Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

Table des matières

Université Paris Sud **Année 2014–2015**

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

0.0 . −Motivation

Il est usuel de développer l'arithmétique des entiers que nous allons étudier au chapitre I.2 à partir d'un système de Peano dont on rappelle la définition :

Définition 0.0.1 (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 :

$$\begin{array}{rccc} \mathfrak{s}: & \mathbb{N} & \to & \mathbb{N} \\ +: & \mathbb{N}\times\mathbb{N} & \to & \mathbb{N} \\ *: & \mathbb{N}\times\mathbb{N} & \to & \mathbb{N} \end{array} \qquad 0.0.1.1$$

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 II s'appuyant notamment sur le paragraphe 0.5. Il semble à ce point à tout le moins raisonnable de ce 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 0.1 à 0.4, soit « le bon cadre » cherché, ce que nous n'affirmerons pas, mais même un « cadre acceptable ». Cependant un résultat comme la proposition 0.3.10 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 I.2 peut 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

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 » »

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.

0.1 . −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. 0.0.1,)) puisse se faire au sein de cette théorie grâce en particulier à des résultats comme la proposition 0.3.10.

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 0.1.1 i) $\forall$: pour tout (quantificateur universel ;)

ii) $\exists$: il existe ;

iii) $\text{et ou} \wedge$: et (conjonction ;)

iv) $\text{ou ou} \vee$: disjonction ;

v) $\text{non ou} \not$ 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 0.4.2. 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 0.3.10 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 0.1.2 ($\Leftrightarrow$) 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 0.1.3 (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,

$\mathbf{Z}_{\text{fini}\,5}$) **(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 0.1.4 (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 0.1.3.$\mathbf{Z}_{\text{fini}\,4}$) sera noté $\mathcal{P}(a)$.

iii) ($\bigcup$:)
L'ensemble b introduit dans l'axiome de l'union 0.1.3.$\mathbf{Z}_{\text{fini}\,3}$) peut être noté

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

iv) ($\cup$:)

Pour deux ensembles a et b l'axiome de la paire 0.1.3.$\mathbf{Z}_{\text{fini}\,2}$) 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 0.1.5 i) (**Formules ensemblistes**)

On appelle *formule ensembliste* une formule comportant des variables, les symboles de la logique (cf. 0.1.1) 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 0.1.4.

Remarque 0.1.6 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 0.1.3 y compris pour formuler de nouveaux axiomes. Un bon exercice consiste à réécrire avec les symboles de 0.1.4 ceux des axiomes de 0.1.3 qui peuvent l'être leur donnant alors une forme plus lisible et plus usuelle.

0.2 . −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 0.2.1 i) (**Couples**)

Au regard des axiomes de 0.1.3, 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 0.1.3 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 0.2.2 (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

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

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

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

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 0.2.3 *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 0.2.4 (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 $\mathrm{Dom}\, f \;=\; a$.

Définition 0.2.5 (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 0.2.6 (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 0.2.7 (Propriétés de la restriction) *i) Si $f \;:\; a \;\to\; b$ est une fonction $f_{|\mathrm{Dom}\, f}$ est une application.*

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.*

4. définie rappelons-le par son graphe (cf. 0.2.1.iv),)

Définition 0.2.8 (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 0.2.9 *Une application strictement croissante (resp. strictement décroissante) entre ensembles ordonnés est injective.*

0.3 . −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 0.1.3. 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 0.0.1. On s'apercevra cependant que les axiomes de 0.1.3 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 0.3.4.

Remarque 0.3.1 Les axiomes 0.1.3.$\mathbf{Z}_{\text{fini}4}$) et 0.1.3.$\mathbf{Z}_{\text{fini}5}$) 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 0.1.4.iv) permet ensuite de définir $\mathfrak{s}(a) \ := \ a \cup \{a\}$.

Exemple 0.3.2 Rien dans l'axiomatique 0.1.3 n'assure jusqu'ici que l'ensemble vide $\emptyset$ défini en 0.1.4.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 0.3.4 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 0.1.5.i) et qu'alors l'existence de l'ensemble vide s'en déduit grâce aux axiomes de séparation 0.1.3.$\mathbf{Z}_{\text{fini}5}$).

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

$$\begin{array}{rcl} \mathfrak{s}(\emptyset) & = & \emptyset \cup \{\emptyset\} \\ & = & \{\emptyset\}, \\ \mathfrak{s}(\mathfrak{s}(\emptyset)) & = & \{\emptyset\} \cup \{\{\emptyset\}\} \\ & = & \big\{\emptyset, \{\emptyset\}\big\} \\ \mathfrak{s}(\mathfrak{s}(\mathfrak{s}(\emptyset))) & = & \big\{\emptyset, \{\emptyset\}\big\} \cup \big\{\big\{\emptyset, \{\emptyset\}\big\}\big\} \\ \big\{\emptyset, \{\emptyset\}, \big\{\emptyset, \{\emptyset\}\big\}\big\} \ \ldots & & \end{array} \qquad 0.3.2.1$$

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 0.3.3 (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. 0.0.1,)devrait être un ensemble récurrent pour satisfaire notamment l'axiome
0.0.1.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 0.1.3. Dans ce cas on a recours à l'introduction d'un nouvel axiome, lequel d'ailleurs ne choque pas la raison :

Définition 0.3.4 (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 0.3.5 (Système de ZERMELO Z) On appelle *système de* ZERMELO le système d'axiomes constitué des axiomes de ZERMELO fini 0.1.3 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 0.3.6 *L'intersection de deux ensembles récurrents est un ensemble récurrent.*

On peut introduire l'ensemble ω défini comme suit :

Définition 0.3.7 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 0.0.1.PA$_1$), 0.0.1.PA$_2$) et 0.0.1.PA$_3$) mais reste la questions des axiomes
0.0.1.PA$_4$) à 0.0.1.PA$_7$).

Notation 0.3.8 Pour deux ensembles a et b les axiomes de 0.1.3 assurent que pour deux ensembles distincts x et y :

$$a + b := (a \times \{x\}) \cup (b \times \{y\}) \qquad 0.3.8.1$$

et

$$a \cdot b := a \times b \qquad 0.3.8.2$$

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 0.3.9 *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 0.3.10 *Le quintuplet* $(\omega, \emptyset, \mathfrak{s}, +, \cdot)$ *vérifie les axiome de* PEANO *0.0.1*

0.4 . −Le système de ZERMELO–FRAENKEL

On présente les derniers axiomes qu'il faut adjoindre au système de ZERMELO 0.3.5 pour arriver au système de ZERMELO–FRAENKEL **ZF** (cf. 0.4.1,) puis finalement au système **ZFC** (cf. 0.4.2.) 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 0.4.1 (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$_F$)

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

$\mathbf{ZF}_8$) (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 0.4.2 (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 0.1.3
de l'axiome de l'infini 0.3.4 des axiomes de remplacement 0.4.1.$\mathbf{ZF}_7$)
de l'axiome de fondation 0.4.1.$\mathbf{ZF}_8$)
et de l'axiome du choix.

0.5 . −Structures algébriques

Nous rappelons dans cette sections un certain nombre de définitions sans doute déjà connues à seule fin de pouvoir s'y rapporter dans la suite du texte et de les relier à l'axiomatique des ensembles dont nous avons esquissé une brève présentation dans les paragraphes 0.1 à 0.3.

Définition 0.5.1 (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. 0.2.4.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 0.5.2 (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

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

Définition 0.5.3 (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 0.5.4 (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 0.5.5 (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

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

Définition 0.5.6 (Groupe) i) (**Groupe**)

Un ensemble $(G, *)$ muni d'une loi de composition associative est un *groupe* si :

Gr_1) (**Élément neutre**)

$(G, *)$ possède un élément neutre ***i.e.***

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

Gr_2) (**Symétrique**)
tout élément de G possède un symétrique *i.e.*

$$\forall x \in G,\ \exists y\ \in\ G,\ (x * y\ =\ y * x\ =\ \epsilon)\ .$$

On dit que le groupe $(G, *)$ est *commutatif* ou *abélien* si la loi $*$ est commutative.

ii) (**morphisme**)
Pour deux groupes $(G, *)$ et $(H, \cdot)$ un *morphisme de groupe* ou *homomorphisme de groupe* est un morphisme pour les lois $*$ et $\cdot$ au sens de la définition 0.5.2 c'est-à-dire une application $f\ :\ G\ \to\ H$ vérifiant

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

iii) (**Noyau**)
Pour un morphisme de groupes $f\ :\ G\ \to\ H$ si l'élément neutre de H est noté ϵ_H on appelle *noyau* de f et on note

$$\mathrm{Ker}\, f\ :=\ \{x\ \in\ G\ ;\ f(x)\ =\ \epsilon_H\}\ =\ f^{-1}(\{\epsilon_H\})\ .$$

iv) (**Sous-groupe**)
On dit qu'une partie $H \subset G$ d'un groupe $(G, *)$ est un *sous-groupe* si la restriction (cf. 0.2.6) de $*$ à H fait de $(H, *)$ un groupe.

Remarque 0.5.7 i) Il n'existe pas de loi de composition $*$ sur $\emptyset$ fasse de $(\emptyset, *)$ un groupe. L'axiome 0.5.6.i).Gr_1) entraîne, en effet, qu'un groupe possède toujours au moins un élément c'est-à-dire n'est jamais vide.

ii) Il est usuel d'appler *inverse* le symétrique dans un groupe et même *opposé* si le groupe est abélien. Dans ce dernier cas la loi sera souvent notée $+$ et lélément neutre 0 en référence au groupe abélien $(\mathbb{Z}, +)$ (cf. I.2.2.4.)

Proposition 0.5.8 (Propriétés des morphismes) *Soit*

$$f\ :\ (G, *, \epsilon_G)\ \to\ (H, \cdot, \epsilon_H)$$

un morphisme de groupes.

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.

iii) L'image $\mathrm{Im}\, f$ *de* f *(cf. 0.2.4.ii)) est un sous-groupe de* $(H, \cdot)$.

iv) Le noyau $\mathrm{Ker}\, f$ *de* f *est un sous-groupe de* $(G, *)$.

Preuve *:*

i) (cf. TD n° II, exercice B, question 2), a).)

ii) (cf. TD n° II, exercice B, question 2), b).)

iii) (cf. TD n° II, exercice B, question 2), c).)

iv) (cf. TD n° II, exercice B, question 2), d).)

Définition 0.5.9 (Anneaux) i) (**Anneau**)
Un triplet $(A, +, *)$ est un *anneau* si :

Ann_1) Le couple $(A, +)$ est un groupe abélien .

Ann_2) La loi de composition $*$ est associative, possède un élément neutre (usuellement noté 1_A ou 1 si aucune confusion n'est à craindre) et est *distributive* à gauche et à droite par rapport à $+$ c'est-à-dire que :

$\forall x \in A,\ \forall y \in A,\ \forall z \in A,\ (x * (y + z) = x * y + x * z$ et $(x + y) * z = x * z + y * z)$.
Si de plus la loi $*$ est commutative, on dira que $(A, +, *)$ est un *anneau commutatif*.

ii) (**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*.

iii) (**Élément inversible**)
Dans un anneau $(A, +, *, 1)$ un élément x est *inversible* s'il existe $y \in A$ tel que $x * y = y * x = 1$ autrement dit si x possède un symétrique pour la loi $*$ (cf. 0.5.5.ii).) On note $A^\times$ l'ensemble des éléments inversibles de l'anneau A.

iv) (**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.* $A^\times = A \setminus \{0_A\}$.

v) (**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 : Étant donnés deux anneaux

$$(A, +_A, *_A, 1_A) \text{ et } (B, +_B, *_B, 1_B)$$

on dit qu'une application $f \ : \ A \ \to \ B$ est un *morphisme d'anneau* ou *homomorphisme d'anneau* si :

MorAnn$_1$) f est un morphisme du groupe $(A, +_A)$ dans le groupe $(B, +_B)$.

MorAnn$_2$) f est un morphisme pour les lois $*_A$ et $*_B$ au sens de 0.5.2 c'est-à-dire que

$$\forall x \in A, \ \forall y \in A, \ (f(x *_A y) \ = \ f(x) \ *_B \ f(y)) \, .$$

MorAnn$_3$) $f(1_A) \ = \ 1_B$.

Proposition 0.5.10 *i) Pour tout anneau (resp. anneau commutatif)*

$$(A, +, *) \textit{ le couple } (A^\times, *) \textit{ est un groupe (resp. un groupe abélien.)}$$

ii) Pour tout morphisme d'anneaux $f \ : \ (A, +_A, *_A) \ \to \ (B, +_B, *_B)$ *la restriction* $f^\times$ *de* f *à* $A^\times$ *est un morphisme de groupes à valeurs dans* $B^\times$.

Preuve *:*

i) (cf. TD n° II, exercice B, question 5), b).)

ii) (cf. TD n° II, exercice B, question 5), c).)

I . −Arithmétique dans $\mathbb{Z}$

I.0 . −Introduction

Le but de ce chapitre est de présenter un certain nombre de résultats concernant l'*arithmétique* de l'ensemble $\mathbb{Z}$ des *entiers relatifs* c'est-à-dire essentiellement des propriétés relatives à la structure d'anneau de $\mathbb{Z}$ (cf. I.2.2.5.)

Il est usuel de construire l'ensemble $\mathbb{Z}$ des entiers relatifs à partir de l'ensemble $\mathbb{N}$ des *entiers naturels*. Nous allons donc construire l'ensemble $\mathbb{N}$ des entiers naturels dans le paragraphe I.1 à partir des axiomes de Peano que nous avons déjà mentionnés en 0.0.1 ce qui est assez usuel également. Nous avons vu mais nous ne reviendrons plus guère sur ce sujet, que le système de Peano lui même admettait une représentation dans la théorie **ZFC** (cf. 0.3.10.)

Le paragraphe I.2 sera consacré à construire l'ensemble $\mathbb{Z}$ ou plutôt l'anneau $(\mathbb{Z}, +, *)$ et à en donner les première propriétés.

I.1 . −L'ensemble $\mathbb{N}$ des entiers naturels

I.1.0 . −Introduction

On choisit, dans ce cours, de définir l'ensemble $\mathbb{N}$ à partir des axiomes de Peano :

Définition I.1.0.1 (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 :

$$\begin{array}{rrcl} \mathfrak{s}: & \mathbb{N} & \to & \mathbb{N} \\ +: & \mathbb{N}\times\mathbb{N} & \to & \mathbb{N} \\ *: & \mathbb{N}\times\mathbb{N} & \to & \mathbb{N} \end{array} \qquad \text{I.1.0.1.1}$$

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**$_2$)

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

Définition I.1.0.2 (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,
— établir les propriétés algébriques (d'ailleurs bien connues) de $\mathbb{N}$ c'est-à-dire les propriétés des opérations $+$ et $*$ au paragraphe I.1.1 ;
— définir une relation d'ordre $\leq$ sur $\mathbb{N}$ au paragraphe I.1.2 et montrer notamment le résultat clef que *toute partie non vide de* $\mathbb{N}$ *possède un plus petit élément* (cf. I.1.2.7 ;)
— introduire la notion d'ensemble fini en I.1.3 et donner quelques propriétés.

Définition I.1.0.3 (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.

Notation I.1.0.4 On notera :

$$1\ :=\ \mathfrak{s}(0)\ . \qquad \text{I.1.0.4.1}$$

En prenant $q\ =\ 0$ dans l'axiome I.1.0.1.PA$_5$) et en utilisant I.1.0.1.PA$_4$), il vient alors :

$$\mathfrak{s}(p)\ =\ \mathfrak{s}(p+0)\ =\ p\ +\ \mathfrak{s}(0)\ =\ p\ +\ 1\ . \qquad \text{I.1.0.4.2}$$

Plutôt que $\mathfrak{s}(p)$ on utilisera $p+1$ qui est plus habituel; ce qui donne à l'axiome de récurrence I.1.0.1.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 :

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

I.1.1 . −Les opérations $+$ et $*$

Nous allons démontrer dans les lemmes I.1.1.1, I.1.1.2 et I.1.1.3 des résultat technique concernant les lois $+$ et $*$. Ces résultats n'ont pas été regroupés de la sorte parce que ce groupement ferait sens par raport aux propriétés de $(\mathbb{N}, +, *)$ mais parce que la méthode de démonstration est exactement identique pour chacune des propriétés énoncée dans ces lemmes. Une synthèse de ces propriétés sera donnée dans les propositions I.1.1.4 et I.1.1.5 qui récapitulent les propriétés algébriques de $(\mathbb{N}, +, *)$.

En outre il peut paraître surprenant d'avoir recours à I.1.1.3.3 et I.1.1.3.1 pour démontrer I.1.1.2.3 alors qu'elles sont démontrées postérieurement. Il est cependant facile de se convaincre qu'il ne s'agit que d'une disposition typographique et qu'il n'y a pas de cercle vicieux en constatant que les démonstrations respectives de I.1.1.3.3 et I.1.1.3.1 n'utilisent ni I.1.1.2.3 directement ni aucun résultat qui en serait déduit.

Un autre point délicat est que pour établir l'associativité de $*$ (cf. I.1.1.3.4,) il faut préalablement établir sa distributivité par rapport à $+$ en fait seulement I.1.1.3.3.

Lemme I.1.1.1 *Pour tout entier $p \in \mathbb{N}$, les propriétés suivantes sont vérifiées :*

$$P_1(p) : 0 + p = p + 0 = p \qquad \textit{I.1.1.1.1}$$

$$P_2(p) : p * 1 = 1 * p = p \qquad \textit{I.1.1.1.2}$$

$$P_3(p) : 0 * p = p * 0 = 0 \qquad \textit{I.1.1.1.3}$$

Preuve *: Pour $1 \leq i \leq 3$ on considdère l'ensemble $A_i := \{p \in \mathbb{N}\,;\, P_i(p)\}$. Il suffit de montrer que $0 \in A_i$ et $p \in A_i \Rightarrow p+1 \in A_i$ pour assurer, en vertu de l'axiome de récurrence I.1.0.1.PA$_3$) que $A_i = \mathbb{N}$ c'est-à-dire que P_i est vérifiée pour tout $p \in \mathbb{N}$ ce qui démontre le lemme.*

i) ***(I.1.1.1.1)***

L'axiome I.1.0.1.PA$_4$) entraîne $0+0 = 0$ *i.e.*$0 \in A_1$. *Par ailleurs* $\forall p \in A_1, (p+1)+0 = p+1$ *toujours d'après I.1.0.1.PA$_4$). Par ailleurs*

$$0 + (p+1) = 0 + \mathfrak{s}(p) = \mathfrak{s}(0+p)$$

en utilisant I.1.0.1.PA$_5$). Enfin puisque $p \in A_1, 0+p = p$, *d'où*

$$0 + (p+1) = \mathfrak{s}(0+p) = \mathfrak{s}(p) = p+1\,;$$

ce qui prouve $p+1 \in A_1$.

ii) ***(I.1.1.1.2)***

L'axiome I.1.0.1.PA$_6$) entraîne que $1 * 0 = 0$. *En outre*

$$0 * 1 = 0 * \mathfrak{s}(0) = 0 * 0 + 0 = 0$$

en vertu des axiomes I.1.0.1.PA$_7$) et I.1.0.1.PA$_4$). Il en résulte que $0 \in A_2$.

Pour $p \in A_2$,

$$(p+1) * 1 = (p+1) * \mathfrak{s}(0) = (p+1) * 0 + p + 1 = p+1$$

d'après I.1.0.1.PA$_6$) et I.1.1.1.1. En outre

$$1 * p+1 = 1 * \mathfrak{s}(p) = 1 * p + 1$$

d'après I.1.0.1.PA$_7$). Comme $p \in A_2$ $1 * p = p$, *d'où* $1 * (p+1) = p+1$ *et finalement* $p+1 \in A_2$.

iii) ***(I.1.1.1.3)***

D'après l'axiome I.1.0.1.PA$_6$),

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

En particulier, pour $p = 0$, $0 * 0 = 0$ *c'est-à-dire que* $0 \in A_3$.

Si l'on suppose que $p \in A_3$, *i.e.*$0 * p = 0$, *alors* $0 * (p+1) = 0 * p + 0$ *en appliquant I.1.0.1.PA$_7$), par conséquent,*

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

autrement dit $p+1 \in A_3$.

Lemme I.1.1.2 *Pour tout $p \in \mathbb{N}$ et tout $q \in \mathbb{N}$, on a les propriétés $P_i(p,q)$,$1 \leq i \leq 5$ suivantes :*

$$P_1(p,q) \; : \; \mathfrak{s}(p) \; + \; q \; = \; \mathfrak{s}(p+q) \; = \; p \; + \; \mathfrak{s}(q) \qquad \textit{I.1.1.2.1}$$

$$P_2(p,q) \; : \; p \; + \; q \; = \; q \; + \; p \qquad \textit{I.1.1.2.2}$$

$$P_3(p,q) \; : \; (p+1) \; * \; q \; = \; p * q \; + \; q \qquad \textit{I.1.1.2.3}$$

$$P_4(p,q) \; : \; p \; * \; q \; = \; q \; * \; p \qquad \textit{I.1.1.2.4}$$

$$P_5(p,q) \; : \; p \; * \; q \; \Rightarrow \; p \; = \; 0 \; \vee \; q \; = \; 0 \qquad \textit{I.1.1.2.5}$$

Preuve : *Pour $1 \leq i \leq 5$ on introduit une famille d'ensemble $\left(A_{i,p}\right)_{,p\in\mathbb{N}}$ définie par*

$$A_{i,p} \; := \; \{q \; \in \; \mathbb{N} \, ; \; P_i(p,q)\} \, .$$

Il suffit alors de montrer, que pour tout $1 \leq i \leq 5$ et tout $p \in \mathbb{N}$, $0 \in A_{i,p}$, et $q \in A_{i,p} \Rightarrow q+1 \in A_{i,p}$, pour assurer, en vertu de l'axiome de récurrence I.1.0.1.PA$_3$), que pour tout $1 \leq i \leq 5$ et pour tout $p \in \mathbb{N}$, $A_{i,p} = \mathbb{N}$, ce qui signifie exactement que pour tout $1 \leq i \leq 5$ tout $p \in \mathbb{N}$ et tout $q \in \mathbb{N}$, $P_i(p,q)$ est satisfaite et prouve finalement le lemme.

i) ***(I.1.1.2.1)***
Pour tout $p \in \mathbb{N}$, l'identité

$$\mathfrak{s}(p) \; + \; 0 \; = \; \mathfrak{s}(p+0) \; = \; p \; + \; \mathfrak{s}(0)$$

résulte simplement de I.1.0.1.PA$_4$) et I.1.0.1.PA$_5$) et signifie exactement que $0 \in A_{1,p}$.
Pour $q \in A_{1,p}$,

$$\mathfrak{s}(p + \mathfrak{s}(q)) \; = \; p \; + \; \mathfrak{s}(\mathfrak{s}(q))$$

d'après I.1.0.1.PA$_5$).
En outre,

$$\mathfrak{s}(p) \; + \; \mathfrak{s}(q) \; = \; \mathfrak{s}(\mathfrak{s}(p) + q)$$

d'après I.1.0.1.PA$_5$). Le second membre de l'égalité précédente vaut, puisque $q \in A_{1,p}$, $\mathfrak{s}(p + \mathfrak{s}(q))$. Appliquant encore I.1.0.1.PA$_5$) à cette dernière quantité, on obtient $p + \mathfrak{s}(\mathfrak{s}(q))$ c'est-à-dire que $\mathfrak{s}(q) \in A_{1,p}$.

ii) ***(I.1.1.2.2)***
Pour tout $p \in \mathbb{N}$, *I.1.1.1.1*

$$p + 0 = 0 + p = p$$

c'est-à-dire que $0 \in A_{2,p}$. *Si maintenant* $q \in A_{2,p}$,

$$\dagger : p + \mathfrak{s}(q) = \mathfrak{s}(p+q) = \mathfrak{s}(q+p) = \mathfrak{s}(q) + p\,.$$

Ceci signifie que $\mathfrak{s}(q) \in A_{2,p}$. *À noter que la dernière égalité de la séquence* † *utilise vraiment I.1.1.2.1 alors que jusqu'ici nous pouvions nous contenter d'utiliser I.1.0.1.PA*$_5$*).*

iii) ***(I.1.1.2.3)***
Il résulte de I.1.1.1.3 et de I.1.0.1.PA$_4$*) que*

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

c'està-dire que $0 \in A_{3,p}$.
Pour $q \in A_{3,p}$.

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

en utilisant I.1.1.3.3. Cette dernière quantité vaut, puisque $q \in A_{3,p}$, $p*q + q + (p+1)$ *et encore grâce à I.1.1.3.1* $p*q + q + p + 1$ *qui vaut encore grâce à I.1.1.2.2,* $p*q + p + q + 1$ *qui vaut encore graçe à I.1.1.3.3*

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

ce qui prouve que $q + 1 \in A_{3,p}$.

iv) ***(I.1.1.2.4)***

Lemme I.1.1.3 *Pour tout* $p \in \mathbb{N}$, *tout* $q \in \mathbb{N}$ *et tout* $r \in \mathbb{N}$, *on a les propriétés* $P_i(p,q,r)\,,_{1 \leq i \leq 4}$ *suivantes :*

$$P_1(p,q,r) : p + (q+r) = (p+q) + r \qquad \textit{I.1.1.3.1}$$

$$P_2(p,q,r) : p + r = q + r \Rightarrow p = q \qquad \textit{I.1.1.3.2}$$

$$P_3(p,q,r) : p * (q+r) = p*q + p*r \qquad \textit{I.1.1.3.3}$$

$$P_4(p,q,r) : p * (q*r) = (p*q) * r \qquad \textit{I.1.1.3.4}$$

Preuve : *Pour* $1 \leq i \leq 4$ *on introduit une famille d'ensemble* $\left(A_{i,p,q}\right)_{,p\in\mathbb{N},q\in\mathbb{N}}$ *définie par*

$$A_{i,p,q} := \{r \in \mathbb{N} ; P_i(p,q,r)\} .$$

Il suffit alors de montrer, que pour tout $1 \leq i \leq 4$ *tout* $p \in \mathbb{N}$ *et tout* $q \in \mathbb{N}$, $0 \in A_{i,p,q}$, *et* $r \in A_{i,p,q} \Rightarrow r+1 \in A_{i,p,q}$, *pour assurer, en vertu de l'axiome de récurrence I.1.0.1.PA*$_3$*), que pour tout* $1 \leq i \leq 4$ *pour tout* $p \in \mathbb{N}$ *et tout* $q \in \mathbb{N}$, $A_{i,p,q} = \mathbb{N}$, *ce qui signifie exactement que pour tout* $1 \leq i \leq 4$ *tout* $p \in \mathbb{N}$, *tout* $q \in \mathbb{N}$ *et tout* $r \in \mathbb{N}$, $P_i(p,q,r)$ *est satisfaite et prouve finalement le lemme.*

i) ***(I.1.1.3.1)***

Pour tout $p \in \mathbb{N}$, *tout* $q \in \mathbb{N}$, *en utilisant I.1.0.1.PA*$_4$*) on a :*

$$(p+q) + 0 = p + q = p + (q+0)$$

c'est-à-dire que $0 \in A_{1,p,q}$.

Pour $r \in A_{1,p,q}$, *en vertu de I.1.0.1.PA*$_5$*),*

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

Le membre de droite de l'égalité ci-dessus vaut encore, puisque $r \in A_{1,p,q}$, $\mathfrak{s}(p+(q+r))$ *qui vaut en appliquant deux fois I.1.0.1.PA*$_5$*),*

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

c'est-à-dire que $\mathfrak{s}(r) \in A_{1,p,q}$.

ii) ***(I.1.1.3.2)***

La propriété I.1.1.1.1 (À noter que I.1.0.1.PA$_4$*) est même suffisant ici,) assure que* $0 \in A_{2,p,q}$. *Pour* $r \in A_{2,p,q}$, $p+\mathfrak{s}(r) = q+\mathfrak{s}(r)$ *équivaut, d'après I.1.0.1.PA*$_5$*) à* $\mathfrak{s}(p+r) = \mathfrak{s}(q+r)$ *qui entraîne, en vertu de I.1.0.1.PA*$_2$*) que* $p+r = q+r$ *ce qui entraîne finalement, puisque* $r \in A_{2,p,q}$, $p = q$, *prouvant par là-même que* $r+1 \in A_{2,p,q}$.

iii) ***(I.1.1.3.3)***

Pour tout couple (p,q) *d'entiers naturels, comme* $q+0 = q$ *(cf. I.1.0.1.PA*$_4$*),) et* $p*0 = 0$ *(cf. I.1.0.1.PA*$_6$*),)*

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

c'est-à-dire que $0 \in A3, p, q$.

Si $r \in A_{3,p,q}$, *par I.1.1.3.1,*

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

qui vaut, par l'axiome I.1.0.1.PA$_7$*)* $p * (q+r) + p$ *qui vaut encore, puisque* $r \in A_{3,p,q}$, $(p*q+p*r) + p$ *qui vaut encore, graçe à I.1.1.3.1* $p*q+(p*r+p)$ *qui vaut encore, en vertu de I.1.0.1.PA*$_7$*),* $p*q + p*(r+1)$ *Ce qui prouve que* $r+1 \in A_{3,p,q}$.

iv) ***(I.1.1.3.4)***
En utilisant successivement I.1.0.1.PA$_6$), on a :

$$p * (q * 0) \;=\; p * 0 \;=\; 0 \;=\; (p * q) * 0$$

C'est-à-dire que $0 \in A_{4,p,q}$. *Si* $r \in A_{4,p,q}$, *en vertu de I.1.1.3.3,*

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

qui vaut encore puisque $r \in A_{4,p,q}$, $(p * q) \;*\; r \;+\; p * q$ *qui vaut encore, en vertu de I.1.1.3.3* $(p * q) \;*\; (r+1)$ *prouvant, par là-même, que* $r + 1 \in A_{4,p,q}$.

Proposition I.1.1.4 (Propriétés de la loi $+$) *La loi* $+$ *sur* $\mathbb{N}$ *a les propriétés suivantes :*

i) Elle est associative (cf. 0.5.3 ;)

ii) 0 *est un élément neutre (cf. 0.5.5.i) ;)*

iii) elle est commutative (cf. 0.5.4 ;)

iv) tout élément est régulier c'est-à-dire que

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

v) On a :

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

Preuve *:*

i) (cf. I.1.1.3.1.)

ii) (cf. I.1.1.1.1.)

iii) (cf. I.1.1.2.2.)

iv) (cf. I.1.1.3.2 et I.1.1.2.2.)

v) 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* p' *c'est-à-dire qu'il existe un entier naturel* p' *tel que* $p = \mathfrak{s}(p')$ *(cf. I.1.0.1.PA$_1$).) Il en résulte que* $\mathfrak{s}(p') \;+\; q \;=\; 0$ *c'est-à-dire, d'après I.1.1.2.1, que* $\mathfrak{s}(p'+q) \;=\; 0$ *ce qui contredit l'axiome I.1.0.1.PA$_1$).*

Proposition I.1.1.5 (Propriétés de la loi $*$) *La loi $*$ sur $\mathbb{N}$ possède les propriétés suivantes :*

i) *elle est associative ;*

ii) 1 *est un élément neutre pour* $*$;

iii) *elle est commutative ;*

iv) *elle est distributive sur* $+$ *i.e.*

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ \Big(\big(p * (q+r) \ = \ p*q + p*r\big) \wedge \big((p+q) * r \ = \ p*r + q*r\big)\Big) ;$$

v) 0 *est absorbant i.e.*

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

vi) *on a :*

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

Preuve *:*

i) *(cf. I.1.1.3.4.)*

ii) *(cf. I.1.1.1.2.)*

iii) *(cf. I.1.1.2.4.)*

iv) *(cf. I.1.1.3.3 et I.1.1.2.4.)*

v) *(cf. I.1.1.1.3.)*

vi) *Le sens réciproque découle du fait que* 0 *est un élément absorbant (cf. v).)*
Dans le sens direct, si $p * q \ = \ 0$, *supposons que* $p \neq 0$. *D'après I.1.0.1.PA*$_1$*), il existe un entier naturel* p' *tel que* $p = p' + 1$. *On a alors* $(p'+1) * q \ = \ p' * q + q \ = \ 0$. *Ceci implique, en vertu de I.1.1.4.v), que* $p' * q$ *et* q *sont nuls donc en particulier que* q *est nul.*

I.1.2 . −La relation $\leq$

On définit maintnant une relation d'ordre sur $\mathbb{N}$ (cf. 0.2.2.vi),) dont on va montrer qu'elle satisfait de « bonnes propriétés » relativement à l'addition $+$ et la multiplication $*$.

Définition I.1.2.1 ($\leq$) On définit la relation $\leq$ sur $\mathbb{N}$, par la formule :

$$\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \big(p \ \leq\ q \ \Leftrightarrow\ \exists r \in \mathbb{N},\ (q \ =\ p + r)\big)\ . \qquad \text{I.1.2.1.1}$$

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

Proposition I.1.2.2 ($\leq$) *La relation $\leq$ définie ci-dessus est une relation d'ordre sur $\mathbb{N}$ (cf. 0.2.2.vi).)*

Preuve *:*

*i) (**Réflexivité**)*
Comme, $\forall p \in \mathbb{N},\ p + 0 \ =\ p$ (cf. I.1.1.4.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. I.1.1.4.iv),) que $u + v = 0$. Il découle alors du point I.1.1.4.v) 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 I.1.2.3 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 I.1.2.4 On notera $\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ :$

$$\begin{array}{rcl} [p;q] & := & \{r \in \mathbb{N}\,;\ p \leq r \leq q\} \\ [p;q[& := & \{r \in \mathbb{N}\,;\ p \leq r < q\} \\ ]p;q] & := & \{r \in \mathbb{N}\,;\ p < r \leq q\} \\ ]p;q[& := & \{r \in \mathbb{N}\,;\ p < r < q\} \\ [p;+\infty[& := & \{r \in \mathbb{N}\,;\ p \leq r\} \\ ]p;+\infty[& := & \{r \in \mathbb{N}\,;\ p < r\}\,. \end{array} \qquad \text{I.1.2.4.1}$$

Proposition I.1.2.5 (Ordre total) *La relation $\leq$ est une relation d'ordre totale sur $\mathbb{N}$ (cf. 0.2.2.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 I.1.2.4, à :*

$$\forall p \in \mathbb{N},\ \big(\mathbb{N} = [0;p] \cup [p;+\infty[\big)\,. \qquad \textit{I.1.2.5.1}$$

On va démontrer que pour tout $p \in \mathbb{N}$, l'ensemble $[0;p] \cup [p;+\infty[$ satisfait l'axiome de récurrence I.1.0.1.PA$_3$) et est donc égal à $\mathbb{N}$ ce qui établit I.1.2.5.1 :

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. I.1.0.1.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 I.1.2.6 *i) Pour tout triplet d'entiers naturels (p,q,r) $q \leq r$ implique $p*q \leq p*r$ la réciproque étant vraie si $p \neq 0$.*

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

Preuve *:*

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

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

Ceci entraîne

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

ce qui entraîne

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

*b) (**Réciproque**)*
Commençons par établir que :

$$\forall p \in \mathbb{N},\; \forall q \in \mathbb{N},\; \forall r \in \mathbb{N},\; \big(q \;\neq r \;\wedge\; p \;\neq\; 0 \;\Rightarrow p * q \;\neq\; p * r\big)\;. \qquad 1$$

En effet,

$$q \;\neq\; r \;\Rightarrow\; q > r \;\vee r > q$$

puisque la relation d'ordre $\leq$ *est totale (cf. I.1.2.5.) Il s'ensuit que*

$$q \;\neq r \;\Rightarrow\; \exists s \in \mathbb{N},\; \big(s \neq\; 0 \;\wedge\; (r \;=\; q + s \;\vee\; q \;=\; r + s)\big)\;.$$

Or

$$\forall p \in \mathbb{N},\; p * q \;=\; p * r \;\Rightarrow\; p * s \;=\; 0$$

en utilisant I.1.1.4.iv). En utilisant ensuite I.1.1.5.vi), il en découle que $p \;=\; 0$ *ce qui prouve 1.*

On utilise désormais le résultat précédent pour montrer :

$$\forall p \in \mathbb{N},\; \forall q \in \mathbb{N},\; \forall r \in \mathbb{N},\; \big((p \;\neq\; 0 \;\wedge p * q \;\leq\; p * r) \;\Rightarrow\; q \;\leq\; r\big)\;. \qquad 2$$

En effet :

$$\begin{aligned} \not(q \;\leq\; r) \;&\Leftrightarrow\; r < q \\ &\Leftrightarrow\; r \leq q \;\wedge\; r \;\neq\; q \\ &\Rightarrow\; p * r \leq p * q \;\wedge\; p * r \;\neq\; p * q \end{aligned}$$

en utilisant à la fois le sens direct i) et 1 ; ce qui achève de prouver 2 par contraposée.

ii) Pour tout $p, q \in \mathbb{N}$, $p * q = 1$, *entraîne par I.1.1.5.vi) que*

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

Il s'ensuit en particulier que $1 \leq q$, *ce qui entraîne, en vertu de i)*

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

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

$$p = q = 1 .$$

Proposition I.1.2.7 (Plus petit élément) *Toute partie non vide de* $\mathbb{N}$ *possède un plus petit élément*
(cf. 0.2.2.vii).)

Preuve *:*

i) Pour tout $p \in \mathbb{N}$, $p = 0 + p$ *(cf. I.1.1.4.ii),) c'est-à-dire que* $0 \leq p$. 0 *est donc un plus petit élément pour* $\mathbb{N}$ *lui-même.*

ii) On en déduit 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.

iii) 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* P *contient* 0 *d'après ce qui précède,* P *contient un plus petit élément. Si* P *ne contient pas* 0, *alors pour tout* $q \in P$, *il existe un unique (cf. I.1.0.1.PA*$_1$*)) et (cf. I.1.0.1.PA*$_2$*)) q'* $\in \mathbb{N}$ *tel que* $q = \mathfrak{s}(q')$ *c'est-à-dire que* P *est l'image par* $\mathfrak{s}$ *d'une partie* P' *de* $\mathbb{N}$ *laquelle contient* p. *Par conséquent,* P' *admet un plus petit élément* p'_0. *Pour tout* $q \in P$, *il existe un unique* q' *tel que* $q = \mathfrak{s}(q')$ *avec* $q' \in P'$ *et par conséquent, il existe* $r' \in \mathbb{N}$, *tel que* $q' = p'_0 + r'$. *Ceci implique que* $q = p'_0 + r + 1 = p'_0 + 1 + r'$ *autrement dit que* $p'_0 + 1$ *est un plus petit élément pour* P.

iv) 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 I.1.2.8 (Plus grand élément) *Une partie non vide P de $\mathbb{N}$ est majorée (cf. 0.2.2.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 I.1.2.7 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

$$\forall p \in P, \ , \ p < m \, . \qquad \text{I.1.2.8.1}$$

Il s'ensuit alors que

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

Donc

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

Il existe donc (cf. I.1.0.1.PA$_1$),) $n \in \mathbb{N}$ tel que $m = n+1$. I.1.2.8.1 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.

I.1.3 . −Ensembles finis

Définition I.1.3.1 (Ensemble fini) On dira qu'un ensemble A est *fini* s'il existe $p \in \mathbb{N}$ et une application injective $i \ : \ A \ \to \ [1; p]$.

Lemme I.1.3.2 *Si A est un ensemble fini*

$$\#(A) \ := \ \min \left(\{ p \in \mathbb{N}, \ ; \ \exists i \ : \ A \ \to \ [1; p] \ \textit{injective} \} \right)$$

est l'unique entier n tel qu'il existe une bijection $A \ \cong \ [1; n]$.

Preuve *:*

*i) (**Existence**)*

L'existence de $\#(A)$ est assurée, pour un ensemble fini, par la proposition I.1.2.7. De plus, il existe une application injective $i \ : \ A \ \to \ [1; \#(A)]$. Si $\#(A) = 0$ $[1; \#(A)] = \emptyset$ ce qui entraîne $A = \emptyset$ et prouve le résultat.

Si $\#(A) \neq 0, [1;\#(A)] \neq \emptyset$ et si i n'est pas surjective, il existe $x \in [1;\#(A)]$ qui n'a pas d'antécédent dans A. Il s'ensuit que $\operatorname{Im} i \subset [1;\#(A)] \setminus \{x\}$ et que $i : A \to [1;\#(A)] \setminus \{x\}$ est encore injective.

Considérons l'application :

$$\begin{array}{rccl} (x\#(A)) : & [1;\#(A)] & \to & [1;\#(A)] \\ & x & \mapsto & \#(A) \\ & \#(A) & \mapsto & x \\ & p & \mapsto & p,\ \forall p \neq x,\ p \neq \#(A) \end{array}$$

qui est une bijection. Il s'ensuit que

$$(x\#(A)) \circ i : A \to [1;\#(A)-1]$$

est encore injective ce qui contredit la minimalité de $\#(A)$. L'application i est donc surjective et par conséquent est une bijection. On a donc établi l'existence d'une bijection de A sur un ensemble de la forme $[1;p]$.

*ii) (**Unicité**)*

Supposons données deux bijections

$$\phi : A \cong [1;p] \text{ et } \psi : A \cong [1;q] .$$

Alors

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

sont des bijections ce qui entraîne en vertu du TD n° I, exercice D, exercice C, question 2) $p = q$ ce qui prouve l'unicité.

Exemple I.1.3.3 (Ensembles finis) [Ensembles finis]

a) L'ensemble $\emptyset$ est un ensemble fini.

b) Si

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

sont des parties finies d'un ensemble E alors

$$A \cup B \text{ et } A \cap B$$

sont finis. Toute partie de A est finie.

Si A et B sont des ensembles finis, $A \times B$ est fini.

c) Pour p et q des entiers naturels, les ensembles

$$[p;q],\ [p;q[,\ ]p;q]\ \text{et}\ ]p;q[$$

sont des ensembles finis.

d) En revanche $\mathbb{N}$ n'est pas fini (cf. TD n° I, exercice D, exercice C, question 3)) ce qui motive la définition suivante :

Définition I.1.3.4 (Ensemble dénombrable) On dit qu'un ensemble A est *dénombrable* s'il existe une bijection $A \cong \mathbb{N}$.

Exemple I.1.3.5 (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 I.1.3.6 (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 $[0;m] \cong P$.

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

Proposition I.1.3.7 *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 :

$$\begin{array}{rrcl} & P_0 & := & P \\ & Q_0 & := & \emptyset \\ \forall n \in \mathbb{N} & P_{n+1} & := & P_n \setminus \{\min(P_n)\} \text{ si } P_n \neq \emptyset \\ & & := & \emptyset \text{ sinon} \\ \forall n \in \mathbb{N} & Q_{n+1} & := & Q_n \cup \{\min(P_n)\} \text{ si } P_n \neq \emptyset \\ & & := & Q_n \text{ sinon } . \end{array} \qquad \text{I.1.3.7.1}$$

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

$$\forall P \subset \mathbb{N}\ ,\ \forall n \in \mathbb{N},\ P\ =\ P_n \cup Q_n \text{ et } Q_n \text{ est finie } . \qquad \text{I.1.3.7.2}$$

Il s'ensuit que si P n'est pas finie, pour tout n P_n n'est pas finie (cf. I.1.3.3.b)) 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.

I.2 . −L'ensemble $\mathbb{Z}$ des entiers relatifs

I.2.0 . −Introduction

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. I.1.2.5.) 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. I.2.2.)

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. 0.2.2.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. I.2.2.7.ii) :)

Notation I.2.0.1 On note :

$$Z \ := \ \mathbb{N} \times \mathbb{N} \qquad \text{I.2.0.1.1}$$

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. 0.2.1.iii) :) $\sim$ définie par :

$$\forall (p,q) \in Z, \ \ \forall (r,s) \in Z, \ \ (p,q) \ \sim \ (r,s) \ \Leftrightarrow \ p+s \ = \ q+r \ . \qquad \text{I.2.0.1.2}$$

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 I.2.0.2 *La relation $\sim$ est une relation d'équivalence (cf. 0.2.2.v).) Pour tout*

$$(p,q) \in Z \text{ on notera } \overline{(p,q)} \ := \ \big\{ (r,s) \ \in \ Z \ ; \ (r,s) \ \sim \ (p,q) \big\}$$

la classe du couple (p,q).

Preuve *: . Cette démonstration très formelle et très facile est laissée en exercice.*

I.2.1 . –Entiers relatifs

Définition I.2.1.1 (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 I.2.1.2 On notera :

$$\begin{array}{rccc} \pi : & Z & \to & \mathbb{Z} \ = \ Z/\sim \\ & (p,q) & \mapsto & \overline{(p,q)} \end{array} \qquad \text{I.2.1.2.1}$$

la *surjection canonique* (cf. TD n° II, exercice A, question 2).)

Proposition I.2.1.3 *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. I.1.2.5) 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'existence

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. I.2.0.1.2)* $r+0 \;=\; r'+0$ *c'est-à-dire* $r \;=\; r'$ *ce qui assure l'unicité.*

Proposition I.2.1.4 *Les applications*

$$\begin{array}{rccc} i_+ : & \mathbb{N} & \longrightarrow & \mathbb{Z} \\ & p & \longmapsto & \overline{(p,0)} \end{array} \qquad \textit{I.2.1.4.1}$$

et

$$\begin{array}{rccc} i_- : & \mathbb{N} & \longrightarrow & \mathbb{Z} \\ & p & \longmapsto & \overline{(0,p)} \end{array} \qquad \textit{I.2.1.4.2}$$

sont injectives. (cf. 0.2.5.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 I.2.1.3 implique que $r = r'$*.*

La vérification pour i_- *est tout à fait identique.*

Corollaire I.2.1.5 *Les propositions I.2.1.3 et I.2.1.4 ont pour conséquence que :*

i) $i_+(\mathbb{N})$ *est une partie de* $\mathbb{Z}$ *en bijection (cf. 0.2.5.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 I.2.1.6 (Entiers positifs/négatifs) On appellera $\mathbb{Z}^+$ l'ensemble des *entiers relatifs positifs* et $\mathbb{Z}^-$ l'ensemble des *entiers relatifs négatifs*.

I.2.2 . −L'anneau $(\mathbb{Z}, +, *)$

Dans ce paragraphe (I.2.2) l'ensemble noté Z est celui introduit en I.2.0.1.1.

Notation I.2.2.1 On définit une loi de composition $+_Z$ sur Z par :

$$\forall (p,q) \in Z\ ,\ \forall (r,s) \in Z\ ,\ (p,q)\ +_Z\ (r,s)\ :=\ (p +_{\mathbb{N}} r, q +_{\mathbb{N}} s) \qquad \text{I.2.2.1.1}$$

cette écriture ayant un sens puisque l'addition sur $\mathbb{N}$ est bien définie (cf. I.1.1.4.)

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 I.2.2.7.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 :

$$\forall (p,q) \in Z\ ,\ \forall (r,s) \in Z\ ,\ (p,q)\ *_Z\ (r,s)\ :=\ (p*r+q*s, p*s+q*r) \qquad \text{I.2.2.1.2}$$

en utilisant les opérations $+$ et $*$ de $\mathbb{N}$ qui sont bien définies.

Lemme I.2.2.2 *Les lois $+_Z$ et $*_Z$ définie ci-dessus sur Z sont compatibles à la relation d'équivalence $\sim$ définie en I.2.0.1.2 au sens où*

$$\begin{array}{l} \forall x \in Z,\ \forall y \in Z,\ \forall x' \in Z, \\ \forall y' \in Z,\ \big(\qquad\qquad x \sim x'\ \wedge\ y \sim y'\ \ \Rightarrow\ \ x +_Z y \sim x' +_Z y' \text{ et } x *_Z y \sim x' *_Z y' \big)\ . \end{array}$$

Preuve *:*

i) $(+)$
On a, par définition (cf. I.2.2.1.1,)

$$(p,q) +_Z (r,s) \;=\; (p+r, q+s) \text{ et } (p',q') +_Z (r',s') \;=\; (p'+r', q'+s') \,.$$

Par ailleurs (cf. I.2.0.1.2,) $p + q' \;=\; p' + q$ *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*

$$\begin{aligned} p*r + q*s + p'*s + q'*r \;&=\; (p+q')*r + (q+p')*s \\ &=\; (p'+q)*r + (p+q')*s \\ &=\; p'*r + q's + p*s + q*r \,; \end{aligned}$$

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 I.2.2.3 *Il existe un unique couple de lois* $(+,*)$ *sur* $\mathbb{Z}$ *tel que la surjection canonique* π *définie en I.2.1.2.1 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 I.2.2.2, le résultat découle du TD n° II, exercice A, question 3), a).*

Proposition I.2.2.4 (Le groupe $(\mathbb{Z},+)$) *Le couple $(\mathbb{Z},+)$ est un groupe abélien (cf. 0.5.6.i).)*

Preuve *:*

*i) (**Associativité**)*
Il faut vérifier que la loi $+$ est associative, mais en vertu du TD n° II, exercice A, question 3), b), 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. I.1.1.4.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 TD n° II, exercice A, question 3), b), 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. I.1.1.4.iii).) On conclut ensuite à la commutativité de $(\mathbb{Z},+)$ une fois encore graçe au TD n° II, exercice A, question 3), b).

Les propriétés établies ci-dessus font de $(\mathbb{Z},+)$ un groupe abélien.

Remarque I.2.2.4.5 (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 I.2.2.4 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 I.2.2.5 (L'anneau $(\mathbb{Z}, +, *)$) *Le triplet $(\mathbb{Z}, +, *)$ est un anneau commutatif (cf. 0.5.9.i).)*

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 TD n° II, exercice A, question 3), b) pour 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 I.2.2.6 *Pour tout couple (p,q) d'entiers naturels,*

$$\begin{aligned}
i_+(p+q) &= i_+(p) + i_+(q) \quad , \quad i_-(p+q) = i_-(p) + i_-(q), \\
i_+(p*q) &= i_+(p) * i_+(q) \quad \text{et} \quad i_-(p*q) = i_-(p) * i_+(q) = i_+(p) * i_-(q)\ .
\end{aligned}$$

Remarque I.2.2.6.1 On dit que i_+ est un *morphisme* (cf. 0.5.2,) pour les lois $+$ et $*$.
C'est également le cas pour i_- vis-à-vis de $+$ mais pas tout à fait pour $*$.

Preuve *: Ce son des calculs faciles laissés en exercice.*

Notation I.2.2.7 i) (**Opposé**)

On sait (cf. I.2.1.5.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. I.2.1.5.i),) de noter simplement p la classe $\overline{(p,0)}$. Nous venons de plus de constater (cf. I.2.2.4) 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 I.2.2.8 (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. I.2.1.5.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. TD n° II, exercice B, question 1), b).)*

Proposition I.2.2.9 (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 (cf. 0.5.9.ii).)*

Preuve *: On laisse le soin au lecteur de déduire cet énoncé de la proposition I.1.1.5.vi).*

Corollaire I.2.2.10 *Pour tout triplet (p,q,r) d'entiers relatifs, $p*r=q*r$ si et seulement si $r=0$ ou $p=q$.*

Proposition I.2.2.11 *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. I.2.1.6,) on a $(p,q)=(1,1)$ d'après la proposition I.1.2.6.ii).

ii) Si p et q sont négatifs, $-p$ et $-q$ sont positifs (cf. I.2.2.8.ii).) De plus, $p*q=(-p)*(-q)$ (cf. I.2.2.6.)

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 I.2.2.6 et I.2.2.8.ii). Cette situation n'est donc pas possible puisque $1=\overline{(1,0)}\in\mathbb{Z}^+$.

Définition I.2.2.12 (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 $\mathbb{Z}$.

I.2.3 . $-$Ordre sur $\mathbb{Z}$

On définit maintnant une relation d'ordre sur $\mathbb{Z}$ (cf. 0.2.2.vi),) dont on va montrer qu'elle satisfait de « bonnes propriétés » relativement à l'addition $+$, la multiplication $*$ et les injection i_+ et i_-.

Définition I.2.3.1 ($\leq$) On définit la relation $\leq$ sur $\mathbb{Z}$, par la formule :

$$\forall p\in\mathbb{Z},\ \forall q\in\mathbb{Z},\ \big(p\leq q\ \Leftrightarrow\ \exists r\in\mathbb{N},\ (q=p+r)\big)\,. \qquad \text{I.2.3.1.1}$$

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

Proposition I.2.3.2 (Ordre) *La relation $\leq$ définie ci-dessus est une relation d'ordre totale sur $\mathbb{Z}$ (cf. 0.2.2.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. I.1.2.2.)*

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. I.2.2.8.ii)) à $q - p \in \mathbb{Z}^-$. On a donc

$$q - p \in \mathbb{Z}^+ \cap \mathbb{Z}^-$$

ce qui implique (cf. I.2.1.5.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 I.2.1.5.ii).

Remarque I.2.3.3 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. I.1.2.3.)

Proposition I.2.3.4 *Pour tout couple d'entiers <u>naturels</u> (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. I.2.1.4.1) 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. 0.2.8.)*

On pourrait encore dire que la relation d'ordre sur $\mathbb{Z}$ « prolonge » la relation d'ordre sur $\mathbb{N}$.

Proposition I.2.3.5 (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 I.2.3.6 On laisse le soin au lecteur d'établir toutes les variantes usuelles de l'énoncé ci-dessus.

Proposition I.2.3.7 *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. I.1.2.8.) 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 I.2.2.8.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 I.1.2.7. Reste à vérifier, ce qui est élémentaire, que $-\ell$ est un plus grand élément pour P.

Proposition I.2.3.8 (Parties finies) *i) Une partie de $\mathbb{Z}$ est soit finie (cf. I.1.3.1,) soit dénombrable (cf. I.1.3.4.)*

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 I.2.3.9 (Valeur absolue) La proposition I.2.2.8.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 I.2.3.10 (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)

$$\forall p \in \mathbb{Z},\ \forall q \in \mathbb{Z},\ ||p|-|q|| \ \leq \ |p+q| \ \leq \ |p| \ + \ |q|\ .$$

I.3 . −Théorème de BÉZOUT et propriétés arithmétiques de $\mathbb{Z}$

I.3.0 . −Introduction

Le théorème principal de ce paragraphe est bien évidemment le théorème I.3.3.3 et son corollaire I.3.3.3. À l'origine de ces résultats se ttrouve bien entendu le théorème de la division euclidienne I.3.2.3. Les autres résultats du paragraphe et notamment le théorème I.3.6.1 et ses corollaires sont des conséquences (voire parfois de simples reformulations) du théorème I.3.3.3.

I.3.1 . −Divisibilité dans un anneau intègre

Soit $(A,+,*)$ un anneau intègre (cf. 0.5.9.ii).) L'anneau $(\mathbb{Z},+*)$ en est un bon exemple. On notera $A^\times$ l'ensemble des éléments inversibles de A (cf. 0.5.9.iii)) et on rappelle que le couple $(A^\times,*)$ est un groupe, (resp. un groupe abélien si A est commutatif) (cf. 0.5.10.)

Définition I.3.1.1 (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 $a * c = b$.

Définition I.3.1.2 (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 I.3.1.3 *La relation d'association est une relation déquivalence.*

Proposition I.3.1.4 (Propriétés de la relation de divisibilité) *La relation de divisibilité $\cdot|\cdot$ satisfait aux propriétés suivantes :*

*i) (**Réflexivité**)*
Elle est réflexive (cf. 0.2.2.i).)

*ii) (**Transitivité**)*
Elle est transitive (cf. 0.2.2.iv).)

iii)

$$\forall x \in A,\ \forall y \in A,\ \big(x|y \text{ et } y|x \ \Rightarrow \exists u \ \in \ A^\times,\ y \ = \ ux\big)$$

autrement dit x et y sont associés.

iv)

$$\forall x \in A,\ \forall y \in A,\ \forall z \in A,\ \big(x|y \text{ et } x|z \ \Rightarrow \ x|y+z\big)\ .$$

Remarque I.3.1.5 Le fait que la relation $|$ ne soit pas « vraiment » *antisymétrique* (cf. 0.2.2.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 $5|3$.

Lemme I.3.1.6 *L'élément neutre pour $+$ 0 est le plus grand élément pour $|$ tandis que tout élément $u \ \in \ A^\times$ est un plus petit élément pour $|$.*

Remarque I.3.1.6.1 On constate d'ores et déjà que $|$ ne se comporte pas tout à fait comme une relation d'ordre puisqu'il n'y a pas unicité d'un plus petit élément.

Notation I.3.1.7 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

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

Définition I.3.1.8 (Pgcd Ppcm) Étant donné un ensemble $X \ \subset \ A$, on appelle *plus grand commun diviseur* ou ***Pgcd*** (resp. *plus petit commun multiple* ou ***Ppcm***)

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

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

$$\forall a \in X,\ d|a \text{ et } \forall b \in \mathcal{D}(X),\ b|d \text{ (resp. } \forall a \in X,\ a|m \text{ et } \forall b \in \mathcal{M}(X),\ m|b\ .) \qquad \text{I.3.1.8.1}$$

Remarque I.3.1.8.2 La définition I.3.1.8 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. 0.2.2.vii).) Nous verrons en outre que la relation $\cdot|\cdot$ n'est pas « vraiment » une relation d'ordre (cf. I.3.1.5,) 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 I.3.1.9 *Pour tout $X \subset A$, d **Pgcd** de X (resp m **Ppcm** de X,) d' est un **Pgcd** de X (resp. m' est un **Ppcm** de X,) si et seulement si d et d' (resp. m et m') sont associés.*

Remarque I.3.1.10 On n'a pas parlé jusqu'ici du **Pgcd** ni du **Ppcm** mais d'un **Pgcd** ou d'un **Ppcm** à cause du défaut d'unicité constaté dans le lemme ci-dessus. Ce dernier énoncé montre en outre que de toute évidence, le « bon objet » à considérer n'est pas un **Pgcd** ou un **Ppcm** mais la classe d'association des **Pgcd** (resp **Ppcm**) qui, pour le coup, et d'après le lemme I.3.1.9 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 .

Pour $x \in A$, soit en effet

$$xA := \mathcal{M}(x) := \mathcal{M}(\{x\})$$

l'ensemble des multiples de x. On remarque que :

$$xA \neq \emptyset\,,\ \forall (y,z) \in xA \times xA,\ \forall (a,b) \in A \times A,\ ax+by \in xA\,. \qquad \text{I.3.1.10.1}$$

Un sous-ensemble de A possédant les propriétés I.3.1.10.1 s'appelle un *idéal* de A et l'on a le résultat suivant :

Lemme I.3.1.11 *Pour tous x et y dans A $yA \subset xA$ si et seulement si $x|y$ en particulier x et y sont associés si et seulement si $xA = yA$.*

Notation I.3.1.12 Pour $X \subset A$ d (resp. m) un **Pgcd** (resp. **Ppcm**) de X, on notera :

$$\bigwedge X := dA \text{ et } \mathrm{PPCM}(X) := mA\,. \qquad \text{I.3.1.12.1}$$

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

$$x \wedge y := \bigwedge \{x,y\} \text{ et } \mathrm{PPCM}(x,y) = \mathrm{PPCM}(\{x,y\})\,. \qquad \text{I.3.1.12.2}$$

Exercice I.3.1.13 Soit $X \subset A$, non vide.

1) () Montrer que

$$I(X) := \Big\{\sum_{i=1}^{n} a_i x_i, n \in \mathbb{N}, a_i\,,_{1\leq i\leq n} \in A\,,\ x_i\,,_{1\leq i\leq n} \in X\Big\}$$

est un idéal de A et que si d est un **Pgcd** de X $I(X) = dA$.

2) () Montrrer que

$$J(X) := \bigcap_{x\in X} xA$$

est un idéal de A et que si m est un **Ppcm** de X, $J(X) = mA$.

3) () Montrer que 0 est un **Pgcd** (resp. un **Ppcm**) de X si et seulement si

$$\forall x \in X,\ x = 0 \,(\text{resp. } \exists x \in X,\ x = 0)\,.$$

4) () **Soient X et Y deux parties non vides de A possédant chacune un Pgcd (resp. un Ppcm).**

Montrer que

$$\bigwedge(X\cup Y) = (\bigwedge X)\wedge(\bigwedge Y)\ \big(\text{resp. } \mathrm{PPCM}(X\cup Y) = \mathrm{PPCM}(\mathrm{PPCM}(X),\mathrm{PPCM}(Y))\big)\,.$$

Définition I.3.1.14 (Éléments irréductibles) Un élément $x \in A$ de A est dit *irréductible* si

$$\forall y \in A,\ \forall z \in A,\ \big(y * z = x \Rightarrow y \in A^\times \vee z \in A^\times\big)\,.$$

Définition I.3.1.15 (Élément premier) Un élément $x \in A$ de A est dit *premier* si

$$\forall y \in A,\ \forall z \in A,\ \big(x|y * z \Rightarrow x|y \vee x|z\big)\,;$$

Lemme I.3.1.16 *Dans un anneau intègre, tout élément premier non nul est irréductible.*

I.3.2 . −Le théorème de la division euclidienne dans $\mathbb{Z}$

On établit dans ce paragraphe (I.3.2) le *théorème de la division euclidienne* I.3.2.3 qui est à l'origine des résultats principaux des paragraphes I.3.3 et I.3.6 et en particulier :

i) le théorème de BÉZOUT (cf. I.3.3.3 ;)

ii) le lemme de GAUSS (cf. I.3.3.8 ;)

iii) le lemme d'Euclide (cf. I.3.3.10 ;)

iv) la décomposition en produit de facteurs premiers (cf. I.3.3.17 ;)

v) le théorème chinois des restes (cf. I.3.6.1.)

Le théorème I.3.2.3 résulte lui-même de la proposition I.3.2.1. Ce dernier résultat se transpose par exemple au cas des anneaux de polynômes sur un corps, en remplaçant la valeur absolue par le degré. Si bien qu'on obtient une arithmétique dans les anneaux de polynômes tout à fait analogue à celle de $\mathbb{Z}$.

Cependant les résultats i) à v) sont en réalité des conséquences du corollaire I.3.2.6 et vaudrait dans n'importe quel anneau dans lequel on aurait un résultat analogue concernant la structure des idéaux : à savoir que tout idéal est de la forme xA, on dit *principal*. De tels anneaux sont dit *principaux* et dans les anneaux principaux on a les énoncés i) à v).

Proposition I.3.2.1 (Compatibilité à $\leq$)

$$\forall p \in \mathbb{Z},\ \forall q \in \mathbb{Z},\ \big(p|q \text{ et } q \neq 0 \ \Rightarrow\ |p| \leq |q|\big)\ .$$

Preuve *:*

$$\begin{array}{lr} \forall p \in \mathbb{Z},\ \forall q \in \mathbb{Z}, & p|q \quad \text{et} \quad q \neq 0 \\ \Rightarrow & \exists r \in \mathbb{Z},\ q = p * r \quad \text{et} \quad r \neq 0 \\ \Rightarrow & \exists r \in \mathbb{Z},\ |r| * |p| = |q| \quad \text{et} \quad r \neq 0 \end{array}$$

Or

$$r \neq 0 \ \Rightarrow\ |r| \neq 0 \ \Rightarrow\ 1 \leq |r| \ \Rightarrow\ |p| * 1 \ \leq\ |p| * |r| \ =\ |q|$$

en utilisant la proposition TD n° I, exercice B, question 3), i).

Lemme I.3.2.2 *Deux éléments A et b de $\mathbb{Z}$ sont associés (cf. I.3.1.2,) si et seulement si*

$$a \ =\ b \text{ ou } a \ =\ -b\ .$$

Preuve *: (cf. I.2.2.12.)*

Théorème I.3.2.3 (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 :*

$$a \ =\ b * q \ +\ r \text{ et } 0 \ \leq\ r \ <\ |b|\ . \qquad \textit{I.3.2.3.1}$$

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 I.2.1.5.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 I.2.3.7, 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 I.1.2.7, 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 I.3.2.3.1 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. I.3.1.1.) 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 I.3.2.1 que $r' - r = 0$. Il s'ensuit que $b * (q - q') = 0$ mais comme $b \neq 0$, d'après la proposition I.2.2.9, $q - q' = 0$ ce qui achève de prouver l'unicité du couple (q, r).

Définition I.3.2.4 Pour un couple (a, b) comme dans le théorème I.3.2.3, trouver le couple (q, r) s'appelle faire la *division euclidienne* de a par b.

i) a s'appelle le *dividende*,

ii) b le *diviseur*,

iii) q le *quotient*

iv) et r le *reste*.

Remarque I.3.2.5 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 I.3.2.6 (Sous-groupes de $(\mathbb{Z},+)$) *i) Pour toute partie $H \subset \mathbb{Z}$, H est un sous-groupe (cf. 0.5.6.iv),) si et seulement si H est un idéal de $\mathbb{Z}$ (cf. I.3.1.10.1,)si et seulement si il existe $d \in \mathbb{Z}$ tel que*

$$H = d\mathbb{Z} := \{d * k \,;\, k \in \mathbb{Z}\} .$$

ii)

$$\forall a \in \mathbb{Z},\ \forall b \in \mathbb{Z},\ \big(b\mathbb{Z} \subset a\mathbb{Z} \Leftrightarrow a|b\big) \text{ (cf. I.3.1.11 .)}$$

iii)

$$\forall a \in \mathbb{Z},\ \forall b \in \mathbb{Z},\ \big(a\mathbb{Z} = b\mathbb{Z} \Rightarrow a = b \vee a = -b\big) .$$

Preuve *:*

i) a) On laisse en exercice le soin de montrer que H est un sous-groupe si et seulement si c'est un idéal.

b) Vérifions d'abord que, tout $d \in \mathbb{Z}$, $d\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Pour tout $x, y \in d\mathbb{Z}$, il existe $a, b \in \mathbb{Z}$ tels que $x = da$ et $y = db$. IL s'ensuit que $x+y = da+db = d(a+b) \in d\mathbb{Z}$ ce qui entraîne que $+$ se restreint à $d\mathbb{Z}$ pour donner une loi de composition sur $d\mathbb{Z}$.

Comme $0 = d*0 \in d\mathbb{Z}$ la loi $+$ sur $d\mathbb{Z}$ possède un élément neutre. Enfin si $x = da \in d\mathbb{Z}$, $-x = d*(-a) \in d\mathbb{Z}$ si bien que tout élément de $d\mathbb{Z}$ possède un symétrique pour la loi $+$ ce qui assure que $(d\mathbb{Z},+)$ est bien un groupe.

On pouvait aussi remarquer que l'application

$$\begin{array}{rccc} \mu_d : & \mathbb{Z} & \to & \mathbb{Z} \\ & x & \mapsto & dx \end{array}$$

est un morphisme de groupes (cf. 0.5.6.ii),) dont $d\mathbb{Z}$ n'est autre que l'image et utiliser la question (cf. TD n° II, exercice B, question 2), c).)

c) Soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$, $H = 0\mathbb{Z}$.

Si $H \neq \{0\}$ il existe $x \in H$, $x \neq 0$. Si $x \in \mathbb{Z}^+$, $H \cap \mathbb{N}^* \neq \emptyset$ sinon $x \in H \Rightarrow -x \in H$ puisque H est un groupe. Comme $x \notin \mathbb{Z}^+$, $-x \in \mathbb{Z}^+$ ce qui entraîne encore $H \cap \mathbb{N}^* \neq \emptyset$.

Il s'ensuit que $H \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}$ qui contient donc un plus petit élément $d \in \mathbb{N}^*$ (cf. I.1.2.7.)

Il s'ensuit que $d * 0 \in H$, que pour tout $n \in \mathbb{N}$,

$$d * n \in H \Rightarrow d * (n + 1) = d * n + d \in H$$

puisque H est un groupe. Donc grâce au principe de récurrence I.1.0.1.PA$_3$), $\forall n \in \mathbb{N}$, $d * n \in H$. Puisque H est un groupe, on a aussi $\forall n \in \mathbb{N}$, $-d * n \in H$, si bien que

$$d\mathbb{Z} \subset H .$$

Réciproquement, pour tout $x \in H$, il existe, puisque $d \neq 0$, grâce au théorème I.3.2.3, un couple (n, y) tel que $x = d * n + y$. Or

$$x \in H \wedge d * n \in H \Rightarrow y = x - d * n \in H$$

puisque H est un groupe. Or si n est le quotient et y le reste de la division euclidienne de x par d, $0 \leq y < d$. Il s'ensuit, d étant le plus petit élément de $H \cap \mathbb{N}^*$ que $y = 0$ ce qui entraîne $x = d * n$ et finalement

$$H \subset d\mathbb{Z}$$

puis

$$H = d\mathbb{Z} .$$

ii) Si $b\mathbb{Z} \subset a\mathbb{Z}$, en particulier, $b \in a\mathbb{Z}$ c'est-à-dire qu'il existe $c \in \mathbb{Z}$ tel que

$$b = a * c \Leftrightarrow a|b .$$

Réciproquement si $a|b$ il existe $c \in \mathbb{Z}$, tel que $b = a * c$. Il s'ensuit que

$$\forall x \in b\mathbb{Z} \; \exists \, n \in \mathbb{Z} x = b * n = a * c * n \in a\mathbb{Z}$$

c'est-à-dire

$$b\mathbb{Z} \subset a\mathbb{Z} .$$

iii) Est une conséquence immédiate du point précédent et de I.3.1.4.iii).

Corollaire I.3.2.7 (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*

$$a = \epsilon \sum_{i=0}^{d} r_i b^i \; ; \qquad \text{I.3.2.7.1}$$

$$\forall 0 \leq i \leq d,\ 0 \leq r_i \leq b \; ; \qquad \text{I.3.2.7.2}$$

$$r_d \neq 0 \; . \qquad \text{I.3.2.7.3}$$

Preuve *: (cf. Problème n° I, exercice A.)*

*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. I.2.3.7,) 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 I.3.2.5, 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 I.1.0.1.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 I.3.2.3 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 I.3.2.8 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 $-$.

I.3.3 . −Théorème de BÉZOUT, lemme de GAUSS lemme d'EUCLIDE

Théorème I.3.3.1 (Existence du PGCD) *Pour tout entier naturel non nul* $n \;\in\; \mathbb{N}^*$, *et toute partie*

$$A \;:=\; \{a_1, \ldots, a_n\} \;\subset\; \mathbb{Z}$$

finie à n *éléments :*

*i) (**PGCD**)*
A possède un PGCD.

*ii) (**Identité de BÉZOUT**)*
Si d est un PGCD de A il existe un n-uplet $(u_1, \ldots, u_n)$ tel que :

$$d \;=\; \sum_{i=1}^{n} u_i a_i \;. \qquad 1$$

Preuve *:*

*i) a) (**Le sous-groupe** $G(A)$)*
Soit

$$G(A) \ := \ \{\sum_{i=1}^{n} x_i a_i \ ; \ x_i \in \mathbb{Z} \forall 1 \leq i \leq n, \ \} \ .$$

Alors $G(A)$ *est un sous-groupe de* $\mathbb{Z}$*. En effet,* $0 \ = \ \sum_{i=1}^{n} 0 * a_i \ \in G(A)$ *et*

$$\forall x \ := \ \sum_{i=1}^{n} x_i a_i \ , \ \forall y \ = \ \sum_{i=1}^{n} y_i a_i \ , \ x - y \ = \ \sum_{i=1}^{n} (x_i - y_i) * a_i \ \in \ G(A) \ .$$

En vertu du résultat établi à l' TD n° II, exercice B, question 4), il en résulte que $G(A)$ *est un sous-groupe de* $\mathbb{Z}$*.*
D'après le résultat relatif à la structure des sous-groupes de $\mathbb{Z}$ *(cf. I.3.2.6,) il existe* $d \ \in \ \mathbb{Z}$ *tel que* $G(A) \ = \ d\mathbb{Z}$*.*

b) Reste à montrer que d *est un PGCD pour* A *: Il est clair que*

$$\forall a \in A \ , \ a \in G(A) \ = \ d\mathbb{Z}$$

ce qui signifie exactement que $d|a$ *.*
Réciproquement si $b \ \in \ \mathbb{Z}$ *est tel que* $\forall a \in A \ , \ b|a$*, pour tout* n*-uplet* $(x_1, \ldots, x_n)$*,*

$$b| \sum_{i=1}^{n} x_i a_i$$

dit $G(A) \subset b\mathbb{Z}$ *c'est-à-dire* $d\mathbb{Z} \ \subset \ b\mathbb{Z}$ *c'est-à-dire, d'après I.3.2.6.ii)*

$$b|d \ .$$

ii) Il suffit de remarquer que $G(A) \ = \ d\mathbb{Z}$ *entraîne* $d \in G(A)$ *ce qui prouve le résultat.*

Définition I.3.3.2 (Identité de BÉZOUT) La formule I.3.3.1.ii).1 est appelée *identité de* BÉZOUT et les entiers $u_{i \ , 1 \leq i \leq n}$ *coefficients de* BÉZOUT.

Corollaire I.3.3.3 (Théorème de BÉZOUT) *Pour tout entier naturel* n *et toute partie*

$$A \ := \ \{a_1, \ldots, a_n\} \ \subset \ \mathbb{Z},$$

les assertions suivantes sont équivalentes :

a) $\mathcal{D}(A) \ = \ \{-1, 1\}$.

b) $\bigwedge A \ = \ 1.$

c) Il existe un n*-uplet d'entiers relatifs* $u_{i\ ,1\leq i\leq n}$ *tel que*

$$\sum_{i=1}^{n} a_i u_i \ = \ 1 \ .$$

Preuve *: La preuve est immédiate.*

Définition I.3.3.4 (Entiers premiers entre eux) Pour tout entier naturel n on dira que des entiers relatifs $a_{i\ ,1\leq i\leq n}$ sont *premiers entre eux dans leur ensemble* s'ils vérifient l'une des conditions équivalentes du théorème I.3.3.3.

Pour $n = 2$ on dira simplement que deux entiers relatifs sont *premiers entre eux*.

Il arrivera qu'on ait a considérer un n-uplet d'entiers relatifs $a_{i\ ,1\leq i\leq n}$ *deux à deux premiers entre eux*. Ceci signifie que pour tout $1 \ \leq \ i \ \leq \ n$ et tout $1 \ \leq \ j \ \leq \ n$ les entiers a_i et a_j sont premiers entre eux si $i \neq j$.

Proposition I.3.3.5 (Algorithme d'Euclide) *Étant donnés deux entiers relatifs* a_0 *et* a_1*, l'algorithme d'Euclide consiste en la donnée des suites*

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

définies par récurrence de la manière suivante :

$$\begin{array}{rcl} u_0 & := & 1 \\ u_1 & := & 0 \\ v_0 & := & 0 \\ v_1 & := & 1 \ ; \end{array} \qquad \textit{I.3.3.5.1}$$

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

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

sinon, q_n *est le quotient de la division euclidienne (cf. I.3.2.4.iii),) de* a_n *par* a_{n+1} *et* $a_{n+2} \ := \ a_n - q_n a_{n+1}$ *le reste. On pose alors :*

$$\begin{array}{rcl} u_{n+2} & := & u_n - q_n u_{n+1} \\ v_{n+2} & := & v_n - q_n v_{n+1} \ . \end{array} \qquad \textit{I.3.3.5.2}$$

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)

$$\forall n \in \mathbb{N},\ a_n \ =\ au_n + bv_n\ .$$

Preuve *: (cf. Problème n° I, exercice B.)*

Corollaire I.3.3.6 *Avec les notations de la proposition I.3.3.5, 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.

Exemple I.3.3.7 a) On peut [5] 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

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

b) On trouvera des exemples d'utilisation de l'algorithme d'Euclide par exemple en TD n° II, exercice D ou TD n° II, exercice F.

Théorème I.3.3.8 (Lemme de GAUSS) *Étant donnés trois entiers relatifs* $a, b, c,$ *si* a *et* b *sont premiers entre eux, et* $a|bc$ *alors* $a|c$.

Preuve *: Si* a *et* b *sont premiers entre eux, il existe (cf. I.3.3.3.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* $a|c$.

5. On n'a jamais dit « on doit »

Remarque I.3.3.9 Il se peut que dans la littérature, le lemme de GAUSS ne soit pas habituellement déduit du théorème de BÉZOUT mais plutôt de la proposition I.3.3.17. 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 la proposition I.3.3.17 est satisfaite mais dans lesquels le théorème de BÉZOUT I.3.3.3 ne l'est pas. Dans de tels anneaux dits *factoriels* le lemme de GAUSS est 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.

Théorème I.3.3.10 (Lemme d'Euclide) *Dans l'anneau $\mathbb{Z}$ tous les éléments irréductibles sont premiers.*

Preuve : *Soit $p \in \mathbb{Z}$ irréductible. Cela signifie en particulier que*

$$diviseurs p = \{-p, -1, 1, p\}$$

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. I.3.3.8,) $p|b$.*

Remarque I.3.3.11 La définition d'élément premier donnée en I.3.1.15 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 I.3.3.12 (Nombre premier) On appellera donc *nombre premier* un entier <u>naturel</u> $p \in \mathbb{N}$ qui en tant qu'élément de $\mathbb{Z}$ a les deux propriétés équivalentes d'être premier non nul (cf. I.3.1.15,) ou irréductible (cf. I.3.1.14.)

Proposition I.3.3.13 (Existence des PPCM) *Toute partie finie*

$$A := \{a_1, \ldots, a_n\} \subset \mathbb{Z}$$

admet un PPCM.

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.

Lemme I.3.3.14 *Pour tout $a, b \in \mathbb{Z}$, si d est un **Pgcd** (resp m est un **Ppcm**)*

$$|ab| \ = \ |md| \ .$$

Preuve : *Est un exercice.*

Lemme I.3.3.15 *Étant donnés un entier naturel $n \geq 1$*

$$A \ := \ \{a_1, \ldots, a_n\} \ \subset \ \mathbb{Z},$$

si les a_i sont deux à deux premiers entre eux, (cf. I.3.3.4,) alors

$$\mathrm{PPCM}(A) \ = \ \prod_{i=1}^{n} a_i \ .$$

Preuve : *Le cas $n = 2$ est une conséquence immédiate du lemme I.3.3.14, et le cas général s'en déduit en appliquant I.3.1.13.question 4).*

Remarque I.3.3.16 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,)

$$\bigwedge A \ := \ d\mathbb{Z} \ (\text{resp. } \mathrm{PPCM}(A) \ := \ m\mathbb{Z}) \qquad \text{I.3.3.16.1}$$

et

$$\forall a \in \mathbb{Z}, \ \forall b \in \mathbb{Z}, \ a \wedge b \ := \ \bigwedge\{a, b\} \ (\text{resp. } \mathrm{PPCM}(a, b) \ := \ \mathrm{PPCM}(\{a, b\})) \ . \qquad \text{I.3.3.16.2}$$

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

$$a \wedge b \ = \ d \ \Leftrightarrow \ a \wedge b \ = \ -d \ .$$

Proposition I.3.3.17 (Décomposition en produit de facteurs irréductibles/premiers) *Pour tout*

$$n \in \mathbb{N} \ , \ n > 1 \ ,$$

i) Soit n est un nombre premier (cf. I.3.3.12,) 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* $1 \leq i \leq d\, p_i = q_{\sigma(i)}$.

Remarque I.3.3.17.1 On pourra être surpris de voir ici que la décomposition en produit de facteurs premiers/irréductibles apparaît comme une conséquence du lemme de GAUSS (cf. I.3.3.8,) ou du lemme d'Euclide (cf. I.3.3.10,) 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.

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 I.1.0.1.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. I.3.3.10,) 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 I.3.3.18 On exprimera le fait que tout entier naturel $n > 1$ satisfait à la proposition I.3.3.17.ii) en disant que n admet une *décomposition en produit de facteurs premiers* et l'on dira, en vertu du point I.3.3.17.iii), et de manière un peu abusive, que cette décomposition est *unique*.

Corollaire I.3.3.19 *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 la proposition I.3.3.17.*

I.3.4 . −Arithmétique modulaire sur $\mathbb{Z}$

Définition I.3.4.1 (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. I.3.1.1.)

On définit ainsi une relation binaire (cf. 0.2.1.iii),) sur $\mathbb{Z}$ qu'on appelle *relation de congruence modulo* n.

Remarque I.3.4.2 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. I.3.2.6.)

Lemme I.3.4.3 *Pour tout $n \in \mathbb{N}$, la relation de congruence modulo n est une relation d'équivalence (cf. 0.2.2.v).)*

Définition I.3.4.4 (Classes de congruence) Une classe d'équivalence pour la relation de congruence modulo n s'appelle une *classe de congruence*.

Notation I.3.4.5 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

$$\begin{array}{rccc} \pi_n : & \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & a & \mapsto & a \bmod n \end{array} \qquad \text{I.3.4.5.1}$$

la surjection canonique *i.e.* :

$$\forall a \in \mathbb{Z},\ \pi_n(a) \ := \ a \bmod n \ .$$

Lemme I.3.4.6 *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 :*

$$\begin{array}{rcl} a & \in & b \bmod n \\ b & \in & a \bmod n \\ a \bmod n & = & b \bmod n \\ a & \sim_n & b \\ a & \equiv & b\,[n] \\ n & \mid & b - a \ . \end{array}$$

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. I.3.2.3,) 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. I.1.3.1,) 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*

$$a = nq + \rho(a) \text{ et } b = ns + \rho(b),$$

$$n|b-a \Rightarrow n|n(s-q)+\rho(b)-\rho(a) \Rightarrow n|\rho(b)-\rho(a) \Rightarrow \big(\rho(b)-\rho(a) = 0 \vee n \leq |\rho(b)-\rho(a)|\big)$$

la dernière implication résultant de I.3.2.1.

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 I.3.4.7 (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. 0.5.9.i);)*

ii) la surjection canonique π_n *(cf. I.3.4.5.1,) soit un morphisme d'anneaux (cf. 0.5.9.*v*).)*

Preuve : *Il faut montrer que la relation* $\sim_n$ *est compatibles aux lois* $+$ *et* $*$ *sur* $\mathbb{Z}$ *ce qui est fait au questions (cf. TD n° II, exercice C, question 1), e)) et (cf. TD n° II, exercice C, question 1), f).) On peut ensuite appliquer les résultats de la question (cf. TD n° II, exercice A, question 3).)*

Remarque I.3.4.8 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 I.3.4.9 (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. I.3.3.4.)

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. I.3.3.3,) 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 I.3.4.10 (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. 0.5.9.iii),) 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 I.3.4.6.iv) $\phi(n)$ est aussi le nombre d'entiers inférieurs ou égaux à n et premiers avec n.

Corollaire I.3.4.11 *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. I.3.1.15,) 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.

I.3.5 . −Structure quotient et structure produit

Proposition I.3.5.1 (Groupe abélien quotient) *i) Étant donné un groupe abélien $(A, +)$ et un sous-groupe $C \subset A$, la relation $\sim_C$ définie par*

$$\forall x \in A,\ \forall y \in C,\ \big(x \sim_C y \ \Leftrightarrow\ y - x \in C\big)$$

est une relation d'équivalence.

ii) Pour A et C comme ci-dessus, la relation $\sim_C$ est compatible à la loi $+$ si bien qu'il existe une unique structyure de groupe sur l'ensemble A/C des classes pour la relation $\sim_C$ telle que la surjection canonique $\pi : A \to A/C$ soit un morphisme de groupe.

Remarque I.3.5.1.1 Les vérifications des points I.3.5.1.i) et I.3.5.1.ii) sont absolument les mêmes que celles faites au TD n° II, exercice C, question 1) mais on les donne une fois encore en insistant bien sur l'importance du caractère abélien de A dans la démonstration de I.3.5.1.ii). Un analogue de ce résultat pour des groupes non abéliens sera donné au chapitre II. Il se démontre rigoureusement de la même manière pour I.3.5.1.i), mais nécessite des hypothèses supplémentaires pour I.3.5.1.ii).

Preuve :

i) On a :

$$\forall x \in A,\ x - x = 0 \in C \ \Rightarrow\ x \sim_C x$$

la relation $\sim_C$ est donc réflexive.

$$\forall x \in A,\ \forall y \in A,\ \big(x \sim_C y \ \Leftrightarrow\ y - x \in C \ \Leftrightarrow\ x - y \in C \ \Leftrightarrow\ y \sim_C x\big)$$

(un sous-groupe contient les opposés de tous ses éléments) la relation $\sim_C$ est donc symétrique.

$$\begin{aligned} & \forall x \in A,\ \forall y \in A,\ \forall z \in A,\ \big(x \sim_C y \ \wedge\ y \sim_C z \\ \Leftrightarrow\quad & y - x \in C \ \wedge\ z - y \in C \\ \Rightarrow\quad & z - y + y - x \ =\ z - x \ \in\ C \\ \Rightarrow\quad & x \sim_C z\big) \end{aligned}$$

(un sous-groupe contient la somme de deux quelconques de ses éléments) la relation $\sim_C$ est donc transitive. C'est donc, d'après ce qui précède, une relation d'équivalence.

ii) On a

$$\begin{aligned} & \forall x \in A,\ \forall x' \in A,\ \forall y \in A,\ \forall y' \in A,\ \big(x \sim_C x' \ \wedge\ y \sim_C y' \\ \Leftrightarrow\quad & x' - x \in C \ \wedge\ y' - y \in C \\ \Rightarrow\quad & (x' - x) + (y' - y) \ =\ x' + y' - (x + y) \ \in\ C \\ \Rightarrow\quad & x' + y' \ \sim_C x + y\big)\ . \end{aligned}$$

Proposition I.3.5.2 *Dans la situation de la proposition I.3.5.1, $C \ = \ \mathrm{Ker}\,\pi$ est encore la classe de 0.*

Preuve *: Exercice.*

Proposition I.3.5.3 (Factorisation des morphismes de groupes) *Pour tout morphisme*

$$f \ :\ A \ \to\ B$$

entre groupes abéliens A et B, pour tout sous-groupe $C \ \subset \ A$, si on note A/C le quotient et

$$\pi \ :\ A \ \to\ A/C$$

la surjection canonique, les assertions suivantes sont équivalentes :

a)

$$C \ \subset\ \mathrm{Ker}\, f,$$

b) il existe un unique morphisme $g \ :\ A/C \ \to\ B$ tel que $g \circ \pi \ =\ f$.

De plus, si $C = \operatorname{Ker} f$, g *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

$$v = v \circ w \Rightarrow \operatorname{Ker} w \subset \operatorname{Ker} u .$$

Or $\operatorname{Ker} \pi = C$ *(cf. I.3.5.2,) si bien que*

$$g \circ \pi = f \Rightarrow C \subset \operatorname{Ker} f .$$

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

$*$*)* ***(Unicité de*** g ***(analyse))***

Si g *existe alors nécessairement pour tout* $y \in A/C$, *il existe* $x \in A$ *tel que* $y = \pi(x)$ *et*

$$g(y) = g[\pi(x)] = f(x) .$$

Ceci établit l'unicité de g.

†*)* ***(Existence de*** g ***(synthèse))***

Or si $x' \in A$ *est tel que* $y = \pi(x')$ *on a encore*

$$g(y) = g[\pi(x')] = f(x') .$$

Or

$$\pi(x) = \pi(x') \Rightarrow x' - x \in C = \operatorname{Ker} f \Rightarrow f(x' - x) = 0 \Rightarrow f(x') = f(x) .$$

Il s'ensuit que g *existe et est bien définie par la formulle :*

$$g(y) = f(x) \, \forall \, x, y = \pi(x) .$$

‡*)* (g ***est un morphisme***)

$$\forall x \in A/C, \, \forall y \in A/C, \, \big(\exists u \in A, \, \exists v \in A, \, (x = \pi(u) \wedge y = \pi(v))\big) .$$

On a alors :

$$\begin{aligned} g(x+y) &= g[\pi(u) + \pi(v)] \\ &= g[\pi(u+v)] \\ &= f(u+v) \\ &= f(u) + f(v) \\ &= g[\pi(u)] + g[\pi(v)] \\ &= g(x) + g(y) . \end{aligned}$$

iii) $*$*)* (g ***est injective***)

$$\forall x \in A/C,\ \exists u \in A,\ x = \pi(u)\,.$$
$$g(x) = 0 \Leftrightarrow g[\pi(u)] = 0 \Leftrightarrow f(u) = 0 \Leftrightarrow u \in \operatorname{Ker} f = C \Leftrightarrow x = 0\,.$$

†) ***(surjectivité)***
Si f est surjective, $\forall y \in B,\ \exists x \in A,\ f(x) = y$. Alors $g[\pi(x)] = y$.

Dans le cas où A est un anneau, le quotient A/C et la surjection canonique ont des propriétés supplémentaires que ous allons établir dans la proposition I.3.5.7 pour peu que C lui-même ait des propriétés convenables ; autrement dit que C soit un idéal. Nous avons esquissé la définition d'idéal en I.3.1.10.1 que nous allons donner ici formellement :

Lemme I.3.5.4 *Étant donné un anneau commutatif $(A, +, *)$ pour $C \subset A$, les propriétés suivantes sont équivalentes :*

a) C est un sous-groupe de $(A, +)$ tel que

$$\forall x \in C,\ \forall a \in A,\ ax \in C\,.$$

b)

$$C \neq \emptyset \text{ et } \forall x \in C,\ \forall y \in C,\ \forall a \in A,\ \forall b \in A,\ ax + by \in C\,.$$

Preuve *: Exercice.*

Définition I.3.5.5 (Idéal) Étant donné un anneau commutatif A, une partie $C \subset A$ vérifiant les assertions équivalentes du lemme I.3.5.4 est un *idéal* de A.

Exemple I.3.5.6 a) Le noyau d'un morphisme d'anneaux $f : A \to B$ est toujours un idéal de A.

b) Une partie $H \subset \mathbb{Z}$ est un idéal de $\mathbb{Z}$ si et seulement si c'est un sous-hgroupe de $\mathbb{Z}$ *i.e.*une partie de la forme $d\mathbb{Z}$ (cf. I.3.2.6.)

Proposition I.3.5.7 *Étant donné un anneau commutatif $(A, +, *)$ et C un idéal de A :*

i) quotient A/C au sens des groupes (cf. I.3.5.1.ii),) possède une unique structure d'anneau tel que la surjection canonique $\pi : A \to A/C$ soit un morphisme d'anneaux et l'on a $\operatorname{Ker} \pi = C$.

ii) Pour tout morphisme d'anneaux $f : A \to B$ (où B est un anneau commutatif,) les conditions suivantes sont équivalentes :

a)

$$C \subset \operatorname{Ker} f ;$$

b) il existe un unique morphisme d'anneaux $g : A/C \to B$ tel que $g \circ \pi = f$.

De plus, si $C = \operatorname{Ker} f$, g est injective et g est surjective dès que f l'est.

***Preuve** :*

i) Il découle de la proposition I.3.5.1 que A/C est déjà un groupe abélien et $\pi : A \to A/C$ un morphisme de groupes. La relation $\sim_C$ étant celle définie en I.3.5.1, i.e. $x \sim_C x' \Leftrightarrow x' - x \in C$, on remarque que :

$$\begin{array}{lrcl} \forall x \in A,\ \forall x' \in A, & & & \\ \forall y \in A,\ \forall y' \in A, & x \sim_C x' & \text{et} & y \sim_C y' \\ \Rightarrow & x'y' - xy & = & x'y' - x'y + x'y - xy \\ & & = & x'(y' - y) + y(x' - x) \\ & & \in & C \\ \Rightarrow & x'y' & \sim_C & xy \end{array}$$

c'est-à-dire, du fait que C est un idéal, que la relation $\sim_C$ est compatible à $*$ et qu'il existe donc une unique loi $*$ sur A/C telle que

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

(cf. TD n° II, exercice A, question 3), a).) Il découle en outre du TD n° II, exercice A, question 3), b) que $\pi(1)$ est un élément neutre pour $*$ sur A/C ce qui entraîne que A/C est un anneau et π un morphisme d'anneaux.

ii) Puisque

$$f : (A, +) \to (B, +) \text{ et } \pi : (A, +) \to (A/C, +)$$

sont en particulier des morphismes de groupes et que C est un sous-hgroupe de $(A, +)$, il résulte de la proposition I.3.5.3 que $C \subset \operatorname{Ker} f$ équivaut à l'existence d'un unique morphisme de groupes

$$g : (A/C, +) \to (B, +)$$

vérifiant $g \circ \pi = f$. Reste donc à vérifier que g est bien un morphisme d'anneaux. Or :

$$\begin{array}{lll} \forall \alpha \in A/C,\ \forall \beta \in A/C, & & \\ \forall x \in A,\ \forall y \in A, & \big(\alpha = \pi(x) \text{ et } \beta = \pi(y) & \Rightarrow\ g(\alpha * \beta) \\ & & = g(\pi(x) * \pi(y)) \\ & & = g(\pi(x * y)) \\ & & = f(x * y) \\ & & = f(x) * f(y) \\ & & = g(\alpha) * g(\beta)\big) \end{array}$$

Exemple I.3.5.8 Dans le cas particulier où $A = \mathbb{Z}$ et $C = n\mathbb{Z}$, la relation $\sim_C$ est exactement la relation de congruence modulo n définie en I.3.4.1 et le groupe (respectivement l'anneau) A/C exactement le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ (respectivement l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, *)$.)

Définition I.3.5.9 (Quotient) Le groupe A/C construit par la proposition I.3.5.1, (respectivement l'anneau A/C construit par la proposition I.3.5.7 est appelé *groupe quotient* (respectivement *anneau quotient*.

Proposition I.3.5.10 (Structure produit) *Soient*

$$(A_i, +_i)\,,1 \leq i \leq n \ \left(\textit{resp. } (A_i, +_i, *_i)\,,1 \leq i \leq n\right)$$

des groupes (abéliens) (resp. des anneaux .) Soit

$$A := A_1 \times \ldots \times A_n = \left\{(x_1, \ldots, x_n) < x_i \in A_i\right\}$$

le produit cartésien des A_i et :

$$\forall 1 \leq i \leq n,\ pi_i : \begin{array}{rcl} A & \to & A_i \\ (x_1, \ldots, x_n) & \mapsto & x_i \end{array} \qquad \textit{I.3.5.10.1}$$

les projections canoniques. Alors les lois $+$ (resp. $+$ et $*$) définies sur A par :

$$\begin{array}{rcl} (x_1, \ldots, x_n) + (y_1, \ldots, y_n) & := & (x_1 +_1 y_1, \ldots, x_n +_n y_n) \\ (x_1, \ldots, x_n) * (y_1, \ldots, y_n) & := & (x_1 *_1 y_1, \ldots, x_n *_n y_n) \end{array} \qquad \textit{I.3.5.10.2}$$

font de $(A, +)$ (resp. $(A, +, *)$) un groupe (abélien) (resp. un anneau) et les $\pi_i\,,1 \leq i \leq n$ sont des morphismes de groupes (resp. d'anneaux.)

Preuve *: Cette démonstration est plus un jeu d'écriture qu'autre chose et ne présente aucune difficulté.*

Définition I.3.5.11 (Produit) Le groupe (respectivement l'anneau) A construit dans la proposition I.3.5.10 est appelé *groupe produit* (respectivement *anneau produit*.)

I.3.6 . −Le théorème chinois des restes

Théorème I.3.6.1 (Théorème chinois des restes) *Soient $n > 1$ un entier naturel et $a_i\,,1 \leq i \leq n > 1$ des entiers naturels. On note m le* ***Ppcm*** *(cf. I.3.1.8,) des a_i et $\pi_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ la surjection canonique*

i) L'application

$$\begin{array}{rcl} \pi : \mathbb{Z} & \longrightarrow & \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z} \\ x & \longmapsto & (x \bmod a_1, \ldots, x \bmod a_n) \end{array} \qquad 1$$

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 I.3.5.11.

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. I.3.3.4,) γ est surjectif et donc bijectif (cf. 0.2.4.iii),) et l'application réciproque γ^{-1} est aussi un morphisme d'anneaux. Dans ce cas, on a

$$m \,=\, \prod_{i=1}^{n} a_i \text{ (cf. I.3.3.15.)}$$

***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 I.3.5.3 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

$$\begin{array}{l}\forall x\in\mathbb{Z}/m\mathbb{Z},\ \forall y\in\mathbb{Z}/m\mathbb{Z},\ \big(\\ \exists u\,\in\,\mathbb{Z},\ \exists v\in\mathbb{Z},\ (\pi_m(u)\,=\,x\,\wedge\,\pi_m(v)\,=\,y)\wedge\ \ \gamma(x*y) \ \ =\ \ \gamma[\pi_m(u)*\pi_m(v)]\\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad =\ \ \gamma[\pi_m(u*v)]\\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad =\ \ \pi(u*v)\\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad =\ \ \pi(u)*\pi(v)\\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad =\ \ \gamma(x)*\gamma(y)\big)\end{array}$$

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. I.3.3.3.) 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 I.3.5.3 que γ l'est aussi.

L'application γ est bijective. Le fait que γ^{-1} est un morphisme d'anneaux est assuré par le lemme I.3.6.2

Lemme I.3.6.2 *i) Étant donnés des ensembles $(A, \cdot)$ et $(B, \dagger)$ des ensembles munis de lois de composition, si $f : A \to B$ est un morphisme pour les lois $\cdot$ et $\dagger$, si f est bijectif d'application réciproque g alors g est aussi un morphisme.*

ii) Si de plus $(A, \cdot)$ (resp. $(B, \dagger)$) possède un élément neutre ϵ (resp. η)

$$f(\epsilon) = \eta \Rightarrow g(\eta) = \epsilon\ .$$

***Preuve** :*

i)

$$\begin{array}{l}\forall x \in B,\ \forall y \in B,\ \big(\\ \exists u \in A,\ \exists v \in A,\ (x = f(u) \wedge y = f(v)) \wedge \quad g(x \dagger y)\\ \qquad\qquad\qquad\qquad\qquad\qquad = g[f(u) \dagger f(v)]\\ \qquad\qquad\qquad\qquad\qquad\qquad = g[f(u \cdot v)]\\ \qquad\qquad\qquad\qquad\qquad\qquad = u \cdot v\\ \qquad\qquad\qquad\qquad\qquad\qquad = g(x) \cdot g(y)\big)\ .\end{array}$$

ii) Est immédiat.

On présente maintenant quelques corollaires du théorème I.3.6.1 :

Corollaire I.3.6.3 *Étant donnés*

$$\begin{cases} \text{un entier naturel } n \geq 1, \\ \text{un } n\text{-uplet d'entiers naturels } a_i \text{ ,} 1 \leq i \leq n \\ \text{et un } n\text{-uplet d'entiers relatifs } k_i \text{ ,} 1 \leq i \leq n \text{ ,} \end{cases}$$

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. I.3.4.6.i),) à

$$(x \bmod a_i \; = \; k_i \bmod a_i \; , \; 1 \leq i \leq n)$$

c'est-à-dire (cf. I.3.6.1.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. I.3.6.1.iii)))*

$$x \bmod \prod_{i=1}^{n} a_i \; = \; \gamma^{-1}(k_1 \bmod a_1, \ldots, k_n \bmod a_n) \; .$$

Corollaire I.3.6.4 *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. I.3.6.1.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. I.3.4.11,) et il apparaîtra qu'il est infiniment plus confortable de résoudre des équations polynomiales dans un corps que dans un anneau quelconque.*

Remarque I.3.6.5 Il existe de nombreuses variantes du théorème I.3.6.1 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 $\mathrm{PPCM}(a,b)$. 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 I.3.3.1,) 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 $\mathbb{Z}/\mathrm{PPCM}(a,b)\mathbb{Z}$.

II . −Groupe symétrique

II.1 . −Compléments sur les groupes

II.1.1 . −Sous-groupes

Proposition II.1.1.1 (Sous-Groupe) *Une partie H d'un groupe $(G, *)$ (cf. 0.5.6.i),) est un sous-groupe (cf. 0.5.6.iv),) si et seulement si H est non vide et pour tout couple (x, y) d'éléments de H, $x * y^{-1} \in H$.*

***Preuve** :*

i) Si H est un sous-groupe de G, en particulier H est un groupe et il est donc non vide (cf. 0.5.7.i).) Notons $*_H$ la restriction de $*$ à $H \times H$. Si e_H est l'élément neutre de H, pour tout $x \in H$, $x *_H e_H = x$. Cependant, x et e_H étant en particulier des éléments de G, on peut encore écrire, $x * e_H = x$. D'autre part, $x * e = x$ d'où,

$$x * e_H = x * e \Rightarrow x^{-1} * x * e_H = x^{-1} * x * e \Rightarrow e_H = e$$

c'est-à-dire que l'élément neutre de H est celui de G.

Tout $y \in H$ possède un inverse y' tel que

$$y *_H y' = y' *_H y = e_H = e\,.$$

Or y et y' étant en particulier des éléments de G, on peut encore écrire,

$$y * y' = y' * y = e$$

c'est-à-dire que y' est l'inverse y^{-1} de y dans G puisque ce dernier est unique (cf. TD n° II, exercice B, question 1), b).)

Pour tout couple (x, y) d'éléments de H, x et y^{-1} sont encore des éléments de H d'après ce qui précède. 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) 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, $e = x * x^{-1} \in H$. Il est clair que e est alors un élément neutre pour H.

De plus, pour tout $x \in H$, $e * x^{-1} = x^{-1} \in H$ 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.

Remarque II.1.1.2 La démonstration de la proposition précédente fait apparaître que, si H est un sous-groupe de $(G, *)$, l'élément neutre de H est celui de G, et le symétrique dans H d'un élément $x \in H$ est son symétrique dans G.

Corollaire II.1.1.3 *Pour tout morphisme de groupes $f : G \to ,H$*

i) Le noyau $\mathrm{Ker}\, f$ *défini par*

$$\mathrm{Ker}\, f := \{x \in G\,;\, f(x) = e\}$$

est un sous-groupe de G.

ii) L'image $\mathrm{Im}\, f$ *c'est-à-dire l'image de G par f (cf. 0.2.4.ii)) est un sous-groupe de H.*

iii) Le morphisme est injectif (resp. surjectif) si et seulement si $\mathrm{Ker}\, f = \{e\}$ *(resp.* $\mathrm{Im}\, f = H$ *.)*

II.1.2 . −Quotient et théorème de Lagrange

Notation II.1.2.1 Dans la suite $(G, *)$ est un groupe et H un sous-groupe. On définit $\sim_{g,H}$ (resp. $\sim_{d,H}$) la relation binaire sur $G \times G$ par :

$$\forall x \in G,\ \forall y \in G,\ \left(x \sim_{g,H} y \Leftrightarrow x^{-1} * y \in H\right) \left(\text{resp. } \forall x \in G,\ \forall y \in G,\ \left(x \sim_{d,H} y \Leftrightarrow y * x^{-1} \in H\right)\right). \qquad \text{II.1.2.1.1}$$

On notera encore, :

$$\forall x \in G,\ x * H := \{x * y\,;\, y \in H\} \left(\text{resp. } H * x := \{y * x\,;\, y \in H\}\,.\right) \qquad \text{II.1.2.1.2}$$

On notera enfin :

$$\forall x \in G,\ x * H * x^{-1} := \{x * y * x^{-1}\,;\, y \in H\}\,. \qquad \text{II.1.2.1.3}$$

Remarque II.1.2.1.4 Il faut prendre garde que les notations introduites en II.1.2.1.2 et II.1.2.1.3 ne sont que des notations et qu'en particulier, rien ne prouve que $(x * H) * x^{-'} = x * H * x^{-1}$ ne serait-ce que parce que stricto sensu le membre de gauche n'est pas défini. Voyez-vous pourquoi ?

Proposition II.1.2.2 *i) Les relations binaires définies en II.1.2.1.1 sont des relations d'équivalence.*

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

Plus précisément :

$$\forall x\in G,\ \mathrm{cl}_g(x)\ =\ \{y\ \in\ G\,;\ x\sim_{g,H}\ y\}\ =\ x{*}H\ \big(\text{resp. } \mathrm{cl}_d(x)\ =\ \{y\ \in\ G\,;\ x\sim_{d,H}\ y\}\ =\ H{*}x\,.\big)$$

1

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

iv) Si G *est fini on a :*

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

***Preuve** :*

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

Par ailleurs :

$$\begin{array}{lrcl}
\forall x\in G,\ \forall y\in G,\ \big(& x & \sim_{g,H} & y\\
\text{(cf. II.}\vec{1}\text{.2.1.1)} & x^{-1}*y & \in & H\\
H \text{ est un } \vec{\text{groupe}} & y^{-1}*x\ =\ (x^{-1}*y)^{-1} & \in & H\\
\text{(cf. II.}\vec{1}\text{.2.1.1)} & y & \sim_{g,H} & x\big)
\end{array}$$

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

Enfin :

$$\begin{array}{lrcl}
\forall x\in G,\ \forall y\in G,\ \forall z\in G,\ \big(& x\sim_{g,H} y & \wedge & y\sim_{g,H} z\\
\text{(cf. II.}\vec{1}\text{.2.1.1) } x^{-1}*y\in H & \wedge\ y^{-1}*z\in H & & \\
H \text{ est un } \vec{\text{groupe}} & x^{-1}*y*y^{-1}*z & \in & H\\
\Rightarrow & x^{-1}*z & \in & H\\
\Rightarrow & x & \sim_{g,H} & z\big)
\end{array}$$

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

L'argument vaut également pour $\sim_{d,H}$ *.*

ii) Pour tout $x\ \in\ G$*, un élément* y *de* G *appartient à la classe de* x *modulo* $\sim_{g,H}$ *si et seulement si*

$$\big((x^{-1}*y\in H)\ \Leftrightarrow\ (\exists z\in H,\ (x^{-1}*y\ =\ z)\ \Leftrightarrow\ y\ \in\ x*H)\big)\,;$$

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

$$G \to G\ ,\ z \mapsto x * z$$

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

$$G \to G\ ,\ z \mapsto x^{-1} * z\ .$$

iv) Ce dernier résultat provient de ce que l'union des classes d'équivalence est égale à G que toutes ces classes ont même cardinal égal à celui de H.

Définition II.1.2.3 Étant donnés un groupe $(G, *)$ et H un sous-groupe de $(G, *)$on appelle *indice de H dans G* le nombre de classes d'équivalences pour la relation $\sim_{d,H}$ encore égal au nombre de classes d'équivalences pour la relation $\sim_{g,H}$

Définition II.1.2.4 Étant donné un groupe fini $(G, *)$ et H un sous-groupe de $(G, *)$, on apelle *ordre de H* le cardinal de H.

Corollaire II.1.2.5 *Si G est un groupe fini et H un sous-groupe, le cardinal de H divise le cardinnal de G.*

Preuve *: (cf. II.1.2.2.iv).)*

Définition II.1.2.6 Pour $x \in G$, on appelle *ordre de x* l'ordre du sous-groupe $\operatorname{Im} \epsilon_x$ où ϵ_x est le morphisme défini au TD n° II, exercice B, question 3).

Lemme II.1.2.7 *Pour $(G, *)$ un groupe et $x \in G$, l'ordre de x est l'unique élément $d \in \mathbb{N}$ tel que $\operatorname{Ker} \epsilon_x = d\mathbb{Z}$ c'est aussi l'unique élément $d \in \mathbb{N}$ tel que*

$$\forall n \in \mathbb{Z},\ x^n = 1 \Rightarrow d | n.\ .$$

Preuve *: (cf. TD n° IV, exercice A.)*

Corollaire II.1.2.8 (Théorème de Lagrange) *Si G est de cardinal fini, l'ordre de tout élément x divise l'ordre de G.*

II.1.3 . −Sous-groupe distingué (normal), groupe quotient

Définition II.1.3.1 (Conjugaison) On dit que deux éléments x et y de G sont *conjugués* s'il existe $z \in G$ tel que

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

Lemme II.1.3.2 *La relation de conjugaison est une relation d'équivalence.*

Lemme II.1.3.3 *Deux éléments conjugués ont même ordre.*

Proposition II.1.3.4 (Sous-groupe normal) *Étant doné un groupe $(G, *)$ pour un sous-groupe H, les conditions suivantes sont équivalentes :*

a)

$$\forall x \in G, \ \left(x * H * x^{-1} \subset H\right) .$$

b)

$$\forall x \in G, \ \left(x * H = H * x\right) .$$

c)

$$\forall x \in G, \ \left(H = x * H * x^{-1}\right) .$$

d) Si $\sim_{g,H}$ (resp. $\sim_{d,H}$) est la relation définie en II.1.2.1.1

$$\forall x \in G, \ \forall y \in G, \ \left(x \sim_{g,H} y \Leftrightarrow x \sim_{d,H} y\right)$$

et on notera simplement $x \sim_H y$ dans ce cas.

e) La relation $\sim_H$ définie ci-dessus est compatible à la loi $*$.

***Preuve** :*

i) Pour l'équivalence entre les assertions a), b) et c) (cf. TD n° IV, exercice G, question 1).)

*ii) (**b)** $\Leftrightarrow$ **d**))*

Deux relations d'équivalence sont les mêmes si et seulement si elles définisssent les mêmes classes ou encore la même partition. Il suffit alors de considérer la caractérisation des classes donnée à la proposition II.1.2.2.ii).1.

*iii) (**a)** $\Leftrightarrow$ **e)**)*

Remarquons que, pour tout $y \in H$, $y \sim_H e$, et que, pour tout $x \in G$, $x \sim_H x$. Il en résulte donc, si l'on suppose l'assertion e) vérifiée, que pour tout $y \in H$ et tout $x \in G$, $x * y \sim_H x$ c'est-à-dire précisément $x * y * x^{-1} \in H$. L'assertion e) entraîne donc l'assertion a).

Réciproquement, étant donné un quadruplet (x, x', y, y') d'éléments de G, si $y \sim_H y'$, $y * y'^{-1} \in H$. Si l'on suppose l'assertion a) vérifiée, $x * y * y'^{-1} * x^{-1} \in H$. Mais $x \sim_H x'$ entraîne que $x * x'^{-1} \in H$ ce qui entraîne, puisque H est un sous-groupe de G, que

$$x * y * (x' * y')^{-1} = x * y * y'^{-1} * x'^{-1} = x * y * y'^{-1} * x^{-1} * x * x'^{-1} \in H$$

c'est-à-dire que $x * y \sim_H x' * y'$. On a donc montré que l'assertion a) entraîne l'assertion e).

Définition II.1.3.5 (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 II.1.3.4.

Exemple II.1.3.6 a) Les sous-groupes $\{e\}$ et G de G sont toujours distingués dans G.

b) Pour tout morphisme de groupes $f : G \to H$ (cf. 0.5.6.ii),) 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.

c) Si G est un groupe abélien ($(\mathbb{Z}, +)$ par exemple,) tout sous-groupe est distingué.

Proposition II.1.3.7 (Quotient et factorisation) *i) 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.*

*ii) (**Factorisation des morphismes**)*

Pour tout morphisme de groupes $f : G \to K$ 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 $g : G/H \to K$ tel que $g \circ \pi = f$.

De plus, si $H = \mathrm{Ker}\, f$, g est injectif et il est surjectif dès que f l'est.

Preuve : *Ce résultat est l'exact analogue de la proposition I.3.5.3 ou plutôt en est une généralisation. Cependant dans un cas comme dans l'autre l'ingrédient esssentiel de la preuve est la compatibilité de la relation d'équivalence à la loi de groupe. Cette compatibilité est automatique dans le cas des groupes abéliens et résulte ici du fait que H et distingué.*

Définition II.1.3.8 Le groupe G/H est appelé *groupe quotient*.

Exemple II.1.3.9 Nous avons remarqué (cf. II.1.3.6.c),) que dans un groupe abélien, et en particulier dans $(\mathbb{Z}, +)$, que tout sous-groupe est distingué. Nous avons aussi établi (cf. I.3.2.6,) qu'une partie K de $\mathbb{Z}$ est un sous-groupe si et seulement s'il existe un entier $d \geq 0$ tel que $K = d\mathbb{Z}$.

On constate alors, que pour deux entiers x et y, $x \sim_K y$ si $y - x \in K$, c'est-à-dire si et seulement si $d|y - x$. La relation $\sim_K$ 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 en I.3.4.7. L'ensemble des classes modulo d que nous avions noté $\mathbb{Z}/d\mathbb{Z}$ s'identifie en tant que groupe au groupe quotient $\mathbb{Z}/K = \mathbb{Z}/d\mathbb{Z}$.

Corollaire II.1.3.10 *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 II.1.3.7.ii) à $H := \mathrm{Ker}\, f$.*

Corollaire II.1.3.11 *Étant donné un groupe fini G et $f : G \to K$ un morphisme de groupes, $\mathrm{Ker}\, f$ et $\mathrm{Im}\, f$ sont des groupes finis et on a :*

$$\#(G) = \#(\mathrm{Ker}\, f) \cdot \#(\mathrm{Im}\, f)\,.$$

Preuve : *Exercice.*

II.1.4 . −Sous-groupe engendré par une partie

Proposition II.1.4.1 (Sous-groupe engendré) *Étant donné un groupe $(G, *)$ pour une partie $S \subset G$ de G et une partie $H \subset G$ de G, les deux assertions suivantes sont équivalentes :*

a) La partie H est l'intersection de tous les sous-groupes K de G contenant S.

b) La partie H est un sous-groupe de G contenant S tel que, pour tout sous-groupe K de G contenant S, $H \subset K$.

Si $S \neq \emptyset$, les deux assertions précédentes sont encore équivalentes à :

c) La partie H est l'ensemble des éléments $x \in G$ tels qu'il existe un entier $d \geq 1$ des éléments $s_{i\ ,1\leq i\leq d} \in S$, des entiers relatifs $\alpha_{i\ ,1\leq i\leq d}$ tels que

$$x \ = \ \prod_{i=1}^{d} s_i^{\alpha_i} \ ,$$

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.

***Preuve** :*

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

Notons I l'intersection de tous les sous-groupes K de G contenant S. On sait (cf. TD n° IV, exercice C, question 3),) que I est un sous-groupe de G. Notons H un sous-groupe vérifiant l'assertion b). En particulier $S \subset H$ ce qui implique que $I \subset H$. Par ailleurs, I lui-même est un sous-groupe contenant S donc $H \subset I$ ce qui prouve que les assertions a) et b) sont équivalentes.

ii) Supposons $S \neq \emptyset$, et notons L l'ensemble des $x \in G$ vérifiant la propriété énoncée en c). Il est alors clair que $S \subset L$ et que donc, $L \neq \emptyset$.

Par ailleurs, pour tout couple (x, y) d'éléments de L, il existe des entiers $d_x \geq 1$ et $d_y \geq 1$, des éléments

$$\begin{aligned} s_{i\ ,1\leq i\leq d_x} &\in S \\ \alpha_{i\ ,1\leq i\leq d_x} &\in \mathbb{Z} \\ t_{i\ ,1\leq i\leq d_y} &\in S \\ \beta_{i\ ,1\leq i\leq d_y} &\in \mathbb{Z} \end{aligned}$$

tels que

$$x \ = \ \prod_{i=1}^{d_x} s_i^{\alpha_i} \text{ et } y \ = \ \prod_{i=1}^{d_y} t_i^{\beta_i} \ .$$

Il en résulte que

$$x * y^{-1} = \prod_{i=1}^{d_x} s_i^{\alpha_i} * \prod_{i=d_y}^{1} t_i^{-\beta_i}$$

est encore un élément de L. Il en résulte que L est un sous-groupe de G contenant S. Il est immédiat que tout sous-groupe K de G contenant S contient L et, par conséquent, que L vérifie l'assertion b).

Corollaire II.1.4.2 *Pour toute partie S d'un groupe G il existe un unique sous-groupe H de G contenant S et inclus dans tout sous-groupe de G contenant S. Le sous-groupe H est défini comme l'intersection de tous les sous-groupes de G contenant S.*

Si $S \neq \emptyset$, l'assertion II.1.4.1.c) donne une description de H.

Définition II.1.4.3 Soit S une partie d'un groupe G.

i) Le sous-groupe H défini par le corollaire II.1.4.2 est appelé *sous-groupe de G engendré par S*.

On dit que S est une *partie génératrice* de H.

ii) Si $H = G$ on dit que G est *engendré* par S ou encore que S est une *partie génératrice* de G.

iii) S'il existe un *singleton* $\{x\} \subset G$ tel que G soit engendré par $\{x\}$ on dit que G est *monogène*.

Remarque II.1.4.4 Si $S = \emptyset$ il résulte des caractérisations II.1.4.1.a) et II.1.4.1.b) que le sous-groupe engendré par S est $\{e_G\}$.

Proposition II.1.4.5 *Si G est un groupe monogène, soit G est isomorphe à $\mathbb{Z}$ soit il existe un entier $d > 0$ tel que G est isomorphe à $\mathbb{Z}/d$. Dans ce deuxième cas, on dit que G est cyclique.*

Preuve *: Si G est monogène il existe $x \in G$ tel que $\{x\}$ est une partie génératrice de G. Cela signifie en particulier, que pour tout $y \in G$, il existe $n \in \mathbb{Z}$ tel que $y = x^n$. Ceci signifie que le morphisme*

$$\begin{array}{rccc} \epsilon_x : & \mathbb{Z} & \longrightarrow & G \\ & n & \longmapsto & x^n \end{array}$$

(cf. TD n° II, exercice B, question 3),)est surjectif.

S'il est injectif, c'est un isomorphisme et, par conséquent G est isomorphe à $\mathbb{Z}$.

Si ϵ_x n'est pas injectif, son noyau est un sous-groupe de $\mathbb{Z}$ différent du singleton $\{0\}$ (cf. II.1.1.3.iii).) Il existe, par conséquent (cf. I.3.2.6) un entier $d > 0$ tel que $\operatorname{Ker} \epsilon_x =$

$d\mathbb{Z}$. Il existe dès lors (cf. II.1.3.7.ii),) un isomorphisme $\mathbb{Z}/\mathrm{Ker}\,\epsilon_x \cong \mathrm{Im}\,\epsilon_x$ c'est-à-dire un isomorphisme

$$\mathbb{Z}/d\mathbb{Z} \cong G\,.$$

II.2 . −Groupe symétrique et groupe alterné

II.2.1 . −Définition et premières propriétés

Définition II.2.1.1 (Groupe symétrique) i) Pour tout ensemble E, on note $\mathcal{S}(E)$ l'ensemble des bijections de E dans lui-même. L'ensemble $\mathcal{S}(E)$ muni de la composition des applications est un groupe.

ii) Si $E := [1;n] \subset \mathbb{N}$ est l'ensemble des n premiers entiers naturels pour $n \geq 1$, on note $\mathcal{S}_n$ le groupe $\mathcal{S}(E)$ et on l'appelle *groupe symétrique*.

iii) Un élément $s \in \mathcal{S}_n$ est appelé *permutation* ou *substitution*.

iv) Pour toute permutation $s \in \mathcal{S}_n$, on notera

$$s = \begin{pmatrix} 1 & 2 & \dots & n \\ s(1) & s(2) & \dots & s(n) \end{pmatrix}\,.$$

Remarque II.2.1.2 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 II.2.1.3 *i) Si $\gamma : E \to F$ est une bijection entre deux ensembles E et F, l'application :*

$$\begin{array}{ccc} \mathcal{S}(E) & \to & \mathcal{S}(F) \\ s & \mapsto & \gamma \circ s \circ \gamma^{-1} \end{array}$$

est un isomorphisme de groupes dont l'application réciproque est donnée par

$$\begin{array}{ccc} \mathcal{S}(F) & \to & \mathcal{S}(E) \\ u & \mapsto & \gamma^{-1} \circ u \circ \gamma\,. \end{array}$$

ii) Si E est un ensemble fini c'est-à-dire qu'il existe une bijection $\gamma : E \to [1;n]$ (cf. I.1.3.2,), il découle du point précédent que les groupes $\mathcal{S}(E)$ et $\mathcal{S}_n$ sont isomorphes si bien qu'on s'intéressera dans la suite essentiellement à l'étude de $\mathcal{S}_n$.

Proposition II.2.1.4 *Pour tout entier $n \geq 1$, $\mathcal{S}_n$ est un ensemble fini. On a la relation*

$$\#(\mathcal{S}_{n+1}) \ = \ (n+1)\#(\mathcal{S}_n) \qquad \textit{II.2.1.4.1}$$

d'où l'on déduit que

$$\#(\mathcal{S}_n) \ = \ n! \ . \qquad \textit{II.2.1.4.2}$$

Preuve *:*

i) Notons tout d'abord H le sous-ensemble de $\mathcal{S}_{n+1}$ constitué des éléments s tels que $s(n+1) = n+1$. On laisse le soin au lecteur de vérifier que H est un sous-groupe de $\mathcal{S}_{n+1}$ (cf. II.1.1.1.)

ii) On rappelle (cf. II.1.2.2.i),) que la relation $\sim_{g,H}$ définie sur $\mathcal{S}_{n+1}$ par

$$s \ \sim_{g,H} \ s' \text{ si } s^{-1}s' \ \in \ H$$

est une relation d'équivalence telle que pour chaque classe $\overline{s}$ il existe une bijection de H dans $\overline{s}$.

iii)

$$\forall s \in \mathcal{S}_{n+1},\ \forall t \in \mathcal{S}_{n+1},\ \big(s \sim_{g,H} t \ \Leftrightarrow \ s^{-1}t \in H \ \Leftrightarrow \ s^{-1}t(n+1) = n+1 \ \Leftrightarrow \ s(n+1) \ = \ t(n+1)\big) \ .$$

iv) Il est dès lors clair que l'application $\overline{s} \mapsto s(n+1)$ est bien définie et induit une bijection de l'ensemble $\mathcal{C}$ des classes selon $\sim_{g,H}$ sur $[1; n+1]$. On en déduit que $\#\big(\mathcal{C}\big) \ = \ n+1$.

v) Enfin, il découle presqu'immédiatement de la définition de H que H est isomorphe à $\mathcal{S}_n$.

vi) Si donc l'on fait l'hypothèse de récurrence que $\mathcal{S}_n$ est un ensemble fini $\mathcal{S}_{n+1} \ = \ \coprod_{c \ \in \ \mathcal{C}} c$, est également un ensemble fini et

$$\#\big(\mathcal{S}_{n+1}\big) \ = \ \#(C)\#(H) \ = \ (n+1)\#\big(\mathcal{S}_n\big) \ .$$

Proposition II.2.1.5 (Orbites) *Pour tout entier $n \geq 1$, 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 *: La démonstration de ce fait est laissée en exercice.*

Définition II.2.1.6 Soit $n \geq 1$ un entier naturel et 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 II.2.1.5 est appelée *orbite de a sous s* et notée $O_s(a)$.

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* 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*.

II.2.2 . −Propriétés des cycles

Théorème II.2.2.1 *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 *: Notons S le support de c, l sa longueur égale au cardinal de S et fixons un élément $a \in S$. On a alors $S = O_c(a)$ et l'application*

$$\begin{array}{rccc} \epsilon_a : & \mathbb{Z} & \to & S \\ & k & \mapsto & c^k(a) \end{array} \qquad \text{II.2.2.1.1}$$

est surjective par définition même d'une orbite.

Lemme II.2.2.1.2 *Il existe un entier $d > 0$ tel que l'ensemble*

$$H_a := \{k \in \mathbb{Z} \,;\, \epsilon_a(k) = a\}$$

soit égal à $d\mathbb{Z}$.

Preuve : *L'ensemble S étant fini tandis que $\mathbb{Z}$ ne l'est pas, l'application ϵ_a ne peut être injective. Il existe, par conséquent, un couple (p,q) d'entiers relatifs distincts tels que*

$$\epsilon_a(p) \;=\; \epsilon_a(q) \;\Leftrightarrow\; c^p(a) \;=\; c^q(a)$$

ce qui équivaut encore, puisque c est une bijection, à $c^{p-q}(a) \;=\; a$. L'ensemble H_a contient donc au moins un élément non nul. Par ailleurs, pour tout couple (r,s) d'éléments de H_a, $c^r(a) \;=\; a \;=\; c^s(a)$, c'est-à-dire que $c^{r-s}(a) \;=\; a$ autrement dit que $r-s \in H_a$. On en déduit donc que H_a est un sous-groupe de $\mathbb{Z}$ (cf. II.1.1.1), différent du singleton $\{0\}$ il existe, par conséquent, un entier $d>0$ tel que

$$H_a \;=\; d\mathbb{Z}\text{(cf. I.3.2.6.)}\,.$$

Lemme II.2.2.1.3 *L'entier d défini dans le lemme II.2.2.1.2, est l'ordre (cf. II.1.2.6) de c dans $\mathcal{S}_n$.*

Preuve : *Si l'on note*

$$H_c \;:=\; \{k \;\in\; \mathbb{Z}\,;\; c^k \;=\; \mathrm{Id}\}\,,$$

démontrer le lemme revient à démontrer que $H_a \;=\; H_c$.

Or il est clair que $H_c \subset H_a$.

Réciproquement, pour tout $k \in H_a$, et pour tout $x \;\in\; [1;n]$,

— si $x \notin S$, $c(x) \;=\; x$ et, par conséquent, $c^k(x) \;=\; x$;

— si $x \;\in\; S$, il existe $p \;\in\; \mathbb{Z}$ tel que $x = c^p(a)$ ce qui implique que

$$c^k(x) \;=\; c^k(c^p(a)) \;=\; c^{p+k}(a) \;=\; c^p(c^k(a)) \;=\; c^p(a) \;=\; x\,.$$

Lemme II.2.2.1.4 *L'entier d défini dans le lemme II.2.2.1.2 est la longueur du cycle c.*

Preuve : *Pour tout couple (p,q) d'éléments de H, il existe un entier k tel que $p-q \;=\; dk$. Il en résulte que*

$$a \;=\; c^{dk}(a) \;=\; c^{p-q}(a)\,;$$

d'où il résulte que $c^p(a) \;=\; c^q(a)$ c'est-à-dire que $\epsilon_a(p) \;=\; \epsilon_a(q)$.

On peut donc définir une application

$$\begin{array}{rccc} \epsilon'_a : & \mathbb{Z}/d\mathbb{Z} & \to & S \\ & k \bmod d & \mapsto & \epsilon_a(k)\,. \end{array} \qquad \text{II.2.2.1.4.1}$$

Pour tout $b \;\in\; S$, il existe $p \;\in\; \mathbb{Z}$ tel que

$$b \;=\; c^p(a) \;=\; \epsilon_a(p) \;=\; \epsilon'_a(p \bmod d)\,,$$

c'est-à-dire que ϵ'_a est surjective.

$$\begin{array}{lrcl} \forall p \in \mathbb{Z},\ \forall q \in \mathbb{Z},\ \Big(& \epsilon'_a(p \bmod d) & = & \epsilon'_a(q \bmod d) \\ \Leftrightarrow & \epsilon_a(p) & = & \epsilon_a(q) \\ \Leftrightarrow & c^p(a) & = & c^q(a) \\ \Leftrightarrow & c^{p-q}(a) & = & a \\ \Leftrightarrow & p-q & \in & H \\ \Leftrightarrow & d & \mid & p-q \\ \Leftrightarrow & p \bmod d & = & q \bmod d \Big) \end{array}$$

d'où l'on tire que ϵ'_a est injective.

L'application ϵ'_a est donc une bijection de $\mathbb{Z}/d\mathbb{Z}$ sur S ce qui implique que

$$\#(S) \ = \ \#(\mathbb{Z}/d\mathbb{Z}) \ = \ d\,.$$

Il suffit maintenant d'appliquer les résultats II.2.2.1.3 et II.2.2.1.4 pour obtenir le théorème.

Remarque II.2.2.2 Pour tout entier $n \geq 1$, tout cycle $c \in \mathcal{S}_n$ de longueur λ et tout élément a du support S de c, on peut définir une bijection $\epsilon'_a : \mathbb{Z}/\lambda\mathbb{Z} \cong S$. Pour tout $k \in \mathbb{Z}$, on a alors $c(\epsilon'_a(\overline{k})) = c^{k+1}(a)$ d'où l'on déduit que $\epsilon'^{,-1}_a \circ c \circ \epsilon'_a$ est la bijection de $\mathbb{Z}/\lambda\mathbb{Z}$ sur lui-même donnée par $\overline{k} \mapsto \overline{k} + \overline{1}$.

On posera alors

$$a_i \ := \ c^i(a)\,,_{0 \,\leq\, i \,\leq\, \lambda-1}$$

et l'on notera

$$c \ = \ (a_0 \ldots a_{\lambda-1})\,. \qquad \text{II.2.2.2.1}$$

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

$$(ab) \ = \ (ba) \text{ et } (ab)^2 \ = \ \mathrm{Id}\,. \qquad \text{II.2.2.2.2}$$

Proposition II.2.2.3 *Étant donné un entier $n \geq 1$, tout cycle $c \in \mathcal{S}_n$ de longueur λ peut être écrit comme un produit de $\lambda - 1$ transpositions.*

Preuve *: On peut, en vertu de la formule II.2.2.2.1 écrire $c = (a_0 \ldots a_{\lambda-1})$ et il est très facile de vérifier qu'alors,*

$$c \ = \ (a_0 a_1) \circ \ldots \circ (a_{\lambda-2} a_{\lambda-1})\,.$$

Proposition II.2.2.4 (Conjugaison de cycles) *Soit $n \in \mathbb{N}^*$.*

i) Deux cycles c_1 et c_2 de $\mathcal{S}_n$ ont même longueur λ, si et seulement s'il existe une permutation $s \in \mathcal{S}_n$ telle que

$$c_2 = s \circ c_1 \circ s^{-1}$$

c'est-à-dire si et seulement si c_1 et c_2 sont conjugués (cf. II.1.3.1.)

ii) Si $c \in \mathcal{S}_n$ est un cycle de support S et de longueur λ, $s \in \mathcal{S}_n$ une permutation et $u \in \mathcal{S}_n$ tels que $u = s \circ c \circ s^{-1}$ alors u est un cycle de longueur λ et de support $s(S)$.

De plus, si c s'écrit $(a_0 \dots a_{\lambda-1})$ u peut s'écrire $(s(a_0) \dots s(a_{\lambda-1}))$.

***Preuve** :*

*i) $*$) (**« même longueur entraîne conjugués »**)*

Il existe des éléments a_1 et a_2 de $[1;n]$ tels que le support de c_1 (resp. c_2) soit $S_1 := O_{c_1}(a_1)$ (resp. $S_2 := O_{c_2}(a_2)$.)

Comme c_1 et c_2 ont même longueur λ, il existe des bijections

$$\epsilon'_1 : \mathbb{Z}/\lambda\mathbb{Z} \to S_1 \text{ et } \epsilon'_2 : \mathbb{Z}/\lambda\mathbb{Z} \to S_2$$

définies comme en II.2.2.1.4.1.

Posons $u := \epsilon'_2 \circ \epsilon'^{,-1}_1$. Il s'ensuit que u est une bijection de S_1 sur S_2.

Pour tout $x \in S_2$, il existe $p \in \mathbb{Z}$ tel que $x = c_2^p(a_2)$. D'où il résulte que

$$\begin{aligned} u[c_1[u^{-1}(x)]] &= \epsilon'_2[\epsilon'^{,-1}_1[c_1[\epsilon'_1[\epsilon'^{,-1}_2(x)]]]] \\ &= \epsilon'_2[\epsilon'^{,-1}_1[c_1[\epsilon'_1(\overline{p})]]] \\ &= \epsilon'_2[\epsilon'^{,-1}_1[c_1(c_1^p(a_1))]] \\ &= \epsilon'_2(\overline{p+1}) \\ &= c_2^{p+1}(a_2) \\ &= c_2(x) \ . \end{aligned}$$

Les complémentaires E_1 de S_1 et E_2 de S_2 dans $[1;n]$ ont même cardinal $n-\lambda$, il existe donc une bijection v de E_1 sur E_2.

On définira s dont la restriction à S_1 est égale à u et la restriction à E_1 est v et l'on vérifiera désormais facilement que

$$c_2 = s \circ c_1 \circ s^{-1} \ .$$

*†) (**« conjugués entraîne même longueur »**)*

Réciproquement, s'il existe $s \in \mathcal{S}_n$ tel que $c_2 = s \circ c_1 \circ s^{-1}$, c_1 et c_2 ont même ordre (cf. II.1.3.3,) c'est-à-dire même longueur (cf. II.2.2.1.)

ii) Pour tout $x \notin s(S)$, $s^{-1}(x) \notin S$, *donc* $c(s^{-1}(x)) = s^{-1}(x)$ *et*

$$u(x) = s[c(s^{-1}(x))] = s(s^{-1}(x)) = x$$

c'est-à-dire qu'une orbite non triviale de u *est nécessairement contenue dans* $s(S)$. *Soit* $b \in s(S)$. *Alors il existe* $a \in S$ *tel que* $b = s(a)$. *Pour tout* $y \in s(S)$, *il existe* $x \in S$ *tel que* $y = s(x)$. *Or comme* c *est un cycle, il existe* $k \in \mathbb{Z}$ *tel que* $x = c^k(a)$ *d'où*

$$y = s(c^k(a)) = s[c^k(s^{-1}(x))] = u^k(x)$$

c'est-à-dire que $s(S)$ *est l'orbite de* x *pour* u *donc* u *n'a qu'une orbite non triviale ;* u *est donc un cycle.*

On peut indifféremment utiliser la proposition II.2.2.4 pour dire que c *et* u *ont même longueur ou dire que* s *étant une bijection,* $\#(S) = \#(s(S))$.

Enfin la notation $c = (a_0 \dots a_{\lambda-1})$ *signifie que, pour tout* $1 \leq i < \lambda$, $a_{i+1} = c(a_i) = c^i(a_0)$. *Or*

$$u^i(s(a_0)) = s[c^i(s^{-1}(s(a_0)))] = s(c^i(a_0)) = s(a_i)$$

c'est-à-dire qu'on peut bien écrire

$$u = (s(a_0) \dots s(a_{\lambda-1}))\ .$$

Proposition II.2.2.5 *Étant donnés deux cycles* c_1 *et* c_2 *du groupe symétrique* $\mathcal{S}_n$ $n \geq 1$, *de supports disjoints (dont l'intersection est vide) alors* $c_1 \circ c_2 = c_2 \circ c_1$.

Preuve : *On laisse le soin au lecteur de démontrer ce résultat.*

II.2.3 . −Décomposition d'une permutation en produit de cycles

Proposition II.2.3.1 *Pour tout entier naturel* $n \geq 1$ *et 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. II.2.1.6.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 II.2.3.2 *Pour tout entier naturel $n \geq 1$ et 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 II.2.3.3 *Pour tout entier naturel $n \geq 1$ toute permutation $s \in \mathcal{S}_n$, s'écrit comme un produit de transpositions.*

Preuve : *Cet énoncé est une conséquence des propositions II.2.3.1 et II.2.2.3.*

Définition II.2.3.4 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 l_i désigne la longueur de c_i on ait, pour tout $1 \leq i < d\, l_i \leq l_{i+1}$. On appelle alors le d-uplet $(l_1, \ldots, l_d)$ le *type cyclique* de s.

On pourra fixer, par convention, que le type cyclique de l'identité est $\emptyset$.

Proposition II.2.3.5 *Étant donnés deux éléments s_1 et s_2 du groupe symétrique $\mathcal{S}_n$, $n \geq 1$ étant un entier naturel les assertions suivantes sont équivalentes :*

a) *s_1 et s_2 sont conjugués (cf. II.1.3.1 ;)*

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 la proposition II.2.2.4 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 la proposition II.2.2.4, 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, d'après la proposition II.2.2.4 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 II.2.3.6 *L'ordre d'une permutation s de type cyclique $(l_1, \ldots, l_d)$ est le **Ppcm** (cf. I.3.1.8,) des l_i.*

***Preuve** : (cf. TD n° IV, exercice H, question 1),) (cf. TD n° IV, exercice H, question 1), b).)*

i) Si s est de type cyclique $(l_1, \ldots, l_d)$, il existe des cycles c_i ,$_{1\leq i\leq d}$ de longueur respective l_i, à supports deux à deux disjoints et tels que

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

*Notons $m \ := \ [l_1, \ldots, l_d]$ le **Ppcm** des l_i. Par définition, $l_i | m$, pour tout $1 \ \leq \ i \ \leq \ d$ donc $c_i^m \ = \ \mathrm{Id}$ (cf. II.1.2.6.) Comme 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. II.2.2.5,) 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* l_i *de* c_i *divise* k. *En bref,* $s^k = \mathrm{Id}$ *implique que* k *est divisible par chacun des* l_i *c'est-à-dire divisible par* m *c'est-à-dire que* m *divise l'ordre de* s.

II.2.4 . −Signature et groupe alterné

Définition II.2.4.1 Soient $n \geq 1$ un entier naturel et $s \in \mathcal{S}_n$ une permutation :

i) On note $\nu(s)$ le nombre d'orbites (cf. II.2.1.6.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 II.2.4.2 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, $\sigma(s) = (-1)^{n-1}$.

Proposition II.2.4.3 *Pour tout entier* $n \geq 1$, *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* $l := \#(O_s(a))$. *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* l. *Il est par conséquent, en vertu du théorème II.2.2.1 d'ordre* l.

Puisque $b \in O_s(a)$, *il existe* $k \in \mathbb{Z}$ *tel que* $b = s^k(a) = c^k(a)$ *et de même il existe* $k' \in \mathbb{Z}$ *tel que* $a = s^{k'}(b) = c^{k'}(b)$. *Notons* p *(resp.* q*) le reste de la division euclidienne de* k *(resp.* k'*) par* l. *Puisque* c *est d'ordre* l, *on a :*

$$b = c^p(a) \text{ et } a = c^q(b) .$$

Le théorème de la division euclidienne (cf. I.3.2.3,) et le fait que $a \neq b$ *donnent les encadrement :*

$$0 < p < l \text{ et } 0 < q < l \,. \qquad 1$$

Par ailleurs,

$$a = c^q(b) = c^q(c^p(a)) = c^{p+q}(a)$$

d'où l'on déduit facilement que, pour tout $x \in O_c(a)$, $c^{p+q}(x) = x$ *et par conséquent* $l|p+q$. *Les encadrements 1 impliquent alors que* $p+q = l$.

Cherchons maintenant à déterminer l'orbite $O_{sot}(a)$. *On a tout d'abord,*

$$s \circ t(a) = s(b) = s^{p+1}(a) = c^{p+1}(a) \,.$$

Pour tout $1 \leq i < q$, *on a*

$$c^{p+i}(a) \neq a \text{ et } c^{p+i}(a) \neq b \,.$$

En effet, $c^{p+i}(a) = a$ *impliquerait* $l|p+i$ *or* $0 < p+i < l$ *ce qui est donc impossible. D'autre part,* $c^{p+i}(a) = b$ *impliquerait* $c^i(a) = a$ *c'est-à-dire* $l|i$ *qui est encore impossible puisque* $0 < i < q < l$.

Il en résulte que, pour tout $1 \leq i < q$, $t(c^{p+i}(a)) = c^{p+i}(a)$ *c'est-à-dire que*

$$s \circ t(c^{p+i}(a)) = s(c^{p+i}(a)) = s^{p+i+1}(a) \,.$$

On en déduit que

$$O_{sot}(a)) = \left\{ s^{p+i}(a) \,; lleq1iq \right\} \subset O_s(a) \qquad 2$$

d'où il résulte, en particulier, que

$$\#(O_{sot}(a)) = q \,. \qquad 3$$

On montre de même que

$$O_{sot}(b) = \left\{ c^i(a) \,; lleq1ip \right\} \subset O_s(a) \qquad 4$$

d'où il résulte, en particulier, que

$$\#(O_{sot}(b)) = p \,. \qquad 5$$

Il résulte de ce qui précède que

$$O_{sot}(a) \cap O_{sot}(b) = \emptyset$$

et que, par conséquent,

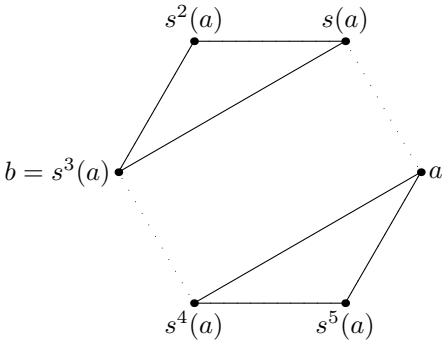
$$\#(O_{s\circ t}(a) \cup O_{s\circ t}(b)) \;=\; \#(O_{s\circ t}(a)) \;+\; \#(O_{s\circ t}(b)) \;=\; p+q \;=\; \#(O_s(a))\,.$$

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

$$l \;=\; 6 \text{ et } p \;=\; q \;=\; 3 \;:$$



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*

$$\nu(s \circ t) \;=\; \nu(s) \;+\; 1\,. \qquad 6$$

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*

$$p \;:=\; \#(O_s(a)) \text{ et } q \;:=\; \#(O_s(b))$$

et cherchons à déterminer $O_{s\circ t}(a)$. *Tout d'abord,* $s \circ t(a) \;=\; s(b)$ *et*

$$\begin{array}{rl} & \forall 1 \leq i < q \quad , \quad s^i(b) \in O_s(b), s^i(b) \neq b, s^i(b) \neq a \\ \Rightarrow & \forall 1 \leq i < q \quad , \quad t(s^i(b)) \;=\; s^i(b) \\ \Rightarrow & \forall 1 \leq i < q \quad , \quad s \circ t(s^i(b)) \;=\; s^{i+1}(b)\,. \end{array}$$

De plus

$$s \circ t(s^q(b)) \;=\; s \circ t(b) \;=\; s(a)\,.$$

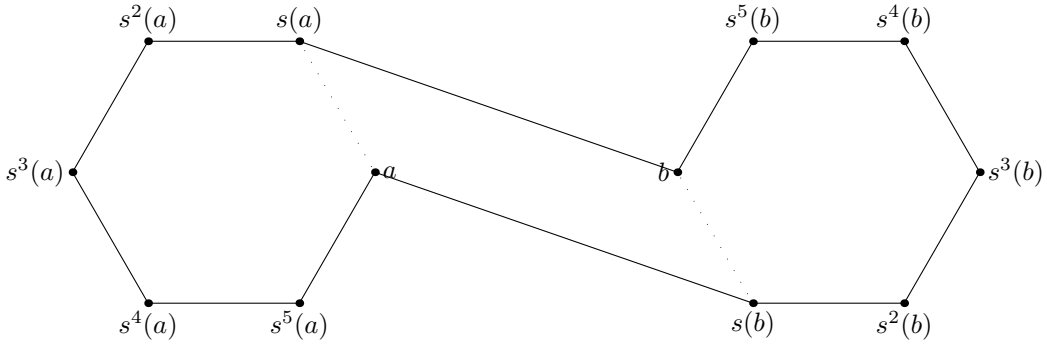
D'où :

$$\begin{array}{rl} & \forall 1 \leq i < p \quad , \quad s^i(a) \in O_s(a), s^i(a) \neq a, s^i(a) \neq b \\ \Rightarrow & \forall 1 \leq i < p \quad , \quad t(s^i(a)) \;=\; s^i(a) \\ \Rightarrow & \forall 1 \leq i < p \quad , \quad s \circ t(s^i(a)) \;=\; s^{i+1}(a)\,. \end{array}$$

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 $p \;=\; q = \;6$:



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 II.2.4.4 *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. II.2.4.1.ii),) que* σ *est à valeurs dans* $\{-1,1\}$.

Pour $n \;=\; 1$, *on a* $\sigma(\mathrm{Id}) \;=\; 1$ *(cf. II.2.4.2) ce qui prouve que* σ *est bien un morphisme.*

Pour $n \;\geq\; 2$, *soit* (s_1, s_2) *un couple d'éléments de* $\mathcal{S}_n$. *Il existe un entier* $d \;>\; 0$ *et des transpositions* $t_{i\,},{}_{1\leq i\leq d} \;\in\; \mathcal{S}_n$, *tels que* $s_2 \;=\; \prod_{i=1}^{d} t_i$ *(cf. II.2.3.3.)*

On a alors, d'après la proposition II.2.4.3 appliquée d *fois :*

$$\begin{aligned}\sigma(s_1\circ s_2) \;&=\; \sigma(s_1) * \prod_{i=1}^{d}\sigma(t_i)\\ &=\; \sigma(s_1)\sigma(s_2)\;.\end{aligned}$$

Définition II.2.4.5 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 II.2.4.6 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 II.2.4.7 (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. II.1.3.8) est isomorphe au groupe $\mathbb{Z}/2\mathbb{Z}$ et, par conséquent,

$$\#\big(\mathcal{A}_n\big) \;=\; \frac{\#\big(\mathcal{S}_n\big)}{2} \;=\; \frac{n!}{2}\,.$$

Preuve *:*

i) Comme $\mathcal{A}_n \;=\; \operatorname{Ker}\sigma$, on peut se rapporter au résultat II.1.3.6.b).

ii) Pour $n \geq 2$, $\mathcal{S}_n$ contient des transpositions et, par conséquent, σ à valeurs dans $\{-1;1\}$ est surjective (cf. II.2.4.2.)

Par la proposition II.1.3.7.ii)on 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 II.1.2.2.iv).

II.3 . −Actions de groupe

Notation II.3.1 Étant donné un ensemble E on notera $(\mathcal{S}(E),\circ)$ ou simplement $\mathcal{S}(E)$ le groupe des bijections de E dans lui-même muni de la loi de composition des applications .

Définition II.3.2 (Action de groupe) Étant donné un ensemble E et un groupe $(G,*)$ on dit que G *agit sur* E ou que E est muni d'une *action* de G, s'il existe un morphisme de groupe (cf. 0.5.6.ii),)

$$\phi \;:\; (G,*) \;\to\; (\mathcal{S}(E),\circ)\,.$$

Remarque II.3.3 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. 0.5.8.i);) et $\forall g \in G,\ \phi(g^{-1}) \,=\, \phi(g)^{-1}$ (cf. 0.5.8.ii).)

Notation II.3.4 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 II.3.5 Pour $n \,\in\, \mathbb{N}^*$:

a) On a défini le groupe symétrique $\mathcal{S}_n$ comme le groupe $\mathcal{S}([1;n])$ (cf. II.2.1.1.ii).) On a donc tautologiquement une action de $\mathcal{S}_n$ sur $[1;n]$.

b) Étant donné une permutation $s \,\in\, \mathcal{S}_n$, posons

$$\forall K \in \mathbb{Z},\ \forall x \in [1;n],\ k\cdot x \,:=\, s^k(x)\ .$$

C'est l'action de $\mathbb{Z}$ sur $[1;n]$ donnée par le morphisme

$$\epsilon_s \,:\, (\mathbb{Z},+) \,\to\, (\mathcal{S}_n,\circ) \,=\, \big(\mathcal{S}([1;n]),\circ\big)\ ,\ k \,\mapsto\, s^k$$

(cf. TD n° II, exercice B, question 3).)

c) Si dans l'exemple b), la permutation s est d'ordre $d \,\in\, \mathbb{N}^*$ le morphisme ϵ_s se factorise en un morphisme $\overline{\epsilon}_s \,:\, \mathbb{Z}/d\mathbb{Z} \,\to\, \mathcal{S}_n$ donnant une action du groupe $(\mathbb{Z}/d\mathbb{Z},+)$ sur l'ensemble $[1;n]$.

d) Pour $(G,*)$ un groupe, on peut définir l'action de G sur lui-même par conjugaison :

$$\forall g \in G,\ \forall x \in G,\ g\cdot x \,:=\, g*x*g^{-1}\ .$$

Il n'est pas difficile de vérifier qu'il s'agit bien d'une action.

Lemme II.3.6 *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. 0.2.2.v),) sur E.

Preuve *: C'est un exercice.*

Définition II.3.7 (Orbite) Étant donnés un groupe G agissant sur un ensemble E, les classes déquivalence pour la relation définie au lemme II.3.6 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 $O(x)$ et l'on a :

$$O(x) = \{g \cdot x \ , \ g \in G\} \ .$$

Exemple II.3.8 Étant donnée un entier $n \in \mathbb{N}^*$, une permutation $s \in \mathcal{S}_n$, un élément $x \in [1;n]$, l'orbite de $O_s(x)$ x sous s définie en II.2.1.6.i) n'est autre que l'orbite de $O(x)$ x au sens de la définition II.3.7 pour l'action de $\mathbb{Z}$ sur $[1;n]$ définie par ϵ_s comme en II.3.5.b) ou encore de manière équivalente pour l'action définie par $\overline{\epsilon}_s$ comme en II.3.5.c).

Lemme II.3.9 *Étant donnée une action d'un groupe G sur un ensemble E, pour tout $x \in E$, l'ensemble :*

$$\mathrm{Stab}_G(x) := \{g \in G \ ; \ g \cdot x = x\} \qquad \textit{II.3.9.1}$$

est un sous-groupe de G.

Définition II.3.10 (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 II.3.9.1 est appelé *stabilisateur* de x.

Théorème II.3.11 *Étant donnée une action d'un groupe G sur un ensemble E, pour tout $x \in E$, l'application naturelle*

$$\phi_x \ : \ G \ \to \ O(x) \ , \ g \ \mapsto \ g \cdot x$$

induit une bijection

$$\overline{\phi}_x \ : \ G/_g\mathrm{Stab}_G(x) \ \to \ O(x)$$

où $G/_g\mathrm{Stab}_G(x)$ est l'ensemble des classes d'équivalences pour la relations $\sim_g$ définie en II.1.2.1.

Preuve *: Pour tout $x \in E$:*

$$\begin{array}{lrcl}
\forall g \in G, \ \forall h \in G, & \phi_x(g) & = & \phi_x(h) \\
\Leftrightarrow & g \cdot x & = & h \cdot x \\
\Leftrightarrow & (g^{-1} * h) \cdot x & = & x \\
\Leftrightarrow & g^{-1} * h & \in & \mathrm{Stab}_G(x) \\
\Leftrightarrow & g & \sim_{g,\mathrm{Stab}_G(x)} & h
\end{array}$$

Il existe donc une unique application injective $\overline{\phi}_x \ : \ G/_g\mathrm{Stab}_G(x) \ \to \ O(x)$ telle que

$$\forall g \in G, \ \overline{\phi}_x(g\mathrm{Stab}_G(x)) \ = \ \phi_x(g) \ .$$

Comme ϕ_x est tautologiquement surjective, il en est de même de $\overline{\phi}_x$.

Corollaire II.3.12 *Sous les hypothèses du théorème II.3.11, 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 du théorème II.3.11 et de II.1.2.2.iv).*

III . −Arithmétique des polynômes

III.1 . −Anneau des polynômes à une indéterminée

Dans toute cette section (III.1), $(A, +_A, *_A, 0_A, 1_A)$ est un anneau commutatif (cf. 0.5.9.i).)

Définition III.1.1 i) On rappelle qu'une *suite à valeurs dans A* est une application $\mathbb{N} \to A$. On note le plus souvent $\alpha_n \in A$ et on appelle *$n^{ième}$ terme général* l'image d'un entier $n \in \mathbb{N}$ par la suite α.

ii) On dira qu'une suite à valeurs dans A de terme général α_n est *presque nulle* s'il existe un entier n_0 tel que pour tout $n > n_0$, $\alpha_n \ = \ 0$.

Notation III.1.2 On notera $A^{\mathbb{N}}$ (resp. $A^{\mathbb{N},0}$) l'ensemble des suites à valeurs dans A (resp. l'ensemble des suites presque nulles à valeurs dans A.) 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

$$\forall n \in \mathbb{N},\ \zeta_n \ = \ 0 \text{ (resp. } \upsilon_0 \ := \ 1_A \ , \ \forall n \in \mathbb{N},\ n \geq 1 \ , \ \upsilon_n \ := \ 0 \ .)$$

On a bien entendu

$$\zeta \ \in \ A^{\mathbb{N},0} \text{ et } \upsilon \ \in \ A^{\mathbb{N},0} \ .$$

Définition III.1.3 (Degré/valuation) Pour toute suite presque nulle $\left(\alpha_n\right)_{,n\in\mathbb{N}} \in A^{\mathbb{N},0}$, $\alpha \ \neq \ \zeta$, l'ensemble $\{n \ \in \ \mathbb{N} \ ; \ \alpha_n \ \neq \ 0\}$ est une partie non vide et majorée de $\mathbb{N}$. Elle admet donc un plus grand élément (cf. I.1.2.8,) qu'on appellera *degré* de α et qu'on notera $\deg(\alpha)$; et un plus petit élément (cf. I.1.2.7,) qu'on appellera *valuation* de α et qu'on notera $\mathrm{val}(\alpha)$.

Par convention on posera

$$\deg(\zeta) \ := \ -\infty \text{ et } \mathrm{val}(\zeta) \ = \ +\infty \ .$$

Sit on note $\overline{\mathbb{N}} \ := \ \mathbb{N} \ \cup \ \{-\infty, +\infty\}$ $\deg(\cdot)$ et $\mathrm{val}(\cdot)$ sont des applications de $A^{\mathbb{N},0}$ 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

$$\forall n \in \mathbb{N},\; -\infty \;<\; n \;<\; +\infty\,.$$

Proposition III.1.4 *i) Si on définit, pour tout* $(\alpha, \beta) \in A^{\mathbb{N}} \times A^{\mathbb{N}}$:

$$(\alpha \;+_{A^{\mathbb{N}}}\; \beta)_n \;:=\; \alpha_n \;+_A\; \beta_n\,, \qquad 1$$

$(A^{\mathbb{N}}, +_{A^{\mathbb{N}}})$ *a une structure de groupe abélien dont* ζ *est lélément neutre.*

ii) L'ensemble $A^{\mathbb{N},0}$ *est un sous-groupe de* $(A^{\mathbb{N}}, +_{A^{\mathbb{N}}})$ *pour la structure définie ci-dessus.*

iii) De plus le groupe abélien $A^{\mathbb{N}}$ *(resp.* $A^{\mathbb{N},0}$*,) est muni d'une loi externe :*

$$\begin{array}{rcl} \cdot : & A \times A^{\mathbb{N}} & \longrightarrow \quad A^{\mathbb{N}} \\ & & \longmapsto \quad (\textit{resp.}\cdot \,:\, A \times A^{\mathbb{N},0} \,\to\, A^{\mathbb{N},0}) \end{array} \qquad 1$$

définie par :

$$\forall a \in A,\; \forall \left(\alpha_n\right)_{,n\in\mathbb{N}} \in A^{\mathbb{N}},\quad (a \cdot \alpha)_n \quad := \quad a \;*_A\; \alpha_n\,;$$

qui vérifie les axiomes :

$$\forall a \in A,\; \forall b \in A,\; \forall \left(\alpha_n\right)_{,n\in\mathbb{N}} \in A^{\mathbb{N}}(\textit{resp.}\; \in A^{\mathbb{N},0}),\; \forall \left(\beta_n\right)_{,n\in\mathbb{N}} \in A^{\mathbb{N}}(\textit{resp.}\; \in A^{\mathbb{N},0}),\; :$$

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 : *La vérification est immédiate et laissée en exercice ; ce résultat étant à rapprocher de la proposition I.3.5.10.*

Remarque III.1.5 On dit que les groupes abéliens $A^{\mathbb{N}}$ et $A^{\mathbb{N},0}$ munis de la loi externe $\cdot$ définie en III.1.4.iii).1 et vérifiant les axiomes III.1.4.iii).Mod$_1$) à III.1.4.iii).Mod$_4$) ont une structure de A-*module*. À noter que si A est un corps, cette structure n'est autre qu'une structure d'espace vectoriel.

Notation III.1.6 Notons que pour tout $n \in \mathbb{N}$, $\{(k,\ell) \in \mathbb{N}\times\mathbb{N} \ ; \ k+\ell = n\}$ est un ensemble fini et que par conséquent pour tout $(\alpha,\beta) \in A^{\mathbb{N}} \times A^{\mathbb{N}}$, de terme général (α_n, β_n) l'élément $\alpha *_{A^{\mathbb{N}}} \beta$ de $A^{\mathbb{N}}$ donné par :

$$(\alpha *_{A^{\mathbb{N}}} \beta)_n := \sum_{k+\ell=n} \alpha_k *_A \beta_\ell \qquad \text{III.1.6.1}$$

est bien défini.

Lemme III.1.7 *Pour tout $\alpha \in A^{\mathbb{N},0}$ et tout $\beta \in A^{\mathbb{N},0}$, $\alpha *_{A^{\mathbb{N}}} \beta \in A^{\mathbb{N},0}$ et :*

$$\deg(\alpha *_{A^{\mathbb{N}}} \beta) \ \leq \ \deg(\alpha) \ + \ \deg(\beta) \qquad \textit{III.1.7.1}$$

Preuve :

$$\begin{array}{ll}
\forall \alpha \in A^{\mathbb{N},0}, \forall \beta \in A^{\mathbb{N},0}, & \\
\forall n \in \mathbb{N}, \ n > \deg(\alpha)+\deg(\beta) & \\
\forall k \in \mathbb{N}, \ \forall \ell \in \mathbb{N}, & k+\ell = n \\
\Rightarrow & k > \deg(\alpha) \ \text{ou} \ \ell > \deg(\beta) \\
\Rightarrow & \alpha_k = 0 \ \text{ou} \ \beta_\ell = 0 \\
\Rightarrow & \alpha_k *_A \beta_\ell = 0 \\
\Rightarrow & (\alpha *_{A^{\mathbb{N}}} \beta)_n = 0 \\
\Rightarrow & (\alpha *_{A^{\mathbb{N}}} \beta) \in A^{\mathbb{N},0} \ .
\end{array}$$

Proposition III.1.8 *i) L'ensemble $A^{\mathbb{N}}$ (resp. $A^{\mathbb{N},0}$) muni de l'addition $+_{A^{\mathbb{N}}}$ définie en III.1.4.i).1 et de la multiplication $*_{A^{\mathbb{N},0}}$ définie en III.1.6.1 est un anneau commutatif délément neutre ζ (resp. υ) pour l'addition (resp. pour la multiplication.)*

ii) L'application

$$i_A \ : \ A \ \to \ A^{\mathbb{N}} \ (\textit{resp.} \ A^{\mathbb{N},0}) \ , \ a \ \mapsto \ a \cdot \upsilon \qquad \textit{1}$$

(où $\cdot$ est la loi externe définie en III.1.4.iii).1 est un morphisme d'anneaux injectif appelé morphisme structural.

Preuve *:*

i) Il faut vérifier que les lois $+_{A^{\mathbb{N}}}$ et $*_{A^{\mathbb{N}}}$ satisfont aux axiomes définissant les anneaux (cf. 0.5.9.i);) ce qui consiste en une série de calculs sans grande difficulté.

Cependant, le seul point délicat et qui mérite d'être souligné est que $*_{A^{\mathbb{N}}}$ est bien une loi interne sur $A^{\mathbb{N},0}$. Ceci est assuré par le lemme III.1.7.

ii) C'est également une série de calculs sans difficulté.

Proposition III.1.9 *i) Pour tout $(\alpha, \beta) \in A^{\mathbb{N},0} \times A^{\mathbb{N},0}$, on a :*

$$\deg(\alpha+\beta) \leq \max(\deg(\alpha),\deg(\beta)) \text{ et } \big(\deg(\alpha) \neq \deg(\beta) \Rightarrow \deg(\alpha+\beta) = \max(\deg(\alpha),\deg(\beta))\,;\big) \qquad 1$$

$$\deg(\alpha * \beta) \leq \deg(\alpha) + \deg(\beta)\,; \qquad 2$$

$$\mathrm{val}(\alpha+\beta) \geq \min(\mathrm{val}(\alpha),\mathrm{val}(\beta)) \text{ et } \big(\mathrm{val}(\alpha) \neq \mathrm{val}(\beta) \Rightarrow \mathrm{val}(\alpha+\beta) = \min(\mathrm{val}(\alpha),\mathrm{val}(\beta))\,;\big) \qquad 3$$

$$\mathrm{val}(\alpha * \beta) \geq \mathrm{val}(\alpha) + \mathrm{val}(\beta)\,. \qquad 4$$

ii) Si A est intègre (cf. 0.5.9.ii),) on a égalité dans les formules i).2 et i).4.

Preuve *: On va démontrer les formules i).1 et i).2 les formules i).3 et i).4 se démontrant exactement sur le même modèle.*

a) ***(i).1)***

$$\begin{array}{lrcl}
\forall \alpha \in A^{\mathbb{N},0}, \forall \beta \in A^{\mathbb{N},0}, \forall n \in \mathbb{N}, & n & \geq & \max(\deg(\alpha),\deg(\beta)) \\
\Rightarrow & \alpha_n = 0 & \text{et} & \beta_n = 0 \\
\Rightarrow & (\alpha +_{A^{\mathbb{N}}} \beta)_n = \alpha_n + \beta_n & = & 0 \\
\Rightarrow & \deg(\alpha +_{A^{\mathbb{N}}} \beta) & \leq & \max(\deg(\alpha),\deg(\beta))\,.
\end{array} \qquad 1$$

Par ailleurs, notons $m := \max(\deg(\alpha),\deg(\beta))$. Alors :

$$\begin{array}{rrcl}
 & \deg(\alpha) & \neq & \deg(\beta) \\
\Rightarrow & \deg(\alpha) = m \text{ et } \beta_m = 0 & \text{ou} & \deg(\beta) = m \text{ et } \alpha_m = 0 \\
\Rightarrow & (\alpha+\beta)_m = \alpha_m \neq 0 & \text{ou} & (\alpha+\beta)_m = \beta_m \neq 0 \\
\Rightarrow & \deg(\alpha+\beta) & \geq & m
\end{array}$$

ce qui combiné avec 1 donne l'égalité demandée.

*b) **(i).2)***

On a déjà montré en III.1.7.1 $\deg(\alpha * \beta) \leq \deg(\alpha) + \deg(\beta)$. *Or il résulte de la définition III.1.6.1 que*

$$(\alpha * \beta)_{\deg(\alpha)+\deg(\beta)} = \alpha_{\deg(\alpha)} * \beta_{\deg(\beta)}$$

qui est non nul si A *est intègre.*

Corollaire III.1.10 *Si* A *est un anneau intègre et en particulier un corps :*

*i) **(Intégrité)***
L'anneau $(A^{\mathbb{N},0}, +, *)$ *est intègre.*

*ii) **(Inversibles)***
L'ensemble $A^{\mathbb{N},0\times}$ *des inversibles de l'anneau* $A^{\mathbb{N},0}$ *s'identifie à* $A^\times$;

*iii) **(Divisibilité)***

$$\forall \alpha \in A^{\mathbb{N},0}, \forall \beta \in A^{\mathbb{N},0}, \left(\alpha | \beta \text{ et } \beta \neq 0 \Rightarrow \deg(\alpha) \leq \deg(\beta)\ .\right)$$

***Preuve** :*

i) Pour tout $(\alpha, \beta) \in A^{\mathbb{N},0} \times A^{\mathbb{N},0}$, *puisque* A *est intègre,*

$$\alpha * \beta = 0 \Rightarrow \deg(\alpha) + \deg(\beta) = \deg(\alpha * \beta) = -\infty$$

(cf. III.1.9.i).2 et III.1.9.ii).) Il s'ensuit que

$$\deg(\alpha) = -\infty \text{ ou } \deg(\beta) = -\infty \Rightarrow \alpha = 0 \text{ ou } \beta = 0\ .$$

ii) Pour tout $(\alpha, \beta) \in A^{\mathbb{N},0} \times A^{\mathbb{N},0}$, *dans le cas où* A *est intègre, (cf. III.1.9.ii),)*

$$\alpha *_{A^{\mathbb{N}}} \beta = \upsilon \Rightarrow \deg(\alpha) + \deg(\beta) = 0 \Rightarrow \deg(\alpha) = \deg(\beta) = 0\ .$$

On a alors

$$\alpha_0 *_A \beta_0 = 1 \Rightarrow \alpha_0 \in A^\times \text{ et } \beta_0 \in A^\times$$

et $\alpha = i_A(\alpha_0)\ ,\ \beta = i_A(\beta_0)$.

iii) Est une conséquence de III.1.9.i).2.

Exemple III.1.11 Notons que dans le corollaire ci-dessus on a besoin de lhypothèse A intègre. Considérons en effet 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 $\deg(\alpha) = \deg(\beta) = 1$.

Définition III.1.12 On appelle *polynôme à coefficients dans A et à une indéterminée* un élément de l'anneau

$$(A^{\mathbb{N},0}, +_{A^{\mathbb{N}}}, *_{A^{\mathbb{N}}}, \zeta, \upsilon) .$$

Notation III.1.13 On abandonnera progressivement les notations $+_{A^{\mathbb{N}}}, *_{A^{\mathbb{N}}}, \zeta, \upsilon$ au profit de $+, *, 0, 1$ si aucune confusion n'est à craindre.

Par ailleurs on notera :

$$X := \left(X_n\right)_{,n\in\mathbb{N}} \mid X_1 = 1_A \, , \, \forall n \in \mathbb{N}, \, n \neq 1 \, , \, X_n = 0 \, . \qquad \text{III.1.13.1}$$

Lemme III.1.14 *Pour tout $k \in \mathbb{N}^*$ X^k est la suite $\left(X_n^k\right)_{,n\in\mathbb{N}}$ telle que*

$$\forall n \in \mathbb{N}, \, n \neq k \Rightarrow X_n^k = 0 \, X_k^k = 1 \, .$$

Preuve *: Pour $k = 1$ le résultat est tautologique (cf. III.1.13.1.) Or $X^{k+1} = X * X^k$ c'est-à-dire que*

$$\forall n \in \mathbb{N}, \, X_n^{k+1} = \sum_{p+q=n} X_p X_q^k = X_1 X_{n-1}^k = X_{n-1}^k$$

si bien que si on suppose que X^k est de la forme donnée dans l'énoncé du lemme il en est de même de X^{k+1}. Ceci établit le résultat par récurrence.

Proposition III.1.15 *L'élément $X \in A^{\mathbb{N},0}$ étant défini comme en III.1.13.1, posons $X^0 := 1 := \upsilon$. Alors $\{X^k\}_{k\in\mathbb{N}}$ est la base de $A^{\mathbb{N},0}$ telle que*

$$\forall \left(\alpha_n\right)_{,n\in\mathbb{N}} \in A^{\mathbb{N},0}, \, \alpha = \sum_{n=0}^{\deg(\alpha)} \alpha_n X^n \, .$$

Preuve *: C'est un exercice sur les définitions.*

Notation III.1.16 L'anneau $A^{\mathbb{N},0}$ des polynômes à une indéterminée et à coefficients dans A est usuelllement noté $A[X]$ et un élément $\alpha \in A[x]$ est noté :

$$P := \sum_{i=0}^{\deg(\alpha)} \alpha_i X^i .$$

On omettra bien souvent d'écrire le morphisme injectif i_A (cf. III.1.8.ii).1,) et on écrira simplement $A \subset A[X]$ en identifiant A à son image par i_A c'est-à-dire aux polynômes de degré 0.

Proposition III.1.17 (Propriété universelle de l'anneau des polynômes) *Rappelons que l'on note*

$$i_A : A \to A[X]$$

le morphisme structural défini en III.1.8.ii).1. Pour tout morphisme d'anneaux $f : A \to B$ et tout élément $b \in B$, il existe un unique morphisme d'anneaux

$$\phi_b : A[X] \to B \text{ tel que } \phi_b(X) = b \text{ et } f \circ i_A = \phi_b .$$

Ceci entraîne en particulier que :

$$\forall \alpha \in A[X], \alpha = \sum_{i=0}^{\deg(\alpha)} \alpha_i X^i \Rightarrow \phi_b(\alpha) = \sum_{i=0}^{\deg(\alpha)} f(\alpha_i) *_B b^i . \qquad \text{III.1.17.1}$$

***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 $\forall n \in \mathbb{N}^*, \phi_b(X^k) = b^k$. Puisque ϕ_b est un morphisme d'anneaux,

$$\phi_b(1_{A[X]} = 1_B \Rightarrow \phi_b(\upsilon) = 1_B \Rightarrow \phi_b(X^0) = 1_B$$

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 III.1.4.iii).1 $\phi_b \circ i_A = f$ entraîne :

$$\begin{array}{lll} \forall \alpha \in A[X], \forall \beta \in A[X], & & \\ \forall a \in A, \forall b \in A, & \phi_b(a \cdot \alpha + b \cdot \beta) & = \phi_b(i_A(a) * \alpha + i_A(b) * \beta) \\ & & = \phi_b(i_A(a)) *_B \phi_b(\alpha) +_B \phi_b(i_A(b)) *_B \phi_b(\beta) \\ & & = f(a) *_B \phi_b(\alpha) +_B f(b) *_B \phi_b(\beta) . \end{array}$$

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 $\forall \alpha \in A[X], \forall \beta \in A[X]$, $\phi_b(\alpha +_{A[X]} \beta) = \phi_b(\alpha) +_B \phi_b(\beta)$ si bien que l'axiome 0.5.9.v).MorAnn$_1$).

Par ailleurs :

$$\forall \alpha \in A[X], \alpha = \sum_{i=0}^{\deg(\alpha)} \alpha_i X^i$$

$$\forall \beta \in A[X], \beta = \sum_{i=0}^{\deg(\beta)} \beta_i X^i \quad \phi_b(\alpha *_{A[X]} \beta) = \sum_{i=0}^{\deg(\alpha)+\deg(\beta)} \Big(\sum_{j+k=i} \alpha_j \beta_k \Big) \cdot X^i$$

$$= \sum_{i=0}^{\deg(\alpha)+\deg(\beta)} f\Big(\sum_{j+k=i} \alpha_j \beta_k \Big) *_B b^i$$

$$= \Big(\sum_{i=0}^{\deg(\alpha)} f(\alpha_i) *_B b^i \Big) *_B \Big(\sum_{i=0}^{\deg(\beta)} f(\beta_i) *_B b^i \Big)$$

$$= \phi_b(\alpha) *_B \phi_b(\beta)$$

ce qui prouve que ϕ_b vérifie l'axiome 0.5.9.v).MorAnn$_2$).

Il est enfin clair que l'axiome 0.5.9.v).MorAnn$_3$) est satisfait.

Corollaire III.1.18 (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 :

$$\forall \alpha \in A[X], \alpha := \sum_{i=0}^{\deg(\alpha)} \alpha_i X^i \Rightarrow f[X](\alpha) = \sum_{i=0}^{\deg(\alpha)} f(\alpha_i) X^i \,. \qquad \textit{III.1.18.1}$$

***Preuve** : Il suffit d'appliquer la proposition III.1.17 au morphisme d'anneaux $i_B \circ f : A \to B[X]$ et à l'élément $X \in B[X]$.*

Exemple III.1.19 Le corollaire III.1.18 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 III.1.18 pour en déduire un morphisme $\sigma[X] : \mathbb{C}[X] \to \mathbb{C}[X]$ qui vérifie, en vertu de III.1.18.1

$$\sigma[X]\big(\sum_{i=0}^{d} \alpha_i X^i\big) = \sum_{i=0}^{d} \sigma(\alpha_i) X^i$$

qu'on écrira de manière plus usuelle :

$$\overline{\sum_{i=0}^{d} \alpha_i X^i} = \sum_{i=0}^{d} \overline{\alpha_i} X^i \,.$$

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 $P := \sum_{i=0}^{d} a_i X^i$ à coefficients entiers le polynôme $\overline{P} = \sum_{i=0}^{d} a_i \bmod n X^i$ 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 paragraphe III.2.

Corollaire III.1.20 (Évaluation) *Pour tout $a \in A$, il existe un unique morphisme d'anneaux*

$$\mathrm{ev}_a : A[X] \to A \mid \mathrm{ev}_a(X) = a \text{ et } \mathrm{ev}_a \circ i_A = \mathrm{Id}_A$$

et en particulier :

$$\forall \alpha \in A[X], \alpha = \sum_{i=0}^{\deg(\alpha)} \alpha_i X^i \Rightarrow \mathrm{ev}_a(\alpha) = \sum_{i=0}^{\deg(\alpha)} f(\alpha_i) *_B a^i \,. \qquad \textit{III.1.20.1}$$

Preuve *: Il suffit d'appliquer la proposition III.1.17 à l'identité de A et à l'élément a de A.*

Notation III.1.21 Étant donné un ensemble X, notons $\mathcal{F}(X, A)$ l'ensemble des fonctions $f : X \to A$ de X à valeurs dans A (cf. 0.2.1.iv).)

Lemme III.1.22 *i) On peut alors munir $\mathcal{F}(X, A)$ d'une structure d'anneau commutatif par :*

$$\forall f \in \mathcal{F}(X, A),\ \forall g \in \mathcal{F}(X, A),\ \forall x \in A,\ (f{+}g)(x) := f(a) +_A g(a) \text{ et } (f{*}g)(x) := f(x){*_A}g(x) \qquad 1$$

lélément neutre pour $+$ (resp. $*$,) étant la fonction constante de valeurs 0_A (resp. 1_A.)

ii) La loi externe $\cdot$ définie sur $A \times \mathcal{F}(X, A)$ par :

$$\forall a \in A,\ \forall f \in \mathcal{F}(X, A),\ \forall x \in X,\ (a \cdot f)(x) := a \cdot f(x) \qquad 1$$

vérifie les axiomes III.1.4.iii).Mod$_1$) à III.1.4.iii).Mod$_4$).

iii) L'application :

$$j_A : A \to \mathcal{F}(X, A)\ ,\ a \mapsto a \cdot 1_{\mathcal{F}(X,A)} \qquad 1$$

est un morphisme d'anneaux.

***Preuve** : Laissée en exercice.*

Proposition III.1.23 *Considérons l'ensemble $\mathcal{F}(A, A)$ des fonctions de A dans lui-même muni de la structure $+, *$ définie en III.1.21 et III.1.22.*

i) Il existe un unique morphisme d'anneaux :

$$\phi : A[X] \to \mathcal{F}(A, A)\ ,\ X \mapsto \mathrm{Id}_A \mid \phi \circ i_A = j_A \qquad 1$$

et l'on a alors :

$$\forall \alpha \in A[X], \alpha = \sum_{i=0}^{\deg(\alpha)} \alpha_i X^i\ ,\ \phi(\alpha) = x \mapsto \sum_{i=0}^{\deg(\alpha)} \alpha_i x^i\ . \qquad 2$$

ii) Si $\cdot$ désigne la loi externe définie en III.1.4.iii).1 (resp. la loi externe définie en III.1.22.ii).1), selon le contexte :

$$\forall a \in A,\ \forall \alpha \in A[X], \phi(a \cdot \alpha) = a \cdot \phi(\alpha)\ . \qquad 1$$

iii)

$$\forall a \in A,\ \forall \alpha \in A[X], \mathrm{ev}_a(\alpha) = \phi(\alpha)(a) = \sum_{i=0}^{\deg(\alpha)} \alpha_i a^i \qquad 1$$

qu'on notera bien évidemment $\alpha(a)$.

Preuve *:*

i) Il suffit d'appliquer la proposition III.1.17 au morphisme j_A et à $\mathrm{Id}_A \in \mathcal{F}(A, A)$.

ii) Vérification sans difficulté.

iii) Idem.

Définition III.1.24 (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 III.1.25 (Fonctions polynômes) On appelle *ensemble des fonctions polynômes* l'image du morphisme ϕ défini en III.1.23.i).1, dans $\mathcal{F}(A, A)$ et *fonction polynôme* un élément de cette image.

Remarque III.1.26 On pourrait se demander pourquoi on a bien pris soin de distinguer les polynômes éléments de $A[X]$ des fonctions polynômes leurs image dans $\mathcal{F}(A, A)$. 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 III.1.23.i).1 est injectif c'est-à-dire que si deux polynômes définisssent la même fonction polynôme ils sont égaux.

b) En revanche si $\mathbb{K}$ 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 d'après le TD n° III, exercice G, question 4) par exemple est la fonction nulle. Or $X^p - X$ n'est pas le polynôme nul à savoir l'élément $\zeta \in A[X]$ défini en III.1.2.

III.2 . −Propriétés arithmétiques de l'anneau $\mathbb{K}[X]$

Dans cette section III.2, $\mathbb{K}$ est un corps commutatif et l'on note $\mathbb{K}[X]$ l'anneau des polynômes à une indéterminée sur $\mathbb{K}$ défini en III.1.16.

III.2.0 . −Introduction

La propriété essentielle de l'anneau $\mathbb{K}[X]$ envisagée ici est le théorème III.2.1 qui est un analogue du théorème I.3.2.3 et qui aura des conséquences très similaires :

i) (**Structure des idéaux**)
Structure des idéaux III.2.4 $\Leftrightarrow$ structure des sous-groupes de $\mathbb{Z}$ I.3.2.6 ;

ii) (**PGCD et théorème de BÉZOUT**)
III.2.6 $\Leftrightarrow$ I.3.3.3 ;

iii) (**Lemme de GAUSS**)
III.2.10 $\Leftrightarrow$ I.3.3.8 ;

iv) (**Lemme d'Euclide**)
III.2.11 $\Leftrightarrow$ I.3.3.10 ;

v) (**Propriétés des anneaux quotients**)
I.3.4.11 $\Leftrightarrow$ III.2.15 ;

vi) (**Théorème des restes chinois**)
I.3.6.1 $\Leftrightarrow$ III.2.16 ;

vii) (**Décomposition en produit d'irréductibles**)
I.3.3.17 $\Leftrightarrow$ III.2.17.

Théorème III.2.1 (de la division euclidienne) *Pour tout couple (A, B) d'éléments de $\mathbb{K}[X]$, avec $B \neq 0$, 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** :*

*i) (**Existence**)*
Remarqons d'abord que $B \neq 0 \Rightarrow \deg(B) \geq 0$.

a) ($\deg(B) > \deg(A)$)
Posons $Q := 0$ et $R = A$, on a bien

$$A \;=\; B * Q + R \,\text{et}\, \deg(R) \;=\; \deg(A) \;<\; \deg(B)\,.$$

b) ($\deg(B) \leq \deg(A)$)
Notons que dans ce cas on a nécessairement $A \neq 0 \Rightarrow \deg(A) \in \mathbb{N}$.

$*$) ($\deg(A) = 0$)
On a alors nécessairement $\deg(B) = 0$ et dans ce cas, $B \in \mathbb{K}$ mais $B \neq 0 \Rightarrow B \in \mathbb{K}^\times$ puisque $\mathbb{K}$ est un corps. $Q := B^{-1} * A$ et $R := 0$ vérifient $A = B * Q + R$ et $\deg(R) = -\infty < \deg(B)$.

†) $(\deg(A) > 0)$
Posons $\deg(A) = n+1, n \in \mathbb{N}$ *et* $\deg(B) = d \in \mathbb{N}, d \leq n+1$. *Écrivons*

$$A = \sum_{i=0}^{n+1} a_i X^i \text{ et } B = \sum_{i=0}^{d} b_i X^i .$$

On a $b_d \neq 0$ *et par conséquent, comme* $\mathbb{K}$ *est un corps,* $b_d \in \mathbb{K}^\times$. *Posons* $Q_1 := \frac{a_{n+1}}{b_d} X^{n+1-d}$. *Il vient alors :*

$$\begin{aligned}
A_1 &:= A - B * Q_1 \\
&= \sum_{i=0}^{n+1} a_i X^i - \frac{a_{n+1}}{b_d} X^{n+1-d} * \sum_{i=0}^{d} b_i X^i \\
&= \sum_{i=0}^{n+1} a_i X^i - \sum_{i=0}^{d} \frac{b_i * a_{n+1}}{b_d} X^{n+1+i-d} \\
&= \sum_{i=0}^{n+1} a_i X^i - \sum_{i=n+1-d}^{n+1} \frac{b_{i+d-n-1} * a_{n+1}}{b_d} X^i \\
&= \sum_{i=0}^{n} a_i X^i + a_{n+1} X^{n+1} - \sum_{i=n+1-d}^{n} \frac{b_{i+d-n-1} * a_{n+1}}{b_d} X^i - \frac{b_d * a_{n+1}}{b_d} X^{n+1} \\
&= \sum_{i=0}^{n-d} a_i X^i + \sum_{i=n+1-d}^{n} a_i - \frac{b_{i+d-n-1} a_{n+1}}{b_d} X^i .
\end{aligned}$$

Il en résulte que $\deg(A_1) \leq n$. *Notons alors* $\mathcal{P}_n$,$_{n\in\mathbb{N}}$ *l'assertion*

$$\forall P \in \mathbb{K}[X],\ \deg(P) \leq n\ ,\ \exists (Q,R) \in \mathbb{K}[X] \times \mathbb{K}[X],\ P = B*Q+R \text{ et } \deg(R) < \deg(B) .$$

Notons que $*$*) et a) assurent que* $\mathcal{P}_0$ *est vérifiée.*
Si l'on supppose $\mathcal{P}_n$ *il existe* $(Q_2, R) \in \mathbb{K}[X] \times \mathbb{K}[X]$,

$$\big(A_1 = B*Q_2+R \text{ et } \deg(R) < \deg(B)\big) \Rightarrow A = A_1 + B*Q_1 = B*(Q_1+Q_2) + R .$$

Il suffit alors de poser $Q := Q_1 + Q_2$.

*ii) (**Unicité**)*
Pour A *et* B *fixés comme dans l'énoncé du théorème, supposons qu'il existe des couples* (Q_1, R_1) *et* (Q_2, R_2) *tels que :*

$$\begin{aligned}
&\big(\deg(R_1) < \deg(B)\ ,\ \deg(R_2) < \deg(B) \quad \text{et} \quad A = B*Q_1 + R_1 = b*Q_2 + R_2\big) \\
\Rightarrow \quad & R_2 - R_1 = B*(Q_1 - Q_2) \\
\Rightarrow \quad & B \mid R_2 - R_1 .
\end{aligned}$$

Or en vertu de la formule III.1.9.i).1

$$\deg(R_1 - R_2) \leq \max(\deg(R_1), \deg(R_2)) < \deg(B) .$$

Ceci entraîne, par contraposée dans l'assertion III.1.10.iii) que $R_1 = R_2$ *d'où il résulte immédiatement que* $Q_1 = Q_2$ *ce qui établit l'unicité du couple* (Q, R).

Définition III.2.2 Les notations étant celle du théorème III.2.1, trouver les polynômes Q et R s'appelle faire la *division euclidienne* de A par B.

On appelle A le *dividende*, B le *diviseur*, Q le *quotient* et R le *reste*.

Il convient évidemment de rapprocher ces définitions de celles données en I.3.2.4.

On redonne ici la définition d'idéal déjà donnée en I.3.5.5 :

Définition III.2.3 (Idéal) Un *idéal* I de $\mathbb{K}[X]$ est une partie non vide $I \subset \mathbb{K}[X]$ telle que

$$\forall P \in I,\ \forall Q \in I,\ \forall A \in \mathbb{K}[X],\ \forall B \in \mathbb{K}[X],\ A * P + B * Q \in I$$

(cf. TD n° V, exercice E pour des caractérisations équivalentes.)

Proposition III.2.4 (Structure des idéaux) *Une partie* $I \subset \mathbb{K}[X]$ *est un idéal de* $\mathbb{K}[X]$ *si et seulement si :*

$$\exists P \in \mathbb{K}[X],\ I = P\mathbb{K}[X] = \{P * Q\ ;\ Q \in \mathbb{K}[X]\} . \qquad \textit{III.2.4.1}$$

Preuve *:*

i) Si $I = P\mathbb{K}[X]$:

$$\begin{array}{rrcl} & \forall P_1 \in I, \ \exists Q_1 \in \mathbb{K}[X], & P_1 = P * Q_1 & \\ & \forall P_2 \in I, \ \exists Q_2 \in \mathbb{K}[X], & P_2 = P * Q_2 & \\ \Rightarrow & \forall A_1 \in \mathbb{K}[X], \ \forall A_2 \in \mathbb{K}[X], & & \\ A_1 * P_1 + A_2 * P_2 & = & A_1 * P * Q_1 + A_2 * P * Q_2 & \\ & = & P * (A_1 * Q_1 + A_2 * Q_2) & \\ & \in & I & \end{array}$$

ce qui prouvve que I *est un idéal.*

ii) Réciproquement si I est un idéal non nul, soit $A := \{\deg(P)\,;\ P \in I\backslash\{0\}\}$. L'ensemble A est une partie non vide de $\mathbb{N}$, et possède donc un plus petit élément d (cf. I.1.2.7.) Soit $P \in I$ avec $\deg(P) = d$. Puisque I est un idéal, $\forall Q \in \mathbb{K}[X],\ PQ \in I$ si bien que si on note $J := P\mathbb{K}[X]$ l'idéal J est inclus dans I.

Pour tout $S \in I$, 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

$$S \in I \ \wedge\ PQ \in J \subset I \ \Rightarrow\ R = S - PQ \in I \ \Rightarrow\ \deg(R) \geq d$$

ce qui est une contradiction et entraîne $R = 0$ et par conséquent $S = PQ \in J$ et finalement $I = J$.

Remarque III.2.5 Dans la proposition précédente, et partant dans le théorème III.2.1 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 III.2.4.1.

Proposition III.2.6 (Théorème de BÉZOUT) *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. I.3.1.8.)

*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 :

$$D = \sum_{i=1}^{n} U_i P_i\,. \qquad 1$$

***Preuve** : La démonstration suit, mutatis mutandis, exactement le schéma de celle du théorème I.3.3.3 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 $\mathbb{Z}$[6] L'argument centrale de la preuve et qui remplace ici la proposition I.3.2.6 est le fait qu'un idéal de $\mathbb{K}[X]$ est de la forme $P\mathbb{K}[X]$ ce qu'on a établi à la proposition III.2.4.*

6. À noter que si la notion d'idéal avait été introduite au moment de la preuve du théorème I.3.3.3, on aurait montré sans peine que $G(A)$ était un idéal de $\mathbb{Z}$. Il se trouve que les idéaux de $\mathbb{Z}$ coïncident exactement avec ses sous-groupes et que par conséquent pour formuler les résultats de l'arithmétique de $\mathbb{Z}$ on n'a pas nécessairement besoin de la notion d'idéal.

Définition III.2.7 (Identité de BÉZOUT) (cf. I.3.3.2.) La formule III.2.6.ii).1 est appelée *identité de* BÉZOUT et les polynômes $U_{i\ ,1\leq i\leq n}$ *coefficients de* BÉZOUT.

Corollaire III.2.8 (Théorème de BÉZOUT) *(cf. I.3.3.3.) Pour tout entier naturel n et toute partie $A := \{P_1, \ldots, P_n\} \subset \mathbb{K}[X]$, les assertions suivantes sont équivalentes :*

a) $\mathcal{D}(A) = \mathbb{K}^\times$.

b) $\bigwedge A = 1$.

c) Il existe un n-uplet de polynômes $U_{i\ ,1\leq i\leq n}$ tel que

$$\sum_{i=1}^{n} P_i U_i = 1\ .$$

Définition III.2.9 (Polynômes premiers entre eux) (cf. I.3.3.4.) Pour tout entier naturel n on dira que des polynômes $P_{i\ ,1\leq i\leq n}$ sont *premiers entre eux dans leur ensemble* s'ils vérifient l'une des conditions équivalentes du corollaire III.2.6.

Pour $n = 2$ on dira simplement que deux polynômes sont *premiers entre eux*.

Il arrivera qu'on ait a considérer un n-uplet de polynômes $P_{i\ ,1\leq i\leq n}$ *deux à deux premiers entre eux*. Ceci signifie que pour tout $1 \leq i \leq n$ et tout $1 \leq j \leq n$ les polynômes P_i et JP_j sont premiers entre eux si $i \neq j$.

Proposition III.2.10 (Lemme de GAUSS) *Étant donnés trois polynômes P, Q, R, si P et Q sont premiers entre eux, et $P|QR$ alors $P|R$.*

Preuve *: Voir la preuve du théorème I.3.3.8.*

Proposition III.2.11 (Lemme d'EUCLIDE) *Dans l'anneau de polynômes $\mathbb{K}[X]$ tous les éléments irréductibles (cf. I.3.1.14,) sont premiers (cf. I.3.1.15.)*

Preuve *: Voir la preuve du théorème I.3.3.10.*

Remarque III.2.12 (Éléments irréductibles) La proposition III.2.11 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 corollaire III.1.10 dans la mesure où un corps 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 III.2.13 *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 III.1.9.i).2 et III.1.9.ii),

$$0 \leq \deg(Q) \leq 1\ 0 \leq \deg(R) \leq 1 \text{ et } \deg(Q)+\deg(R) = 1 \Rightarrow \deg(Q) = 0 \text{ ou } \deg(R) = 0$$

ce qui, en vertu de III.2.12.ii).1 entraîne Q ou R inversible et donc P irréductible.

Remarque III.2.14 (Polynômes irréductibles) Nous venons de montrer en III.2.13 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.

Proposition III.2.15 *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. III.2.11,)) 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 $i \,:\, \mathbb{K} \,\to\, \mathbb{K}[X]$ *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

$$\cdot \,:\, \mathbb{K} \times \mathbb{K}[X]/P\mathbb{K}[X] \,\to\, \mathbb{K}[X]/P\mathbb{K}[X]\,,\; (\lambda, \alpha) \,\mapsto\, \lambda \cdot \alpha \,:=\, \pi[i(\lambda)]\alpha$$

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* $\mathbb{K}[X]/P\mathbb{K}[X]$.

Proposition III.2.16 (Théorème chinois des restes) *(cf. TD n° V, exercice G.)*

Proposition III.2.17 (Décomposition en produit d'irréductibles) *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* α_i $_{,1 \leq i \leq d}$ *et un unique* $\lambda \in \mathbb{K}$ *tels que*

$$P \ = \ \lambda \prod_{i=1}^{d} P_{ii}^{\alpha} \ .$$

Preuve *: Voir la preuve de la proposition I.3.3.17.*

Proposition III.2.18 (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 $D(P)$ l'ensemble de ses diviseurs, pour tout $n \in \mathbb{N}$ $P_{n+1} = 0$ ou

$$D(P_n) \cap D(P_{n+1}) \;=\; D(P_{n+1}) \cap D(P_{n+2})$$

en particulier

$$D(P_m) \;=\; D(P_0) \cap D(P_1)\,. \qquad 1$$

***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 I.3.3.5.*

Pour $n \geq 2$, si $P_n \neq 0$, $\deg(P)_n < \deg(P)_{n-1}$ (cf. III.2.1.)

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.

III.3 . −Étude des racines d'un polynôme

Proposition III.3.1 *Pour tout polynôme $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ est une racine de P (cf. III.1.24,) si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - a) *_{\mathbb{K}[X]} Q$.*

***Preuve** :*

*i) (a **est racine de** P)*

Supposons que a est une racine de P. Considérons le morphisme $\mathrm{ev}_a : \mathbb{K}[X] \to \mathbb{K}$ défini en III.1.20.

Un élément $a \in \mathbb{K}$ est racine de P si et seulement si $P \in \mathrm{Ker}\,\mathrm{ev}_a$. Or $\mathrm{Ker}\,\mathrm{ev}_a$ est un idéal de $\mathbb{K}[X]$ non égal à $\mathbb{K}[X]$. En effet, un corps contient au moins deux éléments distincts, il existe donc $b \in \mathbb{K}$ $b \neq a$, ce qui implique que $X - b \notin \mathrm{Ker}\,\mathrm{ev}_a$.

En vertu de la proposition III.2.4, $\mathrm{Ker}\,\mathrm{ev}_a$ est engendré par un élément M. Comme $\mathrm{Ker}\,\mathrm{ev}_a \neq \mathbb{K}[X]$, $\deg(M) > 0$. Or $X - a \in \mathrm{Ker}\,\mathrm{ev}_a$, ce qui implique que M divise $X - a$ et que $\deg(M) \leq 1$ d'après le corollaire III.1.10.iii). Il en résulte que $X - a$ est un générateur de $\mathrm{Ker}\,\mathrm{ev}_a$ donc qu'il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - a) *_{\mathbb{K}[X]} Q$.

ii) $(X - a|P)$

Réciproquement si $P = (X - a) *_{\mathbb{K}[X]} Q$ il est clair que $P(a) = 0$.

Corollaire III.3.2 (Nombre de racines d'un polynôme) *Un polynôme $P \in \mathbb{K}[X]$ non nul possède au plus $\deg(P)$ racines.*

***Preuve** :*

i) *($\deg(P) = 0$)*
Un polynôme constant non nul n'a pas de racines et le résultat est donc établi pour $\deg(P) = 0$.

ii) *($\deg(P) > 0$)*
Si P n'a pas de racines le résultat est établi. Si a est une racine de P, $X - a | P$ (cf. III.3.1,) c'est-à-dire qu'il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - a) * Q$. Il s'ensuit que

$$\deg(Q) = \deg(P) - 1 < \deg(P) .$$

Si l'on fait donc lh'ypothèse de récurrence que Q a au plus $\deg(Q)$ racines P qui a une racine de plus que Q en aura donc au plus $\deg(P)$ ce qui achève la preuve en raisonnant par récurrence sur le degré des polynômes.

Proposition III.3.3 (Groupe de racines de l'unité) *Pour tout entier $d \in \mathbb{N}^*$ l'ensemble $\Gamma_d \subset \mathbb{K}^\times$ des racines du polynôme $X^d - 1$ est un sous-groupe de $\mathbb{K}^\times$ et $card\Gamma_d \leq d$.*

***Preuve** : Le fait que $\#(\Gamma_d) \leq d$ est une conséquence immédiate du corollaire III.3.2.*
En suite il est clair que $1^d = 1$ i.e.$1 \in \Gamma_d$. De plus

$$\forall x \in \Gamma_d,\ x * x^{d-1} = 1 \wedge (x^{d-1})^d = (x^d)^{-1} = 1$$

si bien que x possède un inverse dans Γ_d. Enfin puisque $(\mathbb{K}^\times, *)$ est commutatif,

$$\forall x \in \Gamma_d,\ \forall y \in \Gamma_d,\ (x * y)^d = x^d * y^d = 1 \Rightarrow x * y \in \Gamma_d .$$

On peut alors utiliser la caractérisation des sous-groupes donnée en II.1.1.1.

Proposition III.3.4 (Polynômes dérivé) *i) Il existe une unique application $\mathbb{K}$-linéaire*

$$\mathbb{K}[X] \to \mathbb{K}[X] ,\ X^n \mapsto nX^{n-1} .$$

L'image d'un polynômes P par cette application sera notée P' et appelée polynôme dérivé.

ii) La dérivation définie ci-dessus satisfait à la règle de Leibnitz à savoir

$$(PQ)' = P'Q + PQ' .$$

Preuve *:*

i) L'ensemble des $X^n{}_{,n\in\mathbb{N}}$ *étant une base du* $\mathbb{K}$*-espace vectoriel* $\mathbb{K}[X]$*, et une application linéaire étant uniquement déterminée par l'image d'une base le résultat est clair.*

ii) C'est une vérification très élémentaire.

Proposition III.3.5 (Polynômes à racines simples) *Pour tout polynôme* $P \in \mathbb{K}[X]$ *si* P *et* P' *sont premiers entre eux les racines de* P *sont simples.*

Preuve *: Soit* $a \in \mathbb{K}$ *une racine de* P*. Alors il existe* $k \in \mathbb{N}^*$*, et* $Q \in \mathbb{K}[X]$ *tels que* $P = (X-a)^k Q$*. On a alors* $P' = k(X-a)^{k-1}Q + (X-a)^k Q'$*. Si* P *et* P' *sont premiers entre eux, il existe* $(U,V) \in \mathbb{K}[X]\times\mathbb{K}[X]$*, tel que*

$$PU + P'V = 1 \Rightarrow (X-a)^k QU + [k(X-a)^{k-1}Q + (X-a)^k Q']V = 1\,.$$

Or $k > 1$ *entraîne que* a *est racine de* $(X-a)^k QU + [k(X-a)^{k-1}Q + (X-a)^k Q']V$ *donc racine du polynôme constant* 1 *ce qui n'est pas. Par conséquent,* $k = 1$ *c'est-à-dire que* a *est racine simple.*

III.4 . −Anneaux de caractéristique p

Proposition III.4.1 (Morphisme structural) *Pour tout anneau* A *il existe un unique morphisme d'anneaux* $f_A : \mathbb{Z} \to A$*. Il est usuellement appelé morphisme structural.*

Preuve *: Si* ϕ *est un morphisme d'anneaux, en particulier* $\phi(1) = 1$*. De plus,* ϕ *est un morphisme de groupes pour les lois* $+$ *sur* $\mathbb{Z}$ *et* A*. Il s'ensuit que :*

$$\begin{array}{rrcl} & \phi(0) & = & 0 \\ \forall n\in\mathbb{N}, & \phi(n+1) & = & \phi(n)+\phi(1) \\ & & = & \phi(n)+1 \\ \forall n\in\mathbb{N}, & \phi(-n) & = & -\phi(n) \end{array}$$

(cf. TD n° II, exercice B, question 2) en particulier, pour une justification.) Le morphisme ϕ *est alors uniquement défini par les formules ci-dessus et un argument de récurrence.*

Proposition III.4.2 *Étant donné un anneau A intègre (cf. 0.5.9.ii),) soit le morphisme structural f_A est injectif soit il existe un unique nombre premier p et un unique morphisme d'anneau injectif*

$$\overline{f}_A \,:\, \mathbb{Z}/p\mathbb{Z} \,\to\, A\,.$$

Preuve *:*

*i) (**Existence de** $\overline{f}_A$)*

Si f_A n'est pas injectif il possède un noyau K non trivial en tant que morphisme de groupes. Or K est un sous-groupe de $\mathbb{Z}$ (cf. TD n° II, exercice B, question 2), d).) Il existe donc un entier naturel n tel que $K = n\mathbb{Z}$ (cf. I.3.2.6.) Il existe alors, en vertu de la proposition I.3.5.3, un unique morphisme injectif de groupes

$$\overline{f}_A \,:\, \mathbb{Z}/\mathrm{Ker}\, f_A \,=\, \mathbb{Z}/n\mathbb{Z} \,\to\, A\,.$$

De plus :

$$\begin{array}{l}\forall x \in \mathbb{Z}/n\mathbb{Z},\ \forall y \in \mathbb{Z}/n\mathbb{Z},\ \big(\\ \exists a \in \mathbb{Z},\ \exists b \in \mathbb{Z},\ (x = \pi_n(a) \wedge y = \pi_n(b) \wedge \\ \qquad\qquad \begin{array}{rcl}\overline{f}_A(x*y) &=& \overline{f}_A[\pi_n(a)*\pi_n(b)]\\ &=& \overline{f}_A[\pi_n(a*b)]\\ &=& f_A(a*b)\\ &=& f_A(a)*f_A(b)\\ &=& \overline{f}_A[\pi_n(a)]*\overline{f}_A[\pi_n(b)]\\ &=& \overline{f}_A(x)*\overline{f}_A(y))\big)\end{array}\end{array}$$

en utilisant que f_A et π_n sont des morphismes d'anneaux. Enfin

$$\overline{f}_A(1) \,=\, \overline{f}_A[\pi_n(1)] \,=\, f_A(1) \,=\, 1$$

en utilisant encore que f_A et π_n sont des morphismes d'anneaux.

Il en résulte que $\overline{f}_A$ est un morphisme d'anneaux (cf. 0.5.9.v).)

*ii) (n **est premier**)*

Soient $a, b \in \mathbb{Z}$ tels que $a * b = n$. On a alors

$$f_A(a) * f_A(b) \,=\, f_A(a*b) \,=\, \overline{f}_A[\pi_n(a*b)] \,=\, \overline{f}_A[\pi_n(n)] \,=\, \overline{f}_A(0) \,=\, 0\,.$$

Comme A est intègre

$$\big(a*b \,=\, n \,\Rightarrow\, f_A(a) \,=\, 0 \,\vee\, f_A(b) \,=\, 0 \,\Rightarrow\, \overline{f}_A[\pi_n(a)] \,=\, 0 \,\vee\, \overline{f}_A[\pi_n(b)] \,=\, 0\big)\,.$$

Or $\overline{f}_A$ est injectif si bien que :

$$\begin{array}{rrcl} & a*b & = & n \\ \Rightarrow & \pi_n(a) = 0 & \vee & \pi_n(b) = 0 \\ \Rightarrow & n|a & \vee & n|b \\ \Rightarrow & \exists a' \in \mathbb{Z},\ a = na' & \vee & \exists b' \in \mathbb{Z},\ b = nb' \\ \Rightarrow & \exists a' \in \mathbb{Z},\ nba' = n & \vee & \exists b' \in \mathbb{Z},\ nab' = n \\ \Rightarrow & \exists a' \in \mathbb{Z},\ ba' = 1 & \vee & ab' = 1 \\ \Rightarrow & b = 1 \vee b = -1 & \vee & a = 1 \vee a = -1 \end{array}$$

c'est-à-dire que n est irréductible (cf. I.3.1.14) dans $\mathbb{Z}$ autrement dit que c'est un nombre premier en vertu du théorème I.3.3.10.

*iii) (**Unicité de** $\overline{f}_A$)*

On vient de montrer ci-dessus que si $\phi_n : \mathbb{Z}/n\mathbb{Z} \to A$ est un morphisme d'anneaux injectif alors n est un nombre premiers. Supposons donc donnés deux nombres premiers p et ℓ et des morphismes injectifs

$$\phi_p : \mathbb{Z}/p\mathbb{Z} \to A \text{ et } \phi_\ell : \mathbb{Z}/\ell\mathbb{Z} \to A\,.$$

La proposition III.4.1 entraîne que

$$\phi_p \circ \pi_p = f_A = \phi_\ell \circ \pi_\ell\,.$$

Ceci implique en particulier que

$$0 = \phi_\ell[\pi_\ell(\ell)] = \phi_p[\pi_p(\ell)]$$

ce qui entraîne, du fait que ϕ_p est injective, $\pi_p(\ell) = 0$ c'est-à-dire que $p|\ell$ mais ℓ étant premier $p = \ell$.

Enfin si

$$\phi : \mathbb{Z}/p\mathbb{Z} \to A \text{ et } \psi : \mathbb{Z}/p\mathbb{Z} \to A$$

sont des morphismes d'anneaux, d'après la proposition III.4.1,

$$\phi \circ \pi_p = f_A = \psi \circ \pi_p$$

ce qui entraîne, puisque π_p est surjectif, que $\phi = \psi$

Définition III.4.3 (Caractéristique d'un anneau intègre) Étant donné un anneau intègre A, on appelle *caractéristique* de A l'unique entier naturel γ tel que $\mathrm{Ker}\, f_A = \gamma\mathbb{Z}$. La caractéristique d'un anneau intègre est donc soit 0 soit un nombre premier en vertu de la proposition III.4.2. Le morphisme injectif $\overline{f}_A : \mathbb{Z}/p\mathbb{Z} \to A$ est appelé *sous-anneau premier* de A.

Remarque III.4.3.1 À noter que si A est de caractéristique 0, puisque $\mathbb{Z} \cong \mathbb{Z}/0\mathbb{Z}$ l'anneau premier de A est $\mathbb{Z}$ lui-même et dans ce cas f_A et $\overline{f}_A$ coïncident.

Pour p un nombre premier le corps $\mathbb{Z}/p\mathbb{Z}$ est appelé *corps premier* à p éléments et usuellement noté $\mathbb{F}_p$.

Exemple III.4.4 Nous ne sommes en mesure, à ce point, que de présenter les *corps premiers* $\mathbb{F}_p$ eux-mêmes à titre d'exemples d'anneaux de caractéristique p. Il pourrait dès lors sembler un peu superflu de développer la théorie pour ces objets qu'on peut tout à fait apréhender de manière élémentaire. Nous montrerons justement dans ce chapitre comment construire d'autres anneaux/corps de caractéristique p (cf. III.2.15e)t l'intérêt qu'ils peuvent présenter pour la résolution de certain problèmes d'arithmétique.

Notation III.4.5 Pour A un anneau de morphisme structural f_A, et de sous-anneau premier

$$\overline{f}_A : \mathbb{Z}/p\mathbb{Z} \to A$$

(p pouvant être 0 ou un nombre premier (cf. III.4.3.1,)) pour tout $n \in \mathbb{Z}$, et tout $a \in A$, on notera $n \cdot a$ ou même simplement

$$na := f_A(n) * a = \overline{f}_A[\pi_p(n)] * a\,.$$

Il est immédiat de constater que du fait que f_A est un morphisme d'anneaux, on a les propriétés suivantes :

Lemme III.4.6 *Mod$_1$)*

$$\forall n \in \mathbb{Z},\ \forall a \in A,\ \forall b \in A,\ n(a+b) = na + nb\,.$$

Mod$_2$)

$$\forall n \in \mathbb{Z},\ \forall m \in \mathbb{Z},\ \forall a \in A,\ (n+m)a = na + ma\,.$$

Mod$_3$)

$$\forall n \in \mathbb{Z},\ \forall m \in \mathbb{Z},\ \forall a \in A,\ (mn)a = m(na)\,.$$

Mod$_4$)

$$\forall a \in A,\ 1a = a\,.$$

Preuve : *La vérification de ce lemme est élémentaire et laissée en exercice.*

Proposition III.4.7 *Soit p un nombre premier et A un anneau de caractéristique p de morphisme structural f_A et de sous-anneau premier $\overline{f}_A : \mathbb{F}_p \to A$.*

i) La loi externe

$$\cdot : \mathbb{F}_p \times A \to A\,,\ (\lambda, x) \mapsto \overline{f}_A(\lambda) * x$$

donne à A une structure de $\mathbb{F}_p$-espace vectoriel.

ii) L'application

$$\sigma_p : A \to A\,,\ x \mapsto x^p$$

est un morphisme injectif d'anneaux de A dans lui-même appelé morphisme de Frobenius.

Preuve :

i) Il suffit de remarquer que,

$$\forall \lambda \in \mathbb{F}_p,\ \exists n \in \mathbb{Z},\ \lambda = \pi_p(n)\ .$$

On a alors

$$\forall x \in A,\ \lambda \cdot x = \overline{f}_A(\lambda) * x = \overline{f}[\pi_p(n)] * x = f_A(n) * x = n \cdot x\ .$$

Le lemme III.4.6 assure alors qu'on définit bien ainsi une structure d'espace vectoriel.

Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

TD n° I

Exercice A : (**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 B : (**Entiers naturels**)

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**$_2$)

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

Supposant donné un système de Peano on va établir dans la suite les propriétés algébrique de $+$ et $*$ qui en découlent.

On notera $1 := \mathfrak{s}(0)$.

1) Montrer que $\mathfrak{s} : \mathbb{N} \to \mathbb{N}^*$ est bijective.

2) (**Addition**)

a) Montrer que $\forall p \in \mathbb{N},\ (\mathfrak{s}(p) = p + 1)$.

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

c) (**Associativité**)
Montrer que : $\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ ((p + q) + r = p + (q + r)$. On notera dorénavant

$$p + q + r := p + (q + r) = (p + q) + r\ .$$

d) (**Élément neutre**)
Montrer que : $\forall p \in \mathbb{N},\ (0 + p = p)$ et en déduire que 0 est un élément neutre pour $+$.

e) (**Commutativité**)
Montrer que : $\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ (p + q = q + p)$.

f) (**Régularité**)
Montrer que : $\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ (p + r = q + r \Rightarrow p = q)$.

g) Montrer que : $\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ (p + q = 0 \Leftrightarrow p = 0 \text{ et } q = 0)$.

3) (**Multiplication**)

a) (**Distributivité à gauche**)
Montrer que : $\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ (p * (q + r) = p * q + p * r)$.

b) (**Associativité**)
Montrer que : $\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ (p * (q * r) = (p * q) * r)$. On notera simplement

$$p * q * r := p * (q * r) = (p * q) * r\ .$$

c) (**Élément neutre**)
Montrer que : $\forall p \in \mathbb{N},\ (1 * p = p * 1 = p)$.

d) (**Élément absorbant**)
Montrer que : $\forall p \in \mathbb{N},\ (0 * p = p * 0 = 0)$.

e) Montrer que : $\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ ((p + 1) * q = p * q + q)$.

f) (**Commutativité**)
Montrer que : $\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \big(p * q = q * p\big)$.

g) (**Distributivité à droite**)
Déduire de ce qui précède que : $\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ \big((p + q) * r = p * r + q * r\big)$.

h) Montrer que : $\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \big(p * q = 0 \Rightarrow p = 0 \vee q = 0\big)$.

i) Montrer que : $\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \forall r \in \mathbb{N},\ \big(q \leq r\ \Rightarrow\ p * q \leq p * r\big)$ la réciproque étant vraie si $p \neq 0$.

j) Montrer que : $\forall p \in \mathbb{N},\ \forall q \in \mathbb{N},\ \big(p * q\ =\ 1\ \Rightarrow\ p\ =\ 1\ \wedge\ q\ =\ 1\big)$.

Exercice C : Sur un ensemble E, on considère deux relations d'équivalence R_1 et R_2.

1) On note $R\ :=\ R_1$ et R_2 la relation binaire définie sur E par

$$\forall x \in E\ ,\ \forall y \in E\ ,\ x\,R\,y\ \Leftrightarrow\ x\,R_1\,y \text{ et } x\,R_2\,y\ .$$

Montrer que R est une relation d'équivalence.

2) On note $R'\ :=\ R_1$ ou R_2 la relation binaire définie sur E par

$$\forall x \in E\ ,\ \forall y \in E\ ,\ x\,R'\,y\ \Leftrightarrow\ x\,R_1\,y \text{ ou } x\,R_2\,y\ .$$

a) Montrer que R' et réflexive et symétrique.

b) La relation R' est-elle transitive ? Est-ce une relation d'équivalence ?

3) Reprendre les questions dans le cas où R_1 et R_2 sont des relations d'ordre.

Exercice D : Exercice A : (Application strictement croissante)

Soient P et Q deux parties de $\mathbb{N}$. Montrer qu'une application strictement croissante (resp. strictement décroissante)

$$f\ :\ P\ \rightarrow\ Q \text{ est injective .}$$

Exercice B : $(f(n) \geq n)$

Soient $n\ \in\ \mathbb{N}$ et $f\ :\ [0;n]\ \rightarrow\ \mathbb{N}$ 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 $f\ :\ [0;p]\ \rightarrow\ [0;q]$ si et seulement si $p \leq q$.

2) En déduire qu'il existe une application bijective $f\ :\ [0;p]\ \rightarrow\ [0;q]$ si et seulement si $p\ =\ q$.

3) En déduire qu'il n'existe pas d'application injective $f\ :\ \mathbb{N}\ \rightarrow\ [0;p]$.

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 $\#(A \cap B)\ \leq\ \min(p, q)$.

Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

TD n° II

Exercice A : (Relation d'équivalence, partition et application surjective)

Soit E un ensemble non vide. On rappelle qu'une *partition* de E est une partie P de l'ensemble $\mathcal{P}(E)$ des parties de E vérifiant :

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

Part$_2$)

$$\forall A \in P,\ \forall B \in P,\ \big(A \cap B \neq \emptyset \Rightarrow A = B\big)\ ;$$

Part$_3$)

$$\bigcup_{A \in P} A = E\ .$$

Dans la suite on notera $\mathbf{R}$ l'ensemble des relation d'équivalence (cf. 0.2.2.v),) sur E, $\mathbf{P}$ l'ensemble des partition de E et $\mathbf{S}$ l'ensemble des couples (π, F) où F est un ensemble et $\pi : E \to F$ est une application surjective.

Pour une telle application et tout $y \in F$, il est commode de parler de la *fibre* de π en y notée :

$$\pi_y := \pi^{-1}(\{y\}) = \{x \in E\ ;\ \pi(x) = y\}\ .$$

1) a) Pour tout $R \in \mathbf{R}$ montrer que l'ensemble des classes d'équivalence selon R forme une partition de E. En déduire une application $f : \mathbf{R} \to \mathbf{P}$.

b) Pour tout $P \in \mathbf{P}$ on définit une relation R sur E par

$$\forall x \in E,\ \forall y \in E,\ \big(x\ R\ y \Leftrightarrow \exists A \in P,\ (x \in A \wedge y \in A)\big)\ .$$

Montrer que R est une relation d'équivalence et qu'on définit ainsi une application $f' : \mathbf{P} \to \mathbf{R}$.

c) Montrer que les application f et f' sont inverses l'une de l'autre.

2) a) POur $R \in \mathbf{R}$ montrer que l'application $\pi : E \to E/R$ qui à tout élément associe sa classe est surjective et en déduire une application $g : \mathbf{R} \to \mathbf{S}$.

b) Étant donnée une application surjective $\pi : E \to F$ on définit une relation R sur E par

$$\forall x \in E,\ \forall y \in E,\ \big(x\ R\ y \Leftrightarrow \pi(x) = \pi(y)\big)\ .$$

Montrer que R ainsi définie est une relation déquivalence et qu'on construit ainsi une application

$$g' : \mathbf{S} \to \mathbf{R}\ .$$

c) Montrer que les applications g et g' sont inverses l'une de l'autre.

3) 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

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

a) Montrer que si l'on note $(\pi, F) \,:=\, g(R)$, 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*.

b) 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 $\dagger$.

c) 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 $\dagger$.

d) Donner des exemples déjà connus des constructions précédentes.

Exercice B : 1) (Unicité des éléments remarquables)

Soit $(E, *)$ un ensemble muni d'une loi associative.

a) (Élément neutre)

Montrer que si $(E, *)$ possède un élément neutre ϵ celui-ci est unique.

b) (Symétrique)

Montrer que si $(E, *)$ possède un élément neutre ϵ, tout élément $x \,\in\, E$ possède au plus un symétrique.

2) (Morphismes de groupes)

Soit

$$f \,:\, (G, *, \epsilon_G) \,\to\, (H, \bullet, \epsilon_H)$$

un morphisme de groupes.

a) (Élément neutre)

Montrer que $f(\epsilon_G) \,=\, \epsilon_H$.

b) (Symétrique)

Montrer que pour tout $x \,\in\, G$, si y est son symétrique, $f(y)$ est le symétrique de $f(x)$.

c) (Image)

Montrer que $\mathrm{Im}\, f$ est un sous-groupe de $(H, \bullet)$.

d) (Noyau)

Montrer que $\mathrm{Ker}\, f$ est un sous-groupe de $(G, *)$.

e) (Isomorphisme)

Montrer que si f est bijective et que g est son applications réciproque, alors g est un morphisme de groupe.

3) Soit $(G, *, e)$ un groupe. Pour tout $x \in G$ on définit une application ϵ_x par

$$\epsilon_x(0) := e\ ,\ \forall n \in \mathbb{N},\ \epsilon_x(n+1) := x * \epsilon_x(n)\ .$$

a) Rappeler pourquoi ϵ_x définit bien une application de $\mathbb{N}$ dans G.

b) 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.

c) 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 ?

4) (Caractérisation des sous-groupes)

Étant donné un groupe $(G, *)$, montrer qu'une partie $H \subset G$ de G est un sous-groupe (cf. cours 0.5.6.iv),) de G si et seulement si, $H \neq \emptyset$ et

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

5) (Propriétés élémentaires des anneaux)
Soit $(A, +, *)$ un anneau dont on note 0 l'élément neutre pour la loi $+$.

a) Montrer que, pour tout $x \in A$, $0 * x = 0$.

b) Montrer que $(A^\times, *)$ est un groupe (abélien si A est commutatif.)

c) 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 $B^\times$.

d) Montrer que pour tout anneau A il existe un unique morphisme d'anneaux $f : \mathbb{Z} \to A$.

Exercice C : (Introduction à $\mathbb{Z}/n\mathbb{Z}$)

1) a) Montrer que tout entier relatif divise 0 tandis que 0 ne divise que lui-même.

Pour tout entier naturel n on définit la *relation de congruence modulo* n sur $\mathbb{Z}$ par a congrue à b modulo n si n divise $b - a$ et l'on écrit

$$a \equiv b\,[n]\ .$$

b) Montrer que la relation de congruence modulo n est une relation d'équivalence.

On notera $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence pour la relation de congruence modulo n, qu'on abrègera en *Classes de congruence modulo* n.
Pour tout $a \in \mathbb{Z}$, on notera $\pi_n(a)$ ou $\overline{a}$ la classe de a modulo n .

c) a) Montrer que $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est une application surjective. On 'lappelle usuellement *surjection canonique*.

b) Est-elle injective ?

d) Donner le cardinal de $\mathbb{Z}/n\mathbb{Z}$.

e) Un entier naturel n étant fixé, montrer que, pour tout quadruplet (a, b, a', b') d'entiers relatifs,

$$a \equiv a'\,[n] \text{ et } b \equiv b'\,[n] \Rightarrow a + b \equiv a' + b'\,[n]\ .$$

f) Sous les mêmes hypothèses qu'à la question précédente, montrer que

$$a \equiv a'\,[n] \text{ et } b \equiv b'\,[n] \Rightarrow ab \equiv a' * b'\,[n]\ .$$

2) (L'addition sur $\mathbb{Z}/n\mathbb{Z}$)
Pour tout entier $n \geq 2$, on note

$$\mathbb{Z}/n\mathbb{Z} \textbf{ l'ensemble des classes de congruence modulo } n$$
$$\text{et } \ \pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \textbf{ la surjection canonique (cf. question 1).)}$$

a) Montrer que l'on définit bien une loi interne

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

en posant, pour tout couple (α, β) d'éléments de $\mathbb{Z}/n\mathbb{Z}$,

$$\alpha + \beta := \overline{a + b}$$

où

$$\overline{a + b} \text{ est la classe de congruence modulo } n \text{ de la somme } a + b$$

pour a (resp. b,) n'importe quel représentant de α (resp. β .)

b) Montrer que $+$ ainsi définie sur $\mathbb{Z}/n\mathbb{Z}$ est associative, possède un élément neutre qu'on déterminera, que tout élément possède un opposé et que $+$ est commutative.

c) Montrer que la loi $+$ ainsi définie sur $\mathbb{Z}/n\mathbb{Z}$ est la seule telle que π_n soit un morphisme de groupes.

d) Montrer qu'en tant que morphisme de groupes, π_n s'identifie au morphisme $\epsilon_{\overline{1}}$ défini comme dans le exercice B, question 3).

3) (**La multiplication sur** $\mathbb{Z}/n\mathbb{Z}$)
Pour tout entier $n \geq 2$, **on note**

$$\mathbb{Z}/n\mathbb{Z} \textbf{ l'ensemble des classes de congruence modulo } n$$
$$\text{et} \quad \pi_n \,:\, \mathbb{Z} \,\to\, \mathbb{Z}/n\mathbb{Z} \textbf{ la surjection canonique (cf. question 1).)}$$

a) Même question qu'en question 2) pour la multiplication $*$.

b) Montrer que la multiplication $*$ sur $\mathbb{Z}/n\mathbb{Z}$ est associative, possède un élément neutre que l'on déterminera et que $*$ est commutative.

c) Montrer que $*$ est distributive sur $+$. On dira que $(\mathbb{Z}/n\mathbb{Z}, +, *)$ a une structure d'*anneau commutatif*. Connaissez-vous d'autres anneaux commutatifs ?

d) Tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ ont-ils un inverse pour $*$?

e) Donner un analogue au question 2), c) pour $*$.

f) Montrer que $\pi_n \,:\, \mathbb{Z} \,\to\, \mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneaux et que c'est le seul.

g) Montrer que,

$$\forall \alpha \,\in\, \mathbb{Z}/n\mathbb{Z},\ \forall k \in \mathbb{Z},\ \epsilon_\alpha(k) \,=\, \pi_n(k) * \alpha$$

(où ϵ_α est le morphisme défini dans le exercice B, question 3).

4) **a)** Montrer que les lois $+_n$ et $*_n$ définies à l'question 1) donnent à $\mathbb{Z}/n$ une structure d'anneau.

b) Cette structure est-elle "raisonnablement" unique ?

c) L'anneau $(\mathbb{Z}/n, +_n, *_n)$ est-il commutatif ?

Exercice D : **1)** Trouver toutes les solutions entières de l'équation $2004x \,+\, 1905y \,=\, 3$ et donner celle pour laquelle la valeur absolue de x est minimale.

2) Résoudre la congruence $2004x \,\equiv\, 3\,[1905]$.

Exercice E : Déterminer l'ensemble des couples (x, y) d'entiers relatifs tels que

$$52x \,+\, 65y \,=\, 39\,.$$

Exercice F : Résoudre le système de congruences suivant :

$$\left\{\begin{array}{rcl} 33x & \equiv & 176\ [1969] \\ 35x & \equiv & 15\ [2005] \end{array}\right\} .$$

Exercice G : (**La « preuve » par** 9 **et par** 11)

Soit $b \in \mathbb{N}, b > 1$. **On sait alors, grâce au Problème n° I, exercice A que, pour tout** $a \in \mathbb{Z}$, **il existe un unique** $\varepsilon \in \{-1, 1\}$ **un unique** $d \in \mathbb{N}$ **et un unique** $d+1$**-uplet** $a_{i\ ,0\leq i\leq d}$ **vérifiant les conditions : Problème n° I, exercice A, 1 à Problème n° I, exercice A, 3.**

Pour $\varphi = \pm$ **on pose :**

$$s_\varphi(a) := \varepsilon \cdot \sum_{i=0}^{d} a_i (\varphi\, 1)^i .$$

0) Vérifier rapidement que :

$$\begin{array}{rrcl} \forall a \in \mathbb{Z}, & s_\varphi(-a) & = & -s_\varphi(a) \\ & |s_\varphi(a)| & = & s_\varphi(|a|) \\ \forall a \in \mathbb{N}, & s_\varphi(a) & \in & \mathbb{N} . \end{array}$$

1) Pour tout $a \in \mathbb{Z}$, que vaut $s_\varphi(a)$ (resp. $s_\varphi[s_\varphi(a)]$,) (resp. ${s_\varphi}^n(a)$) (où ${s_\varphi}^n$ désigne l'itéré $n^{\text{ième}}$ de s_φ *i.e.*${s_\varphi}^{n+1} = s_\varphi \circ {s_\varphi}^n$,) modulo $b - \varphi\, 1$?

2) Montrer que

$$\forall a \in \mathbb{Z},\ \exists n_\varphi(a) \in \mathbb{N},\ \forall m \in \mathbb{N},\ m \geq n_\varphi(a) \Rightarrow -b < {s_\varphi}^m(a) = {s_\varphi}^{n_\varphi(a)}(a) < b .$$

Pour tout $a \in \mathbb{Z}, a \in\ ]-b; b[$, **posons :**

$$\begin{array}{rcll} \rho_+(a) & = & 0 & \textbf{si} \quad |a| = b-1 \\ & = & a & \textbf{si} \quad a \in [0; b-1[\\ & = & a+b-1 & \textbf{si} \quad a \in]b-1; 0[. \end{array} .$$

On définit de même :

$$\begin{array}{rcll} \rho_-(a) & = & a & \textbf{si} \quad a \in [0; b[\\ & = & a+b+1 & \textbf{si} \quad a \in]b; 0[. \end{array} .$$

3) Pour tout $a \in \mathbb{Z}$, comment peut-on interpréter $\rho_\varphi[{s_\varphi}^{n_\varphi(a)}(a)]$?

4) Montrer que

$$\forall x \in \mathbb{Z},\ \forall y \in \mathbb{Z},\ \forall z \in \mathbb{Z},\ x \cdot y = z \Rightarrow \rho_\varphi\big[s_\varphi[{s_\varphi}^{n_\varphi(x)}(x) \cdot {s_\varphi}^{n_\varphi(y)}(y)]\big] = \rho_\varphi[{s_\varphi}^{n_\varphi(z)}(z)] .$$

5) Pourquoi l'égalité

$$9691791 \cdot 40027002 = 387933337760582$$

est-elle fausse ?

6) Quel commentaire peut-on faire par rapport au titre de cet exercice ?

Exercice H : Étant donnés deux groupes abéliens $(G_1, +)$ et $(G_2, +)$, on notera $(G_1 \times G_2, +)$ l'ensemble des couples (x_1, x_2) $x_1 \in G_1$, $x_2 \in G_2$ muni de la loi $+$ définie par

$$(x_1, x_2) \ + \ (y_1, y_2) \ := \ (x_1 + y_1, x_2 + y_2) \ .$$

1) Montrer qu'avec les notations ci-dessus, $(G_1 \times G_2, +)$ est un groupe abélien dont on précisera l'élément neutre. Donner l'opposé de (x_1, x_2).

Dans la suite on utilisera librement la notation

$$(\mathbb{Z}^2, +) \ := \ (\mathbb{Z} \times \mathbb{Z}, +) \ .$$

2) Soient a et b deux entiers relatifs non nuls, d leur pgcd et m leur ppcm. On notera $a \ := \ da'$ et $b \ := \ db'$.

a) Rappeler pourquoi on peut écrire $d \ = \ au + bv$ avec u et v des entiers relatifs.

b) Rappeler pourquoi a' et b' sont premiers entre eux.

c) Donner en la justifiant la relation liant a', b', d et m.

3) Avec les notations de la question 2), a), on définit l'application :

$$\begin{array}{rccc} f : & \mathbb{Z}^2 & \to & \mathbb{Z}^2 \\ & (x, y) & \mapsto & (ux + vy, -b'x + a'y) \end{array}$$

a) Montrer que f est un morphisme de groupes de $(\mathbb{Z}^2, +)$ dans lui-même.

b) Montrer que f est bijective et déterminer son application réciproque g.

c) Rappeler pourquoi g est un morphisme de groupes.

4) On définit les applications :

$$\begin{array}{rccc} p : & \mathbb{Z}^2 & \to & \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & (x, y) & \mapsto & (x \ \mathbf{mod} \ d, y \ \mathbf{mod} \ m) \\ q : & \mathbb{Z}^2 & \to & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ & (x, y) & \mapsto & (x \ \mathbf{mod} \ a, y \ \mathbf{mod} \ b) \ . \end{array}$$

a) Montrer que p (resp. $q,$) est un morphisme de groupe de $(\mathbb{Z}^2, +)$ dans $(\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +)$ (resp. $(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, +)$; puis que $p \circ f$ et $q \circ g$ sont des morphismes de groupes.

b) Déterminer $\mathrm{Ker}\, p$ et $\mathrm{Ker}\, q$.

c) Montrer qu'il existe un unique morphisme de groupes

$$f' \ : \ (\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, +) \ \to \ (\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +)$$

$$(\text{resp. } .g' \ : \ (\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +) \ \to \ (\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, +) \ )$$

tel que

$$f' \circ q \ = \ p \circ f \ (\text{resp. } g' \circ p \ = \ q \circ g \ .)$$

d) Pour des applications

$$u \,:\, X \,\to\, Y \,,\; v \,:\, X \,\to\, Y \text{ et } w \,:\, W \,\to\, X$$

avec w surjective, montrer que

$$u \,=\, v \;\Leftrightarrow\; u \circ w \,=\, v \circ w \,.$$

e) Montrer finalement que f' et g' sont inverses l'un de l'autre c'est-à-dire qu'on a construit un isomorphisme de groupes

$$(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, +) \;\cong\; (\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +) \,.$$

f) Peut-on déduire ce résultat d'un théorème connu lorsque $d = 1$? En d'autres termes quel résultat avons-nous généralisé ici ?

Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

TD n° III

Exercice A : Résoudre le système de congruences simultanées :

$$\left\{\begin{array}{rcl} 14x & \equiv & 7\,[1789] \\ 18x & \equiv & 6\,[1940] \end{array}\right\}.$$

Exercice B : Soient $a_1, a_2, ..., a_n \in \mathbb{N}$, tels que pgcd$(a_i, a_j) = 1$, $i \neq j$, $1 \leq i, j \leq n$.

1) Montrer que tout $x \in \mathbb{N}$ s'écrit de façon unique comme

$$x = s_1 + a_1 s_2 + a_1 a_2 s_3 + \cdots + a_1 a_2 \cdots a_{n-1} s_n + a_1 a_2 \cdots a_n s,$$

avec $s_1, s_2, ..., s_n, s \in \mathbb{N}$, $0 \leq s_i < a_i$, $1 \leq i \leq n$.

Si x satisfait les équations

$$x = y_1 modulea_1\ ,\ x = y_2 modulea_2\ ,\ \ldots\ ,\ x = y_n modulea_n,$$

alors peut-on déterminer $s_1, s_2, \ldots, s_n$?

2) Utiliser 1) pour résoudre le système

$$(\mathrm{S})\ \left\{\begin{array}{l} x = 2 module 3 \\ x = 3 module 5 \\ x = 2 module 7 \end{array}\right.$$

Soit $a = a_1 a_2 \cdots a_n$ et soit

$$\varphi\ :\ \mathbb{Z}/a\mathbb{Z} \to \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z},$$

définie par $\varphi(xmodulea) = (xmodulea_1, xmodulea_2, ..., xmodulea_n)$.

3) Montrer que φ est un isomorphisme.

Soit $\psi = \varphi^{-1}$ et soit $y = (y_1 modulea_1, y_2 modulea_2, ..., y_n modulea_n)$. Quand $y_i = 1$ et $\psi_j = 0$, $j \neq i$, alors on pose $y = e_i$.

4) Écrire l'identité de Bezout pour a_i et $b_i = a_1 \cdots a_{i-1} a_{i+1} \cdots a_n$ et déterminer $\psi(e_i)$.

5) Déterminer $\psi(y)$.

6) Considérons le cas où

$$\varphi\ :\ \mathbb{Z}/105\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z},$$

définie par $\varphi(xmodule105) = (xmodule3, xmodule5, xmodule7)$.

Déterminer $\psi = \phi^{-1}$.

7) Utiliser 6) pour résoudre le système (S).

Exercice C : **1)** **a)** Déterminer les couples d'entiers relatifs (x, y) tels que

$$2006x \ + \ 1955y \ = \ 17 \, .$$

b) Parmi les solutions de l'équation ci-dessus déterminer celle pour laquelle x a la plus petite valeur absolue.

2) Déterminer tous les entiers relatifs x tels que

$$\left\{ \begin{array}{rcl} 118x & \equiv & 5 \, [115] \\ 23x & \equiv & 4 \, [58] \\ 203x & \equiv & 56 \, [91] \end{array} \right\} \, .$$

Exercice D : Montrer

$$\forall n \in \mathbb{N}, \ 11 \mid 2^{6n+3} + 3^{2n+1} \, .$$

Exercice E : **1)** Pour tout nombre premier p, montrer que $p! + 1$ n'a aucun diviseur inférieur ou égal à p.

2) En déduire que pour tout nombre premier p il existe un nombre premier $q > p$.

3) En déduire finalement que l'ensemble des nombres premiers est dénombrable.

Exercice F : Soient $a_{i \, , 1 \leq i \leq n}$ des entiers deux à deux premiers entre eux.

1) Montrer que le **Ppcm** des $a_{i \, , 1 \leq i \leq n}$ est égal à leur produit.

Pour tout $1 \ \leq \ i \ \leq \ n$ **on pose** $b_i \ := \ \displaystyle\prod_{j \in [1,n] \ , \ j \neq i} a_j \, .$

2) Montrer que les $b_{i \, , 1 \leq i \leq n}$ sont premiers entre eux dans leur ensemble.

Soient $u_{i \, , 1 \leq i \leq n}$ des entiers tels que $\displaystyle\sum_{i=1}^{n} u_i b_i \ = \ 1$. On rappelle que, d'après un résultat du cours, l'application

$$\begin{array}{rccc} \gamma : & \mathbb{Z}/(\displaystyle\prod_{i=1}^{n} a_i)\mathbb{Z} & \rightarrow & \times_{i=1}^{n} \mathbb{Z}/a_i\mathbb{Z} \\ & x module \prod_{i=1}^{n} a_i & \mapsto & (x module a_1, \ldots, x module a_n) \end{array}$$

est un isomorphisme.

3) Pour $(x_1, \ldots, x_n)$ un n-uplet d'entiers, calculer $\gamma^{-1}(x_1 module a_1, \ldots, x_n module a_n)$ en fonction des

$$b_{i \, , 1 \leq i \leq n} \ , \ u_{i \, , 1 \leq i \leq n} \text{ et } x_{i \, , 1 \leq i \leq n} \ .$$

Exercice G : (Petit théorème de FERMAT)
Dans cette question on fixe un nombre premier p.

1) rappeler pourquoi $\forall k \in \mathbb{N},\ \binom{p}{k} \in \mathbb{N}$.

2) Pour tout $1 \leq k < p$, montrer que $p | \binom{p}{k}$.

3) En déduire que, pour tout couple d'entiers relatifs (a, b), il existe un entier relatif c tel que

$$(a+b)^p \ - \ a^p \ - \ b^p \ = \ cp \, .$$

4) En déduire que

$$\forall a \in \mathbb{Z},\ a^p \ \equiv \ a \ [p] \, .$$

5) En déduire que pour tout entier relatif a premier à p,

$$a^{p-1} \ \equiv \ 1 \ [p] \, .$$

Exercice H : Soit p un nombre premier. On note $\mathbb{F}_p \ := \ (\mathbb{Z}/p\mathbb{Z}, +, *)$ le corps à p éléments dont on notera 0 et 1 l'élément neutre pour l'addition et la multiplication respectivement.

1) Rappeler pourquoi $\mathbb{F}_p$ est un corps et ce que cela signifie.

2) **On suppose $p \neq 2$; et qu'il existe $\alpha \in \mathbb{F}_p$ tel que**

$$\alpha^2 + 1 \ = \ 0 \, .$$

a) Montrer que le sous-groupe multiplicatif de $({\mathbb{F}_p}^\times, *)$ engendré par α est de cardinal 4.

b) En déduire que $p \ \equiv \ 1 \ [4]$.

c) En déduire que les seules racines du polynôme $X^4 - 1$ dans $\mathbb{Z}/11\mathbb{Z}$ sont 1 et -1.

3) Donner les racines différentes de 1 du polynôme $X^4 - 1$ dans $\mathbb{Z}/5\mathbb{Z}$.

4) Résoudre dans $\mathbb{Z}/55\mathbb{Z}$ l'équation $x^3 + x^2 + x + 1 \ = \ 0$.

Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

TD n° IV

Exercice A : (Théorème de LAGRANGE)

Soit G un groupe. Pour $x \in G$, on renvoie au TD n° II, exercice B, question 3) pour la définition du morphisme $\epsilon_x : \mathbb{Z} \to G$.

1) Pour tout $x \in G$, montrer que soit ϵ_x est injectif soit il existe $d \in \mathbb{Z}$ tel que $\operatorname{Im} \epsilon_x \cong \mathbb{Z}/d\mathbb{Z}$.

2) Rappeler pourquoi dans le cas où ϵ_x n'est pas injectif l'entier d défini ci-dessus est le plus petit entier tel que $dx = 0$ ou $x^d = 1$ suivant la notation adoptée pour le groupe.

On appelle l'entier d l'*ordre de x dans G* et si ϵ_x est injective on dira parfois que l'ordre de x est infini.

3) Montrer que si G est fini alors l'ordre de tout élément $x \in G$ divise le cardinal de G.

Exercice B : **1)** Montrer que tout groupe de cardinal premier est cyclique.

2) **a)** Montrer qu'un groupe G dont tous les éléments x vérifient $x^2 = e$ est abélien.

b) En déduire qu'un groupe de cardinal 4 est abélien.

3) **a)** Trouver, à isomorphisme près, tous les groupes de cardinal au plus 5 et tous les groupes abéliens de cardinal 6 .

b) Connaissez-vous un groupe non abélien de cardinal 6 ?

Exercice C : (Sous-groupes)

1) (Caractérisation des sous-groupes)

Étant donné un groupe $(G, *)$, montrer qu'une partie $H \subset G$ de G est un sous-groupe (cf. cours 0.5.6.iv),) de G si et seulement si, $H \neq \emptyset$ et

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

2) (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.*

3) (**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.

4) 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 D : Pour chacune des permutations suivantes trouver sa décomposition en produit de cycles à supports deux à deux disjoints, son ordre, sa signature. Calculer s^{1515} et t^{1789} .

$$s := \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 6 & 8 & 7 & 4 & 2 & 1 \end{matrix} \text{ et } t := \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 4 & 8 & 7 & 5 & 9 & 3 & 1 & 6 & 2 & 11 & 10 \end{matrix} .$$

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 $c := (1, 2, \dots, n)$. (On pourra calculer le conjugué de $(1, 2)$ par les puissances de c .)

Exercice F : **1)** **a)** Pour $n \in \mathbb{N}^*$ a, b, c des éléments deux à deux distincts de $[1; n]$, calculer

$$(a\,b)(b\,c)\ ,\ (b\,c)(a\,b)\ ,\ (a\,b)(b\,c)(a\,b)\ .$$

b) Décrire

$$\mathcal{S}_1\ ,\ \mathcal{A}_1\ ,\ \mathcal{S}_2\ ,\ \mathcal{A}_2\ ,\ \mathcal{A}_3\ .$$

c) Montrer que le groupe symétrique $\mathcal{S}_n$ n'est pas abélien si $n \geq 3$ et que le groupe alterné $\mathcal{A}_n$ n'est pas abélien si $n \geq 4$.

2) (**Conjugaison dans $\mathcal{S}_5$**)

a) Montrer que tous les 3-cycles de $\mathcal{S}_5$ forment une même classe de conjugaison.

b) En est-il toujours de même dans $\mathcal{A}_5$?

c) Déterminer toutes les classes de conjugaison de $\mathcal{S}_5$ et donner un représentant de chacune d'entre elles.

3) (**Ordre dans le groupe symétrique** $\mathcal{S}_8$)
Le Groupe symétrique $\mathcal{S}_8$

a) contient-il un élément d'ordre 12 ?

b) contient-il un élément d'ordre 14 ?

c) Quel est l'ordre maximal d'un élément de $\mathcal{S}_8$?

4) ($\mathcal{S}_n \subset \mathcal{A}_{n+2}$)
Pour tout $n \in \mathbb{N}^*$, montrer que le groupe symétrique $\mathcal{S}_n$ est isomorphe à un sous-groupe du groupe alterné $\mathcal{A}_{n+2}$.

Exercice G : **1)** Compléter la preuve de la proposition II.1.3.4.

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 H : **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 I : **1) Soient**

$$s_1 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix} \text{ et } s_2 := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 3 & 2 & 5 \end{pmatrix}$$

des éléments de $\mathcal{S}_6$.

a) Donner les décompositions en cycles à supports deux à deux disjoints de $s_1$et s_2.

b) Donner l'ordre et la signature de s_1 et s_2.

c) Calculer s_1^{2006}.

d) Les éléments s_1 et s_2 sont-ils conjugués dans $\mathcal{S}_6$?

2) Soit

$$G := \left\{ s \in \mathcal{S}_6 \,;\, s(\{1,2\}) = \{1,2\} \right\}.$$

a) Montrer que G est un sous-groupe de $\mathcal{S}_6$.

b) G est-il un sous-groupe de $\mathcal{A}_6$?

c) Le sous-groupe G est-il distingué dans $\mathcal{S}_6$?

d) Montrer que G contient un sous-groupe distingué H isomorphe à $\mathcal{S}_4$.

e) Déterminer le quotient G/H.

f) En déduire le cardinal de G.

Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

TD n° V

Exercice A : (**Division euclidienne de polynômes**)

1) Effectuer la division euclidienne de $X^5 + 13X^4 + 11X^3 + 7X^2 + 5X + 3$ par $X^2 + 1$.

2) Calculer le PGCD de $X^6 + 2X^5 + 3X^4 + 5X^3 + 7X^2 + 11X$ et $13X^3 + 17X^2 + 19$.

Exercice B : **1)** (**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** $\alpha := P(a), \beta := P(b)$.

2) Exprimer le reste de la division euclidienne de P par $(X - a)(X - b)$, en fonction de a, b, α et β.

3) 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 C : (**Polynômes d'endomorphismes**)

Soit A **une matrice carrée** $k \times k$ **à coefficients dans** $\mathbb{C}$. **Si** $P := \sum_{n \geq 0} a_n X^n$ **est un élément de** $\mathbb{C}[X]$, **on définit** $P(A)$ **comme la matrice carrée** $k \times k$

$$P(A) := \sum_{n \geq 0} a_n A^n$$

(en posant $A^0 = I$, **la matrice identité). On pourra utiliser sans les démontrer les faits suivants :**

a) **Si** $P, Q, R \in \mathbb{C}[X]$, **et si** $P = QR$ **alors** $P(A) = Q(A)R(A)$;

b) **Si** $P, Q, R \in \mathbb{C}[X]$, **et si** $P = Q + R$, **alors** $P(A) = Q(A) + R(A)$.

Si v **est un élément de** $\mathbb{C}^k$, **on note** $Av \in \mathbb{C}^k$ **le produit de la matrice** A **par le vecteur-(colonne)** v.

On notera $\operatorname{Ker} A := \{v \in \mathbb{C}^k$ **tels que** $Av = 0\}$ **(ici** 0 **désigne l'élément de** $\mathbb{C}^k$ **dont tous les coefficients sont nuls).**

3) **Soient** $P, Q \in \mathbb{C}[X]$ **premiers entre eux.**

Dire pourquoi il existe $U, V \in \mathbb{C}[X]$ tels que

$$I = U(A)P(A) + V(A)Q(A) .$$

4) Toujours en supposant P, Q premiers entre eux, montrer que

$$\operatorname{Ker} P(A) \cap \operatorname{Ker} Q(A) = \{0\} \text{ et } \operatorname{Ker}(P(A)Q(A)) = \operatorname{Ker} P(A) \oplus \operatorname{Ker} Q(A) .$$

Exercice D : **Soient**

$$d \in \mathbb{N}^* \ , \ a_{i\ ,0\leq i\leq d} \in \mathbb{Z} \text{ et } P \ := \ \sum_{i=0}^{d} a_i X^i \ \in \ \mathbb{Q}[X] \ .$$

1) Montrer que si $\frac{r}{s} \in \mathbb{Q}$ avec r et s des entiers premiers entre eux est une racine de P alors

$$r|a_0 \text{ et } s|a_d \ .$$

2) En déduire que si P est unitaire et a une racine rationnelle alors P a une racine entière.

Exercice E : (**Idéaux de** $\mathbb{K}[X]$)

Dans tout cet exercice $\mathbb{K}$ **est un corps et on note** $\mathbb{K}[X]$ **l'anneau des polynômes à une indéterminée sur** $\mathbb{K}$. **On appelle *idéal* de** $\mathbb{K}[X]$ **une partie non vide** $I \subset \mathbb{K}[X]$ **telle que, pour tout couple** $(P, Q) \in I \times I$ **et tout couple** $(R, S) \in \mathbb{K}[X] \times \mathbb{K}[X]$,

$$S * P \ + \ R * Q \ \in \ I \ .$$

1) Montrer qu'une partie $I \subset \mathbb{K}[X]$ est un idéal si et seulement si I est un sous-groupe de $(\mathbb{K}[X], +)$ et pour tout $P \ \in \ I$ et tout $Q \ \in \ \mathbb{K}[X], Q * P \in I$.

2) **a)** Pour tout $P \ \in \ \mathbb{K}[X]$ montrer que $I \ := \ \{P * Q \ , \ Q \in \mathbb{K}[X]\}$ et $\{0\}$ sont des idéaux de $\mathbb{K}[X]$.

b) Pour tout idéal $I \ \neq \ \{0\}$ de $\mathbb{K}[X]$ montrer qu'il existe un élément P de I de plus petit degré. Montrer qu'alors, pour tout $Q \ \in \ I$, il existe $R \ \in \ \mathbb{K}[X]$ tel que $Q \ = \ P * R$.

c) Donner une définition d'idéaux de $\mathbb{Z}$ et établir un résultat analogue.

Un élément P **défini comme ci-dessus est alors appelé un *générateur* de l'idéal** $I \ = \ P * \mathbb{K}[X]$. **On dit alors que** I **est un idéal *principal* de** $\mathbb{K}[X]$. **Comme nous avons montré que tout idéal de** $\mathbb{K}[X]$ **est principal, on dira que** $\mathbb{K}[X]$ **est un *anneau principal*.**

d) Caractériser les éléments de $I \ := \ P * \mathbb{K}[X]$ à l'aide de la relation de divisibilité dans $\mathbb{K}[X]$.

e) Que peut-on dire des polynômes P et Q s'ils sont générateurs d'un même idéal I ?

3) **Pour tout idéal** $I \subset \mathbb{K}[X]$, **on note** $\sim_I$ **la relation définie sur** $\mathbb{K}[X]$ **par** $P \sim_I Q$ **si** $P - Q \in I$.

a) Montrer que $\sim_I$ est une relation d'équivalence.

b) Montrer que $\sim_I$ est compatible aux lois $+$ et $*$ de $\mathbb{K}[X]$.

c) En déduire qu'il existe une unique structure d'anneau sur l'ensemble $\mathbb{K}[X]/I$ des classes modulo $\sim_I$ telle que la surjection canonique $\pi \ : \ \mathbb{K}[X] \ \to \ \mathbb{K}[X]/I$ soit un morphisme d'anneaux.

4) **Soit** $f \ : \ \mathbb{K}[X] \ \to \ A$ **un morphisme d'anneaux de** $\mathbb{K}[X]$ **dans un anneau commutatif** A.

a) Montrer que $\mathrm{Ker}\ f$ est un idéal de $\mathbb{K}[X]$.

b) Montrer qu'il existe un unique isomorphisme d'anneaux

$$\phi \ : \ \mathbb{K}[X]/\mathrm{Ker}\, f \ \rightarrow \ \mathrm{Im}\, f \text{ tel que } \phi \circ \pi \ = \ f$$

où $\pi \ : \ \mathbb{K}[X] \ \rightarrow \ \mathbb{K}[X]/\mathrm{Ker}\, f$ est la surjection canonique.

5) **a)** Pour tout couple $(P, Q) \in \mathbb{K}[X] \times \mathbb{K}[X]$, montrer que

$$(P) + (Q) \ := \ \{A * P + B * Q \ , \ (A, B) \in \mathbb{K}[X] \times \mathbb{K}[X]\}$$

est un idéal de $\mathbb{K}[X]$.

b) Montrer qu'un générateur D de l'idéal $(P) + (Q)$, est un PGCD de P et Q.

c) Que peut-on dire de deux PGCD D et D' de P et Q ?

Exercice F : Dans cet exercice, $\mathbb{K}$ est un corps commutatif et $\mathbb{K}[X]$ désigne l'anneau des polynômes à une indéterminée sur $\mathbb{K}$.

1) Montrer que l'intersection de deux idéaux de $\mathbb{K}[X]$ est encore un idéal de $\mathbb{K}[X]$.

2) 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 G : (**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 H : (Le corps $\mathbb{F}_9$**)**

On note $\mathbb{F}_3$ **le corps** $(\mathbb{Z}/3\mathbb{Z}, +, *)$, I **l'idéal** $(X^2 + 1) * \mathbb{F}_3[X]$ **et** $\mathbb{K}$ **le quotient** $\mathbb{F}_3[X]/I$. **Enfin on note** ω **la classe de** X **dans** $\mathbb{K}$.

1) Calculer ω^2.

2) a) Montrer que $\mathbb{K}$ est un $\mathbb{F}_3$-espace vectoriel dont $(1, \omega)$ est une base.

b) Quel est le cardinal c de $\mathbb{K}$?

3) a) Pour tout $(a, b) \in \mathbb{F}_3 \times \mathbb{F}_3$, $(a, b) \neq (0, 0)$ calculer l'inverse (s'il existe) de $a + b\omega$.

b) En déduire que $\mathbb{K}$ est un corps.

c) Le groupe abélien $(\mathbb{K}, +)$ est-il isomorphe au groupe abélien $(\mathbb{Z}/c\mathbb{Z}, +)$?

Exercice I : (Le corps $\mathbb{F}_{25}$**)**

Dans tout cet exercice, on note $\mathbb{K}\ :=\ (\mathbb{Z}/5\mathbb{Z}, +, *)$ **l'anneau des entiers modulo** 5.

1) Rappeler pourquoi $\mathbb{K}$ est un corps et ce que cela signifie.

Dans la suite, on note $\mathbb{K}[X]$ l'anneau des polynômes à une indéterminée sur $\mathbb{K}$ et $P := X^2 + X + 1 \in \mathbb{K}[X]$.

Par ailleurs, pour tout élément $a \in \mathbb{K}$, on identifie a et le polynôme de degré 0 dont le seul coefficient non nul est a.

Enfin pour tout $Q \in \mathbb{K}[X]$, on note $\overline{Q}$ la classe de Q modulo P c'est-à-dire l'ensemble des $Q' \in \mathbb{K}[X]$ tels que $P|Q' - Q$ et

$$\mathbb{L} := \mathbb{K}[X]/P = \{\overline{Q}\,,\, Q \in k[X]\}\,.$$

2) Rappeler, sans démonstration, comment est définie la structure d'anneau sur $\mathbb{L}$.

3) Pour tout $a \in \mathbb{K}$ et tout $Q \in \mathbb{K}[X]$, on note $a \cdot \overline{Q} := \overline{a * Q}$.

a) Calculer $\overline{X}^3$.

b) Montrer que, pour tout $\alpha \in \mathbb{L}$, il existe un unique couple $(a, b) \in \mathbb{K}^2$ tel que $\alpha = a + b\overline{X}$.

c) En déduire que $\mathbb{L}$ est un ensemble fini et donner son cardinal.

4) **a)** Le polynôme $X^2 + 1 \in \mathbb{K}[X]$ est-il irréductible ?

b) Montrer que P est un polynôme irréductible.

c) Montrer que, pour tout $Q \in \mathbb{K}[X]$ tel que $\overline{Q} \neq \overline{0}$, il existe $R \in \mathbb{K}[X]$ tel que $\overline{Q * R} = \overline{1}$.

d) En déduire que $\mathbb{L}$ est un corps.

5) Soient

$$\sigma : \mathbb{K}[X] \to \mathbb{K}[X]\,,\, Q \mapsto Q^5 \text{ et} \overline{\sigma} : \mathbb{L} \to \mathbb{L}\,,\, \alpha \mapsto \alpha^5\,.$$

a) Montrer que σ est un endomorphisme de $\mathbb{K}[X]$ différent de $\mathrm{Id}_{\mathbb{K}[X]}$.

b) Factoriser $X^5 - X$ dans $\mathbb{K}[X]$.

c) En déduire que $\overline{\sigma}$ est un endomorphisme de $\mathbb{L}$ différent de $\mathrm{Id}_{\mathbb{L}}$.

d) Montrer que $\overline{\sigma}^2 = \mathrm{Id}_{\mathbb{L}}$.

e) Calculer $\overline{\sigma}(\overline{X})$.

Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

Problème n° I

À rendre le 22 octobre 2014

Exercice A : (**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 $1 \leq i \leq d$.

Exercice B : (Algorithme d'EUCLIDE et théorème de BÉZOUT)

Considérons deux entiers relatifs a_0 et a_1.

1) Montrer que l'on définit bien des suites $a := (a_n)_{,n\in\mathbb{N}}$ et $q := (q_n)_{,n\in\mathbb{N}}$ en posant, pour tout $n \in \mathbb{N}$,

Euc$_1$) si $a_{n+1} \neq 0$, q_n est le quotient de la division euclidienne de a_n par a_{n+1} et a_{n+2} son reste ;

Euc$_2$) si $a_{n+1} = 0$, $q_n = a_{n+2} = 0$.

2) **a)** Montrer que, pour tout $n \geq 2$, $a_n \geq 0$.

On note $v := \min(\{a_n\ ,\ n \geq 2\}$.

b) Comparer a_n et a_{n+1} pour $n \geq 2$ et en déduire que $v = 0$.

Il existe donc un entier $p \geq 2$ tel que $a_p = 0$.

c) Montrer que, pour tout $q \geq p$, $a_q = 0$.

On suppose désormais que $a_0 \neq 0$ ou $a_1 \neq 0$.

d) Montrer qu'alors, il existe un plus grand entier naturel m tel que $a_m \neq 0$.

3) **a)** Si $m = 0$ ou 1, déterminer le **Pgcd** $a_0 \wedge a_1$ de a_0 et a_1.

b) Si $m \geq 2$, montrer que pour tout $n \leq m - 2$,

$$a_n \wedge a_{n+1} = a_{n+1} \wedge a_{n+2}$$

et en déduire que $a_m = a_0 \wedge a_1$.

4) **a)** Montrer que pour tout n, il existe des entiers u_n et v_n tels que $a_n = u_n a_0 + v_n a_1$.

b) En déduire qu'il existe des entiers u et v tels que :

$$a_0 \wedge a_1 = a_0 u + a_1 v\ . \qquad 1$$

c) Donner une formule permettant de calculer (u_{n+1}, v_{n+1}) en fonction de (u_n, v_n).

d) En déduire un algorithme permettant de calculer les coefficients u et v dans l'identité b).1. Il sont appelés *coefficients de* BÉZOUT.

e) Calculer le **Pgcd** et des coefficients de BÉZOUT pour les couples

$$(27, 23)\ ,\ (1789, 1969)\ ,\ (1965, 135)\ .$$

Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

Corrigé du Problème n° I

Exercice A : (**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 $b^{\deg(n)+1} > n$.

Solution : *Soit* $n\ \in\ \mathbb{N}^*$, *et* $B\ :=\ \{k\ \in\ \mathbb{N}\ ;\ b^k \leq n\}$. *L'ensemble* B *est une partie de* $\mathbb{N}$, *il est non vide puisque* $b^0\ =\ 1\ \in\ B$ *et il est majoré. Cette dernière affirmation méritant peut-être d'être justifiée. Mais* $b > 1$ *par hypothèse. On peut donc écrire* $b\ =\ 1 + c$ *avec* $c > 0$. *Il s'ensuit que*

$$\forall k \in \mathbb{N},\ b^{k+1}\ =\ (1+c)^{k+1}\ =\ (1+c)b^k\ .$$

Il s'ensuit que

$$(b^k > k\ \Rightarrow\ b^{k+1}\ =\ (1+c)b^k > (1+c)k > k+1)\ .$$

On a donc montré par récurrence que

$$\forall k \in \mathbb{N},\ b^k > k\ .$$

Il en résulte que

$$(b^k \leq n\ \Rightarrow\ k \leq n)\ .$$

Ceci entraîne en particulier que n *est un majorant de* B.

Il résulte alors (cf. cours I.1.2.8,) que B *possède un plus grand élément* $\deg(n)$. *Or* $\deg(n)+1 > \deg(n)$ *si bien que* $\deg(n)+1 \notin B$ *c'est-à-dire que* $b^{\deg(n)+1} > n$.

b) Montrer qu'il existe des entiers q et r tels que $n = b^{\deg(n)}q+r$ avec $0 < q < b$ et $0 \leq r < b^{\deg(n)}$.

Solution : *Effectuons la division euclidienne de n par $b^{\deg(n)}$ (cf. cours I.3.2.3.) Il existe alors un unique couple (q, r) d'entiers relatifs tels que*

$$n = b^{\deg(n)}q + r \text{ et } 0 \leq r < b^{\deg(n)} .$$

Reste à donner l'encadrement de q.

Or d'après a) :

$$\begin{array}{rccccc} & 0 & < & n & < & b^{\deg(n)+1} \\ \Rightarrow & 0 & < & b^{\deg(n)}q + r & < & b^{\deg(n)+1} \\ \Rightarrow & 0 & \leq & r & < & b^{\deg(n)}(b-q) \\ \Rightarrow & 0 & < & b-q & & \\ \Rightarrow & q & < & b & & \end{array}$$

ce qui donne la partie droitte de l'encadrement.

Par ailleurs :

$$\begin{array}{rccc} & 0 & < & n \\ \Rightarrow & & < & b^{\deg(n)}q + r \\ \Rightarrow & -r & < & b^{\deg(n)}q \\ \Rightarrow & -b & < & b^{\deg(n)}q \\ \Rightarrow & 0 & \leq & q \end{array}$$

ce qui achève de donner l'encadrement de q.

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

$$n = \sum_{i=0}^{d} n_i b^i .$$

Solution : *pour tout $k \in \mathbb{N}$, notons :*

$$I_k := [1; b^{k+1}[. \qquad 1$$

Comme $\forall k \in \mathbb{N},\ , [b^k; b^{k+1}[\subset I_k$, et que le point a) signifie exactement que $\mathbb{N}^* = \bigcup_{k\in\mathbb{N}} [b^k; b^{k+1}[$, on a :

$$\mathbb{N}^* = \bigcup_{k\in\mathbb{N}} I_k . \qquad 2$$

Pour $(k, n) \in \mathbb{N}^* \times \mathbb{N}^*$, on dira que le couple (k, n) a la propriété $\mathcal{B}$, ce qu'on notera $\mathcal{B}(k, n)$, s'il existe un entier $d < k$, et des entiers $n_{i\ ,0\leq i\leq d}$ satisfaisant aux conditions 1 et 2 de l'énoncé et tels que

$$n = \sum_{i=0}^{d} n_i b^i .$$

Notons encore :

$$A := \{k \in \mathbb{N}^* ; \forall n \in I_k,\ \mathcal{B}(k, n)\} \subset \mathbb{N}^* . \qquad 3$$

Pour répondre à la question il faut établir que $A = \mathbb{N}^*$. Or :

i) $(1 \in A)$

En effet, pour tout $n \in I_1$, i.e.

$$\forall 1 \leq n < b,$$

$d = 0$ et $n_0 = n$ donnent à $(1, n)$ la propriété $\mathcal{B}$.

ii) $(k \in A \Rightarrow k+1 \in A)$
Pour $k \in \mathbb{N}^*$ *et* $n \in I_{k+1}$:

$*$) *Soit* $n \in I_k$ *et si l'on suppose* $k \in A$, *alors* $\mathcal{B}(k,n)$.

†) *soit* $n \in [b^k; b^{k+1}[$. *Il se trouve, en vertu de a) que* k *est précisément l'entier* $\deg(n)$. *Il existe alors, grâce à b) un couple* (q,r) *avec :*

$$0 \leq r < b^k \text{ et } 0 \leq q < b\,.$$

Si $r = 0$,

$$d := k\,,\ n_d := q\,,\ \forall 0 \leq i < d n_i := 0$$

donnent à $(k+1,n)$ *la propriété* $\mathcal{B}$. *Enfin si* $r \neq 0$, $r \in I_k$. *Si donc on suppose* $k \in A$, *il existe*

$$\delta < k\,,\ r_{i\,,0\leq i\leq\Delta}\,,\ 0 \leq r_i < b\ r = \sum_{i=0}^{\Delta} r_i b^i\,.$$

Prenons alors :

$$d := k\,,\ \forall 0 \leq i \leq \Delta,\ n_i := r_i\,,\ \forall \delta < i < d\ n_i := 0 \text{ et } n_d := q\,.$$

On constate alors que $(k+1,n)$ *vérifie* $\mathcal{B}$.

d) Généraliser le résultat précédent à un entier $z \in \mathbb{Z}^*$.
Solution : *Pour tout* $z \in \mathbb{Z}^*$, *si* $z \in \mathbb{N}^*$ *il existe, grâce à c),*

$$d\,,\ z_{i\,,0\leq i\leq d}$$

vérifiant 1 et 2. En prenant $\epsilon := 1$, *on a également 3.*
Si $z \notin \mathbb{N}^*$, $-z \in \mathbb{N}^*$. *En appliquant alors les résultats de c) à* $-z$, *et en prenant* $\epsilon := -1$, *on obtient encore la conclusion.*

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 $\epsilon = \eta$.
Solution : *Il suffit de constater que*

$$\sum_{i=0}^{d} x_i b^i \in \mathbb{N}^*, \sum_{i=0}^{e} y_i b^i \in \mathbb{N}^*$$

et de rappeler que $\mathbb{Z}^* = \mathbb{N}^* \cup -\mathbb{N}^*$ *avec* $\mathbb{N}^* \cap -\mathbb{N}^* = \emptyset$.

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 $d = e$.
Solution :

i) Montrons d'abord que pour tout $d+1$ -uplet u_i ,$_{0\leq i\leq d}$, tel que $\forall 0 \leq i \leq d,\ 0 \leq u_i < b$, on a

$$\sum_{i=1}^{d} u_i b^i b^{d+1} \ .$$

Pour $d = 0$ le résultat est tautologique. Supposons donc le résultat connu pour d et considérons un $d+2$-uplet u_i ,$_{0\leq i\leq d+1}$ tel que $\forall 0 \leq i \leq d+1,\ 0 \leq u_i < b$. On a alors :

$$\begin{aligned}
\sum_{i=0}^{d+1} u_i b^i &= \sum_{i=0}^{d} u_i b^i + u_{d+1} b^{d+1} \\
&< b^{d+1} + u_{d+1} b^{d+1} \\
&< b^{d+1} + (b-1) b^{d+1} \\
&< b^{d+2}
\end{aligned}$$

ce qui établit le résultat par récurrrence.

ii) Si donc x_i ,$_{0\leq i\leq d}$ est un d-uplet vérifiant 1 et 2 on a

$$b^d \leq \sum_{i=0}^{d} x_i b^i < b^{d+1} \ .$$

En appliquant l'unicité dans la question 1), a), on a $d \ = \ \deg\big(\sum_{i=0}^{d} x_i b^i\big)$. Il s'ensuit que :

$$\begin{aligned}
\sum_{i=0}^{d} x_i b^i &= \sum_{i=0}^{e} y_i b^i \\
\Rightarrow \quad \deg\big(\sum_{i=0}^{d} x_i b^i\big) &= \deg\big(\sum_{i=0}^{e} y_i b^i\big) \\
\Rightarrow \quad d &= e \ .
\end{aligned}$$

c) Montrer que b divise $x_0 - y_0$ et en déduire que $x_0 \ = \ y_0$.
Solution : *On a :*

$$z \ = \ \epsilon \sum_{i=0}^{d} x_i b^i \ = \ \eta \sum_{i=0}^{e} y_i b^i \ .$$

Ceci entraîne grâce à a) et b),

$$\begin{aligned}
\sum_{i=0}^{d} x_i b^i &= \sum_{i=0}^{d} y_i b^i \\
\Rightarrow \quad x_0 - y_0 &= \sum_{i=1}^{d} (y_i - x_i) b^i \\
\Rightarrow \quad x_0 - y_0 &= b \sum_{i=1}^{d} (y_i - x_i) b^{i-1}
\end{aligned}$$

c'est à dire que $b|(x_0 - y_0)$; ce qui entraîne encore $b||x_0 - y_0|$. Or il découle de 1 que $|x_0 - y_0| < b$ si bien que $|x_0 - y_0| \ = \ 0$ i.e.

$$x_0 \ = \ y_0 \ .$$

d) Montrer finalement (par récurrence) que $x_i = y_i$ pour tout $1 \leq i \leq d$.
Solution : *Notons :*

$$\mathcal{H}_k \ : \ \forall 0 \leq i \leq k, \ x_i = y_i \ .$$

Nous venons de montrer $\mathcal{H}_0$ en c). Si l'on fait l'hypothèse $\mathcal{H}_k$, on a :

$$\begin{aligned}
& \sum_{i=0}^{d} x_i b^i = \sum_{i=0}^{d} y_i b^i \\
\Rightarrow \quad & \sum_{i=k+1}^{d} x_i b^i = \sum_{i=k+1}^{d} y_i b^i \\
\Rightarrow \quad & b^{k+1}(x_{k+1} - y_{k+1} = \sum_{i=k+2}^{d} (y_i - x_i) b^i \\
\Rightarrow \quad & b^{k+1}(x_{k+1} - y_{k+1}) = b^{k+2} \sum_{i=k+2}^{d} (y_i - x_i) b^{i--k-2} \\
\Rightarrow \quad & (x_{k+1} - y_{k+1}) = b \sum_{i=k+2}^{d} (y_i - x_i) b^{i--k-2}
\end{aligned}$$

c'est à dire que $b|(x_{k+1} - y_{k+1})$; ce qui entraîne encore $b||x_{k+1} - y_{k+1}|$. Or il découle de 1 que $|x_{k+1} - y_{k+1}| < b$ si bien que $|x_{k+1} - y_{k+1}| = 0$ i.e.$x_{k+1} = y_{k+1}$ c'est-à-dire qu'on a montré que $\mathcal{H}_k \Rightarrow \mathcal{H}_{K+1}$ et finalement par récurrence que $\mathcal{H}_k$ est vérifiée pour tout k.

Exercice B : (Algorithme d'EUCLIDE et théorème de BÉZOUT)
Considérons deux entiers relatifs a_0 et a_1.

1) Montrer que l'on définit bien des suites $a := \big(a_n\big)_{,n\in\mathbb{N}}$ et $q := \big(q_n\big)_{,n\in\mathbb{N}}$ en posant, pour tout $n \in \mathbb{N}$,

Euc$_1$) si $a_{n+1} \neq 0$, q_n est le quotient de la division euclidienne de a_n par a_{n+1} et a_{n+2} son reste ;

Euc$_2$) si $a_{n+1} = 0$, $q_n = a_{n+2} = 0$.
Solution :

a) Par hypothèse le domaine de définition D_a de la suite a, contient 0 et 1 tandis que :
— *Si $a_1 = 0$ on posera pour satisfaire Euc$_2$) $q_0 := 0$ alors 0 appartient au domaine D_q de définition de q.*
— *Si $a_1 \neq 0$ le théorème de la division euclidienne (cf. I.3.2.3,) assure qu'il existe un unique couple (q_0, a_2) tel que*

$$a_0 = q_0 a_1 + a_2 \text{ et } 0 \leq a_2 < |a_1|$$

si bien que 0 appartient encore au domaine de définition D_q de q.

b) Soit

$$\mathcal{H}_k \ : \ \forall 0 \leq i \leq k, \ i \in D_q \ , \ \forall 0 \leq i \leq k+1, \ i \in D_a \ .$$

Nous venons d'établir $\mathcal{H}_0$ en a). Le fait que $\mathcal{H}_k \Rightarrow \mathcal{H}_{k+1}$ résulte du fait que pour un entier, il n'y a pas d'autre possibilité que d'être ou de ne pas être nul et du théorème de la division euclidienne.

c) On a donc établi par récurrence que

$$D_q = D_a = \mathbb{N}$$

ce qui signifie exactement que les suites a et q sont définies.

2) **a)** Montrer que, pour tout $n \geq 2$, $a_n \geq 0$.

Solution : *Pour tout $n \geq 2$, soit a_n est définit comme en question 1), Euc$_1$) et dans ce cas, le théorème de la division euclidienne I.3.2.3 assure que $0 \leq a_n < |a_{n-1}|$; soit a_n est défini comme en question 1), Euc$_2$) et dans ce cas vaut 0 ; si bien qu'on a dans tous les cas $a_n \geq 0$.*

On note $v := \min(\{a_n\ ,\ n \geq 2\}$.

b) Comparer a_n et a_{n+1} pour $n \geq 2$ et en déduire que $v = 0$.

Solution : *Pour $n \geq 2$, si $a_n \neq 0$, a_{n+1} est le reste de la division euclidienne de a_{n-1} par a_n et par conséquent, $a_{n+1} < a_n$. Si $a_n = 0$, $a_{n+1} = 0$.*

L'ensemble $P := \{a_n n \geq 2\}$ est une partie de $\mathbb{N}$ qui possède donc un plus petit élément $v = a_p$ (cf. I.1.2.7.)

$$\forall n \geq 2\ ,\ a_n \in P\ ,\ a_n > 0\ \Rightarrow\ a_{n+1} \in P a_{n+1} < a_n$$

d'après ce qui précède. Il en résulte, par contraposée, que $a_p = 0$.

Il existe donc un entier $p \geq 2$ tel que $a_p = 0$.

c) Montrer que, pour tout $q \geq p$, $a_q = 0$.

Solution : *Mmontrons que*

$$\forall k \in \mathbb{N},\ a_{p+k} == 0\ .$$

Ceci est vérifié pour $k = 0$, par hypothèse sur a_p. Si $a_{p+k} = 0$, a_{p+k+1} est défini par question 1), Euc$_2$) et $a_{p+k+1} = 0$ ce qui prouve le résultat demandé par récurrence.

On suppose désormais que $a_0 \neq 0$ ou $a_1 \neq 0$.

d) Montrer qu'alors, il existe un plus grand entier naturel m tel que $a_m \neq 0$.

Solution : *Considérons*

$$P := \{n \in \mathbb{N}\ ;\ a_n \neq 0\} \subset \mathbb{N}\ .$$

Par hypothèse, $P \neq \emptyset$ et, d'après le point précédent, P est majorée par p. La partie P a donc un plus grand élément m (cf. I.1.2.8.)

3) **a)** Si $m = 0$ ou 1, déterminer le **Pgcd** $a_0 \wedge a_1$ de a_0 et a_1.

Solution :

i) $(m = 0)$

Si $m = 0, a_1 = 0$ et

$$a_0 \wedge a_1 = a_0 = a_m\ .$$

ii) $(m = 1)$

Alors $a_2 = 0$ c'est-à-dire que le reste de la division euclidienne de a_0 par a_1 est nul ou encore que

$$a_1 | a_0\ \Rightarrow\ a_0 \wedge a_1 = a_1 = a_m\ .$$

b) Si $m \geq 2$, montrer que pour tout $n \leq m-2$,

$$a_n \wedge a_{n+1} = a_{n+1} \wedge a_{n+2}$$

et en déduire que $a_m = a_0 \wedge a_1$.

Solution :

i) $(a_n \wedge a_{n+1} = a_{n+1} \wedge a_{n+2})$

Notons $d_n := a_n \wedge a_{n+1}$ *et* $d_{n+1} := a_{n+1} \wedge a_{n+2}$. *On sait d'après question 2), c) que*

$$\forall n \leq m\ ,\ a_n \neq 0\ .$$

Il s'ensuit qu'on a la relation (cf. question 1), Euc$_1$*),)*

$$a_n = q_n a_{n+1} + a_{n+2}\ .$$

D'où

$$\big(d_{n+1}|a_{n+1} \text{ et } d_{n+1}|a_{n+2} \Rightarrow d_{n+1}|a_n\big)\ .$$

Il s'ensuit que :

$$d_{n+1}|d_n\ . \qquad 1$$

En outre

$$\big(d_n|a_n \text{ et } d_n|a_{n+1} \Rightarrow d_n|a_n - q_n a_{n+1} = a_{n+2}\big)$$

si bien que :

$$d_n|d_{n+1}\ . \qquad 2$$

Finalement 2 et 1 entraînent

$$d_n = d_{n+1}\ .$$

ii) $(a_m = a_0 \wedge a_1)$

On peut établir, par récurrence sur l'indice n *grâce au point précédent, que*

$$a_0 \wedge a_1 = a_{m-1} \wedge a_m\ .$$

Or par construction de m*, (cf. question 2), d),)*

$$a_m \neq 0 \text{ et } a_{m+1} = 0\ .$$

Donc en vertu de question 1), Euc$_1$*)*

$$\big(0 = a_{m+1} = a_{m-1} - q_{m-1}a_m \Rightarrow a_m|a_{m-1}\big) \Rightarrow a_m = a_m \wedge a_{m-1} = a_0 \wedge a_1\ .$$

4) **a)** Montrer que pour tout n, il existe des entiers u_n et v_n tels que $a_n = u_n a_0 + v_n a_1$.

Solution :

i) En fait l'existence de tels entiers peut se prouver absttraitement sans besoin de les construire ce qui n'est en fait pas très utile. Cependant, on a montré à la question 3), b) que

$$a_0 \wedge a_1 = a_n \wedge a_{n+1}$$

ce qui entraîne en particulier que

$$a_n \in (a_0 \wedge a_1)\mathbb{Z} = \{a_0 x + a_1 y\ ,\ (x,y) \in \mathbb{Z} \times \mathbb{Z}\}\ .$$

ii) néanmoins on aimerait disposer de suites $\left(u_n\right)_{,n\in\mathbb{N}}$ et $\left(v_n\right)_{,n\in\mathbb{N}}$ construite de manière explicite (et qu'on puisse calculer.) En effet, on remarque en particulier que :

$$a_m \;=\; u_m a_0 \;+\; v_m a_1 \qquad 1$$

signifie que (u_m, v_m) est un couple de coefficients de BÉZOUT *pour (a_0, a_1) (cf. I.3.3.2.)*

Posons alors

$$u_0 \;:=\; 1\;,\; u_1 \;:=\; 0\;,\; v_0 \;:=\; 0\;,\; v_1 \;:=\; 1\;.$$

On a alors immédiatement

$$\mathcal{H}_0 \;:\; a_0 \;=\; u_0 a_0 \;+\; v_0 a_1 \text{ et } a_1 \;=\; u_1 a_0 \;+\; v_1 a_1\;.$$

Définissons maintenant les suites $\left(u_n\right)_{,n\in\mathbb{N}}$ et $\left(v_n\right)_{,n\in\mathbb{N}}$ par récurrence par :

$$u_{n+2} \;:=\; u_n - q_n u_{n=1} \text{ et } v_{n+2} \;:=\; v_n - q_n v_{n+1}$$

qui est exactement la formule qui définit a_n au moins pour $n \leq m$, (cf. question 1), Euc$_1$).) Les suites $\left(u_n\right)_{,n\in\mathbb{N}}$ et $\left(v_n\right)_{,n\in\mathbb{N}}$ sont bien définies par les formules de récurrence ci-dessus et l'on a :

$$\forall n \leq m-2\;,\; \begin{pmatrix} a_{n+2} & u_{n+2} & v_{n+2}\end{pmatrix} \;=\; \begin{pmatrix} 1 & -q_n\end{pmatrix} \begin{pmatrix} a_n & u_n & v_n \\ a_{n+1} & u_{n+1} & v_{n+1}\end{pmatrix}\;. \qquad 2$$

Il faut maintenant vérifier que la propriété $\mathcal{H}_n$ est vérifiée. Comme on a établi $\mathcal{H}_0$ il suffit de vérifier maintenant que $\mathcal{H}_n \Rightarrow \mathcal{H}_{n+2}$. Or :

$$\begin{aligned} a_{n+2} &= a_n - q_n a_{n+1} \\ &= u_n a_0 + v_n a_1 - q_n(u_{n+1}a_0 + v_{n+1}a_1) \\ &= (u_n - q_n u_{n+1})a_0 + (v_n - q_n v_{n+1})a_1 \\ &= u_{n+2}a_0 + v_{n+2}a_1\;. \end{aligned}$$

b) En déduire qu'il existe des entiers u et v tels que :

$$a_0 \;\wedge\; a_1 \;=\; a_0 u \;+\; a_1 v\;. \qquad 1$$

Solution : *Ce résultat est connu a priori (cf. I.3.3.2,) mais peut-être obtenu indépendamment puisque la construction de ce problème montre explicitment l'existence des entiers u_m et v_m qui répondent à la question. On peut redémontrer de cette manière le théorème de* BÉZOUT *(cf. I.3.3.3.)*

*De quelque manière qu'on procède, soit en passant par la construction des sous-groupes de $\mathbb{Z}$ (cf. I.3.2.6,) soit en passant par l'algorithme d'*EUCLIDE *comme dans ce problème, l'ingrédient essentielle reste le théorème de la division euclidienne I.3.2.3.*

c) Donner une formule permettant de calculer (u_{n+1}, v_{n+1}) en fonction de (u_n, v_n).

Solution : *En fait on a donné une formule permettant de calculer $\cdot_{n+2}$ en fonction de $\cdot_n$ et $\cdot_{n+1}$ (cf. a).ii).2,) et on ne peut pas espérer mieux.*

d) En déduire un algorithme permettant de calculer les coefficients u et v dans l'identité b).1. Il sont appelés *coefficients de* BÉZOUT.

Solution : *On a montré en a).ii).1 que les coefficients de* BÉZOUT *étaient les termes* (u_m, v_m) *où* m *est défini comme le dernier indice pour lequel* a_n *est non nul (cf. question 2), d).) Un algorithme permettant de calculer* (u_m, v_m) *est donc un algorithme permettant de calculer les* m *premiers termes des suites* $\left(u_n\right)_{,n\in\mathbb{N}}$ *et* $\left(v_n\right)_{,n\in\mathbb{N}}$. *Cet algorithme est en fait contenu dans la formule a).ii).2. Cette formule signifiant en particulier que le mode de calcul du* $n+2^{\text{ième}}$ *terme en fonction du* $n^{\text{ième}}$ *et du* $n+1^{\text{ième}}$ *est le même pour les trois suites* $\left(a_n\right)_{,n\in\mathbb{N}}$, $\left(u_n\right)_{,n\in\mathbb{N}}$ *et* $\left(v_n\right)_{,n\in\mathbb{N}}$ *incite à présenter les calculs dans un tableau de la forme suivante :*

q	a	u	v
	a_0	1	0
	a_1	0	1
q_0	$a_2 = a_1 - q_0 a_1$	$u_2 = 1$	$v_2 = -q_0$
$\dots$	$\dots$	$\dots$	$\dots$
q_{n-2}	a_n	u_n	v_n
q_{n-1}	a_{n+1}	u_{n+1}	v_{n+1}
q_n	$a_{n+2} = a_n - q_n a_{n+1}$	$u_{n+2} = u_n - q_n u_{n+1}$	$v_{n+2} = v_n - q_n v_{n+1}$
$\dots$	$\dots$	$\dots$	$\dots$
q_{m-2}	a_m	u_m	v_m

e) Calculer le **Pgcd** et des coefficients de BÉZOUT pour les couples

$$(27, 23)\ ,\ (1789, 1969)\ ,\ (1965, 135)\ .$$

Solution : *On met en œuvre l'algorithme présenté en d). On s'aperçoit que quel que soit l'ordre dans lequel sont donnés* a_0 *et* a_1, *il est astucieux de les permuter pour obtenir* $a_0 \geq a_1$ *ce qui fait gagner une étape.*

i) *(*$(27, 23)$*)*

	27	1	0
	23	0	1
1	4	1	-1
5	3	-5	6
1	1	6	-7

d'où il résulte que

$$27 \wedge 23 = 1 \text{ et } 6 * 27 - 7 * 23 = 1\ .$$

ii) *(*$(1789, 1969)$*)*

	1969	1	0
	1789	0	1
1	180	1	-1
9	169	-9	10
1	11	10	-11
15	4	-159	175
2	3	328	-361
1	1	-487	536

d'où il vient

$$1969 \wedge 1789 = 1 \text{ et } 536 * 1789 - 487 * 1969 = 1\ .$$

iii) $((1965, 135))$

On remarque d'abord que $1965 = 5 * 393$ *et* $135 = 5 * 27$, *puis on remarque que* $393 = 3 * 131$ *et* $27 = 3 * 9$. *Si bien qu'on a*

$$\big(1965 = 15 * 131 \text{ et} 135 = 15 * 9 \Rightarrow 1965 \wedge 135 = 15 * (131 \wedge 9)\big) .$$

Reste donc à calculer $131 \wedge 9$. *On peut d'ores et déjà affirmer que ce* ***Pgcd*** *vaut* 1, *puisque* 3 *ne divise pas* 131 *(*$1 + 3 + 1 = 5$ *(cf. TD n° II, exercice G.)) Reste donc à déterminer les coefficients de* BÉZOUT *:*

$$\begin{array}{ccccc} & 131 & 1 & 0 \\ & 9 & 0 & 1 \\ 14 & 5 & 1 & -14 \\ 1 & 4 & -1 & 15 \\ 1 & 1 & 2 & -29 \end{array}$$

d'où il résulte que

$$131 \wedge 9 = 1 \text{ et } 2 * 131 - 29 * 9 = 1$$

ce qui entraîne finalement

$$1965 \wedge 135 = 15 \text{ et } 2 * 1965 - 29 * 135 = 15 .$$

Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

Problème n° III

À rendre le 10 décembre 2014

Si un résultat a déjà été établi dans le cours ou dans un exercice de TD on le citera avec suffisamment de précision sans le redémontrer.

Dans tout cet exercice, pour $A := \{a_1, \ldots, a_n\}$ **un sous-ensemble fini d'un ensemble** E **on notera** $(a_1 \ldots a_n)$ **la permutation circulaire sur** A **telle que** $a_i \mapsto a_{i+1}\ \forall 1 \leq i \leq n-1,\ a_n \mapsto a_1$. **Ainsi** (ab) **désigne la transposition de support** $\{a, b\} \subset E$, **pour** $a \neq b$.

1) **Soient** $(G, *)$ **un groupe fini à** $2k$ **éléments,** $k \in \mathbb{N}^*$, **et** H **un sous-groupe de** G **à** k **éléments.**

a) Pourquoi le groupe quotient G/H existe-t-il ? Quel est ce groupe ?

b) En déduire que, pour tout $g \in G$, $g * g \in H$.

2) **a)** Rappelez la définition du groupe alterné $\mathcal{A}_4$.

b) Quel est le cardinal de $\mathcal{A}_4$?

3) **a)** Montrer que, pour tout $n \geq 3$, un cycle de longueur 3 (un 3-cycle) est une permutation paire (*i.e.*un élément de $\mathcal{A}_n$.)

b) Combien de parties de $\{1, 2, 3, 4\}$ sont des supports de cycles de longueur 3 dans $\mathcal{A}_4$?

c) Combien de cycles de longueur 3 peuvent avoir le même support ?

d) En déduire le nombre de 3-cycles dans $\mathcal{A}_4$.

4) **Soient** x, y, z **trois éléments de** $[1; 4]$ **distincts deux à deux.**

a) Calculer $(xzy)^2$.

b) En déduire que pour tout 3-cycle $c \in \mathcal{A}_4$ il existe un élément $d \in \mathcal{A}_4$ tel que $d^2 = c$.

c) En déduire que si H est un sous-groupe d'ordre 6 de $\mathcal{A}_4$, il contient tous les 3-cycles.

d) En déduire finalement que $\mathcal{A}_4$ ne possède pas de sous-groupe d'ordre 6.

5) **a)** Montrer qu'un élément de $\mathcal{A}_4$ est soit l'identité, soit un produit de deux transpositions à supports disjoints, soit un 3-cycle.

b) Pour x, y, z, t des éléments de $[1; 4]$ distincts deux à deux, calculer $(xyz)(yzt)$.

c) En déduire que $\mathcal{A}_4$ est engendré par les 3-cycles.

Pour $(G, *)$ un groupe, on note

$$\forall g \in G,\ \forall h \in G,\ [g,h] \ :=\ g * h * g^{-1} * h^{-1}$$

qu'on appelle *commutateur* de g et h. On note $D(G)$ le sous-groupe de G engendré par les éléments de la forme $[g,h]$ qu'on appelle *sous-groupe dérivé* de G.

6) a) Que vaut $D(G)$ si G est abélien ? Y-a-t il une assertion réciproque ?

b) Étant donné un morphisme de groupes $f\ :\ G\ \to\ H$, déterminer pour tout $(g,h) \in G \times G$, $f([g,h])$ en fonction de $[f(g), f(h)]$. En déduire que $f(D(G))\ \subset\ D(h)$.

Pour tout couple (g,k) d'éléments de G, on note $g^k\ :=\ k * g * k^{-1}$ le conjugué (cf. II.1.3.1,) de g par k.

Pour tout triplet (g,h,k) d'éléments de G calculer en fonction de g^k et h^k :

c) $(g * h)^k$;

d) $(g^{-1})^k$;

e) $[g,h]^k$.

f) En déduire que $D(G)$ est un sous-groupe distingué de G.

g) Montrer que le groupe $G_{\mathrm{Ab}}\ :=\ G/D(G)$ est abélien. On notera $\pi\ :\ G\ \to\ G_{\mathrm{Ab}}$ la surjection canonique.

h) Pour tout morphisme de groupes $f\ :\ G\ \to\ A$ où A est un groupe abélien, montrer qu'il existe un unique morphisme de groupes $\overline{f}\ :\ G_{\mathrm{Ab}}\ \to\ A$ tel que $f\ =\ \overline{f}\ \circ\ \pi$.

7) Soit $n \geq 2$ un entier.

a) Montrer que, pour tout $s\ \in\ \mathcal{S}_n$, s et son inverse ont même signature.

b) En déduire que, pour tout $n \geq 2$, $D(\mathcal{S}_n)\ \subset\ \mathcal{A}_n$.

c) Montrer finalement que $\mathcal{A}_4\ =\ D(\mathcal{S}_4)$.

Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

Corrigé du Problème n° III

Si un résultat a déjà été établi dans le cours ou dans un exercice de TD on le citera avec suffisamment de précision sans le redémontrer.

Dans tout cet exercice, pour $A := \{a_1, \ldots, a_n\}$ **un sous-ensemble fini d'un ensemble** E **on notera** $(a_1 \ldots a_n)$ **la permutation circulaire sur** A **telle que** $a_i \mapsto a_{i+1}\ \forall 1 \leq i \leq n-1,\ a_n \mapsto a_1$. **Ainsi** (ab) **désigne la transposition de support** $\{a, b\} \subset E$, **pour** $a \neq b$.

1) Soient $(G, *)$ **un groupe fini à** $2k$ **éléments,** $k \in \mathbb{N}^*$, **et** H **un sous-groupe de** G **à** k **éléments.**

a) Pourquoi le groupe quotient G/H existe-t-il ? Quel est ce groupe ?

Solution : *D'après le TD n° IV, exercice G, question 2), H est un sous-groupe distingué de G (cf. II.1.3.5.) Il résulte alors de II.1.3.7.i) que G/H possède une structure de groupe. Par ailleurs il résulte de II.1.2.2.iv) que dans le cas de l'énoncé $\#(G/H) = 2$ et finalement du TD n° IV, exercice B, question 1) que*

$$G/H \cong \mathbb{Z}/2\mathbb{Z}\ .$$

b) En déduire que, pour tout $g \in G$, $g * g \in H$.

Solution : *Notons $\pi : G \to G/H$ la surjection canonique. Alors*

$$\forall g \in G,\ \pi(g * g) = \pi(g) + \pi(g) = 0 \in \mathbb{Z}/2\mathbb{Z} \Rightarrow g * g \in \operatorname{Ker}\pi = H\ .$$

2) a) Rappelez la définition du groupe alterné $\mathcal{A}_4$.

Solution : *(cf. II.2.4.5.i).)*

b) Quel est le cardinal de $\mathcal{A}_4$?

Solution : *On a*

$$\#(\mathcal{A}_4) = \frac{1}{2}\#(\mathcal{S}_4) = \frac{1}{2}4! = 12\ .$$

3) a) Montrer que, pour tout $n \geq 3$, un cycle de longueur 3 (un 3-cycle) est une permutation paire (*i.e.*un élément de $\mathcal{A}_n$.)

Solution : *(cf. II.2.4.2.c).)*

b) Combien de parties de $\{1, 2, 3, 4\}$ sont des supports de cycles de longueur 3 dans $\mathcal{A}_4$?

Solution : *Une partie à 3 éléments de $\{1, 2, 3, 4\}$ est le support d'un 3-cycle. Ces parties sont au nombre de*

$$C_4^3 = 4\ .$$

c) Combien de cycles de longueur 3 peuvent avoir le même support ?

Solution : *L'ensemble $\{x, y, z\}$ est le support des cycles (xyz) et (xzy) autrement dit deux 3-cycles et deux seulement ont le même support.*

d) En déduire le nombre de 3-cycles dans $\mathcal{A}_4$.
Solution : *Il résulte des points précédents que* $\mathcal{A}_4$ *contient* $2 * 4 = 8$ 3*-cycles.*

4) Soient x, y, z **trois éléments de** $[1; 4]$ **distincts deux à deux.**

a) Calculer $(xzy)^2$.
Solution : *On a :* $(xzy)^2 = (xyz)$.

b) En déduire que pour tout 3-cycle $c \in \mathcal{A}_4$ il existe un élément $d \in \mathcal{A}_4$ tel que $d^2 = c$.
Solution : *Pour* $c = (xyz)$ *on a* $(xzy)^2$ *avec* $(xzy) \in \mathcal{A}_4$ *d'après la question 3), a).*

c) En déduire que si H est un sous-groupe d'ordre 6 de $\mathcal{A}_4$, il contient tous les 3-cycles.
Solution : *Pour tout* $d \in \mathcal{A}_4$, $d^2 \in H$, *d'où il résulte que* H *contient tous les* 3*-cycles. On conclut grâce à la question précédente, à la question 1), b) et à la question 2), b).*

d) En déduire finalement que $\mathcal{A}_4$ ne possède pas de sous-groupe d'ordre 6.
Solution : *On vient de montrer qu'un tel sous-groupe contiendrait tous les* 3*-cycles or ceux-ci sont au nombre de* 8 *en vertu de la question 3), d).*

5) a) Montrer qu'un élément de $\mathcal{A}_4$ est soit l'identité, soit un produit de deux transpositions à supports disjoints, soit un 3-cycle.
Solution : *Rappelons que* $\#(\mathcal{A}_4) = 12$ *(cf. question 2), b).) Or nous avons déjà identifié* 8 *de ses éléments qui sont les* 3*-cycles (cf. question 3), d).)*
Pour x, y, z, t *des éléments deux à deux distincts de* $\{1, 2, 3, 4\}$, $\sigma((xy)(zt)) = \sigma((xy))\sigma((zt)) = 1$ *c'est-à-dire que* $(xy)(zt) \in \mathcal{A}_4$. *Or les parties* $\{x, y\} \subset \{1, 2, 3, 4\}$ *et* $\{z, t\} \subset \{1, 2, 3, 4\}$ *déterminent le même élément* $(xy)(zt)$. *Il s'ensuit qu'il y a* 2 *fois moins d'éléments de type* $(2, 2)$ *que de parties à* 2 *éléments parmi* 4 *i.e.* $\frac{1}{2}C_4^2 = 3$. *Nous avons donc identifié* 11 *des* 12 *éléments de* $\mathcal{A}_4$ *le douzième étant bien entendu l'identité qu'i ne correspond à aucun des deux types précédents.*

b) Pour x, y, z, t des éléments de $[1; 4]$ distincts deux à deux, calculer $(xyz)(yzt)$.
Solution : *On a :*

$$(xyz)(yzt) = (xy)(yz)(yz)(zt) = (xy)(zt) .$$

c) En déduire que $\mathcal{A}_4$ est engendré par les 3-cycles.
Solution : *Il résulte de a) que si un élément de* $\mathcal{A}_4$ *n'est ni un* 3*-cycle, ni l'identité il est de la forme* $(xy)(zt)$ *et de b) qu'un tel élément est un produit de* 3*-cycles. Il 's'ensuit donc que* $\mathcal{A}_4$ *est engendré (cf. II.1.4.1.c).) par l'ensemble des* 3*-cycles.*

Pour $(G, *)$ **un groupe, on note**

$$\forall g \in G,\ \forall h \in G,\ [g, h] := g * h * g^{-1} * h^{-1}$$

qu'on appelle *commutateur* de g **et** h. **On note** $D(G)$ **le sous-groupe de** G **engendré par les éléments de la forme** $[g, h]$ **qu'on appelle *sous-groupe dérivé* de** G.

6) a) Que vaut $D(G)$ si G est abélien ? Y-a-t il une assertion réciproque ?
Solution :

i) Si G *est abélien*

$$\forall g \in G,\ \forall h \in G,\ g * h = h * g \Rightarrow g * h * g^{-1} = h \Rightarrow g * h * g^{-1} * h^{-1} = e \Rightarrow D(G) = \{e\} .$$

ii) Réciproquement, si $D(G) = \{e\}$,

$$\forall g \in G,\ \forall h \in G,\ [g,h] = e \Rightarrow g*h*g^{-1}*h^{-1} = e \Rightarrow g*h*g^{-1} = h \Rightarrow g*h = h*g$$

c'est-à-dire que G *est abélien.*

b) Étant donné un morphisme de groupes $f : G \to H$, déterminer pour tout $(g,h) \in G \times G$, $f([g,h])$ en fonction de $[f(g), f(h)]$. En déduire que $f(D(G)) \subset D(h)$.

Solution :

i)

$$\begin{array}{rcl} \forall g \in G,\ \forall h \in G, & & \\ f([g,h]) & = & f(g*h*g^{-1}*h^{-1}) \\ & = & f(g)*f(h)*f(g^{-1})*f(h^{-1}) \\ & = & f(g)*f(h)*f(g)^{-1}*f(h)^{-1} \\ & = & [f(g), f(h)]\,. \end{array}$$

ii) Pour tout $g \in D(G)$, *il existe* $d \in \mathbb{N}$, $s_{i\ ,1\le i\le d} \in G$ $t_{i\ ,1\le i\le d} \in G$ *tels que* $g = \prod_{i=1}^{d} [s_i, t_i]$. *On a alors*

$$f(g) = f\big(\prod_{i=1}^{d} [s_i,t_i]\big) = \prod_{i=1}^{d} f[s_i,t_i] = \prod_{i=1}^{d} [f(s_i), f(t_i)] \in D(H)\,.$$

Pour tout couple (g,k) **d'éléments de** G, **on note** $g^k := k*g*k^{-1}$ **le conjugué (cf. II.1.3.1,) de** g **par** k.

Pour tout triplet (g,h,k) **d'éléments de** G **calculer en fonction de** g^k **et** h^k :

c) $(g*h)^k$;

Solution : *On a :*

$$(g*h)^k = k*g*h*k^{-1} = k*g*k^{-1}*k*h*k^{--1} = g^k*h^k\,.$$

d) $(g^{-1})^k$;

Solution : *Il résulte du point précédent que* $g \mapsto g^k$, *est un morphisme de* g *dans lui-même et que par conséquent* $(g^k)^{-1} = (g^{-1})^k$.

e) $[g,h]^k$.

Solution : *Puisque* $g \mapsto g^k$ *est un morphisme (cf. c),) il résulte de b) que* $[g,h]^k = [g^k, h^k]$.

f) En déduire que $D(G)$ est un sous-groupe distingué de G.

Solution : *Il résulte de b) appliqué au morphisme* $g \mapsto g^k$ *pour tout* $k \in G$, *que* $D(G)^k \subset D(G)$ *ce qui prouve que* $D(G)$ *est distingué.*

g) Montrer que le groupe $G_{\mathrm{Ab}} := G/D(G)$ est abélien. On notera $\pi : G \to G_{\mathrm{Ab}}$ la surjection canonique.

Solution :

$$\forall \alpha \in G_{\mathrm{Ab}},\ \forall \beta \in G_{\mathrm{Ab}},\ \exists g \in G,\ \exists h \in G,\ \alpha = \pi(g)\,,\ \beta = \pi(h)\,.$$

Alors :

$$\begin{array}{rcl} [\alpha,\beta] & = & [\pi(g), \pi(h)] \\ & = & \pi([g,h]) \\ & = & e_{G_{\mathrm{Ab}}}\ ; \end{array}$$

ce qui prouve précisément que G_{Ab} *est abélien grâce à la réciproque dans a).*

h) Pour tout morphisme de groupes $f : G \to A$ où A est un groupe abélien, montrer qu'il existe un unique morphisme de groupes $\overline{f} : G_{\mathrm{Ab}} \to A$ tel que $f = \overline{f} \circ \pi$.

Solution : *d'après b), $f(D(G)) \subset D(A)$ or $D(A) = \{e_A\}$ d'après a). Il s'ensuit que $D(G) \subset \mathrm{Ker}\, f$ et il suffit dès lors d'appliquer la proposition II.1.3.7.ii) puisque $D(G)$ est distingué en vertu de f).*

7) Soit $n \geq 2$ un entier.

a) Montrer que, pour tout $s \in \mathcal{S}_n$, s et son inverse ont même signature.

Solution : *Pour tout $s \in \mathcal{S}_n$,*

$$\sigma(s) * \sigma(s^{-1}) = \sigma(s * s^{-1}) = \sigma(\mathrm{Id}) = 1$$

ce qui puisque σ est à valeurs dans $\{-1, 1\}$, que $\sigma(s) = \sigma(s^{-1})$.

b) En déduire que, pour tout $n \geq 2$, $D(\mathcal{S}_n) \subset \mathcal{A}_n$.

Solution : *Pour tout $x \in D(\mathcal{S}_n)$, il existe $d \in \mathbb{N}$, $s_{i\,,1\leq i\leq d} \in \mathcal{S}_n$, $t_{i\,,1\leq i\leq d} \in \mathcal{S}_n$, tels que :*

$$\begin{aligned}
x &= \prod_{i=1}^{d} [s_i, t_i] \\
\Rightarrow \quad \sigma(x) &= \prod_{i=1}^{d} \sigma([s_i, t_i]) \\
&= \prod_{i=1}^{d} \sigma(s_i)\sigma(t_i)\sigma(s_i^{-1})\sigma(t_i^{-1} \\
&= \prod_{i=1}^{d} \sigma(s_i)^2\sigma(t_i)^2 \\
&= 1 \\
\Rightarrow \quad x &\in \mathcal{A}_n \, .
\end{aligned}$$

c) Montrer finalement que $\mathcal{A}_4 = D(\mathcal{S}_4)$.

Solution : *On a déjà montré que $D(\mathcal{S}_4) \subset \mathcal{A}_4$.*

Réciproquement soit $(xyz) \in \mathcal{A}_4$ un 3-cycle. On a :

$$\begin{aligned}
(xyz) &= (xzy)^2 \\
&= ((xz)(zy))^2 \\
&= (xz)(zy)(xz)(zy) \\
&= (xz)(zy)(xz)^{-1}(zy)^{-1} \\
&= [(xz), (zy)] \\
&\in D(\mathcal{S}_4) \, .
\end{aligned}$$

Comme $\mathcal{A}_4$ est engendré par les 3-cycles,

$$\mathcal{A}_4 \subset D(\mathcal{S}_4) \, .$$

Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

Soutien : séances des 2 et 5 juin 2015

Exercice A : () (**Équations de congruences**)

1) () **a)** () Déterminer l'ensemble des couples d'entiers relatifs $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ vérifiant l'équation

$$91x + 119y \ = \ 44 \, .$$

b) () Même question que ci-dessus pour l'équation

$$91x + 119y \ = \ 42 \, .$$

2) () Déterminer l'ensemble des entiers relatifs $x \in \mathbb{Z}$ vérifiant le système de congruences

$$\mathcal{S} \ : \ \left\{ \begin{array}{rcl} 4x & \equiv & 2 \, [11] \\ 3x & \equiv & 8 \, [13] \\ 6x & \equiv & 14 \, [17] \end{array} \right\} \, .$$

Exercice B : () **1)** () **Soit $f : G \to H$ un morphisme de groupes.**

a) () Montrer que, pour tout $x \in G$, l'ordre de $f(x)$ dans H divise l'ordre de x dans G si l'ordre de x est fini.

b) () Montrer que si f est injectif, pour tout $x \in G$, x et $f(x)$ ont même ordre.

2) () **On note $G := (\mathbb{Z}/10\mathbb{Z})^\times$ (resp. $H := (\mathbb{Z}/12\mathbb{Z})^\times$) le groupe multiplicatif des éléments inversibles de l'anneau $(\mathbb{Z}/10\mathbb{Z}, +, *)$ (resp. $(\mathbb{Z}/12\mathbb{Z}, +, *)$.)**

a) () Donner la liste des éléments et la table de composition des groupes G et H.

b) () Donner l'ordre de chacun des éléments de G et H.

c) () Les groupes G et H sont-ils isomorphes, autrement dit, existe-t-il un isomorphisme de groupes de G sur H ?

d) () Le groupe G est-il isomorphe au groupe additif $(\mathbb{Z}/4\mathbb{Z}, +)$?

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) () (**Conjugaison**)

Soit $(G,*)$ **un groupe d'élément neutre** e.

Pour tout $x \in G$, **on note** $x^G := \{g * x * g^{-1}\ ,\ g \in G\}$ **la classe de conjugaison de** x **par le groupe** G **et** $\mathrm{Stab}_G(x) := \{g \in G \| \ g * x * g^{-1} = x\}$ **le *stabilisateur* de** x.

a) () Montrer que, pour tout $x \in G$, $\mathrm{Stab}_G(x)$ est un sous-groupe de G.

b) () Pour tout $x \in G$, tout couple (g,h) d'éléments de G, montrer que

$$g * x * g^{-1} = h * x * h^{-1}$$

si et seulement si $g^{-1}h \in \mathrm{Stab}_G(x)$.

On rappelle qu'on définit une relation d'équivalence sur G **par** $g \sim h$ **si** $g^{-1}h \in \mathrm{Stab}_G(x)$. **On notera** $\overline{g}$ **la classe d'un élément** g **pour cette relation.**

c) () Montrer qu'on définit bien une application bijective de l'ensemble des classes selon $\sim$ dans x^G par

$$\overline{g} \mapsto g * x * g^{-1} .$$

d) () Déduire de ce qui précède que, si G est un groupe fini,

$$\#(G) = \#(x^G)\#(\mathrm{Stab}_G(x)) .$$

4) () (**Éléments de type** $(3,3)$)

On considère désormais une permutation $s := (a\,b\,c)(d\,e\,f)$ **de type cyclique** $(3,3)$ **dans** $\mathcal{S}_6$. **On reprend les notations de la question 3) c'est-à-dire qu'on note** $s^{\mathcal{A}_6}$ **la classe de conjugaison de** s **dans** $\mathcal{A}_6$ **que nous allons déterminer dans cette question.**

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 : () (**Centre de $\mathcal{S}_4$**)

0) () Étant donné un groupe G et H un sous-groupe distingué d'indice $n \in \mathbb{N}$, c'est-à-dire tel que $\#(G/H) = n$, montrer que
$$\forall x \in G,\ x^n \in H .$$

1) () **a)** () Donner trois sous-groupes normaux deux à deux distincts du groupe symétrique $\mathcal{S}_4$.

b) () Quel peut être le cardinal d'un sous-groupe normal de $\mathcal{S}_4$?

c) () Donner le cardinal et un représentant de chaque classe de conjugaison dans $\mathcal{S}_4$, son type cyclique, son ordre et sa signature.

2) () **Soient v_1, v_2 et v_3 les éléments de $\mathcal{S}_4$ définis par :**
$$\begin{aligned} v_1 &:= (12)(34) \\ v_2 &:= (13)(24) \\ v_3 &:= (14)(23) . \end{aligned}$$

a) () Pour tout $1 \leq i \leq 3$ $1 \leq j \leq 3$ calculer $v_i v_j$.

b) () Déterminer le sous-groupe V de $\mathcal{S}_4$ engendré par les éléments v_1, v_2 et v_3. Montrer que V est abélien.

c) () Pour tout $\{a, b, c, d\} = [1; 4]$ et tout $s \in \mathcal{S}_4$, calculer

$$s \circ (ab)(cd) \circ s^{-1}$$

et en déduire que V est distingué dans $\mathcal{S}_4$.

d) () V est-il un sous-groupe de $\mathcal{A}_4$? distingué dans $\mathcal{A}_4$?

3) () **a)** () Montrer que $\mathcal{S}_4$ ne peut avoir de sous-groupe distingué de cardinal 2 ou 3.

b) () Montrer qu'un sous-groupe distingué de $\mathcal{S}_4$ de cardinal 4 ne contient ni 4-cycle ni transposition et en déduire que le seul sous-groupe distingué de $\mathcal{S}_4$ de cardinal 4 est V.

c) () Montrer que si G est un sous-groupe distingué de $\mathcal{S}_4$ de cardinal 6, alors :

i) pour tout $s \in \mathcal{S}_4$, $s^4 \in G$.

ii) En déduire que G contient tous les 3-cycles.

iii) Le groupe $\mathcal{S}_4$ a-t-il un sous-groupe distingué de cardinal 6 ?

d) () Montrer que $\mathcal{S}_4$ n'a pas de sous-groupe distingué de cardinal 8.
Indication : *On pourra raisonner sur l'ordre des éléments d'un tel sous-groupe et utiliser en le justifiant qu'une classe de conjugaison est soit incluse dans un tel sous-groupe soit disjointe d'un tel sous-groupe.*

e) () i) Montrer que si G est un sous-groupe distingué de $\mathcal{S}_4$ de cardinal 12, alors pour tout $s \in \mathcal{S}_4$, $s^2 \in G$.

ii) En déduire qu'un sous-groupe distingué G de $\mathcal{S}_4$ de cardinal 12 contient nécessairement tous les 3-cycles.

iii) En déduire finalement que le seul sous-groupe distingué de $\mathcal{S}_4$ de cardinal 12 est $\mathcal{A}_4$.

4) () Quels sont finalement les sous-groupes distingués de $\mathcal{S}_4$?

Pour tout groupe $(G, *)$ on appelle *centre de* G et on note $Z(G)$ le sous-ensemble de G défini par

$$Z(G) := \{g \in G \,;\, \forall h \in G,\ g * h = h * g\}\,.$$

5) () **a)** () Montrer que le centre $Z(G)$ d'un groupe G est un sous-groupe distingué de G.

b) () Montrer que $Z(G)$ est abélien.

c) () Quel est le centre de $\mathcal{S}_4$?

Exercice E : () **(Groupe des automorphismes de $\mathbb{Z}/n\mathbb{Z}$)**

Pour tout entier $n \in \mathbb{N}^*$, on note

$$(\mathbb{Z}/n\mathbb{Z}, +, *)$$

l'anneau des entiers modulo n et

$$((\mathbb{Z}/n\mathbb{Z})^\times, *)$$

le groupe des éléments inversibles. Pour tout $x \in \mathbb{Z}$, on note x mod n sa classe modulo n. Enfin, pour deux entiers a et b on notera $a \wedge b$ leur pgcd.

1) () **a)** () Donner la liste des éléments de

$$(\mathbb{Z}/2\mathbb{Z})^\times \text{ , } (\mathbb{Z}/5\mathbb{Z})^\times \text{ et } (\mathbb{Z}/6\mathbb{Z})^\times \text{ .}$$

b) () Donner la liste de tous les sous-groupes de

$$(\mathbb{Z}/5\mathbb{Z}, +) \text{ et } (\mathbb{Z}/6\mathbb{Z}, +) \text{ .}$$

On rappelle, que pour un groupe $(G, *)$ et tout élément $x \in G$, il existe un unique morphisme

$$\epsilon_x : (\mathbb{Z}, +) \to (G, *)$$

tel que $\epsilon_x(1) = x$. On note usuellement $\epsilon_x(k) = x^k$ ou même $\epsilon_x(k) = kx$ si G est abélien et sa loi notée $+$.

Pour tout $k \in \mathbb{Z}$, on définit

$$\begin{array}{rccc} \phi_k : & (G, *) & \to & (G, *) \\ & x & \mapsto & \epsilon_x(k) \text{ .} \end{array}$$

2) () **Soit $(G, *)$ un groupe.**

a) () Que vaut ϕ_1 ?

b) () Exprimer $\phi_{-k}(x)$ en fonction de $\phi_k(x)$ pour tout $k \in \mathbb{Z}$ et tout $x \in G$.

c) () Exprimer $\phi_{k+1}(x)$ en fonction de $\phi_k(x)$ pour tout $x \in G$ et tout $k \in \mathbb{N}$.

d) () Pour tout couple (k, l) d'entiers relatifs, montrer que

$$\phi_k \circ \phi_l = \phi_{kl} \text{ .}$$

e) () Pour tout morphisme $\gamma : G \to G$ et tout $k \in \mathbb{Z}$, montrer que

$$\phi_k \circ \gamma = \gamma \circ \phi_k \text{ .}$$

3) () **a)** () Montrer que si G est un groupe abélien, pour tout $k \in \mathbb{Z}$, ϕ_k est un morphisme de groupes de G dans lui-même.

Indication : *On pourra prouver d'une part que ϕ_{-1} est un morphisme et d'autre part que ϕ_k est un morphisme pour $k \in \mathbb{N}$ puis appliquer les résultats de la question question 2).*

b) () Donner un exemple de groupe non abélien G et d'entier k pour lesquels $\phi_k : G \to G$ n'est pas un morphisme.

4) () **Soit** $n > 1$ **un entier. On pose** $G := (\mathbb{Z}/n\mathbb{Z}, +)$.

a) () Montrer que

$$G = \{\phi_k(1 \bmod n)\ ,\ k \in \mathbb{Z}\}\ .$$

b) () Si γ est un morphisme de G dans lui-même (*i.e.*un *endomorphisme* de $G,)$ montrer qu'il existe $k \in \mathbb{Z}$ tel que

$$\gamma = \phi_k\ .$$

c) () Décrire l'ensemble des endomorphismes de G pour $n = 4$. Donner pour chacun d'entre eux, son image et son noyau ; quels sont ceux qui sont injectifs (resp. surjectifs) (resp. bijectifs ?)

d) () Montrer que pour tout $k \in \mathbb{Z}$, $(k \wedge n) \bmod n$ est un générateur de $\mathrm{Im}\,\phi_k$ et $\dfrac{n}{k \wedge n} \bmod n$ est un générateur de $\mathrm{Ker}\,\phi_k$.

Quels sont les cardinaux de ces deux sous-groupes de G ?

e) () Montrer que l'application $k \mapsto \phi_k$ de $\mathbb{Z}$ dans l'ensemble $\mathrm{End}(G)$ des endomorphismes de G définit en fait une application

$$\begin{array}{rccc} \rho : & \mathbb{Z}/n\mathbb{Z} & \to & \mathrm{End}(G) \\ & k \bmod n & \mapsto & \phi_k\ . \end{array}$$

f) () Montrer que la restriction ρ_0 de l'application ρ définie ci-dessus au groupe $((\mathbb{Z}/n\mathbb{Z})^\times, *)$ est à valeurs dans le groupe $(\mathrm{Aut}(G), \circ)$ des endomorphismes bijectifs de G muni de la loi $\circ$. Montrer que ρ_0 est un isomorphisme.

Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

Examen partiel du 12 novembre 2014
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.

Les exercices sont indépendants même si l'exercice B, question 3) peut donner une indication pour résoudre l'exercice C, question 1).

Exercice A : () (**Équation de congruence**)

Soit

$$\mathcal{E} \ := \ 1969 * x \ + \ 704 * y \ = \ 143 \, .$$

1) () Déterminer l'ensemble $\mathcal{S} \ := \ \{(x, y) \ \in \ \mathbb{Z} \times \mathbb{Z} \, ; \ \text{vérifiant l'équation } \mathcal{E}\}$.

2) () **Soit** $\mathcal{N} \ := \ \{x^2 + y^2 \, , \ (x, y) \in \mathcal{S}\}$.

a) () Montrer que $\mathcal{N}$ possède un plus petit élément.

b) () Donner un plus petit élément de $\mathcal{N}$.

Exercice B : () (**Carrés dans** $\mathbb{Z}/p\mathbb{Z}$)

Soient p **un nombre premier impair et** $G \ := \ \mathbb{Z}/p\mathbb{Z}^{\times}$ **l'ensemble des éléments inversibles de l'anneau** $(\mathbb{Z}/p\mathbb{Z}, +, *)$.

1) () Rappeler pourquoi G muni de la multiplication $*$ de l'anneau $(\mathbb{Z}/p\mathbb{Z}, +, *)$ est un groupe abélien.

2) () **On définit les applications :**

$$\begin{array}{rccc} \gamma : & G & \longrightarrow & G \\ & x & \longmapsto & x^2 \\ \mu : & G & \longrightarrow & G \\ & x & \longmapsto & x^{\frac{p-1}{2}} \, . \end{array}$$

a) () Montrer que γ et μ sont des morphismes de groupes.

b) () Calculer $\gamma \circ \mu$ et $\mu \circ \gamma$.

c) () En déduire des relations liant $\mathrm{Ker}\, \gamma$ et $\mathrm{Im}\, \mu$ d'une part, $\mathrm{Im}\, \gamma$ et $\mathrm{Ker}\, \mu$ d'autre part.

d) () Déterminer $\mathrm{Ker}\,\gamma$ et $\#(\mathrm{Ker}\,\gamma)$.

e) () Majorer $\#(\mathrm{Ker}\,\mu)$.

3) () Montrer qu'il y a $\frac{p-1}{2}$ carrés non nuls dans $\mathbb{Z}/p\mathbb{Z}$ *i.e.* éléments non nuls x qui s'écrivent $x = y^2$ avec $y \in \mathbb{Z}/p\mathbb{Z}$.

4) () Montrer que $x \in \mathbb{Z}/p\mathbb{Z}$ est un carré non nul si et seulement si

$$x^{\frac{p-1}{2}} = 1 .$$

Exercice C : () $(X^2 = 2)$

1) () Donner l'ensemble Q_{17} (resp.Q_{23}) des carrés de $\mathbb{Z}/17\mathbb{Z}$ (resp.$\mathbb{Z}/23\mathbb{Z}$) *i.e.*

$Q_{17} := \left\{x \in \mathbb{Z}/17\mathbb{Z}\,;\, \exists y \in \mathbb{Z}/17\mathbb{Z},\, x = y^2\right\}$ (resp. $Q_{23} := \left\{x \in \mathbb{Z}/23\mathbb{Z}\,;\, \exists y \in \mathbb{Z}/23\mathbb{Z},\, x = y^2\right\}$;

2) () Résoudre dans $\mathbb{Z}/391\mathbb{Z}$ l'équation $X^2 = 2$.

Exercice D : () **Étant donnés deux groupes abéliens** $(G_1, +)$ **et** $(G_2, +)$, **on notera** $(G_1 \times G_2, +)$ **l'ensemble des couples** (x_1, x_2) $x_1 \in G_1$, $x_2 \in G_2$ **muni de la loi** $+$ **définie par**

$$(x_1, x_2) + (y_1, y_2) := (x_1 + y_1, x_2 + y_2) .$$

1) () Montrer qu'avec les notations ci-dessus, $(G_1 \times G_2, +)$ est un groupe abélien dont on précisera l'élément neutre. Donner l'opposé de (x_1, x_2).

Dans la suite on utilisera librement la notation

$$(\mathbb{Z}^2, +) := (\mathbb{Z} \times \mathbb{Z}, +) .$$

2) () **Soient** a **et** b **deux entiers relatifs non nuls,** d **leur pgcd et** m **leur ppcm. On notera** $a := da'$ **et** $b := db'$.

a) () Rappeler pourquoi on peut écrire $d = au + bv$ avec u et v des entiers relatifs.

b) () Rappeler pourquoi a' et b' sont premiers entre eux.

c) () Donner en la justifiant la relation liant a', b', d et m.

3) () **Avec les notations de la question 2), a), on définit l'application :**

$$\begin{array}{rccc} f : & \mathbb{Z}^2 & \to & \mathbb{Z}^2 \\ & (x, y) & \mapsto & (ux + vy, -b'x + a'y) \end{array}$$

a) () Montrer que f est un morphisme de groupes de $(\mathbb{Z}^2, +)$ dans lui-même.

b) () Montrer que f est bijective et déterminer son application réciproque g.

c) () Rappeler pourquoi g est un morphisme de groupes.

4) () **On définit les applications :**

$$\begin{array}{rccl} p: & \mathbb{Z}^2 & \to & \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & (x,y) & \mapsto & (x \,\mathbf{mod}\, d, y \,\mathbf{mod}\, m) \\ q: & \mathbb{Z}^2 & \to & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ & (x,y) & \mapsto & (x \,\mathbf{mod}\, a, y \,\mathbf{mod}\, b)\ . \end{array}$$

a) () Montrer que p (resp. q,) est un morphisme de groupe de $(\mathbb{Z}^2, +)$ dans $(\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +)$ (resp. $(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, +)$; puis que $p \circ f$ et $q \circ g$ sont des morphismes de groupes.

b) () Déterminer $\mathrm{Ker}\, p$ et $\mathrm{Ker}\, q$.

c) () Montrer qu'il existe un unique morphisme de groupes

$$f' \ : \ (\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, +) \ \to \ (\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +)$$

$$(\text{resp. } .g' \ : \ (\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +) \ \to \ (\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, +) \ )$$

tel que

$$f' \circ q \ = \ p \circ f \ (\text{resp. } g' \circ p \ = \ q \circ g \ .)$$

d) () Pour des applications

$$u \ : \ X \ \to \ Y \ , \ v \ : \ X \ \to \ Y \text{ et } w \ : \ W \ \to \ X$$

avec w surjective, montrer que

$$u \ = \ v \ \Leftrightarrow \ u \circ w \ = \ v \circ w \ .$$

e) () Montrer finalement que f' et g' sont inverses l'un de l'autre c'est-à-dire qu'on a construit un isomorphisme de groupes

$$(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, +) \ \cong \ (\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +) \ .$$

f) () Peut-on déduire ce résultat d'un théorème connu lorsque $d = 1$? En d'autres termes quel résultat avons-nous généralisé ici ?

Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

Corrigé de l'examen partiel du 12 novembre 2014

Exercice A : () (**Équation de congruence**)

Soit

$$\mathcal{E} \;:=\; 1969 * x \;+\; 704 * y \;=\; 143\,.$$

1) () Déterminer l'ensemble $\mathcal{S} \;:=\; \{(x,y) \;\in\; \mathbb{Z}\times\mathbb{Z}\,;\;$ vérifiant l'équation $\mathcal{E}\}$.

Solution :

*i) (**PGCD de** 1969 **et** 704)*

Déterminons le PGCD et les coefficients de BÉZOUT *(cf. cours I.3.3.2,) grâce à l'algorithme d'Euclide (cf. cours I.3.3.5 :)*

q	a	u	v
	1969	1	0
	704	0	1
2	561	1	-2
1	143	-1	3
3	132	4	-11
1	11	-5	14

L'algorithme converge ici puisque 11 *est premier. On en déduit donc :*

$$1969 \wedge 704 \;=\; 11 \text{ et } -5 * 1969 + 14 * 704 \;=\; 11\,. \qquad 1$$

*ii) (**Résolution de l'équation** $\mathcal{E}$)*

On constate que $143 \;=\; 13 * 11$ *ce qui entraîne que l'équation* $\mathcal{E}$ *possède des solutions. Elle est équivalentes à l'équation :*

$$\mathcal{E}' \;:\; 179 * x \;+\; 64 * y \;=\; 13\,. \qquad 1$$

Or l'égalité i).1 est équivalentes à :

$$179 \wedge 64 \;=\; 1 \text{ et } -5 * 179 + 14 * 64 \;=\; 1\,. \qquad 2$$

d'où il résulte que :

$$-5 * 13 * 179 \;+\; 14 * 13 * 64 \;=\; 13 \qquad 3$$

c'est-à-dire que $(-65, 182)$ *est une solution de* $\mathcal{E}'$ *et donc de* $\mathcal{E}$.

Pour tout (x,y) solution de $\mathcal{E}'$ on a :

$$
\begin{array}{rl}
& \left\{\begin{array}{rcl} -65*179+182*64 & = & 13 \\ 179*x+64*y & = & 13 \end{array}\right\} \\
\Rightarrow & \left\{\begin{array}{rcl} -65*179+182*64 & = & 13 \\ 179*(x+65)+64*(y-182) & = & 0 \end{array}\right\} \\
\Rightarrow & \left\{\begin{array}{rcl} -65*179+182*64 & = & 13 \\ 179*(x+65) & = & -64*(y-182) \end{array}\right\} \\
\Rightarrow & \left\{\begin{array}{rcl} -65*179+182*64 & = & 13 \\ 179*x+64*y & = & 13 \\ 179|(y-182) & \text{et} & 64|(x+65) \end{array}\right\} \\
\Rightarrow & \left\{\begin{array}{rcl} -65*179+182*64 & = & 13 \\ 179*x+64*y & = & 13 \\ \exists k\in\mathbb{N},\ y=1_2+179*k & \text{et} & \exists \ell\in\mathbb{N},\ x=-65+64*\ell \end{array}\right\} \\
\Rightarrow & \left\{\begin{array}{rcl} -65*179+182*64 & = & 13 \\ 179*x+64*y & = & 13 \\ 179*(-65+64*\ell)+64*(182+179*k) & = & 13 \end{array}\right\} \\
\Rightarrow & \left\{\begin{array}{rcl} -65*179+182*64 & = & 13 \\ 179*x+64*y & = & 13 \\ -65*179+182*64+179*64*(k+\ell) & = & 13 \end{array}\right\} \\
\Rightarrow & \left\{\begin{array}{rcl} x & = & -65+64*k \\ y & = & 182-179*k \end{array}\right\} .
\end{array}
$$

Il s'ensuit que

$$\mathcal{S} \;=\; \{(-65+64*k, 182-179k\} \,.$$

2) () **Soit** $\mathcal{N} \;:=\; \{x^2+y^2\ ,\ (x,y)\in\mathcal{S}\}$.

a) () Montrer que $\mathcal{N}$ possède un plus petit élément.

Solution : *L'ensemble $\mathcal{N}$ est une partie non vide de $\mathbb{N}$ (puisque $\mathcal{S}\;\neq\;\emptyset$,) et possède donc un plus petit élément (cf. cours I.1.2.7.)*

b) () Donner un plus petit élément de $\mathcal{N}$.

Solution : *On constate, en prenant $k\;=\;1$, que $(-1,3)\in\mathcal{S}$. Ainsi $(-1)^2+3^2\;=\;10\;\in\;\mathcal{N}$. Or pour $k>1$, on a*

$$y<-176\;\Rightarrow\;y^2>176^2\;\Rightarrow\;x^2+y^2>165^2>10\,.$$

Pour $k<1$, on a

$$x<-65\;\Rightarrow\;x^2>65^2\;\Rightarrow\;x^2+y^2>65^2>10\,.$$

Il s'ensuit que 10 est le plus petit élément de $\mathcal{N}$.

Exercice B : () **(Carrés dans $\mathbb{Z}/p\mathbb{Z}$)**

Soient p un nombre premier impair et $G\;:=\;\mathbb{Z}/p\mathbb{Z}^\times$ l'ensemble des éléments inversibles de l'anneau $(\mathbb{Z}/p\mathbb{Z},+,*)$.

1) () Rappeler pourquoi G muni de la multiplication $*$ de l'anneau $(\mathbb{Z}/p\mathbb{Z},+,*)$ est un groupe abélien.

Solution :

*i) (**Loi interne**)*

Pour tout $(x,y)\in\mathbb{Z}/p\mathbb{Z}^\times\times\mathbb{Z}/p\mathbb{Z}^\times$, $x*y$ est encore inversible d'inverse $y^{-1}*x^{-1}\;=\;x^{-1}*y^{-1}$ l'anneau $(\mathbb{Z}/p\mathbb{Z},+,*)$ étant commutatif. La loi $*$ est donc interne sur G.

*ii) (**Élément neutre**)*
L'élément neutre 1 *est inversible et appartient donc à* G *et est un élément neutre pour* $(G, *)$.

*iii) (**Inverse**)*
Pour tout $x \in G$,

$$(x^{-1})^{-1} \ = \ x \ \Rightarrow \ x^{-1} \in G$$

et est un inverse pour x *dans* G.

*iv) (**Abélien**)*
Enfin $(\mathbb{Z}/p\mathbb{Z}, +, *)$ *étant un anneau commutatif,* $*$ *est commutative.*
Il résulte de ce qui précède que $(G, *)$ *est un groupe abélien (cf. 0.5.6.i).)*

2) () **On définit les applications :**

$$\begin{array}{rccc} \gamma : & G & \longrightarrow & G \\ & x & \longmapsto & x^2 \\ \mu : & G & \longrightarrow & G \\ & x & \longmapsto & x^{\frac{p-1}{2}} \ . \end{array}$$

a) () Montrer que γ et μ sont des morphismes de groupes.
Solution : *Pour tout groupe abélien* $(H, *)$ *et tout entier* $k \in \mathbb{N}$ *l'application*

$$\mu_k \ : \ H \ \to \ H \ , \ x \ \mapsto \ x^k$$

est un morphisme de groupes. En effet :

$$\mu_k(x * y) \ = \ (x * y)^k \ = \ x^k * y^k_{=} \ \mu_k(x) * \mu_k(y)$$

dès que H *est comutatif.*

b) () Calculer $\gamma \circ \mu$ et $\mu \circ \gamma$.
Solution :

i) ($\gamma \circ \mu$*)*

$$\forall x \in G, \ \gamma[\mu(x)] \ = \ \mu(x)^2 \ = \ (x^{\frac{p-1}{2}})^2 \ = \ x^{p-1} \ = \ 1 \ .$$

ii) ($\mu \circ \gamma$*)*

$$\forall x \in G, \ \mu[\gamma(x)] \ = \ \gamma(x)^{\frac{p-1}{2}} \ = \ (x^2)^{\frac{p-1}{2}}_{=} \ x^{p-1} \ = \ 1 \ .$$

c) () En déduire des relations liant $\mathrm{Ker}\,\gamma$ et $\mathrm{Im}\,\mu$ d'une part, $\mathrm{Im}\,\gamma$ et $\mathrm{Ker}\,\mu$ d'autre part.
Solution : *Il résulte immédiatement du calcul fait précédemment que :*

$$\mathrm{Im}\,\mu \ \subset \ \mathrm{Ker}\,\gamma \text{ et } \mathrm{Im}\,\gamma \ \subset \ \mathrm{Ker}\,\mu \ . \qquad 1$$

d) () Déterminer $\mathrm{Ker}\,\gamma$ et $\#(\mathrm{Ker}\,\gamma)$.
Solution :

$$\begin{aligned}\mathrm{Ker}\,\gamma &= \{x \in G\,;\, x^2 = 1\}\\ &= \{x \in \mathbb{Z}/p\mathbb{Z}\,;\, x^2 = 1\}\\ &= \{x \in \mathbb{Z}/p\mathbb{Z}\,;\, (x-1)(x+1) = 0\}\end{aligned}$$

Or $\mathbb{Z}/p\mathbb{Z}$ étant un corps (cf. I.3.4.11,) l'équation $(x-1)(x+1) = 0$ a pour solutions -1 et 1. Comme de plus p est imppaire $-1 \neq 1[p]$ d'où

$$\mathrm{Ker}\,\gamma = \{-1, 1\} \text{ et } \#(\mathrm{Ker}\,\gamma) = 2\,. \qquad 1$$

e) () Majorer $\#(\mathrm{Ker}\,\mu)$.
Solution :

$$\mathrm{Ker}\,\mu = \{x \in G\,;\, x^{\frac{p-1}{2}} = 1\} = \{x \in \mathbb{Z}/p\mathbb{Z}\,;\, x^{\frac{p-1}{2}} = 1\}\,;$$

Autrement dit les éléments de $\mathrm{Ker}\,\mu$ sont les racines du polynôme $X^{\frac{p-1}{2}} - 1$ puisque 0 n'est pas racine de ce polynôme. Or ce polynôme a au plus $\frac{p-1}{2}$ racines dans le corps $(\mathbb{Z}/p\mathbb{Z}, +, *)$ si bien que :

$$\#(\mathrm{Ker}\,\mu) \leq \frac{p-1}{2}\,. \qquad 1$$

3) () Montrer qu'il y a $\frac{p-1}{2}$ carrés non nuls dans $\mathbb{Z}/p\mathbb{Z}$ *i.e.* éléments non nuls x qui s'écrivent $x = y^2$ avec $y \in \mathbb{Z}/p\mathbb{Z}$.

Solution : *Par définition même de γ, x est un carré non nul si et seulement si $x \in \mathrm{Im}\,\gamma$. Or d'après le corollaire II.1.3.10*

$$\mathrm{Im}\,\gamma \cong G/\mathrm{Ker}\,\gamma\,.$$

Il en résulte, en vertu de TD n° IV, exercice A et question 2), d).1, que :

$$\#(\mathrm{Im}\,\gamma) = \frac{p-1}{2}\,. \qquad 1$$

4) () Montrer que $x \in \mathbb{Z}/p\mathbb{Z}$ est un carré non nul si et seulement si

$$x^{\frac{p-1}{2}} = 1\,.$$

Solution : *L'égalité ci-dessus signifie exactement que $\mathrm{Ker}\,\mu = \mathrm{Im}\,\gamma$. Or on a déjà montré à la question 2), c).1 $\mathrm{Im}\,\gamma \subset \mathrm{Ker}\,\mu$. On a montré à la question 3) $\#(\mathrm{Im}\,\gamma) = \frac{p-1}{2}$ et à la question 2), e).1 $\#(\mathrm{Ker}\,\mu) \leq \frac{p-1}{2}$ ce qui prouve l'égalité demandée.*

Exercice C : () ($X^2 = 2$)

1) () Donner l'ensemble Q_{17} (resp.Q_{23}) des carrés de $\mathbb{Z}/17\mathbb{Z}$ (resp.$\mathbb{Z}/23\mathbb{Z}$) *i.e.*

$Q_{17} := \left\{x \in \mathbb{Z}/17\mathbb{Z}\,;\, \exists y \in \mathbb{Z}/17\mathbb{Z},\, x = y^2\right\}$ (resp. $Q_{23} := \left\{x \in \mathbb{Z}/23\mathbb{Z}\,;\, \exists y \in \mathbb{Z}/23\mathbb{Z},\, x = y^2\right\}$;

Solution :

i) (Q_{17})
Dans $\mathbb{Z}/17\mathbb{Z}$ *on a :*

$$\begin{array}{rcl} -8^2 & = & 8^2 = -4 \\ -7^2 & = & 7^2 = -2 \\ -6^2 & = & 6^2 = 2 \\ -5^2 & = & 5^2 = 8 \\ -4^2 & = & 4^2 = -1 \\ -3^2 & = & 3^2 = -8 \\ -2^2 & = & 2^2 = 4 \\ -1^2 & = & 1^2 = 1 \\ & & 0^2 = 0 \end{array}$$

d'où

$$Q_{17} = \{-8, -4, -2, -1, 0, 1, 2, 4, 8\}\,.$$

ii) (Q_{23})
Dans $\mathbb{Z}/23\mathbb{Z}$ *on a :*

$$\begin{array}{rcl} -11^2 & = & 11^2 = 6 \\ -10^2 & = & 10^2 = 8 \\ -9^2 & = & 9^2 = -11 \\ -8^2 & = & 8^2 = -5 \\ -7^2 & = & 7^2 = 3 \\ -6^2 & = & 6^2 = -10 \\ -5^2 & = & 5^2 = 2 \\ -4^2 & = & 4^2 = -7 \\ -3^2 & = & 3^2 = 9 \\ -2^2 & = & 2^2 = 4 \\ -1^2 & = & 1^2 = 1 \\ & & 0^2 = 0 \end{array}$$

d'où

$$Q_{23} = \{-11, -10, -7, -5, 0, 1, 2, 3, 4, 6, 8, 9\}\,.$$

2) () Résoudre dans $\mathbb{Z}/391\mathbb{Z}$ l'équation $X^2 = 2$.

Solution : *Remarquons que* $391 = 17 * 23$ *que* 17 *et* 23 *sont premiers donc premiers entre eux et que par conséquent on dispose de l'isomorphisme d'anneaux du théorème chinois des restes (cf. cours I.3.6.1 :)*

$$\gamma : \mathbb{Z}/391\mathbb{Z} \to \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}\,.$$

Pour $x \in \mathbb{Z}/391\mathbb{Z}$, *notons* $(y, z) := \gamma(x) \in \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}$. *Puisque* γ *est un isomorphisme d'anneaux, on a alors :*

$$\begin{array}{rcl} & x^2 = 2 \\ \Leftrightarrow & \gamma(x^2) = \gamma(2) \\ \Leftrightarrow & \gamma(x)^2 = \gamma(2) \\ \Leftrightarrow & (y, z)^2 = (2, 2) \\ \Leftrightarrow & (y^2, z^2) = (2, 2) \\ \Leftrightarrow & \left\{\begin{array}{l} y^2 = 2 \in \mathbb{Z}/17\mathbb{Z} \\ z^2 = 2 \in \mathbb{Z}/23\mathbb{Z}\,. \end{array}\right. \end{array}$$

Il résulte de la question 1) que l'équation $x^2 = 2$ *équivaut à*

$$y \ = \ \pm 6 \text{ et } z \ = \ \pm 5 \ \Leftrightarrow \ (y,z) \ \in \ \mathcal{S} \ := \ \{(-6,-5),(-6,5),(6,-5),(6,5)\} \, .$$

finalement l'équation $x^2 \ = \ 2$ *équivaut à* $x \in \gamma^{-1}(\mathcal{S})$. *On remarque que*

$$\alpha \ \in \mathcal{S} \ \Leftrightarrow \ -\alpha \ \in \ \mathcal{S} \, ;$$

si bien qu'il suffit de calculer effectivement $\gamma^{-1}(6,5)$ *et* $\gamma^{-1}(-6,5)$ *par exemple. Cela revient à résoudre les systèmes de congruence :*

$$\left\{ \begin{matrix} x & \equiv & 6\,[17] \\ x & \equiv & 5\,[23] \end{matrix} \right\} \text{ et } \left\{ \begin{matrix} x & \equiv & 6\,[17] \\ x & \equiv & 5\,[23] \end{matrix} \right\} \, . \qquad 1$$

On sait que, quelle que soit la méthode utilisée pour résoudre ce système on sera amené à disposer des coefficients de BÉZOUT *(cf. cours I.3.3.2,) que l'on peut calculer à l'aide de l'algorithme d'Euclide (cf. cours I.3.3.5 :)*

q	a	u	v
	23	1	0
	17	0	1
1	6	1	-1
2	5	-2	3
1	1	3	-4

d'où il résulte que :

$$3 * 23 \ - \ 4 * 17 \ = \ 1 \, . \qquad 2$$

On détaille ici trois manières de procéder même si bien sûr pour résoudre l'exercice une seule est suffisante et qu'on peut même employer toute autre méthode de son choix pourvu qu'elle aboutisse au résultat. On sait de toute manière, en vertu du corollaire (cf. cours I.3.6.3,) que les systèmes 1 possèdent une unique solution dans $\mathbb{Z}/391\mathbb{Z}$.

*i) (**Première méthode**)*
Résolvons le système :

$$\left\{ \begin{matrix} x & \equiv & 6\,[17] \\ x & \equiv & 5\,[23] \end{matrix} \right\} \, :$$

$$\begin{matrix} & \exists u \ \in \ \mathbb{Z}, \ x = 6 + 17u & \text{et} & \exists v \ \in \ \mathbb{Z}, \ x = 5 + 23v \\ \Rightarrow & & 23v - 17u \ = \ 1 & \end{matrix}$$

d'où il résulte, d'après 2 que $u \ = \ 4$ *et* $v \ = \ 3$ *est une solution. Il s'ensuit que :*

$$x \ = \ 6 + 68 \ = \ 5 + 69 \ = \ 74[391] \qquad 1$$

est la solution du système.

*ii) (**Deuxième méthode**)*
Il résulte toujours de 2 que :

$$\begin{matrix} & 69 \ \equiv \ 1\,[17], 69 \ \equiv \ 0\,[23] & , & -68 \ \equiv \ 0\,[17], -68 \ \equiv \ 1\,[23] \\ \Leftrightarrow & & \gamma(69) = (1,0) \ \text{ et } \ \gamma(-68) = (0,1) \, . & \end{matrix}$$

Il s'ensuit, puisque γ *est un morphisme que*

$$\gamma(-6 * 69 - 5 * 68) \ = \ (-6,5)$$

si bien que :

$$x \ = \ -6 * 69 - 5 * 68 \ = \ -754 \ = \ 28\,[391] \qquad 1$$

est la solution du système

$$\left\{ \begin{matrix} x & \equiv & 6\,[17] \\ x & \equiv & 5\,[23] \end{matrix} \right\} \, .$$

*iii) (**Troisième méthode**)*
On peut employer la méthode suivante pour résoudre le système :

$$\left.\begin{cases} x & \equiv & 6\,[17] \\ x & \equiv & -5\,[23] \end{cases}\right\}.$$

On sait qu'alors il existe un unique couple (s_1, s_2) *avec*

$$0 \leq s_1 < 17 \text{ et } 0 \leq s_2 < 23$$

tel que $x \equiv s_1 + 17s_2\,[391]$. *On a alors* $s_1 = 6$, *et*

$$\begin{array}{rrcl} & s_2 & \equiv & \frac{-5-6}{17}\,[23] \\ \Leftrightarrow & S_2 & \equiv & -11 * (-4)\,[23] \\ \Leftrightarrow & s_2 & \equiv & 44\,[23] \\ \Rightarrow & s_2 & = & 21 \\ \Rightarrow & x & \equiv & 6 + 17 * 21\,[391] \end{array}$$

si bien que :

$$x = -28\,[391] \qquad 1$$

est solution du système et l'on n'est pas surpris de trouver lopposé de ce qu'on a trouvé en ii).1.
Il ressort de ce qui précède que

$$x^2 = 2 \Leftrightarrow x \in \{-74, -28, 28, 74\}.$$

Exercice D : () **Étant donnés deux groupes abéliens** $(G_1, +)$ **et** $(G_2, +)$, **on notera** $(G_1 \times G_2, +)$ **l'ensemble des couples** (x_1, x_2) $x_1 \in G_1$, $x_2 \in G_2$ **muni de la loi** $+$ **définie par**

$$(x_1, x_2) + (y_1, y_2) := (x_1 + y_1, x_2 + y_2).$$

1) () Montrer qu'avec les notations ci-dessus, $(G_1 \times G_2, +)$ est un groupe abélien dont on précisera l'élément neutre. Donner l'opposé de (x_1, x_2).
Solution : *Pour tout* (x_1, x_2), (y_1, y_2) *et* (z_1, z_2) *des éléments de* $G_1 \times G_2$,
—

$$\begin{array}{rcl} \big((x_1, x_2) + (y_1, y_2)\big) + (z_1, z_2) & = & (x_1 + y_1, x_2 + y_2) + (z_1, z_2) \\ & = & (x_1 + y_1 + z_1, x_2 + y_2 + z_2) \\ & = & (x_1, x_2) + \big((y_1, y_2) + (z_1, z_2)\big) \end{array}$$

c'est-à-dire que $+$ *est associative.*
— *Par ailleurs*

$$(x_1, x_2) + (0, 0) = (0, 0) + (x_1, x_2) = (x_1, x_2)$$

c'est-à-dire que $(0, 0)$ *est un élément neutre pour* $+$.
— *Enfin,*

$$(x_1, x_2) + (-x_1, -x_2) = (-x_1, -x_2) + (x_1, x_2) = (0, 0)$$

c'est-à-dire que $(-x_1, -x_2)$ *est l'opposé de* (x_1, x_2).
Il en résulte que $(G_1 \times G_2, +)$ *est un groupe. Comme de plus*

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2) = (y_1, y_2) + (x_1, x_2)$$

puisque G_1 *et* G_2 *sont abéliens,* $(G_1 \times G_2, +)$ *est lui-même abélien (cf. cours 0.5.6.i).)*

Dans la suite on utilisera librement la notation

$$(\mathbb{Z}^2,+) \;:=\; (\mathbb{Z}\times\mathbb{Z},+)\;.$$

2) () **Soient** a **et** b **deux entiers relatifs non nuls,** d **leur pgcd et** m **leur ppcm. On notera** $a \;:=\; da'$ **et** $b \;:=\; db'$.

a) () Rappeler pourquoi on peut écrire $d \;=\; au+bv$ avec u et v des entiers relatifs.
Solution : *(cf. cours I.3.3.3.)*

b) () Rappeler pourquoi a' et b' sont premiers entre eux.
Solution : *Comme* $d \;=\; au+bv$, $a = da'$ *et* $b = db'$, *puisque* $d \neq 0$ $a'u+b'v = 1$ *c'est-à-dire, grâce au théorème (cf. cours I.3.3.3,) que* a' *et* b' *sont premiers entre eux.*

c) () Donner en la justifiant la relation liant a', b', d et m.
Solution : *Tout d'abord*

$$a|a'b'd \;=\; ab' \text{ et } b|a'b'd \;=\; ba'$$

si bien que $m|a'b'd$.
Réciproquement :

$$\begin{array}{lrcl}
\forall x\in\mathbb{Z}, & a|x & \text{et} & b|x\\
\Rightarrow \quad \exists z\in\mathbb{Z},\; x=az & \text{et} & \exists w\in\mathbb{Z},\; x=bw & \\
\Rightarrow & az & = & bw\\
\Rightarrow & da'z & = & db'w\\
\Rightarrow & a'z & = & b'w\\
\Rightarrow & a' & | & w
\end{array}$$

on applique en effet le lemme de GAUSS *(cf. cours I.3.3.8,) puisque* a' *et* b' *sont premiers entre eux d'après b). Il s'ensuit qu'il existe* $t \in \mathbb{Z}$ *tel que*

$$w \;=\; a't \;\Rightarrow\; x \;=\; db'w \;=\; da'b't \;\Rightarrow\; da'b'|x \;\Rightarrow\; da'b'|m$$

si bien qu'on a :

$$m \;=\; da'b'\;. \qquad 1$$

3) () **Avec les notations de la question 2), a), on définit l'application :**

$$\begin{array}{rccc} f: & \mathbb{Z}^2 & \to & \mathbb{Z}^2\\ & (x,y) & \mapsto & (ux+vy,\,-b'x+a'y)\end{array}$$

a) () Montrer que f est un morphisme de groupes de $(\mathbb{Z}^2,+)$ dans lui-même.
Solution : *Pour tout* $\big((x_1,y_1),(x_2,y_2)\big) \in \mathbb{Z}^2\times\mathbb{Z}^2$, *on a :*

$$\begin{array}{rcl}
f\big((x_1,y_1)+(x_2,y_2)\big) f(x_1+x_2,y_1+y_2) & & \\
& = & \big(u*(x_1+x_2)+v*(y_1+y_2),\\
& & \quad -b'*(x_1+x_2)+a'*(y_1+y_2)\big)\\
\big(ux_1+vy_1,-b'x_1+a'y_1\big) & & \\
& & +\big(ux_2+vy_2,-b'x_2+a'y_2\big)\\
& = & f(x_1,y_1)+f(x_2,y_2)
\end{array}$$

ce qui prouve que f *est un morphisme de groupes (cf. cours 0.5.6.ii).)*

b) () Montrer que f est bijective et déterminer son application réciproque g.
Solution : *Pour tout $(z,t) \in \mathbb{Z}^2$ on résout l'équation d'inconnue $(x,y) \in \mathbb{Z}^2$:*

$$f(x,y) \;=\; (z,t) \qquad \textit{1}$$

qui équivaut à :

$$\begin{array}{rl} & \left\{\begin{array}{rcl} ux+vy & = & z \\ -b'x+a'y & = & t \end{array}\right\} \\ \Leftrightarrow & \left\{\begin{array}{rcl} ux+vy & = & z \\ (a'u+b'v)x & = & a'z-vt \end{array}\right\} . \end{array}$$

Or d'après la question 2), b), $a'u+b'v \;=\; 1$ si bien que l'équation 1 équivaut à :

$$\begin{array}{rl} & \left\{\begin{array}{rcl} ux+vy & = & z \\ x & = & a'z-vt \end{array}\right\} \\ \Leftrightarrow & \left\{\begin{array}{rcl} x & = & a'z-vt \\ (a'u+b'v)y & = & b'z+ut \end{array}\right\} \\ \Leftrightarrow & \left\{\begin{array}{rcl} x & = & a'z-vt \\ y & = & b'z+ut\,. \end{array}\right\} \end{array}$$

Il en résulte que pour tout $(z,t) \in \mathbb{Z}^2$, l'équation 1 possède une unique solution ce qui assure que f est bijective. Qui plus est on a déterminé ci-dessus cette solution en fonction de (z,t) ce qui définit l'application réciproque g de f par :

$$\begin{array}{rccl} g: & \mathbb{Z}^2 & \to & \mathbb{Z}^2 \\ & (z,t) & \mapsto & (a'z-vt, b'z+ut)\,. \end{array} \qquad \textit{2}$$

c) () Rappeler pourquoi g est un morphisme de groupes.
Solution : *Cela peut se voir directement sur l'expression de g établie en b).2 et qui permet de mener un calcul exactement analogue à celui de a). On peut aussi appliquer le résultat (cf. cours I.3.6.1.)*

4) () **On définit les applications :**

$$\begin{array}{rccl} p: & \mathbb{Z}^2 & \to & \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & (x,y) & \mapsto & (x \,\mathbf{mod}\, d, y \,\mathbf{mod}\, m) \\ q: & \mathbb{Z}^2 & \to & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ & (x,y) & \mapsto & (x \,\mathbf{mod}\, a, y \,\mathbf{mod}\, b)\,. \end{array}$$

a) () Montrer que p (resp. q,) est un morphisme de groupe de $(\mathbb{Z}^2,+)$ dans $(\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z},+)$ (resp. $(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z},+)$; puis que $p \circ f$ et $q \circ g$ sont des morphismes de groupes.
Solution :

*i) (p **et** q **sont des morphismes**)*
On fera la vérification pour p, celle pour q étant exactement la même.

$$\begin{array}{l} \forall (x_1,y_1) \in \mathbb{Z}^2, \\ \forall (x_2,y_2) \in \mathbb{Z}^2, \quad p\big((x_1,y_1)+(x_2,y_2)\big) \;=\; p(x_1+x_2, y_1+y_2) \\ \qquad\qquad\qquad\qquad\qquad\qquad = \; (x_1+x_2 \,\mathbf{mod}\, d, y_1+y_2 \,\mathbf{mod}\, m) \\ \qquad\qquad\qquad\qquad\qquad\qquad = \; (x_1 \,\mathbf{mod}\, d + x_2 \,\mathbf{mod}\, d, y_1 \,\mathbf{mod}\, m + y_2 \,\mathbf{mod}\, m) \\ \qquad\qquad\qquad\qquad\qquad\qquad = \; (x_1 \,\mathbf{mod}\, d, y_1 \,\mathbf{mod}\, m) + (x_2 \,\mathbf{mod}\, d, y_2 \,\mathbf{mod}\, m) \\ \qquad\qquad\qquad\qquad\qquad\qquad = \; p(x_1,y_1) + p(x_2,y_2) \end{array}$$

ce qui prouve que p est un morphisme de groupes (cf. cours 0.5.6.ii).)

*ii) (**Composées**)*

La composée de deux morphismes de groupes est encore un morphisme de groupes ; ce qu'on peut vérifier dans le cas particulier :

$$\begin{array}{l} \forall (x_1,y_1)\in\mathbb{Z}^2,\\ \forall (x_2,y_2)\in\mathbb{Z}^2,\quad p\big[f\big((x_1,y_1)+(x_2,y_2)\big)\big] \\ \qquad\qquad\qquad\qquad\qquad\qquad = \; p\big(f(x_1,y_1)+f(x_2,y_2)\big) \\ \qquad\qquad\qquad\qquad\qquad\qquad = \; p\big(f(x_1,y_1)\big) \\ \qquad\qquad\qquad\qquad\qquad\qquad\quad +p\big(f(x_2,y_2)\big)\ . \end{array}$$

b) () Déterminer $\operatorname{Ker} p$ et $\operatorname{Ker} q$.

Solution :

$$\begin{array}{lrcl} \forall (x,y)\in\mathbb{Z}^2, & q(x,y) & = & (0,0) \\ \Leftrightarrow & x \bmod a \;=\; 0 & \text{et} & y \bmod b \;=\; 0 \\ \Leftrightarrow & x \;\equiv\; 0\,[a] & \text{et} & y \;\equiv\; 0\,[b] \end{array}$$

si bien qu'on en déduit :

$$\operatorname{Ker} q \;=\; \{(ax,by)(x,y)\in\mathbb{Z}^2\} \text{ et } \operatorname{Ker} p \;=\; \{(dx,my)(x,y)\in\mathbb{Z}^2\}\ . \qquad 1$$

c) () Montrer qu'il existe un unique morphisme de groupes

$$f' \;:\; (\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z},+) \;\to\; (\mathbb{Z}/d\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z},+)$$

$$(\text{resp. } .g' \;:\; (\mathbb{Z}/d\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z},+) \;\to\; (\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z},+)\ )$$

tel que

$$f'\circ q \;=\; p\circ f \text{ (resp. } g'\circ p \;=\; q\circ g\ .)$$

Solution :

i) (f')

$$\begin{array}{lrcl} \forall (ax,by)\in\operatorname{Ker} q, & p\big(f(ax,by)\big) & = & p(aux+bvy,-b'ax+ba'y) \\ & & = & (d(a'ux+b'vy) \bmod d, m(x-+y) \bmod m) \\ & & = & (0,0) \end{array}$$

en utilisant question 2), c).1. Si bien que $\operatorname{Ker} q\subset \operatorname{Ker} p\circ f$ *et que d'après (cf. cours II.1.3.7.ii)i)l existe un unique morphisme*

$$f' \;:\; \operatorname{Im} q \;\to\; \mathbb{Z}/d\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z} \text{ tel que } f'\circ q \;=\; p\circ f\ .$$

Or q est surjective et par conséquent $\operatorname{Im} q \;=\; \mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$ *ce qui donne le résultat.*

ii) (g')

Pour tout $(dz,mt)\in\operatorname{Ker} p$, *on a, en utilisant l'expression de g donnée en question 3), b).2 :*

$$\begin{array}{lcl} q\big(g(dz,mt)\big) & = & q(a*dz-vmt,-b'dz+umt) \\ & = & (a(z-vb't) \bmod a, b(-z+ua't) \bmod b \\ & = & (0,0)\ . \end{array}$$

Si bien qu'on obtient un morphisme g' répondant à la question par le même argument que précédemment.

d) () Pour des applications

$$u \,:\, X \,\to\, Y \,,\; v \,:\, X \,\to\, Y \text{ et } w \,:\, W \,\to\, X$$

avec w surjective, montrer que

$$u \,=\, v \;\Leftrightarrow\; u \circ w \,=\, v \circ w \,.$$

Solution :

i) ***(Sens direct)***
Il est clair que $u \,=\, v \;\Rightarrow\; u \circ w \,=\, v \circ w$.

ii) ***(Sens réciproque)***

$$\forall \alpha \in X,\; \exists \beta \,\in\, W,\; \alpha \,=\, w(\beta) \;\Rightarrow\; u(\alpha) \,=\, u(w(\beta)) \,=\, v(w(\beta)) \,=\, v(\alpha) \,.$$

e) () Montrer finalement que f' et g' sont inverses l'un de l'autre c'est-à-dire qu'on a construit un isomorphisme de groupes

$$(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}, +) \;\cong\; (\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +) \,.$$

Solution : *On a :*

$$f' \circ g' \circ p \,=\, f' \circ q \circ g \,=\, p \circ f \circ g \,=\, p \,=\, \mathrm{Id} \circ p$$

d'où, d'après le point précédent, $f' \circ g' \,=\, \mathrm{Id}$.
De même

$$g' \circ f' \circ q \,=\, g' \circ p \circ f \,=\, q \circ g \circ f \,=\, q \,=\, \mathrm{Id} \circ q$$

d'où $g' \circ f' \,=\, q$.

f) () Peut-on déduire ce résultat d'un théorème connu lorsque $d = 1$? En d'autres termes quel résultat avons-nous généralisé ici ?
Solution : *Dans le cas où* $d \,=\, 1$ *l'isomorphisme* g' *est donné par le théorème chinois des restes (cf. cours I.3.6.1.)*

Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

Examen du 7 janvier 2015
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 : () **1)** () **Soit**

$$s := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 7 & 4 & 8 & 9 & 2 & 5 & 3 & 6 & 1 \end{pmatrix} \in \mathcal{S}_{10} .$$

Décomposer s en produit de cycles à supports deux à deux disjoints, donner la signature de s et calculer s^{2015}.

2) () Quelle est le plus grand ordre possible pour un élément de $\mathcal{S}_{10}$? Les éléments d'ordre maximal ont-ils tous même signature ?

Exercice B : () (**Le groupe de Klein**)

0) () (**Questions de cours**)

a) () Rappeler la définition du groupe symétrique $\mathcal{S}_n$ et du groupe alterné $\mathcal{A}_n$ pour $n \in \mathbb{N}^*$. Donner le nombre d'éléments $\#(\mathcal{S}_n)$ (resp. $\#(\mathcal{A}_n)$,) de $\mathcal{S}_n$, (resp. $\mathcal{A}_n$,) en fonction de n.

b) () Soit G un groupe.

i) Quand dit-on que deux éléments x et y de G sont conjugués ?

ii) Rappler ce que signifie que H est un sous-groupe distingué de G,

iii) Si H est un sous-groupe distingué de G, rappeler la définition du groupe quotient G/H.

Soient $v_1 := (1\,2)(3\,4)$ **et** $v_2 = (1\,3)(2\,4)$ **des éléments de** $\mathcal{S}_4$.

1) () Calculer

a) () $v_3 := v_1 v_2$,

b) ()

$$v_1^2 \, , \; v_2^2 \, , \; v_3^2,$$

c) () pour

$$\{a, b, c, d\} = [1; 4] \, , \; (a\,b)(c\,d)(a\,c)(b\,d) \, .$$

On note

$$X := \{v_1, v_2, v_3\} \text{ et } V := X \cup \{\mathrm{Id}\} .$$

2) () **a)** () Montrer que V est un sous-groupe de $\mathcal{A}_4$ et donner sa table de composition.
Indication : *On pourra utiliser la question 1), b) et la question 1), c).*

b) () Que dire de l'application :

$$\begin{array}{rcl} V & \to & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \mathrm{Id} & \mapsto & (0,0) \\ v_1 & \mapsto & (1,0) \\ v_2 & \mapsto & (0,1) \\ v_3 & \mapsto & (1,1) \ ? \end{array}$$

c) () Déterminer l'ensemble des éléments de type cyclique $(2,2)$ dans $\mathcal{S}_4$.

d) () Montrer que, pour tout $x \in X$ et tout $s \in \mathcal{S}_4$, $sxs^{-1} \in X$.

e) () Déduire de ce qui précède que V est un sous-groupe distingué de $\mathcal{S}_4$ et de $\mathcal{A}_4$.

On note

$$\lambda : \mathcal{A}_4 \to K := \mathcal{A}_4/V \text{ et } \pi : \mathcal{S}_4 \to Q := \mathcal{S}_4/V$$

les groupe quotients munis de leur surjection canonique respective.

3) () **a)** () Donner le nombre d'éléments $\#(K)$ (resp. $\#(Q)$,) de K (resp. Q.)

b) () Montrer que K est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

On note désormais $\mathcal{S}(X)$ l'ensemble des bijections de X dans lui-même (où $X = \{v_1, v_2, v_3\}$ est l'ensemble des éléments de type $(2,2)$ déjà considéré préalablement.)

4) () **a)** () Rappeler comment le résultat de la question 2), d) permet de définir un morphisme de groupes

$$\phi : \mathcal{S}_4 \to \mathcal{S}(X) .$$

b) () Montrer que $V \subset \mathrm{Ker}\,\phi$ et en déduire qu'il existe un morphisme de groupes

$$\psi : Q \to \mathcal{S}(X) \text{ tel que } \psi \circ \pi = \phi .$$

c) () Pour $\{a,b,c,d\} = [1;4]$, calculer

$$(b\,c)(a\,b)(c\,d)(b\,c) .$$

d) () Déduire de ce qui précède que $Q \cong \mathcal{S}_3$.

Exercice C : () (**Autour de l'irréductibilité et du critère d'Eisenstein**)
(**Notations**)

i) (PGCD PPCM)
Pour deux éléments a et b d'un anneau A, on note $a \wedge b$ (resp. $[a,b]$) leur PGCD (resp. leur PPCM) lorsqu'il existe (typiquement pour $A = \mathbb{Z}$ ou $A = \mathbb{K}[X]$ avec $\mathbb{K}$ un corps.)

ii) ($\overline{\mathbb{Z}}$)

On introduit le symbole $(+\infty) \notin \mathbb{Z}$ et on définit : $\overline{\mathbb{Z}} := \mathbb{Z} \cup \{(+\infty)\}$. On prolonge l'addition $+$ et la relation d'ordre $\leq$ de $\mathbb{Z}$ à $\overline{\mathbb{Z}}$ par les formules :

$\overline{\mathbb{Z}}_1$**)**

$$\forall n \in \mathbb{Z},\ n\ +\ (+\infty)\ =\ (+\infty)\ +\ n\ =\ (+\infty),$$
$$(+\infty)\ +\ (+\infty)\ =\ (+\infty)\,;$$

$\overline{\mathbb{Z}}_2$**)**

$$\forall n \in \mathbb{Z},\ n\ <\ (+\infty)\ \Leftrightarrow\ n\ \leq\ (+\infty) \text{ et } n\ \neq\ (+\infty)\,;$$
$$(+\infty)\ \leq\ (+\infty)\,.$$

L'ensemble $\overline{\mathbb{N}}$ est évidemment défini comme $\mathbb{N} \cup \{(+\infty)\}\ \subset\ \overline{\mathbb{Z}}$, et hérite de la structure donnée par $\overline{\mathbb{Z}}_1$) et $\overline{\mathbb{Z}}_2$).

iii) ($\mathcal{P}$)

On note $\mathcal{P} \subset \mathbb{N}$ l'ensemble des nombres premiers.

1) () **(Valuations p-adiques)**

Soit $p\ \in\ \mathcal{P}$.

a) () 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 $v_p\ :\ \mathbb{Z}\ \to\ \overline{\mathbb{N}}$.

b) () Pour tout $x\ \in\ \mathbb{Q}\,,\ x\ \neq\ 0$, montrer qu'il existe un unique triplet

$$(r_x, n_x, d_x)\ \in\ \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}^* \text{ tel que } x\ =\ p^{r_x}\frac{n_x}{d_x}\,,\ n_x \wedge d_x\ =\ 1\,,\ p \wedge d_x\ =\ 1 \text{ et } p \wedge n_x\ =\ 1\,.$$

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

$$\mathcal{S}(x)\ :=\ \{p\ \in\ \mathbb{P}\,;\ v_p(x)\ \neq\ 0\} \text{ et } \mathcal{S}(0)\ :=\ \mathcal{P}\,.$$

c) () **(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)

$$\forall\ (x,y)\ \in\ \left(\mathbb{Z}\setminus\{0\}\right)^2\ ,\ x\wedge y\ =\ \prod_{p\in\mathcal{P}} p^{\min(v_p(x),v_p(y))} \text{ et } [x,y]\ =\ \prod_{p\in\mathcal{P}} p^{\max(v_p(x),v_p(y))}\ .$$

2) () **Posons :**

$$\forall P \in \mathbb{Q}[X],\ P\ :=\ \sum_{i=0}^{\delta} a_i X^i\ ,\ \forall p \in \mathcal{P},$$

si $P\ \neq\ 0$

$$\begin{array}{rcl} V_p(P) & := & \min_{i=0}^{\delta}(v_p(a_i)) \\ \mathcal{S}(P) & := & \{p\ \in\ \mathbb{P}\,;\, V_p(P)\ \neq\ 0\} \end{array}$$

si $P\ =\ 0$

$$\begin{array}{rcl} V_p(P) & := & (+\infty) \\ \mathcal{S}(P) & := & \mathcal{P}\ . \end{array}$$

a) () Pour tout $P \in \mathbb{Q}[X]\setminus\{0\}$, vérifier que :

$\text{Val}[X]_1$)

$$\forall P \in \mathbb{Q}[X],\ P\ \in\ \mathbb{Z}[X]\ \Leftrightarrow\ V_p(P)\ \geq\ 0\, \forall\, p\ \in\ \mathcal{P}\ .$$

$\text{Val}[X]_2$) 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

$$R\ :=\ PQ\ =\ \sum_{i=0}^{\deg(R)} c_i X^i\ .$$

b) () Écrire $\{c_i\}_{0\leq i\leq \deg(R)}$ en fonction des

$$\{a_i\}_{0\leq i\leq \deg(P)} \text{ et } \{b_i\}_{0\leq i\leq \deg(Q)}\ .$$

c) () En déduire que :

$$\begin{array}{lrcl} \forall 0 \leq k \leq \deg(R),\ \forall 0 \leq i \leq \deg(P),\ \forall 0 \leq j \leq \deg(Q), & i+j & = & k \\ \Rightarrow & v_p(c_k) & \geq & v_p(a_i)+v_p(b_j) \\ & & \geq & V_p(P)+V_p(Q)\ . \end{array}$$

d) () 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

$$v_p(a_i) \ = \ V_p(P) \text{ (resp. } v_p(b_j) \ = \ V_p(Q) \text{ .)}$$

Montrer que

$$v_p(c_{m+n}) \ = \ V_p(P) \ + \ V_p(Q) \ .$$

e) () Établir finalement que

$$\forall (P,Q) \in \left(\mathbb{Q}[X] \setminus \{0\}\right)^2, \ \forall p \in \mathbb{P}, \ V_p(PQ) \ = \ V_p(P) \ + \ V_p(Q) \ .$$

3) () (**Irréductibilité des polynômes à coefficients entiers**)
Soit $P \in \mathbb{Z}[X] \setminus \{0\}$. **On suppose qu'il existe**

$$(Q,R) \ \in \ \left(\mathbb{Q}[X] \setminus \mathbb{Q}\right)^2 \mid P \ = \ QR \ .$$

a) () 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

$$V_p(aR) \ \geq \ 0 \text{ et } V_p(\frac{1}{a}Q) \ \geq \ 0 \ .$$

b) () En déduire qu'il existe

$$(Q_1,R_1) \ \in \ \left(\mathbb{Z}[X] \setminus \{-1;1\}\right)^2 \mid P \ = \ R_1Q_1 \ .$$

c) () 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 $\mathbb{Q}[X]$.

4) () (**Le critère d'Eisenstein**)
Pour $p \in \mathcal{P}$ **un nombre premier, on note** $\mathbb{F}_p \ := \ (\mathbb{Z}/p\mathbb{Z},+,*)$ **le corps à** p **éléments et pour tout** $a \in \mathbb{Z}$, $\overline{a}$ **sa classe dans** $\mathbb{F}_p$.
Pour $P \ := \ \sum_{i=0}^{\deg(P)} a_iX^i \ \in \ \mathbb{Z}[X]$, **on pose** $\overline{P} \ := \ \sum_{i=0}^{\deg(P)} \overline{a}_iX^i \ \in \ \mathbb{F}_p[X]$.
On dit que P **vérifie** † **si :**

$$\dagger \ : \ a_{\deg(P)} \ = \ 1 \ ; \ v_p(a_0) \ = \ 1 \text{ et } \ v_p(a_i) \ > \ 0 \ , \ \forall 1 \leq i < \deg(P) \ .$$

a) () Pour $a \in \mathbb{Z}$, exprimer la condition $\overline{a} \ = \ 0$ à l'aide de $v_p(\cdot)$.

b) () Rappeler pourquoi

$$\forall P \in \mathbb{Z}[X], \ \forall Q \in \mathbb{Z}[X], \ \overline{P+Q} \ = \ \overline{P} + \overline{Q} \text{ et } \overline{P*Q} \ = \ \overline{P} * \overline{Q} \ .$$

c) () Montrer que pour tout $P \in \mathbb{Z}[X]$, tout $Q \in \mathbb{Z}[X]$, P vérifie † et $Q|P$ entraîne $\overline{Q} \ = \ \pm X^{\deg(Q)}$.

d) () Pour tout

$$P \in \mathbb{Z}[X] \ , \ Q \ := \ \sum_{i=0}^{\deg(Q)} b_iX^i \in \mathbb{Z}[X] \ , \ R \ := \ \sum_{i=0}^{\deg(R)} c_iX^i \in \mathbb{Z}[x],$$

montrer que $P \ = \ Q*R$, P satisfait †, $\deg(Q) > 0$, $\deg(R) > 0$ entraîne $v_p(b_0) \ > \ 0$ et $v_p(c_0) \ > \ 0$.

e) () Déduire de ce qui précède que pour $P \in \mathbb{Z}[X]$, P vérifie † entraîne P est irréductible.

f) () Montrer finalement qu'il existe des polynômes irréductibles de tout degré dans $\mathbb{Q}[X]$.

Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

Corrigé de l'examen du 7 janvier 2015

Exercice A : () **1)** () **Soit**

$$s := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 7 & 4 & 8 & 9 & 2 & 5 & 3 & 6 & 1 \end{pmatrix} \in \mathcal{S}_{10} .$$

Décomposer s en produit de cycles à supports deux à deux disjoints, donner la signature de s et calculer s^{2015}.

Solution : *On a*

$$s = (1\ 10)(27596)(348) = c_1c_2c_3$$

avec

$$c_1 := (1\ 10)\ ,\ c_2 := (27596) \text{ et } c_3 := (348)\ .$$

On peut alors déterminer la signature de s soit en disant que s possède $\nu(s) = 3$ orbites et que

$$\sigma(s) = (-1)^{10-\nu(s)} = (-1)^7 = -1 \textit{ (cf. II.2.4.1.ii);)}$$

on peut aussi utiliser le corollaire II.2.4.4 qui assure que $\sigma(s) = \sigma(c_1) * \sigma(c_2) * \sigma(c_3)$, puis la formule donnant la signature d'un ℓ-cycle.

On constate ensuite que c_1, c_2 et c_3 sont d'ordre respectif $2, 5$ et 3 égal à leur longueur (cf. II.2.2.1.) De plus les cycles c_i ,$_{1\leq i\leq 3}$ étant à support deux à deux disjoints ils commutent (cf. II.2.2.5,) si bien qu'en remarquant que

$$2015 \equiv 1\ [2]\ ,\ 2015 \equiv 0\ [5] \text{ et } 2015 \equiv 2\ [3]\ ,$$

on a :

$$s^{2015} = c_1^{2015} * c_2^{2015} * c_3^{2015} = c_1 * c_3^2 = (1\ 10)(384)\ .$$

2) () Quelle est le plus grand ordre possible pour un élément de $\mathcal{S}_{10}$? Les éléments d'ordre maximal ont-ils tous même signature ?

Solution : *On sait que, dans un groupe, les éléments d'une même classe de conjugaison ont tous même ordre (cf. II.1.3.3.) De plus, dans le groupe symétrique, on sait qu'une classe de conjugaison est caractérisée par le type cyclique commun de ses éléments (cf. II.2.3.5.a),) dont l'ordre est alors le* ***Ppcm*** *des longueurs des cycles qui le décomposent. Il sufffit donc de faire la liste des types cycliques possibles pour les éléments*

de $\mathcal{S}_{10}$ et de donner l'ordre correspondant :

Type cyclique	*ordre*
(2)	2
$(2,2)$	2
$(2,3)$	6
$(2,4)$	4
$(2,5)$	10
$(2,6)$	6
$(2,7)$	14
$(2,8)$	8
$(2,2,2)$	2
$(2,2,3)$	6
$(2,2,4)$	4
$(2,2,5)$	10
$(2,2,6)$	6
$(2,3,3)$	6
$(2,3,4)$	12
$(2,3,5)$	30
$(2,4,4)$	4
(3)	3
$(3,3)$	3
$(3,4)$	12
$(3,5)$	15
$(3,6)$	6
$(3,7)$	21
(4)	4
$(4,4)$	4
$(4,5)$	20
$(4,6)$	12
(5)	5
$(5,5)$	5
(6)	6
(7)	7
(8)	8
(9)	9
(10)	10 .

Il s'ensuit que l'ordre maximal pour un élément de $\mathcal{S}_{10}$ est 30 et qu'il correspond aux éléments de type cyclique $(2,3,5)$. Tous ces éléments appartenant à une même classe de conjugaison, ils ont même signature.

Exercice B : () (**Le groupe de Klein**)

0) () (**Questions de cours**)

a) () Rappeler la définition du groupe symétrique $\mathcal{S}_n$ et du groupe alterné $\mathcal{A}_n$ pour $n \in \mathbb{N}^*$. Donner le nombre d'éléments $\#(\mathcal{S}_n)$ (resp. $\#(\mathcal{A}_n)$,) de $\mathcal{S}_n$, (resp. $\mathcal{A}_n$,) en fonction de n.

Solution : *Le groupe symétrique $\mathcal{S}_n$ est le groupe des bijections de l'ensemble $[1;n]$ des n premiers entiers naturels, muni de la loi de composition des applications (cf. cours II.2.1.1.ii),) et le groupe alterné $\mathcal{A}_n$ est le sous-groupe de $\mathcal{S}_n$ constitué des éléments de signature 1 encore appelés permutations paires (cf. cours II.2.4.5.i).)*

b) () Soit G un groupe.

i) Quand dit-on que deux éléments x et y de G sont conjugués ?

ii) Rappler ce que signifie que H est un sous-groupe distingué de G,

iii) Si H est un sous-groupe distingué de G, rappeler la définition du groupe quotient G/H.

Soient $v_1 := (1\,2)(3\,4)$ **et** $v_2 = (1\,3)(2\,4)$ **des éléments de** $\mathcal{S}_4$.

1) () Calculer

a) () $v_3 := v_1 v_2$,

Solution : *On a*

$$v_3 = v_1 v_2 = (1\,2)(3\,4)(1\,3)(2\,4)$$

d'où :

$$\begin{array}{rcccl} v_3(1) & = & v_1 * v_2(1) & = & 4 \\ v_3(2) & = & v_1 * v_2(2) & = & 3 \\ v_3(3) & = & v_1 * v_2(3) & = & 2 \\ v_3(4) & = & v_1 * v_2(4) & = & 1\,. \end{array}$$

Il en résulte que $v_3 = (1\,4)(2\,3)$.

b) ()

$$v_1^2\,,\ v_2^2\,,\ v_3^2,$$

Solution : *On a*

$$v_1^2 = [(1\,2)(3\,4)]^2 = (1\,2)(3\,4)(1\,2)(3\,4) = (1\,2)(3\,4)^2(1\,2) = (1\,2)^2 = \mathrm{Id},$$

de même

$$v_2^2 = [(1\,3)(2\,4)]^2 = (1\,3)(2\,4)(1\,3)(2\,4) = (1\,3)(2\,4)^2(1\,3) = (1\,3)^2 = \mathrm{Id},$$

enfin

$$v_3^2 = [(1\,4)(2\,3)]^2 = (1\,4)(2\,3)(1\,4)(2\,3) = (1\,4)(2\,3)^2(1\,4) = (1\,4)^2 = \mathrm{Id}\,.$$

c) () pour

$$\{a,b,c,d\} = [1;4]\,,\ (a\,b)(c\,d)(a\,c)(b\,d)\,.$$

Solution :

$$(a\,b)(c\,d)(a\,c)(b\,d) = (a\,d)(b\,c)\,.$$

On note

$$X := \{v_1, v_2, v_3\} \text{ et } V := X \cup \{\mathrm{Id}\}\,.$$

2) () **a)** () Montrer que V est un sous-groupe de $\mathcal{A}_4$ et donner sa table de composition.

Indication : *On pourra utiliser la question 1), b) et la question 1), c).*

Solution : *Il résulte de la question 1), b) que pour tout* $1 \le i \le 3$ $v_i^2 = \mathrm{Id}$, *et de la question 1), c), que, pour tout* $1 \le i \le 3$ *tout* $1 \le j \le 3$ $v_i v_j = v_j v_i = v_k$ *où* $\{i,j,k\} = [1;3]$. *On peut donc écrire la table de composition suivante :*

$$\begin{array}{ccccc} & \mathrm{Id} & v_1 & v_2 & v_3 \\ \mathrm{Id} & \mathrm{Id} & v_1 & v_2 & v_3 \\ v_1 & v_1 & \mathrm{Id} & v_3 & v_2 \\ v_2 & v_2 & v_3 & \mathrm{Id} & v_1 \\ v_3 & v_3 & v_2 & v_1 & \mathrm{Id} \end{array}\,.$$

Cette table assure que la loi de composition est interne sur V, *et que tout élément est son propre inverse. Ainsi* V *est un groupe. Par ailleurs les éléments de* V *sont tous de signature* 1 *si bien que* V *est un sous-groupe de* $\mathcal{A}_4$.

b) () Que dire de l'application :

$$\begin{array}{rcl} V & \to & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \mathrm{Id} & \mapsto & (0,0) \\ v_1 & \mapsto & (1,0) \\ v_2 & \mapsto & (0,1) \\ v_3 & \mapsto & (1,1) \, ? \end{array}$$

Solution : *C'est un isomorphisme de groupes.*

c) () Déterminer l'ensemble des éléments de type cyclique $(2,2)$ dans $\mathcal{S}_4$.

Solution : *Si $s \in \mathcal{S}_4$ est un élément de type cyclique $(2,2)$ il existe des éléments a, b, c, d deux à deux distincts dans $[1;4]$ tels que $s = (a\,b)(c\,d)$. On constate alors qu'on a nécessairement*

$$s = (1\,2)(3\,4) = v_1 \text{ ou } s = (1\,3)(2\,4) = v_2 \text{ ou } s = (1\,4)(2\,3) = v_3$$

si bien que l'ensemble des éléments de type cyclique $(2,2)$ est exactement l'ensemble X.

d) () Montrer que, pour tout $x \in X$ et tout $s \in \mathcal{S}_4$, $sxs^{-1} \in X$.

Solution : *On a vu en c) que X est l'ensemble des éléments de type cyclique $(2,2)$. C'est donc une classe de conjugaison si bien que pour tout $s \in \mathcal{S}_4$ et tout $x \in X$, $sxs^{-1} \in X$.*

e) () Déduire de ce qui précède que V est un sous-groupe distingué de $\mathcal{S}_4$ et de $\mathcal{A}_4$.

Solution : *D'après a), V est un sous-groupe de $\mathcal{A}_4 \subset \mathcal{S}_4$ donc en particulier aussi un sous-hgroupe de $\mathcal{S}_4$.*

De plus on a montré en d) que X est stable sous l'action de $\mathcal{S}_4$ par conjugaison. Comme il en est évidemment de même de $\{\mathrm{Id}\}$, V est distingué dans $\mathcal{S}_4$. Il l'est a fortiori dans $\mathcal{A}_4 \subset \mathcal{S}_4$.

On note

$$\lambda : \mathcal{A}_4 \to K := \mathcal{A}_4/V \text{ et } \pi : \mathcal{S}_4 \to Q := \mathcal{S}_4/V$$

les groupe quotients munis de leur surjection canonique respective.

3) () **a)** () Donner le nombre d'éléments $\#(K)$ (resp. $\#(Q)$,) de K (resp. Q.)

Solution : *Il découle de la définition même de V que $\#(V) = 4$, et l'on a donc :*

$$\#(K) = \#\big(\mathcal{A}_4/V\big) = \frac{\#(\mathcal{A}_4)}{\#(V)} = \frac{12}{4} = 3$$

et

$$\#(Q) = \#\big(\mathcal{S}_4/V\big) = \frac{\#(\mathcal{S}_4)}{\#(V)} = \frac{24}{4} = 6\,.$$

b) () Montrer que K est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

Solution : *Si on le connaît on peut utiliser le résultat qu'un groupe de cardinal premier p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

Sinon, puisque $\#(K) \neq 1$, il existe un élément $x \in K, x \neq 1$. Le théorème de Lagrange assure que l'ordre de x divise 3 i.e. $x^3 = 1$ et $x^2 \neq 1$. Comme on ne peut pas non plus avoir $x^2 = x$ qui entraînerait $x = 1$, on en déduit $K = \{1, x, x^2\}$.

Dès lors le morphisme de groupe

$$\mathbb{Z} \to K\,,\ n \mapsto x^n$$

se factorise en un isomorphisme

$$\mathbb{Z}/3\mathbb{Z} \cong K\,.$$

On note désormais $\mathcal{S}(X)$ l'ensemble des bijections de X dans lui-même (où $X = \{v_1, v_2, v_3\}$ est l'ensemble des éléments de type $(2,2)$ déjà considéré préalablement.)

4) () **a)** () Rappeler comment le résultat de la question 2), d) permet de définir un morphisme de groupes

$$\phi : \mathcal{S}_4 \to \mathcal{S}(X) .$$

Solution : *Pour tout $s \in \mathcal{S}_4$ et tout $x \in X$, on a montré à la question 2), d) que $sxs^{-1} \in X$. Il s'ensuit que pour s fixé, $x \mapsto sxs^{-1}$, est une application de X dans lui-même. De plus $x \mapsto s^{-1}xs^{-1^{-1}}$ étant son application réciproque, c'est une bijection de X dans lui-même qu'on notera $\phi(s)$. On définit ainsi une application $\phi : \mathcal{S}_4 \to \mathcal{S}(X)$.*

Or pour tout $(s,t) \in \mathcal{S}_4 \times \mathcal{S}_4$, et tout $x \in X$,

$$\phi(s\,t)(x) = stx(st)^{-1} = stxt^{-1}s^{-1} = \phi(s)[txt^{-1}] = \phi(s)[\phi(t)(x)] = \phi(s) \circ \phi(t)(x)$$

ce qui assure que ϕ est un morphisme de groupes.

b) () Montrer que $V \subset \operatorname{Ker}\phi$ et en déduire qu'il existe un morphisme de groupes

$$\psi : Q \to \mathcal{S}(X) \text{ tel que } \psi \circ \pi = \phi .$$

Solution : *Pour tout $v \in V$, et tout $x \in X$, en particulier $x \in V$. Comme V est un groupe abélien (cf. question 2), b)question 2), a),)*

$$vx = xv \Rightarrow vxv^{-1} = x \Rightarrow \phi(v)(x) = x \Rightarrow \phi(v) = \mathrm{Id}_X \Rightarrow v \in \operatorname{Ker}\phi .$$

Il s'ensuit que ϕ se factorise en un morphisme de groupe

$$\psi : Q = \mathcal{S}_4/V \to \mathcal{S}(X) \text{ tel que } \psi \circ \pi = \phi .$$

c) () Pour $\{a,b,c,d\} = [1;4]$, calculer

$$(b\,c)(a\,b)(c\,d)(b\,c) .$$

Solution :

$$\begin{aligned}(b\,c)(a\,b)(c\,d)(b\,c) &= (c\,b\,a)(d\,c\,b)\\ &= (a\,c\,b)(c\,b\,d)\\ &= (a\,c)(c\,b)(c\,b)(b\,d)\\ &= (a\,c)(b\,d) .\end{aligned}$$

On peut aussi faire le calcul de la manière suivante :

$$\begin{aligned}(b\,c)(a\,b)(c\,d)(b\,c) &= (b\,c)(a\,b)(b\,c)(b\,c)(c\,d)(b\,c)\\ &= ((b\,c)(a)\,(b\,c)(b))((b\,c)(c)\,(b\,c)(d))\\ &= (a\,c)(b\,d) .\end{aligned}$$

d) () Déduire de ce qui précède que $Q \cong \mathcal{S}_3$.

Solution : *La bijection*

$$X \cong [1;3]\,,\ v_i \mapsto i$$

induit un isomorphisme $\nu : \mathcal{S}(X) \cong \mathcal{S}_3$ *. Il découle de c) que :*

$$\begin{aligned}
\phi[(2\,3)](v_1) &= v_2\\
\phi[(2\,3)](v_2) &= v_1\\
\phi[(2\,3)](v_3) &= v_3\\
\phi[(2\,4)](v_2) &= v_3\\
\phi[(2\,4)](v_3) &= v_2\\
\phi[(2\,4)](v_1) &= v_1\,.
\end{aligned}$$

Donc finalement

$$\nu\big[\phi[(2\,3)]\big] = (1\,2) \text{ et } \nu\big[\phi[(2\,4)]\big] = (2\,3)\,.$$

Or $(1\,2)$ *et* $(2\,3)$ *engendrent* $\mathcal{S}_3$*, si bien que* $\operatorname{Im}\nu\circ\phi = \mathcal{S}_3$*. Il en résulte que* $\nu\circ\phi$ *est un morphisme surjectif. Puisque* ν *est un isomorphisme, il s'ensuit que* ϕ *est un morphisme surjectif. Cela entraîne que* ψ *est un morphisme surjectif. Or*

$$\#(Q) = \#(\mathcal{S}(X)) = \#(\mathcal{S}_3)$$

si bien que ψ *est un isomorphisme et*

$$\nu\circ\psi : Q \cong \mathcal{S}_3$$

est l'isomorphisme désiré.

Exercice C : () (**Autour de l'irréductibilité et du critère d'Eisenstein**)
(**Notations**)

i) (PGCD PPCM)

Pour deux éléments a **et** b **d'un anneau** A**, on note** $a\wedge b$ **(resp.** $[a,b]$**) leur PGCD (resp. leur PPCM) lorsqu'il existe (typiquement pour** $A=\mathbb{Z}$ **ou** $A=\mathbb{K}[X]$ **avec** $\mathbb{K}$ **un corps.)**

ii) ($\overline{\mathbb{Z}}$**)**

On introduit le symbole $(+\infty)\notin\mathbb{Z}$ **et on définit :** $\overline{\mathbb{Z}} := \mathbb{Z}\cup\{(+\infty)\}$**. On prolonge l'addition** $+$ **et la relation d'ordre** $\leq$ **de** $\mathbb{Z}$ **à** $\overline{\mathbb{Z}}$ **par les formules :**

$\overline{\mathbb{Z}}_1$**)**

$$\forall n\in\mathbb{Z},\ n+(+\infty)=(+\infty)+n=(+\infty),$$
$$(+\infty)+(+\infty)=(+\infty)\,;$$

$\overline{\mathbb{Z}}_2$**)**

$$\forall n\in\mathbb{Z},\ n<(+\infty)\Leftrightarrow n\leq(+\infty)\text{ et }n\neq(+\infty)\,;$$
$$(+\infty)\leq(+\infty)\,.$$

L'ensemble $\overline{\mathbb{N}}$ **est évidemment défini comme** $\mathbb{N}\cup\{(+\infty)\}\subset\overline{\mathbb{Z}}$**, et hérite de la structure donnée par** $\overline{\mathbb{Z}}_1$**) et** $\overline{\mathbb{Z}}_2$**).**

iii) ($\mathcal{P}$)

On note $\mathcal{P}\subset\mathbb{N}$ **l'ensemble des nombres premiers.**

1) () **(Valuations p-adiques)**
Soit $p \in \mathcal{P}$.

a) () 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 :

$$x = p^{r_x} y_x \text{ et } p \wedge y_x = 1 .$$

Solution :

*i) (**Existence**)*
Pour tout $x \in \mathbb{Z}$, on a toujours $1 = p^0 | x$ si bien que $R := \{r \in \mathbb{N} ; p^r | x\} \neq \emptyset$. De plus, $p^r | x$ entraîne, pour $x \neq 0$, $|p^r| \leq |x|$. Comme $p \geq 2$, $\forall r \in \mathbb{N}$, $r \leq p^r$. Il s'ensuit que R est borné par $|x|$ et possède donc un plus grand éléments r_x. Il existe donc y_x tel que $x = p^{r_x} y_x$. Par construction $p \not| y_x$. Comme de plus, $p \wedge y_x | p$, $p \wedge y_x \in \{-p; -1; 1; p\}$ donc $p \wedge y_x = 1$. On a ainsi prouvé l'existence du couple (r_x, y_x).

*ii) (**Unicité**)*
Si (r, y) et (s, z) sont deux couples répondant à la question on a $p^r y = x = p^s z$. Si $r \neq s$, on peut supposer $r > s$, d'où

$$p^{r-s} \in \mathbb{Z} \text{ et } p^{r-s} y = z .$$

Ceci entraîne $p | z$ qui contredit $p \wedge z = 1$. on a donc $r = s$ qui entraîne $y = z$ ce qui prouve l'unicité du couple (r_x, y_x).

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 $v_p : \mathbb{Z} \to \overline{\mathbb{N}}$.

b) () Pour tout $x \in \mathbb{Q}$, $x \neq 0$, montrer qu'il existe un unique triplet

$$(r_x, n_x, d_x) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{N}^* \text{ tel que } x = p^{r_x} \frac{n_x}{d_x} ,\ n_x \wedge d_x = 1 ,\ p \wedge d_x = 1 \text{ et } p \wedge n_x = 1 .$$

Solution :

*i) (**Existence**)*
Pour tout $x \in \mathbb{Q}$, $x \neq 0$, il existe un couple $(n, d) \in \mathbb{Z} \times \mathbb{N}^*$ tel que

$$x = \frac{n}{d} \text{ et } d \wedge n = 1 .$$

D'après la question précédente, on peut écrire

$$n = p^{v_p(n)} n_x \text{ et } d = p^{v_p(d)} d_x .$$

Posons alors $r_x := v_p(n) - v_p(d)$. On a alors $x = p^{r_x} \frac{n_x}{d_x}$. Le fait que $n \wedge d = 1$ entraîne bien évidemment que $d_x \wedge n_x = 1$ quant au fait que

$$p \wedge d_x = 1 \text{ et } p \wedge n_x = 1,$$

il découle de la définition même de v_p. On a ainsi assuré l'existence de (r_x, n_x, d_x).

*ii) (**Unicité**)*
L'unicité est une conséquence facile du lemme de GAUSS.

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

$$\mathcal{S}(x) := \{p \in \mathbb{P} ;\, v_p(x) \neq 0\} \text{ et } \mathcal{S}(0) := \mathcal{P} .$$

c) () (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$_6$)
$$\forall\, (x, y) \in \left(\mathbb{Z} \setminus \{0\}\right)^2 ,\ x \wedge y = \prod_{p \in \mathcal{P}} p^{\min(v_p(x), v_p(y))} \text{ et } [x, y] = \prod_{p \in \mathcal{P}} p^{\max(v_p(x), v_p(y))} .$$

Solution :

Val$_1$) Si $y = 0$,
$$\forall p \in \mathcal{P},\ v_p(y) = (+\infty) \ \Rightarrow\ v_p(x) \leq v_p(y)$$
(cf. ii).$\overline{\mathbb{Z}}_2$).) Si $y \neq 0$, $x|y \ \Rightarrow\ x \neq 0$. Il existe alors (r, x', s, y') comme en a) tel que $x = p^r x'$ et $y = p^s y'$. Or
$$\left(r > s \text{ et } x|y\right) \ \Rightarrow\ p^{r-s} x'|y' \ \Rightarrow\ p|y'$$
ce qui contredit la définition de y'. On a donc
$$x|y \ \Rightarrow\ v_p(x) \leq v_p(y) .$$

Val$_2$) *i)* *($x \in \mathbb{Z} \setminus \{0\}$)*

Soit $x_0 := x \in \mathbb{Z} \setminus \{0\}$. *Remarquons que si* $x_0 \in \{-1, 1\}$, $\mathcal{S}(X) = \emptyset$. *Sinon, soit* $p_0 \in \mathcal{S}(x_0)$. *Écrivons alors* $x_0 = p_0^{v_{p_0}(x_0)} x_1$. *Il découle de Val$_1$) que* $\mathcal{S}(x_0) = \mathcal{S}(x_1) \cup \{p_0\}$. *Par ailleurs,* $|x_1| < |x_0|$.

On peut donc ainsi construire par récurrence une suite $(x_n)_{,n\in\mathbb{N}}$ *d'entiers relatifs et une suite* $(p_n)_{,n\in\mathbb{N}}$ *de nombres premiers telles que*

$$\mathcal{S}(x_{n+1}) = \mathcal{S}(x_n) \cup \{p_n\} \text{ et } |x_{n+1}| < |x_n| .$$

Il existe alors un plus petit entier n_0 *tel que* $|x_{n_0}| = 1$, *c'est-à-dire* $\mathcal{S}(x_{n_0}) = \emptyset$. *Il en résulte que*

$$\mathcal{S}(x) = \mathcal{S}(x_0) = \bigcup_{n=0}^{n_0-1} \{p_n\}$$

qui est bien un ensemble fini. Il résulte de plus, presqu'immédiatement de la construction précédente que

$$\forall x \in \mathbb{Z} \setminus \{0\} , \ x = \epsilon \prod_{p\in\mathcal{S}(x)} p^{v_p(x)} , \ \epsilon \in \{-1, 1\} .$$

ii) *($x \in \mathbb{Q} \setminus \{0\}$)*

Pour $x \in \mathbb{Q} \setminus \{0\}$, *écrivons* $x = \dfrac{n}{d}$, *et on conclut en appliquant le résultat précédent à* n *et* d.

Val$_3$) Découle immédiatement de Val$_2$).

Val$_4$) Découle pour ainsi dire de la définition de v_p.

Val$_5$) *i)* ***(Produit)***

Si $x = 0$ *ou* $y = 0$,

$$v_p(xy) = v_p(0) = (+\infty) = v_p(x) + (+\infty) \text{ ou } v_p(y) + (+\infty)$$

(cf. ii).$\overline{\mathbb{Z}}_1$*).)*

Sinon, écrivons comme en b) $x = p^r \frac{n}{d}$ *et* $y = p^s \frac{m}{e}$ *avec* $r = v_p(x)$ *et* $s = v_p(y)$. *Alors* $xy = p^{r+s} \frac{nm}{de}$.

$$\left(p \not| n \text{ et } p \not| m \Rightarrow p \not| mn\right) \text{ et } \left(p \not| d \text{ et } p \not| e \Rightarrow p \not| ed\right)$$

d'après le lemme de GAUSS. *Il s'ensuit que*

$$v_p(xy) = r + s = v_p(x) + v_p(y) .$$

ii) ***(Somme)***

si $x = 0$ *ou* $y = 0$, *le résultat est immédiat. Sinon supposons* $v_p(x) \leq v_p(y)$ *et écrivons comme en b)* $x = p^r \frac{n}{d}$ *et* $y = p^s \frac{m}{e}$. *Il vient alors*

$$x + y = \frac{p^r ne + p^s md}{de} = p^r \frac{ne + p^{s-r} md}{de}$$

comme $p \not| de$,

$$v_p(x + y) \geq r = v_p(x) = \min(v_p(x), v_p(y)) .$$

si $r < s$,

$$p|p^{s-r} \Rightarrow p \not| ne + p^{r-s} md \Rightarrow v_p(x + y) = r = v_p(x) = \min(v_p(x), v_p(y)) .$$

Val$_6$) Est une conséquence presque immédiate des propriétés Val$_1$) à Val$_3$).

2) () **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 $P = 0$

$$\begin{aligned} V_p(P) &:= (+\infty) \\ \mathcal{S}(P) &:= \mathcal{P}\ . \end{aligned}$$

a) () 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.

Solution :

Val$[X]_1$)

$$\begin{aligned} &\forall P := \sum_{i=0}^{\delta} a_i X^i \in \mathbb{Q}[X], && P \in \mathbb{Z}[X] \\ \Leftrightarrow\ & && \forall 0 \leq i \leq \delta,\ a_i \in \mathbb{Z} \\ \Leftrightarrow\ & && \forall 0 \leq i \leq \delta,\ \forall p \in \mathcal{P},\ v_p(a_i) \geq 0 \\ \Leftrightarrow\ & && \forall p \in \mathcal{P},\ \min_{0 \leq i \leq \delta}(v_p(a_i)) \geq 0 \\ \Leftrightarrow\ & && \forall p \in \mathcal{P},\ V_p(P) \geq 0 \end{aligned}$$

en utilisant question 1), c).Val$_4$).

Val$[X]_2$)

$$\begin{aligned} &\forall P := \sum_{i=0}^{\delta} a_i X^i \in \mathbb{Q}[X] \setminus \{0\},\ \forall p \in \mathcal{P}, && V_p(P) \geq 0 \\ \Rightarrow\ & && \min_{0 \leq i \leq \delta}(v_p(a_i)) \geq 0 \\ \Rightarrow\ & && \exists 0 \leq i \leq \delta v_p(a_i) \geq 0 \\ \Rightarrow\ & && p \in \mathcal{S}(a_i) \end{aligned}$$

il s'ensuit que

$$\mathcal{S}(P) \subset \bigcup_{0 \leq i \leq \delta} \mathcal{S}(a_i)$$

qui est donc 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

$$R := PQ = \sum_{i=0}^{\deg(R)} c_i X^i\ .$$

b) () Écrire $\{c_i\}_{0\leq i\leq \deg(R)}$ en fonction des

$$\{a_i\}_{0\leq i\leq \deg(P)} \text{ et } \{b_i\}_{0\leq i\leq \deg(Q)} .$$

Solution :

$$\forall 0 \leq k \leq \deg(R),\ c_k \ = \sum_{i+j=k i(i,j)\in\mathbb{N}\times\mathbb{N}} a_i b_j . \qquad 1$$

c) () En déduire que :

$$\begin{array}{lll} \forall 0 \leq k \leq \deg(R),\ \forall 0 \leq i \leq \deg(P),\ \forall 0 \leq j \leq \deg(Q), & i+j & = & k \\ \Rightarrow & v_p(c_k) & \geq & v_p(a_i) + v_p(b_j) \\ & & \geq & V_p(P) + V_p(Q) . \end{array}$$

Solution : *Découle de b).1 et question 1), c).Val$_5$).*

d) () 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

$$v_p(c_{m+n}) \ = \ V_p(P) \ + \ V_p(Q) .$$

Solution :

i) Par définition $V_p(P) \ = \ \min_{0\leq i\deg(P)}(v_p(a_i))$. Il existe donc $0 \leq i \leq \deg(P)$, tel que $v_p(a_i) \ = \ V_p(P)$ puisque $[0;\deg(P)] \subset \mathbb{N}$ est un ensemble fini. Par conséquent $\{i \ \in \ [0;\deg(P)] \ ; \ v_p(a_i) \ = \ V_p(P)\}$ est une partie finie non vide de $\mathbb{N}$ qui possède donc un plus grand élément m.

ii) on a, en vertu de b).1 :

$$\begin{aligned} c_{m+n} \ &= \ \sum_{i+j=m+n} a_k b_j \\ &= \ \sum_{i=0}^{m-1} a_i b_{m+n-i} + a_m b_n + \sum_{i=m+1}^{mm+n} a_i b_{m+n-i} \\ &= \ a_m b_n + \sum_{j=n+1}^{m+n} a_{m+n-j} b_j \sum_{i=m+1}^{m+n} a_i b_{m+n-i} . \end{aligned}$$

Posons alors $B \ := \ \sum_{j=n+1}^{m+n} a_{m+n-j} b_j$ et $A \ := \ \sum_{i=m+1}^{m+n} a_i b_{m+n-i}$. Il découle alors de question 1), c).Val$_5$) que

$$v_p(A) > v_p(a_m) + V_p(Q) \ = \ V_p(P) \ + \ V_p(Q) \text{ et } v_p(B) > v_p(b_n) + V_p(P) \ = \ V_p(Q) \ + \ V_p(P) .$$

On a alors

$$V_p(R) \ \leq \ v_p(c_{m+n}) \ = \ v_p(a_m b_n + A + B) \ = \ v_p(a_m b_n) \ = \ V_p(P) \ + \ V_p(Q)$$

en utilisant encore question 1), c).Val$_5$).

e) () Établir finalement que

$$\forall (P,Q) \in \left(\mathbb{Q}[X] \setminus \{0\}\right)^2,\ \forall p \in \mathbb{P},\ V_p(PQ) \ = \ V_p(P) \ + \ V_p(Q)\ .$$

Solution : *L'égalité*

$$V_p(R) \ = \ V_p(P) \ + \ V_p(Q)$$

résulte alors de la minoration donnée en d) et de la majoration donnée en c).

3) () **(Irréductibilité des polynômes à coefficients entiers)**
Soit $P \in \mathbb{Z}[X] \setminus \{0\}$. **On suppose qu'il existe**

$$(Q,R) \ \in \ \left(\mathbb{Q}[X] \setminus \mathbb{Q}\right)^2 \mid P \ = \ QR\ .$$

a) () 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

$$V_p(aR) \ \geq \ 0 \text{ et } V_p(\frac{1}{a}Q) \ \geq \ 0\ .$$

Solution : *Il résulte de question 2), a).Val*$[X]_1$*), que* $0 \ \leq \ V_p(P)$ *et de question 2), e) que :*

$$V_p(Q) \ + \ V_p(R) \ = \ V_p(QR) \ = \ V_p(P) \ \geq \ 0\ . \qquad (1)$$

$*$*) Si* $V_p(Q) \geq 0$ *et* $V_p(R) \geq 0$, $a \ = \ 1$ *convient.*

†*) Si* $r \ := \ V_p(Q) \ < \ 0$, *il découle que 1 que* $V_p(R) > r$. *En prenant alors* $a \ := \ p^r$ *on se trouve dans la situation i).*

‡*) Sinon on est dans la situation ii).*

b) () En déduire qu'il existe

$$(Q_1,R_1) \ \in \ \left(\mathbb{Z}[X] \setminus \{-1;1\}\right)^2 \mid P \ = \ R_1Q_1\ .$$

Solution : *Il résulte de la question précédente que, pour tout* $p \in S(Q) \cup S(R)$ *il existe* $a_p \in \mathbb{Q}$ *tel que* $V_p(a_pQ) \ \geq \ 0$ *et* $V_p(\frac{1}{a_p}R) \ \geq \ 0$. *Posons*

$$Q_1 \ := \ \prod_{p \in S(Q) \cup S(R)} a_pQ \text{ et } R_1 \ := \ \frac{1}{\prod\limits_{p \in S(Q) \cup S(R)} a_p}R\ .$$

Il découle alors de question 2), a).Val$[X]_1$*) que* $Q_1 \in \mathbb{Z}[X]$ *et* $R_1 \in \mathbb{Z}[X]$ *et de leur construction même que* $P \ = \ Q_1R_1$.

c) () 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 $\mathbb{Q}[X]$.

Solution : *Il est clair que si on peut factoriser un polynôme dans $\mathbb{Z}[X]$, on obtient également une factorisation dans $\mathbb{Q}[X]$. Nous venons de montrer que la réciproque est vraie ce qui établit le résultat.*

4) () **(Le critère d'Eisenstein)**

Pour $p \in \mathcal{P}$ un nombre premier, on note $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, *)$ le corps à p éléments et pour tout $a \in \mathbb{Z}$, $\overline{a}$ sa classe dans $\mathbb{F}_p$.

Pour $P := \sum_{i=0}^{\deg(P)} a_i X^i \in \mathbb{Z}[X]$, on pose $\overline{P} := \sum_{i=0}^{\deg(P)} \overline{a}_i X^i \in \mathbb{F}_p[X]$.

On dit que P vérifie † si :

$$\dagger \ : \ a_{\deg(P)} = 1 \ ; \ v_p(a_0) = 1 \text{ et } v_p(a_i) > 0 \ , \ \forall 1 \leq i < \deg(P) \ .$$

a) () Pour $a \in \mathbb{Z}$, exprimer la condition $\overline{a} = 0$ à l'aide de $v_p(\cdot)$.

Solution :

$$\forall a \in \mathbb{Z}, \ \overline{a} = 0 \Leftrightarrow p|a \Leftrightarrow v_p(a) > 0 \ .$$

b) () Rappeler pourquoi

$$\forall P \in \mathbb{Z}[X], \ \forall Q \in \mathbb{Z}[X], \ \overline{P+Q} = \overline{P} + \overline{Q} \text{ et } \overline{P * Q} = \overline{P} * \overline{Q} \ .$$

Solution : *On peut tout à fait démontrer ces résultats en écrivant $P = \sum_{i=0}^{\deg(P)} a_i X^i$, $Q = \sum_{i=0}^{\deg(Q)} b_i X^i$ et calculer en utilisant la compatibilité des relations de congruence à la somme et au produit c'est-à-dire en fait que la surjection canonique $\pi_p : \mathbb{Z} \to \mathbb{F}_p$ est un morphisme d'anneaux*

On peut aussi profiter du fait que π_p est un morphisme d'anneaux pour appliquer le résultat III.1.18 donnant l'existence d'un morphisme $\pi_p[X] : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ tel que $\pi_p[X](X) = X$, et $\pi_p(a) = \overline{a} = \pi_p(a)$ pour tout $a \in \mathbb{Z}$. La relation III.1.18.1 assure précisément que $\forall P \in \mathbb{Z}[X], \ \overline{P} = \pi_p[X](P)$ (ce qui a d'ailleurs été établi avec plus de détails en III.1.19.d))Le fait que $\pi_p[X]$ est un morphisme d'anneaux donne alors exactement les formules demandées.

c) () Montrer que pour tout $P \in \mathbb{Z}[X]$, tout $Q \in \mathbb{Z}[X]$, P vérifie † et $Q|P$ entraîne $\overline{Q} = \pm X^{\deg(Q)}$.

Solution : *Si $Q|P$ il existe $R \in \mathbb{Z}[X]$ tel que $P = Q * R$. Or d'après b) $\overline{P} = \overline{Q} * \overline{R}$ c'est-à-dire que $\overline{Q}|\overline{P}$. Or d'après a), si P vérifie †, $\overline{P} = X^{\deg(P)}$. On a donc*

$\overline{Q} * \overline{R} = X^{\deg(P)}$. Or $\deg(X) = 1$ entraîne X irréductible (cf. III.2.13.) On peut allors utiliser l'unicité dans la proposition III.2.17 pour assurer qu'il existe des entiers a et b avec $a + b = \deg(P)$ tels que $\overline{Q} = X^a$ et $\overline{R} = X^b$.

En écrivant enfin $P = Q * R$ dans $\mathbb{Z}[X]$, (avec $Q = \sum_{i=0}^{\deg(Q)} b_i X^i$ et $R = \sum_{i=0}^{\deg(R)} c_i X^i$,) on a en particulier $a_{\deg(P)} = b_{\deg(Q)} c_{\deg(R)}$ ce qui entraîne, si P vérifie †, que $b_{\deg(Q)}$ est inversible i.e. vaut ± 1 et donc que $\overline{b}_{\deg(Q)} = \pm 1$. Il en résulte finalement que

$$\deg(\overline{Q}) = \deg(Q) \text{ et } \overline{Q} = X^{\deg(Q)} = X^{\deg(\overline{Q})} \ .$$

d) () Pour tout

$$P \in \mathbb{Z}[X]\ ,\ Q\ :=\ \sum_{i=0}^{\deg(Q)} b_i X^i \in \mathbb{Z}[X]\ ,\ R\ :=\ \sum_{i=0}^{\deg(R)} c_i X^i \in \mathbb{Z}[x],$$

montrer que $P\ =\ Q * R$, P satisfait †, $\deg(Q) > 0, \deg(R) > 0$ entraîne $v_p(b_0)\ >\ 0$ et $v_p(c_0)\ >\ 0$.

Solution : *D'après c)* $P\ =\ Q * R$ *et* P *satisfait* † *entraîne* $\overline{Q}\ =\ X^{\deg(Q)}$ *et* $\overline{R}^{\deg(R)}$. *Ceci entraîne d'après a),*

$$\forall 0 \leq i \leq \deg(Q) - 1,\ v_p(b_i) > 0 \text{ et } \forall 0 \leq i \leq \deg(R) - 1,\ v_p(c_i) > 0\ .$$

Ceci entraîne bien entendu si $\deg(Q) > 0$ *et* $\deg(R) > 0$,

$$v_p(b_0)\ >\ 0 \text{ et } v_p(c_0)\ >\ 0\ .$$

e) () Déduire de ce qui précède que pour $P\ \in\ \mathbb{Z}[X]$, P vérifie † entraîne P est irréductible.

Solution : *Il résulte de d) que* $P\ =\ Q * R$, P *satisfait* †, $\deg(Q) > 0, \deg(R) > 0$, *entraîne* $v_p(b_0) > 0$ *et* $v_p(c_0) > 0$. *On a alors*

$$v_p(a_0)\ =\ v_p(b_0 * c_0)\ =\ v_p(b_0)\ +\ v_p(c_0)\ >\ 1$$

(cf. question 1), c).Val_5*).) Le fait que* P *satisfait* † *entraîne donc, par contraposée, que*

$$\deg(Q)\ =\ 0 \text{ ou } \deg(R)\ =\ 0\ \Rightarrow\ \big(\deg(Q)\ =\ 0 \text{ et } b_0 | a_{\deg(P)}\ \big) \text{ ou } \big(\deg(R)\ =\ 0 \text{ et } c_0 | a_{\deg(P)}\ \big)$$

c'est-à-dire, comme $a_{\deg(P)}\ =\ 1$, *que* Q *ou* r *est inversible, donc que* P *est irréductible.*

f) () Montrer finalement qu'il existe des polynômes irréductibles de tout degré dans $\mathbb{Q}[X]$.

Solution : *Il résulte de e) que pour tout nombre premier* $p\ \in\ \mathcal{P}$ *et tout entier* $n\ \in\ \mathbb{N}^*$, *le polynôme* $X^n - p \in \mathbb{Z}[X]$ *est irréductible. Or il résulte de la question 3), c) que ce polynôme est alors irréductible dans* $\mathbb{Q}[X]$.

Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

Examen du 16 juin 2015
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 : () I. –

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) ()

$$15x - 21y = 41 .$$

b) ()

$$38x - 105y = 1 .$$

2) () **(Systèmes de congruences)**
Déterminer l'ensemble des entiers relatifs x satisfaisant

$$\mathcal{S} : \left\{ \begin{array}{rcl} 13x & \equiv & 1\,[38] \\ x & \equiv & 2\,[15] \\ x & \equiv & 14\,[21] \end{array} \right\} .$$

Indication : *On pourra chercher à résoudre d'abord*

$$\left\{ \begin{array}{rcl} x & \equiv & 2\,[15] \\ x & \equiv & 14\,[21] \end{array} \right\}$$

II. –
Soient a et b deux entiers naturels non nuls. On note d (resp. m) leur pgcd (resp. ppcm.)

1) () Rappeler la relation liant a, b, cd et m.

2) () **On note $G := \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ le groupe abélien**

$$G := \{(x, y) \ , \ x \in \mathbb{Z}/a\mathbb{Z} y \in \mathbb{Z}/b\mathbb{Z}\}$$

muni de la loi d'addition donnée par

$$(x, y) + (z, t) := (x + z, y + t) .$$

On note

$$f : \mathbb{Z} \to G \ , \ x \mapsto (x \bmod a, x \bmod b)$$

et

$$g : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \ , \ x \mapsto x \bmod m .$$

a) () Rappeler rapidment pourquoi f et g sont des morphismes de groupes.

b) () Déterminer le noyau de f.

c) () En déduire qu'il existe un unique morphisme injectif

$$i \,:\, \mathbb{Z}/m\mathbb{Z} \,\to\, G \text{ tel que } i \,\circ\, g \,=\, f\ .$$

d) () Déterminer l'image $\mathrm{Im}\, i$ de i. En quoi cela aurait-il pu servir à la résolution de I.question 2) ?

Exercice B : () **1)** () Étant donnés deux entiers relatifs a et b premiers entre eux, montrer que le PGCD de $5a + 2b$ et $2a + 3b$ est soit 1 soit 11.

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 : () **0)** () **Soit G un groupe.**

a) () Pour $x \,\in\, G$ rappeler ce que signifie que $y \,\in\, G$ est conjugué à x (dans G).

b) () Rappeler ce que signifie que la relation « être conjugué à » est une relation déquivalence et le justifier rapidement. En quoi cela justifie-t-il qu'on dise « x et y sont conjugués (dans G) » plutôt que « y est conjugué a x (dans G). » On rappelle que les classes d'équivalence pour cette relation s'appellent *classes de conjugaison*.

c) () Étant donné un sous-groupe H de G, montrer que si H est distingué, pour tout $x \,\in\, H$ la classe de conjugaison de x dans G est contenue dans H.

Dans la suite, n est un entier naturel supérieur ou égal à 5.

1) () **a)** () Pour tout quadruplet (a, b, c, d) d'éléments deux à deux distincts de $[1; n]$, calculer les permutations

$$(a\, b)(b\, c) \text{ et } (a\, b\, c)(b\, c\, d)$$

appartenant à $\mathcal{S}_n$.

b) () Pour tout $s \,\in\, \mathcal{A}_n$, montrer qu'il existe un entier $\delta \geq 1$ et des transpositions $t_{i\ ,1\leq i\leq 2\delta} \,\in\, \mathcal{S}_n$ tels que

$$s \,=\, \prod_{i=1}^{\delta} t_{2i-1}t_{2i}$$

(la notation produit ne signifiant pas produit commutatif.)

c) () En déduire que $\mathcal{A}_n$ est engendré par les 3-cycles.

d) () Montrer que $\mathcal{A}_n$ est engendré par les éléments de la forme $(a\, b)(c\, d)$ pour (a, b, c, d) un quadruplet comme en a).
Indication : *On pourra penser à calculer $(x\, y)(z\, t)(z\, t)(y\, u)$ pour 5 éléments x, y, z, t, u de $[1; n]$ convenablement choisis.*

2) () Quels sont les ordres possibles pour un élément de $\mathcal{A}_5$? Donner le type cyclique (une décomposition en cycles à supports deux à deux disjoints) pour chaque ordre.

3) () **a)** () Montrer que tous les 3-cycles sont conjugués dans $\mathcal{A}_5$.

b) () Étant donnés deux éléments $(a\,b)(c\,d)$ et $(a',b')(c',d')$ de $\mathcal{S}_5$ où (a,b,c,d) et (a',b',c',d') sont des quadruplets comme à la question 1), a), montrer que $(a\,b)(c\,d)$ et $(a',b')(c',d')$ sont des éléments de $\mathcal{A}_5$ conjugués dans $\mathcal{A}_5$.

c) () Montrer que $\mathcal{A}_5$ ne contient pas de sous-groupe distingué de cardinal $2, 4, 6$ ou 12.

4) () **Soit** $c \in \mathcal{S}_5$ **d'ordre** 5.

a) () Montrer que $c \in \mathcal{A}_5$ et qu'il existe $s \in \mathcal{S}_4$ tel que $c = (s(1)\,s(2)\,s(3)\,s(4)\,5)$.

b) () En déduire le nombre d'éléments d'ordre 5 dans $\mathcal{A}_5$.

c) () Montrer qu'il y a une partition de l'ensemble des éléments d'ordre 5 de $\mathcal{A}_5$ en deux classes de conjugaison, dans $\mathcal{A}_5$, de même cardinal.

5) () **a)** () Montrer qu'il n'y a pas de sous-groupe distingué de cardinal $5, 10, 15, 20$ ou 30 dans $\mathcal{A}_5$.

b) () En déduire finalement que $\mathcal{A}_5$ ne possède pas d'autre sous-groupe distingué que $\{\mathrm{Id}\}$ et lui-même.

Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

Corrigé de l'examen du 16 juin 2015

Exercice A : () I. –

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) ()

$$15x - 21y \ = \ 41 \ .$$

Solution : *L'algorithme d'Euclide pour* 15 *et* 21 *s'écrit :*

$$\begin{array}{ccc} 15 & 1 & 0 \\ 21 & 0 & 1 \\ 39 & 1 & -2 \\ 3 & -2 & 5 \end{array}$$

c'est-à-dire que $15 \wedge 21 \ = \ 3$. *Il en résultera que pour tout couple* (x, y) *d'entiers relatifs,* $3 \mid 15x - 21y$. *Or* 3 *ne divisant pas* 41, *l'équation n'a pas de solution entière.*

b) ()

$$38x \ - \ 105y \ = \ 1 \ .$$

Solution : *L'algorithme d'Euclide pour* 38 *et* 105 *s'écrit :*

$$\begin{array}{ccccc} & 38 & 1 & 0 \\ & 105 & 0 & 1 \\ 1 & 619 & 1 & -1 \\ 2 & 309 & -2 & 3 \\ 2 & 1 & 5 & -7 \ . \end{array}$$

Il en résulte que $(5, 7)$ *est une solution de l'équation*

$$38x \ - \ 105y \ = \ 1$$

ce qui prouve en outre (cf. cours I.3.3.3,) que 38 *et* 105 *sont premiers entre eux. L'ensemble des couples d'entiers relatifs solution de l'équation ci-dessus est donc*

$$\{(5 + 105k, 7 + 38k) \ , \ k \in \mathbb{Z}\} \ .$$

De plus $(5 + 105k, 7 + 38k) \in \mathbb{N} \times \mathbb{N}$ *si et seulement si* $k \geq 0$.

2) () **(Systèmes de congruences)**

Déterminer l'ensemble des entiers relatifs x satisfaisant

$$\mathcal{S} \ : \ \left\{ \begin{array}{rcl} 13x & \equiv & 1\,[38] \\ x & \equiv & 2\,[15] \\ x & \equiv & 14\,[21] \end{array} \right\} .$$

Indication : *On pourra chercher à résoudre d'abord*

$$\left\{ \begin{array}{rcl} x & \equiv & 2\,[15] \\ x & \equiv & 14\,[21] \end{array} \right\}$$

Solution :

i) Commençons par considérer le système :

$$\mathcal{S}_1 \ : \ \left\{ \begin{array}{rcl} x & \equiv & 2\,[15] \\ x & \equiv & 14\,[21] \end{array} \right\} .$$

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 $15 \wedge 21 \ = \ 13 \ \neq \ 1$. *On a cependant :*

$$\begin{array}{rcl} \mathcal{S}_1 & \leftrightarrow & \exists (r,s) \ \in \ \mathbb{Z} \times \mathbb{Z}, \\ & & \left\{ \begin{array}{rcl} x & = & 2+15r \\ x & = & 14+21s \end{array} \right\} \\ & \leftrightarrow & \left\{ \begin{array}{rcl} x & = & 2+15r \\ 15r-21s & = & 52 \end{array} \right\} \\ & \leftrightarrow & \left\{ \begin{array}{rcl} x & = & 2+15r \\ 17r-7s & = & 4 \end{array} \right\} . \end{array}$$

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 :*

$$\begin{array}{rcl} \mathcal{S}_1 & \Leftrightarrow & \left\{ \begin{array}{rcl} x & = & 2+15(-1+7k) \\ x & = & 14+91(-3+17k) \end{array} \right\} \\ & \leftrightarrow & \left\{ \begin{array}{rcl} x & = & -215+105k \\ x & = & -215+105k \end{array} \right\} \\ & \leftrightarrow & x \ = \ -215+105k \\ & \leftrightarrow & x \ \equiv \ -215\,[105] \, . \end{array}$$

Le système $\mathcal{S}$ *équivaut alors au système*

$$\mathcal{S}_2 \ \Leftrightarrow \ \left\{ \begin{array}{rcl} 13x & \equiv & 1\,[38] \\ x & \equiv & -215\,[105] \end{array} \right\} .$$

ii) L'algorithme d'Euclide pour 38 *et* 13 *s'écrit :*

$$\begin{array}{rrrr} & 38 & 1 & 0 \\ & 13 & 0 & 1 \\ 166 & 8 & 1 & -166 \\ 1 & 5 & -1 & 167 \\ 1 & 3 & 2 & -333 \\ 1 & 2 & -3 & 500 \\ 1 & 1 & 5 & -833 \end{array} \ .$$

D'où il découle que l'inverse de 13 *modulo* 38 *est* $-833 = 1333$.

Le système $\mathcal{S}$ *est donc équivalent au système*

$$\mathcal{S} \ : \ \left\{ \begin{array}{rcl} x & \equiv & 1333\,[38] \\ x & \equiv & 1332\,[105] \end{array} \right\} .$$

iii) Or nous avons montré à la question 1), b) que 38 *et* 105 *sont premiers entre eux. Il en résulte (cf. cours I.3.6.3,) que l'ensemble des solutions du système* $\mathcal{S}''$ *est une classe d'entiers modulo* $38 * 105$. *Or si* $x \in \mathbb{Z}$ *est solution du système* $\mathcal{S}''$, *il existe des entiers relatifs* r *et* s *tels que*

$$\begin{aligned} x &= 1333 + 38r \\ x &= 1332 + 105s \end{aligned}$$

ce qui implique que

$$38r - 105s = -1 .$$

En utilisant les résultats de la question 1), b), on obtient qu'il existe $k \in \mathbb{Z}$ *tel que*

$$\begin{aligned} r &= -5 + 105k \\ s &= -7 + 38k \end{aligned}$$

d'où il résulte que

$$x = 1333 + 38r = 1333 + 38(-5 + 105k) = -9497 + 3350802k .$$

II. –

Soient a **et** b **deux entiers naturels non nuls. On note** d **(resp.** m**) leur pgcd (resp. ppcm.)**

1) () Rappeler la relation liant a, b, cd et m.

Solution : *On a :*

$$ab = md .$$

2) () **On note** $G := \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ **le groupe abélien**

$$G := \{(x, y) , x \in \mathbb{Z}/a\mathbb{Z} y \in \mathbb{Z}/b\mathbb{Z}\}$$

muni de la loi d'addition donnée par

$$(x, y) + (z, t) := (x + z, y + t) .$$

On note

$$f : \mathbb{Z} \to G , x \mapsto (x \,\mathbf{mod}\, a, x \,\mathbf{mod}\, b)$$

et

$$g : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} , x \mapsto x \,\mathbf{mod}\, m .$$

a) () Rappeler rapidment pourquoi f et g sont des morphismes de groupes.

b) () Déterminer le noyau de f.

c) () En déduire qu'il existe un unique morphisme injectif

$$i : \mathbb{Z}/m\mathbb{Z} \to G \text{ tel que } i \circ g = f .$$

d) () Déterminer l'image $\mathrm{Im}\, i$ de i. En quoi cela aurait-il pu servir à la résolution de I.question 2) ?

Exercice B : () **1)** () Étant donnés deux entiers relatifs a et b premiers entre eux, montrer que le PGCD de $5a+2b$ et $2a+3b$ est soit 1 soit 11.

Solution : *Si on pose* $A := \begin{pmatrix}5 & 2\\ 2 & 3\end{pmatrix}$, $B := \begin{pmatrix}3 & -2\\ -2 & 5\end{pmatrix}$, *on a* $A*B = B*A = 11*\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$. *Or :*

$$\begin{array}{rcl} \begin{pmatrix}\alpha\\ \beta\end{pmatrix} & = & A*\begin{pmatrix}a\\ b\end{pmatrix} \\ \Rightarrow \quad B*\begin{pmatrix}\alpha\\ \beta\end{pmatrix} & = & B*A\begin{pmatrix}a\\ b\end{pmatrix} \\ & = & 11*\begin{pmatrix}a\\ b\end{pmatrix} \end{array}$$

ce qui sécrit encore :

$$11a = 3\alpha - 2\beta \text{ et } 11b = -2\alpha + 5\beta\ .$$

Si a *et* b *sont premiers entre eux, il existe un couple de coefficients de* BÉZOUT (u,v) *tel que :*

$$\begin{array}{rcl} 11 & = & 11a*u + 11b*v \\ & = & \alpha(3u-2v) + \beta(-2u+5v) \end{array}$$

si bien qu'il et clair que le PGCD de α *et* β *divise* 11 *qui est premier, si bien qu'il vaut* 1 *ou* 11.

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 :*

$$\begin{array}{rcl} \begin{pmatrix}u & v\end{pmatrix}*B*\begin{pmatrix}\alpha\\ \beta\end{pmatrix} & = & \begin{pmatrix}u & v\end{pmatrix}*B*A*\begin{pmatrix}a\\ b\end{pmatrix} \\ & = & \begin{pmatrix}u & v\end{pmatrix}*\delta*\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}*\begin{pmatrix}a\\ b\end{pmatrix} \\ & = & \delta*\begin{pmatrix}u & v\end{pmatrix}*\begin{pmatrix}a\\ b\end{pmatrix} \\ & = & d\delta \end{array}$$

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 : () **0)** () **Soit** G **un groupe.**

a) () Pour $x \in G$ rappeler ce que signifie que $y \in G$ est conjugué à x (dans G).
Solution : *On dit que* y *est conjugué à* x *s'il existe* $z \in G$ *tel que* $y = z*x*z^{-1}$.

b) () Rappeler ce que signifie que la relation « être conjugué à » est une relation déquivalence et le justifier rapidement. En quoi cela justifie-t-il qu'on dise « x et y sont conjugués (dans G) » plutôt que « y est conjugué a x (dans G). » On rappelle que les classes d'équivalence pour cette relation s'appellent *classes de conjugaison*.
Solution : *On conviendra que* e *désigne l'élément neutre de* G.

i) ***(Réflexivité)***
Pour tout $x \in G$, $x = e*x*e^{-1}$ *si bien que* x *et conjugué à* x *et que la relation est réflexive.*

*ii) (**Symétrie**)*

Si y est conjugué à x il existe $z \in G$ tel que

$$y = z * x * z^{-1} \Rightarrow x = z^{|1} * y * z$$

c'est-à-dire que x est conjugué à y et que la relation est donc symétrique. On dira donc tout simplement que x et y sont conjugués.

*iii) (**Transitivité**)*

Pour x, y, z des éléments de G, x et y (resp. y et z) sont conjugués si et seulement s'il existe u et v dans G tels que

$$y = u * x * u^{-1} \text{ et } z = v * y * v^{-1} \Rightarrow z = v * u * y * u^{-1} * v^{-1} = (v * u) * y * (v * u)^{-1}$$

c'est-à-dire que x et z sont conjugués et que la relation de conjugaison est donc transitive.

Les points précédents assurent que la relation de conjugaison est une relation d'équivalence.

c) () Étant donné un sous-groupe H de G, montrer que si H est distingué, pour tout $x \in H$ la classe de conjugaison de x dans G est contenue dans H.

Dans la suite, n est un entier naturel supérieur ou égal à 5.

1) () **a)** () Pour tout quadruplet (a, b, c, d) d'éléments deux à deux distincts de $[1; n]$, calculer les permutations

$$(a\,b)(b\,c) \text{ et } (a\,b\,c)(b\,c\,d)$$

appartenant à $\mathcal{S}_n$.

Solution : *Pour $n \geq 5$, et (a, b, c, d) un quadruplet d'éléments de $[1; n]$ deux à deux distincts, on a :*

$$\begin{aligned}(a\,b)(b\,c)(a) &= b\\ (a\,b)(b\,c)(b) &= c\\ (a\,b)(b\,c)(c) &= a\end{aligned}$$

et pour tout $x \notin \{a, b, c\}$, $(a\,b)(b\,c)(x) = x$ c'est-à-dire que $(a\,b)(b\,c)$ est le 3-cycle $(a\,b\,c)$.

En outre, on a :

$$\begin{aligned}(a\,b\,c)(b\,c\,d)(a) &= b\\ (a\,b\,c)(b\,c\,d)(b) &= a\\ (a\,b\,c)(b\,c\,d)(c) &= d\\ (a\,b\,c)(b\,c\,d)(d) &= c\end{aligned}$$

et pour tout $x \notin \{a, b, c, d\}$, $(a\,b\,c)(b\,c\,d)(x) = x$ c'est-à-dire que $(a\,b\,c)(b\,c\,d)$ est le produit de deux transpositions disjointes $(a\,b)(c\,d)$.

b) () Pour tout $s \in \mathcal{A}_n$, montrer qu'il existe un entier $\delta \geq 1$ et des transpositions $t_{i\,,1\leq i\leq 2\delta} \in \mathcal{S}_n$ tels que

$$s = \prod_{i=1}^{\delta} t_{2i-1} t_{2i}$$

(la notation produit ne signifiant pas produit commutatif.)

Solution : *Pour tout $s \in \mathcal{S}_n$, on sait (cf. cours II.2.3.3) qu'il existe un entier $\epsilon \geq 1$ et des transpositions $t_{i\,,1\leq i\leq \epsilon}$ telles que*

$$s = \prod_{i=1}^{\epsilon} t_i\ .$$

Or la signature $\sigma : \mathcal{S}_n \to \{-1, 1\}$ est un morphisme de groupes (cf. cours II.2.4.4,) et pour toute transposition $t \in \mathcal{S}_n$, $\sigma(t) = -1$. Par conséquent, $s \in \mathcal{A}_n$ équivalant à $\sigma(s) = 1$, ϵ est nécessairement pair et l'on peut poser $\epsilon := 2\delta$; ce qui répond à la question.

c) () En déduire que $\mathcal{A}_n$ est engendré par les 3-cycles.

Solution : *Écrivons, pour tout* $s \in \mathcal{A}_n$,

$$s := \prod_{i=1}^{\delta} t_{2i-1}t_{2i}$$

grâce à la question précédente.

Pour tout $1 \leq i \leq \delta$

— *soit* $t_{2i} = t_{2i-1}$ *auquel cas* $t_{2i-1}t_{2i} = \mathrm{Id}$;

— *soit il existe trois éléments deux à deux distincts* a, b, c *dans* $[1; n]$ *tels que* $t_{2i-1} = (a\,b)$ *et* $t_{2i} = (b\,c)$ *et dans ce cas*

$$t_{2i-1}t_{2i} = (a\,b)(b\,c) = (a\,b\,c)\,;$$

— *soit il existe quatre éléments deux à deux distincts* a, b, c, d *tels que* $t_{2i-1} = (a\,b)$ *et* $t_{2i} = (c\,d)$ *alors*

$$t_{2i-1}t_{2i} = (a\,b)(c\,d) = (a\,b\,c)(b\,c\,d)\,.$$

On a ainsi répondu à la question.

d) () Montrer que $\mathcal{A}_n$ est engendré par les éléments de la forme $(a\,b)(c\,d)$ pour (a, b, c, d) un quadruplet comme en a).

Indication : *On pourra penser à calculer* $(x\,y)(z\,t)(z\,t)(y\,u)$ *pour* 5 *éléments* x, y, z, t, u *de* $[1; n]$ *convenablement choisis.*

Solution : *Dans le raisonnement de la question précédente, il convient juste de réexaminer le deuxième point. En effet si* $t_{2i-1} = (a\,b)$ *et* $t_{2i} = (b\,c)$, *comme* $n \geq 5$, *il existe des éléments* d *et* e *distincts et n'appartenant pas à* $\{a, b, c\}$. *On peut dès lors écrire*

$$t_{2i-1}t_{2i} = (a\,b)(b\,c) = (a\,b)(d\,e)(d\,e)(b\,c)$$

ce qui répond à la question.

2) () Quels sont les ordres possibles pour un élément de $\mathcal{A}_5$? Donner le type cyclique (une décomposition en cycles à supports deux à deux disjoints) pour chaque ordre.

Solution : *Notons* $\{a, b, c, d, e\} = [1; 5]$. *On peut répartir les éléments de* $\mathcal{S}_5$ *en fonction de leur type cyclique (cf. cours II.2.3.4.) Cette partition correspondant à la partition en classes de conjugaisons dans* $\mathcal{S}_5$ *(cf. cours II.2.3.5.) On résume cette partition dans le tableau suivant en donnant en plus l'ordre des éléments (invariant par conjugaison) et en indiquant s'ils appartiennent à* $\mathcal{A}_5$:

type cyclique	*ordre*	$\in \mathcal{A}_5$
$(a\,b)$	2	$\notin \mathcal{A}_5$
$(a\,b)(c\,d)$	2	$\in \mathcal{A}_5$
$(a\,b\,c)$	3	$\in \mathcal{A}_5$
$(a\,b\,c)(d\,e)$	6	$\notin \mathcal{A}_5$
(a, b, c, d)	4	$\notin \mathcal{A}_5$
(a, b, c, d, e)	5	$\in \mathcal{A}_5$.

En résumé, les ordres possibles pour les éléments de $\mathcal{A}_5$ *sont* $2, 3$ *ou* 5.

D'après le tableau précédent, les éléments d'ordre 2 *(resp.* 3,*) (resp.* 5*) sont les éléments de la forme* $(a\,b)(c\,d)$ *(resp.* $(a\,b\,c)$,*) (resp.* (a, b, c, d, e).*)*

3) () **a)** () Montrer que tous les 3-cycles sont conjugués dans $\mathcal{A}_5$.

Solution : *Pour deux* 3*-cycles* $(a\,b\,c)$ *et* (a',b',c') *de* $\mathcal{A}_5$*, on sait (cf. cours II.2.2.4,) qu'il existe* $s \in \mathcal{S}_5$ *tel que*

$$(a',b',c') \;=\; s\circ(a\,b\,c)\circ s^{-1}\,.$$

Si $s \in \mathcal{A}_5$*, on a répondu à la question. Sinon il existe deux éléments distincts* d *et* e *n'appartenant pas à* $\{a,b,c\}$*. Il en résulte que*

$$(a\,b\,c)(d\,e) \;=\; (d\,e)(a\,b\,c)\,.$$

Il s'ensuit que :

$$\begin{aligned} s\circ(d\,e)\circ(a\,b\,c)\circ(s\circ(d\,e))^{-1} &= s\circ(d\,e)\circ(a\,b\,c)\circ(d\,e)\circ s^{-1}\\ &= s\circ(d\,e)^2\circ(a\,b\,c)\circ s^{-1}\\ &= s\circ(a\,b\,c)\circ s^{-1}\\ &= (a',b',c')\,. \end{aligned}$$

Or $s\circ(d\,e)\in\mathcal{A}_5$.

b) () Étant donnés deux éléments $(a\,b)(c\,d)$ et $(a',b')(c',d')$ de $\mathcal{S}_5$ où (a,b,c,d) et (a',b',c',d') sont des quadruplets comme à la question 1), a), montrer que $(a\,b)(c\,d)$ et $(a',b')(c',d')$ sont des éléments de $\mathcal{A}_5$ conjugués dans $\mathcal{A}_5$.

Solution : *Pour tout quadruplet* (a,b,c,d) *d'éléments deux à deux distincts,*

$$\sigma((a\,b)(c\,d)) \;=\; \sigma((a\,b))\sigma((c\,d)) \;=\; 1$$

c'est-à-dire que $(a\,b)(c\,d)\in\mathcal{A}_5$.

Par ailleurs pour deux tels éléments $(a\,b)(c\,d)$ *et* $(a',b')(c',d')$ *on sait (cf. cours II.2.3.5,) qu'il existe* $s \in \mathcal{S}_5$ *tel que*

$$(a',b')(c',d') \;=\; s\circ(a\,b)(c\,d)\circ s^{-1}\,.$$

Si $s \in \mathcal{A}_5$*, on a répondu à la question sinon*

$$\begin{aligned} s\circ(a\,b)\circ(a\,b)(c\,d)\circ(s\circ(a\,b))^{-1} &= s\circ(a\,b)^2\circ(c\,d)\circ(a\,b)\circ s^{-1}\\ &= s\circ(a\,b)(c\,d)\circ s^{-1}\\ &= (a',b')(c',d')\,. \end{aligned}$$

Or $s\circ(a\,b)\in\mathcal{A}_5$*, ce qui répond à la question.*

c) () Montrer que $\mathcal{A}_5$ ne contient pas de sous-groupe distingué de cardinal $2, 4, 6$ ou 12.

Solution :

*i) (**Cardinal** 2 **ou** 4)*

Un sous-groupe distingué H *de* $\mathcal{A}_5$ *de cardinal* 2 *ou* 4 *contient nécessairement un élément d'ordre* 2 *c'est-à-dire un élément de la forme* $(a\,b)(c\,d)$ *(cf. question 2).) Or ces éléments étant tous conjugués dans* $\mathcal{A}_5$ *(cf. b),) et* H *étant distingué il les contient tous. Ces éléments engendrant* $\mathcal{A}_5$ *(cf. question 1), d),)* H *contient nécessairement* $\mathcal{A}_5$ *ce qui est contradictoire puisque* $\#(\mathcal{A}_5) \;=\; \dfrac{5!}{2} \;=\; 60.$

*ii) (**Cardinal** 6 **ou** 12)*

Si H *est un sous-groupe de* $\mathcal{A}_5$ *de cardinal* 6 *ou* 12*, soit il contient au moins un élément d'ordre* 2 *et l'on est ramené au cas précédent, soit tous ses éléments différents de* Id *sont d'ordre* 3 *c'est-à-dire de la forme* $(a\,b\,c)$ *(cf. question 2).) Mais ces éléments étant tous conjugués dans* $\mathcal{A}_5$ *(cf. a),) et* H *étant distingué il les contient tous. Or ils engendrent* $\mathcal{A}_5$ *(cf. question 1), c),) et il en résulte donc la même contradiction que ci-dessus.*

4) () **Soit** $c \in \mathcal{S}_5$ **d'ordre** 5.

a) () Montrer que $c \in \mathcal{A}_5$ et qu'il existe $s \in \mathcal{S}_4$ tel que $c = (s(1)\, s(2)\, s(3)\, s(4)\, 5)$.

Solution : *Si l'on note* $\{a, b, c, d, e\} := [1; 5]$, *on a vu à la question 2) qu'un élément* c *d'ordre* 5 *est un* 5*-cycle de la forme* (a, b, c, d, e) *et qu'il est dans* $\mathcal{A}_5$.

Pour tout tel 5*-cycle* c, $5 \in [1; 5]$ *n'est pas un point fixe, et par conséquent,* $c(5) \in [1; 4]$. *Posons alors* $s(1) := c(5)$. *Puisque* c *est un* 5*-cycle,* $c(s(1)) = c^2(5) \notin \{5, s(1)\}$. *Posons alors* $s(2) := c^2(5)$ *et de même* $s(3) := c^3(5)$ *et* $s(4) := c^4(5)$. *Alors*

$$c = (5, s(1), s(2), s(3, s(4)) = (s(1), s(2), s(3), s(4), 5) .$$

Il est clair qu'alors $s \in \mathcal{S}_4$ *et que, réciproquement, à tout élément* $s \in \mathcal{S}_4$, *on associe un* 5*-cycle*

$$(s(1), s(2), s(3), s(4), 5) .$$

b) () En déduire le nombre d'éléments d'ordre 5 dans $\mathcal{A}_5$.

Solution : *Il y a donc autant d'éléments d'ordre* 5 *c'est-à-dire de* 5*-cycles dans* $\mathcal{A}_5$ *que d'éléments dans* $\mathcal{S}_4$ *autrement dit* $4! = 24$.

c) () Montrer qu'il y a une partition de l'ensemble des éléments d'ordre 5 de $\mathcal{A}_5$ en deux classes de conjugaison, dans $\mathcal{A}_5$, de même cardinal.

Solution : *Pour tout élément* $c \in \mathcal{A}_5$ *d'ordre* 5, *il existe* $s \in \mathcal{S}_4$ *tel que*

$$c = (s(1), s(2), s(3), s(4), 5) .$$

Notons $s' \in \mathcal{S}_5$ *la permutation dont la restriction à* $[1; 4]$ *est donnée par* s, *et telle que* $s'(5) = 5$. *On a alors*

$$c = (s'(1), s'(2), s'(3), s'(4), s'(5)) = s' \circ (1, 2, 3, 4, 5) \circ s'^{,-1} .$$

Or on constate immédiatement que $\sigma(s) = \sigma(s')$ *autrement dit,* $s \in \mathcal{A}_4$, *si et seulement si* $s' \in \mathcal{A}_5$. *Dans ce cas,* c *est conjugué au cycle* $(1, 2, 3, 4, 5)$ *dans* $\mathcal{A}_5$. *Il y a donc autant d'éléments d'ordre* 5 *conjugués à* $(1, 2, 3, 4, 5)$ *que d'éléments dans* $\mathcal{A}_4$ *c'est-à-dire* $\dfrac{4!}{2} = 12$.

Si $s \notin \mathcal{A}_4$, $s \circ (1, 2) \in \mathcal{A}_4$ *et dans ce cas* c *est conjugué à* $(2, 1, 3, 4, 5)$. *Il y a donc autant d'éléments d'ordre* 5 *conjugués à* $(2, 1, 3, 4, 5)$ *que d'éléments dans le complémentaire de* $\mathcal{A}_4$ *dans* $\mathcal{S}_4$ *soit* $\dfrac{4!}{2} = 12$.

5) () **a)** () Montrer qu'il n'y a pas de sous-groupe distingué de cardinal $5, 10, 15, 20$ ou 30 dans $\mathcal{A}_5$.

Solution : *Soit* H *un sous-groupe distingué de* $\mathcal{A}_5$.

i) ***(Cardinal*** 5*)***

Si $\#(H) = 5$, H *contient au moins un élément d'ordre* 5 *et contient donc au moins toute sa classe de conjugaison soit* 12 *éléments (cf. question 4), c),) ce qui est contradictoire.*

ii) ***(Cardinale*** 10*)***

Si $\#(H) = 10$ H *ne peut contenir d'éléments d'ordre* 2 *d'après la question 3), c). Tous ses éléments différents de* Id *sont donc d'ordre* 5 *c'est-à-dire que* H *contient au moins* 12 *éléments ce qui est encore contradictoire.*

iii) ***(Cardinal*** 15 ***ou*** 20*)***

Si le cardinal de H *est* 15 *(resp.* 20,*) il ne peut, toujours en vertu de la question 3), c) contenir d'éléments d'ordre* 3 *(resp.* 2.*) Tous ses éléments sont donc d'ordre* 5. *Pour un tel élément* c *fixé,* H *contient toute la classe de conjugaison de* c *soit* 12 *éléments, mais il existe nécessairement un élément* $d \in H$ *n'appartenant pas à la classe de conjugaison de* c. *Le sous-groupe* H *doit alors contenir également toute la classe de conjugaison de* d *c'est-à-dire que* H *contiendra nécessairement au moins* 24 *éléments ce qui est contradictoire.*

iv) (***Cardinal*** 30)

Enfin si $\#(H) = 30$, *pour les même raisons qu'à la question 3), c), les éléments de* H *différents de l'identité sont d'ordre* 5. *Or il n'y a que* $24 < 29$ *tels éléments.*

b) () En déduire finalement que $\mathcal{A}_5$ ne possède pas d'autre sous-groupe distingué que $\{\mathrm{Id}\}$ et lui-même.

Solution : *Si* H *est un sous-groupe distingué de* $\mathcal{A}_5$, *son cardinal divise* $\#\big(\mathcal{A}_5\big) = 60$ *c'est-à-dire que* $\#(H)$ *vaut*

$$1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 \text{ ou } 60 \ .$$

Le cas des sous-groupes de cardinal $2, 4, 6$ *ou* 12 *a été traité à la question 3), c).*

Le cas des sous-groupes de cardinal $5, 10, 15, 20$ *ou* 30 *a été traité au point a).*

Or $\{\mathrm{Id}\}$ *est toujours un sous-groupe distingué et tout groupe est distingué dans lui-même.*

Université Paris Sud — Année 2014–2015

L3/S5 M313 — Algèbre Générale

Index