Algèbre et Arithmétique

Université d'Eleuthéria-Polites

Cours de Licence 2 et 3 — 2021/2022

Bruno DEꞒCHAMPS

Version 1.0

On n'est pas d'un pays mais on est d'une ville
Où la rue artérielle limite le décor.
Les cheminées d'usine hululent à la mort.
La lampe du gardien rigole de mon style.

La misère écrasant son mégot sur mon cœur
A laissé dans mon sang la trace indélébile
Qui a le même son et la même couleur
Que la suie des crassiers, du charbon inutile.

Les forges de mes tempes ont pilonné les mots.
J'ai limé de mes mains le creux des évidences.
Les mots calaminés crachent des hauts-fourneaux.
Mes yeux d'acier trempé inventent le silence.

Je me soûle à New York et me bats à Paris.
Je balance à Rio et ris à Montréal
Mais c'est quand même ici que poussa tout petit
Cette fleur de grisou à tige de métal.

Table des matières

0 Les entiers naturels.

0.1 Axiomatique.

L'*ensemble des entiers naturels*, noté $\mathbb{N}$, est un ensemble muni d'un ordre $\leq$ et qui vérifie les axiomes suivants :

S.0. L'ensemble $\mathbb{N} \neq \emptyset$.

S.1. L'ordre $\leq$ est un bon ordre sur E (i.e. toute partie non vide de $\mathbb{N}$ possède un plus petit élément).

S.2. Toute partie majorée non vide de $\mathbb{N}$ possède un plus grand élément.

S.3. $\mathbb{N}$ ne possède pas de plus grand élément.

On peut montrer qu'il n'y qu'un seul ensemble ordonné vérifiant ces axiomes, plus exactement si deux ensembles ordonnés vérifient ces axiomes alors il existe une unique bijection croissante entre ces deux ensembles et on peut donc moralement considérer que ce sont les mêmes (leurs propriétés relatives à leurs ordres respectifs sont les mêmes).

Proposition 1.— 1/ L'ordre $\leq$ sur $\mathbb{N}$ est total.

2/ L'ensemble $\mathbb{N}$ est infini.

3/ L'ensemble ordonné $(\mathbb{N}, \leq)$ possède un plus petit élément (que l'on notera dans la suite 0).

Preuve : Exercice.

0.2 Successeur et prédécesseur.

Considérons un entier naturel $n \in \mathbb{N}$ et considérons l'ensemble

$$S_n = \{m \in \mathbb{N} / \ m > n\}$$

L'ensemble S_n est non vide car, si tel était le cas, comme l'ordre $\leq$ est total, l'élément n serait un plus grand élément de $\mathbb{N}$ ce qui est exclu par l'axiome $S.3.$. Par ailleurs, puisque $\leq$ est un bon ordre et que l'ensemble S_n est non vide, il possède un plus petit élément que l'on notera $s(n)$. Il s'agit donc du plus petit des majorants stricts de l'entier naturel n.

Définition 2.— *Pour tout entier naturel n, on appelle "successeur" de n le plus petit des majorants stricts de n. On le note $s(n)$.*

La correspondance $n \longmapsto s(n)$ définit donc une application $s : \mathbb{N} \longrightarrow \mathbb{N}$ que l'on appelle "fonction successeur".

De même, si l'on considère un entier naturel $n \neq 0$ et l'ensemble $P_n = \{m \in \mathbb{N} / \ m < n\}$ alors la partie P_n est non vide (car $0 \in P_n$) et est majoré (par exemple par n). D'après l'axiome $S.2.$, la partie P_n possède un plus grand élément, noté $p(n)$. Il ce qui précède F n'est pas vide (car $0 \in F$) et est majorée (par n). On appelle prédécesseur de n l'élément noté $p(n)$. Il s'agit donc du plus grand des minorants stricts de l'entier naturel n.

Définition 3.— *Pour tout entier naturel $n \neq 0$, on appelle "prédécesseur" de n le plus grand des minorants stricts de n. On le note $p(n)$.*

La correspondance $n \longmapsto s(n)$ définit donc une application $s : \mathbb{N} - \{0\} \longrightarrow \mathbb{N}$ que l'on appelle "fonction prédécesseur".

Théorème 4.— *1/ Pour tout $n \in \mathbb{N}$ on a $s(n) > n$ et pour tout $m \in \mathbb{N}$ on a*

$$m > n \Longleftrightarrow m \geq s(n)$$

2/ Pour tout $n \in \mathbb{N} - \{0\}$ on a $p(n) < n$ et pour tout $m \in \mathbb{N}$ on a

$$m < n \Longleftrightarrow m \leq p(n)$$

3/ La fonction s est strictement croissante et la fonction p est strictement décroissante.

4/ Pour tout $n \in \mathbb{N} - \{0\}$ on a $s \circ p(n) = n$.

Preuve : 1,2,3/ Exercices.

4/ On a $p(n) < n$, donc $s(p(n)) \leq n$. Posons $m = s(p(n))$ et supposons que $m < n$, on a donc $m \leq p(n)$ mais comme $m = s(p(n))$ on a $m > p(n)$ ce qui est absurde. Ainsi $m = n$.

□

Théorème 5.— (Principe de récurrence) *Soit A une partie de $\mathbb{N}$. Si A vérifie*

• $0 \in A$.

• $\forall n \in \mathbb{N}$, $n \in A \Longrightarrow s(n) \in A$.

alors $A = \mathbb{N}$.

Preuve : Raisonnons par l'absurde en supposant que $A \neq \mathbb{N}$. On considère alors l'ensemble $F = \mathbb{N} - A$ qui est donc non vide. Soit n_0 le plus petit élément de F. On a $n_0 \neq 0$ (car $0 \notin F$) et donc n_0 a un prédécesseur m_0. Comme $n_0 > p(n_0) = m_0$ et que n_0 est le plus petit élément de A on a $m_0 \notin F$, donc $m_0 \in A$ et par suite $n_0 = s(m_0) \in A$ ce qui est absurde.

□

Corollaire 6.— *L'application s est une bijection de $\mathbb{N}$ sur $\mathbb{N} - \{0\}$. Son application réciproque est la fonction p*

Preuve : • Prouvons que s est bien à valeur dans $\mathbb{N} - \{0\}$. Supposons qu'il existe $n \in \mathbb{N}$ tel que $s(n) = 0$, on a donc $0 > n$ ce qui est en contradiction avec le fait que 0 est le plus petit élément de $\mathbb{N}$.

• Montrons l'injectivité de s. Soit $n, m \in \mathbb{N}$ tels que $s(n) = s(m)$. Comme $\leq$ est un ordre total, les éléments n et m sont comparables (disons, par exemple, que $n \leq m$). Si $n < m$ on a donc $m \geq s(n)$ mais comme $s(m) > m$ on en déduit que $s(m) > s(n)$ ce qui est absurde, donc $n = m$.

• Montrons la surjectivité de s. Considérons l'ensemble $A = s(\mathbb{N}) \cup \{0\}$. Par hypothèse, on a $0 \in A$. Si maintenant on prend $n \in A$ alors $n \in \mathbb{N}$ et donc $s(n) \in s(\mathbb{N}) \subset A$. Ainsi, par le principe de réccurence on en déduit que $A = \mathbb{N}$ et donc que $s(\mathbb{N}) = \mathbb{N} - \{0\}$.

□

Sur l'ensemble $\mathbb{N}$ il existe donc une fonction s qui vérifie les axiomes (dits de Peano) suivants :

P.o. il existe un élément $0 \in \mathbb{N}$ et une application $s : \mathbb{N} \to \mathbb{N}$.

P.1. L'application s est injective et à valeurs dans $\mathbb{N} - \{0\}$.

P.2. Toute partie A de $\mathbb{N}$ vérifiant $0 \in A$ et $s(A) \subset A$ est égale à $\mathbb{N}$.

On peut montrer que le couple $(\mathbb{N}, s)$ est le seul à vérifier l'axiomatique de Peano, plus exactement si $(\mathbb{N}', s')$ est un autre couple qui vérifie Peano, alors il existe une unique bijection $\varphi : \mathbb{N} \longrightarrow \mathbb{N}'$ telle que $\varphi \circ s = s' \circ \varphi$.

0.3 Arithmétique sur $\mathbb{N}$

0.3.1 Addition.

Théorème 7.— *Sur l'ensemble* $\mathbb{N}$ *il existe une unique loi de composition interne, appelée "addition" et notée* $+$*, vérifiant :*

1/ $\forall n \in \mathbb{N}$, $0 + n = n + 0 = n$.

2/ $\forall n, m \in \mathbb{N}$, $s(n) + m = n + s(m) = s(n + m)$.

Muni de cette loi de composition interne, le magma $(\mathbb{N}, +)$ *est associatif, commutatif et unitaire. Le seul élément symétrisable de* $\mathbb{N}$ *est* 0.

Preuve : L'existence de $+$ est admise

• Unicité de $+$. Supposons donné $\perp$ une autre loi de composition interne vérifiant 1,2/. Montrons, par récurrence sur n, que pour tout $m \in \mathbb{N}$, $n + m = n \perp m$. La proposition est visiblement vraie pour $n = 0$ à cause de 1/. Supposons la propriété vraie pour un entier $n \geq 0$. Pour $m \in \mathbb{N}$, on a $s(n) + m = s(n + m) = s(n \perp m) = s(n) \perp m$ et la propriété est donc vraie pour $s(n)$.

• Associativité de $+$. Montrons, par récurrence sur l'entier n que, pour tout $n, m, p \in \mathbb{N}$, $n + (m + p) = (n + m) + p$. Pour $n = 0$, on a $0 + (m + p) = m + p = (0 + m) + p$. Supposons la propriété vraie pour un entier $n \geq 0$. Pour $m, p \in \mathbb{N}$ donnés, on a $(s(n) + m) + p = s(n + m) + p = (n + m) + s(p) = n + (m + s(p)) = n + s(m + p) = s(n) + (m + p)$ et la propriété est donc vraie pour $s(n)$.

• Commutativité de $+$. Montrons par récurrence sur l'entier n que, pour tout m, $n+m = m+n$. La propriété est clairement vraie pour $n = 0$ d'après 1/. Supposons la propriété vraie pour un entier $n \geq 0$ donné. Pour tout $m \in \mathbb{N}$, on a $s(n) + m = s(n + m) = s(m + n) = m + s(n)$ et la propriété est donc vraie pour $s(n)$.

• L'élément 0 est un neutre bilatère d'après 1/.

• Supposons qu'il existe $n \neq 0$ et $m \in \mathbb{N}$ tels que $n + m = 0$. On a alors $0 = s(p(n)) + m = s(p(n) + m)$ et donc 0 possède un prédécesseur, ce qui est absurde.

□

Si l'on pose $1 = s(0)$, alors il vient $s(n) = n + 1 = 1 + n$ pour tout $n \in \mathbb{N}$.

Théorème 8.— *Soient* $x, y \in \mathbb{N}$. *Les propriétés suivantes*

i) $x \leq y$,

ii) il existe $k \in \mathbb{N}$, $y = x + k$,

sont équivalentes. En particulier, il existe $k \in \mathbb{N}$ *tel que* $x = y + k$ *ou* $y = x + k$.

Preuve : $ii) \Longrightarrow i)$ s'obtient par récurrence sur l'entier k.

$i) \Longrightarrow ii)$ Raisonons par l'absurde en supposons qu'il existe $x < y$ tel que $\forall k \in \mathbb{N}$, $y \neq x+k$. On considère l'ensemble Y des entiers y vérifiant cette propriété. Par hypothèse, Y est non vide et donc Y possède un plus petit élément y_0. On a $y_0 > x$ et donc y_0 possède un prédécesseur t. Comme $t \notin Y$ et que $t \geq x$ (sinon $t < x$ et donc $y_0 = s(t) \leq x$), il existe k tel que $t = x + k$. On a alors $y_0 = s(t) = s(x + k) = x + s(k)$ ce qui est absurde.

□

Proposition 9.— *Soient* $x, y, y' \in \mathbb{N}$.

a) Si $x + y = x + y'$ *alors* $y = y'$ *(tout entier est simplifiable pour la loi +).*

b) Si $y < y'$ *alors* $x + y < x + y'$ *(l'ordre* $\leq$ *est compatible avec la loi de composition +).*

Preuve : S'obtient par récurrence sur x.

□

0.3.2 Multiplication

Dans la suite on notera $1 = s(0)$.

Théorème 10.— *Sur* $\mathbb{N}$ *il existe une unique loi de composition interne, notée . et appelée "multiplication", vérifiant :*

1/ $\forall x \in \mathbb{N}$, $0.x = x.0 = 0$.

2/ $\forall x, y \in \mathbb{N}$, $x.s(y) = (x.y) + x$.

Muni de cette loi de composition interne, le magma $(\mathbb{N}, +)$ *est associatif, commutatif et unitaire. La multiplication est distributive sur l'addition.*

Preuve : L'existence de la loi . sera admise, les autres propriétés du théorème sont laissées en exercice.

□

Proposition 11.— *Si* $x, y \in \mathbb{N}$ *sont tels que* $xy = 0$ *alors* $x = 0$ *ou* $y = 0$.

Preuve : Si $y \neq 0$, alors y possède un prédécesseur $p(y)$ et donc $x.y = x.s(p(y)) = (x.p(y)) + x = 0$. On en déduit en particulier que $x = 0$.

Proposition 12.— *Soient* $y, y' \in \mathbb{N}$ *et* $x \neq 0$.

a) Si $x.y = x.y'$ *alors* $y = y'$ *(les éléments non nuls sont simplifiables pour .).*

b) Si $y < y'$ *alors* $x.y < x.y'$ *(l'ordre* $\leq$ *est compatible avec la loi de composition .).*

Preuve : S'obtient par récurrence sur x.

□

Exercices : 1/ Montrer que toute partie majorée de $\mathbb{N}$ est finie (procéder par récurrence sur le majorant). En déduire que toute suite décroissante d'entier est stationnaire.

2/ Soit $x, y, u, v \in \mathbb{N}$. Montrer que si $x \leq y$ et $u \leq v$ alors $x + u \leq y + v$ et que $xu \leq yv$. Que devient cette propriété si l'on remplace $\leq$ par $<$?

1 Introduction au langage des groupes et des anneaux

1.1 Eléments de théorie des groupes

1.1.1 Définitions et notations.

Définition 13.— *On appelle groupe, tout ensemble G muni d'une loi de composition interne $*$ $((g,h) \in G^2 \longmapsto g * h \in G$ vérifiant :*

1/ $\forall g, h, k \in G,\ g * (h * k) = (g * h) * k$ *(associativité).*

2/ $\exists e \in G\ \forall g \in G,\ g * e = e * g = g$ *(existence d'un élément neutre).*

3/ $\forall g \in G\ \exists h \in G,\ g * h = h * g = e$ *(existence d'un inverse).*

Si la loi $*$ est commutative, c'est-à-dire si l'on a

4/ $\exists e \in G\ \forall g, h \in G,\ g * h = h * g$,

on dit que G est "abélien".

Proposition 14.— *Dans un groupe $(G,*)$, l'élément neutre e est unique. Par ailleurs, chaque élément possède un unique inverse.*

Preuve : Si e' est un autre neutre, alors par définition de la neutralité, on a $e = e * e' = e'$.

Soient $x \in G$ et $y, y' \in G$ deux inverses de x. On a $(y*x)*y' = e*y' = y'$ et $y*(x*y') = y*e = y$. Comme la loi $*$ est associative, on a$(y * x) * y' = y * (x * y')$ et par suite $y = y'$.

□

Notations 15.— On considère un groupe $(G,*)$.

1/ L'usage veut que, généralement, la loi de composition d'un groupe se note . où même plus fréquement ne se note pas. Ainsi, on pour deux élément x et y d'un groupe, on note xy le résultat de la composition de x et de y par la loi interne. Lorsque le groupe est abélien, on note usuellement + sa loi de composition.

2/ On notera génériquement e_G LE neutre d'un groupe $(G,*)$.

3/ Si $x \in G$, on note généralement x^{-1} (resp. $-x$) son inverse si l'on utilise la notation . (resp. +) pour la loi $*$.

Règles de calcul : (Exercice) Soit $(G,.)$ un groupe de neutre e.

a) Pour tout $x \in G$, $(x^{-1})^{-1} = x$ (l'inverse de l'inverse est égal à l'élément).

b) Pour tout $x, y \in G$, $(xy)^{-1} = y^{-1}x^{-1}$ (le passage à l'inverse renverse l'ordre).

c) Si $x \in G$ et $n \in \mathbb{N}^*$, on note $x^n = x.\cdots.x$ (n fois). On convient que $x^0 = e$. On a alors $(x^n)^{-1} = (x^{-1})^n$. Cela permet de définir x^n lorsque n est un entier négatif, en posant dans ce

cas $x^n = (x^{-1})^{-n} = (x^{-n})^{-1}$. On a alors la relation suivante :

$$\forall x \in G,\ \forall a, b \in \mathbb{Z},\ x^{a+b} = x^a.x^b$$

On fera bien attention à ne pas se laisser piéger : généralement pour $x, y \in G$ et $n \in \mathbb{Z}$, on a $(xy)^n \neq x^n y^n$. Toutefois si x et y sont tels que $xy = yx$ (on dit alors que x et y commutent, ce qui est toujours le cas dans un groupe abélien) alors pour tout $n \in \mathbb{Z}$, on a $(xy)^n = x^n y^n$.

d) Soient $x, a, b \in G$. Si $ax = ay$ (resp. $xa = ya$) alors $x = y$ (on dit que a est régulier).

On en déduit que si dans un groupe un élément y satisfait l'équation $xy = x$ (ou $yx = x$) pour un certain x, alors $y = e$.

Exemples de groupes : (Exercice)

a) Les magmas $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, .)$, $(\mathbb{R}^*, .)$,$(\mathbb{C}^*, .)$ sont des groupes abéliens.

b) Si $n \geq 1$ désigne un entier, l'ensemble

$$\mu_n = \{\exp(2ik\pi/n)/\ k \in \mathbb{Z}\} = \{z \in \mathbb{C}/\ z^n = 1\}$$

est un groupe abélien pour la multiplication complexe. C'est le *groupe des racines n-ième de l'unité*.

De même, l'ensemble $\mathbb{U} = \{z \in \mathbb{C}/\ |z| = 1\}$ est un groupe abélien pour la multiplication complexe. On l'appelle le *groupe unitaire*.

c) Si $n \geq 1$ désigne un entier, les ensembles $GL_n(\mathbb{C}) = \{M \in \mathcal{M}_n(\mathbb{C})/\ \det M \neq 0\}$ et $SL_n(\mathbb{C}) = \{M \in \mathcal{M}_n(\mathbb{C})/\ \det M = 1\}$ sont des groupes pour la multiplication des matrices.

d) Soit E un ensemble non vide et $\mathrm{Perm}(E)$ l'ensemble des bijections de E dans E. L'ensemble $\mathrm{Perm}(E)$ est un groupe (non commutatif sauf pour quelques cas que l'on précisera exaustivement) pour la composition des applications. Si $n \geq 1$ désigne un entier et si $E_n = \{1, \cdots, n\}$, le groupe $(\mathrm{Perm}(E_n), \circ)$ s'appelle le n-ième groupe symétrique et se note S_n. Un élément $\sigma \in S_n$ se note par son image, élément par élément :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Ainsi le neutre de S_n (qui est l'identité) est $e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$.

e) Soit $\mathcal{P}$ le plan affine et euclidien et Ω une partie du plan $\mathcal{P}$. L'ensemble des isométries qui envoient Ω sur lui-même est un groupe pour la composition des applications.

f) Le magma $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien.

g) On considère un ensemble E et $\mathcal{P}(E)$ son ensemble de parties. Sur $\mathcal{P}(E)$, on définit une loi de composition interne appelée différence symétrique, notée Δ et définie par :

$$\forall A, B \in \mathcal{P}(E),\ A\Delta B = C_{A\cup B}A \cap B = (A - B) \cup (B - A)$$

Le magma $(\mathcal{P}(E), \Delta)$ est alors un groupe abélien.

h) On considère l'ensemble constitué des huit matrices de $\mathcal{M}_2(\mathbb{C})$ suivantes :

$$\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},\begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix},\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix},\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\right\}$$

C'est un groupe pour la multiplication des matrices. On le note Q_8 et on l'appelle le groupe quaternionique. Il est non abélien.

1.1.2 Sous-groupes

Définition 16.— *Soit $(G,*)$ un groupe. On appelle sous-groupe de G toute partie H de G tel que H soit stable pour $*$ (i.e. $\forall x,y \in H$, $x*y \in H$ et telle que $(H,*)$ soit un groupe.*

Exemple :

Proposition 17.— *Soit G un groupe de neutre e et H un sous-groupe de G. Le neutre de H est e et pour tout $x \in H$, l'inverse de x dans H est l'inverse de x dans G.*

Preuve : Notons f le neutre de H neutre. On a $f.f = f$ dans H et donc dans G. Mais comme dans G on a $f = fe$, on en déduit que dans G, $ff = fe$ et par suite comme f est régulier (G est un groupe), on a $f = e$.

Soit $x \in H$, notons y son (unique) inverse dans H. On a donc $xy = yx = e$ dans H mais donc dans G aussi. Il s'ensuit que y est un inverse de x dans G, mais comme l'inverse x^{-1} de x dans G est unique, on en déduit que $y = x^{-1}$.

□

Corollaire 18.— (Axiomes faibles) *Soit G un groupe et H une partie de G. Les propositions suivantes*

i) H est un sous-groupe de G,

ii) $H \neq \emptyset$ et pour tout $x,y \in H$, $xy^{-1} \in H$.

sont équivalentes.

Preuve : $i) \Rightarrow ii)$ H n'est clairement pas vide car il contient e. La proposition précédente montre que si $y \in H$ alors $y^{-1} \in H$. Ainsi, si $x,y \in H$, on a $y^{-1} \in H$ et donc, comme H est un groupe, on a $xy^{-1} \in H$.

$ii) \Rightarrow i)$ Soit $x \in H$. En prenant $y = x$, on a $e = xx^{-1} \in H$. Par suite, pour tout $y \in H$, on a $ey^{-1} = y^{-1} \in H$. Donc si $x,y \in H$, on a $x,y^{-1} \in H$ et donc $xy = x(y^{-1})^{-1} \in H$. Ainsi, H est stable par la loi de composition de G. Comme G est associatif, H l'est aussi. Comme $e \in H$, H possède bien un neutre et, enfin, comme tout élément de H admet un inverse, H est bien un groupe.

□

Dans un groupe G de neutre e, il y a deux sous-groupes évident : G tout entier et $\{e\}$. On les appelles les sous-groupes triviaux de G. Les sous-groupes non triviaux sont appelés stricts ou propres.

On remarque que si H est un sous-groupe de G et que D est un sous-groupe de H alors D est un sous-groupe de G (exercice), la relation "être sous-groupe de" est donc transitive.

Dans la suite si H est un sous-groupe de G, on notera $H \leq G$. La transitivité se traduit alors par

$$D \leq H \text{ et } H \leq G \Longrightarrow D \leq G$$

Proposition 19.— *Soit G un groupe et $\{H_i\}_{i\in I}$ une famille de sous-groupes de G. La partie $\bigcap_{i\in I} H_i$ est un sous-groupe de G.*

Preuve : Vérifions les axiomes faibles. Posons $H = \bigcap_{i\in I} H_i$. Si e désigne le neutre de G, alors comme chaque H_i est un sous-groupe de G, on a $e \in H_i$ pour tout $i \in I$ et par suite $e \in H$. Ainsi H est non vide.

Considérons $x, y \in H$. Pour tout $i \in I$, on a $x, y \in H_i$ et par suite $xy^{-1} \in H_i$ puisque chaque H_i est un sous-groupe. On en déduit donc que $xy^{-1} \in H$. H est donc bien un sous-groupe de G.

□

Ce résultat est bien sur faux en général pour la réunion $\bigcup_{i\in I} H_i$ (exercice). On a toutefois le résultat suivant : si $\{H_i\}_{i\in I}$ une famille de sous-groupes de G vérifiants que pour tout $i, j \in I$ il existe $k \in I$ tel que $H_i \leq H_k$ et $H_j \leq H_k$, alors $\bigcup_{i\in I} H_i$ est un sous-groupe de G (exercice). C'est le cas, par exemple, lorsque la famille $\{H_i\}_{i\in I}$ est en fait une suite croissante $H_0 \leq H_1 \leq \cdots \leq H_n \leq \cdots$ de sous-groupes de G.

Exemples de sous-groupes : (Exercice)

a) Les groupes $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ $(\mathbb{R}, +)$ sont des sous-groupes de $(\mathbb{C}, +)$.

b) Pour tout $n \geq 1$, le groupe $(\mu_n, .)$ est un sous-groupe de $(\mathbb{U}, .)$ qui est lui-même un sous-groupe de $(\mathbb{C}^*, .)$.

d) Soit G un groupe, on appelle *centre* de G l'ensemble

$$Z(G) = \{x \in G / \ \forall y \in G,\ xy = yx\}$$

constitué des éléments de G qui commutent avec tous les éléments de G. L'ensemble $Z(G)$ est toujours un sous-groupe de G, c'est bien évidemment un sous-groupe abélien.

1.1.3 Morphismes

Définition 20.— *Soit $(G, *)$ et $(H, \perp)$ deux groupes. On appelle morphisme du groupe G dans le groupe H toute application $f : G \to H$ vérifiant*

$$\forall g, h \in G,\ f(g * h) = f(g) \perp f(h)$$

Suivant l'usage introduit précédement, nous notons . (ou rien) pour désigner la loi de composition d'un groupe. Par commodité, en général, quand nous considérerons deux groupes, nous utiliserons la même notation pour la loi de composition des deux groupes et ainsi nous écrirons pour un morphisme : $f(x.y) = f(x).f(y)$ à la place de $f(x*y) = f(x) \perp f(y)$.

Il faudra faire trés attention à ne pas oublier que malgré ces notations abusives, les lois de groupes ne sont pas les mêmes, et quand cela deviendra trop ambigu, nous choisirons délibérement de bien noter différement ces lois.

Terminologie. Si $f : G \longrightarrow H$ désigne un morphisme de groupes, on dira que f est un

- *monomorphisme* si f est injectif,
- *épimorphisme* si f est surjectif,
- *isomorphisme* si f est bijectif,
- *endomorphisme* si $G = H$,
- *automorphisme* si $G = H$ et f est bijectif.

Proposition 21.— *Soit $f : G \longrightarrow H$ un morphisme de groupes. On a*

1/ $f(e_G) = e_H$.

2/ Pour tout $g \in G$, $f(g^{-1}) = (f(g))^{-1}$ (et plus généralement, pour tout $n \in \mathbb{Z}$, on a $f(x^n) = (f(x))^n$.

Preuve : Exercice.

□

Proposition 22.— *Soit $f : G \longrightarrow G^{'}$ un morphisme de groupes. L'image direct d'un sous-groupe de G par f est un sous-groupe de $G^{'}$ et l'image réciproque d'un sous-groupe de $G^{'}$ par f est un sous-groupe de G.*

Preuve : Notons e et $e^{'}$ les neutres respectifs de G et $G^{'}$. Prenons un sous-groupe H de G et notons $H^{'} = f(H)$ l'image directe de H par f. Vérifions les axiomes faibles : $H^{'}$ n'est pas vide car $e \in H$ et donc $e^{'} = f(e) \in H^{'}$. Soit maintenant $x^{'}, y^{'} \in H^{'}$, par hypothèse, il existe $x, y \in H$ tels que $x^{'} = f(x)$ et $y^{'} = f(y)$. Comme H est un sous-groupe de G, on a $xy^{-1} \in H$ et donc $f(xy^{-1}) \in H^{'}$, or $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)(f(y))^{-1} = x^{'}y^{'-1}$.

Soit maintenant un sous-groupe $H^{'}$ de $G^{'}$ et posons $H = f^{-1}(H^{'})$. Vérifions les axiomes faibles : Comme $e^{'} \in H$ et que $f(e) = e^{'}$, on en déduit que $e \in H$. Soit maintenant $x, y \in H$, c'est-à-dire $f(x) = x^{'} \in H^{'}$ et $f(y) = y^{'} = \in H^{'}$. Comme $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)(f(y))^{-1} = x^{'}y^{'-1} \in H^{'}$, on en déduit que $xy^{-1} \in H$.

□

En particulier, si l'on prend G tout entier comme sous-groupe, alors $f(G)$ est un sous-groupe de $G^{'}$. On l'appelle l'image de f et on le note $\mathrm{Im}(f)$. De même, si l'on prend pour sous-groupe de $G^{'}$ le sous-groupe $\{e^{'}\}$ où $e^{'}$ désigne le neutre de $G^{'}$, alors $f^{-1}(\{e^{'}\})$ est un sous-groupe de G. On l'appelle le noyau de f et on le note $\mathrm{Ker}(f)$.

Proposition 23.— *Soit $f : G \longrightarrow G^{'}$ un morphisme de groupes. On a*

a) f est surjectif si et seulement si $\mathrm{Im}(f) = G^{'}$.

b) f est injectif si et seulement si $\mathrm{Ker}(f) = \{e\}$ (e est le neutre de G).

Preuve : a) est évident.

b) Supposons f injective, comme $f(e) = e^{'}$, si $x \in G$ vérifie $f(x) = e^{'}$ (i.e. si $x \in \mathrm{Ker}(f)$) alors $x = e$ et donc $\mathrm{Ker}(f) = \{e\}$. Réciproquement, supposons que $\mathrm{Ker}(f) = \{e\}$. Soit $x, y \in G$ tel que

$f(x) = f(y)$, on a donc dans $G^{'}$ $f(x)(f(y))^{-1} = e^{'}$, c'est à dire $f(xy^{-1}) = e^{'}$ et donc $xy^{-1} \in \mathrm{Ker}(f)$. Ainsi $xy^{-1} = e$, c'est-à-dire $x = y$. f est bien injective.

□

Exemples de morphismes : (Exercice)

a) Soit G un groupe et H un sous-groupe, l'injection canonique $x \mapsto x$ de H dans G est un morphisme injectif de groupe. Pour $G = H$, ce morphisme est l'identité.

b) Soit G et $G^{'}$ deux groupes, l'application $x \mapsto e^{'}$ est un morphisme de noyau égal à G tout entier. On l'appelle le *morphisme trivial* ou *morphisme nul*.

c) Considérons les groupes $(\mathbb{R}, +)$ et $(\mathbb{C}^*, .)$. L'application définie par $f(x) = \exp(ix)$ est un morphisme de groupe. On a $\mathrm{Ker}(f) = 2\pi\mathbb{Z} = \{2k\pi / \ k \in \mathbb{Z}\}$ et $\mathrm{Im}(f) = \mathbb{U}$.

d) Considérons le groupe $(GL_n(\mathbb{C}), .)$ et $(\mathbb{C}^*, .)$. L'application définie par $f(M) = \det(M)$ est un morphisme de groupe. On a $\mathrm{Im}(f) = \mathbb{C}^*$ (c'est donc un épimorphisme) et son noyau est $\mathrm{Ker}(f) = SL_n(\mathbb{C})$.

Proposition 24.— *Soient $G, G^{'}$ et $G^{''}$ trois groupes.*

1/ Si $f : G \longrightarrow G^{'}$ et $g : G^{'} \longrightarrow G^{''}$ désignent des morphismes alors on a $g \circ f : G \longrightarrow G^{''}$ est un morphisme.

2/ Si $f : G \longrightarrow G^{'}$ est un isomorphisme alors l'application réciproque $f^{-1} : G^{'} \longrightarrow G$ est aussi un isomorphisme.

Preuve : Exercice.

□

Exercices 25.— On considère un groupe G.

1/ (Groupe des automorphismes d'un groupe) On considère un groupe G et l'on note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G. Montrer que $\mathrm{Aut}(G)$ muni de la composition des applications est un groupe.

2/ (Automorphismes intérieurs) Pour tout $g \in G$, on considère l'application

$$\begin{array}{rccc} I_g : & G & \longrightarrow & G \\ & x & \longmapsto & gxg^{-1} \end{array}$$

a) Montrer que l'ensemble $\mathrm{Int}(G) = \{I_g / \ g \in G\}$ est un sous-groupe de $(Aut(G), \circ)$. On l'appelle groupe des *automorphismes intérieurs* de G.

b) Montrer que l'application

$$\begin{array}{rccc} I : & G & \longrightarrow & \mathrm{Int}(G) \\ & g & \longmapsto & I_g \end{array}$$

est un épimorphisme de groupes. Prouver que $\ker(I) = Z(G)$.

1.2 Premiers éléments de théorie des anneaux

1.2.1 Définitions et notations

Définition 26.— *On appelle anneau la donnée d'un triplet $(A, +, .)$ où A est un ensemble et $+$ et $.$*

sont deux lois de composition interne sur A vérifiants :

1/ $(A,+)$ est un groupe abélien.

2/ . est une loi associative.

3/ $\forall a,b,c \in A$, $a.(b+c) = a.b + a.c$ et $(b+c).a = b.a + c.a$ (on dit que . est distributive par rapport à +).

Si la loi . est commutatif, on dit que l'anneau est commutatif. Si la loi . possède un neutre, on dit que l'anneau est est unitaire (ou unifère).

Dans la pratique, si A désigne un anneau, on note 0_A (ou plus simplement 0 s'il n'y a pas d'ambiguité) le neutre de +. Si A est unitaire, alors $(A,.)$ étant un magma unitaire, son neutre est unique. On le note 1_A (ou plus simplement 1 s'il n'y a pas d'ambiguité) .

Si A est un anneau, $a \in A$ et $n \in \mathbb{Z}$, on note $na = a+\cdots+a$ (n fois si $n \geq 0$) et $na = -(a+\cdots+a)$ ($-n$ fois si $n < 0$). Pour $a \in A$ et $n \in \mathbb{N}^*$, on pose $a^n = a\cdots a$ (n fois). Si A est unitaire, on convient que $a^0 = 1_A$.

Règles de calcul dans un anneau : (Exercice)

• $\forall a \in A$, $0_A.a = a.0_A = 0_A$ (on dit que 0_A est absorbant).

• $\forall a,b_i nA$, $(-a).b = a.(-b) = -(a.b)$.

• $\forall a,b \in A$, $\forall n \in \mathbb{Z}$, $(na).b = a.(nb) = n(a.b)$.

• $\forall a,b \in A$ unitaire, $\forall n,m \in \mathbb{N}$, $(a^n)^m = a^{nm}$ et si a et b commutent (i.e. $ab = ba$) alors $a^n b^n = (ab)^n$.

• (Formule du binôme de Newton) Soit A un anneau unitaire et $a,b \in A$. Si $ab = ba$ alors pour tout entier $n \in \mathbb{N}$, on a

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}$$

Remarque : La première régle de calcul montre que si A est un anneau unitaire tel que $0_A = 1_A$ alors $A = \{0_A\}$. Pour cette raison, on conviendra à présent que si A désigne un anneau unitaire alors $0_A \neq 1_A$.

Définition 27.— *Soit A un anneau et $a \neq 0$ un élément de A. On dit que a est un diviseur de zéro à gauche (resp. à droite) s'il existe $b \neq 0$ dans A tel que $a.b = 0$ (resp. $b.a = 0$). Un diviseur de zéro à gauche et à droite est appelé diviseur de zéro.*

Un anneau sans diviseur de zéro non nul est dit intègre.

Définition 28.— *Soit A un anneau unitaire et $a \in A$. On dit que a est inversible à gauche (resp. à droite) s'il existe $b \in A$ tel que $a.b = 1$ (resp. $b.a = 1$). Un élément inversible à gauche et à droite est dit inversible. On note $U(A)$ l'ensemble des éléments inversible de A. Les éléments de $U(A)$ sont appelés les unités de A.*

Un anneau unitaire pour lequel tout élément non nul est inversible est appelé corps. Si un corps est non commutatif, on dit que c'est un corps gauche.

Si A est un anneau unitaire et si $a \in U(A)$ alors a possède un unique inverse (exercice). On le note a^{-1}. Par ailleurs, un élément inversible n'est visiblement pas un diviseur de zéro, on en déduit, en particulier, qu'un corps est un anneau intègre.

Proposition 29.— *Si $(A,+,.)$ désigne un anneau unitaire alors $(U(A),.)$ est un groupe.*

Preuve : Exercice.

Exemples : (Exercice)

a) $(\mathbb{Z},+,.)$ est un anneau commutatif, unitaire et intègre. On a $U(\mathbb{Z}) = \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$. Pour $n \geq 2$, $(n\mathbb{Z},+,.)$ est un anneau intègre mais non unitaire.

b) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps commutatifs.

c) L'ensemble $\mathcal{M}_n(K)$ des matrices carré $n \times n$ à coefficients dans un corps commutatif K est un anneau non commutatif et unitaire pour les lois usuelles. On a

$$U(\mathcal{M}_n(K)) = \{M \in \mathcal{M}_n(K) / \ det(M) \neq 0\}$$

On remarque que les diviseurs de zéro dans $\mathcal{M}_n(K)$ sont exactement les éléments $M \notin U(\mathcal{M}_n(K))$, en particulier $\mathcal{M}_n(K)$ n'est pas intègre.

d) Si E désigne un ensemble non vide, alors $(\mathcal{P}(E), \Delta, \cap)$ (où Δ désigne la différence symétrique) est un anneau commutatif et unitaire.

e) Si K désigne un corps commutatif, l'ensemble des polynômes à coefficients dans K, $K[X]$, est un anneau commutatif unitaire intègre. On a $U(K[X]) = K - \{0\}$.

f) Soit G un groupe abélien (noté additivement) et $\mathrm{End}(G)$ désigne l'ensemble des endomorphismes de G. On définit sur $\mathrm{End}(G)$ une loi de composition $+$ en posant, pour $f, g \in \mathrm{End}(G)$

$$\forall x \in G, \ (f+g)(x) = f(x) + g(x)$$

Le triplet $(\mathrm{End}(G), +, \circ)$ est un anneau (généralement non commutatif) unitaire.

Définition 30.— *Un élément $a \neq 0$ dans anneau A est dit régulier à gauche (resp. à droite) si pour tout $x, y \in A$, on a $ax = ay \Longrightarrow x = y$ (resp. $xa = ya \Longrightarrow x = y$).*

Un élément régulier à droite et à gauche est dit plus simplement régulier.

Exemples : a) Dans $\mathbb{Z}$ tout élément non nul est régulier.

b) Dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{2}$ n'est pas régulier car $\overline{2}.\overline{3} = \overline{0} = \overline{2}.\overline{0}$.

c) Tout élément inversible est régulier.

Proposition 31.— *Soit A un anneau, les propositions suivante sont équivalentes :*

i) A est intègre,

ii) tout élément $a \in A - \{0\}$ est régulier.

Preuve : *non ii)* $\Rightarrow$ *non i)* Soit $a \in A$ non régulier (par exemple à gauche). Il existe donc $x, y \in A$ tels que $ax = ay$ avec $x \neq y$. On a alors $a(x-y) = 0$ et donc a est diviseur à gauche de zéro, ce qui assure que A n'est pas intègre.

non i) $\Rightarrow$ *non ii)* Soit $a, b \neq 0$ dans A tel que $ab = 0$. On a donc $ab = a0$ avec $b \neq 0$ et donc a n'est pas régulier.

□

1.2.2 Morphisme

Définition 32.— *Soit A et B deux anneaux, on appelle homomorphisme (ou morphisme) d'anneaux de A vers B, toute application*

$$f : A \longrightarrow B$$

qui satisfait pour tout $x, y \in A$,

$$f(x+y) = f(x) + f(y) \text{ et } f(x.y) = f(x).f(y)$$

Si les anneaux sont unitaires et si f vérifie, en plus, $f(1_A) = 1_B$ on dit que f est un morphisme d'anneau unitaire.

Comme pour les groupes, on définit les notions d'épimorphisme, monomorphisme, isomorphisme, endomorphisme, automorphisme d'anneaux.

Puisqu'un morphisme d'anneau est, en particulier, un morphisme de groupe, on peut parler du noyau et de l'image. On garde alors les propriétés relatives à l'injectivité et la surjectivité liées à l'image et au noyau.

Proposition 33.— *Soit $f : A \longrightarrow B$ un morphisme d'anneau unitaire. On a*

$$f(U(A)) \subset U(B)$$

Preuve : Exercice.

□

1.2.3 Idéaux et sous-anneaux

Définition 34.— *Soit A un anneau.*

• *On appelle sous-anneau de A toute partie $B \subset A$, stable pour les deux lois de compositions de A et qui est un anneau pour ces lois (en particulier un sous-anneau est un sous-groupe).*

• *On appelle idéal à gauche (resp. à droite) de A tout sous-groupe I qui vérifie*

$$\forall a \in A,\ \forall x \in I,\ a.x \in I \ (resp.\ x.a \in I)$$

En particulier un idéal gauche ou droite de A est un sous-anneau de A.

Un idéal à gauche et à droite est appelé idéal bilatère (ou plus simplement idéal).

Exemples : a) Dans un anneau A il y a toujours au moins deux idéaux : A et $\{0\}$. On les appelles les idéaux triviaux de A. Si A est unitaire et si I est un idéal gauche ou droite de A contenant une unité $a \in U(A)$, alors $I = A$. En effet, par hypothèse, on a $a^{-1}a = 1 \in I$ (resp. $aa^{-1} = 1 \in I$) et donc pour tout $x \in A$, on a $x = x.1 \in I$ (resp. $x = 1.x \in I$).

b) Soit A un anneau unitaire. Un idéal I de A est différent de A si et seulement si il ne contient aucun élément de $U(A)$.

c) Les idéaux de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$ avec $n \geq 1$, ce sont exactement les sous-anneaux de $\mathbb{Z}$. En effet, si I est un idéal de $\mathbb{Z}$ alors comme c'est un sous-groupe, il est forcément de la forme $n\mathbb{Z}$. Réciproquement, $I = n\mathbb{Z}$ est bien un idéal de $\mathbb{Z}$ comme le justifie l'exemple suivant.

d) Si A désigne un anneau et $a \in A$, l'ensemble $aA = \{a.x/\ x \in A\}$ est un idéal à droite.

Définition 35.— *Dans un anneau commutatif A un idéal I est dit principal s'il est de la forme*

$$I = aA = \{ax/\ x \in A\} \text{ pour un certain élément } a \in A$$

On notera alors $I = (a)$ et l'on dira que I est l'idéal principal engendré par l'élément $a \in A$.

Un anneau A sera dit principal s'il est commutatif, unitaire, intègre et si tout idéal de A est principal.

Remarques : a) L'anneau $\mathbb{Z}$ est principal d'après ce qui précède. Il existe des anneaux non principaux comme nous le verrons dans la suite.

b) Dans un anneau commutatif et unitaire A, les idéaux principaux sont exactement les idéaux de la forme (a) avec $a \in A$. On fera bien attention de constater que cette propriété n'est plus vraie si l'on retire une des hypothèses, commutatif ou unitaire, à A.

Proposition 36.— *Soit A un anneau commutatif et unitaire. Les propositions suivantes sont équivalentes :*

i) A est un corps,

ii) Les seuls idéaux de A sont A et $\{0\}$.

Preuve : $i) \Rightarrow ii)$ Soit $I \neq \{0\}$ un idéal de A et $x \neq 0$ dans I. Comme A est un corps, il existe $y \in A$ tel que $xy = 1$ et par suite $1 \in I$ et donc $I = A$.

$ii) \Rightarrow i)$ Soit $x \neq 0$ dans A. L'idéal principal xA est non nul, donc est égal à A. Ainsi, il existe $y \in A$ tel que $xy = 1$ et par suite $U(A) = A - \{0\}$, donc A est un corps.

□

Proposition 37.— *Soit A un anneau commutatif et $\{I_s\}_{s\in S}$ une famille non vide d'idéaux de A. L'intersection $\bigcap_{s\in S} I_s$ est un idéal de A.*

Preuve : Exercice.

□

Proposition-Définition 38.— *Soient I et J deux idéaux d'un anneau commutatif A. L'ensemble*

$$I + J = \{x + y/\ x \in I, y \in J\}$$

est un idéal et c'est le plus petit idéal qui contienne à la fois I et J. On l'appelle l'idéal somme des idéaux I et J.

Proposition 39.— *Soit $f : A \longrightarrow B$ un morphisme d'anneaux. Si I est un idéal à gauche (resp. à droite, resp. bilatère) de B alors $f^{-1}(I)$ est un idéal à gauche (resp. à droite, resp. bilatère) de A.*

En particulier, le noyau $\ker(f)$ *est un idéal bilatère de A.*

Preuve : Effectuons la preuve dans le cas d'un idéal à gauche. On sait déjà que $f^{-1}(I)$ est un sous-groupe de A. Soit $a \in A$ et $x \in f^{-1}(I)$ (disons $x = f^{-1}(y)$). On a $f(ax) = f(a)y$ et comme I est un idéal à gauche de B, on a donc $f(ax) \in I$ ce qui prouve que $ax \in f^{-1}(I)$ et donc que $f^{-1}(I)$ est un idéal à gauche de A.

□

Remarque : Le noyau et l'image d'un sous-anneau sont des sous-anneaux. Par contre, l'image directe d'un idéal n'est pas forcément un idéal. En effet si A est un sous-anneau d'un anneau B et que A n'est pas un idéal, alors l'injection canonique $f : A \longrightarrow B$ est un morphisme d'anneau qui envoit l'idéal A de A sur le sous-anneau A de B qui n'est pas un idéal.

Toutefois, si $f : A \longrightarrow B$ désigne un épimorphisme d'anneaux et si I désigne un idéal à gauche (resp. à droite, resp. bilatère) de A alors $f(I)$ est un idéal à gauche (resp. à droite, resp. bilatère) de A (exercice).

1.2.4 Arithmétique des anneaux

Définition 40.— *Soit A un anneau et $a, b \in A$. On dit que a divise b dans A et l'on note $a|b$ s'il existe $c \in A$ tel que $b = ac$, on dit alors aussi que a est un diviseur de b. Deux éléments a et b de A sont dit associés si $a|b$ et $b|a$.*

Proposition 41.— *Soit A un anneau commutatif et unitaire et $a, b, u \in A - \{0\}$.*

a) On a $a|b$ si et seulement si $(b) \subset (a)$ et, par conséquent, a et b sont associés si et seulement si $(a) = (b)$.

b) L'élément u est une unité si et seulement si $u|x$ pour tout $x \in A$.

c) Si $a = bu$ avec u unité de A, alors a et b sont associés. Réciproquement, si A est intègre et si a et b sont associés, alors il existe $u \in U(A)$ tel que $a = bu$.

Preuve : a) Supposons que $b = ac$, comme $ac \in (a)$ (puisque (a) est un idéal) on a donc $b \in (a)$. Ainsi, $(b) \subset (a)$ puisque (b) est le plus petit idéal contenant l'élément b.

Réciproquement, supposons que $(b) \subset (a)$. Comme A est commutatif et unitaire, on a $(a) = aA$ et comme $b \in (b)$, on a $b \in aA$ c'est-à-dire $b = ac$ pour un certain $c \in A$. Donc $a|b$.

b) Si $u \in U(a)$ alors pour tout $x \in A$, on a $x = u(u^{-1}x)$ et donc $u|x$. Réciproquement si $u|x$ pour tout $x \in A$, on a $u|1$ et donc il existe $u^{-1} \in A$ tel que $1 = uu^{-1}$. Ainsi $u \in U(A)$.

c) Si $a = bu$ alors $b|a$, mais si $u \in U(A)$ alors $b = au^{-1}$ et donc $a|b$. Réciproquement, si A est intègre et que $a|b$ et $b|a$, il existe donc $u, v \in A$ tel que $a = bu$ et $b = av$, on a donc $a = a(uv)$. Comme A est intègre et $a \neq 0$, on a donc $uv = 1$ et, par suite, $u, v \in U(A)$.

2 L'anneau $\mathbb{Z}$ des entiers relatifs

2.1 Construction

Dans $\mathbb{N}$ aucun élément, à part 0, ne possède d'opposé pour l'addition. En particulier le magma $(\mathbb{N}, +)$ n'est pas un groupe. Nous allons tenter de remédier à ce problème en "symétrisant" le magma $(\mathbb{N}, +)$.

Considérons sur le produit cartésien $\mathcal{A} = \mathbb{N} \times \mathbb{N}$ la relation binaire $\mathcal{R}$ définie pour $(a, b), (c, d) \in \mathcal{A}$ par

$$(a, b)\mathcal{R}(c, d) \Longleftrightarrow a + d = b + c$$

Lemme 42.— *La relation binaire $\mathcal{R}$ est une relation d'équivalence et l'ensemble des éléments de $\mathcal{A}$: $(0,0)$, $\{(a,0)/\ a \in \mathbb{N}^*\}$, $\{(0,a)/\ a \in \mathbb{N}^*\}$ est une classe de représentant de l'ensemble quotient $\mathcal{A}/\mathcal{R}$.*

Preuve : Exercice.

□

Définition 43.— *On appelle ensemble des entiers relatifs l'ensemble quotient $\mathcal{A}/\mathcal{R}$ et on le note $\mathbb{Z}$.*

Nous allons maintenant définir sur $\mathbb{Z}$ une addition et une multiplication.

Lemme 44.— *Soient $(a,b),(c,d),(a',b'),(c',d') \in \mathcal{A}$ tels que $(a,b)\mathcal{R}(a',b')$ et $(c,d)\mathcal{R}(c',d')$. On a*

$$(a+c,b+d)\mathcal{R}(a'+c',b'+d') \text{ et } (ac+bd,ad+bc)\mathcal{R}(a'c'+b'd',a'd'+b'c')$$

Preuve : Exercice.

□

Le lemme précédent permet alors de définir une addition et une multiplication sur $\mathbb{Z}$ de la manière suivante : si pour tout $(a,b) \in \mathcal{A}$ on note $\overline{(a,b)}$ la classe de (a,b) dans $\mathbb{Z}$, on pose

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c,b+d)} \text{ et } \overline{(a,b)}.\overline{(c,d)} = \overline{(ac+bd,ad+bc)}$$

(*Rappels sur les groupes et anneaux.*)

Théorème 45.— *$(\mathbb{Z},+,.)$ est un anneau commutatif unitaire.*

Preuve : Montrons que $(\mathbb{Z},+)$ est un groupe abélien.

• La loi + est visiblement associative et commutative.

• $\overline{(0,0)}$ est visiblement un neutre pour +. Enfin on a $\overline{(a,b)} + \overline{(b,a)} = \overline{(a+b,a+b)} = \overline{(0,0)}$, donc tout élément est symétrisable. Notons que nous venons de montrer que $-\overline{(a,b)} = \overline{(b,a)}$.

Montrons que $(\mathbb{Z},+,.)$ est un anneau, c'est-à-dire, compte tenu du fait que $(\mathbb{Z},+)$ est un groupe abélien, que . est distributive sur +. Soit $\overline{(a,b)},\overline{(c,d)},\overline{(e,f)} \in \mathbb{Z}$. On a

$$\begin{aligned}
\overline{(a,b)}.(\overline{(c,d)} + \overline{(e,f)}) &= \overline{(a,b)}.\overline{(c+e,d+f)} \\
&= \overline{(ac+ae+bd+bf,bc+be+ad+af)} \\
&= \overline{(ac+bf,bc+af)} + \overline{(ae+bd,be+ad)} \\
&= \overline{(a,b)}.\overline{(c,d)} + \overline{(a,b)}.\overline{(e,f)}
\end{aligned}$$

donc . est distributive à gauche par rapport à +. Comme . est visiblement commutative on en déduit que . est distributive par rapport à + et donc que $(\mathbb{Z},+,.)$ est un anneau commutatif.

$\overline{(1,0)}$ est visiblement un neutre pour la multiplication.

□

Proposition 46.— *L'application $\varphi : \mathbb{N} \longrightarrow \mathbb{Z}$ définie par $\varphi(a) = \overline{(a,0)}$ est une application injective morphique (i.e. pour tout $a,b \in \mathbb{N}$, $\varphi(a+b) = \varphi(a) + \varphi(b)$ et $\varphi(ab) = \varphi(a).\varphi(b)$.*

Preuve : Exercice.

□

On peut donc identifier l'ensemble $\mathbb{N}$ à un sous-ensemble de $\mathbb{Z}$. Dans la suite si $a \in \mathbb{N}$ on confondra, dans $\mathbb{Z}$, a avec $\overline{(a,0)}$. En vertu de ce qui précède, si l'on pose $\mathbb{Z}^+ = \{\overline{(a,0)}\ a \in \mathbb{N}\}$ et $\mathbb{Z}^- = \{\overline{(0,a)}\ a \in \mathbb{N}\}$, alors $\mathbb{Z}^- = -\mathbb{Z}^+$, $\mathbb{Z}^- \cup \mathbb{Z}^+ = \mathbb{Z}$ et $\mathbb{Z}^- \cap \mathbb{Z}^+ = \{0\}$. On peut donc identifier $\mathbb{N}$ à $\mathbb{Z}^+$.

On en déduit que si $x \in \mathbb{Z}$ est un entier relatif non nul, alors il existe un unique entier naturel non nul a tel que $x = a$ ou $x = -a$. Avec les notations précédentes, on voit alors que $\overline{(a,b)} = a - b$

Corollaire 47.— *L'anneau $\mathbb{Z}$ est intègre.*

Preuve : Soit $x, y \in \mathbb{Z}$. Il existe $a, b \in \mathbb{N}$ tel que $x = \pm a$ et $y = \pm b$, on a donc $xy = \pm ab$. Si x et y sont non nuls alors a et b le sont aussi et donc $xy \neq 0$.

□

Proposition 48.— *L'anneau $\mathbb{Z}$ ne possède que deux unités :* ± 1.

Preuve : Exercice.

Exercice : Ordre sur $\mathbb{Z}$.

a) Montrer que la relation binaire $\leq$ sur $\mathbb{Z}$ définie par $x \leq y \iff y - x \in \mathbb{N}$ définit une relation d'ordre sur $\mathbb{Z}$ qui étant l'ordre naturel de $\mathbb{N}$.

b) Prouver que $(\mathbb{Z}, \leq)$ est un anneau ordonné (i.e. $\leq$ est total et si $x \leq y$ et $u \leq v$ alors $x + u \leq y + v$ et si $w \geq 0$ alors $xw \leq yw$.)

c) Montrer que $\leq$ est le seul ordre sur $\mathbb{Z}$ tel que $(\mathbb{Z}, +)$ soit un anneau ordonné.

d) Montrer que toute partie non vide majorée (resp. minorée) de $\mathbb{Z}$ possède un plus grand (resp. un plus petit) élément. En déduire que pour tout $x \in \mathbb{Z}$, $|x| = \max(x, -x)$ existe. Donner et démontrer les principales propriétés de $|.|$.

e) Prouver que toute suite décroissante minorée d'entiers est stationnaire.

2.2 Propriété de l'anneau $\mathbb{Z}$.

2.2.1 Divisibilité

Définition 49.— *Si $a, b \in \mathbb{Z}$, on dit que "a divise b" ou que "b est multiple de a" et l'on note $a|b$ s'il existe $k \in \mathbb{Z}$ tel que $b = ak$.*

Exercice 50.— Décrire les diviseurs et les multiples de 0.

Proposition 51.— *Soient $a, b, c, d \in \mathbb{Z}$.*

1/ (Réflexivité) $a|a$.

2/ (Transitivité) Si $a|b$ et $b|c$ alors $a|c$.

3/ (Presque-antisymétrie) Si $a|b$ et $b|a$ alors $|a| = |b|$ (la réciproque est vraie).

En particulier, sur $\mathbb{N}$ la relation $.|.$ est une relation d'ordre.

4/ Si $d|a$ et $d|b$ alors pour tous $u, v \in \mathbb{Z}$, $d|(au + bv)$.

5/ Si $a|c$ et $b|d$ alors $ac|bd$, en particulier, si $a|b$ alors $a^n|b^n$ pour tout entier $n \geq 0$.

6/ Si $d \neq 0$ alors $a|b$ si et seulement si $ad|bd$.

2.2.2 Congruence

Définition 52.— *Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. On dit que "a est congru à b modulo n" et l'on note $a \equiv b \bmod(n)$ si $n|(b-a)$.*

Proposition 53.— *1/ Si $n \in \mathbb{N}^*$ alors la relation "être congru à modulo n" est une relation d'équivalence sur $\mathbb{Z}$.*

2/ Si $a \equiv b \bmod(n)$ et $c \equiv d \bmod(n)$ alors $a+c \equiv b+d \bmod(n)$ et $ac \equiv bd \bmod(n)$. (On dit que $+$ et $.$ sont compatibles pour la relation de congruence.)

2.2.3 Euclidienneté

Théorème 54.— *Soient $a, b \in \mathbb{Z}$ avec $b \neq 0$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leq r < |b|$.*

En particulier, l'anneau $\mathbb{Z}$ est euclidien par le stathme $|.|$.

Preuve : Unicité. Supposons que $a = bq + r = bq' + r'$ avec $0 \leq r, r' < |b|$. On a alors $r - r' = b(q - q')$ et donc $b|(r - r')$. Mais l'hypothèse faite sur r et r' implique que $-|b| < r - r' < |b|$. Le seul multiple de b dans cet intervalle est 0, donc $r = r'$ et par suite $q = q'$.

Existence. Supposons pour commencer que a et b sont positifs. Considérons l'ensemble $E = \{k \in \mathbb{Z} / \ a - bk \geq 0\}$, cet ensemble est non vide car $0 \in E$ et il est majoré (par a par exemple). Il possède donc un plus grand élément $q \in \mathbb{Z}$. Posons $r = a - bq$, si $r \geq b$ alors $a - (q+1)b \geq 0$, ce qui est contraire à la maximalité de q. Donc $a = bq + r$ avec $0 \leq r < b$.
Supposons maintenant $a \leq 0$ et $b < 0$. D'après le cas précédent, il existe q, r tels que $a = (-b)q + r$ et $0 \leq r < -b$. On a alors $a = b(-q) + r$ et $r < -b = |b|$.
Supposons pour finir $a < 0$ et b quelconque. D'après ce qui précède il existe q, r tels que $-a = bq + r$ et $0 \leq r < |b|$. On a donc $a = -bq - r$. Si $r \neq 0$ alors $a = b(\pm 1 - q) + (|b| - r)$ et $0 \leq |b| - r < |b|$.

□

Avec les notation du théorème, écrire $a = bq + r$ s'appelle effectuer la division euclidienne de a par b. L'entier q s'appelle le quotient de la division et r le reste.

Exercices : 1/ En considérant l'euclidienneté de $\mathbb{Z}$ pour le stathme $|.|$, combien de quotients et de restes existe-t-il pour un couple d'entiers $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$?

2/ Montrer que $a \equiv b \bmod(n)$ si et seulement les restes des divisions euclidiennes de a et b par n sont égaux.

Algortihme de la descente de Fermat On considère deux entiers positifs a et b avec $b \neq 0$. L'algorithme suivant, appelé "descente de Fermat", permet de trouver le reste et le quotient de la division euclidienne de a par b.

$r := a$
$q := 0$

Tant que $r \geq b$
Faire $r := r - b$, $q := q + 1$.

2.2.4 Nombres premiers et factorialité de $\mathbb{Z}$.

Définition 55.— *On appelle nombre premier, tout entier naturel qui possède exactement* 4 *diviseurs dans* $\mathbb{Z}$*. On note* $\mathcal{P}$ *l'ensemble des nombres premiers*

Lemme 56.— *Tout entier* $n \geq 2$ *est divisible par un nombre premier.*

Preuve : Si n est premier la proposition est vraie. Sinon il existe $1 < n_1 < n$ tel que $n_1 | n$. Si n_1 est premier la proposition est vraie, sinon il existe $1 < n_2 < n_1$ tel que $n_2 | n_1$. On recommence ce procédé et il existe un rang k tel que $n_k | n_{k-1} | ... | n_1 | n$ et n_k premier. En effet, sinon la suite $(n_k)_k$ que l'on obtiendrait serait une suite strictement décroissante d'entiers positifs, ce qui est impossible.

□

Corollaire 57.— (Théorème d'Euclide) *L'ensemble* $\mathcal{P}$ *est infini.*

Preuve : Supposons que $\mathcal{P}$ soit fini et notons $\{p_1, \cdots, p_n\} = \mathcal{P}$. Considérons l'entier $k = p_1 \cdots p_n + 1$. On a $k \geq 2$ et donc k est divisible par un nombre premier, donc par un p_i. Ceci n'étant visiblement pas le cas, on en déduit par l'absurde que $\mathcal{P}$ est infini.

Algorithmes de recherche de nombres premiers.

Crible d'Eratosthène : Le crible d'Eratosthène est un algorithme qui permet de trouver tous les nombres premiers compris entre 2 et un entier n fixé par avance.

• On écrit à la suite tous les entiers entre 2 et n.

• On entoure le nombre 2 et on barre tous les multiples de 2.

• On prend ensuite le premier nombre de la liste non barré et on l'entoure. On barre alors tous les multiples de ce nombre dans la liste.

• On recommence le procédé jusqu'à ce que tous les nombres soient soit barrés soit entourés. Les nombres entourés sont alors les nombres premiers compris entre 2 et n.

Un autre algorithme : Cet algorithme permet de lister les n premiers nombres premiers pour un entier n fixé. On utilise l'algorithme de division euclidienne (descente de fermat) et on crée une routine qui à deux entiers a et b associe $reste(a, b)$ le reste de la division euclidienne de a par b.

Créer un tableau $(u_1, \cdots, u_n)$ à n valeurs.
$u_1 := 2$.
$k := 1$
$h := 1$
Tant que $k \leq n$ Faire
    $h := h + 2$
    $i := 1$
    $v := 2006$
    Tant que $v \neq 0$ et que $u_i \leq \sqrt{h}$ et que $i < k$ Faire
        $v = reste(h, u_i)$ et $i := i + 1$

Si $v \neq 0$ Faire $k := k+1$ et $u_k := h$

Théorème 58.— (Théorème fondamental de l'arithmétique) *Tout entier naturel $n \geq 2$ s'écrit de façon unique, à l'ordre près des facteurs, comme produit de nombres premiers :*

$$n = p_1 \cdots p_r$$

avec $r \geq 1$ et p_i premier pour tout $i = 1, \cdots, r$.

Preuve : Montrons l'existence par récurrence. Pour $n = 2$, la propriété est claire. Pour $n \geq 2$ supposons la vraie pour les entiers de 2 à n.
Pour l'entier $n+1$ il existe un nombre premier p qui divise $n+1$. Si $(n+1)/p = 1$ alors $n+1 = p$ et la propriété est vraie, sinon $2 \leq (n+1)/p < n+1$ et par hypothèse de récurrence $(n+1)/p$ est produit de nombres premier et donc $(n+1) = p(n+1)/p$ aussi.

Montrons l'unicité par récurrence. Pour $n = 2$ si $2 = p_1 \cdots p_r$ avec $p_1, \cdots, p_r$ premiers. Comme $p_i \geq 2$ on a $2 \geq 2^r$ et donc $r = 1$ et par suite $p_1 = 2$. Il y a donc unicité. Pour $n-1 \geq 2$ supposons la propriété vraie pour tout entier compris entre 2 et $n-1$.
Pour l'entier n supposons que $n = p_1 \cdots p_r = q_1 \cdots q_s$ avec $p_1, \cdots, p_r, q_1, \cdots, q_s$ premiers. Distinguons deux cas :
1/ Un des p_i est égal à l'un des q_j, pour simplifier disons $p_1 = q_1$. On a donc $p_2 \cdots p_r = q_2 \cdots q_s$ et en utilisant l'hypothèse de récurrence on a $r = s$ et les p_i sont égaux aux q_j à l'ordre près.
2/ $p_i \neq q_j$ pour tout i et j. En particulier $p_1 \neq q_1$, disons $p_1 < q_1$. On a $s > 1$ sinon $n = q_1$ est premier et est divisible par p_1 qui est un entier différent de 1 et n ce qui est impossible. On a donc

$$0 < p_1 q_2 \cdots q_s < n = q_1 q_2 \cdots q_s$$

Considérons l'entier $m = n - p_1 q_2 \cdots q_s = (q_1 - p_1) q_2 \cdots q_s = p_1(p_2 \cdots p_r - q_2 \cdots q_s)$. On a $1 < m < n$ et donc, en utilisant l'hypothèse de récurrence, m possède une unique factorisation dans laquelle figure p_1. Comme p_1 est différent de $q_2, \cdots, q_s$ on en déduit que p_1 apparait dans la décomposition de $q_1 - p_1$ (qui est unique par hypothèse de récurrence). Ainsi p_1 divise $q_1 - p_1$, et donc $p_1 | q_1$ ce qui est absurde.

□

Si l'on note $(p_i)_i$ la suite (croissante) des nombres premiers on obtient alors : pour tout entier $x \in \mathbb{Z}^*$ il existe un unique $u \in \{-1, 1\}$ et une unique suite $(\alpha_i)_i \in \mathbb{N}^{\mathbb{N}}$ presque partout nulle telle que

$$x = u \prod_i p_i^{\alpha_i}$$

cette écriture s'appelle LA décompositon en facteurs premiers de l'entier x.

Exercice : Décrire un algorithme permettant de calculer la décomposition en facteurs premiers d'un entier.

Pour tout nombre premier p, disons $p = p_i$, l'entier $v_p(x) = \alpha_i$ s'appelle la valuation p-adique de x. Ainsi v_p est une application de $\mathbb{Z}^*$ dans $\mathbb{N}$. On l'étend à $\mathbb{Z}$ tout entier en posant $v_p(0) = +\infty$.

Proposition 59.— *1/ Soit p un nombre premier. Montrer que*

a) Pour tout $x \in \mathbb{Z}$, $v_p(x) = +\infty \iff x = 0$.

b) Pour tout $x, y \in \mathbb{Z}$, $v_p(xy) = v_p(x) + v_p(y)$.

c) Pour tout $x, y \in \mathbb{Z}$, $v_p(x+y) \geq \inf(v_p(x), v_p(y))$ *et il y a égalité dés que* $v_p(x) \neq v_p(y)$.

2/ Soient $x, y \in \mathbb{Z}^*$, *les propriétés suivantes sont équivalentes :*

i) $x|y$,

ii) $\forall p \in \mathcal{P}$, $v_p(x) \leq v_p(y)$.

Preuve : Exercice.

□

2.2.5 pgcd et ppcm

Etant donné deux entiers $a, b \in \mathbb{Z}^*$ on note $\mathscr{D}(\{a,b\})$ (resp. $\mathscr{M}(\{a,b\})$) l'ensemble des diviseurs (resp. multiples) communs de a et de b.

Définition 60.— *On appelle* pgcd *(resp.* ppcm*) de a et b tout entier* δ *(resp.* μ*) tel que*

$$\delta \in \mathscr{D}(\{a,b\}) \text{ et pour tout } d \in \mathscr{D}(\{a,b\}),\ d|\delta$$

resp.

$$\mu \in \mathscr{M}(\{a,b\}) \text{ et pour tout } m \in \mathscr{M}(\{a,b\}),\ \mu|m$$

Théorème 61.— *Soient* $a, b \in \mathbb{Z}$ *non tous les deux nuls. Les entiers a et b possèdent exactement deux* pgcd *(resp.* ppcm*) et ce sont des entiers opposés l'un de l'autre.*

Dans $\mathbb{Z}$ on appelle LE pgcd (resp. LE ppcm) de x et de y, celui des deux qui est positif. On le note $\text{pgcd}(x,y)$ (resp. $\text{ppcm}(x,y)$) ou parfois $x \wedge y$ (resp. $x \vee y$) ou encore (x,y).

Proposition 62.— *1/ Soient* $x, y \in \mathbb{Z}^*$, *l'ensemble des diviseurs (resp. des multiples positifs) communs de x et de y est un ensemble borné (resp. minoré). Le plus grand élément (resp. le plus petit élément) pour l'ordre usuel de cet ensemble est le* pgcd *(resp. le p.p.c.m) de x et de y.*

2/ Soient $x, y \in \mathbb{Z}^*$. *Posons* $d = \text{pgcd}(x,y)$ *et* $m = \text{ppcm}(x,y)$. *Pour tout nombre premier p on a* $v_p(d) = \min(v_p(x), v_p(y))$ *et* $v_p(m) = \max(v_p(x), v_p(y))$.

3/ Pour tout $x, y \in \mathbb{N}^*$, *on a* $xy = \text{pgcd}(x,y).\text{ppcm}(x,y)$.

4/ Pour tout $x, y, z \in \mathbb{Z}^*$ *on a*

a) (associativité)

$x \wedge (y \wedge z) = (x \wedge y) \wedge z$

$x \vee (y \vee z) = (x \vee y) \vee z$

b) (commutativité)

$x \wedge y = y \wedge x$

$x \vee y = y \vee x$

c) (distributivité)
$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

Preuve : Exercice.

□

L'associativité de $\wedge$ (resp. $\vee$) permet de définir la notion de pgcd (resp. ppcm) d'une famille finie d'entiers non nuls : si $x_1, \cdots, x_n \in \mathbb{Z}^*$ on pose $\text{pgcd}(x_1, \cdots, x_n) = x_1 \wedge \cdots \wedge x_n$ (resp. $\text{ppcm}(x_1, \cdots, x_n) = x_1 \vee \cdots \vee x_n$).

Proposition 63.— *Soient $x_1, \cdots, x_n \in \mathbb{Z}^*$.*

1/ L'ensemble des diviseurs (resp. des multiples positifs) communs des entiers x_i un ensemble borné (resp. minoré). Le plus grand élément (resp. le plus petit élément) pour l'ordre usuel de cet ensemble est le pgcd *(resp. le p.p.c.m) des entiers x_i.*

2/ Posons $d = \text{pgcd}(x_1, \cdots, x_n)$ et $m = \text{ppcm}(x_1, \cdots, x_n)$. Pour tout nombre premier p on a $v_p(d) = \min_i(v_p(x_i))$ et $v_p(m) = \max_i(v_p(x_i))$.

Preuve : Exercice.

□

Algorithme d'Euclide : L'algorithme d'Euclide repose sur le lemme suivant :

Lemme 64.— *Soit $a, b \in \mathbb{Z}^*$ et $a = bq + r$ la division euclidienne de a par b. Si $r \neq 0$ alors* $\text{pgcd}(a, b) = \text{pgcd}(b, r)$. *Si $r = 0$ alors* $\text{pgcd}(a, b) = b$.

Preuve : Exercice.

□

Soit (a, b) un couple d'entiers non nuls, $b \geq 1$. L'algorithme d'Euclide pour le couple (a, b) consiste à introduire deux suites finies $(r_n)_n$ et $(q_n)_n$ de la manière suivante :

• On pose $r_0 = b$ et on effectue la division euclidienne de a par r_0

$$a = q_1 r_0 + r_1$$

de quotient q_1 et de reste r_1.

• Tant que $r_n \neq 0$, on effectue la division euclidienne de r_{n-1} par r_n

$$r_{n-1} = q_{n+1} r_n + r_{n+1}$$

de quotient q_{n+1} et de reste r_{n+1}.

Il s'agit bien d'un l'algorithme, autrement dit il existe un entier $N = N(a, b) \in \mathbb{N}$, dépendant de a et de b, tel que $r_{N+1} = 0$. En effet si ce n'était pas le cas la suite $(r_n)_n$ serait une suite strictement décroissante d'entiers positifs, ce qui est impossible.

L'intéret principal de l'algorithme d'Euclide est que $r_N = \text{pgcd}(a, b)$ (exercice). On dit que le dernier reste non nul de l'algorithme d'Euclide est égal au pgcd.

Exercices : 1/ Donner un sens et une interprétation au pgcd d'une famille infinie d'entiers non nuls. Peut-on faire la même chose pour le ppcm?

2/ Décrire des algorithmes qui permettent de calculer le pgcd de deux entiers.

Définition 65.— *Deux entiers $a, b \in \mathbb{Z}^*$ sont dits premiers entre eux si, $(a, b) = 1$.*

Lemme 66.— *Soit $x, y \in \mathbb{Z}^*$. Les propriétés suivantes sont équivalentes :*

i) x et y sont premiers entre eux,

ii) $\forall p \in \mathcal{P}$, $v_p(x).v_p(y) = 0$.

Preuve : Exercice.

□

Proposition 67.— *a) Soient $a_1, \cdots, a_n$ des entiers non nuls. Si un entier a est premier avec chaque a_i, alors il est premier avec $a_1.\cdots.a_n$.*

b) Si d est un diviseur commun à deux entiers non nuls a et b, alors $(a/d, b/d) = (a, b)/d$. En particulier, les entier $a/(a, b)$ et $b/(a, b)$ sont premiers entre eux.

Preuve : Exercice.

□

Théorème 68.— (dit de Gauss) *Si $a, b, c \in \mathbb{Z}^*$ sont tels que $c|ab$ et $(a, c) = 1$ alors $c|b$.*

Preuve : Soit $p \in \mathcal{P}$. Comme $c|ab$ on a $v_p(c) \leq v_p(ab) = v_p(a) + v_p(b)$. Si $v_p(c) = 0$ alors $v_p(c) \leq v_p(b)$. Si $v_p(c) \neq 0$, comme a et c sont premier entre eux, on a $v_p(a) = 0$ et donc $v_p(c) \leq v_p(b)$. Dans tous les cas on a $v_p(c) \leq v_p(b)$, ce qui équivaut à $c|b$.

□

Corollaire 69.— *Si $a, b, c \in \mathbb{Z}^*$ sont tels que $a|c$, $b|c$ et $(a, b) = 1$ alors $ab|c$.*

Preuve : Exercice.

□

2.2.6 Sous-groupes de $\mathbb{Z}$ et théorème de Bezout.

Théorème 70.— *Pour tout $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$. Réciproquement, si G est un sous-groupe additif de $\mathbb{Z}$, il existe un unique entier naturel n tel que $G = n\mathbb{Z}$. En particulier, l'anneau $\mathbb{Z}$ est principal.*

Preuve : Le fait que $n\mathbb{Z}$ soit un groupe et que pour $n, m \geq 0$ on ait $n\mathbb{Z} = m\mathbb{Z} \Longleftrightarrow n = m$ est élémentaire.

Soit G un sous groupe additif de $\mathbb{Z}$. Si $G = \{0\}$ alors $G = n\mathbb{Z}$ avec $n = 0$. Sinon il existe un élément $a \in G$ non nul. Comme $-a \in G$, l'ensemble $G^+ = G \cap N^*$ est non vide et possède donc un plus petit élément n. Il est clair que $n\mathbb{Z} \subset G$. Soit $x \in G$ et $x = qn + r$ la division euclidienne de x par n. Puisque G est un groupe, on a $r = x - qn \in G$. Comme $r \geq 0$ et $r < n$ on a, par minimalité de n, $r = 0$. Ainsi $x = qn \in \mathbb{N}\mathbb{Z}$ et donc $G = n\mathbb{Z}$.

□

Proposition 71.— *Si x, y sont des entiers non nuls, alors $x|y$ si et seulement si $y\mathbb{Z} \subset x\mathbb{Z}$. En conséquence de quoi, si d (resp. m) est un entier naturel non nul, les propriétés suivantes*

i) $d = \text{pgcd}(x, y)$ (resp. $m = \text{ppcm}(x, y)$),

ii) $d\mathbb{Z} = x\mathbb{Z} + y\mathbb{Z}$ *(resp.* $m\mathbb{Z} = x\mathbb{Z} \cap y\mathbb{Z}$*),*

sont équivalentes.

Preuve : La première équivalence est évidente. Soit $d = \text{pgcd}(x, y)$. Comme $x\mathbb{Z} + y\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ différent de $\{0\}$ il existe $d' > 0$ tel que $x\mathbb{Z} + y\mathbb{Z} = d'\mathbb{Z}$. Comme $x\mathbb{Z} \subset d'\mathbb{Z}$ et $y\mathbb{Z} \subset d'\mathbb{Z}$, on a $d'|x$ et $d'|y$ et donc $d'|d$, c'est-à-dire $d\mathbb{Z} \subset d'\mathbb{Z}$. Maintenant comme $d|x$ et $d|y$ on a $x\mathbb{Z} \subset d\mathbb{Z}$ et $y\mathbb{Z} \subset d\mathbb{Z}$. On a donc $d'\mathbb{Z} = x\mathbb{Z} + y\mathbb{Z} \subset d\mathbb{Z}$. Ainsi $d'\mathbb{Z} = d\mathbb{Z}$, et par suite $d' = d$.

L'égalité $m\mathbb{Z} = x\mathbb{Z} \cap y\mathbb{Z}$ où $m = \text{ppcm}(x, y)$ est laissé en exercice.

□

Exercice : Redémontrer le théorème de Gauss en utilisant le théorème de Bezout.

Corollaire 72.— (Théorème de Bachet-Bezout) *Soit* $x, y \in \mathbb{Z}^*$*. Si* $d = \text{pgcd}(x, y)$*, alors il existe* $u, v \in \mathbb{Z}$ *tels que* $ux + vy = d$ *(Bezout). De plus, les propriétés suivantes sont équivalentes (Bachet) :*

i) x *et* y *sont premiers entre eux,*

ii) il existe $u, v \in \mathbb{Z}$ *tels que* $ux + vy = 1$.

Preuve : Soit $d = \text{pgcd}(x, y)$. D'après ce qui précède on a $x\mathbb{Z} + y\mathbb{Z} = d\mathbb{Z}$.
$i) \Longrightarrow ii)$ Si $d = 1$ alors $x\mathbb{Z} + y\mathbb{Z} = \mathbb{Z}$ et comme $1 \in \mathbb{Z}$ il existe bien $(u, v) \in \mathbb{Z}$ tel que $xu + yv = 1$.
$ii) \Longrightarrow i)$ S'il existe $u, v \in \mathbb{Z}$ tels que $ux + vy = 1$ alors $1 \in d\mathbb{Z}$ et donc $d = 1$.

□

Sur la recherche des couples de Bezout, application à la résolution de l'équation diophantienne linéaire $ax + by = c$**.**

On considère deux entiers a, b non nuls, $b \geq 1$. Le théorème de Bezout affirme qu'il existe un couple d'entiers $(u, v) \in \mathbb{Z}$ tels que $ua + vb = d$ où $d = \text{pgcd}(a, b)$. On s'intéresse à la recherche des tous les couples d'entiers (u, v) satisfaisant cette relation, ces couples sont appélés couples de Bezout de a et b. On suppose donné un de ces couples (u_0, v_0).

1er cas/ $d = 1$ (c'est-à-dire a et b premiers entre eux). Soit $(u, v) \in \mathbb{Z}^2$. On a

$$\begin{aligned}
au + bv = 1 &\iff \begin{cases} au + bv = 1 \\ au_0 + bv_0 = 1 \end{cases} \\
&\iff a(u - u_0) = b(v_0 - v) \\
&\iff \exists k \in \mathbb{Z},\ k = \frac{(u - u_0)}{b} = \frac{(v_0 - v)}{a} \text{ (par application du théorème de Gauss)} \\
&\iff \exists k \in \mathbb{Z}, \begin{cases} u = u_0 + bk \\ v = v_0 - ak \end{cases}
\end{aligned}$$

Il y a donc une infinité de couples de Bezout, ce sont les couples de la forme $(u_0 + bk, v_0 - ak)$ pour k parcourant $\mathbb{Z}$.

2ème cas/ $d \neq 1$. On se ramène au cas précédent en remarquant que $ua + vb = d$ si et seulement si $ua' + vb' = 1$ avec $a' = a/d$ et $b' = b/d$. Les couples de Bezout sont donc les couples de la forme $\left(u_0 + \frac{b}{d}k, v_0 - \frac{a}{d}k\right)$ avec $k \in \mathbb{Z}$.

On sait donc trouver les couples de Bezout, modulo le fait que l'on sache en trouver un. Une manière pratique pour y arriver consiste à utiliser l'algorithme d'Euclide. On écrit la suite de divisions euclidiennes

$$\begin{array}{lcl} a & = & bq_0 + r_0 \\ b & = & r_0 q_1 + r_1 \\ r_0 & = & r_1 q_2 + r_2 \\ & \vdots & \\ r_{n-2} & = & r_{n-1} q_n + d \\ r_{n-1} & = & r_n q_{n+1} \end{array}$$

On exprime, grâce à la première équation, r_0 en fonction de a et de b : $r_0 = a - bq_0$ et on injecte cette expression dans la deuxième équation : $b = (a - bq_0)q_1 + r_1$. On recommence avec r_1 puis avec tous les r_i jusqu'à $r_n = d$ et on obtient d en fonction d'une combinaison entière de a et de b.

Par exemple, recherchons les couples de Bezout pour le couple $(a, b) = (-91, 56)$. Commençons par chercher $d = \text{pgcd}(-91, 56)$. Utilisons l'algorithme d'Euclide :

$-91 = -2.56 + 21$
$56 = 2.21 + 14$
$21 = 1.14 + 7$
$14 = 2.7$

On a donc $\text{pgcd}(-91, 56) = d = 7$. Cherchons un couple de Bezout particulier en utilisant l'algorithme d'Euclide : $21 = 1.(-91) + 2.56$, $14 = -2.(-91) - 3.56$, $7 = 3.(-91) + 5.56$. Ainsi $(u_0, v_0) = (3, 5)$ est un couple de Bezout. L'étude précédente montre que les couples de Bezout de $(-91, 56)$ sont donc les $(3 + 8k, 5 + 13k)$ pour $k \in \mathbb{Z}$.

On considère trois entiers non nuls $a, b, c \in \mathbb{Z}^*$ et on cherche à résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation $ax + by = c$. On note d le pgcd de a et b.

1er cas/ c n'est pas un multiple de d. L'équation n'a pas de solution. En effet, les entiers $ax + by$, quand x et y parcourent $\mathbb{Z}$, décrivent exactement le sous-groupe $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Ces entiers sont donc tous divisibles pas d, ce qui n'est pas le cas de c.

2eme cas/ $c = hd$. Un couple $(x, y) \in \mathbb{Z}^2$ satisfait $ax + by = c$ si et seulement si $a'x + b'y = h$ avec $a' = a/d$ et $b' = b/d$. Les entiers a' et b' sont premiers entre eux. D'après ce qui précède, on sais trouver (x'_0, y'_0) tel que $a'x'_0 + b'y'_0 = 1$. On en déduit que $(x_0, y_0) = (hx'_0, hy'_0)$ est solution de l'équation. On a alors, pour un couple $(x, y) \in \mathbb{Z}^2$:

$$\begin{array}{lcl} ax + by = c & \iff & a'x + b'y = h \\ & \iff & \left\{ \begin{array}{l} a'x + b'y = h \\ a'x_0 + b'y_0 = h \end{array} \right. \\ & \iff & a'(x - x_0) = b'(y_0 - y) \\ & \iff & \exists k \in \mathbb{Z},\ k = \dfrac{(x - x_0)}{b'} = \dfrac{(y_0 - y)}{a'} \text{ (par application du théorème de Gauss)} \\ & \iff & \exists k \in \mathbb{Z},\ \left\{ \begin{array}{l} x = x_0 + b'k \\ y = y_0 - a'k \end{array} \right. \end{array}$$

Les solutions de l'équation sont donc les couples de la forme $\left(x_0 + b^{'}k, y_0 - a^{'}k\right)$ avec k parcourant $\mathbb{Z}$.

Théorème 73.— (dit des restes chinois) *Soient $a_1, \cdots, a_n \geq 2$ des entiers premiers entre eux deux à deux. Pour tout $\lambda_1, \cdots, \lambda_n \in \mathbb{Z}$, le système de congruences*

$$(S)\begin{cases} x \equiv \lambda_1 \bmod(a_1) \\ \vdots \\ x \equiv \lambda_n \bmod(a_n) \end{cases}$$

admet des solutions. Si x_0 est solution de (S) alors l'ensemble des solutions de (S) est donné par

$$\{x_0 + ka/\ k \in \mathbb{Z}\}$$

où $a = a_1.\cdots.a_n$. En particulier, il y a une unique solution de (S) modulo a.

Preuve : Pour tout $i = 1, \cdots, n$, on pose $\widehat{a_i} = \dfrac{a}{a_i}$. Puisque les a_j sont premiers entre eux deux à deux, les entiers a_i et $\widehat{a_i}$ sont donc premiers entre eux, et, d'après Bezout, il existe $u_i, v_i \in \mathbb{Z}$ tels que $u_i\widehat{a_i} + v_i a_i = 1$. On a alors $u_i\widehat{a_i} \equiv 1 \bmod(a_i)$ et $u_i\widehat{a_i} \equiv 1 \bmod(a_j)$ pour $j \neq i$. L'entier

$$x_0 = \sum_{i=1}^{n} \lambda_i u_i \widehat{a_i}$$

est alors visiblement solution de (S). Si x désigne une autre solution de (S), alors $x - x_0 \equiv 0 \bmod(a_i)$ pour tout $i = 1, \cdots, n$, c'est-à-dire $a_i | (x - x_0)$. Puisque les a_i sont premiers entre eux deux à deux, on en déduit finalement que $a|(x - x_0)$ et donc qu'il existe $k \in \mathbb{Z}$ tel que $x = x_0 + ka$. Réciproquement, pour tout $k \in \mathbb{Z}$, l'entier $x = x_0 + ka$ est visiblement solution de (S).

□

3 L'anneau $\mathbb{Z}/n\mathbb{Z}$

3.1 Structure de $\mathbb{Z}/n\mathbb{Z}$

On se donne un entier $n \geq 1$ et l'on considère la relation (d'équivalence) de congruence modulo n, $\mathcal{R}_n$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient $\mathbb{Z}/\mathcal{R}_n$ et pour tout entier $k \in \mathbb{Z}$, on note $\overline{k}$ la classe d'équivalence de k modulo $\mathcal{R}_n$.

Proposition 74.— *Le cardinal de $\mathbb{Z}/n\mathbb{Z}$ vaut n et l'on a $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \cdots, \overline{n-1}\}$.*

Pour $a, b \in \mathbb{Z}$ la classe $\overline{a+b}$ ne dépend que des classes $\overline{a}$ et $\overline{b}$ (exercice). Ainsi, la relation $\overline{a+b} = \overline{a} + \overline{b}$ définit une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$ que l'on note improprement $+$. De même la classe $\overline{ab}$ ne dépend que des classes $\overline{a}$ et $\overline{b}$ et la relation $\overline{a+b} = \overline{a} + \overline{b}$ définit une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$ que l'on note improprement $.$

Proposition 75.— *Muni des lois $+$ et $.$ ci-dessus définies, $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif et unitaire.*

Notation : Si $a \in \mathbb{Z}$ et $n \geq 1$, on pose $n.\overline{a} = \overline{a} + \cdots + \overline{a}$ (n fois). On voit alors que $n.\overline{a} = \overline{n}.\overline{a} = \overline{na}$.

Proposition 76.— *Soient $n \in \mathbb{N}^*$, et $k \in \mathbb{Z}$. Les propositions suivantes sont équivalentes :*

i) $\overline{k}$ engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$ (i.e. pour tout $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$, il existe $a \in \mathbb{N}$ tel que $a.\overline{k} = \overline{k} + \cdots \overline{k} = \overline{x}$),

ii) k est premier avec n,

iii) $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^*$,

iv) $\overline{k}$ n'est pas un diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$.

Preuve :

$ii) \Rightarrow iii)$ D'après Bezout, il existe $u, v \in \mathbb{Z}$ tel que $uk + vn = 1$, on a donc

$$\overline{1} = \overline{uk + vn} = \overline{u}.\overline{k} + \overline{v}.\overline{n} = \overline{u}.\overline{k}$$

et, par suite, $k \in (\mathbb{Z}/n\mathbb{Z})^*$.

$iii) \Rightarrow iv)$ Evident.

non $ii) \Rightarrow$ *non* $iv)$ Soit $d = \text{pgcd}(n,k) > 1$ et $a = n/d$, $b = k/d$. On a $0 < a < n$ et donc $\overline{a} \neq \overline{0}$, et alors $\overline{a}.\overline{k} = \overline{n}.\overline{b} = \overline{0}$ et donc $\overline{k}$ est un diviseur de zéro.

$i) \Rightarrow iii)$ Par hypothèse, pour tout $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$, il existe un entier a tel que $a.\overline{k} = \overline{x}$. Pour $x = 1$, on a donc l'existence de a tel que $\overline{ak} = a.\overline{k} = \overline{1}$ et donc $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^*$.

$iii) \Rightarrow i)$ Par hypothèse, il existe $x \in \mathbb{Z}$ tel que $\overline{xk} = \overline{1}$. Pour $y \in \mathbb{Z}$, on a donc

$$xy.\overline{k} = \overline{xy}\ \overline{k} = \overline{x}\ \overline{y}\ \overline{k} = \overline{y}$$

et donc $\overline{k}$ engendre bien $\mathbb{Z}/n\mathbb{Z}$.

□

Corollaire 77.— *Soit $n \in \mathbb{N}^*$, les propositions suivantes*

i) n est premier,

ii) $\mathbb{Z}/n\mathbb{Z}$ est un corps,

iii) $\mathbb{Z}/n\mathbb{Z}$ est intègre,

sont équivalentes.

Les éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ sont exactement les générateurs du groupe additif $\mathbb{Z}/n\mathbb{Z}$. On note $\varphi(n)$ leur nombre. La fonction $n \mapsto \varphi(n)$ s'appelle la *fonction indicatrice d'Euler*.

Proposition 78.— *Pour $n \geq 1$, on note $E(n) = \{k \in \{1, \cdots, n-1\} / (k,n) = 1\}$. On a alors $\varphi(n) = \sharp E(n)$.*

Corollaire 79.— *Soit $n \in \mathbb{N}^*$.*

a) On a $o(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n)$ (fonction indicatrice d'Euler).

b) (Théorème d'Euler) Si $a \in \mathbb{Z}$ est premier avec n, alors $a^{\varphi(n)} \equiv 1\ (n)$.

c) (Théorème de Fermat) Si p est un nombre premier et si $a \in \mathbb{Z}$ n'est pas divisible par p alors $a^{p-1} \equiv 1\ (p)$.

Preuve : a) Immédiat.

b) Si a est premier à n alors $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})*$ qui est un groupe d'ordre $\varphi(n)$. Le théorème de Lagrange assure alors que $\overline{a}^{\varphi(n)} = \overline{1}$ c'est-à-dire que $a^{\varphi(n)} \equiv 1\ (n)$.

c) C'est le b) pour $n = p$ premier.

□

Théorème 80.— *Soit $a, b \in \mathbb{N}^*$ deux entiers premiers entre eux. L'application*

$$f : \mathbb{Z}/ab\mathbb{Z} \longrightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

qui à la classe d'un entier $x \in \mathbb{Z}$ modulo ab associe le couple des classes de l'entier x modulo a (resp. modulo b) est un isomorphisme d'anneaux.

Preuve : C'est une conséquence immédiate du théorème des restes chinois, compte tenu du fait que, puisque a et b sont premier entre eux, d'après Bezout on a $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$.

□

Corollaire 81.— *Soit $n \in \mathbb{N}^*$ et $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ le décomposition en facteurs premiers de n. il existe un isomorphisme d'anneaux*

$$f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$$

3.2 Calcul de $\varphi(n)$

Théorème 82.— *L'indicateur d'Euleur, φ, est une fonction arithmétique simplement multiplicative, c'est-à-dire que si $n, m \in \mathbb{N}^*$ sont premiers entres eux alors $\varphi(nm) = \varphi(n)\varphi(m)$.*

Preuve : Remarquons pour commencer que si $(\overline{x}, \overline{y}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est un générateur de ce groupe, alors $\overline{x}$ en est un de $\mathbb{Z}/n\mathbb{Z}$ et $\overline{y}$ en est un de $\mathbb{Z}/m\mathbb{Z}$. En effet, si ce n'est pas le cas, disons par exemple que $< \overline{x} > \neq \mathbb{Z}/n\mathbb{Z}$ alors il existe $\overline{z} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{z} \neq k\overline{x}$ pour tout $k \in \mathbb{Z}$, il s'ensuit que $(\overline{z}, 0) \neq k(\overline{x}, y)$ pour tout $k \in \mathbb{Z}$ et donc que $< (\overline{x}, \overline{y}) > \neq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Réciproquement, soit $\overline{x}$ un générateur de $\mathbb{Z}/n\mathbb{Z}$ et $\overline{y}$ un générateur de $\mathbb{Z}/m\mathbb{Z}$. Soit $k, k' \in \mathbb{Z}$, il s'agit de montrer qu'il existe $a \in \mathbb{Z}$ tel que $a(\overline{x}, \overline{y}) = (k\overline{x}, k'\overline{y})$. D'après Bezout, puisque n et m sont premier entre eux, il existe $u, v, u', v' \in \mathbb{Z}$ tels que

$$\begin{aligned} k &= un + vm \\ k' &= u'n + v'm \end{aligned}$$

On a donc $\alpha n + k = \alpha' m + k'$ avec $\alpha = u' - u$ et $\alpha' = v - v'$. Notons a cet entier, on a alors

$$\begin{aligned} a(\overline{x}, \overline{y}) &= (\overline{ax}, \overline{ay}) = (\overline{\alpha nx + kx}, \overline{\alpha' my + k'y}) \\ &= (\overline{kx}, \overline{k'y}) = (k\overline{x}, k'\overline{y}) \end{aligned}$$

et donc $(\overline{x}, \overline{y})$ est bien un générateur de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

En conclusion, il existe une bijection entre l'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et le produit cartésien des ensembles de générateurs de $\mathbb{Z}/n\mathbb{Z}$ et de $\mathbb{Z}/m\mathbb{Z}$. La formule

annoncée en découle alors, compte tenu du fait qu'il y a une bijection entre les générateurs de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et ceux de $\mathbb{Z}/nm\mathbb{Z}$ puisque ces deux groupes sont isomorphes.

□

Lemme 83.— *Soit p un nombre premier et $\alpha \geq 1$ un entier, on a*

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1)$$

Preuve : Il s'agit de dénombrer le nombre d'entiers de $\{1, \cdots, p^\alpha\}$ premier à p^α, donc à p puisque p est premier. Les entiers de $\{1, \cdots, p^\alpha\}$ qui ne sont pas premiers à p sont exactement les pk avec $k \in \{1, \cdots, p^{\alpha-1}\}$, il y en a donc $p^{\alpha-1}$. Par suite on a $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$.

□

Théorème 84.— *Soit $n \geq 2$ un entier et $n = p_1^{\alpha_1}.\cdots.p_k^{\alpha_k}$ sa décomposition en facteurs premiers, on a*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

Preuve : Exercice.

□

On dispose donc d'un moyen simple pour calculer $\varphi(n)$ dés que l'on connait la décomposition en facteurs premiers de l'entier n. Jusqu'à l'ordre 49 on trouve :

n	$\varphi(n)$	n	$\varphi(n)$	n	$\varphi(n)$	n	$\varphi(n)$	n	$\varphi(n)$
		10	4	20	8	30	8	40	16
1	1	11	10	21	12	31	30	41	40
2	1	12	4	22	10	32	16	42	12
3	2	13	12	23	22	33	20	43	42
4	2	14	6	24	8	34	16	44	20
5	4	15	8	25	20	35	24	45	24
6	2	16	8	26	12	36	12	46	22
7	6	17	16	27	18	37	36	47	46
8	4	18	6	28	12	38	18	48	16
9	6	19	18	29	28	39	24	49	42

3.3 Etude de $(\mathbb{Z}/n\mathbb{Z})^*$

Proposition 85.— *Soit $n, m \in \mathbb{N}^*$. L'épimorphisme naturel d'anneaux*

$$f : \mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

qui à une classe modulo nm associe son unique classe modulo n, induit, par restriction, un épimorphisme de groupe

$$\tilde{f} : (\mathbb{Z}/nm\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$$

Preuve : Il est clair que $f((\mathbb{Z}/nm\mathbb{Z})^*) \subset (\mathbb{Z}/n\mathbb{Z})^*$ et comme f est un morphisme d'anneau, sa restriction $\tilde{f}$ est bien un morphisme de groupes multiplicatifs. Ce qu'il faut donc montrer

c'est la surjectivité de $\tilde{f}$. Etant donné un entier $k \in \mathbb{Z}$ premier avec n, il s'agit de trouver un entier $l \in \mathbb{Z}$ premier avec nm tel que $l = k + rn$ avec $r \in \mathbb{Z}$. On vérifie alors que l'entier

$$l = k + n \prod_{p \text{ premier, } p \leq nm, \ p \not| k} p$$

convient.

□

Théorème 86.— *Si K désigne un corps commutatif, tout sous-groupe fini Γ de $(K^*, .)$ est cyclique.*

Preuve: Si $x \in \Gamma$, pour tout $n \in \mathbb{N}$, $x^n \in \Gamma$. Γ étant fini, pour tout $x \in \Gamma$, il existe $n \in \mathbb{N}$ tel que $x^n = 1$ (n est l'ordre de x dans Γ). Considérons un élément $\alpha \in \Gamma$ d'ordre maximal N (i.e. si $x \in \Gamma$ est d'ordre n, alors $n \leq N$). Nous allons montrer que α génère Γ.

Soit $\beta \in \Gamma$ d'ordre n. Supposons que n ne divise pas N, il existe donc un nombre premier p et un entier e tel que p^e divise n et p^e ne divise pas N. Soit $f < e$ l'entier tel que $p^f | N$ et $p^{f+1} \not| N$. Considérons alors $\gamma = \alpha^{p^f} \beta^{n/p^e}$, l'ordre de α est N/p^f et celui de β^{n/p^e} est p^e, or p^e et N/p^f sont premiers entre eux, donc l'ordre de γ vaut $p^e.(N/p^f) > N$ (en effet, si a et b sont deux éléments d'un groupe abélien d'ordres respectifs s et t premiers entres eux alors l'ordre $o \leq p.p.c.m(s,t)$ de ab vérifie $a^o = b^{-o}$ et par suite $a^{os} = 1 = b^{-os}$ ce qui implique $t|os$ et donc $t|o$. De même, on a $s|ot$ et donc $s|o$, donc $p.p.c.m(s,t)|o$ et donc $o = p.p.c.m(s,t) = st$). Par conséquent γ a un ordre strictement plus grand que celui de α ce qui est absurde par hypothèse. Donc n divise N.

L'équation $X^n = 1$ a pour solution dans Γ les $\alpha^{k\frac{N}{n}}$ pour $k = 0, \cdots n-1$. Or β est solution de cette équation, donc il existe $k \in \{0, \cdots, n-1\}$ tel que $\beta = \alpha^{k\frac{N}{n}}$. Ainsi Γ est cyclique.

□

Corollaire 87.— *Si p désigne un nombre premier alors*

$$\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \simeq \frac{\mathbb{Z}}{(p-1)\mathbb{Z}}$$

est un groupe cyclique d'ordre $p-1$.

Preuve: Immédiat, compte tenu du fait que, puisque p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps.

□

Lemme 88.— *Soit p un nombre premier impair et $k \geq 2$ un entier. On a*

$$(1+p)^{p^{k-2}} \equiv 1 + p^{k-1} \ (p^k)$$

Preuve: Par récurrence sur $k \geq 2$. Pour $k = 2$ la proposition est claire, supposons la vraie pour $k \geq 2$, il existe donc $\alpha \in \mathbb{Z}$ tel que

$$(1+p)^{p^{k-2}} = 1 + p^{k-1} + \alpha p^k$$

On a donc

$$\begin{aligned}(1+p)^{p^{k-1}} &= (1+p^{k-1}+\alpha p^k)^p \\ &= \sum_{i=0}^{p} C_p^i p^{i(k-1)}(1+\alpha p)^i \\ &= 1+p^k+\alpha p^{k+1}+\sum_{i=2}^{p} C_p^i p^{i(k-1)}(1+\alpha p)^i\end{aligned}$$

et par suite

$$(1+p)^{p^{k-1}} = 1+p^k+\beta p^{k+1}$$

avec $\beta = \alpha + \sum_{i=2}^{p} C_p^i p^{i(k-1)-(k+1)}(1+\alpha p)^i \in \mathbb{Z}$. En effet, pour $i \geq 3$ on a $(i-1)k-(i+1) \geq 0$ puisque $k \geq 2$. pour $i = 2$, comme $p \geq 3$ est premier, on a $p|C_p^2$ et donc $C_p^2 p^{k-3} \in \mathbb{Z}$.

□

Théorème 89.— *Soit p un nombre premier impair et $k \geq 1$ un entier. L'anneau*

$$\left(\frac{\mathbb{Z}}{p^k\mathbb{Z}}\right)^* \simeq \frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \times \frac{\mathbb{Z}}{p^{k-1}\mathbb{Z}}$$

est cyclique d'ordre $(p-1)p^k$.

Preuve : D'après le lemme précédent, on a $(1+p)^{p^{k-2}} \equiv 1+p^{k-1}\ (p^k)$ et donc

$$(1+p)^{p^{k-1}} \equiv 1\ (p^k)$$

Ceci montre que $a = \overline{1+p}$ est d'ordre p^{k-1} dans $(\mathbb{Z}/p^k\mathbb{Z})^*$. Considérons un entier $x \in \mathbb{Z}$ tel que la classe de x modulo p engendre le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ (qui est cyclique d'après ce qui précède). Comme $p \not| x$, on a $\overline{x} \in (\mathbb{Z}/p^k\mathbb{Z})^*$. Soit ω l'ordre de $\overline{x}$. On a $x^\omega \equiv 1(p^k)$, donc, à fortiori, $x^\omega \equiv 1(p)$ et donc ω est un multiple non nul de $p-1$, disons $\omega = r(p-1)$ avec $r \geq 1$.

Posons $b = \overline{x}^r$. L'élément b est d'ordre $p-1$ et comme p^{k-1} et $p-1$ sont premiers entre eux (puisque p est premier), on en déduit que l'élément ab est d'ordre $(p-1)p^{k-1} = \varphi(p^k) = o((\mathbb{Z}/p^k\mathbb{Z})^*)$. Ainsi, $(\mathbb{Z}/p^k\mathbb{Z})^*$ est bien un groupe cyclique.

□

Lemme 90.— *Soit $k \geq 4$ un entier. On a*

$$3^{2^{k-3}} \equiv 1+2^{k-1}\ (2^k) \text{ et } 3^{2^{k-2}} \equiv 1\ (2^k)$$

Preuve : Exercice.

□

Théorème 91.— *Soit $k \geq 2$ un entier. On a*

$$\left(\frac{\mathbb{Z}}{2^k\mathbb{Z}}\right)^* \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^{k-2}\mathbb{Z}}$$

Preuve : Pour $k = 2, 3$ le résultat se vérifie facilement.

Supposons que $k \geq 4$, le lemme précédent assure que $a = \overline{3}$ est un élément de $(\mathbb{Z}/2^k\mathbb{Z})^*$ d'ordre 2^{k-2}. Considérons les éléments $b = \overline{2^{k-1} - 1}$ et $c = \overline{2^{k-1} + 1}$. On a $b^2 = \overline{2^{2k-2} - 2^k + 1} = \overline{1}$ et $c^2 = \overline{2^{2k-2} + 2^k + 1} = \overline{1}$. Ainsi, b et c sont deux éléments distincts de $(\mathbb{Z}/2^k\mathbb{Z})^*$ d'ordre 2.

Comme $< a >$ est cyclique d'ordre 2^{k-2}, il ne contient qu'un seul élément d'ordre 2. Ainsi, au moins un des deux éléments b ou c n'est pas dans $< a >$. On a donc $< a > \cap < b >= \{\overline{0}\}$ ou $< a > \cap < c >= \{\overline{0}\}$ et par suite

$$(\mathbb{Z}/2^k\mathbb{Z})^* =< a > \oplus < b > (\text{ou } < c >) \simeq \mathbb{Z}/2^{k-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

puisque $o((\mathbb{Z}/2^k\mathbb{Z})^*) = \varphi(2^k) = 2^{k-1}$.

□

Décomposition de $(\mathbb{Z}/n\mathbb{Z})^*$ **:** Soit $n \in \mathbb{N}^*$ et $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ sa décomposition en facteurs premier, compte tenu du fait que

$$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* \simeq \left(\frac{\mathbb{Z}}{p_1^{\alpha_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p_k^{\alpha_k}\mathbb{Z}}\right)^* \simeq \left(\frac{\mathbb{Z}}{p_1^{\alpha_1}\mathbb{Z}}\right)^* \times \cdots \times \left(\frac{\mathbb{Z}}{p_k^{\alpha_k}\mathbb{Z}}\right)^*$$

on en déduit, avec ce qui précède, une décomposition en groupes cycliques de $(\mathbb{Z}/n\mathbb{Z})^*$. Par exemple :

- $n = 50 = 2.5^2$, on a $\left(\frac{\mathbb{Z}}{50\mathbb{Z}}\right)^* \simeq \frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}} \simeq \frac{\mathbb{Z}}{20\mathbb{Z}}$.
- $n = 24 = 2^3.3$, on a $\left(\frac{\mathbb{Z}}{24\mathbb{Z}}\right)^* \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$.

3.4 Le cryptosystème R.S.A.

La cryptographie (du grec $\kappa\rho\upsilon\pi\tau o\varsigma$: recouvert, caché, secret et $\gamma\rho\alpha\varphi\omega$ écrire) est l'étude des méthodes pour envoyer des messages sous forme cachée de sorte que seuls les destinataires puissent lire ces messages.

Les messages à envoyer seront appelés les "messages lisibles" et les messages cachés seront appelés "les messages encryptés". Le processus pour passer des messages lisibles au messages encryptés s'appelle l'encryptage, le processus inverse s'appelle le décryptage. Les messages lisibles et encryptés sont écrits dans un certain alphabet (pas forcément le même) consistants en un certain nombre de symboles appelés "lettres" : A,B,o,?,. etc. Les messages lisibles et encryptés sont saucissonés en blocs appelés messages unitaires.

Si $\mathcal{P}$ désigne l'ensemble des messages lisibles et $\mathcal{C}$ l'ensemble des messages cryptés, on appelle fonction d'encryptage, toute application $f : \mathcal{P} \longrightarrow \mathcal{C}$ bijective. La fonction de décryptage associée à f est alors sa réciproque f^{-1}. La donnée d'un tel shéma est appelé cryptosystème.

Exemple 92.— On choisit un alphabet à N lettres et une correspondance numérique entre des lettres de cet alphabet et les entiers $\{0, \cdots, N-1\}$. On choisit alors un entier $b \in \mathbb{Z}$ et on définit la fonction d'encryptage f par : pour une lettre donnée de correspondance

numérique P, on pose $f(P) = P + b \ mod(N)$ (on choisit pour $f(P)$ son représentant dans $\{0, \cdots, N-1\}$. Ainsi pour $N = 26$ et $b = 3$ (cryptosystème de Jules César avec la correspondance $A = 0, B = 1$ etc.), on obtient

$$f(P) = \begin{cases} P + 3, & si\ x \leq 23 \\ P - 23, & si\ x \geq 23 \end{cases}$$

et ainsi le message lisible $P = HUM$ s'encrypte KXP.

Par définition, un cryptosystème à clé publique est un cryptosystème $f : \mathcal{P} \longrightarrow \mathcal{C}$ dont la fonction d'encryptage est facile a calculer mais dont la fonction de décryptage f^{-1} est dans la pratique incalculable sans une information supplémentaire. Une telle fonction f est appelée fontion "trappe".

Dans la pratique un groupe d'utilisateurs se mettent d'accord sur $\mathcal{P}$ et $\mathcal{C}$ et chaque utilisateur E choisi une fontion trappe f_E (que l'on appelle la clé publique de E) qu'il publie à tous et garde secret l'information K_E (appelée clé secrete) qui permet à E et à lui seul de calculer efficacement f_E^{-1}. Ainsi tout utilisateur peut envoyer à E un message par f_E, mais seul E peut dans la pratique décrypter ce message.

Ce principe pose un problème d'authentification important, car si l'on est sur que seul le destinataire peut lire les messages qui lui sont envoyé, comment assurer (puisque tout le monde connait les fonctions d'encryptages de tout le monde) que l'expéditeur est bien celui qu'il prétend être? Un moyen simple d'authentification est le suivant. Si A et B ont des clés publiques respectives f_A et f_B et que A envoit un message à B qu'il veut signer par son nom m. A envoit alors à B le message $M = f_A^{-1}(f_B(m))$ (qu'il peut calculer car il connait f_A^{-1} et f_B). Seul A peut envoyer un tel message, car seul A connait f_A^{-1}, ce qui authentifie son message. Seul B peut décrypter ce message en faisant $f_B^{-1}(f_A(M))$ car seul B connait f_B^{-1}. Ceci assure que seul B pourra connaitre l'expéditeur du message qui lui est adressé.

En 1978 les mathématiciens Rivest, Shamir et Adlemann ont proposé un cryptosystème particulièrement performant qui repose sur l'arithmétique de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Ce cryptosystème, appelé communément R.S.A., repose sur l'idée directrice suivante : un groupe d'utilisateurs veulent s'envoyer des messages cryptés. Chaque utilisateur A choisit un groupe abélien G_A connu de tous mais dont seul A connait l'ordre h_A. Il choisit un entier n_A premier avec h_A et publie sa clef publique (G_A, n_A). Il calcule secrêtement (par exemple grace à l'algorithme d'euclide) un entier s_A qui est un inverse de n_A modulo h_a (i.e. $s_A n_A \equiv 1(h_A)$). L'utilisateur A est le seul à connaitre h_A et s_A.

Pour envoyer un message crypté $m \in G_A$ à A, un utilisateur envoit à A le message $m' = m^{n_A}$. Pour décoder le message, A calcule alors $m'^{s_A} = m^{s_A n_A} = m^{kh_A+1} = m$. La fiabilité de ce principe de cryptosystème repose sur le postulat que dans le groupe G_A choisi, connaissant m^{n_A} et n_A il est trés difficile de retrouver m.

Le cryptosystème R.S.A. utilise le groupe multiplicatif de $\mathbb{Z}/n\mathbb{Z}$. Chaque utilisateur A choisit deux nombres premiers distincts p et q (grands) et calcule $n = pq$. Il calcule en secret $\varphi(n) = (p-1)(q-1)$ et choisit un entier a premier avec $\varphi(n)$ et calcul un inverse s_a de a modulo $\varphi(n)$. Il publie sa clé publique : (n, a). Pour envoyer un message $m \neq 0 \in \mathbb{Z}/n\mathbb{Z}$ à A, on envoit $m' = m^a$. A décode alors le message en calculant m'^{s_a} en effet, deux cas se présentent :

• Premier cas $m \in (\mathbb{Z}/n\mathbb{Z})^*$: L'ordre du groupe $(\mathbb{Z}/n\mathbb{Z})^*$ étant $\varphi(n)$ et comme $s_a = k\varphi(n) + 1$ avec $k \in \mathbb{Z}$, on a $m'^{s_a} = m^{as_a} = m^{k\varphi(n)+1} = m$.

• Deuxième cas $m \notin (\mathbb{Z}/n\mathbb{Z})^*$: m n'est alors pas premier avec $n = pq$ donc pas premier avec p ou q. Supposons que m ne soit pas premier avec p, il est alors premier avec q, sinon m est mutilple de pq et donc vaut 0 dans $\mathbb{Z}/n\mathbb{Z}$. Considérons l'isomorphisme canonique

$$\theta : \mathbb{Z}/pq\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

qui à m associe le couple (m_p, m_q) où m_p et m_q désigne la classe de m modulo p et q. Comme m est divisble par p, on a $m_p = 0$ et comme m est premier avec q on a $m_q \in (\mathbb{Z} : q\mathbb{Z})^*$ et par suite $m_q^{q-1} = 1$. On a alors

$$\theta(m^a s_a) = (m_p^{as_a}, m_q^{as_a}) = (0, {m_q}^{k(p-1)(q-1)+1}) = (0, m_q) = \theta(m)$$

Comme θ est un isomorphisme on a $m = m^{as_a} = {m'}^{s_a}$.

La fiabilité de R.S.A. repose sur deux hypothèses :

1/ Il est considéré que dans $\mathbb{Z}/n\mathbb{Z}$, résoudre l'équation en x : $x^a = y$, connaissant a et y, est quelque chose de trés difficile voire impossible quand n est grand.

2/ Une fois connu n, la connaissance de $\varphi(n)$ équivaut à la connaissance de p et q. Donc algorithmiquement parlant, le connaissance de $\varphi(n)$ équivaut à trouver la décomposition en facteurs premiers de n et cette dernière opération est réputée être infaisable dans la pratique quand p et q sont grands.

Dans la pratique, un ensemble d'utilisateurs choisit un alphabet $A, B, \cdots, Z, 0, \cdots, 9, ., ;$, etc. de N symboles. Ils choisissent ensuite communémment deux entiers $l_1 < l_2$ grands. L'ensemble des messages lisible est l'ensembles des l_1-uplets à coefficients dans $\{0, \cdots, N-1\}$ et l'ensemble des messages cryptés est l'ensemble des l_2-uplets à coefficients dans $\{0, \cdots, N-1\}$ (tous les messages lisibles ont la même longueur, idem pour les messages cryptés).

Ensuite, chaque utilisateur choisit secrêtement deux premiers p, q tels que $n = pq$ vérifie $N^{l_1} < n < N^{l_2}$ et publie sa clé (n, a) comme décrit précédement. Pour envoyer un message $(\alpha_0, \cdots, \alpha_{l_1-1})$ de longueur l_1 à l'utilisateur de la clé publique (n, a), on calcul

$$m = \alpha_0 + \alpha_1 N + \cdots + \alpha_{l_1-1} N^{l_1-1} \in \mathbb{Z}$$

Comme $n < N^{l_1}$ on est sur que m correspond à un unique élément de $\mathbb{Z}/n\mathbb{Z}$. On trouve alors un entier $m' < N^{l_2}$ tel que sa classe modulo n soit la classe de m^a modulo n et on écrit

$$m' = \beta_0 + \beta_1 N + \cdots \beta_{l_2-1} N^{l_2-1}$$

le message cryté envoyé est alors $(\beta_0, \cdots, \beta_{l_2-1})$.

Exemple : On choisit $N = 26$ avec la correspondance $A = 1$, $B = 2$, $\cdots$, $Z = 0$. On prend $l_1 = 3$ et $l_2 = 4$. On cherche donc deux premier p et q tels que $n = pq$ vérifie $17576 < n < 456976$. On choisit $p = 281$ et $q = 167$, ainsi $n = 46927$ satisfait la condition. On calcul $\varphi(n) = 280.166 = 46480$ et on cherche la décomposition en facteur premier de $\varphi(n)$: on a $280 = 2^3.5.7$ et $166 = 2.83$. Ainsi, si l'on prend $a = 13$ on voit que $(a, \varphi(n)) = 1$. Notre clé publique sera donc $(46927, 13)$. On cherche alors un inverse s de a modulo $\varphi(n)$: $46480 = 3575.13 + 5$, $13 = 2.5 + 3$, $5 = 1.3 + 2$, $3 = 1.2 + 1$, $1 = 3 - 2 = 3 - (5 - 3) = -5 + 2.3 = -5 + 2.(13 - 2.5) = -5.5 + 2.13 = -5.(46480 - 3575.13) + 2.13 = -5.46480 + 17877.13$. Ainsi la clé secrête est $s = 17877$.

Quelqu'un veut nous envoyer le message "OUI", qui équivaut dans notre alphabet à $(15-21-09)$. Il calcule donc

$$m = 15 + 21.26 + 9.26^2 = 6645$$

Il lui faut calculer le représentant dans $0, \cdots, 456976$ de m^{13} modulo 46927. Pour calculer plus simplement, il commence par calculer la décomposition en base 2 de 13 : $13 = 2^3 + 2^2 + 2^0$. Ensuite, il calcule les puissances successives de m modulo 46927 : $m^{2^1} = 44156025 \equiv 44645(46927)$, $m^{2^2} \equiv 44645^2 \equiv 45554(46927)$, $m^{2^3} \equiv 45554^2 \equiv 8049(46927)$. Il trouve alors $m^{13} \equiv 8049.45554.6645 \equiv 21744(46927)$. Il écrit ce nombre en base 26 :

$$21744 = 8.26^0 + 4.26 + 6.26^2 + 1.26^3$$

le message encrypté est donc $(08-04-06-01)$ ce qui correspond dans notre alphabet à HDFA.

Exercice : Décryptez, avec cette clé, le message DUHZ qui vous est adressé.

Signature avec R.S.A. Supposons que l'utilisateur A (resp. B) ait la clé publique (n_A, e_A) (resp. (n_B, e_B)) et le clé secrete s_A (resp. s_B). L'utilisateur A veut signer un message (par un texte P) qu'il envoit à B. Si $n_A < n_B$, alors A commence par prendre le plus petit résidu entier positif de P^{s_a} modulo n_a et calcul ensuite $(P^{s_A}(n_A))^{e_B}$ modulo n_B. Dans le cas où $n_A > n_B$ il commence par calculer P^{e_B} modulo n_B puis il prend $(P^{e_B}(n_B))^{s_A}$ modulo n_B. Il envoit donc ce message M à B. En recevant M, B calcule successivement M à la puissance s_B modulo n_B puis $(M^{s_B}(n_B))^{e_A}(n_A)$ si $n_A < n_B$, sinon il calcule M à la puissance e_A modulo n_A puis $(M^{e_A}(n_A))^{s_B}(n_B)$ et obtient P.

Dans ce protocole, seul A peut envoyer ce message, car lui seul connait s_A et seul B peut le lire en sachant que c'est A qui l'envoit car lui seul connait s_B.