s'ensuit donc que* $\overline{\nu}(\overline{s}) \,=\, k$ *et, par conséquent, que* $\overline{\nu}$ *est surjective.*

Pour tout $(s,t) \,\in\, \mathcal{S}_{n+1} \times \mathcal{S}_{n+1}$,

$$\overline{\nu}(\overline{s}) \,=\, \overline{\nu}(\overline{t}) \,\Leftrightarrow\, \nu(s) \,=\, \nu(t) \,\Leftrightarrow\, s(n+1) \,=\, t(n+1) \,\Leftrightarrow\, s\,R\,t \,\Leftrightarrow\, \overline{s} \,=\, \overline{t}$$

si bien que $\overline{\nu}$ *est injective.*

Proposition VI.1.8 *Pour tout* $n \,\in\, \mathbb{N}^*$, *le groupe* $\mathcal{S}_n$ *est un groupe fini et l'on a la relation*

$$\forall n \in \mathbb{N}^*,\ \#(\mathcal{S}_{n+1}) \,=\, (n+1).\#(\mathcal{S}_n)$$

d'où il résulte finalement que

$$\forall n \in \mathbb{N},\ \#(\mathcal{S}_n) \,=\, n!\ .$$

Preuve *: On a vu dans l'exemple VI.1.2 que les groupes* $\mathcal{S}_1$ *et* $\mathcal{S}_2$ *sont des groupes finis.*

Pour $n \,\in\, \mathbb{N}$, *considérons la relation d'équivalence introduite au lemme VI.1.5. On sait que* $\mathcal{S}_{n+1}$ *est alors l'union disjointe des classes dé'quivalence pour* $\sim$. *Comme d'une part chacune de ces classes est en bijection avec* $\mathcal{S}_n$ *en vertu du corollaire VI.1.6, et que d'autre part l'ensemble* $\mathcal{S}_{n+1}/\ \sim$ *des classes est en bijection avec* $[1;n+1]$, *d'après le lemme VI.1.7.ii), si l'on fait l'hypothèse que* $\mathcal{S}_n$ *est un groupe fini* $\mathcal{S}_{n+1}$ *est une union finie d'ensembles finis et est donc un ensemble fini. On a de plus*

$$\#(\mathcal{S}_{n+1}) \,=\, \#\big(\mathcal{S}_{n+1}/\sim\big) \cdot \#(\mathcal{S}_n) \,=\, \#\big([1;n+1]\big) \cdot \#(\mathcal{S}_n) \,=\, (n+1) \cdot \#(\mathcal{S}_n)\ .$$

Définition VI.1.9 Soient $n \,\in\, \mathbb{N}^*$ et $s \,\in\, \mathcal{S}_n$.

i) (**Point fixe**)
On dit que $x \,\in\, [1;n]$ est un *point fixe* pour s si $s(x) \,=\, x$.

ii) (**Support**)

Le *support* de s noté $\mathrm{Supp}(s)$ est le complémentaire de l'ensemble des points fixes de s, autrement dit

$$\mathrm{Supp}(s) \ = \ \{x \ \in \ [1;n] \ ; \ s(x) \ \neq \ x\} \ .$$

Proposition VI.1.10 *Pour tout* $n \ \in \ \mathbb{N}^*$, *tout* $(u,v) \ \in \ \mathcal{S}_n \times \mathcal{S}_n$,

$$\mathrm{Supp}(u) \ \cap \ \mathrm{Supp}(v) \ = \ \emptyset \ \Rightarrow \ u \ \circ \ v \ = \ v \ \circ \ u \ .$$

Preuve : *Voir le TD n° VI, exercice A.*

VI.2 . −Orbites cycles

Dans cette section (VI.2,) on fixe un entier $n \ \in \ \mathbb{N}^*$ **et l'on note** $\mathcal{S}_n$ **le groupe symétrique sur** n **éléments.**

Lemme VI.2.1 *Pour tout* $s \ \in \ \mathcal{S}_n$, *le morphisme*

$$\epsilon_s \ : \ \mathbb{Z} \ \rightarrow \ \mathcal{S}_n \ , \ k \ \mapsto \ s^k$$

(cf. Problème n° III, exercice A,)définit une action de $\mathbb{Z}$ *sur* $[1;n]$,

$$\forall (k,x) \in \mathbb{Z} \times [1;n], \ k \ \cdot \ x \ = \ s^k(x) \ .$$

Preuve : *Cela découle immédiatement de la définition d'action de groupe donnée en V.1.1.*

Corollaire VI.2.2 *Pour tout élément* s *du groupe symétrique* $\mathcal{S}_n$, *la relation* R_s *définie sur* $[1;n]$ *par* aR_sb *s'il existe* $k \ \in \ \mathbb{Z}$ *tel que* $b \ = \ s^k(a)$, *est une relation d'équivalence.*

Preuve : *(cf. V.4.3.)*

Définition VI.2.3 Soit s un élément du groupe symétrique $\mathcal{S}_n$.

i) (**Orbite**)

Pour tout $a \in [1;n]$, la classe de a selon la relation R_s définie à la proposition VI.2.2 est appelée *orbite de* a *sous* s et notée $O_s(a)$. C'est bien évidemment l'orbite de a pour l'action donnée par le lemme VI.2.1 au sens de la définition V.1.9.i).

ii) (**Orbite non triviale**)

Une orbite réduite à un élément est dite *triviale*. On note que l'orbite d'un élément a est triviale si et seulement si $O_s(a) = \{a\}$ c'est-à-dire que a est un *point fixe* (cf. VI.1.9.i),) pour s.

iii) (**Cycle**)

Une permutation $c \in \mathcal{S}_n$ dont l'une seulement des orbites $O_c(a)$ n'est pas triviale, est appelée *cycle* ; $O_c(a)$ est appelé *support du cycle* c, et le cardinal de $O_c(a)$ la *longueur du cycle* c.

Un cycle de longueur l est usuellement appelé un *l-cycle*.

iv) (**Permutation circulaire**)

Un cycle dont le support est égal à $[1;n]$ c'est-à-dire encore une permutation n'ayant qu'une orbite, est appelé *permutation circulaire*.

v) (**Transposition**)

Un cycle de longueur 2 c'est-à-dire encore une permutation ayant $n-1$ orbites est appelé *transposition*.

Exemple VI.2.4 L'identité $\mathrm{Id}_{[1;n]}$ n'est pas un cycle puisque toutes ses orbites sont triviales.

Remarque VI.2.5 (Support) On remarque que le support $\mathrm{Supp}(s)$ d'une permutation $s \in \mathcal{S}_n$ (cf. VI.1.9,) est la réunion des orbites non triviales de s.

Lemme VI.2.6 *Soit $c \in \mathcal{S}_n$ un cycle. On note $O_c(a)$, $a \in [1;n]$ son unique orbite non triviale et $\ell := \#(O_c(a))$ sa longueur.*

i) L'ordre de c dans le groupe $\mathcal{S}_n$ (cf. V.6.9,) est un nombre entier $d \geq 2$.

ii) Il existe un entier $\gamma \geq 2$, tel que pour tout $b \in O_c(a)$ le stabilisateur de b pour l'action de $\mathbb{Z}$ (cf. V.1.15,) soit égal à $\gamma\mathbb{Z}$.

iii) On a :

$$\gamma = d\,.$$

iv) L'application

$$p : \mathbb{Z} \to O_c(a)\,,\ k \mapsto k \cdot a := c^k(a)$$

(cf. V.1.16,) induit une application bijective

$$\overline{p} : \mathbb{Z}/\gamma\mathbb{Z} \to O_c(a)\,,\ \overline{k} \mapsto kp(k) \qquad (1)$$

où $\overline{k}$ désigne la classe d'un entier modulo γ.

Il s'ensuit que

$$\ell = \gamma\,.$$

Preuve *:*

i) Le morphisme

$$\epsilon_c \,:\, \mathbb{Z} \,\to\, \mathcal{S}_n \,,\; k \,\mapsto\, c^k$$

ne peut être injectif puisque $\mathcal{S}_n$ *est fini (cf. VI.1.8,) et que* $\mathbb{Z}$ *ne l'est pas. L'ordre* d *de* c *est donc un entier naturel* > 0*. De plus* $d \,=\, 1$*, entraîne* $c \,=\, \mathrm{Id}$*.*

ii) Soit donc $a \,\in\, [1;n]$*, tel que* $O_c(a)$ *soit la seule orbite non triviale de* c*. Le stabilisateur* S *de* a *pour l'action de* $\mathbb{Z}$ *est un sous-groupe de* $\mathbb{Z}$*. Il existe donc* $\gamma \,\in\, \mathbb{N}$ *tel que* $S \,=\, \gamma\mathbb{Z}$*.*

$\gamma \,=\, 0$ *entraîne que l'application*

$$p \,:\, \mathbb{Z} \,\to\, O_c(a) \,,\; k \,\mapsto\, c^k(a)$$

est injective (cf. V.1.16.ii).) Or $O_c(a) \;\subset\; [1;n]$ *est fini,* p *ne peut donc pas être injective.*

$\gamma \,=\, 1$ *entraîne que* $c(a) \,=\, a$ *i.e.*a *est un point fixe, ce qui contredit le fait que* $O_c a(a)$ *soit une orbite non triviale.*

Il en résulte donc que $\gamma \,\geq\, 2$*.*

Enfin pour tout $b \,=\, c^k(a) \,\in\, O_c(a)$ *il résulte de la proposition V.1.18 que le stabilisateur* T *de* b *vérifie* $T \,=\, k + S - k$ *d'où il découle, puisque* $\mathbb{Z}$ *est un groupe abélien, que* $T \,=\, S$*. Tous les éléments de* $O_c(a)$ *ont donc le même stabilisateur* $\gamma\mathbb{Z}$*.*

iii) Par définition de l'ordre d *de* c*,* $c^d \,=\, \mathrm{Id}$*. Il s'ensuit que*

$$\forall b \in O_c(a),\; c^d(b) \,=\, b$$

c'est-à-dire que d *est dans le stabilisateur de* b *qui, en vertu de ii) est égal à* $\gamma\mathbb{Z}$*. Il en résulte donc que*

$$\gamma | d \,.$$

Toujours en vertu de ii) pour tout $b \,\in\, O_c(a)$*,* $c^\gamma(b) \,=\, b$ *si bien que*

$$c^\gamma{}_{|O_c(a)} \,=\, \mathrm{Id}_{O_c(a)} \,.$$

Or pour tout $b \,\notin\, O_c(a)$*,* $c(b) \,=\, b$ *si bien que pour tout* $b \,\notin\, O_c(a)$ $c^\gamma(b) \,=\, b$ *c'est-à-dire que*

$$c^\gamma{}_{|[1;n]\setminus O_c(a)} \,=\, \mathrm{Id} \,.$$

Il en résulte donc que

$$c^\gamma \,=\, \mathrm{Id}$$

ce qui entraîne

$$d | \gamma$$

et finalement

$$d \,=\, \gamma \,.$$

iv) Pour tout $(k, \ell) \in \mathbb{Z} \times \mathbb{Z}$,

$$p(k) = p(\ell) \Leftrightarrow c^k(a) = c^\ell(a) \Leftrightarrow c^{k-\ell}(a) = a \Leftrightarrow k - \ell \in \gamma\mathbb{Z}$$

(cf. ii).) Il s'ensuit que d'une part on peut définir $\overline{p}$ *par*

$$\forall k \in \mathbb{Z},\ \overline{p}(\overline{k}) = p(k)$$

et que d'autre part $\overline{p}$ *ainsi définie est injective. Comme* p *était surjective,* $\overline{p}$ *l'est encore si bien que* $\overline{p}$ *est bijective.*

Il s'ensuit que

$$\#\big(\mathbb{Z}/\gamma\mathbb{Z}\big) = \#\big(O_c(a)\big) \Leftrightarrow \gamma = \ell\,.$$

Théorème VI.2.7 *Pour tout entier naturel* $n \geq 1$, *tout cycle* $c \in \mathcal{S}_n$, *la longueur du cycle* c *est l'ordre de l'élément* c *dans le groupe* $\mathcal{S}_n$.

Preuve : *C'est bien entendu une conséquence immédiate de VI.2.6.iii) et VI.2.6.iv).*

Remarque VI.2.8 Pour tout cycle $c \in \mathcal{S}_n$ de longueur ℓ et tout élément a du support de c, le point VI.2.6.iv) donne une bijection $\overline{p} : \mathbb{Z}/\ell\mathbb{Z} \cong O_c(a)$. Pour tout $k \in \mathbb{Z}$, on a alors

$$c(\overline{p}(\overline{k})) = c^{k+1}(a)$$

d'où l'on déduit que $\overline{p}^{-1} \circ c \circ \overline{p}$ est la bijection de $\mathbb{Z}/\lambda\mathbb{Z}$ sur lui-même donnée par $\overline{k} \mapsto \overline{k} + \overline{1}$.

On posera alors

$$a_i := c^i(a)\,,0 \leq i \leq \ell-1$$

et l'on notera

$$c = (a_0 \dots a_{\ell-1})\,. \qquad \text{VI.2.8.1}$$

En particulier pour deux éléments distincts a et b de $[1; n]$, on notera (ab) la transposition t telle que $t(a) = b$ et $t(b) = a$. On a immédiatement

$$(ab) = (ba) \text{ et } (ab)^2 = \mathrm{Id}\,. \qquad \text{VI.2.8.2}$$

Proposition VI.2.9 *Tout cycle* $c \in \mathcal{S}_n$ *de longueur* ℓ *peut être écrit comme un produit de* $\ell - 1$ *transpositions.*

Preuve : *(cf. TD n° VI, exercice D, question 2).)*

Théorème VI.2.10 *Étant donnés un entier $n \in \mathbb{N}^*$ pour deux cycles c et d éléments de $\mathcal{S}_n$, les assertions suivantes sont équivalentes :*

a) Les cycles c et d ont même longueur.

b) Il existe $u \in \mathcal{S}_n$ tel que

$$d = u \circ c \circ u^{-1}$$

autrement dit c et d sont conjugués (cf. V.3.3,) dans $\mathcal{S}_n$.

***Preuve** :*

*i) **(b) $\Rightarrow$ a))***

On remarque que, s'il existe $u \in \mathcal{S}_n$ tel que $d = u \circ c \circ u^{-1}$, alors pour tout $k \in \mathbb{Z}$, $d^k = u \circ c^k \circ u^{-1}$; ce qui entraîne que $d^k = \mathrm{Id}$ si et seulement si $c^k = \mathrm{Id}$ et finalement que c et d ont même ordre. Le théorème VI.2.7, assure alors que c et d ont même longueur.

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

Notons

— $O_c(a)$ (resp. $O_d(b)$) le support de c (resp. d,)

—

$$p : \mathbb{Z} \to O_c(a)\ ,\ k \mapsto c^k(a) \text{ (resp. } q : \mathbb{Z} \to O_d(b)\ ,\ k \mapsto d^k(b)\ )$$

l'application définie comme en V.1.16,

— ℓ la longueur commune de c et d,

—

$$\overline{p} : \mathbb{Z}/\ell\mathbb{Z} \cong O_c(a) \text{ resp. } \overline{q} : \mathbb{Z}/\ell\mathbb{Z} \cong O_d(b)\ )$$

la bijection déduite de p (resp. q) comme en VI.2.6.iv).

Pour tout $y \in O_d(b)$ il existe $k \in \mathbb{Z}$ tel que $y = d^k(b)$, il s'ensuit que :

$$\begin{aligned}
(\overline{q} \circ \overline{p}^{-1} \circ c \circ \overline{p} \circ \overline{q}^{-1})(b) &= (\overline{q} \circ \overline{p}^{-1} \circ c \circ \overline{p})(\overline{k}) \\
&= (\overline{q} \circ \overline{p}^{-1} c)\big(c^k(a)\big) \\
&= (\overline{q} \circ \overline{p}^{-1})\big(c^{k+1}(a)\big) \\
&= \overline{q}(\overline{k+1}) \\
&= d^{k+1}(b) \\
&= d(y)\ .
\end{aligned}$$

Définissons donc

$$v := \overline{q} \circ \overline{p}^{-1} : O_c(a) \cong O_d(b)\ .$$

Nous venons de montrer ci-dessus que

$$\forall y \in O_d(b),\ v \circ c \circ v^{-1}(b) = d(b)\ .$$

Puisque $\#\big(O_c(a)\big) \;=\; \#\big(O_d(b)\big)$,

$$\#\big([1;n]\setminus O_c(a)\big) \;=\; \#\big([1;n]\setminus O_d(b)\big)$$

il existe donc une bijection (a priori certainement pas unique,)

$$w \;:\; [1;n]\setminus O_c(a) \;\cong\; [1;n]\setminus O_d(b)\;.$$

Il s'ensuit que pour tout $y \in [1;n] \setminus O_d(b)$, $w^{-1}(y) \notin O_c(a)$ *si bien que* $c\big(w^{-1}(y)\big) = w^{-1}(y)$ *d'où*

$$w\circ c\circ w^{-1}(y) \;=\; y \;=\; d(y)\;.$$

En définissant u *par :*

$$u_{|O_c(a)} \;:=\; v \text{ et } u_{|[1;n]\setminus O_c(a)} \;:=\; w$$

il vient

$$d \;=\; u\circ c\circ u^{-1}\;.$$

Proposition VI.2.11 *Étant donnés des cycles* c *et* d *éléments de* $\mathcal{S}_n$, *s'il existe* $u \in \mathcal{S}_n$ *tel que* $d \;=\; u\circ c\circ u^{-1}$, *(autrement dit si* c *et* d *sont conjugués (cf. V.3.3,)) alors*

$$\mathrm{Supp}(d) \;=\; u\big(\mathrm{Supp}(c)\big)$$

et si l'on peut écrire

$$c \;=\; (a_1\dots a_\ell),$$

on a

$$d \;=\; (u(a_1)\dots u(a_\ell))\;.$$

Preuve *: Exercice.*

VI.3 . −Décomposition d'une permutation en produit de cycles

Dans tout ce paragraphe, un entier $n \in \mathbb{N}^*$ **est donné et on note** $\mathcal{S}_n$ **le groupe symétrique sur** n **éléments ;**

Proposition VI.3.1 *Pour tout élément* $s \in \mathcal{S}_n$, $s \neq \mathrm{Id}$, *il existe un entier* $d \;\geq\; 1$ *et des cycles* $c_{i\ ,1\leq i\leq d} \in \mathcal{S}_n$, *de supports deux à deux disjoints et tels que*

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

Preuve : *Puisque $s \neq \mathrm{Id}$, s possède au moins une orbite non triviale. Notons $O_{i\ ,1\leq i\leq d}$ les orbites non triviales de s. Les $O_{i\ ,1\leq i\leq d}$ étant des classes d'équivalence (cf. VI.2.3.i).) elles sont deux à deux disjointes.*

Pour tout $1 \leq i \leq d$ notons c_i la permutation dont la restriction à O_i est la restriction de s à O_i et la restriction au complémentaire de O_i est l'identité.

Il est alors clair que c_i est un cycle et que

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

Proposition VI.3.2 *Pour tout élément $s \in \mathcal{S}_n$, s'il existe des entiers naturels d et d' des cycles $c_{i\ ,1\leq i\leq d} \in \mathcal{S}_n$, et $c'_{i\ ,1\leq i\leq d'} \in \mathcal{S}_n$ tels que pour tout (i,j) $i \neq j$, les supports de c_i et c_j (resp. c'_i et c'_j) sont disjoints et*

$$s = \prod_{i=1}^{d} c_i = \prod_{i=1}^{d'} c'_i \ ,$$

alors $d = d'$ et il existe une permutation $u \in \mathcal{S}_d$ telle que $c_i = c'_{u(i)}$.

Preuve : *On démontre ce résultat par récurrence sur le maximum $\max(d,d')$.*

i) *($\max(d,d') = 1$)*
Si $\max(d,d') = 1$, on a $s = c_1 = c'_1$, ce qui donne immédiatement le résultat.

ii) *($\max(d,d') > 1$)*
Si $m := \max(d,d')$ est supérieur à 1, posons

$$s = \prod_{i=1}^{d} c_i \text{ et } s' = \prod_{i=1}^{d'} c'_i$$

avec $s = s'$. Soit a un élément du support de c_1. Alors, $c_1(a) \neq a$ et, par conséquent, $s(a) = c_1(a) \neq a$. Il en résulte que $s'(a) = s(a) \neq a$. Il existe donc un entier $1 \leq i \leq d'$ tel que $s'(a) = c'_i(a) \neq a$. On a encore

$$c_1(a) = s(a) = s'(a) = c'_i(a)$$

d'où l'on déduit que, pour tout $k \in \mathbb{Z}$, $c_1^k(a) = c_i'^k(a)$ d'où il résulte que

$$\{c_1^k(a)\ ,\ k \in \mathbb{Z}\} = \{c_i'^k(a)\ ,\ k \in \mathbb{Z}\}$$

c'est-à-dire

$$O_{c_1}(a) = O_{c'_i}(a) \ .$$

On en déduit aussi que, pour tout $x \in O_{c_1}(a) = O_{c'_i}(a)$, $c_1(x) = c'_i(x)$ *c'est-à-dire finalement, que* $c_1 = c'_i$.

L'égalité $s = s'$ *implique donc que*

$$\prod_{j=2}^{d} c_j = \prod_{1 \leq j \leq d' \, j \neq i} c'_j \, .$$

On a alors $\max(d-1, d'-1) = m-1$ *et l'on peut appliquer l'hypothèse de récurrence.*

Proposition VI.3.3 *Toute permutation* $s \in \mathcal{S}_n$, *s'écrit comme un produit de transpositions.*

Preuve : *Cet énoncé est une conséquence des propositions VI.3.1 et VI.2.9.*

Définition VI.3.4 Pour tout entier naturel $n \geq 1$ et toute permutation $s \in \mathcal{S}_n$ différente de l'identité, on peut écrire

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

où d est uniquement déterminé par s et où les c_i sont des cycles à supports deux à deux disjoints.

On peut également choisir une numérotation des c_i telle que, si λ_i désigne la longueur de c_i on ait, pour tout $1 \leq i < d$ $\lambda_i \leq \lambda_{i+1}$. On appelle alors le d-uplet $(\lambda_1, \ldots, \lambda_d)$ le *type cyclique* de s.

On pourra fixer, par convention, que le type cyclique de l'identité est $\emptyset$.

Proposition VI.3.5 *Étant donnés deux éléments* s_1 *et* s_2 *du groupe symétrique* $\mathcal{S}_n$, *les assertions suivantes sont équivalentes :*

a) s_1 *et* s_2 *sont conjugués (cf. V.3.3 ;)*

b) s_1 *et* s_2 *ont le même type cyclique.*

Preuve :

i) Remarquons que la classe de conjugaison de l'identité ne contient que l'identité et que c'est la seule permutation dont le type cyclique est $\emptyset$. *On peut donc, dans la suite, ne considérer que des permutations différentes de l'identité.*

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

Supposons qu'il existe $u \in \mathcal{S}_n$ *tel que* $s_2 = u \circ s_1 \circ u^{-1}$. *Si* $s_1 = \prod_{i=1}^{d} c_i$,

$$\begin{aligned} s_2 &= u \circ s_1 \circ u^{-1} \\ &= u \circ (\prod_{i=1}^{d} c_i) \circ u^{-1} \\ &= \prod_{i=1}^{d} u \circ c_i \circ u^{-1} \end{aligned}$$

ce qui prouve, en utilisant le théorème VI.2.10 que s_1 *et* s_2 *ont même type cyclique.*

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

Réciproquement, si l'on suppose que s *et* s' *ont même type cyclique, il existe un entier naturel* $d \geq 1$ *des cycles* $c_{i\ ,1\leq i\leq d}$ *et* $c'_{i\ ,1\leq i\leq d}$ *tels que les* c_i, *(resp. les* c'_i*) sont à supports deux à deux disjoints,*

$$s = \prod_{i=1}^{d} c_i \ , \ s' = \prod_{i=1}^{d} c'_i$$

et pour tout $1 \leq i \leq d$ c_i *et* c'_i *ont même longueur. D'après le théorème VI.2.10, il existe des éléments* $u_{i\ ,1\leq i\leq d} \in \mathcal{S}_n$ *tels que* $c'_i = u_i \circ c_i \circ u_i^{-1}$ *pour tout* $1 \leq i \leq d$.

Définissons u *de la manière suivante : Pour tout* $1 \leq i \leq d$ *la restriction de* u *au support de* c_i *est la restriction de* u_i *au support de* c_i. *Le complémentaire* E *de la réunion des supports des* c_i *est un ensemble dont le cardinal est égal au cardinal du complémentaire* E' *de la réunion des supports des* c'_i. *Il existe donc une bijection* $v : E \cong E'$. *On définit donc la restriction de* u *à* E *par* v.

On laisse alors le soin au lecteur de vérifier que

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

Proposition VI.3.6 *L'ordre d'une permutation* s *de type cyclique* $(\lambda_1, \ldots, \lambda_d)$ *est le* ***Ppcm*** *des* λ_i.

Preuve *: (cf. TD n° VI, exercice F, question 1),) (cf. TD n° VI, exercice F, question 1), b).)*

i) Si s *est de type cyclique* $(\lambda_1, \ldots, \lambda_d)$, *il existe des cycles* $c_{i\ ,1\leq i\leq d}$ *de longueur respective* λ_i, *à supports deux à deux disjoints et tels que*

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

Notons $m := [\lambda_1, \ldots, \lambda_d]$ *le* ***Ppcm*** *des* λ_i. *Par définition,* $\lambda_i | m$, *pour tout* $1 \leq i \leq d$ *donc* $c_i^m = \mathrm{Id}$. *les* c_i *sont à support deux à deux disjoints, pour tout* $1 \leq i \leq j \leq d$, $c_i c_j = c_j c_i$ *(cf. VI.1.10,) et, par conséquent,*

$$\begin{aligned} s^m &= (\prod_{i=1}^{d} c_i)^m \\ &= \prod_{i=1}^{d} (c_i^m) \\ &= \mathrm{Id} \end{aligned}$$

d'où il résulte que l'ordre de s *divise* m.

ii) Réciproquement, pour tout $k \in \mathbb{Z}$, $s^k = \mathrm{Id}$ *si et seulement si pour tout* $x \in [1; n]$, $s^k(x) = x$. *En particulier, s'il existe* $1 \leq i \leq d$ *tel que* x *soit dans le support de* c_i, *pour tout* $j \neq i, c_j(x) = x$. *Il en résulte que* $s^k(x) = c_i^k(x)$. *Si* $s^k(x) = x$ *alors nécessairement* $c_i^k(x) = x$ *et ce pour tout* x *dans le support de* c_i *ce qui signifie que* $c_i^k = \mathrm{Id}$ *autrement dit que l'ordre* λ_i *de* c_i *divise* k. *En bref,* $s^k = \mathrm{Id}$ *implique que* k *est divisible par chacun des* λ_i *c'est-à-dire divisible par* m *c'est-à-dire que* m *divise l'ordre de* s.

VI.4 . −Signature et groupe alterné

Dans tout ce paragraphe (VI.4,) un entier $n \in \mathbb{N}^*$ **est donné et** $\mathcal{S}_n$ **est le groupe symétrique sur** n **éléments.**

Définition VI.4.1 Soient $s \in \mathcal{S}_n$ une permutation :

i) On note $\nu(s)$ le nombre d'orbites (cf. VI.2.3.i)) de s.
Ainsi, pour tout cycle c de longueur l, $\nu(c) = n - l + 1$ en particulier, pour une transposition t, $\nu(t) = n - 1$.

ii) On appelle *signature* de s et l'on note $\sigma(s)$ l'entier $(-1)^{n-\nu(s)}$ appartenant à $\{-1; 1\}$.

Exemple VI.4.2 a) L'identité ayant exactement n orbites toutes triviales, $\sigma(\mathrm{Id}) = 1$.

b) Si $t \in \mathcal{S}_n$ est une transposition, $\nu(t) = n - 1$ et par conséquent, $\sigma(t) = -1$.

c) Si c est un 3-cycle, $\nu(c) = n - 3 + 1 = n - 2$, d'où $\sigma(c) = 1$.

d) Si s est une permutation circulaire (cf. VI.2.3.iv),) $\sigma(s) = (-1)^{n-1}$.

Proposition VI.4.3 *Pour tout* $(n,p) \in \mathbb{N}\times\mathbb{N}$, *notons*

$$\sigma_n : \mathcal{S}_n \to \{-1,1\} \text{ (resp. } \sigma_{n+p} : \mathcal{S}_{n+p} \to \{-1,1\}\text{)}$$

l'application signature définie en VI.4.1.ii).

Si

$$\widetilde{i_{n,p}} : \mathcal{S}_n \to \mathcal{S}_{n+p}$$

désigne l'application définie en l'injection naturelle (cf. VI.1.3,) on a

$$\sigma_{n+p} \circ \widetilde{i_{n,p}} = \sigma_n .$$

Preuve *: Rappelons que* $\widetilde{i_{n,p}}$ *associe à toute permutation* $s \in \mathcal{S}_n$ *la permutation* $\widetilde{i_{n,p}}(s) \in \mathcal{S}_{n+p}$ *définie par :*

$$\forall 1 \le i \le n,\ \widetilde{i_{n,p}}(s)(i) = s(i)\ ,\ \forall n+1 \le i \le p,\ \widetilde{i_{n,p}}(s)(i) = i\ .$$

Il s'ensuit alors que :

$$\begin{array}{lrcl} \forall s\in\mathcal{S}_n, & \nu(\widetilde{i_{n,p}}(s)) & = & \nu(s)+p \\ \Rightarrow & \sigma_{n+p}(\widetilde{i_{n,p}}(s)) & = & (-1)^{n+p-\nu(\widetilde{i_{n,p}}(s))} \\ & & = & (-1)^{n+p-(\nu(s)+p)} \\ & & = & (-1)^{n-\nu(s)} \\ & & = & \sigma_n(s)\ . \end{array}$$

Proposition VI.4.4 *Pour toute permutation* $s \in \mathcal{S}_n$, *et toute transposition* $t \in \mathcal{S}_n$,

$$\sigma(s\circ t) = -\sigma(s) = \sigma(s)\sigma(t)\ .$$

Preuve *: Il existe des éléments* a *et* b *de* $[1;n]$ *distincts tels que* $t = (ab)$. *On est amené à considérer les deux situations suivantes :*

i) $(O_s(a) = O_s(b))$

Supposons que $O_s(a) = O_s(b)$ *et notons* $\lambda := \#(O_s(a))$. *Notons* c *l'élément de* $\mathcal{S}_n$ *dont la restriction à* $O_s(a)$ *est celle de* s *et la restriction au complémentaire de* $O_s(a)$ *est l'identité. Il est dès lors clair que* c *est un cycle de support* $O_s(a) = O_c(a)$ *et de longueur* λ. *Il est par conséquent, en vertu du théorème VI.2.7 d'ordre* λ. *Soit*

$$\overline{p} : \mathbb{Z}/\lambda\mathbb{Z} \to O_c(a)\ ,\ \overline{k} \mapsto c^k(a)$$

la bijection définie comme en VI.2.6.iv).1. Notons $\alpha \in [0; \lambda - 1]$ *l'unique entier tel que* $c^\alpha(a) = b$ *. On peut en fait prendre* $\alpha \in [1; \lambda - 1]$ *puisque* $a \neq b$*. Il existe alors un unique* $\beta \in [1; \lambda - 1]$ *tel que* $c^\beta(a) = b$ *et l'on a*

$$\alpha + \beta = \lambda .$$

Cherchons maintenant à déterminer l'orbite $O_{sot}(a)$*. On a tout d'abord,*

$$s \circ t(a) = s(b) = s^{\alpha+1}(a) = c^{\alpha+1}(a) .$$

Pour tout $1 \leq i < \beta$*, on a*

$$c^{\alpha+i}(a) \neq a \text{ et } c^{\alpha+i}(a) \neq b .$$

En effet, $c^{\alpha+i}(a) = a$ *impliquerait* $\lambda | \alpha + i$ *or* $0 < \alpha + i < \lambda$ *ce qui est donc impossible. D'autre part,* $c^{\alpha+i}(a) = b$ *impliquerait* $c^i(a) = a$ *c'est-à-dire* $\lambda | i$ *qui est encore impossible puisque* $0 < i < \beta < \lambda$*.*

Il en résulte que, pour tout $1 \leq i < \beta, t(c^{\alpha+i}(a)) = c^{\alpha+i}(a)$ *c'est-à-dire que*

$$s \circ t(c^{\alpha+i}(a)) = s(c^{\alpha+i}(a)) = s^{\alpha+i+1}(a) .$$

On en déduit que

$$O_{sot}(a)) = \left\{ s^{\alpha+i}(a) \, , \; 1 \leq i \leq \beta \right\} \subset O_s(a) \qquad 1$$

d'où il résulte, en particulier, que

$$\#(O_{sot}(a)) = \beta . \qquad 2$$

On montre de même que

$$O_{sot}(b) = \left\{ c^i(a) \, , \; 1 \leq i \leq \alpha \right\} \subset O_s(a) \qquad 3$$

d'où il résulte, en particulier, que

$$\#(O_{sot}(b)) = \alpha . \qquad 4$$

Il résulte de ce qui précède que

$$O_{sot}(a) \cap O_{sot}(b) = \emptyset$$

et que, par conséquent,

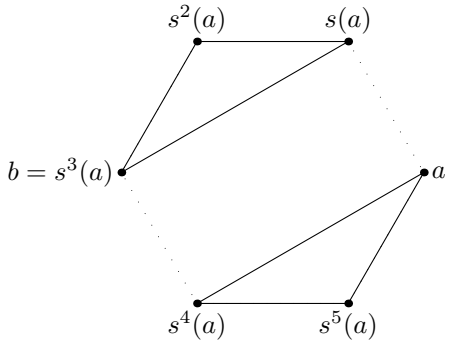
$$\#(O_{sot}(a) \cup O_{sot}(b)) = \#(O_{sot}(a)) + \#(O_{sot}(b)) = \alpha + \beta = \#(O_s(a)) .$$

On en déduit finalement que

$$O_{s\circ t}(a) \cup O_{s\circ t}(b) = O_s(a) .$$

Dans le dessin ci-après, on a représenté le cas particulier où

$$\lambda = 6 \text{ et } \alpha = \alpha = 3 :$$



Comme, par ailleurs, pour tout $x \notin O_s(a)$, $t(x) = x$, *donc* $s \circ t(x) = s(x)$ *et par conséquent,* $O_{s\circ t}(x) = O_s(x)$. *On en déduit donc que*

$$\nu(s \circ t) = \nu(s) + 1 . \qquad 5$$

ii) $(O_s(a) \neq O_s(b))$

Supposons à présent que $O_s(a) \neq O_s(b)$. *On a alors bien évidemment* $O_s(a) \cap O_s(b) = \emptyset$. *Notons*

$$\alpha := \#(O_s(a)) \text{ et } \beta := \#(O_s(b))$$

et cherchons à déterminer $O_{s\circ t}(a)$. *Tout d'abord,* $s \circ t(a) = s(b)$ *et*

$$\begin{array}{rl} & \forall 1 \leq i < \beta \quad , \quad s^i(b) \in O_s(b), s^i(b) \neq b, s^i(b) \neq a \\ \Rightarrow & \forall 1 \leq i < \beta \quad , \quad t(s^i(b)) = s^i(b) \\ \Rightarrow & \forall 1 \leq i < \beta \quad , \quad s \circ t(s^i(b)) = s^{i+1}(b) . \end{array}$$

De plus

$$s \circ t(s^\beta(b)) = s \circ t(b) = s(a) .$$

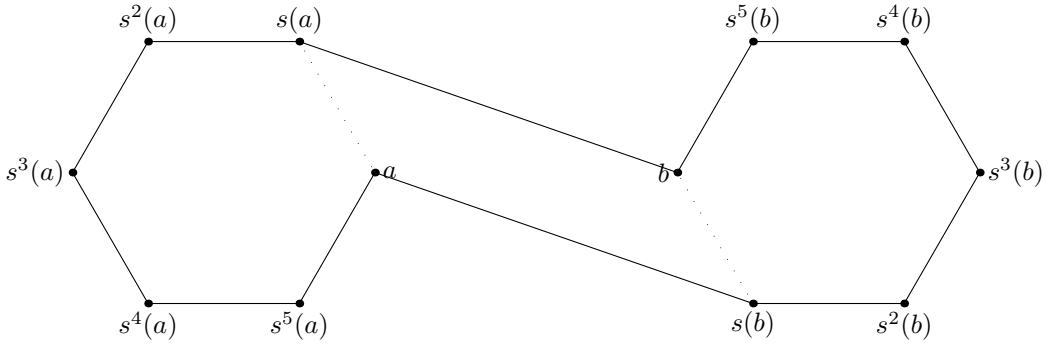
D'où :

$$\begin{array}{rl} & \forall 1 \leq i < \alpha \quad , \quad s^i(a) \in O_s(a), s^i(a) \neq a, s^i(a) \neq b \\ \Rightarrow & \forall 1 \leq i < \alpha \quad , \quad t(s^i(a)) = s^i(a) \\ \Rightarrow & \forall 1 \leq i < \alpha \quad , \quad s \circ t(s^i(a)) = s^{i+1}(a) . \end{array}$$

On en déduit que

$$O_{s\circ t}(a) = O_s(a) \cup O_s(b) = O_{s\circ t}(b) .$$

On a représenté, sur le dessin ci-après la situation pour $\alpha = \beta = 6$:



Comme, par ailleurs, pour tout $x \notin O_s(a) \cup O_s(b)$ $t(x) = x$ *et par conséquent,* $O_{s\circ t}(x) = O_s(x)$, *on a :*

$$\nu(s \circ t) = \nu(s) - 1 \,. \qquad 1$$

Corollaire VI.4.5 *Pour tout* $n \geq 1$, *la signature* σ *est un morphisme du groupe symétrique* $\mathcal{S}_n$ *dans le groupe*

$$(\mathbb{Z}^\times, *) = (\{-1, 1\}, *) \cong \mathbb{Z}/2\mathbb{Z}$$

des éléments inversibles de $\mathbb{Z}$.

Preuve : *Il découle immédiatement de la définition de* σ *(cf. VI.4.1.ii),) que* σ *est à valeurs dans* $\{-1, 1\}$.

Pour $n = 1$, *on a* $\sigma(\mathrm{Id}) = 1$ *(cf. VI.4.2) ce qui prouve que* σ *est bien un morphisme.*

Pour $n \geq 2$, *soit* (s_1, s_2) *un couple d'éléments de* $\mathcal{S}_n$. *Si* $s_2 \neq \mathrm{Id}$, *il existe un entier* $d \geq 0$ *et des transpositions* $t_{i\,,1\leq i\leq d+1} \in \mathcal{S}_n$, *tels que* $s_2 = \prod_{i=1}^{d+1} t_i$ *(cf. VI.3.3.) On a alors*

$$\sigma(s_1 s_2) = \sigma(s_1 \prod_{i=1}^{d} t_i t_{d+1}) = \sigma(s_1 \prod_{i=1}^{d} t_i)\sigma(t_{d=1})$$

en appliquant la proposition VI.4.4. En faisant une hypothèse de récurrence convenable indexée par l'entier d *on a*

$$\sigma(s_1 s_2) = \sigma(s_1)\sigma(\prod_{i=1}^{d} t_i)\sigma(t_{d+1}) = \sigma(s_1)\sigma(\prod_{i=1}^{d+1} t_i)$$

la dernière égalité résultant encore de la proposition VI.4.4. Il en résulte que

$$\sigma(s_1 s_2) = \sigma(s_1)\sigma(s_2) \,.$$

Définition VI.4.6 i) (**Groupe alterné**)
Pour tout entier $n \geq 1$, on appelle *groupe alterné* et on note $\mathcal{A}_n$, le noyau de σ

ii) (**Permutations paires/impaires**)
On dit qu'un élément du groupe alterné $\mathcal{A}_n$ est une *permutation paire* tandis qu'un élément du complémentaire de $\mathcal{A}_n$ dans $\mathcal{S}_n$ est une *permutation impaire*.

Exemple VI.4.7 Une transposition est une permutation impaire, tandis qu'un 3-cycle est une permutation paire. Plus généralement, pour tout entier naturel k, un $2k$-cycle est une permutation impaire tandis qu'un $2k+1$-cycle est une permutation paire.

Proposition VI.4.8 (Propriétés du groupe alterné) *i) Pour tout entier naturel $n \geq 1$, le groupe alterné $\mathcal{A}_n$ est un sous-groupe distingué du groupe symétrique $\mathcal{S}_n$.*

ii) Pour $n \geq 2$, le quotient $\mathcal{S}_n/\mathcal{A}_n$ (cf. V.5.2) est isomorphe au groupe $\mathbb{Z}/2\mathbb{Z}$ et, par conséquent,

$$\#\big(\mathcal{A}_n\big) \;=\; \frac{\#\big(\mathcal{S}_n\big)}{2} \;=\; \frac{n!}{2}\,.$$

iii) Pour tout $(n,p) \in \mathbb{N}\times\mathbb{N}$, le morphisme de groupes

$$\widetilde{i_{n,p}} \;:\; \mathcal{S}_n \;\to\; \mathcal{S}_{n+p}$$

(cf. VI.1.3,) se restreint en un morphisme injectif encore noté

$$\widetilde{i_{n,p}} \;:\; \mathcal{A}_n \;\to\; \mathcal{A}_{n+p}\,.$$

***Preuve** :*

i) Comme $\mathcal{A}_n \;=\; \mathrm{Ker}\,\sigma$, on peut se rapporter au résultat V.4.10.

ii) Pour $n \geq 2$, $\mathcal{S}_n$ contient des transpositions et, par conséquent, σ à valeurs dans $\{-1;1\}$ est surjective (cf. VI.4.2.)
Par la proposition V.5.4on a un isomorphisme

$$\mathcal{S}_n/\mathcal{A}_n \;\cong\; (\{-1;1\},*)$$

ce dernier groupe étant canoniquement isomorphe à $(\mathbb{Z}/2\mathbb{Z},+)$.
Finalement, la relation entre les cardinaux de $\mathcal{A}_n$ et $\mathcal{S}_n$ est obtenue à partir de V.6.4.

iii) C'est une conséquence immédiate de la proposition VI.4.3.

VI.5 . −Exercices

Exercice VI.5.1 [Introduction au groupe symétrique]

1) () Étant donné un ensemble E,
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.

On suppose désormais que E est fini et non vide c'est-à-dire qu'il existe une bijection

$$\iota \,:\, E \,\cong\, [1;n]\,,\; n \,\in\, \mathbb{N}^*\,.$$

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 $n \,\geq\, 0$. On définit sur $\mathcal{S}_{n+1}$ la relation binaire R par

$$s\,R\,t \;\Leftrightarrow\; s(n+1) \,=\, t(n+1)\,.$$

4) () Montrer que R ainsi définie est une relation d'équivalence.

5) () Rappeler pourquoi l'ensemble $\mathcal{S}_{n+1}/R$ des classes d'équivalences selon R forme une partition de $\mathcal{S}_{n+1}$.

6) () Montrer que pour tout $s \,\in\, \mathcal{S}_{n+1}$ il existe une bijection entre la classe $\overline{s}$ de s selon R et $\mathcal{S}_n$.
Indication : *On pourra chercher à construire explicitement une bijection $\phi \,:\, \overline{s} \,\to\, \mathcal{S}_n$ en considérant, pour tout $t \,\in\, \overline{s}$, $s^{-1} \circ t$, ainsi que sa bijection réciproque $j\psi \,:\, \mathcal{S}_n \,\to\, \overline{s}$.*

7) () À quelle condition (nécessaire et suffisante) la classe $\overline{s}$ d'un élément de $\mathcal{S}_{n+1}$ est-elle un sous-groupe de $\mathcal{S}_{n+1}$? Caractériser ce sous-groupe.

8) () Montrer que l'application

$$\nu \,:\, \mathcal{S}_{n+1} \,\to\, [1;n+1]\,,\; s \,\mapsto\, s(n+1)\,.$$

est surjective.

9) () Montrer qu'il existe une bijection

$$\overline{\nu} \ : \ \mathcal{S}_{n+1}/R \ \to \ [1; n+1] \text{ telle que } \forall s \in \mathcal{S}_{n+1}, \ \nu(s) \ = \ \overline{\nu}(\overline{s}) \ .$$

10) () 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.

Exercice VI.5.2 [] Faire la preuve de la proposition VI.1.3.

VII . −Anneau, morphisme . . .

VII.1 . −Anneau

Définition VII.1.1 (Anneau) Un *anneau* est un triplet $(A, +, *)$ (le plus souvent noté $A,)$ tel que :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Remarque VII.1.2 On aurait pu formuler les axiomes VII.1.1.Ann$_2$) et VII.1.1.Ann$_3$) en disant que $(A, *)$ est un magma associatif possédant un élément neutre (cf. I.6.)

Exemple VII.1.3 Un exemple fondamental qui entrera dans un certain nombre de constructions que nous allons envisager, est constitué par l'anneau $(\mathrm{End}_{\mathbf{Gr}}(G), +, \circ)$ où $(G, +)$ est un groupe abélien. Plus précisément :

Proposition VII.1.4 *Soit* $(G, +)$ *un groupe abélien (cf. III.1.3.)*

i) L'ensemble $\mathrm{End}_{\mathbf{Gr}}(G) \;=\; \mathrm{Hom}_{\mathbf{Gr}}(G, G)$ *est un sous-groupe du groupe* G^G *(cf. III.1.6.)*

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

Preuve *:*

VII.1.1.Ann$_1$) Le point i) assure que $(\mathrm{End}_{\mathbf{Gr}}(G), +)$ *est un groupe abélien si bien que l'axiome VII.1.1.Ann$_1$) est vérifié.*
Par ailleurs, si f *et* g *sont deux éléments de* $\mathrm{End}_{\mathbf{Gr}}(G)$, $f \circ g$ *est un élément de* $\mathrm{End}_{\mathbf{Gr}}(G)$ *si bien que* $\circ$ *définit bien une loi interne sur* $\mathrm{End}_{\mathbf{Gr}}(G)$. *Reste donc à vérifier les axiomes :*

VII.1.1.Ann$_2$) C'est un résultat connu concernant les applications que la loi $\circ$ *est associative.*

VII.1.1.Ann$_3$) L'élément $\mathrm{Id}_G \in \mathrm{End}_{\mathbf{Gr}}(G)$ *vérifie*

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

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

VII.1.1.Ann$_4$) Étant donnés trois éléments f, g, h *de* $\mathrm{End}_{\mathbf{Gr}}(G)$, *pour tout* $x \in G$,

$$\begin{aligned}
[h \circ (f +_{\mathrm{End}_{\mathbf{Gr}}(G)} g)](x) &= h[(f +_{\mathrm{End}_{\mathbf{Gr}}(G)} g)(x)] \\
&= h[f(x) +_G g(x)] \\
&= h[f(x)] +_G h[g(x)] \\
&= (h \circ f)(x) +_G (h \circ g)(x) \\
&= [(h \circ f) +_{\mathrm{End}_{\mathbf{Gr}}(G)} (h \circ g)](x) \,;
\end{aligned}$$

et

$$\begin{aligned}[(f +_{\mathrm{End}_{\mathbf{Gr}}(G)} g) \circ h](x) &= (f +_{\mathrm{End}_{\mathbf{Gr}}(G)} g)[h(x)] \\ &= (f[h(x)] +_G f[g(x)] \\ &= (f \circ h)(x) +_G (f \circ g)(x) \\ &= [(f \circ h) +_{\mathrm{End}_{\mathbf{Gr}}(G)} (f \circ g)](x) \, .\end{aligned}$$

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

Définition VII.1.5 (Anneau commutatif) Étant donné un anneau $(A, +, *)$, si

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

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

Exemple VII.1.6 a) L'ensemble $\mathbb{Z}$ des entiers relatifs étudié au chapitre IV, muni de ses opérations $+$ et $*$ est un anneau commutatif.

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

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

alors

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

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

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

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

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

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

et de la multiplication :

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

n'est pas un anneau au sens de la définition VII.1.1. En effet, $\mathcal{C}$ ne possède pas d'élément neutre pour la multiplication $*$ et ne vérifie donc pas l'axiome VII.1.1.Ann$_3$).

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

Les propositions I.6.13 et III.1.4 s'étendent encore au cas des anneaux. On peut en effet remarquer qu'un anneau est un magma à la fois pour sa loi d'addition $+$ ainsi que pour sa loi de multiplication $*$ si bien que :

Proposition VII.1.7 (Propriétés) *Soient $(A,+,*)$ un Anneau. Le couple $(A,+)$ est en particulier un groupe abélien si bien que :*

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

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

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

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

Définition VII.1.8 (Élément inversible) Tous les éléments d'un anneau A différents de 0_A ne possédant pas nécessairement un inverse pour la loi $*$, on notera $A^\times$ l'ensemble des éléments de A *inversibles* pour $*$ *i.e.* ceux qui possèdent un inverse. On appelle parfois également *unité* un élément de $A^\times$.

Proposition VII.1.9 *Si A est un anneau (resp. un anneau commutatif) $(A^\times,*)$ est un groupe (resp. un groupe abélien.)*

Preuve *: (cf. VII.8.1.)*

Exemple VII.1.10 a) Le groupe $(\mathbb{Z}^\times,*)$ des inversibles de $\mathbb{Z}$ est $(\{-1,1\},*)$ (cf. IV.3.13,) 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 VII.1.11 (Anneau intègre) Si $(A, +, *)$ est un anneau tel que

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

on dit que A est un anneau *intègre*.

Exemple VII.1.12 a) Un corps (cf. VII.1.13) est une $\mathbb{Z}$-algèbre (un anneau) intègre.

b) L'anneau $(\mathbb{Z}, +, *)$ est intègre.

c) L'anneau $K[X]$ (cf. VIII) est intègre.

d) Si E est un K-espace vectoriel ? l'anneau $\mathrm{End}(E)$ (cf. VII.1.4) des endomorphismes de E n'est pas intègre.

Définition VII.1.13 (Corps) Un anneau commutatif $(A, +, *)$ est un *corps* si tous les éléments de A différents de 0_A possèdent un inverse pour la loi $*$; *i.e.* $A^\times\ =\ A\ \setminus\ \{0_A\}$.

Remarque VII.1.14 Un corps est un anneau intègre mais la réciproque est fausse. En effet l'anneau $(\mathbb{Z}, +, *)$ est intègre mais n'est pas un corps.

Exemple VII.1.15 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.

Les propositions I.6.20 et III.1.6 ont leur pendant pour les anneaux :

Proposition VII.1.16 *Étant donnés un anneau $(A, +, *)$ et un ensemble E, l'ensemble A^E des applications de E dans A muni des lois induites (cf. I.6.20,) est un anneau (commutatif si A l'est.)*

Preuve *: (cf. VII.8.3.)*

VII.2 . −Morphismes, isomorphismes

Définition VII.2.1 (Morphisme d'anneaux) Une application

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

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

Ann_5) $f\ :\ (A, +_A)\ \to\ (B, +_B)$ est un morphisme de groupes (cf. III.2.1.)

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

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

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

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

On a l'exact analogue des lemmes I.6.3 et III.2.3 :

Lemme VII.2.2 *i) Pour tout anneau $(A, +, *)$ l'identité Id_A est un morphisme de l'anneau A dans lui-même.*

ii) Pour A, B et C des anneaux, $f \;:\; A \;\to\; B$ et $g \;:\; B \;\to\; C$ des morphismes, le composé $g \circ f$ est un morphisme.

On peut donc donner une définition analogue aux définitions I.6.4 et III.2.4 :

Définition VII.2.3 (Isomorphisme) Étant donnés deux anneaux $(A, +, *)$ et $(B, +, *)$, un morphisme $f \;:\; A \;\to\; B$ est un *isomorphisme* s'il existe un morphisme

$$g \;:\; B \;\to\; A \text{ tel que } g \circ f \;=\; \mathrm{Id}_B \text{ et } f \circ g \;=\; \mathrm{Id}_A\,.$$

On notera $\mathrm{Isom}_{\mathbf{Ann}}(A, B)$ (ou simplement $\mathrm{Isom}(A, B)$ si le contexte est clair) l'ensemble des isomorphismes de A dans B.

On a encore, sans surprise puisqu'en fait l'axiomatique n'est pas vraiement différente, un analogue des propositions I.6.5 et III.2.5 :

Proposition VII.2.4 *Étant donnés deux anneaux A et B, une application $f \;:\; A \;\to\; B$ est un isomorphisme si et seulement si c'est un morphisme bijectif.*

Preuve *: Comme précédemment, si f est un isomorphisme c'est en particulier un morphisme bijectif.*

Réciproquement si f est un morphisme bijectif, il résulte de la proposition III.2.5 que son application réciproque $g \;:\; B \;\to\; A$ est un morphisme du groupe $(B, +)$ dans le groupe $(A, +)$ ce qui assure que g vérifie VII.2.1.Ann$_5$).

En outre il résulte de la proposition I.6.5 que g est un morphisme du magma $(B, *)$ dans le magma $(A, *)$ ce qui assure que g vérifie VII.2.1.Ann$_6$).

Enfin f vérifiant VII.2.1.Ann$_7$), $f(1_A) \;=\; 1_B$ d'où

$$1_A \;=\; g[f(1_A)] \;=\; g(1_B)$$

ce qui entraîne que g vérifie VII.2.1.Ann$_7$).

Des définitions analogues à I.6.6 et III.2.7 peuvent donc être données même si elles seront en fait moins utilisées au moins dans ce cours :

Définition VII.2.5 Soit $(A, +, *)$ un anneau.

i) (**Gndomorphismes**)
Un morphisme $f : A \to A$ de A dans lui-même est appelé *endomorphisme*. On note

$$\mathrm{End}_{\mathbf{Ann}}(A) \text{ (ou simplement } \mathrm{End}(A), \text{)}$$

l'ensemble des endomorphismes de A.

ii) (**Automorphisme**)
Un morphisme $f : A \to A$ est un *automorphisme* si c'est à la fois un isomorphisme et un endomorphisme. Il revient au même, grâce à la proposition VII.2.4, de dire que f est un endomorphisme bijectif. On note $\mathrm{Aut}_{\mathbf{Ann}}(A)$ (ou simplement $\mathrm{Aut}(A)$) l'ensemble des automorphismes de A.

Exemple VII.2.6 Pour un anneau A, l'identité Id_A est un automorphisme.

Lemme VII.2.7 *i) Pour tout morphisme d'anneaux $MorfAB$, la restriction $f^\times := f_{|A^\times}$ de f à $A^\times$ est un morphisme de groupes à valeurs dans $B^\times$.*

ii) Pour tout anneau A,

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

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

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

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

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

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

***Preuve** : Voir l'exercice VII.8.5.*

Proposition VII.2.8 *Pour tout anneau $(A, +, *)$ (pas nécessairement commutatif) il existe un unique morphisme d'anneau $\mathbb{Z} \to A$ appelé morphisme structural de A.*

Preuve *: S'il existe un morphisme d'anneaux $f : \mathbb{Z} \to A$, l'axiome VII.2.1.Ann$_7$) entraîne que*

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

Par ailleurs f étant, en particulier un morphisme de groupes de $(\mathbb{Z}, +)$ dans $(A, +)$, $f(0) = 0_A$, pour tout $n \in \mathbb{N}$,

$$f(n+1) = f(n) + f(1) = f(n) + 1_A \text{ et } f(-n) = -f(n) .$$

Il s'ensuit que f est nécessairement le morphisme de groupes ϵ_1 défini au Problème n° III, exercice A.

L'application f est donc déjà un morphisme de groupes pour les structures additives qui, de plus, vérifie l'axiome VII.2.1.Ann$_7$). Ne reste donc qu'à montrer que f satisfait l'axiome VII.2.1.Ann$_6$).

Pour tout $q \in \mathbb{Z}$,

$$f(0 * q) = f(0) = 0_A = 0_A * f(q) = f(0) * f(q) .$$

Par ailleurs pour tout $p \in \mathbb{N}$, et tout $p \in \mathbb{Z}$, si l'on ssupose que $f(p * q) = f(p) * f(q)$, alors :

$$\begin{aligned} f((p+1) * q) &= f(p * q + q) \\ &= f(p * q) + f(q) \\ &= (f(p) + 1_A) * f(q) \\ &= f(p+1) * f(q) \end{aligned}$$

et

$$\begin{aligned} f(-(p) * q) &= f(-(p * q)) \\ &= -f(p) * f(q) \\ &= f(-p) * f(q) ; \end{aligned}$$

ce qui montre le résultat par récurrence.

VII.3 . −Sous

Définition VII.3.1 (Sous-annau) Étant donné un anneau $(A, +, *)$ un *sous-anneau* de A est une partie B de A telle que $1_A \in B$ et les restrictions respectives des lois $+$ et $*$ à B donnent à B une structure d'anneau.

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

Remarque VII.3.2 i) Notons que l'axiome VII.1.1.Ann$_1$) a en particulier pour conséquence que $(B,+)$ est un sous-groupe de $(A,+)$; ce qui entraîne, en particulier (cf. III.3.3,) que l'élément neutre 0_A de $(A,+)$ est aussi l'élément neutre de $(B,+)$ et que l'opposé d'un élément $x \in B$ est son opposé dans A.

ii) Notons que la condition $1_A \in B$, entraîne que 1_A est l'élément neutre pour la loi $*$ sur B (cf. I.8.16.question 1),) et que tout inversible dans B est inversible dans A et que son inverse dans B est encore son inverse dans A (cf. I.8.16.question 2).) Il s'ensuit que $(B^\times,*)$ est alors un sous-groupe de $(A^\times,*)$.

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

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

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

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

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

La condition $1_A \in B$ est à rapprocher de la condition VII.2.1.Ann$_7$) et donne sa cohérence à un énoncé comme la proposition VII.3.3.c).

Proposition VII.3.3 (Caractérisation des sous-anneaux) *Étant donnés un anneau*

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

une partie de A, les assertions suivantes sont équivalentes :

a) B est un sous-anneau au sens de la définition VII.3.1.

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

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

c) La restriction

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

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

Preuve : *Voir l'exercice VII.8.7.*

Exemple VII.3.4 L'anneau $\mathbb{Z}$ des entiers relatifs est un sous-anneau du corps $\mathbb{Q}$ des nombres rationnels, lui-même un sous-anneau du corps $\mathbb{R}$ des nombres réels, lui-même un sous-anneau du corps des nombres complexes $\mathbb{C}$.

Proposition VII.3.5 (Image directe/réciproque) *Soit $f : A \to B$ un morphisme d'anneaux.*

i) (***Image directe***)
Pour tout sous-anneau A' de A, l'image directe de A'

$$f(A') = \{y \in B \,;\, \exists x \in A', \ , \ y = f(x)\}$$

est un sous-anneau de B.

ii) (***Image réciproque***)
Pour tout sous-anneau B' de B, l'image réciproque

$$f^{-1}(B') = \{x \in A \,;\, f(x) \in B'\}$$

est un sous-anneau de A.

Définition VII.3.6 (Noyau/image) Étant donné un morphisme d'anneaux $f : A \to B$, 0_B étant l'élément neutre du groupe $(B, +)$, on appelle

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

$$\operatorname{Ker} f := f^{-1}(\{0\}_B) = \{x \in A \,;\, f(x) = 0_B\},$$

c'est-à-dire en fait le noyau du morphisme de groupes

$$f : (A, +) \to (B, +)$$

(cf. III.3.8.i),)

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

$$\operatorname{Im} f := f(A) = \{y \in B \,;\, \exists x \in A, \ , \ y = f(x)\}\,.$$

Corollaire VII.3.7 *Pour un morphisme d'anneaux $f : A \to B$, l'image de f est un sous-anneau de B.*

Proposition VII.3.8 *Un morphisme d'anneaux $f : A \to B$ est injectif (resp. surjectif) (cf. I.2.4.iii),) si et seulement si* $\mathrm{Ker}\, f = \{0_A\}$ *(resp.* $\mathrm{Im}\, f = B$.)

Remarque VII.3.9 Remarquons que le noyau d'un morphisme d'anneaux $f : A \to B$, n'est pas un sous-eanneau de A en général. En effet, si $\mathrm{Ker}\, f$ est un sous anneau de A, $1_A \in \mathrm{Ker}\, f$ si bien que $f(1_A) = 0_B$. Or, d'après l'axiome VII.2.1.Ann$_7$), $f(1_A) = 1_B$, si bien que $0_B = 1_B$, ce qui entraîne que $B = \{0\}$ qui est un cas très particulier.

Définition VII.3.10 Si $i : A \to B$ est un morphisme d'anneaux injectif, il induit un isomorphisme $A \cong \mathrm{Im}\, i$; si bien que A est isomorphe à un sous-anneau de B. On dira parfois même par abus de langage que A est lui-même un sous-anneau de B.

VII.4 . −Idéaux

Soit $(A, +, *)$ un anneau commutatif (cf. VII.1.5.) L'anneau $(\mathbb{Z}, +, *)$ (cf. IV,) en est un bon exemple. On notera $A^\times$ l'ensemble des éléments inversibles de A (cf. VII.1.8) et on rappelle que le couple $(A^\times, *)$ est un groupe, (resp. un groupe abélien si A est commutatif) (cf. VII.1.9.)

Définition VII.4.1 (Idéal) Étant donné un anneau commutatif $(A, +, *)$, une partie $\mathfrak{I} \subset A$ de A est un *idéal* si $\mathfrak{I}$ est un sous-groupe de $(A, +)$ tel que

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

Proposition VII.4.2 (Caractérisation des idéaux) *Une partie $\mathfrak{I}$ d'un anneau commutatif $(A, +, *)$ est un idéal de a si et seulement si $\mathfrak{I} \neq \emptyset$ et*

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

Preuve *: Voir l'exercice VII.8.9.*

Exemple VII.4.3 a) Les sous-ensembles $\{0\}$, et A de A sont des idéaux de A. Ce sont les seuls idéaux de A si A est un corps.

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

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

est un idéal de A.

c) Les idéaux de l'anneau $(\mathbb{Z}, +, *)$ sont exactement les sous-groupes du groupe $(\mathbb{Z}, +)$ c'est-à-dire les sous-ensemble de $\mathbb{Z}$ de la forme $d\mathbb{Z}$ avec $d \in \mathbb{Z}$ comme nous l'avons vu dans le corollaire IV.5.5.

Nombre des résultats établis pour les sous-groupes aux paragraphes III.3 et suivants ont leur analogue dans le cadre des idéaux. La proposition qui suit est à rapprocher de la proposition III.3.7 :

Proposition VII.4.4 *Soit*

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

un morphisme d'anneaux (cf. VII.2.1) (où $(B, +_B, *_B)$ est un anneau commutatif.) Pour tout idéal $\mathfrak{J}$ de B, $f^{-1}(\mathfrak{J})$ est un idéal de A.

***Preuve** : Puisque f est un morphisme d'anneaux, donc en particulier un morphisme de groupes $(A, +) \ \to \ (B, +_B)$, $f(0) \ = \ 0_B \ \in \ J$ si bien que $f^{-1}(J) \ \neq \ \emptyset$.*
Par ailleurs

$$\forall (x, y) \in f^{-1}(J) \times f^{-1}(J), \forall (a, b) \in A \times A, \ f(a*x+b*y) \ = \ f(a)*_B f(x)+_B f(b)*_B f(y) \ \in \ J$$

ce qui entraîne que $a * x + b * y \ \in \ f^{-1}(J)$ assurant que $f^{-1}(J)$ est un idéal.

Corollaire VII.4.5 *Avec les notations de la proposition VII.4.4, le noyau $\mathrm{Ker}\, f$ du morphisme f est un idéal de A.*

***Preuve** : En effet, $\mathrm{Ker}\, f \ = \ f^{-1}(\{0\})$.*

;

On a, pour les idéaux d'un anneau A, l'exact analogue de la proposition III.3.6 pour les sous-groupes.

Proposition VII.4.6 (Propriétés des idéaux) *Étant donnés deux idéaux*

$$\mathfrak{I} \ \subset \ A \, \text{et} \, \mathfrak{J} \ \subset \ A \ :$$

i) $\mathfrak{I} \cap \mathfrak{J}$ *est un idéal de* A ;

Preuve : *Comme* $\mathfrak{I}$ *et* $\mathfrak{J}$ *sont en particulier des sous-groupes de* $(A,+)$, $0 \in \mathfrak{I} \cap \mathfrak{J}$ *si bien que* $\mathfrak{I} \cap \mathfrak{J} \neq \emptyset$. *Par ailleurs,*

$$\begin{array}{ll} \forall (x,y) \in (\mathfrak{I} \cap \mathfrak{J}) \times (\mathfrak{I} \cap \mathfrak{J}), & \\ \forall (a,b) \in A \times A, & (x,y) \in \mathfrak{I} \times \mathfrak{I} \\ \Rightarrow & a*x+b*y \in \mathfrak{I} \\ \text{et} & (x,y) \in \mathfrak{J} \times \mathfrak{J} \\ \Rightarrow & a*x+b*y \in \mathfrak{J} \end{array}$$

puisque $\mathfrak{I}$ *et* $\mathfrak{J}$ *sont des idéaux. Il s'ensuit que* $a*x+b*y \in \mathfrak{I} \cap \mathfrak{J}$ *ce qui assure que* $\mathfrak{I} \cap \mathfrak{J}$ *est un idéal.*

ii) Plus généralement pour $\mathcal{I}$ *un ensemble non vide d'idéaux de* A, $\bigcap_{\mathfrak{I} \in \mathcal{I}} \mathfrak{I}$ *est un idéal de* A.

iii) $\mathfrak{I} \cup \mathfrak{J}$ *est un idéal de* A *si et seulement si* $\mathfrak{I} \subset \mathfrak{J}$ *ou* $\mathfrak{J} \subset \mathfrak{I}$.

iv) Si $\left(\mathfrak{I}_n\right)_{,n\in\mathbb{N}}$ *est une suite d'idéaux de* A *telle que*

$$\forall (p,q) \in \mathbb{N} \times \mathbb{N},\ \exists r \in \mathbb{N},\ \mathfrak{I}_p \subset \mathfrak{I}_r \text{ et } \mathfrak{I}_q \subset \mathfrak{I}_r,$$

alors $\bigcup_{n\in\mathbb{N}} \mathfrak{I}$ *est un idéal de* A.

Un cas particulier est celui où $\left(\mathfrak{I}_n\right)_{,n\in\mathbb{N}}$ *est croissante, i.e.*

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

car alors

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \mathfrak{I}_p \subset \mathfrak{I}_{\max(p,q)} \text{ et } \mathfrak{I}_q \subset \mathfrak{I}_{\max(p,q)} .$$

Le corollaire VII.4.7 qui suit est l'exact analogue du lemme III.4.1 :

Corollaire VII.4.7 *Pour* $S \subset A$ *une partie de* A, *l'ensemble* $\mathcal{I}_S$ *des idéaux de* A *contenant* S *possède un plus petit élément pour l'inclusion noté* (S). *autrement di* (S) *est l'unique idéal de* A *caractérisé par le fait que* $S \subset (S)$, *et pour tout idéal* $\mathfrak{J}$ *contenant* S, $(S) \subset \mathfrak{J}$.

Preuve : *Il faut remarquer que* $A \in \mathcal{I}_S$ *entraîne que* $\mathcal{I}_S \neq \emptyset$ *et qu'on peut donc appliquer VII.4.6.ii) si bien que*

$$(S) := \bigcap_{\mathfrak{I} \in \mathcal{I}} \mathfrak{I}$$

répond à la question.

Définition VII.4.8 Pour toute partie $S \subset A$, l'idéal (S) construit grâce au corollaire VII.4.7 ci-dessus est appelé *idéal engendré par* S.

Exemple VII.4.9 a) $(\emptyset) = \{0\}$.

b) Pour tout idéal $\mathfrak{I}$ de A,

$$(\mathfrak{I}) = \mathfrak{I} .$$

Les résultat qui suivent sont à rapprocher de la proposition III.4.7 :

Lemme VII.4.10 *Pour tout $S \subset A$, tout $x \in A$, $x \in (S)$, si et seulement s'il existe $r \in \mathbb{N}$, $x_{i\ ,1\leq i\leq r} \in S$, et $a_{i\ ,1\leq i\leq r} \in A$ tels que*

$$x = \sum_{i=1}^{r} a_i * x_i .$$

Preuve *: Notons $\mathfrak{I} \subset A$, l'ensemble des éléments $x \in A$ tels qu'il existe $r \in \mathbb{N}$, $x_{i\ ,1\leq i\leq r} \in S$, $a_{i\ ,1\leq i\leq r} \in A$, telque $x = \sum_{i=1}^{r} a_i * x_i$. Pour tout $(x, y) \in \mathfrak{I} \times \mathfrak{I}$, on peut, par définition,écrire $x = \sum_{i=1}^{m} a_i * x_i$ et $y = \sum_{i=1}^{n} b_i * y_i$, $a_{i\ ,1\leq i\leq m} \in A$, $b_{i\ ,1\leq i\leq n} \in A$, $x_{i\ ,1\leq i\leq m} \in S$, $y_{i\ ,1\leq i\leq n} \in S$. Pour tout $(a, b) \in A \times A$, notons*

$$\forall 1 \leq i \leq m,\ c_i := a * a_i \text{ et } z_i := x_i$$

$$\forall i \leq m1 \leq m + n,\ c_i := b * b_{i-m} \text{ et } z_i := y_{i-m} .$$

Il s'ensuit que

$$a * x + b * y = \sum_{i=1}^{m+n} c_i * z_i \in \mathfrak{I} .$$

C'est-à-dire que $\mathfrak{I}$ est un idéal.

Il est immédiat de constater que $S \subset \mathfrak{I}$, et que pour tout idéal $\mathfrak{J}$ contenant S, $\mathfrak{I} \subset \mathfrak{J}$, si bien que

$$\mathfrak{I} = (S) .$$

Définition VII.4.11 Pour tout $X \subset A$, l'idéal (X) s'appelle l'*idéal engendré par* X.

Notation VII.4.12 Pour $\mathcal{I}$ un ensemble d'idéaux de A, on note $\sum_{\mathfrak{I}\in\mathcal{I}} \mathfrak{I}$ l'idéal engendré par l'union $\bigcup_{\mathfrak{I}\,\in\,\mathcal{I}} \mathfrak{I}$.

Corollaire VII.4.13 *Pour deux idéaux $\mathfrak{I}$ et $\mathfrak{J}$ de A, l'idéal $\mathfrak{I}+\mathfrak{J}$ engendré par $\mathfrak{I}\cup\mathfrak{J}$ est l'ensemble des $x+y$ avec $x\in\mathfrak{I}$ et $y\in\mathfrak{J}$.*

***Preuve** : Preuve tout à fait analogue à celle donnée pour les groupes au TD n° III, exercice H.*

Notation VII.4.14 Si $a \in A$, l'idéal $(\{a\})$ engendré par le singleton $\{a\}$, est usuellement noté aA ou (a), et l'on a :

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

Un tel idéal est dit *principal* (cf. IX.1.)

Lemme VII.4.15 *Étant donné un idéal $\mathfrak{I}$ de A, les assertion suivantes sont équivalentes :*

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

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

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

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

***Preuve** :*

i) ***(a)*** $\Rightarrow$ ***b))***
Ceci est immédiat puisque $A^\times \subset A$.

ii) ***(b)*** $\Rightarrow$ ***c))***
Puisque $\mathfrak{I}\cap A^\times\neq\emptyset$, il existe $u\in A^\times$ tel que $u\in\mathfrak{I}$. Puisque $\mathfrak{I}$ est un idéal, pour tout $a\in A$, $u*a = u*a+u*0\in\mathfrak{I}$ c'est-à-dire que $uA\subset\mathfrak{I}$.
Réciproquement, puisque $u\in A^\times$, il existe $v\in A^\times$ tel que $u*v=1$. Ainsi pour tout $x\in\mathfrak{I}$, $x = u*v*x = u*(v*x)\in uA$ si bien que $\mathfrak{I}\subset uA$ et finalement

$$\mathfrak{I} = uA\ .$$

iii) ***(c)*** $\Rightarrow$ ***d))***
Puisque $u \in A^\times$, *il existe* $v \in A^\times$ *tel que* $u * v = 1$. *Donc*

$$1 = u * v \in uA = \mathfrak{I} .$$

iv) ***(d)*** $\Rightarrow$ ***a))***
Si $1 \in \mathfrak{I}$, *pour tout* $a \in A$, $a = a * 1 \in \mathfrak{I}$ *si bien que* $A \subset \mathfrak{I}$. *Comme, par définition* $\mathfrak{I} \subset A$,

$$A = \mathfrak{I} .$$

Définition VII.4.16 (Idéal stricte/propre) Un idéal $\mathfrak{I} \subset A$, est un *idéal strict* ou un *idéal propre* si $\mathfrak{I} \neq A$.

Définition VII.4.17 Un idéal $\mathfrak{p} \subset A$ est *premier* si $\mathfrak{p} \neq A$ (*i.e.* $\mathfrak{p}$ est un idéal propre) et

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

Définition VII.4.18 (Idéaux comaximaux) On dit que deux idéaux I et J de A sont *comaximaux* ou *étrangers* (ou éventuellement *premiers entre eux*) si $I + J = A$.

VII.5 . −Divisibilité et idéaux

La relation de divisibilité peut être introduite, comme nous allons le faire dans ce paragraphe pour n'importe quel anneau commutatif et être reliée à la notion d'idéal introduite en VII.4. Nous verrons cependant qu'elle acquiert d'intéressantes propriétés (cf. VII.6,) lorsque l'anneau est intègre.

Supposons donc dans cette section (VII.5) que $(A, +, *)$ est un anneau commutatif (cf. VII.1.1.)

Définition VII.5.1 (Divisibilité) Pour tout couple $(a, b) \in A \times A$, on dit que a *divise* b ou que a est un *diviseur* de b ou encore que b est un *multiple* de a et l'on note $a|b$, s'il existe $c \in A$ tel que $a * c = b$.

Lemme VII.5.2

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

(où aA *est l'idéal principal engendré par* a *(cf. IX.1.1.))*

Preuve *: Presqu'immédiat sur les définitions.*

Remarque VII.5.3 On remarque que la notion de divisibilité « correspond » à l'inclusion sur les idéaux laquelle est une relation d'ordre partielle. La réflexivité et la transitivité ne posent aucune difficulté pour la relation de divisibilité mais il n'est pas clair qu'elle soit antisymétrique : $a|b$ et $b|a$ n'implique pas forcément que $a = b$. Même dans $\mathbb{Z}$ $5|-5$ et $-5|5$.

On verra comment on peut affiner cette notion de manière intéressante dans le paragraphe concernant les anneaux intègres (cf. VII.6.)

Définition VII.5.4 (Élément premier) Un élément $a \in A$ est dit *premier* si l'idéal principal engendré par a (cf. IX.1.1,) aA est premier (cf. VII.4.17 ;) ce qui équivaut à dire que $a \notin A^\times$ (cf. VII.4.15,) et

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

Définition VII.5.5 (Éléments irréductibles) Un élément $x \in A$ de A est dit *irréductible* si $a \notin A^\times$ (a n'est pas inversible) et

$$\forall y \in A,\ \forall z \in A,\ \big(y*z = x \ \Rightarrow\ y \in A^\times \ \vee\ z \in A^\times\big)\,.$$

Notation VII.5.6 On notera

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

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

De manière un peu abusive, on notera encore

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

Proposition VII.5.7 *Pour tout $X \subset A$,*

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

(où (X) est l'idéal engendré par X défini en (cf. VII.4.11.)

Preuve *: Si $d \in \mathcal{D}(X)$,*

$$\forall x \in X,\ d|x\,.$$

Par conséquent, pour tout $y := \sum_{i=1}^{n} a_i * x_i \in (X)$, $d|y$ i.e.$y \in dA$ ce qui entraîne

$$(X) \subset dA\,.$$

Réciproquement si $(X) \subset dA$, pour tout $y \in (X)$, $d|y$. Comme $X \subset (X)$,

$$\forall x \in X,\ d|x$$

ce qui entraîne

$$d \in \mathcal{D}(X)\,.$$

Corollaire VII.5.8 *Pour tout $X \subset A$, $A^\times \subset \mathcal{D}(X)$.*

Preuve *: C'est une conséquence de la proposition VII.5.7 et du lemme VII.4.15.*

Définition VII.5.9 Pour $X \subset A$, si $\mathcal{D}(X) = A^\times$ on dit que les éléments de X sont *premiers entre eux (dans leur ensemble).*

Remarque VII.5.10 Cependant la situation que nous aurons souvent à considérer par la suite est celle où deux éléments x et y de A sont premiers entre eux *i.e.*où $\mathcal{D}(\{x, y\}) = A^\times$ ou vien où $X \subset A$ est constitué d'éléments *deux à deux premiers entre eux* c'est-à-dire

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

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

Définition VII.5.11 (Pgcd Ppcm) Étant donné un ensemble $X \subset A$, on appelle *plus grand commun diviseur* ou ***Pgcd*** (resp. *plus petit commun multiple* ou ***Ppcm***)

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

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

$$\forall a \in X,\ d|a \text{ et } \forall b \in \mathcal{D}(X),\ b|d \text{ (resp. } \forall a \in X,\ a|m \text{ et } \forall b \in \mathcal{M}(X),\ m|b\ .) \quad \text{VII.5.11.1}$$

Remarque VII.5.12 La définition VII.5.11 peut sembler un peu abusive au sens où nous n'avons parlé de *plus grand élément* ou de *plus petit élément* que pour une relation d'ordre (cf. I.2.2.vii).) Nous verrons en outre que la relation $\cdot|\cdot$ n'est pas « vraiment » une relation d'ordre (cf. VII.6.6,) met en particulier en défaut le fait que de tels éléments, s'ils existent, (ce que nous n'avons pas encore établi mais qui le sera pour les anneaux principaux est unique ; cependant :

Lemme VII.5.13 *Étant donné une partie $X \subset A$, tous les **Pgcd** (resp. **Ppcm**) de X s'ils existent engendrent un même idéal*

Preuve *: An effet si d et d' (resp. m et m') sont deux **Pgcd** (resp. **Ppcm**) de X, par définition on a*

$$d'|d \text{ et } d|d' \text{ (resp. } m'|m \text{ et } m|m'\ )$$

ce qui entraîne, en vertu du lemme VII.5.2

$$dA = d'A \text{ (resp. } A = m'A\ .)$$

Notation VII.5.14 Le lemme ci-dessus peux motiver les notations suivantes :Pour $X \subset A$ d (resp. m) un **Pgcd** (resp. **Ppcm**) de X, on notera :

$$\bigwedge X \ := \ dA \text{ et } (X\vee\,) := \ mA\,. \qquad \text{VII.5.14.1}$$

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

$$x \wedge y \ := \bigwedge \{x, y\} \text{ et } (x, y\vee\,) = \ (\{x, y\}\vee\,). \qquad \text{VII.5.14.2}$$

VII.6 . −Éléments remarquables d'un anneau intègre

Dans cette section (VII.6,) $(A, +, *)$ est un anneau commutatif intègre (cf. VII.1.1, VII.1.11.)

Proposition VII.6.1 *Dans un anneau commutatif intègre A, tout élément premier (cf. VII.5.4,) non nul est irréductible (cf. VII.5.5.)*

Preuve *: Soit en effet $p \in A$ et $(a, b) \in A \times A$ tels que $p = a*b$. Alors $p|a*b$ et puisque p est premier , $p|a$ ou $p|b$. Si $p|a$ il existe $c \in A$ tel que $a = p*c$. L'égalité $p = a*b$ entraîne alors $p = p*c*b$ qui entraîne encore*

$$p*(1-c*b) \ = \ 0\,.$$

Or $p \neq 0$ et A est intègre donc

$$c*b \ = \ 1$$

c'est-à-dire que b est inversible, ce qui assure que p est irréductible .

Définition VII.6.2 (Éléments associés) Pour $(x, y) \in A \times A$, on dit que y est *associé* à x s'il existe un élément inversible $u \in A^\times$, tel que $y \ = \ u*x$.

Lemme VII.6.3 *La relation d'association est une relation déquivalence .*

Preuve *: (cf. VII.8.11.)*

Lemme VII.6.4 *Pour tout $(a, b) \in A \times A$, les assertions suivantes sont équivalentes :*

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

b) $aA \ = \ bA$;

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

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

e) a *et* b *sont associés.*

Preuve *:*

i) ***(a)*** $\Leftrightarrow$ ***b))***
L'équivalence entre a) et b) est une conséquence immédiate du lemme VII.5.2.

ii) ***(c)*** $\Rightarrow$ ***d)*** $\Leftrightarrow$ ***e))***
L'équivalence entre c) et d) signifie exactement que la relation « être associés » est symétrique. L'équivalence avec e) est tautologique.

iii) ***(c)*** $\Rightarrow$ ***a))***
Puisque d) et c) sont équivalentes, c) entraîne c) et d) qui entraînent tautologiquement a).

iv) ***(a)*** $\Rightarrow$ ***d))***

Remarque iv).1 Notons que dans cette partie seulement de la démonstration l'hypothèse que A est intègre sera utilisée.

Si $a|b$ *et* $b|a$*, il existe* $(u, v) \in A \times A$ *tels que* $a = b * u$ *et* $b = a * v$*. Il s'ensuit que* $a = a * v * u$ *ou encore que*

$$a * (1 - v * u) = 0\ .$$

$a = 0$ *Si* $a = 0$*,* $a|b$ *entraîne* $b = 0$*, et pour tout* $w \in A^\times$*,* $a = b * w$*.*
$a \neq 0$ *Si* $a \neq 0$*, puisque* A *est intègre* $1 - v * u = 0$ *c'est-à-dire que* $v * u = 1$ *si bien que* u *et* v *sont inversibles, ce qui achève la preuve.*

Remarque VII.6.5 L'équivalence entre VII.6.4.b) et VII.6.4.e) peut se reformuler en disant qu'on a une bijection naturelle entre les classes d'équivalences pour la relation d'association et les idéaux principaux de A.

Remarque VII.6.6 Bien qu'elle soit réflexive et transitive, la relation $|$ (divise) n'est pas « vraiment » *antisymétrique* (cf. I.2.2.iii),) fait qu'on ne peut pas dire que $|$ est une relation d'ordre.

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

Remarque VII.6.7 On sait que dans un anneau A, pour tout $a \in A$, $0 * a = 0$ (cf. TD n° VII, exercice A, question 1).)Il en résulte que pour tout $a \in A$, $a|0$.

Par ailleurs

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

Lemme VII.6.8 *Pour tout $X \subset A$, les PGCD de X (resp. **Ppcm** de X) forment une classe d'équivalence pour la relation d'association.*

Preuve *: C'est une conséquence du lemme VII.5.13 et de la remarque VII.6.5.*

Remarque VII.6.9 On n'a pas parlé jusqu'ici du **Pgcd** ni du **Ppcm** mais d'un **Pgcd** ou d'un **Ppcm** à cause du défaut d'unicité constaté dans le lemme ci-dessus. Ce dernier énoncé montre en outre que de toute évidence, le « bon objet » à considérer n'est pas un **Pgcd** ou un **Ppcm** mais la classe d'association des **Pgcd** (resp **Ppcm**) qui, pour le coup, et d'après le lemme VII.6.8 est unique. Cette classe d'association ne semble pourtant pas être un objet très utilisable sauf à remarquer qu'on peut la représenter par un objet tout à fait maniable à savoir un idéal. Grâce au lemme VII.6.4 on sait en effet que tous les PGCD (resp. PPCM) engendrent le même idéal.

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

VII.7 . −Anneau quotient et factorisation des morphismes

Remarque VII.7.1 On a remarqué en VII.3.9, que pour un morphisme d'anneaux $f : A \to B$, le noyau $\mathrm{Ker}\, f$ de f n'est pas un sous-anneau de A. En revanche, puisque c'et le noyau du morphisme de groupes $f : (A,+) \to (B,+)$ c'est un sous-groupe de $(A,+)$ (cf. III.3.9.)

De plus pour tout couple (x,y) d'éléments de $\mathrm{Ker}\, f$ et tout couple $((a,b)$ d'éléments de A, puisque f est un morphisme d'anneaux,

$$f(a*x+b*y) \ =\ a*f(x)+b*f(y) \ =\ 0,$$

si bien que $a*x+b*y \in \mathrm{Ker}\, f$. On constate, comme on l'a déjà remarqué dans le corollaire VII.4.5, que le noyau d'un morphisme d'anneaux est un idéal.

Remarque VII.7.2 Pour un anneau $(A,+,*)$ puisque $(A,+)$ est un groupe abélien tout idéal $\mathfrak{I}$ de A est en particulier un sous-groupe distingué de $(A,+)$. les consttructions de la section V.5 peuvent s'appliquer mutatis mutandis. Néanmoins elles sont plus riches en générale, puisqu'on dispose d'une structure plus riche que celle de groupe.

Proposition VII.7.3 (Relations déquivalences compatibles) *Soient $(A,+,*)$ un anneau commutatif et $\mathfrak{I}$ un idéal de A la relation $\sim_{\mathfrak{I}}$ définie par*

$$\forall (x,y)\in A\times A,\ x\sim_{\mathfrak{I}} y\ \Leftrightarrow\ y-x\ \in\ \mathfrak{I}$$

est une relation d'équivalence compatible aux lois $+$ et $*$ de A. Il s'ensuit qu'il existe une unique structure d'anneau sur le quotient $A/\mathfrak{I}\ :=\ A/\sim_{\mathfrak{I}}$ telle que la surjection canonique $\pi\ :\ A\ \to\ A/\mathfrak{I}$ soit un morphisme d'anneaux.

Preuve *: On a déjà remarqué mais on rappelle encore que $(A,+)$ étant un groupe abélien, et $\mathfrak{I}$ un sous-groue, il est distingué (cf. V.4.9.b).) On constate que, de plus, la relation $\sim_{\mathfrak{I}}$ définie ici est exactement celle définie dans la section V.4. Il s'ensuit que la proposition V.5.1 s'applique si bien qu'il existe une unique structure de groupe (encore notée $+$) sur $A/\mathfrak{I}$ telle que*

$$\pi\ :\ (A,+)\ \to\ (A/\mathfrak{I},+)$$

soit un morphisme de groupes.

De plus :

$$\begin{array}{lrcl}
\forall x\in A,\ \forall z\in A, & & & \\
\forall y\in A,\ \forall t\in A, & x\sim_{\mathfrak{I}} z & \text{et} & y\sim_{\mathfrak{I}} t \\
\Rightarrow & z*t-x*y & = & z*t-z*y+z*y-x*y \\
 & & = & z*(t-y)+y*(z-x) \\
 & & \in & \mathfrak{I} \\
\Rightarrow & z*t & \sim_{\mathfrak{I}} & x*y
\end{array}$$

c'est-à-dire, du fait que I est un idéal, que la relation $\sim_{\mathfrak{I}}$ est compatible à $*$ et qu'il existe donc une unique loi $*$ sur $A/\mathfrak{I}$ telle que

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

(cf. I.6.18.)

Il reste encore à vérifier que $(A/\mathfrak{I},+,*)$ satisfait aux axiomes VII.1.1.Ann$_2$) à VII.1.1.Ann$_4$) et que π vérifie bien la définition VII.2.1.

Certaines des propriétés de la surjection canonique $\pi\ :\ A\ \to\ A/\mathfrak{I}$ sont, pour ainsi dire, presque évidentes au vu de ce qui précède mais il n'est pas mauvais de les dégager de manière formelle :

Proposition VII.7.4 (Propriétés de la surjection canonique) *Dans la situation de la proposition VII.7.3 :*

i) Le morphisme π est surjectif .

ii) $\operatorname{Ker}\pi = \mathfrak{I}$.

Preuve *:*

i) Remarqons encore une fois que pour tout élément $\alpha \in A/I$, α *est une classe d'équivalence qui est par conséquent non vide. Les écritures* $x \in \alpha$ *ou* $\pi(x) = \alpha$ *renvoient toute deux au même fait que* $x \in A$ *est un représentant de la classe* α.

Les expressions « x est au-dessus de α » « x relève α » ou « x est un relèvement de α » pourraient bien échapper au rédacteur de ces lignes sans qu'elles signfient pourtant ni plus ni moins que

$$\pi(x) = \alpha\,.$$

ii) Pour tout $x \in A$, $\pi(x) = 0$, *signifie exactement* $x \sim_{\mathfrak{I}} 0$, *c'est-à-dire* $x - 0 \in \mathfrak{I}$, *i.e.*$x \in \mathfrak{I}$.

Définition VII.7.5 (Anneau quotient) L'anneau

$$A/\mathfrak{I} \text{ ou même le couple } \big(A/\mathfrak{i}, \pi : A \to A/\mathfrak{i}\big)$$

construit par la proposition VII.7.3 est appelé *anneau quotient*. On dit encore que l'ensemble $A/\sim_{\mathfrak{I}}$ est muni de la *structure quotient*.

Remarque VII.7.6 On remarque que, si on oublie la multiplication $*$ sur A, $(A, +)$ est un groupe abélien et $\mathfrak{I}$ un sous-groupe, nécessairement distingué. La structure de groupe qu'on obtient sur $A/\mathfrak{I}$ en oubliant aussi la multiplication, donne un groupe abélien qui est exactement le groupe quotient défini en V.5.2.

Exemple VII.7.7 La situation considérée dans l'exemple V.5.3 peut être complétée. En effet pour tout $d \in \mathbb{Z}$, l'ensemble $d\mathbb{Z}$ des multiples de d est non seulement un sous-groupe de $(\mathbb{Z}, +)$ mais encore un idéal de $(\mathbb{Z}, +, *)$. Il s'ensuit, hormis pour $d = 1$, que $\mathbb{Z}/d\mathbb{Z}$ a une structure d'anneau telle que $\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ soit un morphisme d'anneaux.

Proposition VII.7.8 (Factorisation des morphismes) *Soient* $(A, +, *)$ *un anneau comutatif et* $\mathfrak{I}$ *un idéal. On note* $\pi : A \to A/\mathfrak{I}$ *la surjection canonique.*

Pour tout morphisme d'anneaux $f : A \to B$ *les assertions suivantes sont équivalentes :*

a) $\mathfrak{I} \subset \operatorname{Ker} f$,

b) il existe un unique morphisme d'anneaux

$$\overline{f} : A/\mathfrak{I} \to B \text{ tel que } \overline{f} \circ \pi = f\,.$$

De plus, si $\mathfrak{I} = \operatorname{Ker} f$, $\overline{f}$ *est injectif et il est surjectif dès que* f *l'est.*

***Preuve** :*

i) ***(b)*** $\Rightarrow$ ***a))***

C'est un fait général et facile à vérifier que, dès qu'on a des morphismes de groupes, u, v, w

$$u = v \circ w \Rightarrow \operatorname{Ker} w \subset \operatorname{Ker} u .$$

Or $\operatorname{Ker} \pi = \mathfrak{I}$ *(cf. VII.7.4.ii),) si bien que*

$$\overline{f} \circ \pi = f \Rightarrow \mathfrak{I} \subset \operatorname{Ker} f .$$

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

$*$*)* ***(Unicité de*** $\overline{f}$ ***(analyse))***

Si $\overline{f}$ *existe alors nécessairement pour tout* $\alpha \in A/\mathfrak{I}$, *il existe* $x \in A$ *tel que* $\alpha = \pi(x)$ *et*

$$\overline{f}(\alpha) = \overline{f}[\pi(x)] = f(x) .$$

Ceci établit l'unicité de $\overline{f}$.

†*)* ***(Existence de*** $\overline{f}$ ***(synthèse))***

Or si $z \in A$ *est tel que* $\alpha = \pi(z)$ *on a encore*

$$\overline{f}(\alpha) = \overline{f}[\pi(z)] = f(z) .$$

Or

$$\pi(x) = \pi(z) \Rightarrow z - x \in \mathfrak{I} \subset \operatorname{Ker} f \Rightarrow f(z - x) = 0 \Rightarrow f(z) = f(x) .$$

Il s'ensuit que $\overline{f}$ *existe et est bien définie par la formulle :*

$$\overline{f}(\alpha) = f(x) \, \forall \, x, \alpha = \pi(x) .$$

‡*)* ***(*** $\overline{f}$ ***est un morphisme de groupes)***

$$\forall \alpha \in A/\mathfrak{I}, \, \forall \beta \in A/\mathfrak{I}, \, \big(\exists x \in A, \, \exists y \in A, \, (\alpha = \pi(x) \wedge \beta = \pi(y)) \big) .$$

On a alors :

$$\begin{aligned} \overline{f}(\alpha + \beta) &= \overline{f}[\pi(x) + \pi(y)] \\ &= \overline{f}[\pi(x + y)] \\ &= f(x + y) \\ &= f(x) + f(y) \\ &= \overline{f}[\pi(x)] + \overline{f}[\, \pi(y)] \\ &= \overline{f}(\alpha) + \overline{f}(\beta) . \end{aligned}$$

*§) ($\overline{f}$ **est un morphisme d'anneaux**)*

$$\begin{array}{lll} \forall \alpha \in A/\mathfrak{I},\ \forall \beta \in A/\mathfrak{I}, & & \\ \forall x \in A,\ \forall y \in A, & \big(\alpha = \pi(x) \text{ et } \beta = \pi(y) & \Rightarrow\ \overline{f}(\alpha * \beta) \\ & & =\ \overline{f}(\pi(x) * \pi(y)) \\ & & =\ \overline{f}(\pi(x * y)) \\ & & =\ f(x * y) \\ & & =\ f(x) * f(y) \\ & & =\ \overline{f}(\alpha) * \overline{f}(\beta)\big) \end{array}$$

De plus $\overline{f}(1) \ = \ \overline{f}[\pi(1)] \ = \ f(1) \ = \ 1.$

*iii) $*$) ($\overline{f}$ **est injective**)*

$$\forall \alpha \in A/\mathfrak{I},\ \exists x \ \in \ A,\ \alpha \ = \ \pi(x)\,.$$

$$\overline{f}(\alpha) \ = \ 0 \ \Leftrightarrow \ \overline{f}[\pi(x)] \ = \ 0 \ \Leftrightarrow \ f(x) \ = \ 0 \ \Leftrightarrow \ x \in \mathrm{Ker}\, f \ = \ \mathfrak{I} \ \Leftrightarrow \ \alpha \ = \ 0\,.$$

*†) (**surjectivité**)*
Si f est surjective, $\forall y \in B,\ \exists x \ \in \ A,\ f(x) \ = \ y$. Alors $\overline{f}[\pi(x)] \ = \ y$.

Remarque VII.7.9 Notons que dans la preuve de la proposition VII.7.8, nous avons redonné des arguments que nous avions déjà donnés dans la preuve de la proposition V.5.4 et qu'on aurait pu simplement déduire les résultats concernant la structure de groupe de l'anneau $(A, +, *)$ de cette même proposition V.5.4.

Corollaire VII.7.10 (de la proposition VII.7.8) *Étant donné un morphisme d'anneaux $f \ : \ A \ \to \ B$ il existe un unique isomorphisme d'anneaux*

$$\overline{f} \ : \ A/\mathrm{Ker}\, f \ \cong \ \mathrm{Im}\, f \ \textit{ tel que } \ f \ = \ \overline{f} \circ \pi$$

où $\pi \ : \ A \ \to \ A/\mathrm{Ker}\, f$ est la surjection canonique. En particulier si f est surjectif

$$\overline{f} \ : \ A/\mathrm{Ker}\, f \ \cong \ B$$

est un isomorphisme.

***Preuve** : Il suffit d'appliquer la proposition VII.7.8 à $\mathfrak{I} \ := \ \mathrm{Ker}\, f$.*

Corollaire VII.7.11 *Étant donné un morphisme surjectif d'anneaux* $p : A \to B$, *il existe un unique isomorphisme d'anneaux*

$\phi : A/\mathrm{Ker}\, p \to B$ *tel que* $p = \phi \circ \pi$ *où* $\pi : A \to A/\mathrm{Ker}\, p$ *est la surjection canonique*.

Preuve : *C'est une conséquence immédiate du corollaire VII.7.10 puisque* $\mathrm{Im}\, p = B$.

Remarque VII.7.12 Les constructions du début de ce paragraphe et en particulier les propositions VII.7.3 et VII.7.8 peuvent être faites, sans presque d'ajout aux preuvent, dans le cadre de structures algébriques qui sont des groupes abéliens. Ainsi on obtiendrait facilement des résultats analogues dans le cas où A est un espace vectoriel et $\mathfrak{I}$ un sous-espace vectoriel. Pour peu qu'on connaisse la définition de ces objets, le cas où A est un module et $\mathfrak{I}$ un sous-module ne présenterait aucune difficulté supplémentaire.

La proposition suivante VII.7.13 étend au cas des anneaux les constructions donées dans les propositions II.5.4 et V.5.8.

Proposition VII.7.13 *Étant donnés un entier* $n \in \mathbb{N}^*$, $(A_k, +_k, *_k)_{,1 \leq k \leq n}$ *des anneaux*

$$\forall 1 \leq k \leq n,\ p_k : \prod_{i=1}^{n} A_i \to A_k \text{ les projections}$$

(cf. II.5.1.ii).) Alors :

i) Il existe un unique couple de lois de composition $(+, *)$ *sur* $\prod_{k=1}^{n} A_k$ *tel que pour tout* $1 \leq k \leq n$ p_k *soit un morphisme d'anneaux ; les loi* $+$ *et* $*$ *sont données par*

$$\begin{gathered}\forall\big((x_1, \ldots, x_n), (y_1, \ldots, x_n)\big) \in \prod_{k=1}^{n} A_k \times \prod_{k=1}^{n} A_K, \\ (x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 +_1 y_1, \ldots, x_n +_n y_n), \\ (x_1, \ldots, x_n) * (y_1, \ldots, y_n) = (x_1 *_1 y_1, \ldots, x_n *_n y_n).\end{gathered}$$

ii) Les lois $+$ *et* $*$ *étant définies sur* P *comme ci-dessus, si*

a) pour tout $1 \leq k \leq n$ 0_k *est l'élément neutre de* $(A_k, +_k)$, $(0_1, \ldots, 0_n)$ *est l'élément neutre pour* $+$;

b) pour tout $1 \leq k \leq n$ 1_k *est l'élément neutre de* $(A_k, *_k)$, $(1_1, \ldots, 1_n)$ *est l'élément neutre pour* $*$;

c) $x \in \prod_{k=1}^{n} A_k$ *est tel que pour tout* $1 \leq k \leq n$ $y_k \in A_k$ *est l'opposé de* $p_k(x)$*, alors* $(y_1, \ldots, y_n)$ *est l'opposé de* x *dans* $\big(\prod_{k=1}^{n} A_k, +\big)$;

d) $x \in \prod_{k=1}^{n} A_k$ *est tel que pour tout* $1 \leq k \leq n$ $y_k \in A_k$ *est l'inverse de* $p_k(x)$*, alors* $(y_1, \ldots, y_n)$ *est l'inverse de* x *dans* $\big(\prod_{k=1}^{n} A_k, *\big)$;

iii) Si pour tout $1 \leq k \leq n$ $(A_k, +_k, *_k)$ *est un anneau commutatif,* $\big(\prod_{k=1}^{n} A_k, +, *\big)$ *est un anneau commutatif.*

iv) Pour tout n*-uplet de morphismes d'anneaux*

$$f_k : B \to A_k \,, 1 \leq k \leq n \,,$$

il existe un unique morphisme d'anneaux

$$f : B \to \prod_{k=1}^{n} A_k \text{ tel que } \forall 1 \leq k \leq n,\ f_k = p_k \circ f \,.$$

v) Dans le cas où il existe A *tel que* $\forall 1 \leq k \leq n,\ A_k = A$*, la bijection* $\phi : A^{[1;n]} \cong \prod_{k=1}^{n} A$ *définie par la proposition II.5.1.iv) est un isomorphisme, pour peu que* $A^{[1;n]}$ *soit muni de la structure définie par la proposition I.6.20.*

Définition VII.7.14 (Anneau produit) Avec les notations de la proposition VII.7.13, les lois $+$ et $*$ définies sur $\prod_{k=1}^{n} A_k$ comme en VII.7.13.i) sont appelées *lois produits* et le triplet

$$\big(\prod_{k=1}^{n} G_k, +, *\big)$$

anneau produit.

Remarque VII.7.15 On constatera que, contrairement aux points V.5.8.i) à V.5.8.v), le point V.5.8.vi) ne peut se formuler de manière identique dans le cas des anneaux. En effet, en reprenant les notations de V.5.8.vi), l'application

$$i_1 \,:\, A_1 \,\to\, A_1 \times A_2 \,,\ (\text{resp. } i_2 \,:\, A_2 \,\to\, A_1 \times A_2 \,)$$

n'est pas un morphisme d'anneaux ; et son image n'est donc pas un sous-anneau de $A_1 \times A_2$ (voir la remarque VII.3.2.iii).) On pourrait néanmoins vérifier (et c'est un bon exercice) que $\operatorname{Im} i_1$ et $\operatorname{Im} i_2$ sont des idéaux de $A_1 \times A_2$ et qu'on a toujours

$$\operatorname{Ker} p_1 \,=\, \operatorname{Im} i_2 \text{ et } \operatorname{Ker} p_2 \,=\, \operatorname{Im} i_1 \text{ (cf. V.5.8.vi).c) ,)}$$

ainsi que

$$p_1 \circ i_1 \,=\, \mathrm{Id}_{A_1} \text{ et } p_2 \circ i_2 \,=\, \mathrm{Id}_{A_2} \text{ (cf. V.5.8.vi).b).)}$$

VII.8 . −Exercices

Exercice VII.8.1 [] Faire la preuve de la proposition VII.1.9.

Exercice VII.8.2 [] Donner la preuve de VII.1.4.i). Ce résultat reste-t-il vrai si G n'est plus supposé abélien ?

Exercice VII.8.3 [] Faire la preuve de la proposition VII.1.16.

Exercice VII.8.4 [] Pour un anneau A, le fait que A soit intègre (respectivement un corps) entraîne-t-il que l'anneau A^E considéré à la proposition VII.1.16 soit intègre (resp. un corps ?)

Exercice VII.8.5 [] Faire la preuve du lemme VII.2.7.

Exercice VII.8.6 [] Donner les détails de l'argument dans la remarque VII.3.2.iii).

Exercice VII.8.7 [] Faire la preuve de la proposition VII.3.3. À noter qu'une bonne partie de cette preuve a déjà été faite pour prouver la proposition III.3.4.

Exercice VII.8.8 [] Expliquer pourquoi le noyau d'un morphisme d'anneaux n'est pas en général un sous-anneau de l'ensemble de départ.

Exercice VII.8.9 [] Faire la preuve de la proposition VII.4.2.

Exercice VII.8.10 [] Faire la preuve de la proposition VII.4.6.

Exercice VII.8.11 [] Faire la preuve du lemme VII.6.3.

Exercice VII.8.12 [] Que devient l'énoncé de la proposition VII.7.3 si $\mathfrak{I} = A$?

Exercice VII.8.13 [] Soit $X \subset A$.

1) () Montrer que (X) est le plus petit idéal contenant X au sens de l'inclusion ; c'est-à-dire que, (X) est un idéal contenant X et pour tout idéal $\mathfrak{I}$ contenant X, $(X) \subset \mathfrak{I}$.

2) () Montrer que si $Y \subset A$ est une autre partie de A,

$$(X \cup Y) = (X) + (Y) .$$

Exercice VII.8.14 []

Étant donné un morphisme d'anneau $f : A \to B$, montrer que :

1) () si f est surjectif, pour tout idéal $\mathfrak{I}$ de A, $f(\mathfrak{I})$ est un idéal de B ;

2) () pour tout idéal premier $\mathfrak{p}$ de B, $f^{-1}(\mathfrak{p})$ est un idéal premier de A.

Exercice VII.8.15 []

Soient A un anneau commutatif, $\mathfrak{I}$ et $\mathfrak{J}$ des idéaux de A. On note

$$\pi_{\mathfrak{I}} : A \to A/\mathfrak{I} \text{ et } \pi_{\mathfrak{J}} : A \to A/\mathfrak{J}$$

les surjections canoniques (cf. VII.7.5,) et

$$\pi : A \to A/\mathfrak{I} \times A/\mathfrak{J}$$

le morphisme qui s'en déduit grâce à VII.7.13.iv) autrement dit,

$$\forall x \in A,\ \pi(x) = \big(\pi_{\mathfrak{I}}(x), \pi_{\mathfrak{J}}(x)\big) .$$

1) () Montrer que $\operatorname{Ker}\pi = \mathfrak{I} \cap \mathfrak{J}$.

2) () En déduire qu'il existe un unique morphisme injectif d'anneaux

$$\gamma : A/(\mathfrak{I} \cap \mathfrak{J}) \to A/\mathfrak{I} \times A/\mathfrak{J}$$

vérifiant

$$\gamma \circ \pi_{\mathfrak{I}\cap\mathfrak{J}} = \pi$$

où

$$\pi_{\mathfrak{I}\cap\mathfrak{J}} : A \to A/(\mathfrak{I} \cap \mathfrak{J})$$

est la surjection canonique.

3) () Le morphisme γ étant construit comme à la question 2), montrer que si $\mathfrak{I}$ et $\mathfrak{J}$ sont comaximaux (cf. VII.4.18,) γ est surjective et donc un isomorphisme.

Exercice VII.8.16 []

1) () Montrer que

$$\forall X \subset A, \forall Y \subset A, \mathcal{D}(X \cup Y) = \mathcal{D}(X) \cap \mathcal{D}(Y) .$$

2) () En déduire que s'il existe $(x, y) \in X \times X$ premiers entre eux, les éléments de X sont premiers entre eux dans leur ensemble.

VIII . −Les anneaux de polynômes

Dans tout ce chapitre (VIII), $(A, +_A, *_A, 0_A, 1_A)$ est un anneau (commutatif) (cf. VII.1.5,) qu'on supposera même assez vite intègre (cf. VII.1.11,) et l'on ne finira même par considérer, au chapitre IX que le cas où A est un corps.

VIII.1 . −L'anneau des séries formelles à coefficients dans A

On ne construit, dans ce paragraphe (VIII.1,) l'anneau $A[[X]]$ des séries formelles à coefficients dans A que pour servir de cadre à la construction de l'anneau $A[X]$ des polynômes à une indéterminée et à coefficients dans A construit au paragraphe VIII.2.

On n'aura malheureusement pas le loisir de sintéresser à l'anneau $A[[X]]$ pour lui-même ce qui pourtant est à la base de nombreux développements.

Définition VIII.1.1 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.

Notation VIII.1.2 On rappelle que l'ensemble des suites à valeurs dans A est usuellement noté $A^{\mathbb{N}}$ (cf. II.0.6.) On notera $\left(\zeta_n\right)_{,n\in\mathbb{N}} \in A^{\mathbb{N}}$ (resp. $\left(\upsilon_n\right)_{,n\in\mathbb{N}} \in A^{\mathbb{N}}$) la suite définie par

$$\forall n \in \mathbb{N},\ \zeta_n := 0 \text{ (resp. } \upsilon_0 := 1_A\ ,\ \forall n \in \mathbb{N},\ n \geq 1\ ,\ \upsilon_n := 0\ .)$$

Pour tout $(\alpha, \beta) \in A^{\mathbb{N}} \times A^{\mathbb{N}}$, on définit l'élément $\alpha +_{A^{\mathbb{N}}} \beta \in A^{\mathbb{N}}$ par :

$$(\alpha +_{A^{\mathbb{N}}} \beta)_n := \alpha_n +_A \beta_n \qquad \text{VIII.1.2.1}$$

et

$$(\alpha *_{A^{\mathbb{N}}} \beta)_n := \sum_{k=0}^{n} \alpha_k *_A \beta_{n-k} . \qquad \text{VIII.1.2.2}$$

Proposition VIII.1.3 *Le triplet $(A^{\mathbb{N}},\ +_{A^{\mathbb{N}}}\ ,\ *_{A^{\mathbb{N}}})$ est un anneau (commutatif si A l'est) d'élément neutre ζ pour la loi $+_{A^{\mathbb{N}}}$ et υ pour la loi $*_{A^{\mathbb{N}}}$.*

Preuve *: Il s'agit, en premier lieu , de montrer que $(A,\ +_{A^{\mathbb{N}}})$ est un groupe abélien, ce qui est fait dans l'exercice VIII.5.1 et résulte également de la proposition III.1.6*

On montre ensuite dans l'exercice VIII.5.2 que $(A,\ +_{A^{\mathbb{N}}}\ ,\ *_{A^{\mathbb{N}}})$ est un anneau commutatif.

.

Définition VIII.1.4 (Anneau des séries formelles) L'anneau $(A,\ +_{A^{\mathbb{N}}}\ ,\ *_{A^{\mathbb{N}}})$ est appelé *anneau des séries formelles à coefficients dans A.*

Notation VIII.1.5 Pour tout $a\ \in\ A$, on définit l'élément $i(a)$ de $A^{\mathbb{N}}$ par :

$$i(a)_0\ :=\ a \text{ et } \forall n \in \mathbb{N},\ n\ >\ 0\ \Rightarrow\ i(a)_n\ =\ 0\ . \qquad \text{VIII.1.5.1}$$

Pour tout $\alpha\ \in\ A^{\mathbb{N}}$, on définit $p(\alpha)\ \in\ A$ par :

$$p(\alpha)\ :=\ \alpha_0\ . \qquad \text{VIII.1.5.2}$$

Proposition VIII.1.6 *i)*

$$p\ \circ\ i\ =\ \mathrm{Id}_A\ .$$

ii) L'application i est injective et l'application p surjective.

Preuve *: Découle du point précédent.*

iii) Les applications i et p définies ci-dessus sont des morphismes d'anneaux.

Preuve *: Le fait que i est un morphisme d'anneaux est démontré dans le VIII.5.5. La vérification du fait que p est aussi un morphisme est très simple et laissée en exercice.*

Notation VIII.1.7 Pour tout $a\ \in\ A$ et tout $\alpha\ \in\ A^{\mathbb{N}}$, on note

$$a\ \cdot\ \alpha\ :=\ i(a)\ *_{A^{\mathbb{N}}}\ \alpha$$

qu'on finira par noter $a * \alpha$ en confondant A et l'image de i qui sont isomorphes et même $a\alpha$ si aucune confusion ne devait en résulter.

On remarque, en tout cas que :

$$\forall n \in \mathbb{N},\ (a \cdot \alpha)_n\ =\ \big(i(a) *_{A^{\mathbb{N}}} \alpha\big)_n\ =\ a *_A \alpha_n\ .$$

Proposition VIII.1.8 *On a alors :*

$$\forall a \in A,\ \forall b \in A,\ \forall \big(\alpha_n\big)_{,n\in\mathbb{N}} \in A^{\mathbb{N}},\ \forall \big(\beta_n\big)_{,n\in\mathbb{N}} \in A^{\mathbb{N}},\ :$$

Mod_1)

$$a\ \cdot\ (\alpha\ +_{A^{\mathbb{N}}}\ \beta)\ =\ a\ \cdot\ \alpha\ +_{A^{\mathbb{N}}}\ a\ \cdot\ \beta\ ;$$

Mod$_2$)

$$(a +_A b) \cdot \alpha = a \cdot \alpha +_{A^{\mathbb{N}}} b \cdot \beta ;$$

Mod$_3$)

$$(a *_A b) \cdot \alpha = a \cdot (b \cdot \alpha) ;$$

Mod$_4$)

$$1_A \cdot \alpha = \alpha .$$

Preuve : *Ce n'est qu'un jeu d'écriture sur le fait que i est un morphisme d'anneaux.*

Remarque VIII.1.9 Si A était un corps les propriétés VIII.1.8.Mod$_1$) à VIII.1.8.Mod$_4$) assureraient que $A^{\mathbb{N}}$ est un A-*espace vectoriel* . Cependant dans le cas où A est simplement un anneau on parle de A-*module*

Notation VIII.1.10 Pour tout $j \in \mathbb{N}$, on note $\varepsilon_j \in A^{\mathbb{N}}$ l'élément de $A^{\mathbb{N}}$ défini par :

$$(\varepsilon_j)_j := 1 \text{ et } \forall n \in \mathbb{N},\ n \neq j \Rightarrow (\varepsilon_j)_n = 0 .$$

Notons qu'on a immédiatement $\varepsilon_0 = \upsilon$.

Lemme VIII.1.11 *Pour tout $j \in \mathbb{N}$,*

$$\varepsilon_{j+1} = \varepsilon_1 *_{A^{\mathbb{N}}} \varepsilon_j$$

et par conséquent

$$\forall (j,k) \in \mathbb{N} \times \mathbb{N},\ \varepsilon_j *_{A^{\mathbb{N}}} \varepsilon_k = \varepsilon_{j+k} .$$

Preuve : *C'est un exercice.*

Notation VIII.1.12 Il est d'usage de noter $X := \varepsilon_1$, le lemme ci-dessus assurant que $X^j = \varepsilon_j$. L'anneau $(A^{\mathbb{N}}, +_{A^{\mathbb{N}}}, *_{A^{\mathbb{N}}})$ est usuellement notté $A[[X]]$ et appelé *anneau des séries formelles à coefficients dans* A. Un élément $\big(\alpha_n\big)_{,n\in\mathbb{N}} \in A^{\mathbb{N}}$ est noté

$$\alpha = \sum_{n=0}^{+\infty} \alpha_n X^n$$

cette notation ne devant cependant pas laisser croire qu'on ait pu écrire α comme combinaison linéaire et par conséquent trouver une base.

La notation $A[[X]]$ ne recouvre pas seulement $A^{\mathbb{N}}$ en tant qu'ensemble mais bel et bien l'anneau

$$(A^{\mathbb{N}}, +_{A^{\mathbb{N}}}, *_{A^{\mathbb{N}}}, \zeta, \upsilon)$$

si bien que lorsqu'on écrit $A[[X]]$ il n'est nul besoin de spécifier quelle est la structure d'anneau. Les éléments

$$\zeta \text{ (resp. } \upsilon \text{)sont, bien entendu, notés } 0 \text{ (resp. } 1 \text{ .)}$$

Proposition VIII.1.13 *i) Pour tout* $\big(\alpha_n\big)_{,n\in\mathbb{N}} \in A^{\mathbb{N}}$, $\alpha \neq \zeta$, *il existe un entier naturel* $\mathrm{val}(\alpha)$ *tel que*

$$\alpha_{\mathrm{val}(\alpha)} \neq 0 \text{ et } \forall n \in \mathbb{N},\ n < \mathrm{val}(\alpha) \Rightarrow \alpha_n = 0\ .$$

Preuve *: Voir l'exercice VIII.5.4.question 2).*

ii)

$$\forall (\alpha, \beta) \in (A^{\mathbb{N}} \setminus \{\zeta\}) \times (A^{\mathbb{N}} \setminus \{\zeta\}),\ \mathrm{val}(\alpha *_{A^{\mathbb{N}}} \beta) \geq \mathrm{val}(\alpha) + \mathrm{val}(\beta)$$

avec égalité dans le cas où A *est un anneau intègre.*

Preuve *: Voir l'exercice VIII.5.4.question 3).*

iii)

$$\forall (\alpha, \beta) \in (A^{\mathbb{N}} \setminus \{\zeta\}) \times (A^{\mathbb{N}} \setminus \{\zeta\}),\ \mathrm{val}(\alpha +_{A^{\mathbb{N}}} \beta) \geq \min\big(\mathrm{val}(\alpha)\ ,\ \mathrm{val}(\beta)\big)$$

avec égalité dans le cas où $\mathrm{val}(\alpha) \neq \mathrm{val}(\beta)$.

Preuve *: Voir l'exercice VIII.5.4.question 5).*

Définition VIII.1.14 (Valuation) Pour tout $\alpha \in A^{\mathbb{N}} \setminus \{\zeta\}$, on appellera *valuation* de α, l'entier $\mathrm{val}(\alpha)$.

Remarque VIII.1.15 a) On peut interpréter la valueation d'un élément α de $A^{\mathbb{N}} \setminus \{\zeta\}$, comme la plus grande puissance de X divisant α. La définition de valuation donnée en VIII.1.14 est alors à rapprocher de la notion de valuation p-adique donnée en IX.6.5, et on aurait affaire ici à la « valuation X-adique » en quelque sorte.

b) On peut prolonger l'application valuation de $A^{\mathbb{N}} \setminus \{\zeta\}$ à $A^{\mathbb{N}}$ en posant :

$$\mathrm{val}(\zeta) = (+\infty) .$$

Si on note $\overline{\mathbb{N}} := \mathbb{N} \cup \{(-\infty), (+\infty)\}$ $\mathrm{val}(\cdot)$ est une application de $A^{\mathbb{N}}$ à valeurs dans $\overline{\mathbb{N}}$.

On peut prolonger partiellement l'addition $+$ de $\mathbb{N}$ à $\overline{\mathbb{N}}$ en posant :

$$\begin{aligned} \forall n \in \mathbb{N},\ n + (+\infty) &= (+\infty) + n = (+\infty) \\ n + (-\infty) &= (-\infty) + n = (-\infty) \\ (+\infty) + (+\infty) &= (+\infty) \\ (-\infty) + (-\infty) &= (-\infty) . \end{aligned}$$

On peut aussi prolonger la relation d'ordre sur $\mathbb{N}$, en posant

$$\forall n \in \mathbb{N},\ (-\infty) < n < (+\infty) .$$

Avec ces définitions, les énoncés VIII.1.13.ii) et VIII.1.13.iii) sont vérifiés pour tout $(\alpha, \beta) \in A^{\mathbb{N}} \times A^{\mathbb{N}}$.

Proposition VIII.1.16 *Si A est un anneau commutatif intègre il en est de même de $A^{\mathbb{N}}$.*

Preuve *: Voir l'exercice VIII.5.4.question 4).*

VIII.2 . −Anneau des polynômes à une indéterminée

On reprend les notations du paragraphe VIII.1.

Notation VIII.2.1 On notera $A^{\mathbb{N},0} \subset A^{\mathbb{N}}$ l'ensemble des éléments de $A^{\mathbb{N}}$ qui sont des « *suites presque nulles* » c'est-à-dire que $A^{\mathbb{N},0}$ est l'ensemble des éléments $(\alpha_n)_{,n\in\mathbb{N}} \in A^{\mathbb{N}}$ tel qu'il existe $p \in \mathbb{N}$, tel que

$$\forall n \in \mathbb{N},\ n \geq p \Rightarrow \alpha_n = 0 .$$

Il est immédiat de constater que

$$\zeta \in A^{\mathbb{N},0} ,\ \upsilon \in A^{\mathbb{N},0} \text{ et } \forall n \in \mathbb{N},\ \varepsilon_n \in A^{\mathbb{N},0} .$$

Proposition VIII.2.2 *i) Pour tout* $\left(\alpha_n\right)_{,n\in\mathbb{N}} \in A^{\mathbb{N},0}$, $\alpha \neq \zeta$, *il existe un unique entier naturel* $\deg(\alpha)$ *tel que*

$$\alpha_{\deg(\alpha)} \neq 0 \text{ et } \forall n \in \mathbb{N},\ n > \deg(\alpha) \Rightarrow \alpha_n = 0\ .$$

Preuve *: Voir l'exercice VIII.5.6.question 1).*

ii)

$$\forall(\alpha,\beta) \in A^{\mathbb{N},0} \times A^{\mathbb{N},0},\ \deg(\alpha *_{A^{\mathbb{N}}} \beta) \leq \deg(\alpha) + \deg(\beta)$$

avec égalité dans le cas où A *est un anneau intègre.*

Preuve *: Voir l'exercice VIII.5.6.question 2).*

iii)

$$\forall(\alpha,\beta) \in (A^{\mathbb{N},0} \setminus \{\zeta\}) \times (A^{\mathbb{N},0} \setminus \{\zeta\}),\ \deg(\alpha +_{A^{\mathbb{N}}} \beta) \leq \max\left(\deg(\alpha)\ ,\ \deg(\beta)\right)$$

avec égalité dans le cas où $\deg(\alpha) \neq \deg(\beta)$.

Preuve *: Voir l'exercice VIII.5.6.question 3).*

iv) ***(Divisibilité)***
Si A *est un anneau intègre,*

$$\forall\alpha \in A^{\mathbb{N},0}, \forall\beta \in A^{\mathbb{N},0},\ \left(\alpha|\beta \text{ et } \beta \neq 0 \Rightarrow \deg(\alpha) \leq \deg(\beta)\ .\right)$$

Preuve *: Voir l'exercice VIII.5.6.question 6).*

Définition VIII.2.3 (Degré) Pour tout $\alpha \in A^{\mathbb{N},0} \setminus \{\zeta\}$, l'entier $\deg(\alpha)$ sera appelé *degré* de α.

Remarque VIII.2.4 De même que pour la valuation, on peut prolonger le degré à $A^{\mathbb{N},0}$ en posant

$$\deg(\zeta) := (-\infty)$$

(cf. VIII.1.15.b).) Les assertions VIII.2.2.ii) et VIII.2.2.iii) sont alors vérifiées pour tout $(\alpha,\beta) \in A^{\mathbb{N},0} \times A^{\mathbb{N},0}$.

Proposition VIII.2.5 *i) Le triplet* $(A^{\mathbb{N},0}, +_{A^{\mathbb{N}}}, *_{A^{\mathbb{N}}})$ *est un anneau (commutatif si* A *l'est), (intègre si* A *est intègre)* .

Preuve *: Voir l'exercice VIII.5.6.question 4).*

ii) Le morphisme $i : A \to A^{\mathbb{N}}$ *étant celui défini en VIII.1.5.1, l'image de* i *est incluse dans* $A^{\mathbb{N},0}$ *et l'on a*

$$\mathrm{Im}\, i \;=\; \{\alpha \;\in\; A^{\mathbb{N},0}\,;\, \deg(\alpha) \;=\; 0\}\,.$$

Il s'ensuit que $i : A \to A^{\mathbb{N},0}$ *est un morphisme injectif d'anneaux.*

Preuve *: Voir l'exercice VIII.5.6.question 7).*

iii) L'ensemble $A^{\mathbb{N},0\times}$ *des éléments inversibles de* $A^{\mathbb{N},0}$ *s'identifie (c'est-à-dire est isomorphe en tant que groupe abélien) à* $A^{\times}$.

Preuve *: Voir l'exercice VIII.5.6.question 8).*

iv) La loi externe $\cdot$ *définie en VIII.1.7 se restreint à* $A^{\mathbb{N},0}$ *et vérifie encore les axiomes VIII.1.8.Mod*$_1$*) à VIII.1.8.Mod*$_4$*).*

Preuve *: Est une conséquence presque immédiate du point ii).*

v) La famille $X^n{}_{,n\in\mathbb{N}}$ *est une base de* $A^{\mathbb{N},0}$ *c'est-à-dire que :*

a) ***(elle est génératrice)***
pour tout $\alpha \in A^{\mathbb{N},0}$ *il existe* $d \in \mathbb{N}$ *et un* d*-uplet* $a_i{}_{,1\leq i\leq d} \in A$ *tels que*

$$\alpha \;=\; \sum_{j=0}^{d} a_j \cdot X^j;$$

b) ***(elle est libre)***
pour tout $n \in \mathbb{N}$, *tout* n*-uplet* $a_i{}_{,1\leq i\leq n} \in A$,

$$\sum_{j=0}^{n} a_j \cdot X^j \;=\; \zeta \;\Rightarrow\; \forall 1 \leq j \leq n,\; a_j \;=\; 0\,.$$

Preuve *:*

a) C'est presqu'uniquement un jeu d'écriture. On peut cependant donner un argument un peu plus formel par récurrence. On remarque en effet que si $\deg(\alpha) \;=\; 0$,

$$\alpha \;=\; i(a) \;=\; i(a) *_{A^{\mathbb{N}}} \upsilon \;=\; a \cdot X^0\,.$$

Pour $d \in \mathbb{N}$, *si* $\deg(\alpha) \;=\; d+1$, *on écrit*

$$\alpha \;=\; \alpha_d \cdot X^d \;+\; \beta$$

et l'on constate que $\deg(\beta) \;\leq\; d$. *Si on fait donc l'hypothèse de récurrence qu'on peut écrire*

$$\beta \;=\; \sum_{j=0}^{d} \beta_j \cdot X^j$$

on peut décomposer α *de manière analogue ce qui prouve le résultat par récurrence sur le degré.*

b) Exercice.

Notation VIII.2.6 Il est donc usuel de noter les éléments $\alpha \in A^{\mathbb{N},0}$:

$$\alpha = \sum_{j=0}^{\deg(\alpha)} \alpha_j X^j$$

et l'anneau $(A^{\mathbb{N},0}, +_{A^{\mathbb{N}}}, *_{A^{\mathbb{N}}}) A[X]$.

De même que pour l'anneau des séries formelles (cf. VIII.1.12,) la notation $A[X]$ recouvre toute la structure d'anneau de $A^{\mathbb{N},0}$ si bien qu'il n'est n'ul besoin de spécifier que l'addition est donée par $+_{A^{\mathbb{N}}}$ et la multiplication par $*_{A^{\mathbb{N}}}$. L'élément neutre ζ sera bien entendu noté 0 et l'élément unité υ 1.

Définition VIII.2.7 L'anneau $A[X]$ est appelé *anneau des polynômes àune indéterminée à coefficients dans* A. Un élément de A est appelé *polynôme*.

Exemple VIII.2.8 Dans l'anneau $A := \mathbb{Z}/p^2\mathbb{Z}$, pour p un nombre premier, les éléments

$$\alpha := (1, p, 0, \ldots, 0, \ldots \text{ et } \beta := (1, -p, 0, \ldots, 0, \ldots$$

de $A^{\mathbb{N},0}$. On constate qu'alors

$$\alpha *_{A^{\mathbb{N}}} \beta = (1, 0, -p^2, 0, \ldots, 0, \ldots = (1, 0, \ldots, 0, \ldots = \upsilon$$

alors qu'on a $\deg(\alpha) = \deg(\beta) = 1$.

Proposition VIII.2.9 (Propriété universelle de l'anneau des polynômes) *Soient*

$$f : A \to B \text{ un morphisme d'anneaux et } b \in B .$$

Il existe un unique morphisme d'anneaux

$$\phi_b : A[X] \to B \text{ tel que } \phi_b(X) = b \text{ et } f = \phi_b \circ i$$

(où $i : A \to A[X]$ est le morphisme défini en VIII.1.5.1.)

Ceci entraîne en particulier que :

$$\forall \alpha \in A[X], \alpha = \sum_{k=0}^{\deg(\alpha)} \alpha_k X^k \Rightarrow \phi_b(\alpha) = \sum_{k=0}^{\deg(\alpha)} f(\alpha_k) *_B b^k . \qquad \text{VIII.2.9.1}$$

Preuve *:*

*i) (**Unicité**)*

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 $\forall n \in \mathbb{N}^*,\ \phi_b(X^n) = b^n$. Puisque ϕ_b est un morphisme d'anneaux,

$$\phi_b(1_{A[X]} = 1_B \Rightarrow \phi_b(v) = 1_B \Rightarrow \phi_b(X^0) = 1_B$$

d'où il résulte finalement :

$$\forall n \in \mathbb{N},\ \phi_b(X^n) = b^n\ . \qquad 1$$

Par ailleurs si on note $\cdot$ la loi externe définie en VIII.1.7, $\phi_b \circ i = f$ entraîne :

$$\begin{array}{l} \forall \alpha \in A[X], \forall \beta \in A[X], \\ \forall a \in A,\ \forall b \in A, \end{array} \qquad \begin{array}{rcl} \phi_b(a \cdot \alpha +_{A^{\mathbb{N}}} b \cdot \beta) & = & \phi_b(i(a) *_{A^{\mathbb{N}}} \alpha +_{A^{\mathbb{N}}} i(b) *_{A^{\mathbb{N}}} \beta) \\ & = & \phi_b(i(a)) *_B \phi_b(\alpha) +_B \phi_b(i(b)) *_B \phi_b(\beta) \\ & = & f(a) *_B \phi_b(\alpha) +_B f(b) *_B \phi_b(\beta)\ . \end{array}$$

L'application ϕ_b est donc « A-linéaire » et l'image de la base $\{X^n\}_{n\in\mathbb{N}}$ étant déterminée d'après 1, ϕ_b est nécessairement unique.

*ii) (**Existence**)*

Il existe une unique application « A-linéaire » $\phi_b : A[X] \to B$ telle que $\forall n \in \mathbb{N},\ \phi_b(X^n) = b^n$. Puisque ϕ_b est linéaire, en particulier $\forall \alpha \in A[X], \forall \beta \in A[X], \phi_b(\alpha +_{A^{\mathbb{N}}} \beta) = \phi_b(\alpha) +_B \phi_b(\beta)$ si bien que l'axiome VII.2.1.Ann$_5$) est satisfait.

Par ailleurs :

$$\forall \alpha \in A[X],\ \alpha = \sum_{k=0}^{\deg(\alpha)} \alpha_k X^k$$

$$\forall \beta \in A[X],\ \beta = \sum_{k=0}^{\deg(\beta)} \beta_k X^k \qquad \begin{array}{rcl} \phi_b(\alpha *_{A^{\mathbb{N}}} \beta) & = & \displaystyle\sum_{k=0}^{\deg(\alpha)+\deg(\beta)} \Big(\sum_{\ell+m\,=\,k} \alpha_\ell \beta_m \Big) \cdot X^k \\ & = & \displaystyle\sum_{k=0}^{\deg(\alpha)+\deg(\beta)} f\Big(\sum_{\ell+m\,=\,k} \alpha_\ell \beta_m \Big) *_B b^k \\ & = & \Big(\displaystyle\sum_{k=0}^{\deg(\alpha)} f(\alpha_k) *_B b^k \Big) *_B \Big(\sum_{k=0}^{\deg(\beta)} f(\beta_k) *_B b^k \Big) \\ & = & \phi_b(\alpha) *_B \phi_b(\beta) \end{array}$$

ce qui prouve que ϕ_b vérifie l'axiome VII.2.1.Ann$_6$).

Il est enfin clair que l'axiome VII.2.1.Ann$_7$) est satisfait.

Notation VIII.2.10 Avec les hypothèses et notations de la proposition VIII.2.9 ci-dessus, on notera $A[b]$ l'image de $A[X]$ dans B par le morphisme ϕ_b.

Corollaire VIII.2.11 (Fonctorialité de l'anneau des polynômes) *En particulier, étant donné un*
morphisme d'anneaux $f : A \to B$, *il existe un unique morphisme d'anneaux*

$$f[X] : A[X] \to B[X] \text{ caractérisé par : } f[X](X) = X \text{ et } f[X] \circ i_A = i_B \circ f$$

ce qui entraîne en particulier que :

$$\forall \alpha \in A[X], \alpha := \sum_{k=0}^{\deg(\alpha)} \alpha_k X^k \Rightarrow f[X](\alpha) = \sum_{k=0}^{\deg(\alpha)} f(\alpha_k) X^k . \qquad \textit{VIII.2.11.1}$$

Preuve *: Il suffit d'appliquer la proposition VIII.2.9 au morphisme d'anneaux* $i_B \circ f : A \to B[X]$ *et à l'élément* $X \in B[X]$.

Exemple VIII.2.12 Le corollaire VIII.2.11 justifie un certain nombre d'opérations :

a) Si $f : \mathbb{R} \to \mathbb{C}$ est l'inclusion naturelle du corps $\mathbb{R}$ des réels dans le corps $\mathbb{C}$ des complexes, le morphisme

$$f[X] : \mathbb{R}[X] \to \mathbb{C}[X]$$

consiste simplement à considérer les coefficients d'un polynôme à coefficients réels comme des nombres complexes.

b) En considérant l'inclusion $\mathbb{Z} \subset \mathbb{Q}$, on obtient également une inclusion $\mathbb{Z}[X] \subset \mathbb{Q}[X]$ et comme dans l'exemple a) elle consiste juste à considérer les coefficients entiers comme des nombres rationnels.

c) Soit $\sigma : \mathbb{C} \to \mathbb{C}$ la conjugaison complexe. L'application σ est bien un morphisme d'anneaux de $\mathbb{C}$ dans lui-même si bien qu'on peut lui appliquer le corrollaire VIII.2.11 pour en déduire un morphisme

$$\sigma[X] : \mathbb{C}[X] \to \mathbb{C}[X] \text{ qui vérifie,}$$

en vertu de VIII.2.11.1

$$\sigma[X]\big(\sum_{k=0}^{d} \alpha_k X^k\big) = \sum_{k=0}^{d} \sigma(\alpha_k) X^k$$

qu'on écrira de manière plus usuelle :

$$\overline{\sum_{k=0}^{d} \alpha_k X^k} = \sum_{k=0}^{d} \overline{\alpha_k} X^k .$$

d) Dans le cas où l'on considère la surjection canonique $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ le morphisme $\pi_n[X]$ associe, à un polynôme $P := \sum_{i=0}^{d} a_k X^k$ à coefficients entiers, le polynôme $\overline{P} = \sum_{i=0}^{d} a_k \bmod n X^k$ dont les coefficients sont des entiers modulo n. En particulier si n est un nombre premier on obtient un polynôme à coefficients dans un corps et l'on peut appliquer tous les résultats du chapitre IX.

VIII.3 . −Évaluation et fonctions polynômes

Dans cette section (VIII.3) A **est un anneau.**

Proposition VIII.3.1 (Évaluation) *Pour tout $a \in A$, il existe un unique morphisme d'anneaux*

$$\mathrm{ev}_a : A[X] \to A \mid \mathrm{ev}_a(X) = a \text{ et } \mathrm{ev}_a \circ i = \mathrm{Id}_A$$

et en particulier :

$$\forall \alpha \in A[X], \alpha = \sum_{k=0}^{\deg(\alpha)} \alpha_k X^k \Rightarrow \mathrm{ev}_a(\alpha) = \sum_{k=0}^{\deg(\alpha)} \alpha_k * a^k . \qquad \textit{VIII.3.1.1}$$

Preuve *: Il suffit d'appliquer la proposition VIII.2.9 à l'identité de A et à l'élément a de A.*

Notation VIII.3.2 Étant donné un ensemble X, notons

$$\mathcal{F}(X, A) := \{f : X \to A\}$$

l'ensemble des fonctions $f : X \to A$ de X à valeurs dans A (cf. I.2.1.iv).)

Lemme VIII.3.3 *i) Pour tout ensemble X, on peut munir l'ensemble A^X des applications de X dans A d'une structure d'anneau (commutatif) par :*

$$\forall f \in A^X, \forall g \in A^X, \forall x \in A, (f+g)(x) := f(a) +_A g(a) \text{ et } (f*g)(x) := f(x) *_A g(x) \quad 1$$

lélément neutre pour $+$ (resp. $*$,) étant la fonction constante de valeurs 0_A (resp. 1_A.)

Preuve *: Voir la proposition VII.1.16*

ii) La loi externe $\cdot$ définie sur $A \times A^X$ par :

$$\forall a \in A,\ \forall f \in A^X,\ \forall x \in X,\ (a\ \cdot\ f)(x)\ :=\ a\ \cdot\ f(x) \qquad 1$$

vérifie les axiomes VIII.1.8.Mod$_1$) à VIII.1.8.Mod$_4$).

iii) L'application :

$$j_A\ :\ A\ \to\ A^X\ ,\ a\ \mapsto\ a \cdot 1_{A^X} \qquad 1$$

est un morphisme d'anneaux.

Proposition VIII.3.4 *Considérons l'ensemble A^A des applications de A dans lui-même muni de la structure $+, *$ définie en VIII.3.2 et VIII.3.3.*

i) Il existe un unique morphisme d'anneaux :

$$\phi\ :\ A[X]\ \to\ A^A\ ,\ X\ \mapsto\ \mathrm{Id}_A \mid \phi\ \circ\ i_A\ =\ j_A \qquad 1$$

et l'on a alors :

$$\forall \alpha \in A[X], \alpha\ =\ \sum_{k=0}^{\deg(\alpha)} \alpha_k X^k\ ,\ \phi(\alpha)\ =\ x\ \mapsto\ \sum_{k=0}^{\deg(\alpha)} \alpha_k x^k\ . \qquad 2$$

Preuve *: Il suffit d'appliquer la proposition VIII.2.9 au morphisme j_A et à $\mathrm{Id}_A \in A^A$.*

ii) Si $\cdot$ désigne la loi externe définie en VIII.1.7 (resp. la loi externe définie en VIII.3.3.ii).1), selon le contexte :

$$\forall a \in A,\ \forall \alpha \in A[X], \phi(a \cdot \alpha)\ =\ a \cdot \phi(\alpha)\ . \qquad 1$$

Preuve *: Vérification sans difficulté.*

iii)

$$\forall a \in A,\ \forall \alpha \in A[X], \mathrm{ev}_a(\alpha)\ =\ \phi(\alpha)(a)\ =\ \sum_{k=0}^{\deg(\alpha)} \alpha_k a^k \qquad 1$$

qu'on notera bien évidemment $\alpha(a)$.

Preuve *: Idem.*

Définition VIII.3.5 (Racine) Pour tout polynôme $\alpha \in A[X]$ on appelle *racine de α dans A* un élément $a \in A$ tel que : $\alpha(a) = 0_A$.

Définition VIII.3.6 (Fonctions polynômes) On appelle *ensemble des fonctions polynômes* l'image du morphisme ϕ défini en VIII.3.4.i).1, dans A^A et *fonction polynôme* un élément de cette image.

Remarque VIII.3.7 On pourrait se demander pourquoi on a bien pris soin de distinguer les polynômes éléments de $A[X]$ des fonctions polynômes leurs image dans A^A. En effet :

a) Si A est le corps $\mathbb{R}$ le corps $\mathbb{C}$, et plus généralement un corps infini le morphisme ϕ défini en VIII.3.4.i).1 est injectif c'est-à-dire que si deux polynômes définisssent la même fonction polynôme ils sont égaux.

b) En revanche si κ est un corps fini, typiquement le corps $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, *)$ pour p un nombre premier, on peut considérer le polynôme $X^p - X \in \mathbb{F}_p[X]$. La fonction polynôme qu'il définit sur $\mathbb{F}_p$ est la fonction $x \mapsto x^p - x$ qui est la fonction nulle. Or $X^p - X$ n'est pas le polynôme nul à savoir l'élément $\zeta \in A[X]$ défini en VIII.2.1.

VIII.4 . −Le théorème de la division euclidienne

Dans ce paragraphe (VIII.4,) $\mathbb{K}$ est un corps et l'on s'intéresse à l'anneau $\mathbb{K}[X]$ des polynômes à une indéterminée et à coefficients dans $\mathbb{K}$.

Proposition VIII.4.1

$$\forall P \in \mathbb{K}[X],\ \forall Q \in \mathbb{K}[X],\ \big(P|Q \text{ et } Q \neq 0 \ \Rightarrow\ \deg(P) \leq \deg(Q)\big)\ .$$

Preuve *: Résulte de VIII.2.2.ii).*

Théorème VIII.4.2 (de la division euclidienne) *Pour tout couple (A, B) d'éléments de $\mathbb{K}[X]$, $B \neq 0$, il existe un unique couple (Q, R) d'éléments de $\mathbb{K}[X]$ tel que*

$$A = B * Q + R \text{ et } \deg(R) < \deg(B)\ .$$

Preuve *: (cf. VIII.5.7.)*

Remarque VIII.4.3 a) On peut faire ici la même observation qu'en IV.5.4.a) à savoir qu'on a unicité du couple (quotient , rest) dans l'énoncé du théorème de la division euclidienne. Ce résultat d'unicité se déduit de la propriété $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$ (cf. VIII.2.2.iii).) On a déjà mentionné et on rappelle encore que cet énoncé d'unicité n'est pas nécessaire pour établir que l'anneau $\mathbb{K}[X]$ est principal (cf. IV.5.5,) et qu'elle n'est pas vérifiée, par exemple, par le stathme euclidien de l'anneau des entiers de GAUSS (cf. Problème n° VII,) qui n'en jouit pas moin de toute les propriétés des anneaux principaux.

b) Les termes de *dividende*, *diviseur*, *quotient* et *reste* introduits en IX.7.1 sont bien entendu, utilisés dans le cas de l'anneau $\mathbb{K}[X]$ et l'on peut même, en vertu de a), parler du reste et du quotient.

Théorème VIII.4.4 (Structure des idéaux de $\mathbb{K}[X]$) *Une partie $\mathfrak{I} \subset \mathbb{K}[X]$ est un idéal (cf. VII.4.1,) de $\mathbb{K}[X]$ si et seulement si :*

$$\exists P \in \mathbb{K}[X],\ \mathfrak{I} = P\mathbb{K}[X] = \{P * Q\ ;\ Q \in \mathbb{K}[X]\} \qquad \textit{VIII.4.4.1}$$

c'est-à-dire que l'anneau $\mathbb{K}[X]$ est un anneau principal (cf. IX.1.2.)
(Voir la proposition IX.7.4 et comparer au corollaire IV.5.5.)

***Preuve** :*

i) Si $\mathfrak{I} = P\mathbb{K}[X]$:

$$\begin{array}{rrcl} & \forall P_1 \in \mathfrak{I},\ \exists Q_1 \in \mathbb{K}[X],\ P_1 = P * Q_1 & & \\ & \forall P_2 \in \mathfrak{I},\ \exists Q_2 \in \mathbb{K}[X],\ P_2 = P * Q_2 & & \\ \Rightarrow & \forall A_1 \in \mathbb{K}[X],\ \forall A_2 \in \mathbb{K}[X], & & \\ A_1 * P_1 + A_2 * P_2 & = & A_1 * P * Q_1 + A_2 * P * Q_2 & \\ & = & P * (A_1 * Q_1 + A_2 * Q_2) & \\ & \in & \mathfrak{I} & \end{array}$$

ce qui prouvve que $\mathfrak{I}$ est un idéal.

ii) Réciproquement si $\mathfrak{I}$ est un idéal non nul, soit $A := \{\deg(P)\ ;\ P \in \mathfrak{I}\backslash\{0\}\}$. L'ensemble A est une partie non vide de $\mathbb{N}$, et possède donc un plus petit élément d (cf. II.2.9.) Soit $P \in \mathfrak{I}$ avec $\deg(P) = d$. Puisque $\mathfrak{I}$ est un idéal, $\forall Q \in \mathbb{K}[X],\ PQ \in \mathfrak{I}$ si bien que si on note $\mathfrak{J} := P\mathbb{K}[X]$ l'idéal $\mathfrak{J}$ est inclus dans $\mathfrak{I}$.

Pour tout $S \in \mathfrak{I}$, il existe un couple $(Q, R) \in \mathbb{K}[X] \times \mathbb{K}[X]$ tel que

$$S = PQ + R \text{ et } \deg(R) < d\,.$$

Or

$$S \in \mathfrak{I} \wedge PQ \in \mathfrak{J} \subset \mathfrak{I} \Rightarrow R = S - PQ \in \mathfrak{I} \Rightarrow \deg(R) \geq d \text{ ou } R = 0$$

ce qui et entraîne $R = 0$ et par conséquent $S = PQ \in \mathfrak{J}$ et finalement $\mathfrak{I} = \mathfrak{J}$.

Remarque VIII.4.5 Dans la proposition précédente, et partant dans le théorème VIII.4.2 on ne peut pas omettre l'hypothèse que $\mathbb{K}$ est un corps. Prenons en effet $A := \mathbb{K}[X]$ alors $A[Y]$ est l'anneau $\mathbb{K}[X,Y]$ dans lequel l'idéal engendré par X et Y n'est pas de la forme VIII.4.4.1.

VIII.5 . −Exercices

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 $n \in \mathbb{N}$.

Exercice VIII.5.1 [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.

Exercice VIII.5.2 [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 :

1) () l'élément $\upsilon \in A^{\mathbb{N}}$ défini par

$$\upsilon_0 := 1 \text{ et } \forall n \in \mathbb{N},\ n \geq 1 \ \Rightarrow\ \upsilon_n := 0,$$

est un élément neutre pour $*_{A^{\mathbb{N}}}$;

2) ()

$$\forall (a,b) \in A^{\mathbb{N}} \times A^{\mathbb{N}},\ a *_{A^{\mathbb{N}}} b = b *_{A^{\mathbb{N}}} a \, ;$$

3) ()

$$\forall (a,b,c) \in A^{\mathbb{N}} \times A^{\mathbb{N}} \times A^{\mathbb{N}},\ a *_{A^{\mathbb{N}}} (b +_{A^{\mathbb{N}}} c) = a *_{A^{\mathbb{N}}} b +_{A^{\mathbb{N}}} a *_{A^{\mathbb{N}}} c \, .$$

De même on notera $*$ au lieu de $*_{A^{\mathbb{N}}}$ si aucune confusion n'est à craindre.

Exercice VIII.5.3 [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.

Exercice VIII.5.4 [Valuation]

1) () Rappeler ce que signifie que l'anneau A est intègre.

On suppose, dans toute la suite de la VIII.5.4 que $(A, +, *)$ est intègre.

2) () 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 : $\mathrm{val}(\zeta) = (+\infty)$, $(+\infty) \leq (+\infty)$, $(+\infty) + (+\infty) = (+\infty)$

$$\forall n \in \mathbb{N},\ n + (+\infty) = (+\infty) \text{ et } n < (+\infty)\ .$$

3) () Montrer que

$$\forall (a, b) \in A^{\mathbb{N}} \times A^{\mathbb{N}},\ \mathrm{val}(a *_{A^{\mathbb{N}}} b) = \mathrm{val}(a) + \mathrm{val}(b)\ ;$$

4) () En déduire que $(A^{\mathbb{N}},\, +_{A^{\mathbb{N}}}\,,\, *_{A^{\mathbb{N}}}\,)$ est un anneau intègre.

5) () 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 $\mathrm{val}(a) \neq \mathrm{val}(b)$.

6) () 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.

Exercice VIII.5.5 [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.

Exercice VIII.5.6 [degré]

On suppose encore dans cette question que A est un anneau intègre.

1) () 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 : $\deg(\zeta) = (-\infty), (-\infty) \leq (-\infty), (-\infty) + (-\infty) = (-\infty)$

$$\forall n \in \mathbb{N},\ n + (-\infty) = (-\infty) \text{ et } n > (-\infty)\,.$$

2) () Montrer que

$$\forall (a, b) \in \mathcal{P} \times \mathcal{P},\ \deg(a *_{A^{\mathbb{N}}} b) = \deg(a) + \deg(b)\,.$$

3) () 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 $\deg(a) \neq \deg(b)$.

4) () En déduire que $(\mathcal{P}, +_{A^{\mathbb{N}}}, *_{A^{\mathbb{N}}})$ est un anneau commutatif intègre.

5) () 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 VIII.5.4.question 6).)

6) () Montrer que pour tout $(a, b) \in \mathcal{P} \times \mathcal{P}$, si b divise a et $a \neq \zeta$, $\deg(b) \leq \deg(a)$

7) () Montrer que l'image du morphisme i défini à la VIII.5.5, 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.

8) () 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.*

Exercice VIII.5.7 [Division euclidienne]

1) () Rappeler ce que signifie l'assertion : A est un corps.

On suppose, jusqu'à la fin de VIII.5.7 que A est un corps.
Soit $b \in \mathcal{P}, b \neq \zeta$.

2) () 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

$$a = b *_{A^{\mathbb{N}}} q +_{A^{\mathbb{N}}} r \text{ et } \deg(r) < \deg(b) .$$

3) () 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

$$a = b *_{A^{\mathbb{N}}} s +_{A^{\mathbb{N}}} c \text{ et } \deg(c) < \deg(a) .$$

4) () 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 VIII.5.8 [Théorème chinois des restes dans $\mathbb{K}[X]$]

Dans tout cet exercice, $\mathbb{K}$ est un corps commutatif et $\mathbb{K}[X]$ l'anneau des polynômes à une indéterminée sur $\mathbb{K}$.

Pour tout couple $(P, Q) \in \mathbb{K}[X]^2$, on notera Q mod P la *classe de Q modulo P* c'est-à-dire l'ensemble des $Q' \in \mathbb{K}[X]$ tels que $P|Q' - Q$ et

$$\mathbb{K}[X]/P = \{Q' \textbf{ mod } P \,,\, Q' \in \mathbb{K}[X]\} .$$

1) () Montrer que $\mathbb{K}[X]/P$ est en fait l'anneau quotient $\mathbb{K}[X]/P\mathbb{K}[X]$ de $\mathbb{K}[X]$ par l'idéal engendré par P.

2) () Montrer que si P_1 et P_2 sont deux éléments premiers entre eux de $\mathbb{K}[X]$, leur **Ppcm** est leur produit.

Pour tout couple $(P_1, P_2) \in \mathbb{K}[X]$, **on notera** $\mathbb{K}[X]/P_1 \times \mathbb{K}[X]/P_2$ **l'ensemble des couples** (α_1, α_2) $\alpha_1 \in \mathbb{K}[X]/P_1$ $\alpha_2 \in \mathbb{K}[X]/P_2$, **muni des lois :**

$$\begin{aligned}(\alpha_1, \alpha_2) + (\beta_1, \beta_2) &:= (\alpha_1 + \beta_1, \alpha_2 + \beta_2)\\ (\alpha_1, \alpha_2) * (\beta_1, \beta_2) &:= (\alpha_1 * \beta_1, \alpha_2 * \beta_2)\ .\end{aligned}$$

3) () **a)** () Pour tout $(P_1, P_2) \in \mathbb{K}[X]^2$, montrer que $\mathbb{K}[X]/P_1 \times \mathbb{K}[X]/P_2$ est un anneau dont on déterminera l'unité et l'élément neutre pour $+$.

b) () Montrer que l'application

$$\begin{aligned}\phi : \ \mathbb{K}[X] &\to \mathbb{K}[X]/P_1 \times \mathbb{K}[X]/P_2\\ Q &\mapsto (Q \bmod P_1, Q \bmod P_2)\end{aligned}$$

est un morphisme d'anneaux.

c) () Déterminer le noyau K de ϕ puis en déduire qu'il existe un morphisme d'anneaux injectif

$$\gamma \ : \ \mathbb{K}[X]/K \ \to \ \mathbb{K}[X]/P_1 \times \mathbb{K}[X]/P_2 \ \text{ tel que } \ \phi \ = \ \gamma \circ \pi$$

où π est la surjection canonique $\mathbb{K}[X] \ \to \ \mathbb{K}[X]/K$.

d) () Si P_1 et P_2 sont premiers entre eux, montrer que ϕ est surjectif ; en déduire, dans ce cas, que γ est un isomorphisme ; décrire K plus précisément.

4) () **Soient** a **et** b **deux éléments distincts de** k **et** P **un élément de** $\mathbb{K}[X]$.

Déterminer le reste de la division euclidienne de P par $(X - a)(X - b)$ si le reste de la division euclidienne de P par $X - a$ (resp. $X - b$,) vaut 1.

Exercice VIII.5.9 [Division euclidienne, applications]

1) () (**Division euclidienne de polynômes**)

a) () Effectuer la division euclidienne de $X^5 + 13X^4 + 11X^3 + 7X^2 + 5X + 3$ par $X^2 + 1$.

b) () Calculer le PGCD de $X^6 + 2X^5 + 3X^4 + 5X^3 + 7X^2 + 11X$ et $13X^3 + 17X^2 + 19$.

2) () **Soient** $k \in \mathbb{N}^*$ et $P \in \mathbb{C}[X]$.

a) () Montrer qu'il existe

$$P_{j\ ,0\leq j\leq k-1} \in \mathbb{C}[X] \mid P(X^k) \ = \ P_0(X^k) \ + \ XP_1(X^k) \ + \ \ldots \ + \ X^{k-1}P_{k-1}(X^k)\ .$$

b) () En déduire le reste de la division de P par $X^k - a, a \in \mathbb{C}$.

c) () (**Exemple**)
Déterminer le reste de la division de $X^{38} - X^7 + X^4 - 1$ par $X^5 - 1$.

3) () **a)** () (**Cours**)
Soit $\mathbb{K}$ un corps. Énoncer (sans démonstration) le théorème de division euclidienne dans $\mathbb{K}[X]$.

Soit maintenant $P \in \mathbb{K}[X]$. **Soient** $a, b \in \mathbb{K}$ **distincts et notons** $\alpha := P(a)$, $\beta := P(b)$.

b) () Exprimer le reste de la division euclidienne de P par $(X - a)(X - b)$, en fonction de a, b, α et β.

c) () Dans $\mathbb{C}[X]$ ou $\mathbb{R}[X]$, donner le reste de la division euclidienne de $(\cos\theta \ + \ X \sin\theta)^n$ par $X^2 + 1$.

Exercice VIII.5.10 [**Pgcd** et **Ppcm** de polynômes]

1) () (**PGCD**)
On considère les polynômes à coefficients réels

$$A \ := \ X^5 + X^4 - X^3 - 2X^2 - 2X \text{ et } B \ := \ X^3 + 4X^2 + 4X + 3\ .$$

a) () Déterminer le PGCD D de A et B, et trouver deux polynômes U et V tels que $UA + VB \ = \ D$.

b) () Factoriser A en facteurs irréductibles, dans $\mathbb{C}[X]$, $\mathbb{R}[X]$ et $\mathbb{Q}[X]$.

2) () (**PGCD de polynômes**)
On considère le polynôme à coefficients réels

$$A \ := \ X^4 - 4X^3 + 2X^2 + 8X - 8\ .$$

a) () Déterminer le PGCD D de A et du polynôme dérivé A', et trouver deux polynômes U et V tels que $UA + VA' \ = \ D$.

b) () Factoriser A en facteurs irréductibles, dans $\mathbb{C}[X]$, $\mathbb{R}[X]$ et $\mathbb{Q}[X]$.

c) () **Soit** $B := (X-1)^2(X^3-3)$.

a) () Factoriser B en facteurs irréductibles, dans $\mathbb{C}[X]$, $\mathbb{R}[X]$ et $\mathbb{Q}[X]$ (*on peut admettre, sans le démontrer, que* X^3-3 *n'a pas de racine dans* $\mathbb{Q}$*).*

b) () Donner le PGCD de B et B' *(avec une phrase d'explication, mais sans long calcul).*

3) () **Soient**

$$m \geq 1 \quad n \geq 1 \text{ et } d := m \wedge n$$

des entiers.

a) () **a)** () Soit $z \in \mathbb{C}$, montrer que

$$\left(z^m = 1 \text{ et } z^n = 1 \right) \Rightarrow z^d = 1 .$$

b) () En déduire que

$$X^m - 1 \wedge X^n - 1 = X^d - 1 .$$

b) () **On suppose** $m \geq n$ **et on note** r **le reste de la division euclidienne de** m **par** n.

a) () Montrer que le reste de la division de X^m-1 par X^n-1 est X^r-1.

b) () Retrouver le résultat de la première question.

c) () **Soit** $P \in \mathbb{C}[X]$.

a) () Quel est le PGCD de P^m-1 et P^n-1 ?

b) () Montrer que, si m et n sont premiers entre eux, $(P^m-1)(P^n-1)$ divise $(P-1)(P^{mn}-1)$.

d) () Soit $q \in \mathbb{N}^*$. Donner une condition pour que $1+X^m+\ldots+X^q$ divise $1+X^m+\ldots+X^{qm}$.

4) () **Dans cet exercice, $\mathbb{K}$ est un corps commutatif et $\mathbb{K}[X]$ désigne l'anneau des polynômes à une indéterminée sur $\mathbb{K}$.**

a) () Montrer que l'intersection de deux idéaux de $\mathbb{K}[X]$ est encore un idéal de $\mathbb{K}[X]$.

b) () **Pour deux polynômes P et Q non nuls, on note M un générateur de $P * \mathbb{K}[X] \cap Q * \mathbb{K}[X]$.**

a) () Montrer que $P|M$, $Q|M$ et que pour tout $R \in \mathbb{K}[X]$ tel que $P|R$ et $Q|R$, $M|R$.

b) () En déduire que $\deg(M)$ est minimal parmi les multiples communs de P et Q.

On dira qu'un élément $\mu \in \mathbb{K}[X]$ est un Ppcm de P et Q s'il vérifie les conditions de a).

c) () Montrer que $\mu \in \mathbb{K}[X]$ est un **Ppcm** de P et Q si et seulement si μ est un générateur de $P * \mathbb{K}[X] \cap Q * \mathbb{K}[X]$.

d) () Que peut-on dire de deux **Ppcm** μ et μ' de P et Q ?

Exercice VIII.5.11 []

Posons :

$$\forall P \in \mathbb{Q}[X],\ P := \sum_{i=0}^{\delta} a_i X^i\ ,\ \forall p \in \mathcal{P},$$

si $P \neq 0$

$$\begin{aligned} V_p(P) &:= \min_{i=0}^{\delta}(v_p(a_i)) \\ \mathcal{S}(P) &:= \{p \in \mathbb{P}\,;\, V_p(P) \neq 0\} \end{aligned}$$

si $P = 0$

$$\begin{aligned} V_p(P) &:= (+\infty) \\ \mathcal{S}(P) &:= \mathcal{P}\ . \end{aligned}$$

1) () Pour tout $P \in \mathbb{Q}[X] \setminus \{0\}$, vérifier que :

Val$[X]_1$)

$$\forall P \in \mathbb{Q}[X],\ P \in \mathbb{Z}[X] \Leftrightarrow V_p(P) \geq 0\, \forall\, p \in \mathcal{P}\ .$$

Val$[X]_2$) L'ensemble $\mathcal{S}(P)$ est fini.

Soient

$$P := \sum_{i=0}^{\deg(P)} a_i X^i \text{ et } Q := \sum_{i=0}^{\deg(Q)} b_i X^i$$

des éléments de $\mathbb{Q}[X] \setminus \{0\}$ **et** $p \in \mathcal{P}$.

On pose

$$R := PQ = \sum_{i=0}^{\deg(R)} c_i X^i .$$

2) () Écrire $\{c_i\}_{0 \leq i \leq \deg(R)}$ en fonction des

$$\{a_i\}_{0 \leq i \leq \deg(P)} \text{ et } \{b_i\}_{0 \leq i \leq \deg(Q)} .$$

3) () En déduire que :

$$\begin{array}{lrcl} \forall 0 \leq k \leq \deg(R),\ \forall 0 \leq i \leq \deg(P),\ \forall 0 \leq j \leq \deg(Q), & i+j & = & k \\ \Rightarrow & v_p(c_k) & \geq & v_p(a_i) + v_p(b_j) \\ & & \geq & V_p(P) + V_p(Q) . \end{array}$$

4) () Justifier l'existence de m (resp. n) le plus grand entier $0 \leq i \leq \deg(P)$, (resp. $0 \leq j \leq \deg(Q)$,) tel que

$$v_p(a_i) = V_p(P) \text{ (resp. } v_p(b_j) = V_p(Q) .)$$

Montrer que

$$v_p(c_{m+n}) = V_p(P) + V_p(Q) .$$

5) () Établir finalement que

$$\forall (P,Q) \in \left(\mathbb{Q}[X] \setminus \{0\}\right)^2,\ \forall p \in \mathbb{P},\ V_p(PQ) = V_p(P) + V_p(Q) .$$

Exercice VIII.5.12 [Irréductibilité des polynômes à coefficients entiers]

Soit $P \in \mathbb{Z}[X] \setminus \{0\}$. **On suppose qu'il existe**

$$(Q,R) \in \left(\mathbb{Q}[X] \setminus \mathbb{Q}\right)^2 \mid P = QR .$$

1) () Pour tout $p \in \mathcal{P}$, montrer qu'il existe $a \in \mathbb{Z} \setminus \{0\}$, tel que :

i) soit

$$V_p(aQ) \geq 0 \text{ et } V_p(\frac{1}{a}R) \geq 0,$$

ii) soit

$$V_p(aR) \ \geq \ 0 \text{ et } V_p(\frac{1}{a}Q) \ \geq \ 0 \, .$$

2) () En déduire qu'il existe

$$(Q_1, R_1) \ \in \ \big(\mathbb{Z}[X] \setminus \{-1; 1\}\big)^2 \mid P \ = \ R_1 Q_1 \, .$$

3) () Établir finalement qu'un polynôme $P \in \mathbb{Z}[X] \setminus \{0\}$ unitaire est irréductible dans $\mathbb{Z}[X]$ si et seulement si il l'est dans $\mathbb{Q}[X]$.

Exercice VIII.5.13 [Polynômes irréductibles de $\mathbb{Q}[X]$]
Soient $a_1, a_2, \ldots, a_n, n \geq 1$ **des entiers deux à deux distincts,**

$$H \ := \ (X - a_1) \ldots (X - a_n) - 1 \, .$$

1) () Montrer que H est irréductible dans $\mathbb{Q}[X]$ (Si $H \ = \ H_1 H_2$ dans $\mathbb{Z}[X]$ avec $\deg(H_i) > 0$, on montrera que $H_1 + H_2 \ = \ 0$ et on obtiendra une contradiction en considérant $\lim_{x \to \infty} H(x)$).

2) () En déduire qu'il existe une infinité de polynômes de degré n, irréductibles dans $\mathbb{Q}[X]$.

IX . −Arithmétique des anneaux principaux

IX.0 . −Introduction

Il pourrait être déjà suffisant de justifier ce chapitre IX par l'envie d'éviter de pénibles redites dans l'étude de l'arithmétique des anneaux $\mathbb{Z}$ (cf. IV,) et $\mathbb{K}[X]$ (cf. VIII.) On sait en effet d'ores et déjà qu'on peut obtenir des résultats très semblables pour ces deux anneaux :

l'existence de **Pgcd** et de **Ppcm** (cf. IX.2 (théorème IX.2.7 et théorème IX.2.8 ;))
le théorème de BÉZOUT (cf. IX.3.1 (théorème IX.3.9.1 et théorème IX.3.10.1 ;))
le lemme de GAUSS (cf. IX.3.3 (théorème IX.3.9.3 et théorème IX.3.10.3 ;))
le lemme d'Euclide (cf. IX.3.6 (théorème IX.3.9.4 et théorème IX.3.10.4 ;))
les applications à l'arithmétique modulaire (cf. IX.3.8 IX.4.2.11 IX.4.3.1 ;)
le théorème chinois des restes (cf. IX.5.4 (théorème IX.5.5.1 et théorème IX.5.6.1 ;))
le théorème fondamental de l'arithmétique (cf. IX.6.3 (théorème IX.6.6.1 et théorème IX.6.7.1.))

On va voir que ces résultats se déduisent en fait d'analogues pour le cas plu général des anneaux principaux : le théorème de BÉZOUT (théorème IX.3.1,) le lemme de GAUSS (théorème IX.3.3,) le lemme d'Euclide (théorème IX.3.6) le théorème fondamental de l'arithmétique (théorème IX.6.3) et le théorème chinois des restes (théorème IX.5.4.)

On sait déjà ou bien on constatera que ces résultats découlent tous de l'existence pour $\mathbb{Z}$ comme pour $\mathbb{K}[X]$ d'une *division euclidienne* (théorème IV.5.2 et théorème VIII.4.2.) Il s'ensuit que l'un comme l'autre sont des anneaux principaux (théorème IV.5.7 et théorème VIII.4.4a)uxquels on peut appliquer le formalisme que nous allons développer dans les paragraphes IX.2 à IX.6. On obtiendra donc les résultats arithmétiques ci-dessus pour une plus large classe d'anneaux que ceux que nous allons étudier en détail à savoir $\mathbb{Z}$ et $\mathbb{K}[X]$. En particulier certains anneaux d'entiers de corps de nombrs (pas tous pour le malheur mais peut-être aussi la réputation de certain grands mathématiciens du passsé,) sont des anneaux principaux et notamment le plus connu peut-être d'entre eux l'anneau des entiers de GAUSS (cf. Problème n° VII.) On s'aperçoit pourtant dans ce dernier exemple encore, que l'anneau des entiers de GAUSS est principal par le fait qu'il est muni d'une division euclidienne. Il est établi qu'il existe des anneaux qui sont principaux sans disposer d'une division euclidienne mais ces exemples sont loin d'être aisés à construire.

Outre la perte de généralité qu'on s'infligerait à se restreindre aux anneaux qui ne seraient qu'euclidiens (*i.e.*disposant d'une division euclidienne) le formalisme auquel il faudrait alors avoir recours serait bien moins confortable et bien moins élégant que celui des anneaux principaux. On se restreindra cependant au cas des anneaux euclidiens dans le paragraphe IX.7 puisque l'on peut alors metre en œuvre des méthodes de calcul.

La présentation de ce chapitre IX pourra sembler ardue dans la mesure où l'on a donné le maximum de définitions en essayant de faire le moins d'hypothèses inutiles possible. Le lecteur pourra donc supposer dès le début que les anneaux considérer sont principaux (cf. IX.1.2.) L'idée dont on voudrait que le lecteur puisse être convaincu après lecture de ce chapitre est qu'en matière d'arithmétique *i.e.*de divisibilité, les objets qui comptent vraiement sont les idéaux ou ce qui revient à peu près au même que le rôle des éléments inversibles est négligeable.

IX.1 . −Anneaux principaux

Définition IX.1.1 (Idéal principal) Un idéal aA pour $a \in A$ comme dans l'exemple VII.4.3.b), est dit *principal*. On dit que l'idéal aA est *engendré* par a ou encore que a est un *générateur* de l'idéal aA.

Définition IX.1.2 (Anneau principal) Un anneau commutatif A est *principal* s'il est intègre (cf. VII.1.11,) et si tout idéal de A est principal (cf. IX.1.1.)

Exemple IX.1.3 a) Un corps est un anneau principal, puisqu'on a déjà remarqué (cf. VII.4.3.a),) que ses seuls idéaux sont $\{0\}$ et lui-même qui sont évidemment principaux. Néanmoins cet

exemple ne présente qu'un intérêt très limité du point de vue de l'arithmétique.

b) La proposition IX.7.4 nous permettra de donner un certain nombre d'exemple d'anneaux principaux qui ne sont pas des corps à savoir les anneaux euclidiens :

Exemple IX.1.4 D'autres exemples d'anneaux principaux sont donnés par :

a) (**L'anneau des entiers relatifs**)
l'anneau $\mathbb{Z}$ (cf. IV.5.5,) des entiers relatifs ;

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

c) (**Les entiers de GAUSS**)
l'anneau des entiers de GAUSS (cf. Problème n° VII) ;

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

IX.2 . −Existence de Pgcd et de Ppcm dans les anneaux principaux

Dans la suite, c'est-à-dire dans les paragraphes IX.2 à IX.6 A est un anneau principal.

Lemme IX.2.1 *Pour tout $X \subset A$, il existe $d \in A$, tel que $(X) = dA$.*

Preuve *: Puisque A est un anneau principal et que (X) est un idéal, il existe $d \in A$ tel que $(X) = dA$.*

Lemme IX.2.2 *Pour $X \subset A$, si d est un générateur de (X), i.e.si $(X) = dA$, il existe $n \in \mathbb{N}$, $a_{i\,,1\leq i\leq n} \in A$ et $x_{i\,,1\leq i\leq n} \in X$ tels que*

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

Preuve *: Il suffit de remarquer que $(X) = dA$, entraîne que $d = d * 1 \in (X)$.*

Proposition IX.2.3 (PGCD) *Soit $X \subset A$ une partie de A (qui peut être finie ou non.)*

i) X admet un PGCD (cf. VII.5.11 ;)

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

iii) pour tout PGCD d *de* X :

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

Preuve : *En vertu du lemme IX.2.1, ii) entraîne i).*

En vertu du lemme IX.2.2, ii) entraîne iii).

Il suffit donc de démontrer ii) :

Si d *est un générateur de* (X)*, en particulier* $(X) \subset dA$ *ce qui entraîne, en vertu de la proposition VII.5.7 que* $d \in \mathcal{D}(X)$*. Or pour tout* $y \in \mathcal{D}(X)$ *la proposition VII.5.7 entraîne que*

$$dA = (X) \subset yA \Rightarrow y|d\ .$$

Il s'ensuit que d *est un PGCD pour* X*.*

Réciproquement si d *est un PGCD pour* X*,* $d \in \mathcal{D}(X)$ *et d'après la proposition VII.5.7,* $(X) \subset dA$*. Or d'après le lemme IX.2.1, il existe* $y \in A$ *tel que* $(X) = yA$*. Il s'ensuit immédiatement que* $yA \subset dA$*. Mais d'après la proposition VII.5.7,* $y \in \mathcal{D}(X)$ *si bien que,* d *étant un* ***Pgcd*** *pour* X*,* $y|d$*. Ceci entraîne* $dA \subset yA$*, et finalement*

$$dA = yA = (X)\ .$$

Définition IX.2.4 (Identité de BÉZOUT) La formule IX.2.3.iii).1 est appelée *identité de* BÉZOUT et les éléments $a_{i\ ,1\leq i\leq n} \in A$ *coefficients de* BÉZOUT.

Remarque IX.2.5 La proposition IX.2.3 montre en particulier que, dans le cas où A est un anneau principal et $X \subset A$, les notations (X) introduite en VII.4.7 et $\bigwedge X$ introduite en VII.5.14.1, sont redondantes au sens où elles désignent le même objet, à savoir l'idéal engendré par X. Cependant dans le cas où A est principal, cet idéal est aussi celui engendré par n'importe quel PGCD des éléments de X.

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

Proposition IX.2.6 (Ppcm) *Pour tout* $X \subset A$*,* X *admet un* ***Ppcm*** *et les* ***Ppcm*** *de* X *sont les générateurs de l'idéal*

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

Preuve : *Laissée en exercice.*

IX.2.7 . −PGCD et Ppcm dans $\mathbb{Z}$

Proposition IX.2.7.1 (Existence du PGCD) *Pour tout entier naturel non nul $n \in \mathbb{N}^*$, et*

$$\text{toute partie } X := \{x_1, \ldots, x_n\} \subset \mathbb{Z}$$

finie à n éléments :

*i) (**PGCD**)*
X possède un PGCD.

*ii) (**Identité de** BÉZOUT)*
Si d est un PGCD de X il existe un n-uplet $(u_1, \ldots, u_n)$ tel que :

$$d = \sum_{i=1}^{n} u_i x_i \ . \qquad 1$$

(voir la proposition IX.2.3 et comparer à la proposition IX.2.8.1.)

***Preuve** :*

*i) a) (**Le sous-groupe** $< X >$)*
Soit

$$< X > := \ \{\sum_{i=1}^{n} n_i x_i \ ; \ n_{i \in \mathbb{Z}} \forall 1 \leq i \leq n, \ \} \ .$$

Alors $< X >$ est un sous-groupe de $\mathbb{Z}$. En effet, $0 = \sum_{i=1}^{n} 0 * x_i \in < X >$ et

$$\forall a := \sum_{i=1}^{n} a_i x_i \ , \ \forall b = \sum_{i=1}^{n} b_i x_i \ , \ a - b = \sum_{i=1}^{n} (a_i - b_i) * x_i \in < X > \ .$$

Il en résulte que $< X >$ est un sous-groupe de $\mathbb{Z}$.

D'après le résultat relatif à la structure des sous-groupes de $\mathbb{Z}$ (cf. IV.5.5,) il existe $d \in \mathbb{Z}$ tel que $< X > = d\mathbb{Z}$.

b) Reste à montrer que d est un PGCD pour X : Il est clair que

$$\forall x \in X \ , \ x \in < X > = \ d\mathbb{Z}$$

ce qui signifie exactement que $d|x$.

Réciproquement si $b \in \mathbb{Z}$ est tel que $\forall x \in X \ , \ b|x$, pour tout n-uplet $(n_1, \ldots, n_n)$,

$$b| \sum_{i=1}^{n} n_i x_i$$

d'où $< X > \subset b\mathbb{Z}$ c'est-à-dire $d\mathbb{Z} \subset b\mathbb{Z}$ c'est-à-dire, d'après $b|d$.

ii) Il suffit de remarquer que $< X >= d\mathbb{Z}$ *entraîne* $d \in < X >$ *ce qui prouve le résultat.*

Définition IX.2.7.2 (Identité de BÉZOUT) La formule IX.2.7.1.ii).1 est appelée *identité de* BÉZOUT et les entiers u_i ,$1 \leq i \leq n$ *coefficients de* BÉZOUT.

Remarque IX.2.7.3 a) Dans la preuve de la proposition IX.2.7.1, on aurait pu, sans grande difficulté, montrer que l'objet $< X >$ qu'on a introduit est un idéal et pas seulement un sous-groupe. C'est en fait l'objet (X) introduit en VII.4.11. Cependant cette preuve montre que la notion d'idéal n'est pas absolument nécessaire pour étudier l'arithmétique de $\mathbb{Z}$. On peut néanmoins difficilement éviter d'introduire les idéaux lorsqu'il s'agit de l'arithmétique des polynômes.

b) L'hypothèse que X est fini dans la proposition IX.2.7.1 n'est pas indispensable et l'on peut tout à fait s'en passer.

Proposition IX.2.7.4 (Existence des Ppcm) *Toute partie finie*

$$A := \{a_1, \ldots, a_n\} \subset \mathbb{Z}$$

admet un PPCM. (voir la proposition IX.2.6 et comparer à la proposition IX.2.7.4.)

Preuve *: Considérons*

$$G(a) := \bigcap_{i=1}^{n} a_i\mathbb{Z} .$$

moyennant de remarquer qu'une intersection de sous-groupes est un sous-groupe, il existe $m \in \mathbb{Z}$ *tel que* $G(A) = m\mathbb{Z}$*. En outre* $G(A)$ *est tautologiquement ou presque constitué des multiples communs à tous les* a_i*. L'entiers* m *est donc un multiple commun aux* a_i *mais divise tout élément de* $G(A)$ *par construction c'est donc le plus petit d'entre eux.*

Remarque IX.2.7.5 Il est usuel d'appeler PGCD (resp. PPCM) l'entier naturel qui est un PGCD (resp. Un PPCM) autrement dit le PGCD (resp. le PPCM) positif mais en fait bien des résultats énoncé dans la suite gagnent en concision et en simplicité, sans pour autant perdre de leur portée si au lieu de considérer l'entier d on considère le sous-groupe $d\mathbb{Z}$. On notera donc dans la suite, si A possède un PGCD d, (resp. un **Ppcm** m,)

$$\bigwedge A := d\mathbb{Z} \text{ (resp. } (A\vee) := m\mathbb{Z}) \qquad \text{IX.2.7.5.1}$$

et

$$\forall a \in \mathbb{Z},\ \forall b \in \mathbb{Z},\ a \wedge b := \bigwedge\{a, b\} \text{ (resp. } (a, b\vee) := (\{a, b\}\vee)) . \qquad \text{IX.2.7.5.2}$$

On ne s'interdira pas cependant dans la suite, d'écrire $a \wedge b = d$ au lieu de $a \wedge b = d\mathbb{Z}$ en sachant qu'alors

$$a \wedge b = d \Leftrightarrow a \wedge b = -d .$$

IX.2.8 . −PGCD et Ppcm dans $\mathbb{K}[X]$

Proposition IX.2.8.1 *Pour tout entier $n \in \mathbb{N}^*$, et toute partie*

$$A := \{P_1, \ldots, P_n\} \subset \mathbb{K}[X]$$

finie à n éléments :

*i) (**PGCD**)*
A possède un PGCD (cf. VII.5.11.)

*ii) (**Identité de BÉZOUT**)*
Si D est un PGCD de A il existe un n-uplet $(U_1, \ldots, U_n) \in \mathbb{K}[X]^n$ tel que :

$$D = \sum_{i=1}^{n} U_i P_i \,. \qquad 1$$

(voir la proposition IX.2.3 et comparer à la proposition IX.2.7.1.)

***Preuve** : La démonstration suit, mutatis mutandis, exactement le schéma de celle de la proposition IX.2.7.1, en remplaçant l'anneau $\mathbb{Z}$ par l'anneau $\mathbb{K}[X]$. En particulier l'ensemble $G(A)$ défini dans cette démonstration sera ici un idéal de $\mathbb{K}[X]$ et non plus un sous-groupe de $\mathbb{Z}$ et l'on conclura grâce au théorème VIII.4.4.*

Définition IX.2.8.2 (Identité de BÉZOUT) (cf. IX.2.7.2.) La formule IX.2.8.1.ii).1 est appelée *identité de* BÉZOUT et les polynômes $U_{i\,,1\leq i\leq n}$ *coefficients de* BÉZOUT.

Remarque IX.2.8.3 L'hypothèse que A est fini dans la proposition IX.2.8.1 n'est pas indispensable et l'on peut tout à fait s'en passer comme le montre la preuve de la proposition IX.2.3

Proposition IX.2.8.4 *Toute famille de polynômes admet un PPCM. (voir la proposition IX.2.6 et comparer à la proposition IX.2.7.4.)*

IX.3 . −Théorème de BÉZOUT,

lemme de GAUSS,
lemme d'EUCLIDE

On insiste que dans cettte section (IX.3) l'anneau A est principal. Certains résultats comme le lemme de GAUSS (cf. IX.3.3,) le lemme d'EUCLIDE (cf. IX.3.6,) pourrraient être obtenus dans un cadre plus général, à savoir celui des anneaux factoriels, mais l'hypothèse A principal est indispensable pour disposer du théorème de BÉZOUT IX.3.1. Dans la mesure où, dans ce paragraphe les résultas qui suivent sont des corollaires de ce premier théorème, il est évident que la stratégie de démonstration devra être tout à fait différente pour les obtenir dans un autre cadre que celui des anneaux principaux.

Théorème IX.3.1 (Théorème de BÉZOUT) *Pour tout $X \subset A$, les assertions suivantes sont équivalentes :*

a) $\mathcal{D}(X) = A^\times$ c'est-à-dire que les éléments de X sont premiers entre eux dans leur ensemble (cf. VII.5.9.)

b)

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

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

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

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

***Preuve** : On sait, d'après la proposition IX.2.3 que X admet un PGCD et que celui-ci engendre (X). Si donc tous les diviseurs commun des éléments de X sont inversibles il en va de même de n'importe lequel de ses PGCD et il en résulte que $(X) = A$ (cf. VII.4.15.a).) On a ainsi montré que a) entraîne b).*

Réciproquement si $\bigwedge X = A$, tout élément de $\mathcal{D}(X)$ divise 1 i.e.est inversible ce qui montre que b) entrraîne a).

L'équivalence entre a) et c) est immédiate.

La proposition IX.2.3 assure que c) entraîne d).

Enfin d) entraîne que $1 \in (X)$, ce qui entraîne b) en vertu du lemme VII.4.15.

Corollaire IX.3.2 (Idéaux comaximau) *Deux idéaux $\mathfrak{I}$ et $\mathfrak{J}$ de A sont comaximaux (cf. VII.4.18,) si et seulement si pour tout couple $(x, y) \in A \times A$ tel que $\mathfrak{I} = xA$ et $\mathfrak{J} = yA$ x et y sont premiers entre eux.*

***Preuve** : C'est un exercice.*

Théorème IX.3.3 (Lemme de GAUSS) *Pour tout $(a, b, c) \in A \times A \times A$, si a et b sont premiers entre eux, et $a|bc$ alors $a|c$.*

***Preuve** : Si a et b sont premiers entre eux, il existe (cf. IX.3.1,) des éléments u et v de A tels que $au + bv = 1$. Il en résulte que $acu + bcv = c$. Or $a|ac$ tautologiquement, $a|bc$ par hypothèse, donc $a|c$.*

Remarque IX.3.4 Il se peut que dans la littérature, le lemme de GAUSSne soit pas habituellement déduit du théorème de BÉZOUT mais plutôt du théorème fondamental de l'arithmétique (théorème IX.6.3.) Il pourrait alors sembler surprenant de procéder comme on l'a fait. Pour expliquer cette différence d'approche, il faudrait mentionner qu'il existe des anneaux dans lesquels le théorème IX.6.3 est satisfait mais dans lesquels le théorème de BÉZOUT IX.3.1 ne l'est pas. Dans de tels anneaux dits *factoriels* le lemme de GAUSSest encore vérifié mais ne peut alors se déduire du théorème de BÉZOUT. Pour donner une quelconque pertinence aux considérations qui précède il faudrait encore montrer qu'il existe vraiment des anneaux factoriels qui n'ont pas la propriété de BÉZOUT, ce qui est effectivement le cas.

Lemme IX.3.5 *Pour tout $p \in A$ irréductible et tout $a \in A$, si p ne divise pas a, a et p sont premiers entre eux.*

Preuve *:*

Soit $p \in A$ irréductible. Pour tout $a \in A$, si $\mathcal{D}(\{a,p\}) \neq A^\times$ il existe

$$x \in \mathcal{D}(\{p,a\})_= \mathcal{D}(\{p\}) \cap \mathcal{D}(\{a\})$$

qui n'est pas inversible. Il existe donc $(u,v) \in A \times A$, tels que

$$p = x * u \text{ et } a = x * v \, .$$

Or p étant irréductible, et x non inversible, u est inversible. Il existe donc $w \in A$ tel que $u * w = 1$. Ceci entraîne que $x = p * w$ qui entraîne encore que $a = p * v * w$ si bien que $p|a$.

Par contraposée,

$$p \not| a \Rightarrow \mathcal{D}(\{p,a\}) = A^\times$$

i.e.a et p sont premiers entre eux.

Théorème IX.3.6 (Lemme d'EUCLIDE) *Dans un anneau principal A, tout éléments irréductibles (cf. VII.5.5,) est premier (cf. VII.5.4.)*

Preuve *: Pour tout $(a,b) \in A \times A$, si $p \not| a$, a et p sont premiers entre eux en vertu du lemme IX.3.5. Il résulte alors du lemme de GAUSSIX.3.3, que $p|b$ ce qui asssure que p est premier.*

Remarque IX.3.7 Comme on a supposé dans cette section que A est intègre, tout élément premier non nul de A est irréductible (cf. VII.6.1,). Le lemme d'EUCLIDE ci-dessus montre donc que les notions de premiers et d'irréductibles coïncident peu ou prou, et correspondent à l'idée que l'on a depuis longtemps des nombres premiers.

Proposition IX.3.8 *Étant donné un anneau principal A qui n'est pas un corps, pour tout élément $p \in A$, le quotient A/pA est un corps si et seulement si p est irréductible (cf. VII.5.5.)*

Preuve *:*

*i) (p **irréductible** $\Rightarrow A/pA$ **corps**)*

Supposons donc p irréductible. Notons $\pi : A \to A/pA$ la surjection canonique (cf. VII.7.4.) Pour tout $\alpha \in A/pA$, il existe $x \in A$, tel que $\alpha = \pi(x)$. Dès lors, $\alpha \neq 0$, si et seulement si $x \notin \operatorname{Ker}\pi$, si et seulement si $x \notin pA$ si et seulement si p ne divise pas x. Il résulte alors du lemme IX.3.5 que x et p sont premiers entreu eux, puis du théorème de BÉZOUT *IX.3.1, qu'il existe $(y, z) \in A \times A$ tel que*

$$x * y + p * z = 1 .$$

Il s'ensuit que

$$\pi(x * y + p * z) = \pi(1) \Rightarrow \pi(x * y) = 1 \Rightarrow \pi(x) * \pi(y) = 1 \Rightarrow \alpha * \pi(y) = 1$$

c'est-à-dire que tout α non nul est inversible dans A/pA i.e. A/pA est un corps.

*ii) (A/pA **corps** $\Rightarrow p$ **irréductible**)*

Supposons donc que A/pA est un corps. Pour tout $(x, y) \in A \times A$,

$$p|x * y \Rightarrow \pi(x * y) = 0 \Rightarrow \pi(x) * \pi(y) = 0 .$$

Or A/pA étant un corps, c'est en particulier un anneau intègre. Il s'ensuit donc que $\pi(x) = 0$ ou $\pi(y) = 0$ c'est-à-dire $p|x$ ou $p|y$. On a donc démontré que p est premier (cf. VII.5.4.) Il résulte alors de la proposition VII.6.1 que p est nul ou irréductible. Mais $p = 0$ entraîne que $A/pA = A$ or on a supposé que A n'est pas un corps si bien que $p \neq 0$ est donc irréductible.

IX.3.9 . −Théorème de BÉZOUT,

lemme de GAUSS,
lemme d'EUCLIDE

Théorème IX.3.9.1 (de BÉZOUT) *Pour tout entier naturel n et toute partie*

$$X := \{x_1, \ldots, x_n\} \subset \mathbb{Z},$$

les assertions suivantes sont équivalentes :

a) $\mathcal{D}(X) = \{-1, 1\}$ *c'est-à-dire que les éléments de X sont premiers entre eux dans leur ensemble (cf. VII.5.9.)*

b) $\bigwedge X = 1$.

c) Il existe un n-uplet d'entiers relatifs u_i ,$1 \leq i \leq n$ tel que

$$\sum_{i=1}^{n} x_i u_i = 1 .$$

(voir le théorème IX.3.1 et comparer au théorème IX.3.10.1.)

Preuve : *La preuve découle immédiatement de la proposition IX.2.7.1.*

Remarque IX.3.9.2 Le théorème de BÉZOUT IX.3.9.1 est le plus souvent appliqué pour deux éléments puisque dans un certain nombre d'applications la condition utilisée est qu'une famille d'éléments soit constituée d'éléments deux à deux premiers entre eux et non premiers entre eux dans leur ensemble. C'est notamment le cas pour le théorème IX.5.5.1 chinois des restes. C'est de toute façon la situation à laquelle on peut avoir accès de manière calculatoire à travers l'*algorithme d'Euclide* (cf. IX.7.9.1.)

Théorème IX.3.9.3 (lemme de GAUSS) *Étant donnés trois entiers relatifs a, b, c, si a et b sont premiers entre eux, et $a|bc$ alors $a|c$.*
(voir le théorème IX.3.3 et comparer au théorème IX.3.10.3.)

Preuve : *Si a et b sont premiers entre eux, il existe (cf. IX.3.9.1.c)), des entiers relatifs u et v tels que $au + bv = 1$. Il en résulte que $acu + bcv = c$. Or $a|ac$ tautologiquement, $a|bc$ par hypothèse, donc $a|c$.*

Théorème IX.3.9.4 (lemme d'EUCLIDE) *Dans l'anneau $\mathbb{Z}$ tous les éléments irréductibles sont premiers. (voir le théorème IX.3.6 et comparer au théorème IX.3.10.4.)*

Preuve *: Soit $p \in \mathbb{Z}$ irréductible. Cela signifie en particulier que*

$$\mathcal{D}(p) \;=\; \{-p, -1, 1, p\}$$

et entraîne en particulier que $\forall a \in \mathbb{Z}$, si $p \not| a$ p et a sont premiers entre eux. Pour tout $a, b \in \mathbb{Z}$, si $p|ab$, et $p \not| a$, d'après le lemme de GAUSS*(cf. IX.3.9.3,) $p|b$.*

Remarque IX.3.9.5 La définition d'élément premier donnée en VII.5.4 peut dérouter dans la mesure où ce qu'on a l'habitude d'appeler *nombre premier* serait plutôt un élément irréductible de $\mathbb{Z}$ et même un tel élément dans $\mathbb{N}$. Heureusement que le lemme d'EUCLIDE nous permet de ne pas perdre nos « bonnes habitudes » en assurant que pour l'anneau $\mathbb{Z}$ les deux notions d'irréductible et de premier coïncident.

Définition IX.3.9.6 (Nombre premier) On appellera donc *nombre premier* un entier naturel $p \in \mathbb{N}$ qui en tant qu'élément de $\mathbb{Z}$ a les deux propriétés équivalentes d'être premier non nul (cf. VII.5.4,) ou irréductible (cf. VII.5.5.)

IX.3.10 . −Théorème de BÉZOUT,

lemme de GAUSS,
lemme d'EUCLIDE
dans l'anneau $\mathbb{K}[X]$

Théorème IX.3.10.1 (de BÉZOUT) *Pour tout entier naturel n et toute partie $A := \{P_1, \ldots, P_n\} \subset \mathbb{K}[X]$, les assertions suivantes sont équivalentes :*

a) $\mathcal{D}(A) \;=\; \mathbb{K}^\times$ c'est-à-dire que les éléments de A sont premiers entre eux dans leur ensemble (cf. VII.5.9.)

b) $\bigwedge A \;=\; 1$.

c) Il existe un n-uplet de polynômes $U_{i\,,1\leq i\leq n}$ tel que

$$\sum_{i=1}^{n} P_i U_i \;=\; 1\,.$$

(voir le théorème IX.3.1 et comparer au théorème IX.3.9.1.)

Remarque IX.3.10.2 Le théorème de BÉZOUT IX.3.10.1 est le plus souvent appliqué pour deux éléments puisque dans un certain nombre d'applications la condition utilisée est qu'une famille d'éléments soit constituée d'éléments deux à deux premiers entre eux et non premiers entre eux dans leur ensemble. C'est notamment le cas pour le théorème IX.5.6.1 chinois des restes. C'est de toute façon la situation à laquelle on peut avoir accès de manière calculatoire à travers l'*algorithme d'Euclide* (cf. IX.7.10.1.)

Théorème IX.3.10.3 (lemme de GAUSS) *Étant donnés trois polynômes P, Q, R, si P et Q sont premiers entre eux, et $P|QR$ alors $P|R$.*
(voir le théorème IX.3.3 et comparer au théorème IX.3.9.3.)

Théorème IX.3.10.4 (lemme d'Euclide) *Dans l'anneau de polynômes $\mathbb{K}[X]$ tous les éléments irréductibles (cf. VII.5.5,) sont premiers (cf. VII.5.4.)*
(voir le théorème IX.3.6 et comparer au théorème IX.3.9.4.)

Remarque IX.3.10.5 (Éléments irréductibles) Le théorème IX.3.10.4 assure que les deux notions de premier et d'irréductible sont équivalentes dans l'anneaux $\mathbb{K}[X]$ mais elle ne permet pas pour autant facilement de donner l'ensemble des polynômes irréductibles de $\mathbb{K}[X]$. Rappelons d'abord quelques résultats qui sont des conséquences directes du fait que le corps $\mathbb{K}$ est en particulier un anneau intègre :

i) (**Intégrité**)
L'anneau $\mathbb{K}[X]$ est intègre.

ii) (**Inversibles**)
L'ensemble $\mathbb{K}[X]^\times$ s'identifie à $\mathbb{K}^\times$ qui dans le cas d'un corps s'identifie à $\mathbb{K} \setminus \{0\}$ qu'on peut encore identifier à l'ensemble des polynômes de degré 0 et l'on a ainsi :

$$\forall P \in \mathbb{K}[X],\ P \in \mathbb{K}[X]^\times \Leftrightarrow \deg(P) = 0\,. \qquad 1$$

Lemme IX.3.10.6 *Pour tout $P \in \mathbb{K}[X]$ $\deg(P) = 1$ entraîne P irréductible.*

Preuve *: En effet si*

$$\deg(P) = 1 \text{ et } \exists Q \in \mathbb{K}[X],\ \exists R \in \mathbb{K}[X],\ P = Q * R$$

alors d'après VIII.2.2.ii) et VIII.2.2.iii),

$$0 \leq \deg(Q) \leq 1\ 0 \leq \deg(R) \leq 1 \text{ et } \deg(Q)+\deg(R) = 1 \Rightarrow \deg(Q) = 0 \text{ ou } \deg(R) = 0$$

ce qui, en vertu de IX.3.10.5.ii).1 entraîne Q ou R inversible et donc P irréductible.

Remarque IX.3.10.7 (Polynômes irréductibles) Nous venons de montrer en IX.3.10.6 que les polynômes de degré 1 à coefficients dans un corps sont irréductibles mais il n'existe pas d'argument aussi élémentaire pour dire qu'il n'en existe pas d'autres ou bien sous quelle(s) condition(s) il n'en existe pas d'autre. On peut certes dire que si $\mathbb{K}$ est *algébriquement clos* les seuls polynômes irréductibles sont les polynômes de degré 1 mais c'est pratiquement une définition et l'on n'a donc pas donné beaucoup plus d'information.

a) (**Le cas complexe**)

Le théorème de d'Alembert-GAUSS assure justement que dans $\mathbb{C}[X]$ les seuls polynômes irréductibles sont les polynômes de degré 1, c'està-dire que $\mathbb{C}$ est algébriquement clos. Cependant la démonstration de ce théorème fait intervenir des arguments d'analyse qu'on ne peut pas développer ici.

b) (**Le cas réel**)

On peut déduire de la situation sur $\mathbb{C}[X]$ que les polynômes irréductibles de $\mathbb{R}[X]$ sont au plus de degré 2 en utilisant la conjugaison complexe. Néanmoins il existe aussi des polynômes de degré 2 qui ne sont pas irréductibles.

c) (**Le cas rationnel/entier**)

La situation dans $\mathbb{Q}[X]$ est beaucoup plus compliquée, puisqu'on peut montrer qu'il existe des polynômes irréductibles de degré arbitrairement grand.

IX.4 . −Arithmétique modulaire

Proposition IX.4.1 *Étant donné un anneau principal A et $p \in A$, si p est irréductible l'anneau quotient A/Ap est un corps. La réciproque est vraie, pour peu que A ne soit pas déjà lui-même un corps.*

IX.4.2 . −L'anneau $(\mathbb{Z}/n\mathbb{Z}, +*)$

On a vu dans la proposition IX.3.8 à quelle condition A/pA est un corps. La formulation de ce résultat dans le cas où lanneau A est l'anneau $\mathbb{Z}$ (cf. IX.4.2.11,) est sans doute déjà bien connue et n'apporterait en soit que peu d'information suplémentaire par rappport à la proposition IX.3.8. L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, *)$ possède cependant suffisamment de propriétés intéressantes d'un point de vue arithmétique, pour qu'on s'atarde un peu à son étude. Les résultats de ce paragraphe et notamment la proposition IX.4.2.11 sont à rapprocher des résultats analogues pour les polynomes développés au paragraphe IX.4.3 et notamment la proposition IX.4.3.1.

Définition IX.4.2.1 (Congruences) Pour tout entier naturel n, on dit que deux entiers relatifs a et b sont *congrus modulo* n et l'on note $a \sim_n b$ ou encore $a \equiv b\,[n]$ si $n|(b-a)$ (cf. VII.5.1.)

On définit ainsi une relation binaire (cf. I.2.1.iii),) sur $\mathbb{Z}$ qu'on appelle *relation de congruence modulo* n.

Remarque IX.4.2.2 Pour $n \in \mathbb{N}$, a et b éléments de $\mathbb{Z}$, on remarque que $a \equiv b\,[n]$, signifie exactement que $b-a$ est élément du sous groupe $n\mathbb{Z}$ de $\mathbb{Z}$ (cf. IV.5.5) , que l'on peut également considérer comme un idéal. La relation de congruence modulo n n'est autre en fait que la relation $\sim_I$ pour $I = n\mathbb{Z}$ définie en VII.7.3.

Lemme IX.4.2.3 *Pour tout $n \in \mathbb{N}$, la relation de congruence modulo n est une relation d'équivalence (cf. I.2.2.v).)*

Preuve *: Ce résultat est réétabli en détail dans ce cas particulier (cf. TD n° IV, exercice B, question 2)m)ais peut aussi être déduit du cas général établi dans la proposition VII.7.3.*

Définition IX.4.2.4 (Classes de congruence) Une classe d'équivalence pour la relation de congruence modulo n s'appelle une *classe de congruence*.

Notation IX.4.2.5 Pour tout $a \in \mathbb{Z}$, on notera $a \bmod n$ ou simplement $\overline{a}$ s'il n'y a pas d'ambiguïté sur l'entier n, la classe de a.

Un entier naturel n étant fixé, on notera $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes de congruence modulo n et

$$\begin{array}{rccc} \pi_n : & \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & a & \mapsto & a \bmod n \end{array} \qquad \text{IX.4.2.5.1}$$

la surjection canonique *i.e.* :

$$\forall a \in \mathbb{Z},\ \pi_n(a) := a \bmod n\ .$$

Lemme IX.4.2.6 *i) Pour tout entier naturel $n \in \mathbb{N}$ et tout couple d'entiers relatifs $(a,b) \in \mathbb{Z} \times \mathbb{Z}$, les assertions suivantes sont équivalentes :*

$$\begin{array}{rcl} a & \in & b \bmod n \\ b & \in & a \bmod n \\ a \bmod n & = & b \bmod n \\ a & \sim_n & b \\ a & \equiv & b\,[n] \\ n & | & b-a\ . \end{array}$$

ii)

$$\forall a \in \mathbb{Z},\ \forall b \in \mathbb{Z},\ \big(a \ \equiv\ b\,[0] \ \Leftrightarrow\ a \ =\ b\big)\ .$$

iii)

$$\forall a \in \mathbb{Z},\ a \ \equiv\ 0\,[1]\ .$$

iv) Pour tout entier naturel $n \geq 1$, l'application de $\mathbb{Z}$ à valeurs dans $[0; n-1]$ qui à tout entier relatif a associe son reste dans la division euclidienne par n (cf. IV.5.2,) définit une bijection de $\mathbb{Z}/n\mathbb{Z}$ dans $[0; n-1]$. En particulier, $\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini (cf. II.4.1,) à n éléments.

Les assertions équivalentes i) sont encore équivalentes au fait que, a et b ont même reste dans la division euclidienne par n.

***Preuve** : Les points i) à iii) sont très très élémentaires.*

Considérons donc l'application $\rho\ :\ \mathbb{Z}\ \to\ [0; n-1]$ qui à tout entier relatif a associe son reste dans la division euclidienne par n. Si $a\ \equiv\ b\,[n]$, en écrivant

$$a\ =\ nq + \rho(a) \text{ et } b\ =\ ns + \rho(b),$$

$$\begin{array}{lrcl}
 & n & \mid & b-a \\
\Rightarrow & n & \mid & n(s-q) + \rho(b) - \rho(a) \\
\Rightarrow & n & \mid & \rho(b) - \rho(a) \\
\Rightarrow & \big(\rho(b) - \rho(a)\ =\ 0 & \vee & n \leq |\rho(b) - \rho(a)|\big)
\end{array}$$

la dernière implication résultant de IV.5.1.

Or on a un encadrement sur $\rho(b) - \rho(a)$ qui interdit cette dernière possibilité donc $\rho(a)\ = \rho(b)$.

On peut donc définir une application $C\ :\ \mathbb{Z}/n\mathbb{Z}\ \to\ [0; n-1]$ par $C(\alpha)\ :=\ \rho(a)$ pour $a\ \in\ \alpha$.

L'application C est manifestement surjective, puisqu'il est immédiat que pour tout

$$a\ \in\ [0; n-1]\ ,\ C(a \bmod n)\ =\ a\ .$$

Il est ensuite immédiat de remarquer que

$$\forall a \in \mathbb{Z},\ \rho(a)\ \in\ a \bmod n\ .$$

Il s'ensuit que

$$\begin{array}{lrcl}
\forall \alpha \in \mathbb{Z}/n\mathbb{Z}, & \forall \beta \in \mathbb{Z}/n\mathbb{Z},\ \big(C(\alpha) & = & C(\beta) \\
\Leftrightarrow & \forall a \in \alpha,\ \forall b \in \beta,\ (\rho(a) & = & \rho(b)) \\
\Rightarrow & \alpha \cap \beta & \neq & \emptyset \\
\Rightarrow & \alpha & = & \beta\big)
\end{array}$$

c'est-à-dire que C est injective.

Proposition IX.4.2.7 (L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, *)$) *Pour tout entier naturel n, il existe un unique couple de lois $(+, *)$ sur $\mathbb{Z}/n\mathbb{Z}$ tel que :*

i) $(\mathbb{Z}/n\mathbb{Z}, +, *)$ soit un anneau (cf. VII.1.1 ;)

ii) la surjection canonique π_n (cf. IX.4.2.5.1,) soit un morphisme d'anneaux (cf. VII.2.1.)

***Preuve** : Il faut montrer que la relation $\sim_n$ est compatibles aux lois $+$ et $*$ sur $\mathbb{Z}$ ce qui est fait au TD n° IV, exercice B, question 5) et au TD n° IV, exercice B, question 6).*

On pourrait aussi voir ce résultat comme un cas particulier de la proposition VII.7.3.

Remarque IX.4.2.8 On remarque, même si ce cas n'apporte rien par rapport à ce qu'on sait déjà, que si $n = 0$, la loi $+$ définie sur $\mathbb{Z}/0\mathbb{Z}$ qui s'identifie à $\mathbb{Z}$ comme ensemble, coïncide bien avec l'addition déjà connue sur $\mathbb{Z}$.

Le groupe $\mathbb{Z}/1\mathbb{Z}$ ne contient qu'un élément et son étude ne présente guère d'intérêt aussi nous considérerons les cas où $n > 1$ par la suite.

Proposition IX.4.2.9 (Éléments inversibles dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, *)$) *Soit un entier naturel $n > 1$ et $\alpha \in \mathbb{Z}/n\mathbb{Z}$. Les assertions suivantes sont équivalentes :*

a) L'élément α est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

b) Pour tout $a \in \alpha$, a et n sont premiers entre eux (cf. VII.5.9.)

c) Il existe $a \in \alpha$ tel que a et n sont premiers entre eux.

***Preuve** :*

*i) (**a)** $\Leftrightarrow$ **b**))*

Pour tout $\alpha \in \mathbb{Z}/n\mathbb{Z}$ α est inversible s'il existe $\beta \in \mathbb{Z}/n\mathbb{Z}$ tel que $\alpha * \beta = 1 \bmod n$ c'est-à-dire que pour tout $a \in \alpha$ et tout $b \in \beta$ $ab \equiv 1\,[n]$ c'est-à-dire encore qu'il existe $k \in \mathbb{Z}$ tel que $ab + nk = 1$ ce qui équivaut en vertu du théorème de BÉZOUT *(cf. IX.3.9.1,) au fait que a et b sont premiers avec n. On établit ainsi l'équivalence entre les assertions a) et b).*

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

Pour établir l'équivalence entre b) et c) il suffit de résoudre l'exercice qui consiste à montrer que a est premier avec n si et seulement si pour tout $a' \in a \bmod n$, a' et n sont premiers entre eux.

Définition IX.4.2.10 (Indicateur d'EULER) Pour tout entier naturel $n > 1$, on notera

$$\phi(n) \ := \ \#((\mathbb{Z}/n\mathbb{Z})^\times)$$

le nombre d'éléments inversibles (cf. VII.1.8,) dans lanneau $(\mathbb{Z}/n\mathbb{Z}, +, *)$ qu'on appelle l'*indicateur d'*EULER. La fonction ϕ définie de $\mathbb{N}$ dans $\mathbb{N}$ est appelée *fonction indicatrice d'*EULER. D'après la proposition ci-dessus et le point IX.4.2.6.iv) $\phi(n)$ est aussi le nombre d'entiers inférieurs ou égaux à n et premiers avec n.

Proposition IX.4.2.11 *Pour tout entier naturel $n > 1$, l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, *)$ est un corps c'est-à-dire que tous ses éléments non nuls sont inversibles si et seulement si n est un nombre premier (cf. VII.5.4,) si et seulement si $\phi(n) \ = \ n - 1$.*

***Preuve** : Tout d'abord il est clair sur la définition même de corps et celle de l'indicateur d'Euler $\phi(n)$ que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $\phi(n) = n - 1$.*

Reste donc à montrer que ceci équivaut encore au fait que n est un nombre premier. Si n est premier, pour tout $\alpha \ \in \ \mathbb{Z}/n\mathbb{Z}$,$\alpha \neq 0 \bmod n$ signifie que pour tout $a \ \in \ \alpha$, n ne divise pas a qui équivaut encore, puisque n est premier à ce que n et a sont premiers entre eux, donc que $\alpha \ = \ a \bmod n$ est inversible.

Supposons maintenant que tout $\alpha \ \in \ \mathbb{Z}/n\mathbb{Z}$ $\alpha \ \neq \ 0 \bmod n$, est inversible. Si n n'est pas premier, il existe $2 \leq m < n$ tel que $m|n$. Il en résulte que $m \bmod n \ \neq \ 0 \bmod n$ et que pour autant m et n ne sont pas premiers entre eux puisque $m \wedge n \ = \ m$ et donc que $m \bmod n$ n'est pas inversible.

IX.4.3 . −Arithmétique modulaire sur $\mathbb{K}[X]$

Proposition IX.4.3.1 *Soit $P \ \in \ \mathbb{K}[X]$ un polynôme irréductible non nul (ou premier ce qui revient au même en vertu du lemme d'Euclide (cf. IX.3.10.4,)) de degré $d > 0$. Alors :*

i) L'anneau $\mathbb{K}[X]/P\mathbb{K}[X]$ est un corps contenant $\mathbb{K}$.

ii) De plus l'inclusion $\mathbb{K} \subset \mathbb{K}[X]/P\mathbb{K}[X]$ donne à $\mathbb{K}[X]/P\mathbb{K}[X]$ une structure naturelle de $\mathbb{K}$-espace vectoriel qui est de dimension d.

***Preuve** : Notons*

$$\pi \ : \ \mathbb{K}[X] \ \to \ \mathbb{K}[X]/P\mathbb{K}[X] \ , \ P \ \mapsto \ \overline{P}$$

la surjection canonique dont on sait que c'est un morphisme d'anneaux.

i)

$$\forall \alpha \in \mathbb{K}[X]/P\mathbb{K}[X], \ \exists Q \ \in \ \mathbb{K}[X], \ \alpha \ = \ \pi(Q) \ \wedge \ \alpha \ \neq \ 0 \ \Rightarrow \ P \not| Q \ .$$

Comme P est irréductible, il existe $(U,V) \in \mathbb{K}[X] \times \mathbb{K}[X]$ tel que

$$PU + QV \ = \ 1 \ \Rightarrow \ \pi(PU+QV) \ = \ 1 \ \Rightarrow \ \alpha\pi(V) \ = \ 1$$

c'est-à-dire que tout $\alpha \in \mathbb{K}[X]/P\mathbb{K}[X]$ $\alpha \ \neq \ 0$ est inversible autrement dit que $\mathbb{K}[X]/P\mathbb{K}[X]$ est un corps.

Il est clair que l'injection naturelle $i \ : \ \mathbb{K} \ \rightarrow \ \mathbb{K}[X]$ qui à tout élément λ de $\mathbb{K}$ associe le polynôme constant λ est un morphisme d'anneaux. Il en va donc de même de $\pi \circ i$.

$$\forall \lambda \in \mathbb{K}, \ \forall \mu \in \mathbb{K}, \ \pi[i(\lambda)] \ = \ \pi[i(\mu)] \ \Leftrightarrow \ P | i(\lambda - \mu) \ .$$

Or $\deg(P) \ = \ d \ > \ 0$ et $\deg(i(\lambda-\mu)) \ \leq \ 0$, par conséquent, $i(\lambda-\mu) \ = \ 0 \ \Rightarrow \ \lambda - \mu \ = \ 0$ c'est-à-dire que $\pi \circ i$ est injective et qu'on peut donc considérer que $\mathbb{K}$ est un sous-corps de $\mathbb{K}[X]/P\mathbb{K}[X]$.

ii) On laisse le soin au lecteur de vérifier que

$$\cdot \ : \ \mathbb{K} \times \mathbb{K}[X]/P\mathbb{K}[X] \ \rightarrow \ \mathbb{K}[X]/P\mathbb{K}[X] \ , \ (\lambda, \alpha) \ \mapsto \ \lambda \cdot \alpha \ := \ \pi[i(\lambda)]\alpha$$

donne à $\mathbb{K}[X]/P\mathbb{K}[X]$ une structure de $\mathbb{K}$-espace vectoriel.

$$\forall \alpha \in \mathbb{K}[X]/P\mathbb{K}[X], \ \exists Q \ \in \ \mathbb{K}[X], \ \alpha \ = \ \pi(Q) \ .$$

Or si R est le reste de la division euclidienne de Q par P, $\deg(R) \ < \ d$ et $\pi(R) \ = \ \alpha$. Il existe donc $\lambda_{j \ , 0 \leq j \leq d-1} \ \in \ \mathbb{K}$ tels que

$$R \ = \ \sum_{j=0}^{d-1} \lambda_j X^j$$

(où l'on revient ici à une notation plus conventionnelle et où l'on note simplement $\lambda \ = \ i(\lambda)$.) Si bien que :

$$\alpha \ = \ \sum_{j=0}^{d-1} \pi(\lambda_j)\pi(X)^j \ . \qquad 1$$

Il s'ensuit que la famille $\pi(X)^{j \ , 0 \ \leq \ j \ \leq \ d-1}$ est une famille génératrice de $\mathbb{K}[X]/P\mathbb{K}[X]$.

Or si

$$\alpha \ = \ \sum_{j=0}^{d-1} \pi(\mu_j)\pi(X)^j,$$

en posant $S \ := \ \sum_{j=0}^{d-1} \mu_j X^j$, on a $\pi(R) \ = \ \alpha \ = \ \pi(S)$ c'est-à-dire que $P | R - S$. Or $\deg(R-S) \ \leq \ d-1 \ < \ d$ si bien que $R - S \ = \ 0$ c'est-à-dire que la décomposition 1 est unique et que par conséquent la famille $\pi(X)^{j \ , 0 \ \leq \ j \ \leq \ d-1}$ est une base du $\mathbb{K}$-espace vectoriel $\mathbb{K}[X]/P\mathbb{K}[X]$.

IX.5 . −Le théorème chinois des restes

Notation IX.5.1 i) Pour tout idéal I de A, on notera $\pi_I \,:\, A \,\to\, A/I$ la surjection canonique (cf. VII.7.4.)

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

ii)

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

la projection du produit sur le $k^{\text{ième}}$ facteur (cf. VII.7.14,)

iii) Il existe alors un unique morphisme d'anneaux

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

caractérisé par le fait que

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

(cf. VII.7.14,) Plus explicitement, pour tout $x \,\in\, A$,

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

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

v) Enfin on notera

$$\psi_{\mathcal{I}} \text{ ou simplement } \psi \,:\, A \,\to\, A/\big(\bigcap_{1\,\leq\, j\,\leq\, n} A/I_j\big)$$

la surjection canonique.

On peut synthétiser ces notations dans le diagramme suivant :

$$\begin{array}{ccc} A & \xrightarrow{\pi_{\mathcal{I}}} & \prod_j 1nA/I_j \\ {\scriptstyle \psi_{\mathcal{I}}}\big\downarrow & \searrow\, \pi_{I_k} & \big\downarrow{\scriptstyle p_k} \\ A/\big(\bigcap_{1\,\leq\, j\,\leq\, n} A/I_j\big) & & A/I_k\;. \end{array} \qquad \text{IX.5.1.1}$$

Proposition IX.5.2 *Soient $n \,\in\, \mathbb{N}, \mathcal{I} \,:=\, I_1\,,_{k\leq 1\leq n}$ un n-uplet d'idéaux de A.*

i) Il existe un unique morphisme injectif d'anneaux

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

ii) Si les idéaux $I_{k\ ,1\leq k\leq n}$ sont deux à deux comaximaux (cf. VII.4.18,) π est surjective et partant γ est surjective et donc un isomorphisme.

***Preuve** : Cet énoncé n'est en fait qu'une généralisation de VII.8.15.question 3). Cependant nous allons en redonner une preuve ici.*

i) Déterminons tout d'abord $\mathrm{Ker}\,\pi$ *: Pour tout* $x \in A$,

$$\begin{array}{rcl} \pi(x) & = & 0 \\ \Leftrightarrow \quad \forall 1 \leq k \leq n,\ p_k[\pi(x)] & = & 0 \\ \Leftrightarrow \quad \forall 1 \leq k \leq n,\ \pi_k(x) & = & 0 \\ \Leftrightarrow \quad \forall 1 \leq k \leq n,\ x & \in & I_k \\ \Leftrightarrow \quad x & \in & A/\big(\bigcap_{1\ \leq\ j\ \leq\ n} A/I_j\big)\ . \end{array}$$

On utilise ici la caractérisation du noyau de la surjection canonique donnée en VII.7.4.ii).

La proposition VII.7.8 assure alors l'existence et l'unicité du morphisme γ comme demandé.

ii) Si les idéaux $I_{k\ ,1\leq k\leq n}$ sont deux à deux comaximau, cela signifie que

$$\forall 1 \leq k \leq n,\ \forall 1 \leq j \leq n,\ k \neq j, I_k \text{ et } I_j \text{ sont comaximaux}$$

c'està-dire que $I_k + I_j = A$, ou encore que $1 \in I_k + I_j$ c'est-à-dire qu'il existe $u_{k,j} \in I_k$ et $u_{j,k} \in I_j$ tels que $u_{k,j} + u_{j,k} = 1$. Cela entraîne encore que :

$$\begin{array}{rcl} \pi_k(u_{k,j}) & = & 0 \\ \pi_k(u_{j,k}) & = & 1 \\ \pi_j(u_{k,j}) & = & 1 \\ \pi_j(u_{j,k}) & = & 0\ . \end{array}$$

Posons alors

$$\forall 1 \leq k \leq n,\ u_k := \prod_{1\ \leq\ j\ \leq\ n,\ j\neq k} u_{j,k}\ .$$

On a alors

$$\pi_k(u_k) = \pi_k\big(\prod_{1\ \leq\ j\ \leq\ n,\ j\neq k} u_{j,k}\big) = \prod_{1\ \leq\ j\ \leq\ n,\ j\neq k} \pi(u_{j,k}) = 1$$

et

$$\forall 1 \leq j \leq n,\ j \neq k\ ,\ \pi_j\big(\prod_{1\ \leq\ j\ \leq\ n,\ j\neq k} u_{j,k}\big) = \prod_{1\ \leq\ j\ \leq\ n,\ j\neq k} \pi_j(u_{j,k}) = 0\ .$$

Pour tout $\alpha \in \prod_j 1nA/I_j$, *notons*

$$\forall 1 \leq k \leq n,\ \xi_k := p_k(\alpha) \in A/I_k\ .$$

Alors pour tout $1 \leq k \leq n$ *il existe* $x_k \in A$ *tel que* $\pi_k(x_k) = \xi_k$. *Définissons finalement* $x \in A$, *par* $x := \sum_{k=1}^{n} x_k * u_k$. *Il s'ensuit alors que, pour tout* $1 \leq k \leq n$

$$\begin{aligned} p_k[\pi(x)] &= \pi_k(x) \\ &= \pi_k\big(\sum_{j=1}^{n} x_j * u_j\big) \\ &= \sum_{j=1}^{n} \pi_k(x_j * u_j) \\ &= \sum_{j=1}^{n} \pi_k(x_j) * \pi_k(u_j) \\ &= \pi_k(x_k) * \pi_k(u_k) \\ &= \pi_k(x_k) \\ &= \xi_k \end{aligned}$$

ce qui assure que $\pi(x) = \alpha$ *et donc que* π *est surjective.*

Pour tout $\alpha \in \prod_j 1nA/I_j$, *il existe donc* $x \in A$ *tel que* $\pi(x) = \alpha$, *ce qui entraîne que*

$$\gamma[\psi(x)] = \alpha$$

et donc que γ *est surjective.*

Remarque IX.5.3 Une lecture attentive montrera que dans la preuve de la proposition IX.5.2 il n'a jamais été fait usage du fait que A est un anneau principal ni d'aucun des résultats que nous avons établis pour ce type d'anneau . De toute façon le résultat de la proposition IX.5.2 avait déjà été établi en VII.8.15.question 3) avant même que la notion d'anneau principal ne soit introduite.

La particularité du cas des anneaux principaux va consister à traduire en termes de PGCD l'hypothèse que les idéaux sont deux à deux comaximaux grâce au corollaire IX.3.2, et conduira à la forme suivante (théorème IX.5.4,) plus usuelle, du théorème chinois des restes. Des formulations plus particulières encores dans le cas de l'anneau $\mathbb{Z}$ (resp. de l'anneau $\mathbb{K}[X]$) pourront être données en IX.5.5.1 (resp. IX.5.6.1.)

Théorème IX.5.4 *Soient $n \in \mathbb{N}$, $a_{k\ ,1\leq k\leq n}$ des éléments de A et m un* ***Ppcm*** *(cf. IX.2.6,) des $a_{k\ ,1\leq k\leq n}$.*

Pour tout $1 \leq k \leq n$ on note $\pi_k : A \to A/a_kA$ (qui correspond à la notation donnée en IX.5.1.iv) pour peu qu'on définisse l'idéal I_k par $I_k := a_kA$. Il s'en déduit comme en IX.5.1.iii) un morphisme d'anneaux

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

Notons encore $\psi : A \to A/mA$ la surjection canonique (qui n'est autre que le morphisme ψ défini en IX.5.1.v) dans la mesure où

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

(cf. IX.2.6.))

Alors :

i) Il existe un unique morphisme injectif d'anneaux

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

ii) Si les $a_{k\ ,1\leq k\leq n}$ sont <u>deux à deux</u> premiers entre eux (cf. VII.5.9,) le morphisme π est surjectif ce qui entraîne que γ est surjectif et donc un isomorphisme.

Preuve *: Ce théorème est bien entendu un corollaire de la proposition IX.5.2 pour peu qu'on remarque que si pour tout $1 \leq k \leq n$ $I_k := a_kA$:*

—

$$mA = A/\big(\bigcap_{1 \leq j \leq n} A/I_j\big)$$

comme on l'a déjà remarqué ce qui permet de déduire i) de IX.5.2.i) ;

— *l'hypothèse que les $a_{k\ ,1\leq k\leq n}$ sont deux à deux premiers entre eux équivaut au fait que les idéaux $I_{k\ ,1\leq k\leq n}$ sont deux à deux comaximaux en vertu du corollaire IX.3.2, ce qui permet de déduire ii) de IX.5.2.ii).*

IX.5.5 . −Théorème chinois des restes sur $\mathbb{Z}$

Théorème IX.5.5.1 (Théorème chinois des restes) *Soient*

$$n > 1 \text{ un entier naturel et } a_{i\ ,1\leq i\leq n} > 1$$

des entiers naturels. On note m le ***Ppcm*** *(cf. VII.5.11,) des a_i et $\pi_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ la surjection canonique*

i) L'application

$$\begin{array}{rccc} \pi : & \mathbb{Z} & \longrightarrow & \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z} \\ & x & \longmapsto & (x \bmod a_1, \ldots, x \bmod a_n) \end{array} \qquad 1$$

est un morphisme d'anneaux de $(\mathbb{Z}, +, *)$ dans $(\mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z}, +, *)$ muni de la structure produit définie en VII.7.14.

ii) Il existe un unique morphisme injectif d'anneaux :

$$\gamma : (\mathbb{Z}/m\mathbb{Z}, +, *) \to (\mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z}, +, *) \text{ tel que } \gamma \circ \pi_m = \pi . \qquad 1$$

iii) Si les $a_{i\ ,1\leq i\leq n}$ sont deux à deux premiers entre eux (cf. VII.5.9,) γ est surjectif et donc bijectif (cf. I.2.4.iii),) et l'application réciproque γ^{-1} est aussi un morphisme d'anneaux. Dans ce cas, on a

$$m = \prod_{i=1}^{n} a_i .$$

Preuve *:*

i) Est une vérification facile.

ii) Les morphismes π et μ_m sont en particulier des morphismes de groupes pour les lois $+$. De plus on a

$$\forall x \in \mathbb{Z},\ \big(x \in \operatorname{Ker}\pi \Leftrightarrow \forall 1 \leq i \leq n,\ clmodxa_i = 0 \Leftrightarrow \forall 1 \leq i \leq n,\ a_i | x \Leftrightarrow m | x \Leftrightarrow x \in m\mathbb{Z}\big)$$

c'est-à-dire que $\operatorname{Ker}\pi = m\mathbb{Z}$. Il résulte alors de VII.7.8 qu'il existe un unique morphisme injectif de groupes

$$\gamma : (\mathbb{Z}/m\mathbb{Z}, +, *) \to (\mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z}, +, *) \text{ tel que } \gamma \circ \pi_m = \pi .$$

Or

$$\begin{array}{l} \forall x \in \mathbb{Z}/m\mathbb{Z},\ \forall y \in \mathbb{Z}/m\mathbb{Z},\ \big(\\ \exists u \in \mathbb{Z},\ \exists v \in \mathbb{Z},\ (\pi_m(u) = x \wedge \pi_m(v) = y) \wedge \end{array} \begin{array}{rcl} \gamma(x * y) & = & \gamma[\pi_m(u) * \pi_m(v)] \\ & = & \gamma[\pi_m(u * v)] \\ & = & \pi(u * v) \\ & = & \pi(u) * \pi(v) \\ & = & \gamma(x) * \gamma(y)\big) \end{array}$$

en utilisant ici que π_m et π sont des morphismes d'anneaux.

Enfin

$$\gamma(1) \;=\; \gamma[\pi_m(1)] \;=\; \pi(1) \;=\; 1$$

en utilisant encore que π_m et π sont des morphismes d'anneaux.

iii) Si les $a_{i\,,1\leq i\leq n}$ sont deux à deux premiers entre eux, alors pour tout $1 \;\leq\; i \;\leq\; n$ et tout $1 \;\leq\; j \;\leq\; n$ avec $i \neq j$, il existe un couple d'entiers relatifs $(u_{i,j}, v_{i,j})$ tels que

$$a_i u_{i,j} \;+\; a_j v_{i,j} \;=\; 1$$

(cf. IX.3.9.1.) Posons alors, pour tout $1 \;\leq\; i \;\leq\; n$

$$e_i \;:=\; \prod_{1\,\leq\, j\,\leq\, n\,,\; j\neq i} a_j v_{i,j}\;.$$

Il est alors élémentaire de vérifier que

$$e_i \;\equiv\; 1\,[a_i] \;et\; e_i \;\equiv\; 0\,[a_j]\;\forall 1 \leq j \leq n,\; j \neq i\;.$$

Pour tout $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}/a_1 \times \ldots \times \mathbb{Z}/a_n$, soit $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ tel que pour tout $1 \;\leq\; i \;\leq\; n\; x_i \in \alpha_i$.

Posons finalement

$$x \;:=\; \prod_{i=1}^{n} x_i e_i\;.$$

C'est un calcul élémentaire sur les règles de congruence de montrer que, pour tout $1 \;\leq\; i \;\leq\; n$ $x \;\equiv\; x_i\,[a_i]$ c'est-à-dire que π est surjective. Il s'ensuit en vertu de VII.7.8 que γ l'est aussi.

L'application γ et donc un isomorphisme (cf. VII.2.4.)

Corollaire IX.5.5.2 (Application à la résolution des systèmes de congruence) *Étant donnés*

$$\begin{cases} \text{un entier naturel } n \geq 1, \\ \text{un } n\text{-uplet d'entiers naturels } a_{i\,,1\leq i\leq n} \\ \text{et un } n\text{-uplet d'entiers relatifs } k_{i\,,1\leq i\leq n}\,, \end{cases}$$

le système de congruences

$$(x \;\equiv\; k_i\,[a_i]\,,\; 1 \;\leq\; i \;\leq\; n)\,,$$

a pour solution la classe de congruence (modulo $\prod_{i=1}^{n} a_i$) $\gamma^{-1}(k_1 \bmod a_1, \ldots, k_n \bmod a_n)$ si les a_i sont deux à deux premiers entre eux.

Preuve : *Le système de congruences*

$$(x \equiv k_i\,[a_i]\ ,\ 1 \leq i \leq n)$$

équivaut (cf. IX.4.2.6.i),) à

$$(x \bmod a_i = k_i \bmod a_i\ ,\ 1 \leq i \leq n)$$

c'est-à-dire (cf. IX.5.5.1.i).1,)

$$pi(x) = (k_1 \bmod a_1, \ldots, k_n \bmod a_n)$$

c'est-à-dire encore, par définition même de γ, à

$$\gamma(x \bmod \prod_{i=1}^{n} a_i) = (k_1 \bmod a_1, \ldots, k_n \bmod a_n)$$

autrement dit, puisque γ est un isomorphisme (sous l'hypothèse que les a_i sont deux à deux premiers entre eux (cf. IX.5.5.1.iii)))

$$x \bmod \prod_{i=1}^{n} a_i = \gamma^{-1}(k_1 \bmod a_1, \ldots, k_n \bmod a_n)\ .$$

Corollaire IX.5.5.3 *Étant donnés des entiers naturels $n \geq 1$, $d \geq 1$, $a_{i\ ,1\leq i\leq n}$ tels que les a_i sont deux à deux premiers entre eux et des entiers relatifs $b_{i\ ,0\leq i\leq d}$, l'équation*

$$\sum_{i=0}^{d} b_i x^i \equiv 0\ [\prod_{j=1}^{n} a_j]$$

d'inconnue $x \in \mathbb{Z}$ équivaut au système

$$\left(\sum_{i=0}^{d} b_i \bmod a_j x \bmod a_j^i = 0\ ,\ 1 \leq j \leq n\right)\ .$$

Preuve : *C'est une conséquence immédiate du fait que γ est un isomorphisme d'anneaux (cf. IX.5.5.1.iii),) mais peut s'avérer fort utile, surtout si on peut faire en sorte que les a_i soient des nombres premiers car alors, $\mathbb{Z}/a_i\mathbb{Z}$ est un corps (cf. IX.4.2.11,) et il apparaîtra qu'il est infiniment plus confortable de résoudre des équations polynomiales dans un corps que dans un anneau quelconque.*

Remarque IX.5.5.4 Il existe de nombreuses variantes du théorème IX.5.5.1 mais nous n'en présenterons qu'une ici :

Étant donnés deux entiers naturels a et b et $d := a \wedge b$ et deux entiers relatifs k et l le système de congruences

$$\left\{\begin{array}{rcl} x & \equiv & k\,[a] \\ x & \equiv & \ell\,[b] \end{array}\right\}$$

a des solutions si et seulement si $d|k-\ell$ et dans ce cas, l'ensemble de ses solutions est une classe de congruence modulo $(a, b \vee .)$ On peut même expliciter cette dernière. Si, en effet, (u, v) est un couple d'entiers relatifs tel que $d = au + bv$ (dont l'existence est assurée par le théorème IX.2.7.1.i),) et si l'on note $a := da'$ et $b := db'$, on constate que $a'u + b'v = 1$ et si $d|k-\ell$, $x := \ell a'u + kb'v$ est une solution du système ci-dessus.

On pourrait énoncer un résultat encore plus précis, en disant que l'application

$$\begin{array}{rcl} \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z}/d\mathbb{Z} \\ (x, y) & \mapsto & (x \bmod d, y \bmod d) \end{array}$$

induit un morphisme de groupes $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ dont le noyau est $\mathbb{Z}/(a, b \vee \mathbb{Z})$.

IX.5.6 . −Théorème chinois des restes sur $\mathbb{K}[X]$

Proposition IX.5.6.1 (Théorème chinois des restes) *Soient $(P, Q) \in \mathbb{K}[X] \times \mathbb{K}[X]$ un couple de polynômes et M leur* ***Ppcm****. On note*

$$\pi_P : \mathbb{K}[X] \to \mathbb{K}[X]/P\mathbb{K}[X]\,,\ \pi_Q : \mathbb{K}[X] \to \mathbb{K}[X]/Q\mathbb{K}[X] \text{ et } \pi_M : \mathbb{K}[X] \to \mathbb{K}[X]/M\mathbb{K}[X]$$

les surjections canoniques, $\mathbb{K}[X]/P\mathbb{K}[X] \times \mathbb{K}[X]/Q\mathbb{K}[X]$ l'anneau produit défini comme en VII.7.14, et

$$\begin{array}{rccl} \pi : & \mathbb{K}[X] & \longrightarrow & \mathbb{K}[X]/P\mathbb{K}[X] \times \mathbb{K}[X]/Q\mathbb{K}[X] \\ & R & \longmapsto & \big(\pi_P(R), \pi_Q(R)\big)\,. \end{array}$$

i) Il existe un unique morphisme injectif d'anneaux γ tel que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} \mathbb{K}[X] & & \\ {\scriptstyle \pi_M}\downarrow & \searrow {\scriptstyle \pi} & \\ \mathbb{K}[X]/M\mathbb{K}[X] & \xrightarrow{\gamma} & \mathbb{K}[X]/P\mathbb{K}[X] \times \mathbb{K}[X]/Q\mathbb{K}[X]\,. \end{array}$$

ii) Si P et Q sont premiers entre eux, γ est surjectif et est donc un isomorphisme.

Preuve *: (cf. VIII.5.8.)*

Remarque IX.5.6.2 Bien entendu le résultat du théorème IX.5.6.1 ci-dessus peut s'étendre à une famille finie de polynômes deux à deux premiers entre eux .

IX.6 . −Théorème fondamental de l'arithmétique

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

Lemme IX.6.1 *Tout élément $a \in A \setminus A^\times$ possède un diviseur irréductible.*

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

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

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

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

Notons $\mathfrak{I}_n := a_nA$, l'idéal engendré par a_n. Puisque $a_{n+1}|a_n$, la suite $\left(\mathfrak{I}_n\right)_{,n\in\mathbb{N}}$ est croissante. Il résulte alors de la proposition VII.4.6.iv), que $\mathfrak{I} := \bigcup_{n\in\mathbb{N}} \mathfrak{I}_n$ est un idéal de A.

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

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

On a

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

si bien que

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

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

Remarque IX.6.2 En considérant attentivement la preuve du lemme IX.6.1, on constate qu'on a montré que dans un anneau principal toute suite croissante d'idéaux est stationnaire à partir d'un certain rang. Un anneau possédant cette propriété est dit *noethérien*.

Théorème IX.6.3 (fondamental de l'arithmétique) *i) Pour tout élément $a \in A, a \neq 0$, il exist un entier $n \in \mathbb{N}$ des éléments irréductibles $p_{i\ ,1\leq i\leq n}$ deux à deux non associés, des entiers naturels $\alpha_{i\ ,1\leq i\leq n} \in \mathbb{N}$, et un élément inversible u tels que :*

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

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

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

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

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

Preuve *:*

i) Si $a \in A^\times$ est inversible, prenons simplement $u := a$ et $n := 0$.

Sinon construisons des suites $\left(a_n\right)_{,n\in\mathbb{N}}$ et $\left(b_n\right)_{,n\in\mathbb{N}}$ à valeurs dans A de la manière suivante : $a_0 := a$ et $b_0 := 1$. Pour tout $n \in \mathbb{N}$,

— si a_n n'est pas irréductible on choisit b_{n+1} un diviseur irrréductible de a_n qui existe en vertu du lemme IX.6.1, et on définit a_{n+1} par

$$a_n = a_{n+1} * b_{n+1} .$$

— si a_n est irréductible, on pose $a_{n+1} := a_n$ et $b_{n+1} := 1$.

On définit la suite d'idéaux $\left(I_n\right)_{,n\in\mathbb{N}}$ par $I_n := a_nA$. Puisque, pour tout $n \in \mathbb{N}$, $a_{n+1}|a_n$, la suite $\left(I_n\right)_{,n\in\mathbb{N}}$ est croissante. Par le même argument que dans la preuve du lemme IX.6.1 et que nous avons mis en évidence dans la remarque IX.6.2, on peut montrer que la suite $\left(I_n\right)_{,n\in\mathbb{N}}$ est stationnaire à partir d'un certain rang ; autrement dit il existe $p \in \mathbb{N}$ tel que $I_p = I_{p+1}$. Cela entraîne, pour peu que $a_p \neq 0$, que b_{p+1} est inversible et donc vaut 1 puisque b_n est soit irréductible soit vaut 1 et qu'un élément irréductible n'est pas inversible par définition. Il s'ensuit, par construction des suites $\left(a_n\right)_{,n\in\mathbb{N}}$ et $\left(b_n\right)_{,n\in\mathbb{N}}$, que a_n est irréductible et également que

$$a = \prod_{i=1}^{n} -1b_i * a_n .$$

L'élément a s'écrit donc comme un produit d'irréductibles. Quitte à regroupper les éléments associés on obtient la formule demandée.

ii) Nous allons raisonner par récurrence sur l'entier $n := \max(d, e)$.

$n = 1$ *Pour* $n = 1$, *l'identité ii).1 s'écrit* $u * p^\alpha = v * q^\beta$. *Il en résulte, d'après le lemme d'Euclide (cf. IX.3.6,) que* $p|q$ *i.e.il existe* $w \in A$, *tel que* $q = p * w$. *Or* p *et* q *sont irréductibles donc* p *n'est pas inversible ; si bien que* w *est inversible. Il s'ensuit que* p *et* q *sont associés. Il découle presqu'immédiatement du fait que* A *est intègre que* $\alpha = \beta$.

— *Supposons l'implication établie pour* $n \geq 1$ *et supposons que* $\max(d, e) = n + 1$.

Il est clair que l'identité ii).1 implique que $p_d | \prod_{i=1}^{e} q_i^{\beta_i}$. p_d *étant irréductible, on peut appliquer le lemme d'Euclide (cf. IX.3.6,) d'où il résulte qu'il existe* $1 \leq i \leq e$ *tel que* $p_d | q_i$. *On peut, quitte à renuméroter (c'est le rôle que joue la bijection* σ,) *supposer que* $i = e$. *Le même argument que précédemment montre que* p_d *et* q_e *sont associés. L'identité ii).1 s'écrit donc*

$$u' * \prod_{i=1}^{d-1} p_i^{\alpha_i} = v' * \prod_{i=1}^{e-1} q_i^{\beta_i} .$$

Comme $\max(d-1, e-1) = n$, *on peut appliquer l'hypothèse de récurrence et conclure.*

Remarque IX.6.4 On pourra être surpris de voir ici que la décomposition en produit de facteurs premiers (irréductibles) apparaît comme une conséquence du lemme de GAUSS (cf. IX.3.3,) ou du lemme d'Euclide (cf. IX.3.6,) alors que souvent l'on présente ces deux résultats comme conséquence de la décomposition en produit de facteurs premiers. On pourrrait montrer qu'en fait ces propriétés sont équivalentes pour un anneau et qu'en particulier un anneau dans lequel le théorème de BÉZOUT est vérifié, les possède.

Définition IX.6.5 (Valuation p-adique) Le théorème IX.6.3.ii) assure que pour tout

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

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

IX.6.6 . −Théorème fondamental de l'arithmétique

Théorème IX.6.6.1 (fondamental de l'arithmétique) *Pour tout*

$$n \in \mathbb{N} , \ n > 1 ,$$

i) Soit n est un nombre premier (cf. IX.3.9.6,) soit il existe un nombre premier p tel que $p|n$ et $p < n$.

ii) Il existe un entier naturel $d \geq 1$ et des nombres premiers p_i ,$1 \leq i \leq d$ tels que

$$n \ = \ \prod_{i=1}^{d} p_i \ . \qquad 1$$

iii) Étant donnés des entiers d et e et des nombres premiers p_i ,$1 \leq i \leq d$, et des nombres premiers q_i ,$1 \leq i \leq e$,

$$\prod_{i=1}^{d} p_i \ = \ \prod_{i=1}^{e} q_i \qquad 1$$

si et seulement si $d = e$ et il existe une bijection $\sigma : [1; d] \to [1; d]$ telle que pour tout $1 \leq i \leq d$, $p_i = q_{\sigma(i)}$.
(Voir le théorème IX.6.3 et comparer au théorème IX.6.7.1.)

***Preuve** :*

i) On remarque que l'ensemble des diviseurs de 2 est $\{-2; -1; 1; 2\}$ donc que 2 est premier.
Notons D l'ensemble des entiers $n > 1$ tels que, pour tout entier naturel $1 < k \leq n$, soit k est un nombre premier soit k possède un facteur premier $p < k$.
Nous venons de montrer que $2 \in D$. Si maintenant $n \in D$, soit $n + 1$ est premier et donc $n+1 \in D$, soit il existe $k \in \mathbb{Z}$ tel que $k|n + 1$ et $k \notin \{-n-1; -1; 1; n+1\}$. Il en résulte que $|k||n + 1$ et $|k| \leq n$. Soit donc $|k|$ est premier, et dans ce cas $n+1 \in D$, soit il existe $p < |k|$ premier et divisant $|k|$. Il en résulte qu'alors $p|n + 1$ et $p < n + 1$ et donc que $n + 1 \in D$.
L'ensemble D satisfait donc au principe de récurrence II.0.PA$_3$) ce qui achève la preuve.

ii) Notons D l'ensemble des entiers naturels $n > 1$ tels que, pour tout $k \leq n$, k admette une décomposition de la forme ii).1. Il est clair que $2 \in D$. Si $n \in D$, soit $n + 1$ est premier, et donc $n + 1 \in D$, soit $n + 1$ possède un facteur premier d'après le point précédent $2 \leq p < n + 1$. Il existe alors $m \in \mathbb{N}$ tel que $n + 1 = pm$. Or $2 \leq p$ implique $m < n + 1$ c'est-à-dire $m \leq n$ et l'on peut donc appliquer l'hypothèse de récurrence à m et conclure que $n + 1$ possède donc une décomposition ii).1 et appartient de ce fait à D. Ce dernier satisfait donc au principe de récurrence ce qui permet de conclure.

iii) Nous allons raisonner par récurrence sur l'entier $n := \max(d, e)$ *. Pour* $n = 1$*, l'identité iii).1 s'écrit* $p_1 = q_1$ *et le résultat est immédiat.*

Supposons l'implication établie pour $n \geq 1$ *et supposons que* $\max(d, e) = n + 1$.

Il est clair que l'identité iii).1 implique que $p_d | \prod_{i=1}^{e} q_i$*. L'entier* p_d *étant un nombre premier, on peut appliquer le lemme d'Euclide (cf. IX.3.9.4,) d'où il résulte qu'il existe* $1 \leq i \leq e$ *tel que* $p_d | q_i$*. On peut, quitte à renuméroter (c'est le rôle que joue la bijection* $\sigma,)$ *supposer que* $i = e$*. Cependant* $p_d | q_e$ *et* q_e *premier implique que* $p_d \in \{-q_e; -1; 1; q_e\}$*. Or* p_d *lui-même est premier, donc positif et différent de* 1 *donc* $p_d = q_e$*. L'identité iii).1 s'écrit donc*

$$\prod_{i=1}^{d-1} p_i = \prod_{i=1}^{e-1} q_i \, .$$

Comme $\max(d - 1, e - 1) = n$*, on peut appliquer l'hypothèse de récurrence et conclure.*

Définition IX.6.6.2 On exprimera le fait que tout entier naturel $n > 1$ satisfait à la proposition IX.6.6.1.ii) en disant que n admet une *décomposition en produit de facteurs premiers* et l'on dira, en vertu du point IX.6.6.1.iii), et de manière un peu abusive, que cette décomposition est *unique*.

Corollaire IX.6.6.3 *Pour tout entier relatif* $z \in \mathbb{Z} \setminus \{-1; 0; 1\}$ *il existe un unique entier naturel* $d \geq 1$*, un unique (à permutation près)* d*-uplet* $p_{i\,,1 \leq i \leq d}$ *d'entiers irréductibles (ou premiers) et un unique* $\epsilon \in \{-1; 1\}$ *tels que*

$$z = \epsilon \prod_{i=1}^{d} p_i \, .$$

Preuve *: C'est un corollaire presque immédiat de du théorème IX.6.6.1.*

IX.6.7 . −Théorème fondamental de l'arithmétique

Théorème IX.6.7.1 (fondamental de l'arithmétique) *Pour tout polynômes* $P \in \mathbb{K}[X], P \neq 0$*, il existe une unique (à permutation près) famille de polynômes irréductibles unitaires* $P_{i\,,1 \leq i \leq d}$ *deux à deux premiers entre eux, une unique famille* $\alpha_{i\,,1 \leq i \leq d}$ *et un unique* $\lambda \in \mathbb{K}$ *tels que*

$$P = \lambda \prod_{i=1}^{d} P_{ii}^{\alpha} \, .$$

IX.7 . −Algorithme d'EUCLIDE

Il ne suffit pas que l'anneau A soit principal pour qu'on puisse mettre en œuvre l'algorithme d'Euclide, celui-ci s'appuyant en effet sur la *division euclidienne*. Les anneaux $\mathbb{Z}$ (cf. IV.5.2,) et $\mathbb{K}[X]$ (cf. VIII.4.2,) disposent néanmoins de cette propriété. Nous allons introduire la notion d'anneau euclidien à seule fin de donner une dénommination commune à ces situations et remarquer que les anneaux euclidiens sont principaux de manière à pouvoir utiliser toutes les ressources dévloppées dans le paragraphe IX, à propos des anneaux principaux..

Définition IX.7.1 Étant donné un anneau commutatif intègre A, un *stathme euclidien* sur A est une application

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

vérifiant :

$$\forall (a,b) \in A \times (A\setminus\{0\}),\ \exists (q,)r \in A \times A,\ a = b*q + r \text{ et } \big(r = 0 \text{ ou } \mathbf{v}(r) < \mathbf{v}(b)\big), \qquad \text{IX.7.1.1}$$

$$\forall (a,b) \in (A \setminus \{0\}) \times (A \setminus \{0\}),\ \mathbf{v}(b) \leq \mathbf{v}(a*b)\ . \qquad \text{IX.7.1.2}$$

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

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

Exemple IX.7.2 a) $((\mathbb{Z}, |\cdot|))$

L'anneau $\mathbb{Z}$ muni de la valeur absolue est un anneau euclidien (cf. IV.5.)

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

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

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

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

d) (**Entiers de GAUSS**)

(cf. Problème n° VII.)

Remarque IX.7.3 On constate que dans la définition IX.7.1 aucun énoncé d'unicité du couple (q, r) n'est donné contrairement à ce qui est le cas dans le cas de l'anneau $\mathbb{Z}$ au théorème IV.5.2 ou même pour l'anneau $\mathbb{K}[X]$ (cf. VIII.4.2.) Dans ces deux cas, le stathme euclidien considéré possède une propriété supplémentaire de « compatibilité » à l'addition $|a+b| \leq |a| + |b|$, $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$ qui n'est pas exigé par les axiomes IX.7.1.1 et IX.7.1.2. On constatera que l'anneau des entiers de GAUSS (cf. Problème n° VII,) n'a pas de telle propriété et que néanmoins une arithmétique similaire à celle des anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ peut y être développée.

En particulier l'absence d'énoncé d'unicité dans la division euclidienne n'interdit pas de montrer que l'anneau est principal comme nous allons le voir dans la proposition IX.7.4 qui peut servir de point de départ à toute l'arithmétique de ces anneaux.

Proposition IX.7.4 *Un anneau euclidien $(A, \mathbf{v})$ (où A est un anneau commutatif intègre et $\mathbf{v}$ un stathme euclidien) est principal.*

Preuve : *Soit donc $\mathfrak{I}$ un idéal de A. Si $\mathfrak{I} = 0$, $\mathfrak{I} = 0A$ est un idéal principal.*

Sinon il existe un élément $a \in \mathfrak{I}$, $a \neq 0$. L'ensemble $\mathbf{V} := \{\mathbf{v}(a)\ ,\ a \in \mathfrak{I} \setminus \{0\}\}$ est donc une partie non vide de $\mathbb{N}$, qui admet donc un plus petit élément. Choisissons donc $b \in \mathfrak{I}$ tel que $\mathbf{v}(b) = \min(\mathbf{V})$.

Puisque $\mathfrak{I}$ est un idéal, pour tout $x \in A$, $b * x \in \mathfrak{I}$ si bien que $bA \subset \mathfrak{I}$.

Pour tout $a \in \mathfrak{I}$, écrivons, grâce à IX.7.1.1, $a = b*q+r$. Comme $a \in \mathfrak{I}$ et $b*q \in \mathfrak{I}$, $r = a - b*q \in \mathfrak{I}$. Or soit $r = 0$, soit $\mathbf{v}(r) < \mathbf{v}(b)$. Comme $\mathbf{v}(b) = \min(\mathbf{V})$, $r = 0$, c'est-à-dire que $a = b*q$ i.e. $a \in bA$ ce qui entraîne $\mathfrak{I} \subset bA$ et finaelement

$$\mathfrak{I} = bA\ .$$

Remarque IX.7.5 En lisant atentivement la preuve de la proposition IX.7.4 ci-dessus, on constate qu'on y retrouve exactement les arguments de la preuve du corollaire IV.5.5 ainsi que ceux de la preuve du théorème VIII.4.4.

Proposition IX.7.6 (Algorithme d'EUCLIDE) *Soit $(A, \mathbf{v})$ un anneau euclidien (cf. IX.7.1.) Étant donnés deux éléments a_0 et a_1 de A, l'algorithme d'Euclide consiste en la donnée des suites*

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

définies par récurrence de la manière suivante :

$$\begin{array}{rcl} u_0 & := & 1 \\ u_1 & := & 0 \\ v_0 & := & 0 \\ v_1 & := & 1\ ; \end{array} \qquad \textit{IX.7.6.1}$$

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

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

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

$$\begin{array}{rcl} u_{n+2} & := & u_n - q_n * u_{n+1} \\ v_{n+2} & := & v_n - q_n * v_{n+1}\,. \end{array} \qquad \textit{IX.7.6.2}$$

Alors :

i) Soit

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

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

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

ii)

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

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

iii)

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

iv) L'élément $a_{m \in A}$ *est un PGCD pour* a_0 *et* a_1, u_m *et* v_m *des coefficients de* BÉZOUT *(cf. IX.2.4.)*

Preuve *:*

i) Remarquons d'abord que s'il existe $p \in \mathbb{N}$, *tel que* $a_p = 0$, *pour tout* $q \geq p$, $a_q = 0$. *En effet, si, pour* $k \in \mathbb{N}$, $a_{p+k} = 0$, *par définition de la suite* $\big(a_n\big)_{,n\in\mathbb{N}}$, $a_{p+k+1} = 0$, *si bien que l'on peut démontrer, par récurrence, que pour tout* $k \in \mathbb{N}$, $a_{p+k} = 0$. *Cela peut encore se reformuler en disant que l'ensemble* $E := \{n \in \mathbb{N}\,;\ a_n \neq 0\}$ *est un intervalle* $[0;\xi[$ *où* ξ *peut être un entier naturel dans le cas où* E *est fini ou bien* $+\infty$ *dans le cas où* $E = \mathbb{N}$.

Si la suite $\big(a_n\big)_{,n\in\mathbb{N}}$ *n'est pas identiquement nulle,* $E \neq \emptyset$. *Si*

$$E = [0;1[\,=\,[0;0]\ (\textit{resp. } E = [0;2[\,=\,[0;1]\,)$$

on a $m = 0$ *(resp.* $m = 1$.*)*

Sinon considérons la restriction du stathme euclidien $\mathbf{v}$ *à* E *qui est une application de* E *dans* $\mathbb{N}$. *Puisque* $E \neq [0;0]$ *et* $E \neq [0;1]$, $\mathbf{v}\big(E \setminus [0;1]\big)$ *est une partie non vide de* $\mathbb{N}$, *qui possède donc un plus petit élément* μ. *Il existe donc* $m \in E \setminus [0;1]$ *tel que* $\mathbf{v}(a_m) = \mu$. *Pour tout* $n \geq 1$, *il résulte de IX.7.1.1, que si* $n+1 \in E$, $\mathbf{v}(a_{n+1} < \mathbf{v}(a_n)$. *Il s'ensuit que* $a_{m+1} \notin E$ *et que* $E = intff1m$.

ii) Est un exercice facile.

iii) Les identité

$$a_0 \;=\; a_0 * u_0 \;+\; a_1 * v_0 \text{ et } a_1 \;=\; a_0 * u_1 \;+\; a_1 * v_1$$

sont satisfaites par définitions même des suites (cf. IX.7.6.1.)

Supposons donc établie la relation iii) pour n *et* $n+1$. *On a alors, en vertu de IX.7.6.2,*

$$\begin{aligned} a_{n+2} &= a_n - q_n * a_{n+1} \\ &= a_0 * u_n + a_1 * v_n - q_n * (a_0 * u_{n+1} + a_1 * v_{n+1}) \\ &= a_0 * (u_n - q_n * u_{n+1}) + a_1 * (v_n - q_n * v_{n+1}) \\ &= a_0 * u_{n+2} + a_1 * v_{n+2} \end{aligned}$$

ce qui prouve le résultat par récurrence.

iv) Si $m \;=\; 0$, *par construction (cf. i),) la suite* $\left(a_n\right)_{,n\in\mathbb{N}}$ *est soit identiquement nulle auqel cas le PGCD de* a_0 *et* a_1 *est* 0, *soit* $a_1 \;=\; 0$, *auquel cas un PGCD de* a_0 *et* 0 *est bien* a_0.

Supposons donc $m \;\geq 1$. *par définition de* m, $a_{m+1} \;=\; 0$. *Il s'ensuit que* a_m *est un PGCD de* a_m *et* a_{m+1}. *En raisonnant par récurrence grâce à ii), on montre que c'est aussi un PGCD de* a_0 *et* a_1.

Enfin grâce à iii), on a bien

$$a_m \;=\; a_0 * u_m \;+\; a_1 * v_m \;.$$

Exemple IX.7.7 On peut [7] mettre en oeuvre l'algorithme d'Euclide de la manière suivante :

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

d'où il résulte que

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

7. On n'a jamais dit « on doit »

Remarque IX.7.8 En considérant attentivement la proposition IX.7.6, on constaterait qu'il n'est nul besoin de savoir a priori qu'il existe un PGcD dans l'anneau A. En particulier nul besoin de savoir si l'anneau A est principal ou non. l'algorithme d'Euclide établit directement l'existence du pGCD à partir de la division euclidienne. Comme il donne également les coefficients de BÉZOUT il permet de démontrer le théorème de BÉZOUT sans recours au formalisme des idéaux. Reformuler le théorème chinois des restes dans ce contexte commencerait peut-être à devenir moins séduisant moins encore si on s'avisait d'en donner une formulation pour l'anneau $\mathbb{K}[X]$.

IX.7.9 . −Algorithme d'Euclide sur $\mathbb{Z}$

Proposition IX.7.9.1 (Algorithme d'Euclide) *Étant donnés deux entiers relatifs a_0 et a_1, l'algorithme d'Euclide consiste en la donnée des suites*

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

définies par récurrence de la manière suivante :

$$\begin{array}{rcl} u_0 & := & 1 \\ u_1 & := & 0 \\ v_0 & := & 0 \\ v_1 & := & 1\,; \end{array} \qquad \textit{IX.7.9.1.1}$$

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

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

sinon, q_n est le quotient de la division euclidienne (cf. IV.5.4,) de a_n par a_{n+1} et $a_{n+2}:=a_n-q_na_{n+1}$ le reste. On pose alors :

$$\begin{array}{rcl} u_{n+2} & := & u_n-q_nu_{n+1} \\ v_{n+2} & := & v_n-q_nv_{n+1}\,. \end{array} \qquad \textit{IX.7.9.1.2}$$

Alors :

i) Soit

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

soit

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

ii)

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

iii)

$$\forall n \in \mathbb{N},\ a_n \ = \ au_n + bv_n \ .$$

(voir la proposition IX.7.6 et comparrer à la proposition IX.7.10.1.)

Corollaire IX.7.9.2 *Avec les notations de la proposition IX.7.9.1, si* $(a_0, a_1) \ \neq \ (0,0)$, a_m *est un PGCD de* a_0 *et* a_1 *et* (u_m, v_m) *des coefficients de* BÉZOUT. *Si* a_0 *et* a_1 *sont positifs, (autrement dit des entiers naturels) il en est de même de* a_m *qui est alors le PGCD au sens usuel de* a_0 *et* a_1.

IX.7.10 . −Algorithme d'EUCLIDE sur $\mathbb{K}[X]$

Proposition IX.7.10.1 (Algorithme d'EUCLIDE) *Soient* P_0 *et* P_1 *des éléments de* $\mathbb{K}[X]$ *non tous deux nuls. On définit une suite* P_n *par récurrence pour tout* $n \geq 2$:

— *si* $P_{n-1} \ = \ 0$, $P_n \ := \ 0$;

— *sinon,* P_n *est le reste de la division euclidienne de* P_{n-2} *par* P_{n-1}.

Alors :

i) Il existe un entier naturel m, *tel que* $P_m \neq 0$ *et pour tout* $n > m$, $P_m = 0$.

ii) Pour tout entier naturel n, *il existe un couple* (U_n, V_n) *d'éléments de* $\mathbb{K}[X]$ *tel que*

$$P_n \ = \ U_n * P_0 \ + \ V_n * P_1 \ .$$

En particulier, il existe un couple (U, V) *d'éléments de* $\mathbb{K}[X]$ *tel que*

$$P_m \ = \ U * P_0 \ + \ V * P_1 \qquad 1$$

iii) Si pour tout élément $P \ \in \ \mathbb{K}[X]$, *on note* $\mathcal{D}(P)$ *l'ensemble de ses diviseurs, pour tout* $n \ \in \ \mathbb{N}\ P_{n+1} = 0$ *ou*

$$\mathcal{D}(P_n) \cap \mathcal{D}(P_{n+1}) \ = \ \mathcal{D}(P_{n+1}) \cap \mathcal{D}(P_{n+2})$$

en particulier

$$\mathcal{D}(P_m) \ = \ \mathcal{D}(P_0) \ \cap \ \mathcal{D}(P_1) \ . \qquad 1$$

(voir la proposition IX.7.6 et comparer à la proposition IX.7.9.1.)

Preuve *: Seul le point i) de cette proposition nécessite des arguments nouveaux par rapport à ceux donnés pour l'anneau* $\mathbb{Z}$ *dans la proposition IX.7.9.1 ou dans le cas général pour les anneaux euclidiens dans la proposition IX.7.6.*

Pour $n \geq 2$, *si* $P_n \neq 0$, $\deg(P)_n < \deg(P)_{n-1}$ *(cf. VIII.4.2.) On en déduit, par récurrence, que* P_{n+1} *est soit nul, soit* $\deg(P)_{n+1} \leq \deg(P)_1 - n$. *Le degré d'un polynôme étant un entier positif, nécessairement, soit* $P_1 = 0$ *et dans ce cas,* $P_n = 0$ *pour tout* $n \geq 1$, *soit pour* $n > \deg(P)_1$, $P_{n+1} \ = \ 0$.

On vient donc de montrer que l'ensemble des entiers n *tels que* $P_n \neq 0$, *est une partie majorée de* $\mathbb{N}$ *et possède donc un plus grand élément* m.

IX.8 . −Exercices

Exercice IX.8.1 [] Pour $X \subset A$, montrer que d et un PGCD de X si et seulement si d est un générateur de $\bigcap_{y \in \mathcal{D}(X)} yA$.

Exercice IX.8.2 [] Montrer que pour $X \subset A$ et $Y \subset A$,

1) () si on note d un PGCD de X et e un PGCD de Y f est un PGCD de $X \cup Y$ si et seulement si f est un PGCD de d et e.

2) () Énoncer et démontrer un résulta analogue pour les PPCM.

Exercice IX.8.3 [] Étant donné un anneau principal intègre A, notons $\mathcal{P}$ un ensemble de représentants des classes d'association des éléments irréductibles.

1) () Montrer que pour tout $a \in A$, il existe un unique $u \in A^\times$ tel que

$$a = u * \prod_{p \in \mathcal{P}} p^{v_p(a)} .$$

2) () **Pour tout couple** $(a, b) \in A \times A$,

a) () montrer que d (resp. m) est un PGCD (resp. un PPCM) de a et b si et seulement si

$$d = u * \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))} \text{ (resp. } m = u * \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))} .$$

b) () En déduire que $m * d$ et $a * b$ sont associés.

3) () Montrer que

$$\forall (a, b) \in A \times A,\ \forall p \in \mathcal{P},\ v_p(a * b) = v_p(a) + v_p(b) \text{ et } v_p(a + b) \geq \min(v_p(a), v_p(b))$$

avec égalité dans la dernière inégalité si $v_p(a) \neq v_p(b)$.

Exercice IX.8.4 [Valuations p-adiques]
Soit $p \in \mathcal{P}$.

1) () Pour tout $x \in \mathbb{Z}$, $x \neq 0$, montrer qu'il existe un unique couple $(r_x, y_x) \in \mathbb{N} \times \mathbb{Z}$ tel que :

$$x = p^{r_x} y_x \text{ et } p \wedge y_x = 1 .$$

Dans la suite on notera

$$\forall x \in \mathbb{Z},\ x \neq 0\ ,\ v_p(x) := r_x \text{ et } v_p(0) := (+\infty)$$

qu'on appelle la *valuation* p-*adique* de x. On définit donc ainsi, pour tout $p \in \mathcal{P}$, une application $v_p : \mathbb{Z} \to \overline{\mathbb{N}}$.

2) () Pour tout $x \in \mathbb{Q}\ ,\ x \neq 0$, montrer qu'il existe un unique triplet

$(r_x, n_x, d_x) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{N}^*$ tel que $x = p^{r_x}\dfrac{n_x}{d_x}\ ,\ n_x \wedge d_x = 1\ ,\ p \wedge d_x = 1$ et $p \wedge n_x = 1$.

On peut donc prolonger l'application v_p en une application $v_p : \mathbb{Q} \to \overline{\mathbb{Z}}$ en posant

$$v_p(x) := r_x\ \forall\ x \in \mathbb{Q}\setminus\{0\} \text{ et } v_p(0) := (+\infty)\ .$$

Pour tout $x \in \mathbb{Q}\setminus\{0\}$, on notera

$$\mathcal{S}(x) := \{p \in \mathbb{P}\ ;\ v_p(x) \neq 0\} \text{ et } \mathcal{S}(0) := \mathcal{P}\ .$$

3) () **(Propriétés de v_p)**
Établir les propriétés suivantes de v_p :

Val$_1$)

$$\forall x \in \mathbb{Z},\ \forall y \in \mathbb{Z},\ x|y \Rightarrow \forall p \in \mathcal{P},\ v_p(x) \leq v_p(y)\ .$$

Val$_2$) Pour tout $x \in \mathbb{Z}\setminus\{0\}$, (resp. tout $x \in \mathbb{Q}\setminus\{0\}$,) $\mathcal{S}(x)$ est un ensemble fini éventuellement vide et que l'on a

$$x = \epsilon \prod_{p\in\mathcal{S}(x)} p^{v_p(x)}\ ,\ \epsilon \in \{-1, 1\}\ .$$

Val$_3$) La réciproque de Val$_1$) est vraie.

Val$_4$)

$$\forall x \in \mathbb{Q},\ x \in \mathbb{Z} \Leftrightarrow v_p(x) \geq 0\ \forall\ p \in \mathcal{P}\ .$$

Val$_5$)

$$\forall x \in \mathbb{Q},\ \forall y \in \mathbb{Q},\ \forall p \in \mathbb{P},\ v_p(xy) = v_p(x) + v_p(y) \text{ et } v_p(x+y) \geq \min(v_p(x), v_p(y))$$

avec égalité dans la dernière inégalité si $v_p(x) \neq v_p(y)$.

Val$_6$)

$$\forall\ (x, y) \in \left(\mathbb{Z}\setminus\{0\}\right)^2\ ,\ x \wedge y = \prod_{p\in\mathcal{P}} p^{\min(v_p(x),v_p(y))} \text{ et } [x, y] = \prod_{p\in\mathcal{P}} p^{\max(v_p(x),v_p(y))}\ .$$

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

TD n° I

Logique, ensembles, applications, relations

Exercice A : Écrire la négation des assertions suivantes où P, Q, R, S sont des propositions.

1) $P \Rightarrow Q$,

2) P et non Q,

3) P et (Q et R),

4) P ou (Q et R),

5) (P et Q) $\Rightarrow$ $(R \Rightarrow S)$.

Exercice B : (**Intersection** $(\cap)$ **et réunion** $(\cup)$)

1) Étant donnés trois ensembles $A,\ B$ et C tels que

$$A \cup B \subset A \cup C \text{ et } A \cap B \subset A \cap C$$

que peut on dire de B et C ?

2) Étant donné un ensemble E, A et B des parties de E, résoudre les équations d'inconnue $X \in \mathcal{P}(E)$:

$$A \cup X = B\ ;\ A \cap X = B\ .$$

Exercice C : (**Propriétés des applications**)
Soit $f : E \to F$ **une application.**

1) **a)** Montrer que

$$\forall A \in \mathcal{P}(F),\ f(f^{-1}(A)) \subset A\ .$$

b) Montrer que f est surjective si et seulement si

$$\forall A \in \mathcal{P}(F),\ A = f(f^{-1}(A))\ .$$

2) (**Injectivité (facultatif)**)

a) Montrer que

$$\forall A \in \mathcal{P}(E),\ A \subset f^{-1}(f(A))\,.$$

b) Montrer que f est injective si et seulement si

$$\forall A \in \mathcal{P}(E),\ A = f^{-1}(f(A))\,.$$

Exercice D : (**Surjection**)
Étant donnée une application $f : A \to B$, démontrer que les propositions suivantes sont équivalentes

i) f est surjective.

ii) il existe une application g de B dans A telle que $f \circ g = \mathrm{Id}_B$.
On dit alors que g est une *section* de f.
Une telle section est elle unique ? Démontrer que si deux sections ont même image elles coïncident.

Exercice E : Donner la preuve de la proposition I.5.4.

Exercice F : Faire la preuve de la proposition I.5.6.

Exercice G : Soit E un ensemble.

1) On suppose que E est muni d'une relation d'équivalence R. On note $\pi : E \to E/R$ la surjection canonique.

Montrer que si F est un ensemble et $f : E \to F$ une application constante sur les classes de R c'est-à-dire que

$$\forall x \in E,\ \forall y \in E,\ \big((xRy) \Leftrightarrow (f(x) = f(y))\big)$$

Il existe une unique application $\overline{f} : E/R \to F$ vérifiant $f = \overline{f} \circ \pi$.

2) Soit $p : E \to E'$ une application surjective et $f : E \to F$ une application constante sur les fibres de p, c'est-à-dire que

$$\forall x \in E,\ \forall y \in E,\ \big((p(x) = p(y)) \Leftrightarrow (f(x) = f(y))\big)\,.$$

Montrer qu'alors il existe une unique application $\overline{f} : E' \to F$ telle que $f = \overline{f} \circ p$.

Exercice H : On suppose que E est munie d'une relation d'équivalence R et d'une loi

$$\cdot : E \times E \to E\,.$$

On suppose que $\cdot$ et R sont *compatibles* c'est-à-dire que

$$\forall x, y, z, t \in E,\ \big(xRy \wedge zRt \Rightarrow x \cdot z\ R\ y \cdot t\big)\,.$$

On note $\pi : E \to E/R$ la surjection canonique.

1) Montrer qu'il existe une unique loi $\dagger : F \times F \to F$ tel que π soit un morphisme c'est-à-dire que

$$\forall x, y \in E?\ \big(\pi(x \cdot y) = \pi(x) \dagger \pi(y)\big)\,.$$

On parle alors de *structure quotient*.

2) Montrer que si $\cdot$ est associative, (resp. possède un élément neutre) (resp. est commutative) il en est de même de $\dagger$. Montrer que si $x \in E$ possède un symétrique y pour $\cdot$ alors $\pi(y)$ est le symétrique de $\pi(x)$ pour $\dagger$.

3) Montrer que si E est muni d'une autre loi $\times$ également compatible à R, qui induit une loi $\sharp$ sur F et si $\times$ est distributive sur $\cdot$ alors $\sharp$ est distributive sur $\dagger$.

4) Donner des exemples déjà connus des constructions précédentes.

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

TD n° II

Entiers naturels, axiome de récurrence

Dans les exercices qui suivent on suppose établies les propriétés de l'addition $+$ sur $\mathbb{N}$ *i.e.*on considère comme acquis les résultats du paragraphe II.1.

Exercice A : (**La multiplication dans** $\mathbb{N}$)

On suppose donné, dans cet exercice, un ensemble $\mathbb{N}$ contenant un élément 0, muni d'une application $\mathfrak{s} : \mathbb{N} \to \mathbb{N}$ et d'une applications $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ satisfaisant les axiomes II.0.PA$_1$), II.0.PA$_2$), II.0.PA$_3$), II.1.1.PA$_4$) et II.1.1.PA$_5$).

On veut définir la multiplication $* : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ satisfaisant les axiomes :

PA$_6$) (Mult$_1$)

$$\forall p \in \mathbb{N},\ (0 * p = 0)\,.$$

PA$_7$) (Mult$_2$)

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \big(\mathfrak{s}(p) * q = (p * q) + q\big)\,.$$

ainsi qu'un certain nombre d'autres propriétés.

1) On cherche à définir une application $\pi : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ ou encore un élément de $(\mathbb{N}^{\mathbb{N}})^{\mathbb{N}}$ de la manière suivante :

i) $\pi(0) := 0$ *i.e.*

$$\forall n \in \mathbb{N},\ \pi(0)(n) = 0\,;$$

ii)

$$\forall n \in \mathbb{N},\ \pi(\mathfrak{s}(n)) = \pi(n) + \mathrm{Id}_{\mathbb{N}}\,,\ \textit{i.e.}\ \forall n \in \mathbb{N},\ \forall p \in \mathbb{N},\ \pi(\mathfrak{s}(n))(p) = \pi(n)(p) + p\,.$$

Montrer que π est bien définie c'est-à-dire que le domaine de définition D de π est égal à $\mathbb{N}$.

2) On note désormais,

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ p * q := \pi(p)(q)\,.$$

Vérifier que $*$ ainsi définie vérifie les axiomes PA$_6$) et PA$_7$).

Exercice B : ($f(n) \geq n$)

Soient $n \in \mathbb{N}$ et $f : [0; n] \to \mathbb{N}$ une application strictement croissante.

1) Montrer que pour tout $0 \leq k \leq n$ $f(k) \geq k$.

2) A-t-on, sans hypothèse supplémentaire $f(k) > k$?

3) Que deviennent les résultats ci-dessus si f est simplement croissante ?

Exercice C : Soient p et q deux entiers naturels.

1) Montrer qu'il existe une application injective $f : [0;p] \to [0;q]$ si et seulement si $p \leq q$.

2) En déduire qu'il existe une application bijective $f : [0;p] \to [0;q]$ si et seulement si $p = q$.

3) En déduire qu'il n'existe pas d'application injective $f : \mathbb{N} \to [0;p]$.

Exercice D : (**Intersection et réunion de parties finies**)

Soit E un ensemble A et B des parties de E. On suppose que A (resp. B ,) est une partie finie et que $\#(A) = p \in \mathbb{N}$ (resp. $\#(B) = q \in \mathbb{N}$.)

1) Montrer que $\#(A \cup B) \leq p + q$.

2) Montrer que $\#(A \cap B) \leq \min(p, q)$.

Exercice E : (**Parties à k éléments**)

Pour deux entiers naturels n et k on note $\binom{n}{k}$ le nombre de parties à k éléments dans un ensemble à n éléments. On ne supposera connue, avant qu'elle n'ait été démontrée, aucune des propriétés de ce nombre et en particulier son expresion en fonction de k et de n qu'on établira à la question 3).

1) Rappeler pourquoi

$$\forall n \in \mathbb{N},\ \forall k \in \mathbb{N},\ \left(k > n \ \Rightarrow\ \binom{n}{k} = 0\right) .$$

2) Montrer que

$$\forall n \in \mathbb{N},\ \forall k \in \mathbb{N},\ \left(\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}\right) .$$

Indication : *Dans un ensemble à $n+1$ éléments, on pourra fixer un élément x, et considérer les parties à $k+1$ éléments qui contiennent x d'une part et celles qui ne le contiennent pas d'autre part.*

3) On pose $0! := 1$ et $\forall n \in \mathbb{N},\ (n+1)! := (n+1) * n!$.

Déduire de ce qui précède que

$$\forall n \in \mathbb{N},\ \forall k \in \mathbb{N},\ \left(k \leq n \ \Rightarrow\ \binom{n}{k} = \frac{n!}{(n-k)!k!}\right) .$$

4) On adoptera la convention que $\forall a \in \mathbb{Z},\ a^0 = 1$.

Montrer que

$$\forall n \in \mathbb{N},\ \forall a \in \mathbb{Z},\ \forall b \in \mathbb{Z},\ \left((a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right) .$$

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

TD n° III

Groupes, morphismes, sous-groupes

Exercice A : Pour chacun de ces ensembles, déterminer s'il est un groupe ou non.
- — $(\mathbb{R},\ +)$,
- — $(\mathbb{R},\ \times)$,
- — $(\mathbb{C}^*,\ \times)$,
- — $([0,1],+)$,
- — $(\mathbb{Q}[\sqrt{2}]^*,\ \times)$,
- — $(\mathbb{R}^* \times \mathbb{R},\ *)$ où $*$ est définie, pour $n \in \mathbb{N}^*$, par

$$(x,y) * (x',y') := (xx', xy' + yx'^n) .$$

Exercice B : (**Unicité des éléments remarquables**)
Soit $(E,*)$ un ensemble muni d'une loi associative.

1) (**Élément neutre**)
Montrer que si $(E,*)$ possède un élément neutre ϵ celui-ci est unique.

2) (**Symétrique**)
Montrer que si $(E,*)$ possède un élément neutre ϵ, tout élément $x \in E$ possède au plus un symétrique.

Exercice C : (**Morphismes de groupes**)
Soit

$$f : (G,*,\epsilon_G) \to (H,\bullet,\epsilon_H)$$

un morphisme de groupes.

1) (**Élément neutre**)
Montrer que $f(\epsilon_G) = \epsilon_H$.

2) (**Symétrique**)
Montrer que pour tout $x \in G$, si y est son symétrique, $f(y)$ est le symétrique de $f(x)$.

3) (**Image**)
Montrer que $\mathrm{Im}\, f$ est un sous-groupe de $(H,\bullet)$.

4) (**Noyau**)
Montrer que $\mathrm{Ker}\, f$ est un sous-groupe de $(G,*)$.

5) (**Isomorphisme**)
Montrer que si f est bijective et que g est son applications réciproque, alors g est un morphisme de groupe.

Exercice D : (**Intersection de deux sous-groupes**)
Pour deux sous-groupes H et K d'un groupe G, $H \cap K$ est un sous-groupe de G.

Exercice E : (**Union de deux sous-groupes**)
Étant donnés des sous-groupes H et K d'un groupe commutatif $(G, +)$, montrer que $H \cup K$ est un sous-groupe de $(G, +)$ si et seulement si $H \subset K$ ou $K \subset H$.
Indication : *Montrer qu'il revient au même de démontrer que [$H \not\subset K$ et $H \cup K$ sous-groupe entraîne $K \subset H$] puis prouver cette dernière assertion.*

Exercice F : Faire la preuve de la proposition III.3.6.iv).

Exercice G : Soit S une partie de G et H une autre partie de G. Montrer que les assertions suivantes sont équivalentes :

a) L'ensemble H est l'intersection de tous les sous-groupes de G contenant S.

b) L'ensemble H est un sous-groupe de G contenant S et tel que, pour tout sous-groupe K de G contenant S, $H \subset K$.

c) H est constitué des éléments $t_1 t_2 \dots t_r$ avec $r \geq 1$ où un élément t_i est dans S ou a son inverse dans S.

Exercice H : (**Somme de groupes abéliens**)
Montrer que si G est un groupe abélien, H et K deux sous-groupes de G,

$$H + K \ = \ \{x \ \in \ G \, ; \, \exists y \ \in \ H, \, \exists z \ \in \ K, \, x \ = \ y + z\} \, .$$

Exercice I : **Soit**

$$\mathcal{SO}_2(\mathbb{R}) \ := \ \left\{ M(\theta) \ := \ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \, \theta \in \mathbb{R} \right\} \, .$$

Montrer que $(\mathcal{SO}_2(\mathbb{R}), \, \times)$ est un groupe abélien, et que l'application

$$\begin{array}{rccc} M : & (\mathbb{R}, +) & \longrightarrow & \mathcal{SO}_2(\mathbb{R}) \\ & \theta & \longmapsto & M(\theta) \end{array}$$

est un morphisme de groupes.

Exercice J : Soit

$$P \ \subset \ \mathbb{R}^3 \text{ et } G \ := \ \{g \ \in \ \mathcal{SO}_3(\mathbb{R}) \, ; \, g(P) \ = \ P\} \, .$$

Montrer <que G est un sous-groupe de $\mathcal{SO}_3(\mathbb{R})$.

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

TD n° IV

Entiers relatifs

Exercice A : (**Caractérisation des sous-groupes de** $\mathbb{Z}$)

Montrer qu'une partie $H \subset \mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ si et seulement s'il existe un entier naturel d tel que

$$H \ = \ d\mathbb{Z} \ = \ \{dz \ , \ z \in \mathbb{Z}\} \ .$$

Exercice B : **1)** 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**

$$a \ \equiv \ b \, [n] \ .$$

2) 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 .

3) **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 ?

4) Donner le cardinal de $\mathbb{Z}/n\mathbb{Z}$.

5) Un entier naturel n étant fixé, montrer que, pour tout quadruplet (a, b, a', b') d'entiers relatifs,

$$a \ \equiv \ a' \, [n] \text{ et } b \ \equiv \ b' \, [n] \ \Rightarrow \ a + b \ \equiv \ a' + b' \, [n] \ .$$

6) Sous les mêmes hypothèses qu'à la question précédente, montrer que

$$a \ \equiv \ a' \, [n] \text{ et } b \ \equiv \ b' \, [n] \ \Rightarrow \ ab \ \equiv \ a' * b' \, [n] \ .$$

Exercice C : (**L'addition sur** $\mathbb{Z}/n\mathbb{Z}$)

Pour tout entier $n \geq 2$, **on note**

$$\mathbb{Z}/n\mathbb{Z} \textbf{ l'ensemble des classes de congruence modulo } n$$
$$\text{et} \quad \pi_n \,:\, \mathbb{Z} \,\to\, \mathbb{Z}/n\mathbb{Z} \textbf{ la surjection canonique (cf. exercice B.)}$$

1) 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 .)

2) 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.

3) Montrer que la loi $+$ ainsi définie sur $\mathbb{Z}/n\mathbb{Z}$ est la seule telle que π_n soit un morphisme de groupes.

4) Montrer qu'en tant que morphisme de groupes, π_n s'identifie au morphisme $\epsilon_{\overline{1}}$ défini comme dans le Problème n° III, exercice A.

Exercice D : (**Numération en base** b)

Dans tout cet exercice b **est un entier naturel strictement supérieur à** 1. **On cherche à établir le résultat suivant : pour tout entier relatif** z **non nul, il existe un unique** $\epsilon \in \{-1, 1\}$, **un unique entier naturel** d **et un unique** $d+1$**-uplet** $z_{i\ ,0\leq i\leq d}$ **tels que :**

$$\forall\, 0 \leq i < d\ ,\ 0 \leq z_i < b\ ; \qquad \textbf{1}$$

$$0 < z_d < b\ ; \qquad \textbf{2}$$

$$z \;=\; \epsilon \sum_{i=0}^{d} z_i b^i\ . \qquad \textbf{3}$$

1) (**Existence**)

a) Pour tout $n \in \mathbb{N}^*$, montrer qu'il existe un plus grand entier $\deg(n)$ tel que $b^{\deg(n)} \leq n$ et qu'alors $b^{\deg(n)+1} > n$.

b) Montrer qu'il existe des entiers q et r tels que $n \;=\; b^{\deg(n)}q + r$ avec $0 < q < b$ et $0 \leq r < b^{\deg(n)}$.

c) En déduire que pour tout $n \in \mathbb{N}^*$, il existe un entier d, et des entiers $n_{i\ ,0\leq i\leq d}$ satisfaisant aux conditions 1 et 2 de l'énoncé et tels que

$$n \;=\; \sum_{i=0}^{d} n_i b^i\ .$$

d) Généraliser le résultat précédent à un entier $z \in \mathbb{Z}^*$.

2) (**Unicité**)

Pour $z \in \mathbb{Z}^*$, on suppose donnés dans cette question, un élément ϵ (resp. η) de $\{-1, 1\}$, un entier naturel d (resp. $e,$) un $d+1$-uplet $x_{i\ ,0\leq i\leq d}$ (resp. un $e+1$-uplet $y_{i\ ,0\leq i\leq e}$) satisfaisant respectivement aux conditions 1 à 3.

a) Montrer que $\epsilon = \eta$.

b) Montrer que

$$\sum_{i=0}^{d} x_i b^i < b^{d+1} .$$

En déduire que si l'on suppose $d < e$ on aboutit à une contradiction. Conclure que $d = e$.

c) Montrer que b divise $x_0 - y_0$ et en déduire que $x_0 = y_0$.

d) Montrer finalement (par récurrence) que $x_i = y_i$ pour tout $1 \leq i \leq d$.

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

TD n° V

Actions de groupe

Exercice A : (**Sous-groupe d'un groupe fini**)
Faire la preuve de la proposition V.6.3 et comparer avec la proposition III.3.4.

Exercice B : (**Sphère unité**)
L'espace vectoriel $\mathbb{R}^3$ étant muni de son produit scalaire canonique, on note $\mathcal{S}$ l'ensemble des vecteurs de norme 1 (la *sphère unité*.)

1) Montrer que les groupes $\mathcal{O}_3(\mathbb{R})$ et $\mathcal{SO}_3(\mathbb{R})$ agissent sur $\mathcal{S}$.

2) L'action de $\mathcal{O}_3(\mathbb{R})$ (resp. $\mathcal{SO}_3(\mathbb{R})$) sur $\mathcal{S}$ est-elle transitive ?

Exercice C : (**Pôles d'une isométrie**)
Les notations étant par ailleurs celles de l'exercice B, on considère un sous-groupe G de $\mathcal{SO}_3(\mathbb{R})$. Pour tout $f \in \mathcal{SO}_3(\mathbb{R})$, ses pôles sont les éléments $v \in \mathcal{S}$ tels que $f(v) = v$. On rappelle qu'un élément de $\mathcal{SO}_3(\mathbb{R})$ différent de l'identité a exactement deux pôles et on note P l'ensemble des pôles des éléments de $G \setminus \mathrm{Id}$.
Que l'on définit bien une action de G sur P par

$$(g, p) \mapsto g \cdot p := g(p) .$$

Est-elle transitive ?

Exercice D : **1)** Compléter la preuve de la proposition V.4.4.

2) Soit G un groupe fini.
Montrer que si H est un groupe dont le cardinal est moitié de celui de G, alors H est un sous-groupe distingué de G.

Exercice E : (**Équation aux classes**)
Soit $(G, *)$ un groupe dont on note e l'élément neutre.
Pour tout $(x, y) \in G \times G$, on dit que y est *conjugué à* x s'il existe $g \in G$ tel que $y = g^{-1} * x * g$. On notera $x \sim y$.

1) Montrer que la relation « est conjugué à » est une relation d'équivalence dite *relation de conjugaison* ce qui permettra de dire dorénavant x et y *sont conjugués*. On appellera *classe de conjugaison d'un élément* $x \in G$ et on notera $\overline{x}$ sa classe pour la relation de conjugaison.

2) On appelle *centre du groupe* G qu'on note $\mathcal{Z}(G)$ le sous-ensemble

$$\mathcal{Z}(G) \ := \ \{g \ \in \ G \, ; \, \forall h \in G, \ g * h \ = \ h * g\} \ \subset \ G \, .$$

a) Montrer que $\mathcal{Z}(G)$ est un sous-groupe distingué de G.

b) À quellle condition nécessaire et suffisante sur $\mathcal{Z}(G)$ G est-il abélien ?

c) Caractériser les éléments de $\mathcal{Z}(G)$ à l'aide de leur classe de conjugaison.

d) Montrer que si $G/\mathcal{Z}(G)$ est monogène alors G est abélien.

Indication : *On pourra penser à écrire (en le justifiant bien entendu !) un élément* $x \ \in \ G$ *sous la forme*

$$x \ = \ z * g^n \ , \ z \in \mathcal{Z}(G) \ , \ \overline{g} \ \textit{générateur de} \ G/\mathcal{Z}(G) \ , \ n \in \mathbb{N} \, .$$

3) Pour tout $x \in G$, on appelle *stabilisateur de* x et on note $\mathrm{Stab}_G(x)$ l'ensemble

$$\mathrm{Stab}_G(x) \ := \ \{g \ \in \ G \, ; \ x \ = \ g^{-1} * x * g\} \ \subset \ G \, .$$

a) Montrer que, pour tout $x \in G$, $\mathrm{Stab}_G(x)$ est un sous-groupe de G.

b) Quelle sous-groupe remarquable de G est contenu dans $\mathrm{Stab}_G(x)$ pour tout $x \in G$, Que vaut

$$\bigcap_{x \in G} \mathrm{Stab}_G(x) \ ?$$

Pour tout $x \in G$, tout $(y, z) \in G \times G$, on note $z \ \sim_x \ y$ si $y * z^{-1} \in \mathrm{Stab}_G(x)$.

c) Rappeler pourquoi $\sim_x$ est une relation d'équivalences.

d) Montrer que, pour tout $x \in G$, on a une bijection

$$G/ \sim_x \cong \ \overline{x} \, .$$

e) En déduire que si G est fini

$$\forall x \in G, \ \#(G) \ = \ \#(\overline{x}) \cdot \ \#(\mathrm{Stab}_G(x)) \, .$$

4) Soit p un nombre premier et $r \ \in \ \mathbb{N}^*$. on suppose désormais que $\#(G) \ = \ p^r$.

a) Montrer que si $r = 1$, *i.e.*$\#(G) \ = \ p$ G est cyclique et par conséquent abélien.

On suppose maintenant que $r \ \in \ \mathbb{N}^*$ est quelconque.

b) Quelles valeurs peut prendre $\#(\overline{x})$ pour $x \in G$?

Notons $\mathcal{C}$ l'ensemble des classes de conjugaison de G,

$$\mathcal{C}_0 \ := \ \{c \ \in \ \mathcal{C} \, ; \ \#(c) \ = \ 1\} \ \text{et} \ \mathcal{C}_\infty \ := \ \mathcal{C} \ \setminus \ \mathcal{C}_0 \, .$$

c) Montrer que

$$\#(\mathcal{Z}(G)) \ = \ \#(G) - \sum_{c \in \mathcal{C}_\infty} \#(c)$$

et en déduire que $p | \#(\mathcal{Z}(G))$.

d) En déduire qu'il existe $k \ \in \ \mathbb{N} \, 1 \ \leq \ k \ \leq \ r$ tel que $\#(\mathcal{Z}(G)) \ = \ p^k$.

e) Déduire de ce qui précède que, si $\#(G) \ = \ p^2$, G est abélien.

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

TD n° VI

Groupe symétrique

Exercice A : (**Permutations qui commutent**)
Montrer que si c_1 et c_2 sont deux cycles dans $\mathcal{S}_n$ de supports disjoints alors

$$c_1 c_2 \;=\; c_2 c_1 \;.$$

Généraliser le résultat pour

$$(s_1, s_2) \;\in\; \mathcal{S}_n \;\times\; \mathcal{S}_n \;\text{ quelconques}\;.$$

Exercice B : (**Exemples**)
Simplifier, quand c'est possible, les écritures suivantes :

$$(1,2)^2, \qquad (1,2,3)^2, \qquad (1,2,3)^3,$$
$$(1,2,3,4)^k, \quad 1 \le k \le 4 \qquad (1,2,3,4)(1,4,3,2), \qquad (1,2,3,4)(1,3)(1,2,3,4)^{-1},$$
$$(1,2)(2,3), \qquad \big((1,2)(3,4)\big)^2, \qquad \big((1,2)(3,4,5)\big)^6,$$
$$\big((1,2,3)(4,5,6)\big)^3, \qquad (1,2,3)(4,5,6)(1,2,3)^{-1}(4,5,6)^{-1}$$

Exercice C : **1) Soient**

$$s_1 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 6 & 8 & 9 & 1 & 2 & 4 & 7 \end{pmatrix} \text{ et } s_2 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 5 & 6 & 2 & 4 & 8 & 3 & 7 & 1 \end{pmatrix}$$

des éléments de $\mathcal{S}_9$.

a) Décomposer s_1 et s_2 en produit de cycles à supports deux à deux disjoints.

b) Donner l'ordre et la signature de s_1 et s_2.

c) Calculer

$$s_1^{2016} \text{ et } s_2^{2016}\;.$$

d) Les permutations s_1 et s_2 sont-elles conjuguées

i) dans $\mathcal{S}_9$?

ii) dans $\mathcal{A}_9$?

2) Quel est l'ordre maximal d'un élément de $\mathcal{S}_9$? Les éléments d'ordre maximal

a) sont-ils tous conjugués dans $\mathcal{S}_9$?

b) ont-ils tous même signature ?

c) sont-ils tous conjugués dans $\mathcal{A}_9$?

Exercice D : (**Engendrement par les transpositions**)

1) Soit $n \in \mathbb{N}\, \ell \in \mathbb{N}$, $\ell \geq 2$, c un ℓ-cycle dont on note $O_c(a)$ l'unique orbite non-triviale et $t := (c^{\ell-2}(a)\, c^{\ell-1}(a))$. Montrer que $c \circ t$ est soit l'identité soit un $\ell - 1$-cycle.

2) Déduire de ce qui précède (par récurrence) que pour tout ℓ-cycle c,

$$c = (a\, c(a)) \circ \ldots \circ (c^{\ell-2}(a)\, c^{\ell-1}(a)) .$$

3) En déduire que pour tout $s \in \mathcal{S}_n$, il existe r transpositions t_i, $1 \leq i \leq r$ telles que

$$s = t_1 \circ \ldots \circ t_r .$$

Exercice E : **1)** **a)** Montrer que, pour tout entier $n \geq 2$, $\mathcal{S}_n$ est engendré par les transpositions

$$(i, i+1)\,,_{1 \leq i \leq n-1} .$$

b) Montrer que si l'on omet l'une de ces transpositions l'ensemble de celles qui restent n'engendre plus $\mathcal{S}_n$.

2) Même question pour les transpositions $(1, i)\,,_{2 \leq i \leq n}$.

3) Montrer que $\mathcal{S}_n$ est engendré par $(1, 2)$ et le cycle $c := (1, 2, \ldots, n)$. (On pourra calculer le conjugué de $(1, 2)$ par les puissances de c .)

Exercice F : **1)** **a)** 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.

b) 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 G : ($\mathcal{S}_n \not\subset \mathcal{A}_{n+1}$)

1) Montrer qu'il n'existe pas de morphisme de groupe injectif $i : \mathcal{S}_4 \to \mathcal{A}_5$.
Indication : *On pourra raisonner sur le nombre d'éléments des groupes en question.*

2) Plus généralement, montrer que si $n \in \mathbb{N}^*$ est pair, il n'existe pas de morphisme injectif $i : \mathcal{S}_n \to \mathcal{A}_{n+1}$.
Indication : *On pourra penser à utiliser les valuations 2-adiques.*

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

TD n° VII

Anneaux

Exercice A : (**Propriétés élémentaires des anneaux**)
Soit $(A, +, *)$ **un anneau dont on note** 0 **l'élément neutre pour la loi** $+$.

1) Montrer que, pour tout $x \in A$, $0 * x = 0$.

2) Montrer que $(A^\times, *)$ est un groupe (abélien si A est commutatif.)

3) Pour $f : A \to B$ un morphisme d'anneaux, montrer que la restriction $f^\times$ de f à $A^\times$ est un morphisme de groupes à valeurs dans $B^\times$.

4) Montrer que pour tout anneau A il existe un unique morphisme d'anneaux $f : \mathbb{Z} \to A$.

Exercice B : (**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 C : **1)** Pour chacune des équations suivantes, déterminer l'ensemble des couples (x, y) d'entiers relatifs puis l'ensemble des couples (x, y) d'entiers naturels la satisfaisant.

a)

$$221x - 91y = 42 .$$

b)

$$2166x - 1547y = 1 .$$

2) (**Systèmes de congruences**)
Déterminer l'ensemble des entiers relatifs x satisfaisant

$$\mathcal{S} : \left\{ \begin{array}{rcl} 13x & \equiv & 1\ [2166] \\ x & \equiv & 6\ [221] \\ x & \equiv & 58\ [91] \end{array} \right\} .$$

Indication : *On pourra chercher à résoudre d'abord*

$$\left\{ \begin{array}{rcl} x & \equiv & 6\ [221] \\ x & \equiv & 58\ [91] \end{array} \right\}$$

Dans l'exercice D l'anneau $\mathbb{G}$ est celui introduit au Problème n° VII.

Exercice D : Soit $p \in \mathbb{Z}$ un nombre premier. On note (p) l'idéal engendré par p dans $\mathbb{G}$.

1) Montrer que les assertions suivantes sont équivalentes.

i) L'élément p n'est pas irréductible dans $\mathbb{G}$.

ii) Il existe $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$.

2) Montrer que les anneaux $\mathbb{G}/(p)$ et $(\mathbb{Z}/p\mathbb{Z}[X])/(X^2 + 1)$ sont isomorphes.

3) En déduire que p est un élément irréductible de $\mathbb{G}$ si et seulement si -1 n'est pas un carré modulo p.

4) Conclure que si p est un nombre premier impair alors p est somme de deux carrés entiers si et seulement si $p \equiv 1[4]$.

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

Problème n° I

À rendre le 3 octobre 2018

Définition n° I.0 (Partition) On rappelle la définition I.5.3, du cours : Soit E un ensemble. On rappelle qu'une *partition* de E est une partie B de l'ensemble $\mathcal{P}(E)$ des parties de E (ou encore un élément de $\mathcal{P}\big(\mathcal{P}(E)\big)$) vérifiant :

Part$_1$) $\emptyset \notin B$;

Part$_2$)
$$\forall X \in B,\ \forall Y \in B,\ \big(X \cap Y \neq \emptyset \Rightarrow X = Y\big)\ ;$$

Part$_3$)
$$\bigcup_{X \in B} X = E\ .$$

Exercice A : Donner la preuve de la proposition I.5.4.

Exercice B : (**Nombre de Bell**)

Étant donné un ensemble E, on rappelle qu'on note $\mathcal{P}(E)$ l'ensemble des parties (ou sous-ensembles) de E :
$$\mathcal{P}(E) = \{A | A \subset E\} = \{A | \forall x\ ,\ x \in A \Rightarrow x \in E\}\ .$$

1) (**Ensemble des parties**)

Montrer que si E est un ensemble fini, $\mathcal{P}(E)$ est aussi un ensemble fini et déterminer $\#\big(\mathcal{P}(E)\big)$ en fonction de $\#(E)$.

Indication : *On poura étudier $\mathcal{P}(E \cup \{x\})$ en fonction de $\mathcal{P}(E)$.*

Dans la suite, E est un ensemble fini et l'on note $\mathcal{B}(E)$ l'ensemble des partitions de E.

Soit E un ensemble. On rappelle qu'une *partition* de E est une partie B de l'ensemble $\mathcal{P}(E)$ des parties de E (ou encore un élément de $\mathcal{P}\big(\mathcal{P}(E)\big)$) vérifiant :

Part$_1$) $\emptyset \notin B$;

Part$_2$)
$$\forall X \in B,\ \forall Y \in B,\ \big(X \cap Y \neq \emptyset \Rightarrow X = Y\big)\ ;$$

Part$_3$)
$$\bigcup_{X \in B} X = E\ .$$

2) (**Ensembles des partitions**)

Montrer que $\mathcal{B}(E)$ est un ensemble fini et donner un majorant de $\#\big(\mathcal{B}(E)\big)$.

3) On suppose dans cette question que $E \neq \emptyset$.

a) Montrer que pour tout $P \in \mathcal{B}(E)$ et tout $x \in E$, il existe un unique $p \in P$ tel que $x \in p$. On le notera $p_{P,x}$.

Pour tout $k \in \mathbb{N}$ **et tout** $x \in E$, **on note**

$$\mathcal{B}^{\flat}_{k,x}(E) := \{P \in \mathcal{B}(E)\,;\, \#\big(p_{P,x}\big) = k\}\,.$$

b) Montrer que

$$\forall x \in E,\ \mathcal{B}(E) = \bigcup_{k=1}^{\#(E)} \mathcal{B}^{\flat}_{k,x}(E)\,.$$

c) Montrer que

$$\forall (k,\ell) \in [1;\#(E)] \times [1;\#(E)],\ \forall x \in E,\ \mathcal{B}^{\flat}_{k,x}(E) \cap \mathcal{B}^{\flat}_{\ell,x}(E) \neq \emptyset \ \Rightarrow\ \mathcal{B}^{\flat}_{k,x}(E) = \mathcal{B}^{\flat}_{\ell,x}(E)\,.$$

d) En déduire une expression de $\#\big(\mathcal{B}(E)\big)$ en fonction des $\#\big(\mathcal{B}^{\flat}_{k,x}(E)\big)\,,1 \leq k \leq \#(E)}$.

4) Pour tout $x \in E, p \in \mathcal{P}(E)$, **on note**

$$\mathcal{B}^{\sharp}_{p,x}(E) := \{P \in \mathcal{B}(E)\,;\, p_{P,x} = p\}\,.$$

On suppose encore $E \neq \emptyset$.

a) Montrer que

$$\forall x \in E,\ \forall 1 \leq k \leq \#(E),\ \#(\mathcal{B}^{\flat}_{k,x}(E)) = \sum_{p \in \mathcal{P}(E),\ x \in p,\ \#(p) = k} \#\big(\mathcal{B}^{\sharp}_{p,x}(E)\big)\,.$$

b) Pour tout $x \in E$, tout $p \in \mathcal{P}(E)$, tels que $x \in p$, que peut-on dire de l'application

$$u : \mathcal{B}(E \setminus p) \to \mathcal{B}^{\sharp}_{p,x}(E)\,,\ P \mapsto P \cup \{p\}\ ?$$

Que peut-on en déduire pour $\#\big(\mathcal{B}(E \setminus p)\big)$ et $\#\big(\mathcal{B}^{\sharp}_{p,x}(E)\big)$?

5) (Le cas de l'ensemble vide)

a) Déterminer $\mathcal{P}\big(\mathcal{P}(\emptyset)\big)$.

b) Lesquels parmi les éléments de $\mathcal{P}\big(\mathcal{P}(\emptyset)\big)$ sont des partitions *i.e.* des éléments de $\mathcal{B}(\emptyset)$?

c) En déduire que le nombre b_0 de partitions d'un ensemble à 0 élément, est égal à 1.

6) (Une formule de récurrence)

Montrer finalement que $\forall n \in \mathbb{N}$, il existe un entier π_n tel que pour tout ensemble E tel que $\#(E) = n$, $\#\big(\mathcal{B}(E)\big) = \pi_n$ et établir une relation entre π_n et $\pi_k\,,0 \leq k \leq n-1}$.

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

Corrigé du Problème n° I

Exercice A : Donner la preuve de la proposition I.5.4.

Solution :

*i) (**Preuve de I.5.4.i**)*

Soit E un ensemble muni d'une relation d'équivalence $\sim$ et

$$P := \{\overline{x}\,,\ x \in E\}$$

l'ensemble des classes d'équivalence selon $\sim$. Autrement dit, pour tout $x \in E$, $\overline{x} \in P$ est définie par

$$\overline{x} := \{y \in E\,;\ y \sim x\}\,.$$

— *Pour tout $\overline{x} \in P$, $x \in \overline{x}$, en effet $x \sim x$ puisque $\sim$ est réflexive ; si bien que $\overline{x} \neq \emptyset$; ce qui assure que l'axiome I.5.3.Part$_1$) est satisfait par P.*

— *Pour tout $(\overline{x}, \overline{y}) \in P \times P$, il découle du lemme I.5.2 que,*

$$\overline{x} \cap \overline{y} \neq \emptyset \Rightarrow \overline{x} = \overline{y}\,;$$

c'est-à-dire que l'axiome I.5.3.Part$_2$) est satisfait pour P.

— *Enfin pour tout $x \in E$, $x \in \overline{x}$ (comme nous l'avons déjà dit, par réflexivité de $\sim$,) si bien que*

$$E \subset \bigcup_{\overline{x} \in P} \overline{x}\,.$$

Come par ailleurs $\forall x \in E$, $\overline{x} \subset E$,

$$\bigcup_{\overline{x} \in P} \overline{x} \subset E,$$

d'où finalement

$$E = \bigcup_{\overline{x} \in P} \overline{x}$$

ce qui assure que l'axiome I.5.3.Part$_3$) est satisfait par P.

L'ensemble P satisfaisant les axiomes de la définition I.5.3 c'est donc bien une partition de E.

*ii) (**Preuve de I.5.4.ii**)*

Soit E un ensemble et P une partition de E. S'il existe une relation d'équivalence $\sim$ telle que les classes selon $\sim$ sont les éléments de P, alors pour tout $x \in E$, d'après I.5.3.Part$_3$), il existe $A \in P$ tel que $x \in A$. De plus d'après I.5.3.Part$_2$), s'il existe $B \in P$ tel que $x \in B$, alors $A \cap B \neq \emptyset$ et par conséquent $A = B$.

Pour tout $x \in E$, il existe donc un unique $A \in P$ tel que $x \in A$. Si A est la classe de x, pour tout $y \in E$,

$$y \sim x \Leftrightarrow y \in A\,.$$

La relation $\sim$ est alors caractérisée par le fait que $x \sim y$ si et seulement si il existe $A \in P$ tel que $x \in A$ et $y \in A$. L'unicité de $\sim$ est alors assurée.

Reste à montrer que $\sim$ ainsi définie est bien une relation d'équivalence : Or

— *d'après I.5.3.Part$_3$), pour tout $x \in E$, il existe $A \in P$ tel que $x \in A$, ce qui entraîne que $x \sim x$, c'est-à-dire que $\sim$ est réflexive ;*

— *la définition même de $\sim$ assure qu'elle est symétrique ;*

— *enfin pour tout $(x, y, z) \in E \times E \times E$, $x \sim y$ et $y \sim z$, entraîne qu'il existe $(A, b) \in P \times P$, tel que*

$$x \in A\,,\ y \in A\,,\ y \in B\,,\ z \in B\,.$$

Il en résulte que $y \in A \cap B$ si bien que, d'après I.5.3.Part$_2$), $A = B$, si bien que $z \in A$, c'est-à-dire que $x \sim Z$. Il en résulte que $\sim$ est transitive.

Exercice B : (Nombre de Bell)

Étant donné un ensemble E, on rappelle qu'on note $\mathcal{P}(E)$ l'ensemble des parties (ou sous-ensembles) de E :

$$\mathcal{P}(E) \;=\; \{A | A \subset E\} \;=\; \{A | \forall x \;,\; x \in A \Rightarrow x \in E\} \;.$$

1) (Ensemble des parties)

Montrer que si E est un ensemble fini, $\mathcal{P}(E)$ est aussi un ensemble fini et déterminer $\#\big(\mathcal{P}(E)\big)$ en fonction de $\#(E)$.

Indication : *On poura étudier $\mathcal{P}(E \cup \{x\})$ en fonction de $\mathcal{P}(E)$.*

Solution :

i) Soit E un ensemble et $x \notin E$. Construisons une application

$$f \;:\; \mathcal{P}(E \cup \{x\}) \;\to\; \{\emptyset, \{x\}\} \times \mathcal{P}(E) \;,\; A \;\mapsto\; (A \cap \{x\}, A \cap E) \;.$$

Il est alors clair que f est une bijection puisqu'une partie de $E \cup \{x\}$ contient x ou ne le contient pas.

ii) Démontrons par récurrence l'assertion $\mathcal{H}_n$: Pour tout ensemble E avec $\#(E) \;=\; n$, $\mathcal{P}(E)$ est fini et

$$\#\big(\mathcal{P}(E)\big) \;=\; 2^n \;=\; 2^{\#(E)} \;.$$

*a) (**Initialisation**)*

Si E est un ensemble tel que $\#(E) \;=\; 0$, $E \;=\; \emptyset$. Alors $\mathcal{P}(E) \;=\; \{\emptyset\}$ et

$$\#\big(\mathcal{P}(E)\big) \;=\; \#\big(\{\emptyset\}\big) \;=\; 1 \;=\; 2^0 \;=\; 2^{\#(E)}$$

si bien que $\mathcal{H}_0$ est établie.

*b) (**Héridité**)*

Soit $n \;\in\; \mathbb{N}$ et F un ensemble tel que $\#(F) \;=\; n+1$. Alors $F \;\neq \emptyset$ et l'on choisit $x \in F$. On peut alors écrire $F \;=\; E \cup \{x\}$ avec $E \;:=\; F \setminus \{x\}$. On a alors $\#(E) \;=\; n$ et l'on peut construire la bijection $f \;:\; \mathcal{P}(F) \;\to\; \{\emptyset, \{x\}\} \times \mathcal{P}(E)$ comme en i).

Si l'on suppose $\mathcal{H}_n$, $\mathcal{P}(E)$ est un ensemble fini ce qui entraîne que $\{\emptyset, \{x\}\} \times \mathcal{P}(E)$ est encore fini et

$$\#\big(\mathcal{P}(F)\big) \;=\; \#\big(\{\emptyset, \{x\}\} \times \mathcal{P}(E)\big) \;=\; 2 * \#\big(\mathcal{P}(E)\big) \;=\; 2 * 2^n \;=\; 2^{n+1} \;=\; 2^{\#\left(\mathcal{P}(F)\right)} \;.$$

Dans la suite, E est un ensemble fini et l'on note $\mathcal{B}(E)$ l'ensemble des partitions de E.

Soit E un ensemble. On rappelle qu'une *partition* de E est une partie B de l'ensemble $\mathcal{P}(E)$ des parties de E (ou encore un élément de $\mathcal{P}\big(\mathcal{P}(E)\big)$) vérifiant :

Part$_1$) $\emptyset \notin B$;

Part$_2$)

$$\forall X \in B,\; \forall Y \in B,\; \big(X \;\cap\; Y \;\neq\; \emptyset \;\Rightarrow X \;=\; Y\big) \;;$$

Part$_3$)

$$\bigcup_{X \;\in\; B} X \;=\; E \;.$$

2) (**Ensembles des partitions**)
Montrer que $\mathcal{B}(E)$ est un ensemble fini et donner un majorant de $\#\big(\mathcal{B}(E)\big)$.

Solution : *Il découle de la définition de partition que* $\mathcal{B}(E) \subset \mathcal{P}\big(\mathcal{P}(E)\big)$. *Or on a vu à la question 1) que si* E *est fini,* $\mathcal{P}(E)$ *est aussi fini ce qui entraîne encore que* $\mathcal{P}\big(\mathcal{P}(E)\big)$ *est fini. De plus, toujours en vertu de la question 1),*

$$\#\big(\mathcal{P}\big(\mathcal{P}(E)\big)\big) \;=\; 2^{\#\left(\mathcal{P}(E)\right)} \;=\; 2^{2^{\#(E)}} \,.$$

Si bien qu'on obtient du même coup une majoration explicite

$$\#\big(\mathcal{B}(E)\big) \;\leq\; 2^{2^{\#(E)}} \,.$$

3) On suppose dans cette question que $E \neq \emptyset$.

a) Montrer que pour tout $P \in \mathcal{B}(E)$ et tout $x \in E$, il existe un unique $p \in P$ tel que $x \in p$. On le notera $p_{P,x}$.

Solution :

i) L'existence de p *est assurée par l'axiome* Part_3*).*

ii) L'unicité est assurée par l'axiome Part_2*).*

Pour tout $k \in \mathbb{N}$ **et tout** $x \in E$, **on note**

$$\mathcal{B}^{\flat}_{k,x}(E) \;:=\; \{P \in \mathcal{B}(E)\,;\, \#\big(p_{P,x}\big) \;=\; k\} \,.$$

b) Montrer que

$$\forall x \in E,\; \mathcal{B}(E) \;=\; \bigcup_{k=1}^{\#(E)} \mathcal{B}^{\flat}_{k,x}(E) \,.$$

Solution : *Pour tout* $P \in \mathcal{B}(E)$, $p_{P,x} \neq \emptyset$ *((cf.* Part_1*),) donc* $\#\big(p_{P,x}\big) \geq 1$. *D'autrepart*

$$p_{P,x} \subset E \;\Rightarrow\; \#\big(p_{P,x}\big) \leq \#(E) \,.$$

Enfin par définition $P \in \mathcal{B}^{\flat}_{\#\left(p_{P,x}\right),x}(E)$.

c) Montrer que

$$\forall (k,\ell) \in [1;\#(E)] \times [1;\#(E)],\; \forall x \in E,\; \mathcal{B}^{\flat}_{k,x}(E) \cap \mathcal{B}^{\flat}_{\ell,x}(E) \neq \emptyset \;\Rightarrow\; \mathcal{B}^{\flat}_{k,x}(E) \;=\; \mathcal{B}^{\flat}_{\ell,x}(E) \,.$$

Solution : *Si* $P \in \mathcal{B}^{\flat}_{k,x}(E) \cap \mathcal{B}^{\flat}_{\ell,x}(E)$, *par définition*

$$k \;=\; \#\big(p_{P,x}\big) \;=\; \ell \;\Rightarrow\; \mathcal{B}^{\flat}_{k,x}(E) \;=\; \mathcal{B}^{\flat}_{\ell,x}(E) \,.$$

d) En déduire une expression de $\#\big(\mathcal{B}(E)\big)$ en fonction des $\#\big(\mathcal{B}^{\flat}_{k,x}(E)\big)\,,_{1\,\leq\,k\,\leq\,\#(E)}$.

Solution : *Il découle immédiatement de a) et c) que :*

$$\#\big(\mathcal{B}(E)\big) \;=\; \sum_{k=1}^{\#(E)} \#\big(\mathcal{B}^{\flat}_{k,x}(E)\big) \,. \qquad \textit{1}$$

4) Pour tout $x \in E, p \in \mathcal{P}(E)$, **on note**

$$\mathcal{B}^{\sharp}_{p,x}(E) := \{P \in \mathcal{B}(E) \,;\, p_{P,x} = p\} .$$

On suppose encore $E \neq \emptyset$.

a) Montrer que

$$\forall x \in E,\ \forall 1 \leq k \leq \#(E),\ \#(\mathcal{B}^{\flat}_{k,x}(E)) = \sum_{p \in \mathcal{P}(E),\ x \in p,\ \#(p) = k} \#\big(\mathcal{B}^{\sharp}_{p,x}(E)\big) .$$

Solution : *Pour tout* $x \in E$, *tout* $1 \leq k \leq \#(E)$ *et tout* $P \in \mathcal{B}^{\flat}_{k,x}(E)$ *par définition*

$$\#(p_{P,x}) = k \text{ et } P \in \mathcal{B}^{\sharp}_{p_{P,x},x}(E)$$

ce qui prouve que :

$$\forall x \in E,\ \forall 1 \leq k \leq \#(E),\ \mathcal{B}^{\flat}_{k,x}(E) = \bigcup_{p \in \mathcal{P}(E),\ x \in p\, \#(p) = k} \mathcal{B}^{\sharp}_{p,x}(E) . \qquad 1$$

D'autrepart pour tout $x \in E$, *tout* $p \in \mathcal{P}(E)$, *tout* $q \in \mathcal{P}(E)$,

$$P \in \mathcal{B}^{\sharp}_{p,x}(E) \cap \mathcal{B}^{\sharp}_{q,x}(E) \Rightarrow p = p_{P,x} = q \Rightarrow \mathcal{B}^{\sharp}_{p,x}(E) = \mathcal{B}^{\sharp}_{q,x}(E) .$$

On a donc montré que :

$$\forall x \in E,\ \forall (p,q) \in \mathcal{P}(E) \times \mathcal{P}(E),\ \mathcal{B}^{\sharp}_{p,x}(E) \cap \mathcal{B}^{\sharp}_{q,x}(E) \neq \emptyset \Rightarrow \mathcal{B}^{\sharp}_{p,x}(E) = \mathcal{B}^{\sharp}_{q,x}(E) . \qquad 2$$

Dès lors 1 et 2 entraînent le résultat demandé.

b) Pour tout $x \in E$, tout $p \in \mathcal{P}(E)$, tels que $x \in p$, que peut-on dire de l'application

$$u : \mathcal{B}(E \setminus p) \to \mathcal{B}^{\sharp}_{p,x}(E) ,\ P \mapsto P \cup \{p\} \ ?$$

Que peut-on en déduire pour $\#\big(\mathcal{B}(E \setminus p)\big)$ et $\#\big(\mathcal{B}^{\sharp}_{p,x}(E)\big)$?

Solution : *L'application* u *est clairement bijective si bien qu'on en déduit :*

$$\forall x \in E,\ \forall p \in \mathcal{P}(E),\ x \in p \Rightarrow \#\big(\mathcal{B}(E \setminus p)\big) = \#\big(\mathcal{B}^{\sharp}_{p,x}(E)\big) . \qquad 1$$

5) (Le cas de l'ensemble vide)

a) Déterminer $\mathcal{P}\big(\mathcal{P}(\emptyset)\big)$.

Solution : *On a* $\mathcal{P}(\emptyset) = \{\emptyset\}$ *d'où*

$$\mathcal{P}\big(\mathcal{P}(\emptyset)\big) = \big\{\emptyset, \{\emptyset\}\big\} .$$

b) Lesquels parmi les éléments de $\mathcal{P}\big(\mathcal{P}(\emptyset)\big)$ sont des partitions *i.e.* des éléments de $\mathcal{B}(\emptyset)$?

Solution : *Il est clair que* $\{\emptyset\}$ *ne peut-être une partition puisque* $\emptyset \in \{\emptyset\}$ *ce qui contredirait l'axiome* Part$_1$*).*

Il est peut-être moins évident de se convaincre que $\emptyset$ *est une partition mais en y regardant de plus près :*

*i) (***Part**$_1$*))*

Puisque $\emptyset$ *n'a aucun élément on n'a pas en particulier* $\emptyset \in \emptyset$ *ce qui assure que* Part$_1$*) est satisfait.*

*ii) (**Part**$_2$))*

Dans l'implication la prémice est toujours fausse ce qui assure que l'implication elle-même est toujours vraie.

*iii) (**Part**$_3$))*

Il faut vérifier que

$$\bigcup_{p\in\emptyset} p \;=\; \emptyset\,.$$

c) En déduire que le nombre b_0 de partitions d'un ensemble à 0 élément, est égal à 1.

Solution : *Un ensemble à 0 élément étant forcément égal au vide, on déduit de ce qui précède que :*

$$b_0 \;=\; 1\,. \qquad \textit{1}$$

6) (Une formule de récurrence)

Montrer finalement que $\forall n \in \mathbb{N},$ il existe un entier π_n tel que pour tout ensemble E tel que $\#(E) \;=\; n$, $\#\big(\mathcal{B}(E)\big) \;=\; \pi_n$ et établir une relation entre π_n et $\pi_{k\ ,0\leq k\leq n-1}$.

Solution :

i) ($n \;=\; 0$)

On a déjà établi le résultat pour $n \;=\; 0$ à la question 5) et en particulier à la question 5), c).1 que $b_0 \;=\; 1$.

ii) ($n \;>\; 0$)

Remarquons d'abord que pour tout ensemble fini E, $\mathcal{B}(E)$ est un ensemble fini puisque $\mathcal{B}(E) \;\subset\; \mathcal{P}\big(\mathcal{P}(\,)\big)E$ qui lui-même est fini. $\#\big(\mathcal{B}(E)\big)$ est donc bien un élément de $\mathbb{N}$. Cependant, celui-ci pourrait dépendre de E lui-même et non uniquement de $\#(E)$. Faisons donc l'hypothèse

$$\mathcal{H}_n \;:\; \forall 0 \leq k \leq n,\; \exists b_k\; \forall F\; \#(F) \;=\; k \;\Rightarrow\; \#\big(\mathcal{B}(F)\big) \;=\; b_k\,.$$

Démontrons alors $\mathcal{H}_n$ par récurrence :

*a) (**Initialisation**)*

Elle a été faite en i) qui découle de la question 5).

*b) (**Heridite**)*

Soit $n \;\in\; \mathbb{N}$, et E un ensemble à $n+1$ éléments. En particulier E est non vide si bien que les résultats de la question 3) et de la question 4) s'appliquent ici. Choisissons un élément $x \in E$. On a alors, d'après la question 3), d).1 :

$$\#\big(\mathcal{B}(E)\big) \;=\; \sum_{k=1}^{\#(E)} \#\big(\mathcal{B}^{\flat}_{k,x}(E)\big)\,. \qquad \textit{1}$$

En utilisant la question 4), a) l'égalité précédente devient :

$$\#\big(\mathcal{B}(E)\big) \;=\; \sum_{k=1}^{\#(E)} \sum_{p\in\mathcal{P}(E),\ x\in p,\ \#(p)\,=\,k} \#\big(\mathcal{B}^{\sharp}_{p,x}(E)\big)\,. \qquad \textit{2}$$

En utilisant maintenant la question 4), b).1, l'égalité précédente s'écrit :

$$\#\big(\mathcal{B}(E)\big) \;=\; \sum_{k=1}^{\#(E)} \sum_{p\in\mathcal{P}(E),\ x\in p,\ \#(p)\,=\,k} \#\big(\mathcal{B}(E\setminus p)\big)\,. \qquad \textit{3}$$

On remarque alors que

$$\forall p \in \mathcal{P}(E),\ 1 \ \leq\ \#(p) \ \leq\ \#(E) \ \Rightarrow\ 0 \ \leq\ \#\big(E \setminus p\big) \ \leq\ \#(E) - 1 \ =\ n\,.$$

En appliquant l'hypothèse de récurrrence $\mathcal{H}_n$, l'égalité 3 s'écrit :

$$\begin{aligned} \#\big(\mathcal{B}(E)\big) \ &=\ \sum_{k=1}^{\#(E)} \ \sum_{p\in\mathcal{P}(E),\ x\in p,\ \#(p)\,=\,k} b_{n+1-k} \\ &=\ \sum_{k=1}^{\#(E)} b_{n+1-k} \cdot \sum_{p\in\mathcal{P}(E),\ x\in p,\ \#(p)\,=\,k} 1\,. \end{aligned} \qquad 4$$

Reste donc à déterminer $\displaystyle\sum_{p\in\mathcal{P}(E),\ x\in p,\ \#(p)\,=\,k} 1$ *. Or l'application*

$$v\ :\ \{p\ \in\ \mathcal{P}(E\setminus\{x\})\,;\ \#(p)\ =\ k-1\}\ \to\ \{p\ \in\ \mathcal{P}(E)\,;\ \#(p)\ =\ k\,,\ x\in p\}\,,\ p\ \mapsto\ p\cup\{x\}$$

est une bijection d'où il découle que

$$\#\big(\{p\ \in\ \mathcal{P}(E)\,;\ \#(p)\ =\ k\,,\ x\in p\}\big)\ =\ \#\big(\{p\ \in\ \mathcal{P}(E\setminus\{x\})\,;\ \#(p)\ =\ k-1\}\big)\ =\ C^{k-1}_{\#(E\setminus\{x\})}\ =\ \binom{n}{k-1}.$$

Il en découle que $\displaystyle\sum_{p\in\mathcal{P}(E),\ x\in p,\ \#(p)\,=\,k} 1\ =\ \binom{n}{k-1}$.

Et finalement 4 entraîne :

$$\#\big(\mathcal{B}(E)\big)\ =\ \sum_{k=1}^{\#(E)} b_{n+1-k}\binom{n}{k-1}\,. \qquad 5$$

Cette égalité ayant été établie pour tout ensemble E tel que $\#(E)\ =\ n+1$, elle ne dépend que de l'entier $n+1$ ce qui assure que $\mathcal{H}_n\ \Rightarrow\ \mathcal{H}_{n+1}$ et achève donc la preuve par récurrence.

La formule 5 peut finalement s'écrire :

$$b_{n+1}\ =\ \sum_{k=1}^{n+1} b_{n+1-k}\binom{n}{k-1}\,. \qquad 6$$

Université Paris Sud **Année 2018–2019**

L3/S5 M313 **Algèbre Générale**

Problème n° III

À rendre le 22 octobre 2018

Exercice A : Soit $(G, *, e)$ un groupe. Pour tout $x \in G$ on définit une application ϵ_x par

$$\epsilon_x(0) := e\ ,\ \forall n \in \mathbb{N},\ \epsilon_x(n+1) := x * \epsilon_x(n)\ .$$

1) Rappeler pourquoi ϵ_x définit bien une application de $\mathbb{N}$ dans G.

2) Si y désigne le symétrique de x dans G, on pose

$$\forall n \in \mathbb{N},\ \epsilon_x(-n) := \epsilon_y(n)\ .$$

Montrer qu'alors ϵ_x définit bien une application de $\mathbb{Z}$ dans G.

3) Montrer que ϵ_x est un morphisme de groupes. En déduire une justification des notation

$$x^n := \epsilon_x(n) \text{ et } x^{-1} := y$$

couramment utilisées.

4) Pour $x \in G$, le morphisme ϵ_x est défini comme ci-dessus.

a) Quelle propriété de x équivaut au fait que ϵ_x est surjectif ?

b) Si ϵ_x n'est pas injectif, montrer qu'il existe $d \in \mathbb{N}$, tel que $\mathrm{Ker}\ \epsilon_x = d\mathbb{Z}$ et caractériser autrement l'entier d.

5) On suppose, dans cette question que G est abélien et l'on note $+$ sa loi de composition. On définit une loi externe

$$\cdot\ :\ \mathbb{Z} \times G \to G\ ,\ (n, x) \mapsto n \cdot x := \epsilon_x(n)\ .$$

a) Pour tout $(p, q) \in \mathbb{Z} \times \mathbb{Z}$ et tout $(x, y) \in G \times G$, montrer que :

i)
$$p \cdot (x + y) = p \cdot x + p \cdot y\ ;$$

ii)
$$(p + q) \cdot x = p \cdot x + q \cdot x\ ;$$

iii)
$$1 \cdot x = x\ .$$

iv)
$$(p * q) \cdot x = p \cdot (q \cdot x)\ ;$$

b) Les propriétés a).i) à a).iv) vous rappellent-elles quelque chose ? Est-on pour autant exactement dans une situation connue ?

Exercice B : (Stabilisateur)

Soit $(G, *)$ un groupe et E un ensemble muni d'une action de G notée $g \cdot x$ pour tout $(g, x) \in G \times E$.

Montrer que pour tout $(x, g) \in E \times G$,

$$\mathrm{Stab}_G(g \cdot x) = g * \mathrm{Stab}_G(x) * g^{-1}\ .$$

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

Corrigé du Problème n° III

Exercice A : Soit $(G, *, e)$ un groupe. Pour tout $x \in G$ on définit une application ϵ_x par

$$\epsilon_x(0) := e\ ,\ \forall n \in \mathbb{N},\ \epsilon_x(n+1) := x * \epsilon_x(n)\ .$$

1) Rappeler pourquoi ϵ_x définit bien une application de $\mathbb{N}$ dans G.

Solution : *Si D_x est le domaine de définition de ϵ_x, par définition même de ϵ_x, $0 \in D_x$. La propriété $\epsilon_x(n+1) = x * \epsilon_x(n)$, assure alors que*

$$\forall n \in \mathbb{N},\ n \in D_x \Rightarrow n+1 \in D_x\ ,$$

c'est-à-dire que D_x, satisfait au principe de récurrence (cf. cours II.0.PA$_3$),) si bien que $D_x = \mathbb{N}$ i.e. ϵ_x est définie sur $\mathbb{N}$.

2) Si y désigne le symétrique de x dans G, on pose

$$\forall n \in \mathbb{N},\ \epsilon_x(-n) := \epsilon_y(n)\ .$$

Montrer qu'alors ϵ_x définit bien une application de $\mathbb{Z}$ dans G.

Solution : *Il suffit de constater que ϵ_x est définie sur $\mathbb{N}$ grâce à la question 1), que ϵ_x est aussi définie sur $-\mathbb{N}$ graçe à ce qui précède. Puisque $\mathbb{N} \cap -\mathbb{N} = \{0\}$, et que les deux définitions de ϵ_x coïncident en 0, ($\epsilon_x(0) = e$,) on définit donc bien une application $\epsilon_x : \mathbb{Z} \to G$.*

3) Montrer que ϵ_x est un morphisme de groupes. En déduire une justification des notation

$$x^n := \epsilon_x(n) \text{ et } x^{-1} := y$$

couramment utilisées.

Solution :

i) Démontrons d'abord, par récurrence, que :

$$\forall x \in G,\ \forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \epsilon_x(p+q) = \epsilon_x(p) * \epsilon_x(q)\ . \qquad 1$$

Soit

$$E := \{p \in \mathbb{N}\ ;\ \forall q \in \mathbb{N},\ \epsilon_x(p+q) = \epsilon_x(p) * \epsilon_x(q)\}\ .$$

On a, par définition de ϵ_x,

$$\forall q \in \mathbb{N},\ \epsilon_x(0+q) = \epsilon_x(q) = e * \epsilon_x(q) = \epsilon_x(0) * \epsilon_x(q)$$

c'est-à-dire que $0 \in E$.

Pour tout $p \in E$,

$$\forall q \in \mathbb{N},\ \epsilon_x(p+1+q) = \epsilon_x(p+q+1) = x * \epsilon_x(p+q) = x * \epsilon_x(p) * \epsilon_x(q) = \epsilon_x(p+1) * \epsilon_x(q)$$

c'est-à-dire que $p+1 \in E$.

Il s'ensuit que E satisfait au principe de récurrrence (cf. cours II.0.PA$_3$),) et donc que $E = \mathbb{N}$ ce qui prouve le résultat.

On en déduit immédiatement :

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \epsilon_x(p) * \epsilon_x(q) = \epsilon_x(p+Q) = \epsilon_x(q+p) = \epsilon_x(q) * \epsilon_x(p)\ . \qquad 2$$

On en déduit également, en notant y le symétrique de $x \in G$, que :

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \epsilon_x(-p-q) = \epsilon_x(-(p+q)) = \epsilon_y(p+q) = \epsilon_y(q)p * \epsilon_y(q) = \epsilon_x(-p) * \epsilon_x(-q)\ . \quad 3$$

ii) Montrons Maintenant, par récurrence, que :

$$\forall x \in G,\ \forall p \in \mathbb{N},\ \epsilon_x(p-p) \ =\ \epsilon_x(p) * \epsilon_x(-p)\ . \qquad 1$$

Notons

$$E \ :=\ \{p \ \in\ \mathbb{N}\,;\ \epsilon_x(p-p) \ =\ \epsilon_x(p) * \epsilon_x(-p)\}\ .$$

On a $0 \ \in\ E$ *de manière évidente.*
Par ailleurs, pour tout $p \ \in\ E$,

$$\begin{aligned}
\epsilon_x(p+1) * \epsilon_x(-(p+1)) &= \epsilon_x(p+1) * \epsilon_y(p+1) \\
&= \epsilon_x(p) * \epsilon_x(1) * y * \epsilon_y(p) \\
&= \epsilon_x(p) * x * y * \epsilon_y(p) \\
&= \epsilon_x(p) * \epsilon_y(p) \\
&= \epsilon_x(p) * \epsilon_x(-p) \\
&= \epsilon_x(p-p) \\
&= \epsilon_x(0) \\
&= e \\
&= \epsilon_x((p+1)-(p+1))\ ,
\end{aligned}$$

ce qui prouve que $p+1 \ \in\ E$, *et donc que* E *satisfait au principe de récurrence et donc finalement que* $E \ =\ \mathbb{N}$ *et établit le résultat.*

iii) Établissons enfin que :

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \epsilon_x(p-q) \ =\ \epsilon_x(p) * \epsilon_x(-q)\ . \qquad 1$$

Raisonnons sur la différence $r \ :=\ p-q$. *Si* $r \ \leq\ 0$,

$$\epsilon_x(p-q) \ =\ \epsilon_x(r) \ =\ \epsilon_y(-r)$$

et il suffit donc d'établir le résultat pour $r \ \geq\ 0$.
Notons donc

$$E \ :=\ \{r \ \in\ \mathbb{N}\,;\ \forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ p-q \ =\ r \ \Rightarrow\ \epsilon_x(p-q) \ =\ \epsilon_x(p) * \epsilon_x(-q)\}\ .$$

L'assertion ii).1 assure que $0 \ \in\ E$.
Pour

$$r \ \in\ E\ ,\ p \ \in\ \mathbb{N}\ ,\ q \ \in\ \mathbb{N}\ ,\ p-q \ =\ r+1$$

on a $p-q-1 \ \in\ \mathbb{N}$, *et* $p-q-1 \ =\ r$ *d'où, par hypothèse de récurrence*

$$\epsilon_x(p-q-1) \ =\ \epsilon_x(p) * \epsilon_x(-(q+1)) \ =\ \epsilon_x(p) * \epsilon_y(q+1)\ .$$

Or $p-q-1 \ \in\ \mathbb{N}$ *et* $1 \ \in\ \mathbb{N}$, *si bien que d'après i).1,*

$$\begin{aligned}
\epsilon_x(p-q) &= \epsilon_x(p-(+1)+1) \\
&= \epsilon_x(p-(q+1)) * \epsilon_x(1) \\
&= \epsilon_x(p) * \epsilon_y(q+1) * x \\
&= \epsilon_x(p) * \epsilon_y(q) * y * x \\
&= \epsilon_x(p) * \epsilon_y(q) \\
&= \epsilon_x(p) * \epsilon_x(-q)\ ,
\end{aligned}$$

ce qui prouve que $r+1 \ \in\ E$, *et donc par récurrence que* $E \ =\ \mathbb{N}$, *ce qui établit le résultat.*

iv) On en déduit finalement que pour tout $(p,q) \in \mathbb{Z}\times\mathbb{Z}$, d'après i).1, si p et q sont positifs, d'après iii).1, si p et q sont négatifs, d'après iii).1, si p et q sont de signe contraire, que :

$$\epsilon_x(p+q) \;=\; \epsilon_x(p) * \epsilon_x(q)$$

c'est-à-dire que ϵ_x est un morphisme de groupes.

4) Pour $x \in G$, le morphisme ϵ_x est défini comme ci-dessus.

a) Quelle propriété de x équivaut au fait que ϵ_x est surjectif ?

Solution : *Le morphisme ϵ_x est surjectif si et seulement si pour tout $g \in G$, il existe $n \in \mathbb{Z}$, tel que $g = \epsilon_x(n)$. Ceci revient exactement à dire que G est engendré par x.*

b) Si ϵ_x n'est pas injectif, montrer qu'il existe $d \in \mathbb{N}$, tel que $\mathrm{Ker}\,\epsilon_x = d\mathbb{Z}$ et caractériser autrement l'entier d.

Solution : *Si ϵ_x n'est pas injectif, $\mathrm{Ker}\,\epsilon_x \neq \{0\}$, et c'est un sous-groupe de $\mathbb{Z}$. Alors (cf. cours IV.5.5,) il existe $d \in \mathbb{N}^*$ tel que $\mathrm{Ker}\,\epsilon_x = d\mathbb{Z}$.*

Il s'ensuit alors que, pour tout $n \in \mathbb{Z}$,

$$\epsilon_x(n) \;=\; e \;\Leftrightarrow\; d|n\;.$$

L'entier d est alors le plus petit (aussibien au sens de la divisibilité que de la relation d'ordre sur $\mathbb{N}$) entier positif tel que $\epsilon_x(n) = e$, ce qu'on peut encore écrire $x^n = e$. C'est, par définition, l'ordre de x dans G.

5) On suppose, dans cette question que G est abélien et l'on note $+$ sa loi de composition. On définit une loi externe

$$\cdot \;:\; \mathbb{Z}\times G \;\to\; G\;,\; (n,x) \;\mapsto\; n\cdot x \;:=\; \epsilon_x(n)\;.$$

a) Pour tout $(p,q) \in \mathbb{Z}\times\mathbb{Z}$ et tout $(x,y) \in G\times G$, montrer que :

i)

$$p\cdot(x+y) \;=\; p\cdot x \;+\; p\cdot y\;;$$

Solution : *Remarquons d'abord que pour tout $p \in \mathbb{N}$,*

$$(-p)\cdot(x+y) \;=\; \epsilon_{x+y}(-p) \;=\; \epsilon_{-(x+y)}(p)$$

et qu'il suffit donc d'établir le résultat pour $p \in \mathbb{N}$.

On Le fait par récurrence. En effet

$$0\cdot(x+y) \;=\; \epsilon_{x+y}(0) \;=\; 0_G \;=\; \epsilon_x(0)+\epsilon_y(0) \;=\; 0\cdot x + 0\cdot y\;.$$

Si p vérifie la propriété :

$$\begin{aligned}(p+1)\cdot(x+y) &= \epsilon_{x+y}(p+1)\\ &= \epsilon_{x+y}(p)+x+y\\ &= p\cdot(x+y)+x+y\\ &= p\cdot x+x+p\cdot y+y\;.\end{aligned}$$

Remarquons ici qu'on utilise l'hypothèse que G est abélien et que sans celle-ci on ne pourrait établir ce résultat.

Il résulte donc de ce qui précède que

$$(p+1)\cdot(x+y) \;=\; p\cdot x+x+p\cdot y+y \;=\; \epsilon_x(p)+x+\epsilon_y(y)+y \;=\; \epsilon_x(p+1)+\epsilon_y(p+1) \;=\; (p+1)\cdot x+(p+1)\cdot y\;.$$

ii)

$$(p+q)\cdot x \;=\; p\cdot x \;+\; q\cdot x\,;$$

Solution : *Ce r'ésultat n'est autre, aux notation près, que celui établi à la question 3).*

iii)

$$1\cdot x \;=\; x\,.$$

Solution : *Immédiat.*

iv)

$$(p*q)\cdot x \;=\; p\cdot(q\cdot x)\,;$$

Solution : *Considérons*

$$E \;:=\; \{p \;\in\; \mathbb{N}\,;\; \forall q\in\mathbb{N},\; (p*q)\cdot x \;=\; p\cdot(q\cdot x)\}\,.$$

Comme

$$0_G \;=\; (0*q)\cdot x \;=\; 0\cdot(q\cdot x),$$

$0 \;\in\; E$.

Pour $p \;\in\; E$,

$$((p+1)*q)\cdot x \;=\; (p*q)\cdot x + q\cdot x$$

en utilisant ii).

En utilisant iii), il vient

$$((p+1)*q)\cdot x \;=\; (p*q)\cdot x + 1\cdot(q\cdot x)$$

puis en utilisant l'hypothèse de récurrence

$$((P+1)*q)\cdot x \;=\; p\cdot(q\cdot x) \;=\; 1\cdot(q\cdot x)\,.$$

En utilisant finalement encore ii) il vient

$$((p+1)*q)\cdot x \;=\; (p+1)\cdot(q\cdot x)$$

ce qui achève la preuve.

b) Les propriétés a).i) à a).iv) vous rappellent-elles quelque chose ? Est-on pour autant exactement dans une situation connue ?

Solution : *Ces propriétés sont exactement celles qui définissent les espaces vectoriels. Cependant pour qu'on ait réellement affaire à un espace vectoriel, il faut que les « scalaires » soient éléments d'un corps. Ici ils sont éléments de* $\mathbb{Z}$ *qui n'est qu'un anneau. Cette apparente similitude dans l'axiomatique disssimule en fait un saut considérable de complexité.*

Exercice B : (Stabilisateur)

Soit $(G, *)$ un groupe et E un ensemble muni d'une action de G notée $g \cdot x$ pour tout $(g, x) \in G \times E$.

Montrer que pour tout $(x, g) \in E \times G$,

$$\mathrm{Stab}_G(g \cdot x) = g * \mathrm{Stab}_G(x) * g^{-1} .$$

Solution : *(Voir aussi la proposition V.1.18 du cours.)*

Pour tout $(x, g, h) \in E \times G \times G$, $h \in \mathrm{Stab}_G(g \cdot x)$ si et seulement si $h \cdot (g \cdot x) = g \cdot x$ si et seulement si

$$g^{-1} \cdot (h \cdot (g \cdot x)) = x \Leftrightarrow (g^{-1} * h * g) \cdot x = x \Leftrightarrow g^{-1} * hg \in \mathrm{Stab}_G(x)$$

c'est-à-dire qu'il existe $k \in \mathrm{Stab}_G(x)$ tel que $g^{-1} * h * g = k$ i.e.$h = g * k * g^{-1}$ c'est-à-dire finalement que

$$h \in g * \mathrm{Stab}_G(x) * g^{-1} .$$

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

Problème n° V

à rendre le 19 novembre

Exercice A : (Équation caractéristique d'un sous-groupe du groupe spécial orthogonal)

Les notations étant celles du TD n° V, exercice B et du TD n° V, exercice C, on considère un sous-groupe fini G de cardinal n de $\mathcal{SO}_3(\mathbb{R})$, P l'ensemble de ses pôles et

$$\mathcal{F} \,:=\, \{(g,p) \,\in\, (G\setminus \mathrm{Id})\times P\,;\; g(p) \,=\, p\}\,.$$

1) Montrer que

$$\#(\mathcal{F}) \,=\, 2(n-1)\,.$$

Pour tout $p \in P$, on note $\mathrm{Stab}_G(p)$ son stabilisateur dans G.

2) Rappeler pourquoi, pour tout $p \in P$, $\mathrm{Stab}_G(p)$ est un sous-groupe de G.

3) Montrer que

$$\#(\mathcal{F}) \,=\, \sum_{p\in P} \#((\mathrm{Stab}_G(p)-1))\,.$$

Pour tout $p \in P$, on note $O(p)$ son orbite sous l'action de G.

4) Montrer que P est la réunion d'un nombre fini d'orbites $O(p_1),\ldots,O(p_r)$ deux à deux disjointes, chacune d'entre elle étant un ensemble fini.

5) En déduire que

$$\#(\mathcal{F}) \,=\, \sum_{i=1}^{r}\ \sum_{p\in O(p_i)} (\#(\mathrm{Stab}_G(p))-1)\,.$$

6) Rappeler ce qu'on peut dire de $\mathrm{Stab}_G(p)$ et $\mathrm{Stab}_G(q)$ si $O(p) \,=\, O(q)$ (ou encore, ce qui revient au même $p \in O(q)$ ou encore $q \in O(p)$.)

7) En déduire que

$$\#(\mathcal{F}) \,=\, \sum_{i=1}^{r} \#(O(p_i))(\#(\mathrm{Stab}_G(p_i))-1)\,.$$

8) En déduire que

$$\#(\mathcal{F}) \,=\, \sum_{i=1}^{r} n - \#(O(p_i)),$$

puis l'*équation caractéristique du group G* :

$$2-\frac{2}{n} \,=\, \sum_{i=1}^{r} 1-\frac{1}{\#(\mathrm{Stab}_G(p_i))}\,.$$

Exercice B : (**Le groupe** $\mathcal{S}_7$)

1) Soient

$$s_1 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 \end{pmatrix} \text{ et } s_2 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 1 & 4 & 3 & 6 \end{pmatrix}$$

des éléments du groupe symétrique $\mathcal{S}_7$.

a) Écrire les permutations s_1 et s_2 comme produits de cycles à supports deux à deux disjoints.

b) Quels sont l'ordre et la signature de s_1 et s_2 (respectivement ?)

c) Les éléments s_1 et s_2 sont-ils conjugués dans $\mathcal{S}_7$ (resp. dans $\mathcal{A}_7$?) Si oui donner explicitement un élément conjuguant s_1 et s_2.

2) **a)** Quel est l'ordre maximal d'un élément de $\mathcal{S}_7$? (Justifier.)

b) Les éléments d'ordre maximal dans $\mathcal{S}_7$ sont-ils tous conjugués dans $\mathcal{S}_7$ (resp. dans $\mathcal{A}_7$?)

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

Corrigé du Problème n° V

Exercice A : (Équation caractéristique d'un sous-groupe du groupe spécial orthogonal)

Les notations étant celles du TD n° V, exercice B et du TD n° V, exercice C, on considère un sous-groupe fini G de cardinal n de $\mathcal{SO}_3(\mathbb{R})$, P l'ensemble de ses pôles et

$$\mathcal{F} \ := \ \{(g,p) \ \in \ (G \setminus \mathrm{Id}) \times P \ ; \ g(p) \ = \ p\} \ .$$

1) Montrer que

$$\#(\mathcal{F}) \ = \ 2(n-1) \ .$$

Solution : *On a*

$$\mathcal{F} \ = \ \coprod_{g \in G \setminus \mathrm{Id}} \{(g,p) p \in P \ , \ g(p) \ = \ p\} \ .$$

Or un élément de $G \setminus \mathrm{Id}$ a exactement 2 pôles si bien que

$$\#(\mathcal{F}) \ = \ 2\#(G \setminus \mathrm{Id}) \ = \ 2(n-1) \ .$$

Pour tout $p \ \in \ P$, on note $\mathrm{Stab}_G(p)$ son stabilisateur dans G.

2) Rappeler pourquoi, pour tout $p \ \in \ P$, $\mathrm{Stab}_G(p)$ est un sous-groupe de G.
Solution : *(cf. cours V.1.14.)*

3) Montrer que

$$\#(\mathcal{F}) \ = \ \sum_{p \in P} \#((\mathrm{Stab}_G(p) - 1)) \ .$$

Solution : *On a encore*

$$\mathcal{F} \ = \ \coprod_{p \in P} \{(g,p) g \ \in G not g(p) \ = \ p\} \ = \ \coprod_{p \in P} \{(g,p) g \ \in \ G \setminus \mathrm{Id} \cap \mathrm{Stab}_G(p)\} \ .$$

Or pour tout $p \in P$, $\mathrm{Id} \in \mathrm{Stab}_G(p)$ si bien que

$$\#(G \setminus \mathrm{Id} \cap \mathrm{Stab}_G(p)) \ = \ \#(\mathrm{Stab}_G(p)) - 1$$

d'où il vient

$$\#(\mathcal{F}) \ = \ \sum_{p \in P} (\#(\mathrm{Stab}_G(p)) - 1) \ .$$

Pour tout $p \in P$, on note $O(p)$ son orbite sous l'action de G.

4) Montrer que P est la réunion d'un nombre fini d'orbites $O(p_1), \ldots, O(p_r)$ deux à deux disjointes, chacune d'entre elle étant un ensemble fini.

Solution : *Si l'on note $\sim$ la relation d'équivalence définie sur P par l'action de G, (cf. cours V.1.8,) la surjection canonique $\pi : P \to P/\sim$ est une application surjective. Or tout élément de $G \setminus \mathrm{Id}$ a exactement 2 pôles si bien que P est un ensemble fini avec $\#(P) \leq 2\#(G \setminus \mathrm{Id})$ [8]. Il s'ensuit que $P/\sim$ est un ensemble fini.*

Or les classes d'équivalence pour $\sim$ sont exactement les orbites de l'action : il y a donc un nombre fini d'orbite $O(p_1), \ldots, O(p_r)$.

Chaque orbite étant un sous-ensemble de P qui est fini, c'est également un ensemble fini.

5) En déduire que

$$\#(\mathcal{F}) = \sum_{i=1}^{r} \sum_{p \in O(p_i)} (\#(\mathrm{Stab}_G(p)) - 1) .$$

Solution : *Les orbites sous l'action de G étant des classes d'équivalence elles forment une partition de P ce qui donne immédiatement la formule souhaitée.*

6) Rappeler ce qu'on peut dire de $\mathrm{Stab}_G(p)$ et $\mathrm{Stab}_G(q)$ si $O(p) = O(q)$ (ou encore, ce qui revient au même $p \in O(q)$ ou encore $q \in O(p)$.)

Solution : *Si $q \in O(p)$ il existe $g \in G$ tel que $q = g \cdot p = g(p)$ et l'on a établi à la proposition V.1.18 du cours que*

$$\mathrm{Stab}_G(q) = g\mathrm{Stab}_G(p)g^{-1} .$$

Il s'ensuit, puisque la conjugaison par g est un automorphisme que

$$\#(\mathrm{Stab}_G(q)) = \#(\mathrm{Stab}_G(p)) .$$

7) En déduire que

$$\#(\mathcal{F}) = \sum_{i=1}^{r} \#(O(p_i))(\#(\mathrm{Stab}_G(p_i)) - 1) .$$

Solution : *C'est une conséquence des deux questions précédentes.*

8) En déduire que

$$\#(\mathcal{F}) = \sum_{i=1}^{r} n - \#(O(p_i)),$$

puis l'*équation caractéristique du group G* :

$$2 - \frac{2}{n} = \sum_{i=1}^{r} 1 - \frac{1}{\#(\mathrm{Stab}_G(p_i))} .$$

Solution : *La formule*

$$\#(\mathcal{F}) = \sum_{i=1}^{r} n - \#(O(p_i))$$

résulte de celle établie à la question 7), et du résultat donné dans le corollaire V.1.17 du cours.

On établit finalement l'équation caractéristique en utilisant la formule ci-dessus et le résultat de la question 1).

8. On n'a pas nécessairement égalité , en effet, deux éléments de $G \setminus \mathrm{Id}$ peuvent avoir les mêmes pôles.

Exercice B : (**Le groupe** $\mathcal{S}_7$)

1) Soient

$$s_1 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 \end{pmatrix} \text{ et } s_2 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 1 & 4 & 3 & 6 \end{pmatrix}$$

des éléments du groupe symétrique $\mathcal{S}_7$.

a) Écrire les permutations s_1 et s_2 comme produits de cycles à supports deux à deux disjoints.
Solution : *On a*

$$s_1 \;=\; (1\,3\,5\,7) \circ (2\,4\,6) \text{ et } s_2 \;=\; (1\,2\,5\,4) \circ (3\,7\,6)\,.$$

b) Quels sont l'ordre et la signature de s_1 et s_2 (respectivement ?)
Solution : *Les permutations s_1 et s_2 sont toute deux d'ordre 12* ***Ppcm*** *de 3 et 4 et de signature -1.*

c) Les éléments s_1 et s_2 sont-ils conjugués dans $\mathcal{S}_7$ (resp. dans $\mathcal{A}_7$?) Si oui donner explicitement un élément conjuguant s_1 et s_2.
Solution : *Les permutations s_1 et s_2 étant de même type cyclique $(3,4)$ elles sont conjuguées dans $\mathcal{S}_7$ en vertu de la proposition VI.3.5. Définissons :*

$$u := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 2 & 7 & 5 & 6 & 4 \end{pmatrix}.$$

On a alors

$$s_2 \;=\; u \circ s_1 \circ u^{-1}\,;$$

Les permutations s_1 et s_2 n'étant pas des éléments de $\mathcal{A}_7$ elles ne sont évidemment pas conjuguées dans $\mathcal{A}_7$.

2) a) Quel est l'ordre maximal d'un élément de $\mathcal{S}_7$? (Justifier.)
Solution : *On sait que l'ordre d'un élément est entièrement déterminé par son type cyclique. Or les éléments de $\mathcal{S}_7$ on les type cycliques et les ordres correspondants suivants :*

Type	(2)	$(2,2)$	$(2,2,2)$	$(2,3)$	$(2,2,3)$	$(2,4)$	$(2,5)$	(3)	$(3,4)$	(4)	(5)	(6)	(7)
Ordre	2	2	2	6	6	4	10	3	12	4	5	6	7

.

L'ordre maximal pour un élément de $\mathcal{S}_7$ est donc 12.

b) Les éléments d'ordre maximal dans $\mathcal{S}_7$ sont-ils tous conjugués dans $\mathcal{S}_7$ (resp. dans $\mathcal{A}_7$?)
Solution : *Le point précédent montre que les éléments d'ordre maximal sont de type cyclique $(3,4)$ et d'ordre 12. Puisqu'ils ont tous le même type cyclique $(3,4)$ ils sont tous conjugués dans $\mathcal{S}_7$ toujours en vertu de la proposition VI.3.5.*

En revanche le type cyclique $(3,4)$ correspond à des éléments de signature -1, qui ne sont donc pas dands $\mathcal{A}_7$ et ne sont donc pas conjugués dans $\mathcal{A}_7$.

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

Problème n° VII

à rendre le 3 décembre

Les entiers de GAUSS

On notera $\mathbb{G}$ le sous-ensemble du corps des nombres complexes $\mathbb{C}$, défini par :

$$\mathbb{G} \ := \ \{a + ib \ , \ a \in \mathbb{Z}, b \in \mathbb{Z}\} \ \subset \ \mathbb{C} \, .$$

Pour tout $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, **on notera** $N(a + ib) \ := \ a^2 + b^2$.

1) (Structure d'anneau sur $\mathbb{G}$)
Montrer que l'addition $+$ et la multiplication $*$ du corps des complexes $\mathbb{C}$ se restreignent à $\mathbb{G}$ et qu'alors $(\mathbb{G}, +, *)$ est un anneau commutatif intègre.

On notera désormais

$$\forall (\alpha, \beta) \in \mathbb{G} \times \mathbb{G}, \ \alpha | \beta \ \Leftrightarrow \ \exists \gamma \ \in \ \mathbb{G}, \ \beta \ = \ \alpha * \gamma$$

et on dira que α *divise* β.

2) (L'application N)
Montrer que :

a)

$$\forall (\alpha, \beta) \in \mathbb{G} \times \mathbb{G}, \ N(\alpha * \beta) \ = \ N(\alpha) \ * \ N(\beta) \, ;$$

b)

$$\forall \alpha \in \mathbb{G}, \ N(\alpha) \ = \ 0 \ \Leftrightarrow \ \alpha \ = \ 0 \, .$$

3) (Conjugaison)
Montrer que l'application

$$\sigma \ : \ \mathbb{G} \ \to \ \mathbb{G} \ , \ a + ib \ \mapsto \ a - ib$$

est un automorphisme de l'anneau $\mathbb{G}$ *i.e.*un morphisme bijectif de $\mathbb{G}$ dans lui-même.

4) (Division euclidienne)
Pour tout nombre complexe $z \ = \ x + iy \ \in \ \mathbb{C}$, **on notera** $|z| \ := \ x^2 + y^2$. **Notons que pour** $\alpha \ = \ a + ib \in \mathbb{G}$,

$$|\alpha| \ = \ N(\alpha) \, .$$

a) Montrer que pour tout nombre complexe $z \ \in \ \mathbb{C}$, il existe un élément $\alpha \in \mathbb{G}$ tel que

$$|z - \alpha| \ < \ 1 \, .$$

Indication : *Un dessin pourra être très éclairant voire tenir lieu de preuve ...*

b) En déduire que

$$\forall(\alpha,\beta)\in\mathbb{G}\times(\mathbb{G}\setminus\{0\}),\ \exists(\chi,\rho)\ \in\ \mathbb{G}\times\mathbb{G},\ \alpha\ =\ \beta*\chi\ +\ \rho\,\text{et}\,N(\rho)\ <\ N(\beta)\,.$$

5) (**Le groupe** $(\mathbb{G}^\times,*)$)

a) Déterminer le sous ensemble

$$U\ :=\ \{\alpha\ \in\ \mathbb{G}\,;\ N(\alpha)\ =\ 1\}\ \subset\ \mathbb{G}$$

de $\mathbb{G}$.

b) Montrer que $(U,*)$ est un groupe isomorphe à $(\mathbb{Z}/4\mathbb{Z},+)$.

c) Montrer finalement que U est l'ensemble $\mathbb{G}^\times$ des éléments inversibles de l'anneau $(\mathbb{G},+,*)$.

6) (**Structure des idéaux de** $\mathbb{G}$)
Un *idéal* de $\mathbb{G}$ est une partie non vide $I\subset\mathbb{G}$ telle que

$$\forall(\alpha,\beta)\in I\times I,\ \forall(\gamma,\delta)\in\mathbb{G}\times\mathbb{G},\ \gamma*\alpha\ +\ \delta*\beta\ \in\ I\,.$$

a) Montrer que si $\mathfrak{I}\subset\mathbb{G}$ est un idéal, $\mathfrak{I}$ est en particulier un sous-groupe de $(\mathbb{G},+)$.

b) Montrer que $\{0\}$ et $\mathbb{G}$ sont des idéaux de $\mathbb{G}$.

c) Montrer que

$$\forall\alpha\in\mathbb{G},\ \alpha*\mathbb{G}\ :=\ \{\alpha*\beta\ ,\ \beta\in\mathbb{G}\}\ =\ \{\beta\ \in\ \mathbb{G}\,;\ \alpha|\beta\}$$

est un idéal de $\mathbb{G}$.

d) Montrer que pour tout idéal $\mathfrak{I}$ de $\mathbb{G}$ il existe $\alpha\in\mathbb{G}$ tel que $\mathfrak{I}\ =\ \alpha*\mathbb{G}$.
Indication : *On pourra considérer un plus petit élément dans l'ensemble* $\big\{N(\beta)\ ,\ \beta\in\mathfrak{I}\setminus\{0\}\big\}$.

e) i) Montrer que

$$\forall(\alpha,\beta)\in\mathbb{G}\times\mathbb{G},\ \alpha*\mathbb{G}\ =\ \beta*\mathbb{G}\ \Leftrightarrow\ \exists\xi\ \in\ \mathbb{G}^\times,\ \beta\ =\ \xi*\alpha\,.$$

On dit alors que β est *associé* à α.

ii) Que peut-on dire de la relation « est associé à » ?

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

Corrigé du Problème n° VII

Les entiers de GAUSS

On notera $\mathbb{G}$ le sous-ensemble du corps des nombres complexes $\mathbb{C}$, défini par :

$$\mathbb{G} \ := \ \{a+ib \ , \ a \in \mathbb{Z}, b \in \mathbb{Z}\} \ \subset \ \mathbb{C} \ .$$

Pour tout $(a,b) \in \mathbb{Z} \times \mathbb{Z}$, **on notera** $N(a+ib) \ := \ a^2+b^2$.

1) (Structure d'anneau sur $\mathbb{G}$)

Montrer que l'addition $+$ et la multiplication $*$ du corps des complexes $\mathbb{C}$ se restreignent à $\mathbb{G}$ et qu'alors $(\mathbb{G},+,*)$ est un anneau commutatif intègre.

Solution :

*i) ($+$ **et** $*$ **sont internes sur** $\mathbb{G}$)*

$$\begin{array}{rcl} \forall (a,b,c,d) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}, \quad (a+ib)+(c+id) & = & a+c+i(b+d) \\ & \in & \mathbb{G} \\ (a+ib)*(c+id) & = & a*c-b*d+i(bc+ad) \\ & \in & \mathbb{G} \end{array}$$

Les lois $+$ et $*$ de $\mathbb{C}$ se restreignent donc àç $\mathbb{G}$ et donnent des lois internes sur $\mathbb{G}$.

*ii) (**Propriétés héritées de celle de** $\mathbb{C}$)*

Il est clair que les lois $+$ et $*$ en se restreignant à $\mathbb{G}$ restent associatives, commutatives et $*$ reste distributive sur $+$.

*iii) ($(\mathbb{G},+)$ **est un groupe abélien**)*

En effet, $0 \ = \ 0+0i \in \mathbb{C}$ est élément de $\mathbb{G}$ et est évidemment un élément neutre pour $+$. De plus pour tout $(a,b) \in \mathbb{Z}\times\mathbb{Z}$, $-a-ib \in \mathbb{G}$ est un opposé pour $a+ib$.

On aurait également pu dire que $\mathbb{G}$ était une partie non vide de $\mathbb{C}$ telle que

$$\forall (\alpha,\beta) \in \mathbb{G}\times\mathbb{G}, \ \alpha-\beta \in \mathbb{G}$$

ce qui entraîne que $\mathbb{G}$ est un sous-groupe de $(\mathbb{C},+)$ et par conséquent un groupe abélien.

*iv) ($(\mathbb{G},+,*)$ **est un anneau commutatif**)*

on a déjà vu que $*$ était interne, distributive sur $+$ et commutative. Reste à remarquer que $1 \ = \ 1+0i \in \mathbb{G}$ est un élément neutre pour $*$ pour conclure que $(\mathbb{G},+,*)$ est un anneau commutatif.

*v) (**Intègre**)*

Pour tout $(\alpha,\beta) \in \mathbb{G}\times\mathbb{G}$, $\alpha*\beta \ = \ 0$ peut être vue comme une égalité entre deux nombres complexes. Or $\mathbb{C}$ étant un corps est en particulier intègre ce qui entraîne que $\alpha \ = \ 0$ ou $\beta \ = \ 0$. Il s'ensuit que $\mathbb{G}$ est intègr.

On notera désormais

$$\forall(\alpha,\beta)\in\mathbb{G}\times\mathbb{G},\ \alpha|\beta\ \Leftrightarrow\ \exists\gamma\ \in\ \mathbb{G},\ \beta\ =\ \alpha*\gamma$$

et on dira que α ***divise*** β.

2) (L'application N**)**
Montrer que :

a)

$$\forall(\alpha,\beta)\in\mathbb{G}\times\mathbb{G},\ N(\alpha*\beta)\ =\ N(\alpha)\ *\ N(\beta)\,;$$

Solution : *Cette propriété est bien connue dans* $\mathbb{C}$ *et reste évidemment vraie dans* $\mathbb{G}$.

b)

$$\forall\alpha\in\mathbb{G},\ N(\alpha)\ =\ 0\ \Leftrightarrow\ \alpha\ =\ 0\,.$$

Solution : *Pour* $\alpha\ =\ a+ib$,

$$N(\alpha)\ =\ 0\ \Leftrightarrow\ a^2+b^2\ =\ 0\ \Leftrightarrow\ a\ =\ b\ =\ 0\ \Leftrightarrow\ \alpha\ =\ 0\,.$$

3) (Conjugaison)
Montrer que l'application

$$\sigma\ :\ \mathbb{G}\ \to\ \mathbb{G}\,,\ a+ib\ \mapsto\ a-ib$$

est un automorphisme de l'anneau $\mathbb{G}$ *i.e.*un morphisme bijectif de $\mathbb{G}$ dans lui-même.
Solution : *Il est d'abord immédiat de constater que*

$$\forall a+ib\in\mathbb{G},\ \sigma(a+ib)\ =\ a-ib\in\mathbb{G}\,.$$

Ensuite

$$\begin{array}{rcl}\forall(a+ib,c+id)\in\mathbb{G}\times\mathbb{G},\quad \sigma[(a+ib)+(c+id)] & = & \sigma(a+c+i(b+d))\\ & = & a+c-i(b+d)\\ & = & a-ib+c-id\\ & = & \sigma(a+ib)+\sigma(c+id)\end{array}$$

c'est-à-dire que σ *et un morphisme de groupes de* $(\mathbb{G},+)$ *dans lui-même. De plus* $\sigma(1)$ $=\ 1$ *et finalement :*

$$\begin{array}{rcl}\forall(a+ib,c+id)\in\mathbb{G}\times\mathbb{G},\quad \sigma[(a+ib)*(c+id)] & = & \sigma[ac-bd+i(ad+bc)]\\ & = & ac-bd-i(ad+bc)\\ & = & (a-ib)*(c-id)\\ & = & \sigma(a+ib)*\sigma(c+id)\end{array}$$

ce qui prouve finalement que σ *est bien un endomorphisme de l'anneau* $(\mathbb{G},+,*)$.
Enfin il est immédiat de constater que $\sigma\circ\sigma\ =\ \mathrm{Id}_{\mathbb{G}}$ *ce qui assure que* σ *est bijectif.*

4) (**Division euclidienne**)

Pour tout nombre complexe $z = x + iy \in \mathbb{C}$, **on notera** $|z| := x^2 + y^2$. **Notons que pour** $\alpha = a + ib \in \mathbb{G}$,

$$|\alpha| = N(\alpha) .$$

a) Montrer que pour tout nombre complexe $z \in \mathbb{C}$, il existe un élément $\alpha \in \mathbb{G}$ tel que

$$|z - \alpha| < 1 .$$

Indication : *Un dessin pourra être très éclairant voire tenir lieu de preuve ...*

Solution : *Notons* $z = x + iy$. *Il existe alors un unique couple* $(p, q) \in \mathbb{Z} \times \mathbb{Z}$ *tel que*

$$p \leq x < p + 1 \text{ et } q \leq y < q + 1 .$$

Il faut alors constater que pour l'un au moins des quatre sommets

$$\alpha_1 := p + iq \ , \ \alpha_2 := p + 1 + iq \ , \ \alpha_3 := p + 1 + i(q + 1) \ , \ \alpha_4 := p + i(q + 1)$$

du carré « entourant » z,

$$|z - \alpha_i| < 1 .$$

b) En déduire que

$$\forall (\alpha, \beta) \in \mathbb{G} \times (\mathbb{G} \setminus \{0\}), \ \exists (\chi, \rho) \in \mathbb{G} \times \mathbb{G}, \ \alpha = \beta * \chi + \rho \text{ et } N(\rho) < N(\beta) .$$

Solution : *Soit* $(\alpha, \beta) \in \mathbb{G} \times (\mathbb{G} \setminus \{0\})$. *Puisque* $\beta \neq 0$, β *possède un inverse dans* $\mathbb{C}$ *(qui est un corps). D'après le point précédent il existe donc* $\chi \in \mathbb{G}$ *tel que* $|\frac{\alpha}{\beta} - \chi| < 1$. *Notons*

$$\rho := \beta * (\frac{\alpha}{\beta} - \chi) = \alpha - \beta * \chi \in \mathbb{G} .$$

On a par ailleurs

$$N(\rho) = |\beta * (\frac{\alpha}{\beta} - \chi)| = |\beta| * |\frac{\alpha}{\beta} - \chi| = N(\beta) * |\frac{\alpha}{\beta} - \chi| < N(\beta) .$$

5) (**Le groupe** $(\mathbb{G}^\times, *)$)

a) Déterminer le sous ensemble

$$U := \{\alpha \in \mathbb{G} \, ; \, N(\alpha) = 1\} \subset \mathbb{G}$$

de $\mathbb{G}$.

Solution : *Pour tout* $(a, b) \in \mathbb{Z} \times \mathbb{Z}$,

$$a + ib \in U \Leftrightarrow a^2 + b^2 = 1 \Leftrightarrow \big(a^2 = 1 \text{ et } b^2 = 0\big) \text{ ou } \big(a^2 = 0 \text{ et } b^2 = 1\big) \Leftrightarrow U = \{1, i, -1, -i\} .$$

b) Montrer que $(U, *)$ est un groupe isomorphe à $(\mathbb{Z}/4\mathbb{Z}, +)$.
Solution : *La question question 2), a) assurre que*

$$\forall(\alpha,\beta) \in \mathbb{G}\times\mathbb{G},\ \alpha \in U\ ,\ \beta \in U\ \Rightarrow\ N(\alpha) = 1\ ,\ N(\beta) = 1 \Rightarrow N(\alpha*\beta) = N(\alpha)*N(\beta) = 1 \Rightarrow \alpha*\beta \in U\ .$$

Complétons la table de $*$ sur U : et mettonts la en regard de la table de $(\mathbb{Z}/4\mathbb{Z}, +)$:

$$(U,*)\ :\ \begin{array}{|cccccc|}\hline * & 1 & i & -1 & -i \\ 1 & 1 & i & -1 & -i \\ i & i & -1 & -i & 1 \\ -1 & -1 & -i & 1 & i \\ -i & -i & 1 & i & -1 \\ \hline\end{array}\quad ,\ (\mathbb{Z}/4\mathbb{Z},+)\ :\ \begin{array}{|ccccc|}\hline + & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \\ \hline\end{array}\ .$$

Il est dès lors clair que $(U, *)$ est un groupe puisque on voit dans la table que 1 est un élément neutre et que tout éléments possède un symétrique (inverse.) Enfin l'application :

$$\begin{array}{rcl} \mathbb{Z}/4\mathbb{Z} & \to & U \\ 0 & \mapsto & 1 \\ 1 & \mapsto & i \\ 2 & \mapsto & -1 \\ 3 & \mapsto & -i \end{array}$$

est évidemment un isomorphisme.

c) Montrer finalement que U est l'ensemble $\mathbb{G}^\times$ des éléments inversibles de l'anneau $(\mathbb{G}, +, *)$.
Solution : *Il résulte de b) que $U \subset \mathbb{G}^\times$. Par ailleurs,*

$$\begin{array}{rrcl} & \forall\alpha \in \mathbb{G},\ \alpha & \in & \mathbb{G}^\times \\ \Leftrightarrow & \exists\beta\ \in\ \mathbb{G},\ \alpha*\beta & = & 1 \\ \Rightarrow & N(\alpha)*N(\beta) & = & N(\alpha*\beta) \\ & & = & 1 \\ \Rightarrow & N(\alpha) & = & N(\beta) \\ & & = & 1 \\ \Rightarrow & \alpha \in U & \text{et} & \beta \in U\ . \end{array}$$

6) (Structure des idéaux de $\mathbb{G}$)
Un *idéal* de $\mathbb{G}$ est une partie non vide $I \subset \mathbb{G}$ telle que

$$\forall(\alpha,\beta) \in I \times I,\ \forall(\gamma,\delta) \in \mathbb{G} \times \mathbb{G},\ \gamma*\alpha\ +\ \delta*\beta\ \in\ I\ .$$

a) Montrer que si $\mathfrak{I} \subset \mathbb{G}$ est un idéal, $\mathfrak{I}$ est en particulier un sous-groupe de $(\mathbb{G}, +)$.
Solution : *Le sous-ensemble $\mathfrak{I}$ est en particulier non vide par définition. De plus $\forall(\alpha,\beta) \in \mathfrak{I} \times \mathfrak{I},$, comme $(1,-1) \in \mathbb{G} \times \mathbb{G}$, $\alpha - \beta \in \mathfrak{I}$, ce qui assure que $\mathfrak{I}$ est un sous-groupe de $(\mathbb{G}, +)$.*

b) Montrer que $\{0\}$ et $\mathbb{G}$ sont des idéaux de $\mathbb{G}$.
Solution : *C"est immédiat.*

c) Montrer que

$$\forall \alpha \in \mathbb{G},\ \alpha * \mathbb{G} \ := \ \{\alpha * \beta \ , \ \beta \in \mathbb{G}\} \ = \ \{\beta \ \in \ \mathbb{G} \ ; \ \alpha | \beta\}$$

est un idéal de $\mathbb{G}$.

Solution :

$$\begin{array}{rrcl} & \forall (\beta,\gamma) \in \mathfrak{I} \times \mathfrak{I}, & \forall (\lambda,\mu) \in \mathbb{G} \times \mathbb{G}, & \exists (\xi,\eta) \ \in \ \mathbb{G} \times \mathbb{G}, \\ & \beta \ = \ \alpha * \xi & , & \gamma \ = \ \alpha * \eta \\ \Rightarrow & \lambda * \beta + \mu * \gamma & = & \alpha * \lambda * \xi + \alpha * \mu * \eta \\ & & = & \alpha * (\lambda * \xi + \mu * \eta) \\ & & \in & \mathfrak{I} \ . \end{array}$$

d) Montrer que pour tout idéal $\mathfrak{I}$ de $\mathbb{G}$ il existe $\alpha \in \mathbb{G}$ tel que $\mathfrak{I} \ = \ \alpha * \mathbb{G}$.

Indication : *On pourra considérer un plus petit élément dans l'ensemble* $\big\{N(\beta) \ , \ \beta \in \mathfrak{I} \setminus \{0\}\big\}$.

Solution : *Soit* $\mathfrak{I}$ *un idéal de* $\mathbb{G}$. *Si* $\mathfrak{I} \ = \ \{0\}$, $\mathfrak{I} \ = \ 0 * \mathbb{G}$ *et l'on a répondu à la question.*

Si $\mathfrak{I} \ \neq \ \{0\}$,

$$E \ := \ \big\{N(\beta)\beta \in \mathfrak{I} \setminus \{0\}\big\} \ \subset \ \mathbb{N}^*$$

est une partie non vide de $\mathbb{N}^*$ *et contient donc un plus petit élément* $N(\alpha)$. *Dès lors*

$$\alpha \in \mathfrak{I} \ \Rightarrow \ \forall \beta \in \mathbb{G},\ \alpha * \beta \in \mathfrak{I} \ \Rightarrow \ \alpha * \mathbb{G} \ \subset \ \mathfrak{I} \ .$$

Réciproquement, graçe à la question 4), b), puisque $\alpha \ \neq \ 0$,

$$\begin{array}{rrcl} & \forall \beta \in \mathfrak{I}, & \exists (\chi,\rho) \ \in \ \mathbb{G} \times \mathbb{G}, & \beta \ = \ \alpha * \chi + \rho \ , \ N(\rho) < N(\alpha) \\ \Rightarrow & \rho \ = \ \beta - \chi * \alpha \ \in \ \mathfrak{I} & , & N(\rho) < N(\alpha) \\ \Rightarrow & N(\rho) & = & 0 \\ \Rightarrow & \rho & = & 0 \\ \Rightarrow & \beta & \in & \alpha * \mathbb{G} \\ \Rightarrow & \mathfrak{I} & \subset & \alpha * \mathbb{G} \\ \Rightarrow & \mathfrak{I} & = & \alpha * \mathbb{G} \ . \end{array}$$

e) i) Montrer que

$$\forall (\alpha,\beta) \in \mathbb{G} \times \mathbb{G},\ \alpha * \mathbb{G} \ = \ \beta * \mathbb{G} \ \Leftrightarrow \ \exists \xi \ \in \ \mathbb{G}^{\times},\ \beta \ = \ \xi * \alpha \ .$$

On dit alors que β est *associé* à α.

ii) Que peut-on dire de la relation « est associé à » ?

Solution :

i)

$$\begin{array}{rrcl} & \forall (\alpha,\beta) \in \mathbb{G} \times \mathbb{G}, & \alpha * \mathbb{G} \ = \ \beta * \mathbb{G} & \\ \Leftrightarrow & & \alpha \in \beta * \mathbb{G} \ \text{ et } \ \beta \in \alpha * \mathbb{G} & \\ \Leftrightarrow & & \exists (\xi,\eta) \ \in \ \mathbb{G} \times \mathbb{G}, & \\ & & \alpha \ = \ \beta * \xi \ \text{ et } \ \beta \ = \ \alpha * \eta & \\ \Rightarrow & & \alpha \ = \ \alpha * \xi * \eta & \\ \Rightarrow & & \alpha * (1 - \xi * \eta) \ = \ 0 & \\ \Rightarrow & & \xi * \eta \ = \ 1 & \\ \Rightarrow & & (\xi,\eta) \ \in \ \mathbb{G}^{\times} \times \mathbb{G}^{\times} \ . & \end{array}$$

On utilise ici que $\mathbb{G}$ *est un anneau intègre.*

Le sens réciproque est immédiat.

ii) La relation « est associé à » est clairement une relation d'équivalence.

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

Examen partiel du 24 octobre 2018
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.

Exercice B : () **(Groupe produit)**

Soient $(H, *_H)$ **et** $(K, *_K)$ **des groupes d'élément neutre** e_H **(resp.** e_K.**) On note**

$$G := H \times K = \{(x, y)\ ,\ x \in H\ ,\ y \in K\}$$

et

$$\begin{array}{rrcl} p_H : & G & \to & H \\ & (x, y) & \mapsto & x, \\ p_K : & G & \to & K \\ & (x, y) & \mapsto & y\ . \end{array}$$

On pourra alléger les notations, en supprimant les $_H$ **et** $_K$ **notamment, si l'on estime qu'aucune confusion n'en résultera.**

1) () Montrer que $* : G \times G \to G$, définie par

$$\forall\big((x, y), (z, t)\big) \in G \times G,\ (x, y) * (z, t) := (x *_H z, y *_K t)$$

donne à G une structure de groupe, pour laquelle on précisera l'élément neutre et le symétrique de tout élément. Remarquer que si $(H *_H)$ et $(K, *_K)$ sont abéliens, $(G, *)$ l'est aussi.

2) () Montrer que la loi $*$ définie sur G à la question 1), est la seule pour laquelle p_H et p_K sont des morphismes de groupes.

3) () **Notons**

$$i_K : K \to G\ ,\ y \mapsto (e_H, y)\ .$$

a) () Vérifier que i_K est un morphisme de groupes.

b) () Comparer $\operatorname{Im} i_K$ et $\operatorname{Ker} p_H$.

Exercice C : () **(Groupes à** 4 **éléments)**

Soit $(G, *)$ **un groupe d'élément neutre** e, **avec** $\#(G) = 4$. **Pour tout** $a \in G$, **tout** $n \in \mathbb{N}$, **on notera** a^n **le produit de** n **facteur égaux à** a, **qu'on peut tout à fait définir rigoureusement par récurrence.**

1) () Montrer que

$$\forall a \in G,\ a \neq e \Rightarrow a^3 \neq e\ .$$

2) () Donner la table de composition de G dans le cas où

$$\forall a \in G,\ a^2 \ = \ e\ .$$

Dans ce cas, G est-il abélien ?

3) () **On suppose qu'il existe** $a \in G$ **tel que** $a^2 \neq e$.

a) () Montrer que $a^4 \ = \ e$.

b) () Donner la table de composition de G dans ce cas.

c) () G est-il abélien ?

4) () Combien y a-t-il de classes d'isomorphismes de groupes de cardinal 4 ?

Exercice D : () (**Introduction au groupe symétrique**)

1) () Étant donné un ensemble E,
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.

On suppose désormais que E **est fini et non vide c'est-à-dire qu'il existe une bijection**

$$\iota \ : \ E \ \cong \ [1;n]\ ,\ n \ \in \ \mathbb{N}^*\ .$$

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 $n \ \geq \ 0$. **On définit sur** $\mathcal{S}_{n+1}$ **la relation binaire** R **par**

$$s \ R \ t \ \Leftrightarrow \ s(n+1) \ = \ t(n+1)\ .$$

4) () Montrer que R ainsi définie est une relation d'équivalence.

5) () Rappeler pourquoi l'ensemble $\mathcal{S}_{n+1}/R$ des classes d'équivalences selon R forme une partition de $\mathcal{S}_{n+1}$.

6) () Montrer que pour tout $s \ \in \ \mathcal{S}_{n+1}$ il existe une bijection entre la classe $\overline{s}$ de s selon R et $\mathcal{S}_n$.
Indication : *On pourra chercher à construire explicitement une bijection* $\phi \ : \ \overline{s} \ \to \ \mathcal{S}_n$ *en considérant, pour tout* $t \ \in \ \overline{s}$, $s^{-1} \circ t$, *ainsi que sa bijection réciproque* $j\psi \ : \ \mathcal{S}_n \ \to \ \overline{s}$.

7) () À quelle condition (nécessaire et suffisante) la classe $\overline{s}$ d'un élément de $\mathcal{S}_{n+1}$ est-elle un sous-groupe de $\mathcal{S}_{n+1}$? Caractériser ce sous-groupe.

8) () Montrer que l'application

$$\nu \ : \ \mathcal{S}_{n+1} \ \to \ [1;n+1]\ ,\ s \ \mapsto \ s(n+1)\ .$$

est surjective.

9) () Montrer qu'il existe une bijection

$$\overline{\nu} \ : \ \mathcal{S}_{n+1}/R \ \to \ [1;n+1] \text{ telle que } \forall s \in \mathcal{S}_{n+1},\ \nu(s) \ = \ \overline{\nu}(\overline{s})\ .$$

10) () 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.

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

Corrigé de l'examen partiel du 24 octobre 2018

Exercice A : () **(Parties dénombrables de $\mathbb{N}$)**

Soit $P \subset \mathbb{N}$, une partie (ou encore un sous-ensemble) de l'ensemble $\mathbb{N}$ des entiers naturels. On suppose que P n'est pas un ensemble fini.

1) () Montrer que P a un plus petit élément que l'on notera $f(0)$.

Solution : *Puisque P n'est pas fini, P n'est pas l'ensemble vide $\emptyset$. Alors P possède un plus petit élément (cf. cours II.2.9.)*

2) () En notant

$$P = \{f(0)\} \cup Q\,, \text{ avec } f(0) \notin Q,$$

montrer que Q n'est pas un ensemble fini et que

$$\forall x \in Q,\ f(0) < x\,.$$

Solution : *Si l'ensemble Q est fini, comme le singleton $\{f(0)\}$ est fini, il résulte de la proposition II.4.2.iii) du cours que P est fini. Par contraposée, Q n'est donc pas fini.*

Par ailleurs $f(0)$ étant le plus petit élément de P, pour tout $x \in P$, $f(0) \leq x$, et donc a fortiori, puisque $Q \subset P$, pour tout $x \in Q$, $f(0) \leq x$. Or $f(0) \notin_Q$, entraîne que $x \in Q$ implique $x \neq f(0)$ donc $f(0) < x$.

3) () Démontrer par récurrence l'assertion $\mathcal{H}_n$ ($n \in \mathbb{N}$,) suivante : *i*l existe des entiers naturels $f(i)$,$0 \leq i \leq n$ tels que :

App$_1$)
$$\forall 0 \leq i \leq n-1,\ f(i) < f(i+1)\,;$$

App$_2$)
$$P = \{f(0), \ldots, f(n)\} \cup R\,;$$

App$_3$) l'ensemble R n'est pas fini ;

App$_4$)
$$\forall x \in R,\ f(n) < x\,.$$

Solution :

*i) (**Initialisation**)*

L'existence d'un entier $f(0)$ est assurée par la question 1). La condition App$_1$) est automatiquement satisfaite.

Les conditions App$_2$), App$_3$) et App$_4$) sont assurées par la question 2).

L'assertion $\mathcal{H}_0$ est donc établie.

ii) ***(Hérédité)***

Si $\mathcal{H}_n$ est satisfaite, d'après App$_3$), R est non vide et possède donc un plus petit élément que l'on note $f(n+1)$.

D'après App$_4$) et App$_1$), les entiers $f(i)\,,0 \leq i \leq n+1$ satisfont App$_1$).

D'après la question 2) appliqué à R puisque R n'est pas fini, il existe un ensemble S tel que

—
$$R \;=\; \{f(n+1)\} \;\cup\; S\,;$$

—
$$\{f(n+1)\} \;\cap\; S \;=\; \emptyset\,;$$

— *S n'est pas fini ;*

—
$$\forall x \in S,\; f(n+1) \;<\; x\,.$$

Or
$$P \;=\; \{f(0),\ldots,f(n)\} \;\cup\; R \;=\; \{f(0),\ldots,f(n+1)\} \;\cup\; S$$

et les propriétés de S établies ci-dessus assurent que les assertions App$_2$) à App$_4$) sont satisfaites pour P, S et les enteiers $f(i)\,,0 \leq i \leq n+1$; c'est-à-dire que $\mathcal{H}_{n+1}$ est établie.

4) () En déduire qu'on a ainsi construit une application strictement croissante $f \;:\; \mathbb{N} \;\to\; P$.

Solution : *Puisque $\mathcal{H}_n$ est vérifiée pour tout n, d'après la question 3), on peut définir l'entier $f(n) \;\in\; P$ pour tout n ce qui signifie que f est bien définie.*

De plus en appliquant $\mathcal{H}_{n+1}$ on a immédiatement

$$\forall n \in \mathbb{N},\; f(n) \;<\; f(n+1)\,.$$

On peut en déduire, par récurrence que

$$\forall m \in \mathbb{N},\; \forall n \in \mathbb{N},\; m \;<\; n \;\Rightarrow\; f(m) \;<\; f(n)\,.$$

5) () En déduire que f est injective et que

$$\forall n \in \mathbb{N},\; n \;\leq\; f(n)\,.$$

Solution : *Une application strictement croissante est toujours injective.*

L'inégalité $n \;\leq\; f(n)$ a été établie au TD n° II, exercice B.

6) () Montrer que, pour tout $p \;\in\; P, p \;\in\; \{f(0),\ldots,f(p)\}$ et par conséquent que f est surjective.

Solution : *Pour tout $p \;\in\; P, p \;\in\; \mathbb{N}$, en particulier, si bien que d'après la question 5), $p \;\leq\; f(p)$ et $\mathcal{H}_p$ est satisfaite d'après la question 3). Il s'ensuit que d'après la question 3), App$_2$) et la question 3), App$_4$), $p \;\in\; \{f(0),\ldots,f(p)\}$.*

Pour tout $p \;\in\; P$, il existe donc $0 \;\leq\; i \;\leq\; p$ tel que $f(i) \;=\; p$, c'est-à-dire que f est surjective.

7) () Conclure qu'alors, pour une partie $P \;\subset\; \mathbb{N}$,

— soit P est finie,

— soit il existe une bijection $f \;:\; \mathbb{N} \;\to\; P$. Dans ce dernier cas, on dit que P est *dénombrable*.

Exercice B : () **(Groupe produit)**

Soient $(H, *_H)$ **et** $(K, *_K)$ **des groupes d'élément neutre** e_H **(resp.** e_K.**) On note**

$$G \ := \ H \times K \ = \ \{(x, y) \ , \ x \in H \ , \ y \in K\}$$

et

$$\begin{array}{rrcl} p_H : & G & \to & H \\ & (x, y) & \mapsto & x, \\ p_K : & G & \to & K \\ & (x, y) & \mapsto & y \ . \end{array}$$

On pourra alléger les notations, en supprimant les $_H$ **et** $_K$ **notamment, si l'on estime qu'aucune confusion n'en résultera.**

1) () Montrer que $* \ : \ G \times G \ \to \ G$, définie par

$$\forall\big((x, y), (z, t)\big) \in G \times G, \ (x, y) * (z, t) \ := \ (x *_H z, y *_K t)$$

donne à G une structure de groupe, pour laquelle on précisera l'élément neutre et le symétrique de tout élément. Remarquer que si $(H *_H)$ et $(K, *_K)$ sont abéliens, $(G, *)$ l'est aussi.

Solution : *Tout d'abord puisque* $*_H$ *(resp.* $*_K$*) est une loi de groupe sur* H *(resp.* K*) i.e. interne,* $(x *_H z, y *_K t)$ *est bien un élément de* G*, si bien que* $*$ *est une loi interne.*

En outre la loi $*_H$ *(resp.* $*_K$*) étant associative,*

$$\begin{array}{rcl} \forall\big((x, y), (z, t), (u, v)\big) \in G \times G \times G, \quad \big((x, y) * (z, t)\big) * (u, v) & = & (x *_H z, y *_K t) * (u, v) \\ & = & \big((x * z) * u, (y * t) * v\big) \\ & = & \big(x * (z * u), y * (t * v)\big) \\ & = & (x, y) * \big((z, t) * (u, v)\big) \end{array}$$

ce qui assure que $*$ *est associative.*

De plus,

$$\begin{array}{rcl} \forall (x, y) \in G, \quad (x, y) * (e_H, e_K) & = & (x *_H e_H, y *_K e_K) \\ & = & (x, y) \\ & = & (e_H *_H x, e_K *_K y) \\ & = & (e_H, e_K) * (x, y) \ , \end{array}$$

ce qui prouve que (e_H, e_K) *est un élément neutre pour* G.

Enfin pour tout $x \ \in \ H$ *(resp.* $y \ \in \ K$*,) notons* x^{-1}*, son inverse dans* H *(resp.* y^{-1} *son inverse dans* K.*) Alors :*

$$\begin{array}{rcl} \forall (x, y) \in G, \quad (x, y) * (x^{-1}, y^{-1}) & = & (x * x^{-1}, y * y^{-1}) \\ & = & (e_H, e_K) \\ & = & (x^{-1} * x, y^{-1} * y) \\ & = & (x^{-1}, y^{-1}) * (x, y) \ , \end{array}$$

ce qui assure que (x^{-1}, y^{-1}) *est un inverse pour* (x, y) *dans* G*. Le couple* $(G, *)$ *est donc un groupe.*

Si H *et* K *sont abéliens :*

$$\begin{array}{rcl} \forall\big((x, y), (z, t)\big) \in G \times G, \quad (x, y) * (z, t) & = & (x * z, y * t) \\ & = & (z * x, t * y) \\ & = & (z, t) * (x, y) \ , \end{array}$$

ce qui prouve que G *est abélien.*

2) () Montrer que la loi $*$ définie sur G à la question 1), est la seule pour laquelle p_H et p_K sont des morphismes de groupes.

Solution :

$$\begin{array}{rcl} \forall\big((x,y),(z,t)\big) \in G\times G,\quad p_H\big((x,y)*(z,t)\big) & = & p_H\big((x *_H z, y *_K t)\big) \\ & = & x *_H z \\ & = & p_H\big((x,y)\big) *_H p_H\big((z,t)\big)\ , \end{array}$$

ce qui assure que p_H est un morphisme de groupes, le même résultat valant pour p_K, par un raisonnement tout à fait similaire.

Si maintenant $\cdot$ est une loi de composition sur G pour laquelle p_H et p_K sont des morphismes de groupes,

$$\begin{array}{lrcccl} \forall\big((x,y),(z,t)\big) \in G\times G, & p_H\big((x,*y)\cdot(z,t)\big) & = & p_H\big((x,y)\big) *_H p_H\big((z,t)\big) & = & x *_H z \\ \text{et} & p_K\big((x,*y)\cdot(z,t)\big) & = & p_K\big((x,y)\big) *_K p_K\big((z,t)\big) & = & y *_K t\ , \end{array}$$

si bien que

$$(x,y)\ \cdot\ (z,t)\ =\ (x *_H z, y *_K t)$$

c'est-à-dire que $\cdot$ n'est autre que la loi $*$ défini à la question 1).

3) () **Notons**

$$i_K\ :\ K\ \to\ G\ ,\ y\ \mapsto\ (e_H,y)\ .$$

a) () Vérifier que i_K est un morphisme de groupes.

Solution :

$$\begin{array}{rcl} \forall (y,t)\in K\times K,\quad i_K(y *_K t) & = & (e_H, y *_K t) \\ & = & (e_H,y)*(e_H,t) \\ & = & i_K(y)*i_K(t)\ , \end{array}$$

ce qui assure que i_K est un morphisme.

b) () Comparer $\operatorname{Im} i_K$ et $\operatorname{Ker} p_H$.

Solution : *Pour tout $(x,y)\ \in\ G$,*

$$p_H\big((x,y)\big)\ =\ e_H\ \Leftrightarrow\ x\ =\ e_H$$

c'est-à-dire que

$$(x,y)\ =\ (e_H,y)\ =\ i_K(y)\ .$$

On en déduit donc que

$$\operatorname{Im} i_K\ =\ \operatorname{Ker} p_H\ .$$

Exercice C : () **(Groupes à 4 éléments)**

Soit $(G,*)$ un groupe d'élément neutre e, avec $\#(G)\ =\ 4$. Pour tout $a\ \in\ G$, tout $n\ \in\ \mathbb{N}$, on notera a^n le produit de n facteur égaux à a, qu'on peut tout à fait définir rigoureusement par récurrence.

1) () Montrer que

$$\forall a\in G,\ a\ \neq\ e\ \Rightarrow\ a^3\ \neq\ e\ .$$

Solution : *D'abord*

$$a^2\ =\ a\ \Rightarrow\ a\ =\ e$$

ce qui contredit l'hypothèse donc

$$a^2 \neq a\ .$$

Pour la même raison

$$a^3 \neq a^2\ .$$

Si $a^3 = e$, *on a encore* $a^3 \neq a$, *et* $a^2 \neq e$, *si bien que* e, a, a^2, *sont* 3 *éléments deux à deux distincts de* G. *On peut donc écrire*

$$G = \{e, a, a^2, b\}\ ,\ b \neq e\ ,\ b \neq a\ ,\ b \neq a^2\ .$$

Or $a * b \in G$, *on a donc :*

$$\begin{array}{lrcl} & a*b & = & e \\ \Rightarrow & a*b & = & a^3 \\ \Rightarrow & b & = & a^2 \\ & \textit{contradiction} & & \\ \text{ou} & a*b & = & a \\ \Rightarrow & b & = & e \\ & \textit{contradiction} & & \\ \text{ou} & a*b & = & a^2 \\ \Rightarrow & b & = & a \\ & \textit{contradiction} & & . \end{array}$$

2) () Donner la table de composition de G dans le cas où

$$\forall a \in G,\ a^2 = e\ .$$

Dans ce cas, G est-il abélien ?

Solution : *Écrivons* $G = \{e, a, b, c, \}$ *où* e, a, b, *et* c *sont deux à deux distincts. On a, par hypothèse,*

$$a^2 = b^2 = c^2 = e\ .$$

Or :

$$\begin{array}{lllll} a*b = e & \Rightarrow & b = a & & \textit{contradiction} \\ a*b = a & \Rightarrow & b = e & & \textit{contradiction}\ . \end{array}$$

d'où l'on déduit que $a * b = c$. *Le même argument prouve que* $b * a = c$, *et de même que*

$$b * c = c * b = a \text{ et } c * a = a * c = b$$

ce qui donne la table de composition de G *et prouve qu'il est abélien.*

3) () **On suppose qu'il existe** $a \in G$ **tel que** $a^2 \neq e$.

a) () Montrer que $a^4 = e$.

b) () Donner la table de composition de G dans ce cas.

c) () G est-il abélien ?

4) () Combien y a-t-il de classes d'isomorphismes de groupes de cardinal 4 ?

Exercice D : () (**Introduction au groupe symétrique**)

1) () Étant donné un ensemble E,
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.

Solution : *(cf. cours III.1.2.c).)*

On suppose désormais que E est fini et non vide c'est-à-dire qu'il existe une bijection

$$\iota \, : \, E \, \cong \, [1; n] \, , \, n \, \in \, \mathbb{N}^* \, .$$

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.

Solution : *(cf. cours III.2.6.)*

3) () Quel est le cardinal de $\mathcal{S}_2$?

Fixons un entier $n \, \geq \, 0$. On définit sur $\mathcal{S}_{n+1}$ la relation binaire R par

$$s \, R \, t \, \Leftrightarrow \, s(n+1) \, = \, t(n+1) \, .$$

4) () Montrer que R ainsi définie est une relation d'équivalence.

Solution :

*i) (**Réflexivité**)*
Pour tout $s \, \in \, \mathcal{S}_{n+1}$, $s(n+1) \, = \, s(n+1)$ si bien que $s \, R \, s$, et que R est réflexive.

*ii) (**symétrie**)*
Pour tout $(s, t) \, \in \, \mathcal{S}_{n+1} \times \mathcal{S}_{n+1}$,

$$s(n+1) \, = \, t(n+1) \, \Leftrightarrow \, t(n+1) \, = \, s(n+1)$$

si bien que

$$s \, R \, t \, \Leftrightarrow \, t \, R \, s$$

et que R est donc symétrique.

*iii) (**Transitivité**)*

$$\begin{array}{lrcl} \forall (s, t, u) \in \mathcal{S}_{n+1} \times \mathcal{S}_{n+1} \times \mathcal{S}_{n+1}, & sRt & \text{et} & tRu \\ \Leftrightarrow & s(n+1) \, = \, t(n+1) & \text{et} & t(n+1) \, = \, u(n+1) \\ \Rightarrow & s(n+1) & = & u(n+1) \\ \Rightarrow & s & R & u \, , \end{array}$$

si bien que R est transitive.

On a ainsi montré que R est une relation d'équivalence.

Remarque 4).4 Dans le lemme VI.1.5, on a considéré une relation d'équivalence $\sim$ à peine différente. Cependant la relation R considérée ici conduirait à envisager une action à droite (cf. cours V.2.5.) Or nous avons surtout développé la théorie des actions à gauche.

5) () Rappeler pourquoi l'ensemble $\mathcal{S}_{n+1}/R$ des classes d'équivalences selon R forme une partition de $\mathcal{S}_{n+1}$.

6) () Montrer que pour tout $s \in \mathcal{S}_{n+1}$ il existe une bijection entre la classe $\overline{s}$ de s selon R et $\mathcal{S}_n$.
Indication : *On pourra chercher à construire explicitement une bijection $\phi : \overline{s} \to \mathcal{S}_n$ en considérant, pour tout $t \in \overline{s}$, $s^{-1} \circ t$, ainsi que sa bijection réciproque $j\psi : \mathcal{S}_n \to \overline{s}$.*
Solution : *Pour tout $t \in \overline{s}$, par définition de R, $t(n+1) = s(n+1)$. Il s'ensuit que*

$$s^{-1}[t(n+1)] = s^{-1}[s(n+1)] = n+1 .$$

Il en résulte que

$$\forall 1 \leq k \leq n, \int s \circ t(k) \in [1;k]$$

la restriction de $s^{-1} \circ t_{|[1;n]}$ de $s^{-1} \circ t$ à $[1;n]$ est injective puisque $s^{-1} \circ t$ l'est et que la restriction d'une application injective reste injective. En vertu de la proposition II.4.12.i) du cours,

$$\phi(t) := s^{-1} \circ t_{|[1;n]}$$

est bijective donc $\phi(t) \in \mathcal{S}_n$. On a ainsi construit une application

$$\phi : \overline{s} \to \mathcal{S}_n .$$

Réciproquement, pour tout $u \in \mathcal{S}_n$, notons $\tilde{u}$ l'application de $[1;n+1]$ dans lui-même définie par

$$\forall 1 \leq k \leq n, \ \tilde{u}(k) := u(k) \text{ et } u(n+1) = n+1 .$$

Il est presque immédiat de constater que $\tilde{u}$ est surjective. Il découle alors de la proposition II.4.12.ii) du cours que $\tilde{u}$ est bijective, c'est-à-dire que $\tilde{u} \in \mathcal{S}_{n+1}$. Posons alors

$$\psi(u) := s \circ \tilde{u} \in \mathcal{S}_{n+1} .$$

Il s'ensuit que

$$\psi(u)(n+1) = s[\tilde{u}(n+1)] = s(n+1)$$

c'est-à-dire que $\psi(u) \in \overline{s}$. On a ainsi défini une application

$$\psi : \mathcal{S}_n \to \overline{s} .$$

Il est désormais très facile de montrer que ϕ et ψ sont inverses l'une de l'autre.
On peut aussi utiliser le corollaire VI.1.6 du cours, pour peu qu'on tienne comte de la remarque question 4), 4).4.

7) () À quelle condition (nécessaire et suffisante) la classe $\overline{s}$ d'un élément de $\mathcal{S}_{n+1}$ est-elle un sous-groupe de $\mathcal{S}_{n+1}$? Caractériser ce sous-groupe.
Solution : *Si $\overline{s}$ est un sous-groupe, en particulier $\mathrm{Id}_{[1;n+1]} \in \overline{s}$. La classe $\overline{s}$ d'un élément s est donc un sous-groupe si et seulement si*

$$\overline{s} = \overline{\mathrm{Id}_{[1;n+1]}} = \mathcal{S}_n .$$

8) () Montrer que l'application

$$\nu : \mathcal{S}_{n+1} \to [1;n+1] , \ s \mapsto s(n+1) .$$

est surjective.
Solution : *Voir le lemme VI.1.7.i) du cours.*

9) () Montrer qu'il existe une bijection

$$\overline{\nu} : \mathcal{S}_{n+1}/R \to [1;n+1] \text{ telle que } \forall s \in \mathcal{S}_{n+1}, \ \nu(s) = \overline{\nu}(\overline{s}) .$$

Solution : *Voir le lemme VI.1.7.ii) du cours.*

10) () 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.

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

Examen du 19 décembre 2018
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.

Exercice A : () (**Équations et systèmes de congruence**)

1) () Pour chacune des équations suivantes, déterminer l'ensemble des couples (x, y) d'entiers relatifs puis l'ensemble des couples (x, y) d'entiers naturels la satisfaisant.

a) ()

$$26x - 22y = 49651\,.$$

b) ()

$$19x - 286y = 1\,.$$

2) () (**Systèmes de congruences**)
Déterminer l'ensemble des entiers relatifs x satisfaisant

$$\mathcal{S} : \left\{\begin{array}{rcl} 13x & \equiv & 1\,[19] \\ x & \equiv & 2\,[26] \\ x & \equiv & 14\,[22] \end{array}\right\}\,.$$

Indication : *On pourra chercher à résoudre d'abord*

$$\left\{\begin{array}{rcl} x & \equiv & 2\,[26] \\ x & \equiv & 14\,[22] \end{array}\right\}$$

Exercice B : () **1)** () Étant donnés deux entiers relatifs a et b premiers entre eux, montrer que le PGCD de $3a + 2b$ et $7a + 11b$ est soit 1 soit 19.

2) () Plus généralement, soient $a, b, a_{1,1}, a_{1,2}, a_{2,1}, a_{2,2}$ des entiers relatifs. Soient d le PGCD de a et b et $\delta := a_{1,1}a_{2,2} - a_{2,1}a_{1,2}$. Montrer qu'alors le PGCD de $aa_{1,1} + ba_{1,2}$ et $aa_{2,1} + ba_{2,2}$ divise $d\delta$.

Exercice C : () **1)** () **Soient**

$$s_1 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} \text{ et } s_2 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 6 & 3 & 2 \end{pmatrix}$$

des éléments du groupe symétrique $\mathcal{S}_6$.

a) () Écrire s_1 et s_2 comme produits de cycles à supports deux à deux disjoints.

b) () Donner l'ordre et la signature des permutations s_1 et s_2.

c) () Les éléments s_1 et s_2 sont-ils conjugués dans le groupe symétrique $\mathcal{S}_6$?

d) () Donner un élément $u \in \mathcal{A}_6$ tel que

$$s_2 = u \circ s_1 \circ u^{-1} .$$

2) () (**Le groupe alterné** $\mathcal{A}_6$)

a) () Quel est le nombre d'éléments du groupe alterné $\mathcal{A}_6$?

b) () Donner les classes de conjugaison dans $\mathcal{S}_6$ des éléments de $\mathcal{A}_6$.

c) () Combien y a-t-il d'éléments de type cyclique $(3,3)$ dans $\mathcal{A}_6$? Sont-ils tous conjugués dans $\mathcal{S}_6$?

3) () (**Éléments de type** $(3,3)$)
On considère désormais une permutation $s := (a\,b\,c)(d\,e\,f)$ **de type cyclique** $(3,3)$ **dans** $\mathcal{S}_6$.

a) () Rappeler la relation qui lie le nombre d'éléments de $s^{\mathcal{A}_6}$, $\mathrm{Stab}_{\mathcal{A}_6}(s)$ et $\mathcal{A}_6$.

b) () Montrer que le stabilisateur $\mathrm{Stab}_{\mathcal{A}_6}(s)$ de s dans $\mathcal{A}_6$ est un sous-groupe du stabilisateur $\mathrm{Stab}_{\mathcal{S}_6}(s)$ de s dans $\mathcal{S}_6$.

c) () Pour $u \in \mathrm{Stab}_{\mathcal{S}_6}(s)$, montrer que les conditions suivantes sont équivalentes :

i)
$$u(a) \in \{a;b;c\} .$$

ii)
$$u(\{a;b;c\}) \subset \{a;b;c\} .$$

iii)
$$u(\{d;e;f\}) \subset \{d;e;f\} .$$

d) () Montrer que l'ensemble H_s des éléments de $\mathrm{Stab}_{\mathcal{S}_6}(s)$ vérifiant l'une des conditions équivalentes ci-dessus est un sous-groupe de $\mathrm{Stab}_{\mathcal{A}_6}(s)$.
Indication : *On pourra chercher à exprimer les éléments de* H_s *en fonction des cycles* $(a\,b\,c)$ *et* $(d\,e\,f)$.

e) () Déterminer le nombre d'éléments de H_s et montrer qu'il est moitié de celui de $\mathrm{Stab}_{\mathcal{S}_6}(s)$.

f) () Montrer que
$$u := \begin{pmatrix} a & b & c & d & e & f \\ d & e & f & a & b & c \end{pmatrix}$$
est un élément de $\mathrm{Stab}_{\mathcal{S}_6}(s)$ qui n'appartient pas à $\mathrm{Stab}_{\mathcal{A}_6}(s)$.

g) () Déduire de ce qui précède que

$$\mathrm{Stab}_{\mathcal{A}_6}(s) = H_s$$

puis le nombre d'éléments de $s^{\mathcal{A}_6}$ puis retrouver que les permutations s_1 et s_2 de la question question 1) sont conjuguées dans $\mathcal{A}_6$.

Exercice D : () **On note $\mathbb{R}[X]$ l'ensemble des polynômes à une indéterminée et à coefficients réels.**

1) () Rappeler ce que signifie que $\mathbb{R}[X]$ est un anneau principal et énoncer sans démonstration le théorème dont c'est une conséquence.

2) () Montrer que l'ensemble

$$I := \{(X^2+1)P\,,\ P \in \mathbb{R}[X]\} \subset \mathbb{R}[X]$$

est un idéal de $\mathbb{R}[X]$.

On note $A := \mathbb{R}[X]/I$ l'anneau quotient et i la classe de X dans A.

3) () Montrer que pour tout $\alpha \in A$, il existe un unique $(a,b) \in \mathbb{R}\times\mathbb{R}$ tel que α soit la classe de $aX+b$.

4) () Que vaut i^2 ?

5) () Quel objet peut-on reconnaître dans l'anneau A ?

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

Corrigé de l'examen du 19 décembre 2018

Exercice A : () **(Équations et systèmes de congruence)**

1) () Pour chacune des équations suivantes, déterminer l'ensemble des couples (x, y) d'entiers relatifs puis l'ensemble des couples (x, y) d'entiers naturels la satisfaisant.

a) ()

$$26x - 22y \;=\; 49651\,.$$

Solution : *L'algorithme d'Euclide pour* 26 *et* 22 *s'écrit :*

$$\begin{array}{ccc} 26 & 1 & 0 \\ 22 & 0 & 1 \\ 39 & 1 & -2 \\ 2 & -2 & 5 \end{array}$$

c'est-à-dire que $26 \wedge 22 \;=\; 2$. *Il en résultera que pour tout couple* (x, y) *d'entiers relatifs,* $2 \mid 26x - 22y$. *Or* 2 *ne divisant pas* 49651, *l'équation n'a pas de solution entière.*

b) ()

$$19x \;-\; 286y \;=\; 1\,.$$

Solution : *L'algorithme d'Euclide pour* 19 *et* 286 *s'écrit :*

$$\begin{array}{ccccc} & 19 & 1 & 0 \\ & 286 & 0 & 1 \\ 1 & 619 & 1 & -1 \\ 2 & 309 & -2 & 3 \\ 2 & 1 & 5 & -7\,. \end{array}$$

Il en résulte que $(5, 7)$ *est une solution de l'équation*

$$19x \;-\; 286y \;=\; 1$$

ce qui prouve en outre (cf. cours IX.3.9.1,) que 19 *et* 286 *sont premiers entre eux. L'ensemble des couples d'entiers relatifs solution de l'équation ci-dessus est donc*

$$\{(5 + 286k, 7 + 19k)\;,\; k \in \mathbb{Z}\}\,.$$

De plus $(5 + 286k, 7 + 19k) \in \mathbb{N} \times \mathbb{N}$ *si et seulement si* $k \geq 0$.

2) () **(Systèmes de congruences)**

Déterminer l'ensemble des entiers relatifs x satisfaisant

$$\mathcal{S} \ : \ \left\{ \begin{array}{rcl} 13x & \equiv & 1\,[19] \\ x & \equiv & 2\,[26] \\ x & \equiv & 14\,[22] \end{array} \right\} .$$

Indication : *On pourra chercher à résoudre d'abord*

$$\left\{ \begin{array}{rcl} x & \equiv & 2\,[26] \\ x & \equiv & 14\,[22] \end{array} \right\}$$

Solution :

i) Commençons par considérer le système :

$$\mathcal{S}_1 \ : \ \left\{ \begin{array}{rcl} x & \equiv & 2\,[26] \\ x & \equiv & 14\,[22] \end{array} \right\} .$$

On constate qu'on ne peut assurer a priori que ce système possède une solution dans la mesure où l'on ne peut pas appliquer le théorème chinois des restes puisque $26 \wedge 22 \ = \ 13 \ \neq \ 1$. *On a cependant :*

$$\begin{array}{rcl} \mathcal{S}_1 & \leftrightarrow & \exists (r,s) \ \in \ \mathbb{Z} \times \mathbb{Z}, \\ & & \left\{ \begin{array}{rcl} x & = & 2+26r \\ x & = & 14+22s \end{array} \right\} \\ & \leftrightarrow & \left\{ \begin{array}{rcl} x & = & 2+26r \\ 26r-22s & = & 52 \end{array} \right\} \\ & \leftrightarrow & \left\{ \begin{array}{rcl} x & = & 2+26r \\ 17r-7s & = & 4 \end{array} \right\} . \end{array}$$

On constate alors que $(-1,-3)$ *est une solution particulière de l'équation* $17r-7s \ = \ 4$. *On sait alors que l'ensemble des solutions de cette équation est* $S_1 \ := \ \{(-1+7k-3+17k) \ , \ k \in \mathbb{Z}\}$. *Il an résulte que :*

$$\begin{array}{rcl} \mathcal{S}_1 & \Leftrightarrow & \left\{ \begin{array}{rcl} x & = & 2+26(-1+7k) \\ x & = & 14+91(-3+17k) \end{array} \right\} \\ & \leftrightarrow & \left\{ \begin{array}{rcl} x & = & -215+286k \\ x & = & -215+286k \end{array} \right\} \\ & \leftrightarrow & x \ = \ -215+286k \\ & \leftrightarrow & x \ \equiv \ -215\,[286] \, . \end{array}$$

Le système $\mathcal{S}$ *équivaut alors au système*

$$\mathcal{S}_2 \ \Leftrightarrow \ \left\{ \begin{array}{rcl} 13x & \equiv & 1\,[19] \\ x & \equiv & -215\,[286] \end{array} \right\} .$$

ii) L'algorithme d'Euclide pour 19 *et* 13 *s'écrit :*

$$\begin{array}{rrrr} & 19 & 1 & 0 \\ & 13 & 0 & 1 \\ 166 & 8 & 1 & -166 \\ 1 & 5 & -1 & 167 \\ 1 & 3 & 2 & -333 \\ 1 & 2 & -3 & 500 \\ 1 & 1 & 5 & -833 \end{array} \ .$$

D'où il découle que l'inverse de 13 *modulo* 19 *est* $-833 = 1333$.

Le système $\mathcal{S}$ *est donc équivalent au système*

$$\mathcal{S} \ : \ \left\{ \begin{array}{rcl} x & \equiv & 1333\,[19] \\ x & \equiv & 1332\,[286] \end{array} \right\} .$$

iii) Or nous avons montré à la question 1), b) que 19 *et* 286 *sont premiers entre eux. Il en résulte (cf. cours IX.5.5.2,) que l'ensemble des solutions du système* $\mathcal{S}''$ *est une classe d'entiers modulo* $19 * 286$. *Or si* $x \in \mathbb{Z}$ *est solution du système* $\mathcal{S}''$, *il existe des entiers relatifs* r *et* s *tels que*

$$\begin{aligned} x &= 1333 + 19r \\ x &= 1332 + 286s \end{aligned}$$

ce qui implique que

$$19r - 286s = -1 .$$

En utilisant les résultats de la question 1), b), on obtient qu'il existe $k \in \mathbb{Z}$ *tel que*

$$\begin{aligned} r &= -5 + 286k \\ s &= -7 + 19k \end{aligned}$$

d'où il résulte que

$$x = 1333 + 19r = 1333 + 19(-5 + 286k) = -9497 + 3350802k .$$

Exercice B : () **1)** () Étant donnés deux entiers relatifs a et b premiers entre eux, montrer que le PGCD de $3a + 2b$ et $7a + 11b$ est soit 1 soit 19.

Solution : *Si on pose* $A := \begin{pmatrix} 3 & 2 \\ 7 & 11 \end{pmatrix}$, $B := \begin{pmatrix} 11 & -2 \\ -7 & 3 \end{pmatrix}$, *on a* $A * B = B * A = 19 * \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. *Or :*

$$\begin{aligned} & \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = A * \begin{pmatrix} a \\ b \end{pmatrix} \\ \Rightarrow \quad & B * \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = B * A \begin{pmatrix} a \\ b \end{pmatrix} \\ & = 19 * \begin{pmatrix} a \\ b \end{pmatrix} \end{aligned}$$

ce qui sécrit encore :

$$19a = 11\alpha - 2\beta \text{ et } 19b = -7\alpha + 3\beta .$$

Si a *et* b *sont premiers entre eux, il existe un couple de coefficients de* BÉZOUT (u, v) *tel que :*

$$\begin{aligned} 19 &= 19a * u + 19b * v \\ &= \alpha(11u - 7v) + \beta(-2u + 3v) \end{aligned}$$

si bien qu'il et clair que le PGCD de α *et* β *divise* 19 *qui est premier, si bien qu'il vaut* 1 *ou* 19.

2) () Plus généralement, soient $a, b, a_{1,1}, a_{1,2}, a_{2,1}, a_{2,2}$ des entiers relatifs. Soient d le PGCD de a et b et $\delta := a_{1,1}a_{2,2} - a_{2,1}a_{1,2}$. Montrer qu'alors le PGCD de $aa_{1,1} + ba_{1,2}$ et $aa_{2,1} + ba_{2,2}$ divise $d\delta$.

Solution : *Considérons les matrices* $A := \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$ *et* $B := \begin{pmatrix} a_{2,2} & -a_{1,2} \\ -a_{2,1} & a_{1,1} \end{pmatrix}$. *On remarque qu'alors on a :* $A * B = B * A = \delta \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. *Posons* $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} := A * \begin{pmatrix} a \\ b \end{pmatrix}$. *On cherche des propriétés du PGCD de* α *et* β. *Soit* (u, v) *un couple de coefficient de* BÉZOUT *pour* a *et* b *c'est-à-dire que* $au + bv = d$ *ce qui s'écrit encore matriciellement* $\begin{pmatrix} u & v \end{pmatrix} * \begin{pmatrix} a \\ b \end{pmatrix} = d$. *Il s'ensuit alors que :*

$$\begin{aligned} \begin{pmatrix} u & v \end{pmatrix} * B * \begin{pmatrix} \alpha \\ \beta \end{pmatrix} &= \begin{pmatrix} u & v \end{pmatrix} * B * A * \begin{pmatrix} a \\ b \end{pmatrix} \\ &= \begin{pmatrix} u & v \end{pmatrix} * \delta * \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} * \begin{pmatrix} a \\ b \end{pmatrix} \\ &= \delta * \begin{pmatrix} u & v \end{pmatrix} * \begin{pmatrix} a \\ b \end{pmatrix} \\ &= d\delta \end{aligned}$$

si bien qu'il existe des entiers relatifs k et l tels que $k\alpha + l\beta = d\delta$ ce qui prouve le résultat.

Exercice C : () **1)** () **Soient**

$$s_1 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} \text{ et } s_2 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 6 & 3 & 2 \end{pmatrix}$$

des éléments du groupe symétrique $\mathcal{S}_6$.

a) () Écrire s_1 et s_2 comme produits de cycles à supports deux à deux disjoints.
Solution :

$$s_1 = (1\,3\,5)(2\,4\,6)\,,\ s_2 = (1\,5\,3)(2\,4\,6)\,.$$

b) () Donner l'ordre et la signature des permutations s_1 et s_2.
Solution : *Les permutations s_1 et s_2 sont d'ordre 3 et de signature 1.*

c) () Les éléments s_1 et s_2 sont-ils conjugués dans le groupe symétrique $\mathcal{S}_6$?
Solution : *Les permutations s_1 et s_2 ont même type cyclique $(3,3)$ et sont donc conjuguées dans $\mathcal{S}_6$ en vertu de la proposition VI.3.5 du cours.*

d) () Donner un élément $u \in \mathcal{A}_6$ tel que

$$s_2 = u \circ s_1 \circ u^{-1}\,.$$

Solution : *L'élément $u := (1\,2)(3\,4\,5\,6)$ vérifie*

$$u \circ s_1 \circ u^{-1} = (u(1)\,u(3)\,u(5))(u(2)\,u(4)\,u(6)) = (2\,4\,6)(1\,5\,3) = s_2$$

et $u \in \mathcal{A}_6$.

2) () **(Le groupe alterné $\mathcal{A}_6$)**

a) () Quel est le nombre d'éléments du groupe alterné $\mathcal{A}_6$?

Solution : *Pour $n \geq 2$, le nombre d'éléments du groupe alterné $\mathcal{A}_n$ est $\frac{n!}{2}$ (cf. cours VI.4.8.ii).) Il en résulte donc que $\mathcal{A}_6$ a 360 éléments.*

b) () Donner les classes de conjugaison dans $\mathcal{S}_6$ des éléments de $\mathcal{A}_6$.
Solution : *Toujours en vertu de la proposition VI.3.5 du cours, les classes de conjugaison des éléments de $\mathcal{A}_6$ sont caractérisées par le type cyclique commun de leurs éléments. Dans $\mathcal{A}_6$ hormis l'identité, on a des éléments de type cyclique $(2,2)$, $(2,4)$, (3) $(3,3)$, et (5).*

c) () Combien y a-t-il d'éléments de type cyclique $(3,3)$ dans $\mathcal{A}_6$? Sont-ils tous conjugués dans $\mathcal{S}_6$?
Solution : *Dès qu'on a une partie $\{a;b;c\}$ à 3 éléments parmi 6, on a aussi son complémentaire $\{d;e;f\}$ et l'on peut construire les permutations de type cyclique $(3,3)$*

$$(a\,b\,c)(d\,e\,f)\,,\ (a\,c\,b)(d\,e\,f)\,,\ (a\,b\,c)(d\,f\,e) \text{ et } (a\,c\,b)(d\,f\,e)$$

et aucune autre. On peut donc construire ainsi 4 permutations de type cyclique $(3,3)$. Or si l'on recense toutes les parties à 3 éléments on recensera également leur complémentaire et les permutations de type cyclique $(3,3)$ construites sur une partie sont exactement celles construites sur son complémentaire. Il faut donc se limiter à la moitié des parties à 3 éléments et on peut construire 4 permutations pour chacune d'entre elles. Le nombre de permutations qu'on peut donc finalement construire est double du nombre de parties à 3 éléments soit 40.

3) () **(Éléments de type** $(3,3)$**)**

On considère désormais une permutation $s := (a\,b\,c)(d\,e\,f)$ **de type cyclique** $(3,3)$ **dans** $\mathcal{S}_6$.

a) () Rappeler la relation qui lie le nombre d'éléments de $s^{\mathcal{A}_6}$, $\mathrm{Stab}_{\mathcal{A}_6}(s)$ et $\mathcal{A}_6$.

b) () Montrer que le stabilisateur $\mathrm{Stab}_{\mathcal{A}_6}(s)$ de s dans $\mathcal{A}_6$ est un sous-groupe du stabilisateur $\mathrm{Stab}_{\mathcal{S}_6}(s)$ de s dans $\mathcal{S}_6$.

Solution : *On a tout simplement*

$$\mathrm{Stab}_{\mathcal{A}_6}(s) \;=\; \mathrm{Stab}_{\mathcal{S}_6}(s) \,\cap\, \mathcal{A}_6$$

et l'intersection de deux sous-groupes est toujours un sous-groupe de chacun d'entre eux.

c) () Pour $u \in \mathrm{Stab}_{\mathcal{S}_6}(s)$, montrer que les conditions suivantes sont équivalentes :

i)
$$u(a) \;\in\; \{a;b;c\}\,.$$

ii)
$$u(\{a;b;c\}) \;\subset\; \{a;b;c\}\,.$$

iii)
$$u(\{d;e;f\}) \;\subset\; \{d;e;f\}\,.$$

Solution : *Rappelons tout d'abord la formule utile*

$$usu^{-1} \;=\; (u(a)\,u(b)\,u(c))(u(d)\,u(e)\,u(f))$$

.

Si $u(a) \in \{a;b;c\}$, *comme*

$$(u(a)\,u(b)\,u(c))(u(d)\,u(e)\,u(f)) \;=\; (a\,b\,c)(d\,e\,f),$$

nécessairement

$$(u(a)\,u(b)\,u(c)) \;=\; (a\,b\,c)$$

ce qui prouve que l'assertion (i) entraîne l'assertion (ii). Le fait que (ii) entraîne (i) est évident. L'équivalence entre (ii) et (iii) est simplement une conséquence du fait que u *est une bijection.*

d) () Montrer que l'ensemble H_s des éléments de $\mathrm{Stab}_{\mathcal{S}_6}(s)$ vérifiant l'une des conditions équivalentes ci-dessus est un sous-groupe de $\mathrm{Stab}_{\mathcal{A}_6}(s)$.

Indication : *On pourra chercher à exprimer les éléments de* H_s *en fonction des cycles* $(a\,b\,c)$ *et* $(d\,e\,f)$.

Solution : *Il est d'abord clair que l'identité est dans* H_s *celui-ci est donc non vide. La condition (ii) est ensuite stable par composition et passage à l'inverse ce qui assure que* H_s *est un sous-groupe de* $\mathrm{Stab}_{\mathcal{S}_6}(s)$ *en vertu de la proposition du cours.*

Il est moins immédiat, en revanche, de prouver que $H_s \subset \mathcal{A}_6$.

Si $u \in H_s$, $u(a) \in \{a;b;c\}$. *Nous avons alors déjà vu que* $(a\,b\,c) \;=\; (u(a)\,u(b)\,u(c))$. *On constate alors que*

$$\begin{aligned} u(a) = a \;&\Rightarrow\; u(b) = b, u(c) = c \\ u(a) = b \;&\Rightarrow\; u(b) =, cu(c) = a \\ u(a) = c \;&\Rightarrow\; u(b) = a, u(c) = b\,. \end{aligned}$$

La restriction de u *à* $\{a;b;c\}$ *est donc nécessairement une puissance du cycle* $(a\,b\,c)$.

La condition (iii) implique que $u(d) \in \{d;e;f\}$ *et l'on en tire la conclusion analogue que la restriction de* u *à* $\{d;e;f\}$ *est une puissance du* 3*-cycle* $(d\,e\,f)$. *La permutation* u *est donc un produit de* 3*-cycles et par conséquent un élément de* $\mathcal{A}_6$.

e) () Déterminer le nombre d'éléments de H_s et montrer qu'il est moitié de celui de $\mathrm{Stab}_{\mathcal{S}_6}(s)$.

Solution : *On a vu à la question précédente qu'un élément* $u \in H_s$ *s'écrivait* $(a\,b\,c)^i(d\,e\,f)^j$ i *et* j *pouvant prendre les valeurs* $0, 1, 2$. *Il en résulte que* $\#(H_s) = 9$.

On peut utiliser la formule de la question pour déterminer le nombre d'éléments de $\mathrm{Stab}_{\mathcal{S}_6}(s)$ *puisqu'on a montré que* $\#(s^{\mathcal{S}_6}) = 40$ *à la question . Il en résulte donc que*

$$\#(\mathrm{Stab}_{\mathcal{S}_6}(s)) = \frac{6!}{40} = 18 = 2 * \#(H_s)\ .$$

f) () Montrer que

$$u := \begin{pmatrix} a & b & c & d & e & f \\ d & e & f & a & b & c \end{pmatrix}$$

est un élément de $\mathrm{Stab}_{\mathcal{S}_6}(s)$ qui n'appartient pas à $\mathrm{Stab}_{\mathcal{A}_6}(s)$.

Solution : *Il est tout d'abord clair que* $u \in \mathrm{Stab}_{\mathcal{S}_6}(s)$. *Mais d'autre part,* $u = (a,d)(b,e)(c,f)$ *qui est un produit de* 3 *transpositions et n'est donc pas dans* $\mathcal{A}_6$.

g) () Déduire de ce qui précède que

$$\mathrm{Stab}_{\mathcal{A}_6}(s) = H_s$$

puis le nombre d'éléments de $s^{\mathcal{A}_6}$ puis retrouver que les permutations s_1 et s_2 de la question question 1) sont conjuguées dans $\mathcal{A}_6$.

Solution : *Le groupe* $\mathrm{Stab}_{\mathcal{A}_6}(s)$ *est un sous-groupe de* $\mathrm{Stab}_{\mathcal{S}_6}(s)$ *son cardinal divise donc celui de* $\mathrm{Stab}_{\mathcal{S}_6}(s)$. *Par ailleurs, on a montré à la question que* $H_s \subset \mathrm{Stab}_{\mathcal{A}_6}(s)$, *d'où il résulte que*

$$\#(\mathrm{Stab}_{\mathcal{A}_6}(s)) \geq \#(H_s) = \frac{\#(\mathrm{Stab}_{\mathcal{S}_6}(s))}{2}$$

d'après la question .

Enfin on a vu à la question que

$$\#(\mathrm{Stab}_{\mathcal{A}_6}(s)) < \#(\mathrm{Stab}_{\mathcal{S}_6}(s))\ .$$

Il en résulte que

$$\#(\mathrm{Stab}_{\mathcal{S}_6}(s)) = 2 * \#(\mathrm{Stab}_{\mathcal{A}_6}(s))\ .$$

Comme d'autre part,

$$\#(\mathcal{S}_6) = 2 * \#(\mathcal{A}_6)$$

il résulte de la formule que

$$\#(s^{\mathcal{A}_6}) = \#(s^{\mathcal{S}_6})$$

d'où comme naturellement $s^{\mathcal{A}_6} \subset s^{\mathcal{S}_6}$,

$$s^{\mathcal{A}_6} = s^{\mathcal{S}_6}$$

c'est-à-dire que toutes les permutations de type cyclique $(3,3)$ *sont non seulement conjuguées dans* $\mathcal{S}_6$ *mais encore dans* $\mathcal{A}_6$ *et en particulier les permutations* s_1 *et* s_2 *de la question .*

Exercice D : () **On note** $\mathbb{R}[X]$ **l'ensemble des polynômes à une indéterminée et à coefficients réels.**

1) () Rappeler ce que signifie que $\mathbb{R}[X]$ est un anneau principal et énoncer sans démonstration le théorème dont c'est une conséquence.

2) () Montrer que l'ensemble

$$I := \{(X^2+1)P\,,\ P \in \mathbb{R}[X]\} \subset \mathbb{R}[X]$$

est un idéal de $\mathbb{R}[X]$.

On note $A := \mathbb{R}[X]/I$ l'anneau quotient et i la classe de X dans A.

3) () Montrer que pour tout $\alpha \in A$, il existe un unique $(a,b) \in \mathbb{R}\times\mathbb{R}$ tel que α soit la classe de $aX+b$.

4) () Que vaut i^2 ?

5) () Quel objet peut-on reconnaître dans l'anneau A ?

Université Paris Sud — Année 2018–2019

L3/S5 M313 — Algèbre Générale

Examen du 7 juin 2018
Durée 2h30

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.

Université Paris Sud **Année 2018–2019**

L3/S5 M313 **Algèbre Générale**

Corrigé de l'examen du 7 juin 2018

Université Paris Sud **Année 2018–2019**

L3/S5 M313 **Algèbre Générale**

Index