Introduction à l'algèbre générale

Groupes, anneaux et corps

Université d'Eleuthéria-Polites

Cours de Licence 3 — 2017/2018

Bruno Deschamps

Version 3.0

Table des matières

Chapitre 1

Structure de groupe

1.1 Magmas

1.1.1 Lois de compositions internes.

Définition.— *Soit E un ensemble. On appelle loi de composition interne sur E toute application de $E \times E$ dans E. Si $*$ désigne une loi de composition interne sur E et si x et y sont deux éléments de E, on note plus volontier $x*y$ à la place de $*(x,y)$. Un ensemble non vide muni d'une loi de composition s'appelle un magma.*

Exemples : a) $E = \mathbb{R}$ et pour $x, y \in \mathbb{R}$, $x * y = x^2 + y^2$.

b) $E = \mathcal{P}(X)$ (ensembles des parties d'un ensemble X) et pour $A, B \in \mathcal{P}(X)$, $A * B = A \cup B$.

c) $E = \mathbb{C}^{\mathbb{C}}$ et pour $f, g \in E$, $f * g = f \circ g$.

d) $E \neq \emptyset$ et pour $a, b \in E$, $a * b = a$.

e) $E = \mathcal{M}_n(\mathbb{C})$ et pour $A, B \in E$, $A * B = AB - BA$.

f) $E = \mathbb{Z}$ et pour $n, m \in E$, $n * m = n - m$.

Définition.— *Etant donné un magma fini $(E,*)$, disons $E = \{x_1, \cdots, x_n\}$ on appelle table de Cayley le tableau carré de n lignes et n colonnes obtenu en inscrivant à la i-ème ligne et à la j-ième colonne l'élément $x_i * x_j$ du magma.*

Réciproquement, étant donné un ensemble fini $E = \{x_1, \cdots, x_n\}$ et un tableau carré $(u_{i,j})_{1 \leq i,j \leq n}$ avec $u_{i,j} \in E$, on définit une loi de composition interne $*$ sur E par $x_i * x_j = u_{i,j}$. On remarque qu'alors, la table de Cayley du magma $(E,*)$ est le tableau $(u_{i,j})_{1 \leq i,j \leq n}$.

Définition.— *Soit $(E,*)$ un magma. On dit que $*$ est*

• *commutative, si $\forall x, y \in E$, $x * y = y * x$. On dit alors que le magma $(E,*)$ est commutatif.*

• *associative, si $\forall x, y, z \in E$, $(x * y) * z = x * (y * z)$. On dit alors que le magma $(E,*)$ est associatif.*

Dans les exemples précédent, a) est commutative non associative, b) est commutative et associative, c) et d) sont associatives et non commutatives, e) et f) ne sont ni associatives ni commutatives.

Exercice : Comment se lit sur une table de Cayley le fait qu'un magma fini soit commutatif?

Définition.— *Soit $(E,*)$ un magma et e un élément de E. On dit que e est*

• *est un neutre à gauche pour $*$ si pour tout $x \in E$, $e * x = x$.*

• *est un neutre à droite pour $*$ si pour tout $x \in E$, $x * e = x$.*

• *est un neutre bilatère (ou plus simplement neutre) pour $*$ si e est un neutre à droite et à gauche pour $*$, c'est-à-dire si pour tout $x \in E$, $x * e = e * x = x$.*

Un magma muni d'un élément neutre bilatère est appelé magma unifère (ou unitaire).

Proposition.— *Soit $(E,*)$ un magma et $e, e' \in E$. Si e est un neutre à gauche et e' est un neutre à droite alors $e = e'$. En particulier, dans un magma unifère il n'y a qu'un seul élément neutre bilatère, c'est aussi le seul neutre à gauche (resp. à droite).*

Preuve : Par définition, pour tout $x \in E$, on a $e * x = x$, donc pour $x = e^{'}$, on a $e * e^{'} = e^{'}$. De même, pour tout $y \in E$, on a $y * e^{'} = y$ donc pour $y = e$ on a $e * e^{'} = e$, ce qui prouve bien que $e = e^{'}$.

□

Exercice : Dresser la liste des neutres à droite (resp. à gauche, resp. bilatères) dans les exemples a), b), c), d), e) et f). En particulier, montrer qu'un magma peut trés bien posséder plusieurs neutres à droite (resp. à gauche).

Définition.— *Soit $(E,*)$ un magma, $e \in E$ un neutre à droite (resp. à gauche) et $x \in E$. On dit que x possède un inverse à gauche (resp. à droite) relativement à e s'il existe $y \in E$ tel que $y * x = e$ (resp. $x * y = e$). Si $(E,*)$ est unifère on dit que x possède un inverse s'il possède un inverse à droite qui est aussi un inverse à gauche.*

Exercice : Dans les exemples a), b), c), d), e) et f) donner, le cas échéant, des exemples d'éléments inversibles à droite ou à gauche et donner leurs inverses.

Définition.— *Soit $(E,*)$ un magma. On appelle sous-magma de E toute partie non vide A de E stable pour $*$ (i.e. si $x, y \in A$ alors $x * y \in A$).*

Si A est un sous-magma de $(E,*)$, on voit alors que la restriction de $*$ à $A \times A$ est une loi de composition interne et donc que $(A,*)$ est lui-même un magma. On remarqu'alors si E est associatif (resp. commutatif) alors A l'est aussi. Que penser de $(A,*)$ si $(E,*)$ est unifère?

1.1.2 Morphismes

Définition.— *Soit $(E,*)$ et $(F,\perp)$ deux magmas. On appelle morphisme (ou homomorphisme) du magma E vers le magma F toute application $f : E \to F$ qui satisfait*

$$\forall x, y \in E,\ f(x * y) = f(x) \perp f(y)$$

Si f est injective (resp. surjective, resp. bijective) on dit que f est un monomorphisme (resp. épimorphisme, resp. isomorphisme) de magmas. Lorsque $E = F$, les morphismes sont appelés des endomorphismes et les isomorphismes des automorphismes.

Proposition.— *Si $f : (E,*) \to (F,\perp)$ est un morphisme de magma, alors $f(E)$ est un sous magma de $(F,\perp)$. Si $(E,*)$ est associatif (resp. commutatif, resp. unifère) alors $f(E)$ l'est aussi.*

Preuve : Exercice.

□

1.1.3 Relations d'équivalences compatibles

Rappels : Une relation d'équivalence sur un ensemble E est une relation binaire $\mathcal{R}$ qui est reflexive, symétrique et transitive. Si $x \in E$ on note $\overline{x}$ la classe de x modulo $\mathcal{R}$, c'est-à-dire l'ensemble des éléments $y \in E$ tel que $x\mathcal{R}y$ (on écrit alors $x \equiv y(\mathcal{R})$).

L'ensemble des classes d'équivalences modulo $\mathcal{R}$ forme une partition de l'ensemble E et que cet ensemble est noté $E/\mathcal{R}$, on l'appelle *ensemble quotient de E modulo $\mathcal{R}$*.

L'application $s : E \to E/\mathcal{R}$ définie par $s(x) = \overline{x}$ est une surjection que l'on appelle surjection canonique de E sur son quotient. Une famille $\{x_i\}_{i\in I}$ d'éléments de E satisfaisant aux deux conditions suivantes

$$\begin{array}{ll} (1) & s(\{x_i\}_{i\in I}) = E/\mathcal{R} \\ (2) & \forall i, j \in I,\ i \neq j \Longrightarrow s(x_i) \neq s(x_j) \end{array}$$

est appelée *classe de représentants* de $E/\mathcal{R}$ dans E.

Définition.—*Soit $(E,*)$ un magma et $\mathcal{R}$ une relation d'équivalence sur E. On dit que $\mathcal{R}$ est compatible à gauche (resp. à droite) si pour tout $a, x, y \in E$ on a*

$$x \equiv y(\mathcal{R}) \Longrightarrow a * x \equiv a * y(\mathcal{R})\ (resp.\ x * a \equiv y * a(\mathcal{R}))$$

Quand $\mathcal{R}$ est compatible à droite et à gauche, on dit plus simplement que $\mathcal{R}$ est compatible.

Proposition.— *Soit $(E,*)$ un magma et $\mathcal{R}$ une relation d'équivalence compatible sur E. Soient $x, x^{'}, y, y^{'} \in E$ tels que $x \equiv x^{'}(\mathcal{R})$ et $y \equiv y^{'}(\mathcal{R})$. On a*

$$x * y \equiv x^{'} * y^{'}(\mathcal{R})$$

Preuve : Comme $x \equiv x'(\mathcal{R})$, on a $x*y \equiv x'*y(\mathcal{R})$. De même comme $y \equiv y'(\mathcal{R})$, on a $x'*y \equiv x'*y'(\mathcal{R})$. Par transitivité de $\mathcal{R}$, on en déduit que $x*y \equiv x'*y'(\mathcal{R})$.

□

En particulier, quand $\mathcal{R}$ est compatible, si $x, y \in E$ la classe $\overline{x*y}$ de $x*y$ modulo $\mathcal{R}$ ne dépend pas du choix des représentants des classes $\overline{x}$ et $\overline{y}$. Ainsi, on peut définir sur l'ensemble quotient $E/\mathcal{R}$ une loi de composition $\bar{*}$ (et une seule) qui satisfait, pour tout $x, y \in E$,

$$\overline{x} \,\bar{*}\, \overline{y} = \overline{x*y}$$

Définition.— *Le magma $(E/\mathcal{R}, \bar{*})$ défini précédement s'appelle le magma quotient de E modulo $\mathcal{R}$.*

Exercice : Montrer que la surjection canonique $s : E \to E/\mathcal{R}$ est un épimorphisme de magma. En déduire que si $(E,*)$ est associatif (resp. commutatif, resp. unifère) alors $E/\mathcal{R}$ l'est aussi.

Exemple fondamental : On considère le magma $(\mathbb{Z},+)$. Soit $n \geq 2$ un entier. On considère sur $\mathbb{Z}$ la relation binaire $\mathcal{R}_n$ définie pour $a, b \in \mathbb{Z}$, par

$$a\mathcal{R}_n b \iff n \text{ divise } b-a$$

Usuellement, on note $a \equiv b(n)$ à la place de $a \equiv b(\mathcal{R}_n)$. La relation $\mathcal{R}_n$ est une relation d'équivalence sur $\mathbb{Z}$ compatible avec la structure de magma (exercice), on l'appelle relation de congruence modulo n et la relation $a \equiv b(n)$ se lit "a est congru à b modulo n".

Le magma quotient $\mathbb{Z}/\mathcal{R}_n$ se note plus usuellement $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}/n$. Par exemple, pour $n = 4$, la table de Cayley du magma $\mathbb{Z}/4\mathbb{Z}$ est :

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Exercice : Montrer que pour tout $n \geq 1$, $\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini à n éléments et qu'une classe de représentants dans $\mathbb{Z}$ de $\mathbb{Z}/n\mathbb{Z}$ est, par exemple, l'ensemble $\{0, 1, \cdots, n-1\}$.

Montrer que c'est un magma associatif, commutatif et unifère dans lequel tout élément possède une unique inverse.

1.2 Généralité sur les groupes

1.2.1 Groupes

Définition.— *On appelle groupe, tout magma associatif et unifère dans lequel tout élément admet un inverse. Un groupe dont la loi de composition est commutative est appelé groupe abélien.*

Nous avons vu précédement que le neutre d'un magma unifère est unique. Dans un groupe, on a aussi :

Proposition.— *Dans un groupe, chaque élément possède un unique inverse.*

Preuve : Soit $(G,*)$ un groupe de neutre e, $x \in G$ 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 $y = y'$.

□

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.

Si G est un groupe et x un élement de G, on note généralement x^{-1} son inverse, si l'on utilise la notation . et $-x$ si l'on utilise la notation + pour sa loi de composition.

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 remarquera que cette propriété ne caractérise pas les groupes parmis les magmas associatif et unifère (penser, par exemple, au magma $(\mathbb{Z}^*, .)$).

On en déduit que si dans un groupe un élément y satisfait l'équation $xy = x$ (ou $yx = x$) pour un seul 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 $\mu_n = \{\exp(2ik\pi/n) / \ k \in \mathbb{Z}\}$ est un groupe abélien pour la multiplication complexe. De même, l'ensemble $\mathbb{U} = \{z \in \mathbb{C} / \ |z| = 1\}$ est un groupe abélien pour la multiplication complexe.

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 :

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

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

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.

Table de Cayley d'un groupe fini : (Exercice) La table de Cayley d'un groupe fini a une particularité : c'est toujours un carré latin (c'est-à-dire un tableau carré dans lequel dans chaque ligne et chaque colonne apparait une et une seule fois chaque élément du groupe). Il est à noté que le fait d'être un carré latin ne caractérise pas les

tables de Cayley des groupes, comme le montre l'exemple suivant avec un ensemble $E = \{e, a, b, c, d\}$ à 5 éléments :

$*$	e	a	b	c	d
e	e	a	b	c	d
a	a	e	d	b	c
b	b	c	e	d	a
c	c	d	a	e	b
d	d	b	c	a	e

(Vérifier que la loi de composition $*$ n'est pas associative)

1.2.2 Sous-groupes

Généralités

Définition.— *Soit $(G,.)$ un groupe. On appelle sous-groupe de G tout sous-magma H de G tel que $(H,.)$ soit un groupe.*

Exemple : $\mathbb{N}$ est un sous-magma de $(\mathbb{Z},+)$ mais n'est pas un sous-groupe.

Proposition.— *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 : Par hypothèse, $(H,.)$ est un groupe. Notons f son neutre. On a $f.f = f$ dans H et donc dans G. Mais comme dans G on a $f = f.e$, on en déduit que dans G, $f.f = f.e$ 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.— (Axiomes faibles) *Soit $(G,.)$ un groupe et H une partie de G. Les propositions suivantes sont équivalentes :*

i) H est un sous-groupe de G,

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

Preuve : $i) \Rightarrow ii)$ H n'est clairement pas vide car $(H,.)$ est un magma. 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 magma, 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 un sous-magma de $(G,.)$. Comme G est associatif, H l'est aussi. Comme $e \in H$, H est unifère 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.— *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 $(\mathbb{C}^*,.)$.

c) (Sous-groupes de $(\mathbb{Z},+)$)

• Si $n \in \mathbb{Z}$, alors le sous-ensemble $n\mathbb{Z} = \{nk/\ k \in \mathbb{Z}\}$ est un sous-groupe du groupe additif $(\mathbb{Z},+)$.

• Pour tout $n \in \mathbb{Z}$, on a $n\mathbb{Z} = (-n)\mathbb{Z}$. Plus précisément, si $a, b \in \mathbb{Z}$ alors

$$a\mathbb{Z} = b\mathbb{Z} \Longleftrightarrow |a| = |b|$$

• Si $a, b \in \mathbb{Z}$, alors $a\mathbb{Z}$ est un sous-groupe de $b\mathbb{Z}$ si et seulement si b divise a.

• La proposition suivante est un résultat qui permet de dresser la liste exaustive des sous-groupes de $(\mathbb{Z},+)$:

Proposition.— *Soit G un sous-groupe de $(\mathbb{Z},+)$. Il existe un unique entier $n \geq 0$ tel que $G = n\mathbb{Z}$.*

Preuve : Si $G = \{0\}$, on voit que $n = 0$ est le seul entier qui convienne. Supposons que $G \neq \{0\}$ et soit $x \in G - \{0\}$, comme $-x \in G$, on en déduit que $G \cap \mathbb{N}^* \neq \emptyset$. Il existe donc un plus petit entier strictement positif n dans $G \cap \mathbb{N}^*$. Comme G est un groupe, on a $2n = n+n \in G$ et par récurrence immédiate, on a pour tout $k > 0$, $kn \in G$. Par passage à l'opposé on en déduit que $k \in \mathbb{Z}$, $kn \in G$, c'est-à-dire que $n\mathbb{Z} \subset G$.

Réciproquement, considérons un entier $m \in G$ et effectuons sa division euclidienne par l'entier n. Il existe donc un unique $q \in \mathbb{Z}$ et un unique $r \in \{0, \cdots, n-1\}$ tels que

$$m = qn + r$$

Comme G est un groupe et que m et qn sont dans G, on en déduit que $r = m - qn \in G$, mais comme $r \geq 0$, on a $r \in G \cap \mathbb{N}$. Comme $r < n$, par minimalité de n, on en déduit que $r \notin G \cap \mathbb{N}^*$ et par suite que $r = 0$, c'est-à-dire $m = qn$. Ainsi $G \subset n\mathbb{Z}$.

L'unicité de l'entier positif n découle des remarques précédentes.

□

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.

Parties génératrices

Proposition-Définition.— *Soit G un groupe et A une partie de G. Il existe un plus petit sous-groupe (au sens de l'inclusion) qui contienne A. On le note $< A >$ et on l'appelle le sous-groupe de G engendré par A.*

Preuve : Considérons la famille $\{H_i\}_{i\in I}$ constituée des sous-groupe de G qui contienne A. Cette famille n'est pas vide car G tout entier est un sous-groupe de G qui contient A par hypothèse. Considérons la partie $H = \bigcap_{i\in I} H_i$. On sait que H est un sous-groupe, il contient visiblement la partie A. C'est le plus petit sous-groupe de G contenant A car si $H^{'}$ désigne un autre sous-groupe contenant A, il existe $j \in I$ tel que $H^{'} = H_j$ et donc $H = \bigcap_{i\in I} H_i \subset H_j$.

□

Proposition.— *Soit G un groupe et A une partie non vide de G. On a*

$$< A >= \{x_1.\cdots.x_n/\ n \in \mathbb{N}^*,\ x_i \in A \text{ ou } x_i^{-1} \in A \text{ pour tout } i = 1, \cdots, n\}$$

Preuve : Posons

$$H = \{x_1.\cdots.x_n/\ n \in \mathbb{N}^*,\ x_i \in A \text{ ou } x_i^{-1} \in A \text{ pour tout } i = 1,\cdots,n\}$$

et vérifions par les axiomes faibles que H est un sous-groupe : H n'est visiblement pas vide puisque A ne l'est pas. Soit $\alpha, \beta \in H$, il existe donc $n \in \mathbb{N}^*$, $x_1,\cdots,x_n \in G$ avec $x_i \in A$ ou $x_i^{-1} \in A$, $m \in \mathbb{N}^*$, $y_1,\cdots,y_n \in G$ avec $y_i \in A$ ou $y_i^{-1} \in A$ tels que $\alpha = x_1.\cdots.x_n$ et $\beta = y_1.\cdots.y_m$. On a alors

$$\alpha.\beta^{-1} = x_1.\cdots.x_n.y_m^{-1}.\cdots.y_1^{-1} = z_1.\cdots.z_l$$

avec $l = n+m$, $z_i = x_i$ pour $i = 1,\cdots,n$ et $z_i = y_{l-i+1}^{-1}$ pour $i = n+1,\cdots,l$. On a $z_i \in A$ ou $z_i^{-1} \in A$ par hypothèse, donc $\alpha\beta^{-1} \in H$.

Par ailleurs, il est clair que $A \subset H$. Il ne nous reste plus qu'à montrer que H est la plus petit sous-groupe ayant cette propriété. Soit H' un sous-groupe de G contenant A et soit $n \in \mathbb{N}^*$ et $x_1,\cdots,x_n$ des éléments de G tels que $x_i \in A$ ou $x_i^{-1} \in A$. Puisque H' est un groupe, il est stable par passage à l'inverse, et comme $A \subset H'$, on en déduit que $x_i \in H$ pour tout $i = 1,\cdots n$ et par suite que $x_1.\cdots.x_n \in H'$. Ainsi $H \subset H'$.

□

Exemples : (Exercice) a) Quand $A = \{x\}$ est une partie à un seul élément, on a

$$< A >= \{x^n/\ n \in \mathbb{Z}\}$$

b) Quand $A = \bigcup_{i\in I} H_i$ où $\{H_i\}_{i\in I}$ désigne une famille de sous-groupes de G, alors

$$< A >= \{x_1.\cdots.x_n/\ n \in \mathbb{N}^*,\ x_i \in A \text{ pour tout } i = 1,\cdots,n\}$$

Définition.— *Soit G un groupe et A une partie de G. On dit que A est génératrice si $< A >= G$ (on dit aussi que A engendre G).*

S'il existe une partie A finie génératrice de G, on dit que G est de type fini.

Si G est engendré par une partie réduite à un seul élément on dit que G est monogène et si, de plus, G est fini on dit que G est cyclique.

Si G est un groupe monogène, alors tout élément $x \in G$ tel que $G =< x >$ est appelé générateur de G.

Exemples : (Exercice)

a) Un groupe fini G est de type fini. La réciproque de cette proposition est bien sur fausse : $(\mathbb{Z},+)$ est un groupe infini mais de type fini (c'est même un groupe monogène puisque $\mathbb{Z} =< 1 >$).

b) Les groupes $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ sont des groupes monogènes.

Définition.— *Etant donné un groupe fini G, on appelle ordre de G le cardinal de G (fini ou infini), on le note $o(G)$. Etant donné un élément $x \in G$, on appelle ordre de x dans G l'ordre du groupe $< x >$, on le note $o(x)$.*

Proposition.— *Soit G un groupe de neutre e, $x \in G$ et $O_x = \{n \in \mathbb{N}^*/\ x^n = e\}$.*

• *Si $O_x = \emptyset$, alors x est d'ordre infini. On a alors*

$$< x >= \{\cdots,x^{-2},x^{-1},e,x,x^2,x^3,\cdots\}\ \ (x^n \neq x^m \text{ pour } n \neq m)$$

• *si $O_x \neq \emptyset$, alors x est d'ordre fini et $o(x) = \min O_x$. On a alors*

$$< x >= \{e,x,\cdots,x^{n-1}\}$$

où $n = o(x)$.

En particulier, un élément $x \in G$ est d'ordre n si et seulement si $x^n = e$ et $x^k \neq e$ pour tout $k = 1,\cdots,n-1$.

Preuve : Si $O_x = \emptyset$ alors pour tout $n \neq m$, on a $x^n \neq x^m$, car sinon, $x^{n-m} = e$ et $|n-m| \in O_x$ ce qui est impossible.

Supposons $O_x \neq \emptyset$ et soit $n = \min O_x$. On sait que

$$< x >= \{\cdots,x^{-2},x^{-1},e,x,x^2,x^3,\cdots\}$$

Montrons que pour tout $a \in \mathbb{Z}$, il existe $r \in \{0,\cdots,n-1\}$ tel que $x^a = x^k$: on effectue la division euclidienne de a par n

$$a = qn + r,\ q \in \mathbb{Z},\ r \in \{0,\cdots,n-1\}$$

et on trouve alors que $x^a = x^{qn}x^r$. Mais comme $x^{qn} = (x^n)^q = e^q = e$ on a $x^a = x^r$. On en déduit donc que

$$< x >= \{e, x, \cdots, x^{n-1}\}$$

Les éléments x^k sont distincts deux à deux pour $k = 0, \cdots, n-1$, sinon il existerait deux entiers $a < b$ dans $\{0, \cdots, n-1\}$ tels que $x^a = x^b$. On aurait alors $x^{b-a} = e$ et par conséquent $b - a \in O_x$, mais comme $b - a < n$ ceci serait alors absurde.

On en déduit donc que

$$o(x) = \sharp < x >= \sharp\{e, x, \cdots, x^{n-1}\} = n$$

□

Il est à noter que (exercice) dans cette proposition, la condition $O_x \neq \emptyset$ équivaut à dire qu'il existe $a, b \in \mathbb{Z}$ avec $a \neq b$ tels que $x^a = x^b$.

Exemples.— (Exercice)

a) Dans un groupe, le seul élément d'ordre 1 est le neutre.

b) Dans $(\mathbb{Z}, +)$ tous les éléments (sauf 0) sont d'ordre infini.

c) Dans $\mathbb{Z}/n\mathbb{Z}$, $o(\overline{1}) = n$.

d) On considère le groupe symétrique S_3 et les deux éléments $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. On a $\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ et $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. On en déduit donc que

$$S_3 = \{e, \sigma, \sigma^2, \tau, \sigma \circ \tau, \tau \circ \sigma\}$$

c'est-à-dire que σ et τ engendre S_3. Par ailleurs, on a $\sigma^2 \circ \tau = \tau \circ \sigma$ et $\tau \circ \sigma^2 = \sigma \circ \tau$, ce qui permet de dresser la table de Cayley de S_3 :

$\circ$	e	σ	σ^2	τ	$\sigma \circ \tau$	$\tau \circ \sigma$
e	e	σ	σ^2	τ	$\sigma \circ \tau$	$\tau \circ \sigma$
σ	σ	σ^2	e	$\sigma \circ \tau$	$\tau \circ \sigma$	τ
σ^2	σ^2	e	σ	$\tau \circ \sigma$	τ	$\sigma \circ \tau$
τ	τ	$\tau \circ \sigma$	$\sigma \circ \tau$	e	σ^2	σ
$\sigma \circ \tau$	$\sigma \circ \tau$	τ	$\tau \circ \sigma$	σ	e	σ^2
$\tau \circ \sigma$	$\tau \circ \sigma$	$\sigma \circ \tau$	τ	σ^2	σ	e

On voit aussi que $o(\sigma) = 3$ et que $o(\tau) = 2$.

Sous-groupes engendrés par des sous-groupes

Soit G un groupe et H et K deux sous-groupes de G. On note

$$HK = \{hk / \ h \in H \ et \ k \in K\}$$

De manière général l'ensemble HK diffère de KH et n'est pas forcément un sous-groupe de G. En fait, on a :

Proposition.— *Soit G un groupe et H, K deux sous-groupes de G. Les propriétés suivantes sont équivalentes :*

i) HK est un sous-groupe de G,

ii) KH est un sous-groupe de G,

iii) $HK = KH$.

Preuve: *i)* $\Rightarrow$ *iii)* Soit $h \in H$ et $k \in K$, on a $kh = (h^{-1}k^{-1})^{-1} \in HK$. Comme H et K sont des sous-groupes, on a $h^{-1} \in H$ et $k^{-1} \in K$ et donc $kh \in HK$, c'est-à-dire $KH \subset HK$. Soit $z \in HK$, on a $z^{-1} \in HK$, donc il existe $h \in H$ et $k \in K$ tels que $z^{-1} = hk$ et par suite $z = k^{-1}h^{-1} \in KH$. Donc $HK \subset KH$.

iii) $\Rightarrow$ *i)* Vérifions les axiomes faibles. Comme e est dans H et dans K, on a $e \in HK$ et donc $HK \neq \emptyset$.

Soit $h_1, h_2 \in H$ et $k_1, k_2 \in K$, on a $(h_1k_1)(h_2k_2)^{-1} = h_1((k_1k_2^{-1})h_2^{-1})$. Comme $(k_1k_2^{-1})h_2^{-1} \in KH = HK$, il existe $h_3 \in H$ et $k_3 \in K$ tel que $(k_1k_2^{-1})h_2^{-1} = h_3k_3$ et par suite $(h_1k_1)(h_2k_2)^{-1} = (h_1h_3)k_3 \in HK$.

On démontre de la même manière que $ii) \Longleftrightarrow iii)$.

□

Remarques : a) Dans cette situation, on a alors $HK = KH =< H \cup K >$.

b) Si G est abélien, alors HK est toujours un sous-groupe de G.

Corollaire.— *Soit G un groupe et $H_1, \cdots, H_n$ des sous-groupes de G vérifiants que pour tout $i, j = 1, \cdots, n$, $H_i H_j = H_j H_i$, alors l'ensemble*

$$H_1 \cdots H_n = \{x_1 \cdots x_n / \ x_i \in H_i \ pour \ tout \ i = 1, \cdots, n\}$$

est un sous-groupe de G.

Preuve: Exercice.

□

1.2.3 Morphismes

Définition.— *Soit $(G, *)$ et $(H, \perp)$ deux groupes. On appelle morphisme du groupe G dans le groupe H tout morphisme de magma de G dans H.*

Dans cette situation, un morphisme de groupe est donc une application $f : G \to H$ qui vérifie pour tout $x, y \in G$, $f(x * y) = f(x) \perp f(y)$. 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.

Proposition.— *Soit $f : G \longrightarrow G^{'}$ un morphisme de groupes. Si e (resp. $e^{'}$) désigne le neutre de G (resp. de $G^{'}$), alors $f(e) = e^{'}$. Par ailleurs, si $x \in G$, alors $f(x^{-1}) = (f(x))^{-1}$ et plus généralement, consécutivement à la convention décrite préalablement, pour tout $n \in \mathbb{Z}$, on a $f(x^n) = (f(x))^n$.*

Preuve : Exercice.

□

Proposition.— *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.— *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, où le 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 $\mathrm{Ker}(f) = SL_n(\mathbb{C})$.

Notations : Etant donnés deux groupe G et $G^{'}$, l'ensemble des morphismes de G dans $G^{'}$ est noté $\mathrm{Hom}(G, G^{'})$. C'est un ensemble qui n'est jamais vide (voir b) ci-dessus). Lorsque $G = G^{'}$, on note plus simplement $\mathrm{Hom}(G)$. Le sous-ensemble de $\mathrm{Hom}(G)$ constitué des automorphismes de groupes est noté $\mathrm{Aut}(G)$.

Proposition.— *Soient $G, G^{'}$ et $G^{''}$ trois groupes. Pour tous $f \in \mathrm{Hom}(G, G^{'})$ et $g \in \mathrm{Hom}(G^{'}, G^{''})$ on a $g \circ f \in \mathrm{Hom}(G, G^{''})$.*

Preuve : Exercice.

□

Proposition.— *Soient $G, G^{'}$ deux groupes et $f \in \mathrm{Hom}(G, G^{'})$. Si f est un isomorphisme, alors $f^{-1} \in \mathrm{Hom}(G^{'}, G)$ et, en particulier, f^{-1} est aussi un isomorphisme.*

Preuve : Soit $x^{'}, y^{'} \in G^{'}$. Par hypothèse il existe un unique $x \in G$ et un unique $y \in G$ tel que $f(x) = x^{'}$ et $f(y) = y^{'}$. Comme $f(xy) = f(x)f(y) = x^{'}y^{'}$, on a $f^{-1}(x^{'}y^{'}) = f^{-1} \circ f(xy) = xy = f^{-1}(x^{'})f^{-1}(y^{'})$. Ainsi, $f^{-1} \in \mathrm{Hom}(G^{'}, G)$. La bijectivité de f^{-1} assure que f^{-1} est bien un isomorphisme.

□

Définition.— *Soit $G, G^{'}$ deux groupes. On dit que G et $G^{'}$ sont isomorphes s'il existe un isomorphisme de groupe entre G et $G^{'}$. On note alors $G \simeq G^{'}$.*

Remarque : L'intérêt de la notion de groupes isomorphes est que, quand deux groupes sont isomorphes, toutes les propriétés liées à la structure de groupe valable pour l'un sont valable pour l'autre. Par exemple si G et $G^{'}$ sont deux groupes isomorphes alors si l'un est fini l'autre l'est aussi et dans ce cas leurs ordres sont les mêmes. De manière générale, la théorie des groupes s'intéresse à décrire tous les groupes à isomorphismes près (vaste programme...).

Proposition.— *Soit $f : G \longrightarrow G^{'}$ un isomorphisme de groupes. L'application f définit une bijection entre les sous-groupes de G et ceux de $G^{'}$.*

Preuve : Exercice.

□

Proposition.— *Soit G un groupe. Le magma $(\mathrm{Aut}(G), \circ)$ est un groupe, c'est un sous-groupe de $(\mathrm{Perm}(G), \circ)$.*

Preuve : La composition donne visiblement une structure de magma associatif à $\mathrm{Aut}(G)$. La fonction identité est visiblement un élément neutre de $\mathrm{Aut}(G)$. La proposition précédente montre que si $f \in \mathrm{Aut}(G)$ alors $f^{-1} \in \mathrm{Aut}(G)$. Ainsi, $\mathrm{Aut}(G)$ est bien un groupe.

Reste à voir que $\mathrm{Aut}(G)$ est un sous-ensemble de $\mathrm{Perm}(G)$. Ceci est évident puisque par définition, $\mathrm{Perm}(G)$ est l'enesemble des bijections de G dans lui-même.

□

Automorphismes intérieurs (Exercice) Soit G un groupe. Pour tout g, on considère l'application

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

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

Proposition.— *Soit $f : G \longrightarrow G^{'}$ un morphisme de groupes et A une partie de G. On a $f(< A >) =< f(A) >$. En particulier, si A engendre G et si f est un épimorphisme alors $f(A)$ engendre $G^{'}$.*

Preuve : Comme $f(A) \subset f(< A >)$ et que $f(< A >)$ est un sous-groupe, on a $< f(A) > \subset f(< A >)$. Soit $H^{'}$ un sous-groupe de $G^{'}$ contenant $f(A)$, alors $H = f^{-1}(H^{'})$ est un sous-groupe de G qui contient A. Donc

$$f^{-1}(< f(A) >) = f^{-1}(\bigcap_{f(A)\subset H^{'}} H^{'}) = \bigcap_{f(A)\subset H^{'}} f^{-1}(H^{'})$$

et par suite

$$< A >= \bigcap_{A\subset H} H \subset \bigcap_{f(A)\subset H^{'}} f^{-1}(H^{'}) = f^{-1}(< f(A) >)$$

et donc $f(< A >) \subset < f(A) >$.

□

On en déduit que si $f : G \longrightarrow G^{'}$ est un épimorphisme de groupe et que G est de type fini (resp. monogène, resp. cyclique) alors $G^{'}$ est de type fini (resp. monogène, resp. cyclique).

Bien qu'il soit tentant de le penser, si B est une partie de $G^{'}$, alors $f^{-1}(< B >)$ n'est pas forcément égal à $< f^{-1}(B) >$. Par exemple, considérons $G = \mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ et $G^{'} = \mathbb{Z}/4\mathbb{Z} == \{\overset{\circ}{0}, \overset{\circ}{1}, \overset{\circ}{2}, \overset{\circ}{3}\}$ et l'application $f : G \longrightarrow G^{'}$ définie par

$$f(\overline{0}) = \overset{\circ}{0} \text{ et } f(\overline{1}) = \overset{\circ}{2}$$

On vérifie sans mal que f est un morphisme de groupe. Posons $B = \{\overline{1}\}$, on a $< B >= \mathbb{Z}/4\mathbb{Z}$ et donc $f^{-1}(< B >) = \mathbb{Z}/2\mathbb{Z}$, mais $f^{-1}(B) = \emptyset$ et donc $< f^{-1}(B) >= \{\overline{0}\}$.

1.2.4 Groupes produits

On considère une famille non vide de groupes $\{G_i\}_{i\in I}$. Par commodité, on note la loi de composition de chacun des G_i par l'absence de notation, et pour tout $i \in I$, on note e_i le neutre de G_i. Sur le produit cartésien

$$\prod_{i\in I} G_i = \{(x_i)_{i\in I} / \ \forall i \in I,\ x_i \in G_i\}$$

on définit la loi de composition suivante :

$$\begin{array}{ccc} \prod_{i\in I} G_i \times \prod_{i\in I} G_i & \longrightarrow & \prod_{i\in I} G_i \\ ((x_i)_{i\in I}, (y_i)_{i\in I}) & \longmapsto & (x_i y_i)_{i\in I} \end{array}$$

(la composition se fait coordonnée par coordonnée)

On voit alors que muni de cette loi de composition, $\prod_{i\in I} G_i$ est un groupe. En effet, la loi est visiblement associative puisqu'elle l'est pour chaque G_i, l'élement $(e_i)_{i\in I} \in \prod_{i\in I} G_i$ est visiblement un neutre et pour tout $(x_i)_{i\in I} \in \prod_{i\in I} G_i$, on constate que $(x_i^{-1})_{i\in I} \in \prod_{i\in I} G_i$ est un inverse de $(x_i)_{i\in I}$.

Définition.— *Avec les notation, précédent le groupe obtenu s'appelle le groupe produit direct des G_i.*

Toujours dans cette situation, on considère pour tout $k \in I$, les applications suivantes

$$\begin{array}{lccc} \text{la } k\text{-ième projection canonique} \quad p_k : & \prod_{i\in I} G_i & \longrightarrow & G_k \\ & (x_i)_i & \longmapsto & x_k \end{array}$$

et

$$\begin{array}{lccc} \text{la } k\text{-ième injection canonique} \quad q_k : & G_k & \longrightarrow & \prod_{i\in I} G_i \\ & x_k & \longmapsto & (x_i)_i \end{array}$$

où l'élément $(x_i)_i$ est défini par $x_i = e_i$ si $i \neq k$ et $x_i = x_k$ si $i = k$.

Les applications p_k et q_k sont respectivement des épimorphismes et monomorphismes de groupes (exercice).

En conséquence de quoi, pour tout $i \in I$, il y a dans $\prod_{i\in I} G_i$ un sous-groupe canoniquement isomorphe à G_i : $q_i(G_i)$. On remarque aussi que pour tout $k \in I$, on a $p_k \circ q_k = Id_{G_k}$.

Théorème.— (Propriété universelle du groupe produit) *Soit I un ensemble non vide d'indices, $\{G_i\}_{i\in I}$ une famille de groupes et $\{p_i\}_{i\in I}$ la famille des projections canoniques associées au groupe produit direct $\prod_{i\in I} G_i$.*

Soit G un groupe et pour tout $i \in I$ un élément $f_i \in \mathrm{Hom}(G, G_i)$. Il existe un unique morphisme $f : G \longrightarrow \prod_{i\in I} G_i$ tel que pour tout $i \in I$ on ait $p_i \circ f = f_i$.

Preuve : Existence. Pour $x \in G$, posons

$$f(x) = (f_i(x))_{i\in I}$$

On vérifie sans mal que f est bien un morphisme. Par ailleurs, pour tout $i \in I$, on

$$p_i \circ f(x) = p_i((f_i(x))_{i\in I}) = f_i(x)$$

donc cette application f convient.

Unicité. Supposons avoir $f, f' \in \mathrm{Hom}(G, \prod_{i\in I} G_i)$ satisfaisant pour tout $x \in G$, $p_i \circ f(x) = f_i(x) = p_i \circ f'(x)$. On a alors, pour tout $x \in G$,

$$f(x) = (p_i \circ f(x))_{i\in I} = (p_i \circ f'(x))_{i\in I} = f'(x)$$

on en déduit que $f = f'$.

□

Cas d'un produit fini

On reprend les mêmes notations que dans le paragraphe précédent et on suppose ici que l'ensemble I est fini, disons par exemple $I = \{1, \cdots, n\}$. On note alors plus courament $G_1 \times \cdots \times G_n$ à la place de $\prod_{i\in I} G_i$. Si les groupes G_i sont finis, alors il en est de même du groupe $G_1 \times \cdots \times G_n$ et l'on voit que $o(G_1 \times \cdots \times G_n) = o(G_1).\cdots.o(G_n)$.

Pour tout $x = (x_1, \cdots, x_n) \in G_1 \times \cdots \times G_n$ et tout $\sigma \in S_n$, on a

$$x = q_{\sigma(1)}(x_{\sigma(1)}) \cdots q_{\sigma(n)}(x_{\sigma(n)})$$

(par exemple pour $n = 2$, on a $x = q_1(x_1)q_2(x_2) = q_2(x_2)q_1(x_1)$). Il en découle que, si l'on note $H_i = q_i(G_i)$, alors

$$G_1 \times \cdots \times G_n = H_1.\cdots.H_n$$

Par ailleurs, on voit (exercice) que pour tout $k = 1, \cdots i$, on a

$$H_k \cap H_1.\cdots.H_{k-1}.H_{k+1}.\cdots.H_n = e$$

où $e = (e_1, \cdots, e_n)$ désigne le neutre de $G_1 \times \cdots \times G_n$. Enfin, on voit aussi que si $h_i \in H_i$ et $h_j \in H_j$, on a $h_i h_j = h_j h_i$. En fait ces propriétés caractérisent les produits directs finis de groupes :

Proposition.— *Soit $G_1, \cdots, G_n$ des groupes et G un autre groupe. Le groupe G est isomorphe au groupe produit direct $G_1 \times \cdots \times G_n$ si et seulement si il existe une famille $H_1, \cdots, H_n$ de sous-groupes de G vérifiant :*

1/ pour tout $i = 1, \cdots, n$, $H_i \simeq G_i$,

2/ pour tout $i, j = 1, \cdots, n$ et tout $h_i \in H_i$ et $h_j \in H_j$, on a $h_i h_j = h_j h_i$,

3/ $G = H_1.\cdots.H_n$,

4/ pour tout $k = 1, \cdots, n$, $H_k \cap H_1.\cdots.H_{k-1}.H_{k+1}.\cdots.H_n = \{e\}$ où e désigne le neutre de G.

Preuve : Supposons 1/,2/,3/ et 4/ vérifiés et considérons le groupe produit $G_1 \times \cdots \times G_n$ où $G_i = H_i$ pour tout $i = 1, \cdots, n$. Soit $x \in G$, le 3/ montre qu'il existe un n-uplet $(h_1, \cdots, h_n) \in H_1 \times \cdots \times H_n$ tel que $x = h_1 \cdots h_n$. Supposons avoir un n-uplet $(h_1', \cdots, h_n') \in H_1 \times \cdots \times H_n$ tel que $x = h_1' \cdots h_n'$. La condition 2/ montre alors que

$$e = (h_1 \cdots h_n)(h_1' \cdots h_n')^{-1} = (h_1 {h_1'}^{-1}) \cdots (h_n {h_n'}^{-1})$$

et par suite, toujours en appliquant la condition 2/, on a

$$h_1 {h_1'}^{-1} = (h_2' h_2^{-1}) \cdots (h_n' h_n^{-1}) \in H_2 \cdots H_n$$

La condition 4/, montre alors que $h_1 {h_1'}^{-1} = e$ c'est-à-dire que $h_1 = h_1'$. En procédant par récurrence, on montre que pour tout $i = 1, \cdots, n$, on a $h_i = h_i'$. On vient donc de montrer que pour tout $x \in G$, il existe un unique n-uplet

$(h_1,\cdots,h_n) \in H_1 \times \cdots \times H_n$ tel que $x = h_1 \cdots h_n$. Ceci nous permet de définir une application (avec les notations précédentes) :

$$\begin{array}{rccc} \psi : & G & \longrightarrow & H_1 \times \cdots \times H_n \\ & x & \longmapsto & (h_1,\cdots,h_n) \end{array}$$

Cette application est par définition surjective. C'est un morphisme de groupe, car d'après la propriété 2/, on a $(h_1 \cdots h_n)(h_1^{'} \cdots h_n^{'}) = (h_1 h_1^{'}) \cdots (h_n h_n^{'})$. Enfin le noyau de ψ est visiblement e. Donc ψ est un isomorphisme.

La réciproque a été faite en préliminaire à l'énoncé de cette proposition.

□

1.2.5 Somme directe dans un groupe abélien

On considère dans ce paragraphe un groupe $(G,+)$ abélien de neutre 0 (ATTENTION au changement de notations!).

Somme directe de deux sous-groupes

Soit H et K deux sous-groupes de G, on sait que $H + K = K + H =< H \cup K >$ est un sous-groupe de G. On l'appelle la somme des sous-groupe H et K.

Définition.— *On dit que H et K sont en somme directe si $H \cap K = \{0\}$. Dans ces conditions le groupe $H + K$ est appellé la somme directe des sous-groupe H et K et est noté $H \oplus K$.*

Proposition.— *Soit $(G,+)$ un groupe abélien et H et K deux sous-groupes de G. Les propriétés suivantes sont équivalentes :*

i) H et K sont en somme directe,

ii) Pour tout $x \in H + K$, il existe un unique couple $(h,k) \in H \times K$ tel que $x = h + k$.

Preuve : $i) \Rightarrow ii)$ Par définition, pour tout $x \in H + K$ il existe $(h,k) \in H \times K$ tel que $x = h + k$. Supposons qu'il existe $(h^{'},k^{'}) \in H \times K$ tel que $x = h^{'} + k^{'}$. En soustrayant, on a donc $h - h^{'} = k^{'} - k$ et donc comme H et K sont des sous-groupes, on a $h - h^{'} \in H \cap K$ et $k^{'} - k \in H \cap K$, mais comme $H \cap K = \{0\}$, on en déduit $h = h^{'}$ et $k = k^{'}$.

$ii) \Rightarrow i)$ Soit $x \in H \cap K$, on a $x = x + 0 = 0 + x$ avec $(x,0) \in H \times K$ et $(0,x) \in H \times K$, donc par unicité de l'écriture, on a $x = 0$.

□

Somme directe d'une famille de sous-groupes

On s'intéresse maintenant aux cas d'une famille quelconque de sous-groupes $\{H_i\}_{i\in I}$ de G. On définit la somme des sous-groupes H_i comme étant

$$\begin{aligned} \sum_{i\in I} H_i &= \left\{ h_{i_1} + \cdots + h_{i_n} / \; n \in \mathbb{N}^*,\; i_1,\cdots,i_n \in I \text{ et } \forall j = 1,\cdots,n \; h_{i_j} \in H_j \right\} \\ &= < \bigcup_{i\in I} H_i > \end{aligned}$$

Définition.— *On dit que la famille $\{H_i\}_{i\in I}$ est en somme directe, si pour tout $i_0 \in I$, on a $H_{i_0} \cap \sum_{i\neq i_0} H_i = \{0\}$. Dans cette situation, la somme des sous-groupes H_i se note $\bigoplus_{i\in I} H_i$.*

Comme dans le cas de deux sous-groupes, on a la caractérisation suivante :

Proposition.— *Soit $(G,+)$ un groupe abélien et H et K deux sous-groupes de G. Les propriétés suivantes sont équivalentes :*

i) Les H_i sont en somme directe,

ii) Pour tout $x \in \sum_{i\in I} H_i$, $x \neq 0$, il existe un unique entier $n \in \mathbb{N}^*$, une suite finie unique $i_1,\cdots,i_n \in I$ d'indices distincts deux à deux et une suite finie d'éléments $h_{i_1},\cdots,h_{i_n} \in G$ tels que $h_{i_j} \in H_{i_j}$ et $h_{i_j} \neq 0$ pour tout $j = 1,\cdots,n$ tels que $x = h_{i_1} + \cdots + h_{i_n}$.

Preuve : Exercice.

□

Cas où I est fini : Dans le cas où $I = \{1, \cdots, n\}$ est fini, on obtient alors la caractérisation suivante (qui généralise le cas $n = 2$) : la famille $\{H_i\}_{i\in I}$ est en somme directe si et seulement si pour tout $x \in H_1 + \cdots + H_n$, il existe un unique n-uplet $(h_1, \cdots, h_n) \in H_1 \times \cdots \times H_n$ tel que $x = h_1 + \cdots + h_n$. (Exercice)

Proposition.— *Soit $(G, +)$ un groupe abélien et $\{G_i\}_{1\leq i\leq n}$ une famille de groupe abéliens. Les propriétés suivantes sont équivalentes :*

i) G est isomorphe au groupe produit $G_1 \times \cdots \times G_n$,

ii) il existe une famille de sous-groupes $\{H_i\}_{1\leq i\leq n}$ de G tels que $G = H_1 \oplus \cdots \oplus H_n$ et tels que pour tout $i = 1, \cdots, n$, $H_i \simeq G_i$.

Preuve : Immédiat.

□

Attention : Cette propriété n'existe que dans le cas d'une famille finie de groupes : considérons une famille dénombrable infinie de groupes abéliens finis non triviaux $(G_n)_{n\in\mathbb{N}}$ et un groupe G abélien muni d'une famille $(H_n)_{n\in\mathbb{N}}$ de sous-groupes telle que $G = \bigoplus_{n\in\mathbb{N}} H_n$ et telle que $H_n \simeq G_n$. Il est alors impossible que G et $\prod_{n\in\mathbb{N}} G_n$ soit isomorphe. En effet, le produit cartésien $\prod_{n\in\mathbb{N}} G_n$ a pour cardinal $2^{\aleph_0}$ alors que G a pour cardinal $\aleph_0$ (exercice).

1.3 Groupes quotients

1.3.1 Indice, théorème de Lagrange

Classes modulo un sous-groupe

Etant donnés un groupe G, un sous-groupe H de G et un élément x de G, on note

$$\begin{aligned} x.H &= \{xh/\ h \in H\} \\ H.x &= \{hx/\ h \in H\} \end{aligned}$$

Ce sont les translatés à droite et à gauche de x par H.

Les ensembles $x.H$ et $H.x$ ne sont, en général, pas des sous-groupes de G. Toutefois, il est remarquable que les trois ensembles H, $x.H$ et $H.x$ sont toujours équipotents (exercice). En particulier, si H est fini, alors H, $x.H$ et $H.x$ ont même nombre d'éléments.

Considérons sur G les relations binaires, $\mathcal{R}_H$ et ${}_H\mathcal{R}$, définies de la manière suivante : pour $x, y \in G$, on pose

$$x\mathcal{R}_H y \Longleftrightarrow xy^{-1} \in H \quad et\ x\,{}_H\mathcal{R}y \Longleftrightarrow x^{-1}y \in H$$

La preuve des propriétés suivantes, relatives aux relations $\mathcal{R}_H$ et ${}_H\mathcal{R}$, est laissée en exercice :

1/ $\mathcal{R}_H$ et ${}_H\mathcal{R}$ sont des relations d'équivalences.

2/ Pour tout $x, y \in G$ on a

$$\begin{aligned} y \equiv x(\mathcal{R}_H) &\iff y \in Hx \\ y \equiv x({}_H\mathcal{R}) &\iff y \in xH \end{aligned}$$

3/ La relation $\mathcal{R}_H$ est compatible à droite et la relation ${}_H\mathcal{R}$ est compatible à gauche (exercice).

4/ Pour tout $x \in G$, la classe d'équivalence de x modulo $\mathcal{R}_H$ (resp. ${}_H\mathcal{R}$) est l'ensemble Hx (resp. xH).

On appelle $\mathcal{R}_H$ (resp. ${}_H\mathcal{R}$) la relation d'équivalence à droite (resp. à gauche) modulo H dans G. Pour $x \in G$, l'ensemble Hx (resp. xH) est appelé classe à droite (resp. à gauche) de x modulo H. Les ensembles quotients $G/\mathcal{R}_H$ et $G/{}_H\mathcal{R}$ sont notés respectivement $\left(\frac{G}{H}\right)_d$ et $\left(\frac{G}{H}\right)_g$.

Indices

Théorème.— (Lagrange) *Soit G un groupe fini et H un sous-groupe de G. L'ordre de H divise l'ordre de G.*

Preuve : Considérons l'ensemble quotient $\left(\frac{G}{H}\right)_d$ et choisissons une classe de représentants de cet ensemble quotient dans G : $x_1, \cdots, x_n$ (forcément en nombre fini, car G est fini). Les éléments de $\left(\frac{G}{H}\right)_d$ sont donc les parties $Hx_1, \cdots, Hx_n$ et ces parties forment une partition de G. On a donc $o(G) = \sum_{i=1}^{n} \sharp Hx_i$, mais comme on remarqué que $\sharp Hx_i = o(H)$, on en déduit que $o(G) = n.o(H)$.

□

Corollaire.— *Soit G un groupe fini d'ordre n. L'ordre d'un élément divise l'ordre de G et donc pour tout $x \in G$, $x^n = e$.*

Preuve : Par définition l'ordre m de $x \in G$ est l'ordre du sous-groupe $< x >$ qui divise n. On a donc $n = km$ avec k entier et par suite $x^n = x^{km} = (x^m)^k = e^k = e$.

□

Application : Tout groupe fini d'ordre p premier est cyclique. En effet, soit G un groupe fini d'ordre p et de neutre e. Soit $x \in G$ tel que $x \neq e$. On a $o(x)|p$, mais comme $x \neq e$, on a $o(x) \neq 1$ et comme p est premier, on trouve $o(x) = p$ et donc $< \{x\} >= G$. On vient, au passage de montrer que tout $x \neq e$ est générateur de G.

Remarquons que dans la preuve du théorème de Lagrange l'entier n n'est autre que le cardinal de l'ensemble quotient $\left(\frac{G}{H}\right)_d$. Par ailleurs, on aurait faire cette preuve en utilisant l'ensemble quotient $\left(\frac{G}{H}\right)_g$ et on serait arriver à la même conclusion avec le même entier n. On vient donc de justifier que si G est fini, alors les ensembles $\left(\frac{G}{H}\right)_d$ et $\left(\frac{G}{H}\right)_g$ ont même nombres d'éléments (il y a autant de classe à gauche que de classe à droite), c'est-à-dire sont équipotents. De manière générale, on a

Proposition.— *Soit G un groupe et H un sous-groupe de G. Les ensembles quotients $\left(\frac{G}{H}\right)_d$ et $\left(\frac{G}{H}\right)_g$ sont équipotents.*

Preuve : Considérons l'application

$$\begin{array}{rccc} \theta : & \left(\frac{G}{H}\right)_d & \longrightarrow & \left(\frac{G}{H}\right)_g \\ & Hx & \longmapsto & x^{-1}H \end{array}$$

C'est bien une application, car si $x, y \in G$ sont tels que $Hx = Hy$ alors x, y sont dans la même classe à droite modulo H, c'est-à-dire que $(x^{-1})^{-1}(y^{-1}) = xy^{-1} \in H$, et donc x^{-1} et y^{-1} sont dans la même classe à gauche modulo H, c'est-à-dire que $x^{-1}H = y^{-1}H$.

L'application θ est clairement surjective. Vérifions qu'elle est injective : si $x, y \in G$ sont tels que $x^{-1}H = y^{-1}H$ alors x^{-1}, y^{-1} sont dans la même classe à gauche modulo H, c'est-à-dire que $xy^{-1} \in H$, et donc x et y sont dans la même classe à droite modulo H, c'est-à-dire que $Hx = Hy$.

□

Définition.— *Soit G un groupe et H un sous-groupe de G, on appelle indice de H dans G le cardinal (fini ou non) commun de $\left(\frac{G}{H}\right)_d$ et $\left(\frac{G}{H}\right)_g$. On le note $[G : H]$.*

Si G est fini, l'indice de tout sous-groupe est fini. Si G est infini ses sous-groupes peuvent être d'indice fini ou non : par exemple, dans le groupe $(\mathbb{Z}, +)$, tout sous-groupe différent de $\{0\}$ est d'indice fini et $\{0\}$ est d'indice infini.

Proposition.— *Soit G un groupe fini et H un sous-groupe de G. On a*

$$o(G) = o(H).[G : H]$$

Preuve : C'est une conséquence immédiate du théorème de Lagrange et de la preuve qu'on en a donné.

□

Théorème.— (Poincaré) *Soit G un groupe et $H_1, \cdots, H_n$ une famille finie de sous-groupes de G d'indices finis. Le sous groupe $H_1 \cap \cdots \cap H_n$ est d'indice fini.*

Preuve : Si l'on montre le résultat pour $n = 2$, alors par récurrence immédiate, il sera établi pour tout entier $n \geq 2$. Soit donc H_1 et H_2 deux sous-groupes d'indice fini de G. Soit $x \in G$, on a

$$(H_1 \cap H_2)x \subset H_1x \cap H_2x$$

Réciproquement, si $y \in H_1x \cap H_2x$ alors $yx^{-1} \in H_1$ et $yx^{-1} \in H_2$, donc $y \in (H_1 \cap H_2)x$ et par suite

$$(H_1 \cap H_2)x = H_1x \cap H_2x$$

Par hypothèse, les classes à droites modulo H_1 et H_2 sont en nombre fini, respectivement, $[G : H_1]$ et $[G : H_2]$. La formule précédente montre que les classes à droite de G modulo $H_1 \cap H_2$ sont des intersections de classes à droite modulo H_1 (resp. H_2). Or il y a au maximum $[G : H_1].[G : H_2]$ telles intersections. Ainsi :

$$[G : H_1 \cap H_2] \leq [G : H_1].[G : H_2]$$

et donc $H_1 \cap H_2$ est d'indice fini dans G.

□

Proposition.— (Formule des indices) *Soit G un groupe, K un sous-groupe de G et H un sous-groupe de K ($H \leq K \leq G$). On a*

$$[G : H] = [G : K].[K : H]$$

En particulier, les propositions suivantes sont équivalentes

i) H est d'indice fini dans G,

ii) H est d'indice fini dans K et K est d'indice fini dans G.

Preuve : Soit $\{x_i\}_{i\in I}$ une famille de représentants des classes à droite modulo K dans G. Les ensembles $\{Kx_i\}_{i\in I}$ forment une partition de G. De même, soit $\{y_j\}_{j\in J}$ une famille de représentants des classes à droite modulo H dans K. Les ensembles $\{Hy_j\}_{j\in J}$ forment une partition de K. Considérons la collection d'ensembles

$$\left\{Hy_jx_i\right\}_{(i,j)\in I\times J}$$

et montrons qu'elle forme une partition de G.

Soit $g \in G$, il existe un unique $i \in I$ tel que $g \in Kx_i$ et donc un unique $a \in K$ tel que $g = ax_i$. Par ailleurs, il existe un unique $j \in J$ tel que $a \in Hy_j$, on a donc $g \in Hy_jx_i$ et par suite

$$G = \bigcup_{(i,j)\in I\times J} Hy_jx_i$$

Les ensembles Hy_jx_i étant des classes de conjugaison (à droite modulo H) on sait qu'ils sont soit disjoints, soit égaux. Ainsi pour finir de montrer que nous sommes bien en présence d'une partition il suffit de montrer que si $Hy_jx_i = Hy_{j'}x_{i'}$ alors $i = i^{'}$ et $j = j^{'}$. Comme $H \subset K$, on a $KH = K$, de même, on a

$$Hy_jx_i = Hy_{j'}x_{i'} \Longrightarrow KHy_jx_i = KHy_{j'}x_{i'}$$

et par suite, comme $KHy_j = Ky_j = K$ (car $y_j \in K$) et que $KHy_{j'} = Ky_{j'} = K$ (car $y_{j'} \in K$), on en déduit que $Kx_i = Kx_{i'}$, c'est-à-dire $i = j$. Une fois obtenu cela, on voit alors que $Hy_j = Hy_{j'}$ c'est-à-dire $j = j^{'}$.

On vient de montrer que la famille $\left\{Hy_jx_i\right\}_{(i,j)\in I\times J}$ forme une partition de G, mais comme chaque Hy_jx_i est une classe de conjugaison à droite de G modulo H on en déduit que la famille $\left\{y_jx_i\right\}_{(i,j)\in I\times J}$ est une classe de représentants des classes à droite modulo H dans G. On en déduit que

$$[G : H] = \sharp\left\{y_jx_i\right\}_{(i,j)\in I\times J} = \sharp(I \times J) = \sharp I.\sharp J = [G : K][K : H]$$

L'équivalence annoncée découle alors immédiatement de la formule ci-dessus.

□

1.3.2 Relations d'équivalences compatibles et groupes quotients

Proposition.— *Soit $(G,*)$ un groupe et $\mathcal{R}$ une relation d'équivalence compatible (avec la loi $*$). Le magma quotient $(G/\mathcal{R},\bar{*})$ est un groupe et la surjection canonique $s : G \to G/\mathcal{R}$ est un épimorphisme de groupes.*

Preuve : On sait que $(G/\mathcal{R},\bar{*})$ est un magma associatif et unifère puisque G en est un. Il suffit donc de vérifier que tout élément de $(G/\mathcal{R})$ est inversible, mais ceci est évident compte tenu du fait que $\overline{x * x^{-1}} = \overline{x} \,\bar{*}\, \overline{x^{-1}} = \overline{e}$ (i.e. $(\overline{x})^{-1} = \overline{x^{-1}}$).

□

On se propose dans cette partie de caractériser les relations d'équivalence compatible sur un groupe.

Proposition.— *Soit G un groupe et $\mathcal{R}$ une relation d'équivalence. Si $\mathcal{R}$ est compatible à droite (resp. à gauche), alors il existe un unique sous-groupe H de G tel que $\mathcal{R} = \mathcal{R}_H$ (resp. $\mathcal{R} =_H \mathcal{R}$).*

Preuve : Supposons $\mathcal{R}$ compatible à droite et notons H la classe d'équivalence du neutre e de G modulo $\mathcal{R}$. H n'est pas vide car $e \in H$, maintenant, si $x, y \in H$ alors on a $x\mathcal{R}y$ et donc, puisque $\mathcal{R}$ est compatible à droite, on a $xy^{-1}\mathcal{R}yy^{-1}$, c'est-à-dire $xy^{-1}\mathcal{R}e$, et donc $xy^{-1} \in H$ et, par les axiomes faibles, H est un sous-groupe de G.

Par ailleurs, on voit que pour $x, y \in G$, on a

$$x\mathcal{R}y \iff xy^{-1}\mathcal{R}e \iff xy^{-1} \in H \iff x\mathcal{R}_H y$$

et donc $\mathcal{R} = \mathcal{R}_H$. On voit immédiatement que H est unique pour cette propriété car H est la classe de e modulo $\mathcal{R}$.

□

Corollaire.— *Soit G un groupe et $\mathcal{R}$ une relation d'équivalence. Les propriétés suivantes sont équivalentes :*

i) $\mathcal{R}$ est compatible,

ii) il existe un (unique) sous-groupe H de G tel que $\mathcal{R} =_H \mathcal{R} = \mathcal{R}_H$.

Preuve : En vertu de la proposition précédente, il suffit de prouver que si H et H' sont deux sous-groupes de G tel que ${}_H\mathcal{R} = \mathcal{R}_{H'}$ alors $H = H'$, mais ceci est évident puisque la classe du neutre e modulo ${}_H\mathcal{R}$ est H alors que modulo $\mathcal{R}_{H'}$ c'est H'.

□

En particulier, on voit qu'il existe une correspondance biunivoque entre les relations d'équivalences compatibles sur G et les sous-groupes H de G vérifiants ${}_H\mathcal{R} = \mathcal{R}_H$.

Définition.— *Un sous-groupe H d'un groupe G est dit distingué (ou normal) dans G si ${}_H\mathcal{R} = \mathcal{R}_H$. On note alors $H \triangleleft G$.*

Lorsque H est distingué dans G, le magma quotient $\left(\frac{G}{H}\right)_d = \left(\frac{G}{H}\right)_g$ (qui est un groupe) est appelé groupe quotient de G par H et est noté plus simplement $\frac{G}{H}$.

Exemple : Si l'on prend le groupe $G = (\mathbb{Z}, +)$ et le sous-groupe $H = n\mathbb{Z}$ on voit que H est distingué dans G et que la relation $\mathcal{R}_H =_H \mathcal{R}$ n'est rien d'autre que la relation $\mathcal{R}_n$ de congruence modulo n. Ceci justifie pour quoi nous avons noté avant $\mathbb{Z}/n\mathbb{Z}$ à la place de $\mathbb{Z}/\mathcal{R}_n$.

1.3.3 Sous-groupes normaux

Proposition.— *Soit G un groupe et H un sous-groupe de G. Les propriétés suivantes sont équivalentes :*

i) H est distingué dans G,

ii) $\forall x \in G$, $xH = Hx$,

iii) $\forall x \in G$, $xHx^{-1} = H$,

iv) $\forall x \in G$, $x^{-1}Hx = H$,

v) $\forall \sigma \in \mathrm{Int}(G)$, $\sigma(H) = H$,

vi) $\forall h \in H$, $\forall x \in G$, $xhx^{-1} \in H$,

vii) $\forall h \in H$, $\forall x \in G$, $x^{-1}hx \in H$.

Preuve : Exercice.

□

Exemples : a) Si G est abélien alors tout sous-groupe de G est distingué dans G. La réciproque de cette propriété est fausse. En effet, le groupe Q_8 est non abélien et pourtant chacun de ses sous-groupes est distingué : soit H un sous-groupe non trivial de Q_8. Le théorème de Lagrange assure que $o(H) = 2$ ou 4. Si $o(H) = 4$, alors $[Q_8 : H] = 2$ et nous verrons au h) qu'un tel sous-groupe est forcément distingué. Supposons maintenant que $o(H) = 2$. Ainsi

H est cyclique, donc $H = \{I, M\}$ avec $M^2 = I$ et $M \neq I$, or il n'y a qu'une seule telle matrice M dans Q_8 et donc

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

Ce sous-groupe est distigué car I et $-I$ commuttent avec toutes matrices.

b) Si $f : G \longrightarrow G^{'}$ est un morphisme de groupe alors $\mathrm{Ker}(f)$ est distingué dans G. Par ailleurs, si H est distingué dans G, alors le neutre $\overline{e}$ du groupe quotient G/H est donc la classe d'équivalence du neutre e de G qui est visiblement H. Ainsi, on voit que le noyau de la surjection canonique $s : G \longrightarrow G/H$ est égal au sous-groupe H. Ceci permet de caractériser les sous-groupes distingués :

Proposition.— *Un sous-groupe H d'un groupe G est distingué si et seulement si il existe un épimorphisme de groupe $f : G \longrightarrow G^{'}$ tel que $H = \mathrm{Ker}(f)$.*

Preuve : Si $H = \mathrm{Ker}(f)$ alors H est distingué. Réciproquement, si H est distingué, alors H est le noyau de la surjection canonique $s : G \longrightarrow G/H$.

□

L'étude du groupe quotient $\dfrac{G}{\mathrm{Ker}(f)}$ est particulièrement instructif :

Théorème.— (Premier théorème d'isomorphisme) *Soit $f : G \longrightarrow G^{'}$ un morphisme de groupe. Les groupes $\mathrm{Im}(f)$ et $\dfrac{G}{\mathrm{Ker}(f)}$ sont isomorphes.*

Preuve : Considérons $x, y \in G$. On a

$$f(x) = f(y) \Longleftrightarrow f(x)(f(y))^{-1} = e^{'} \Longleftrightarrow f(xy^{-1}) = e^{'} \Longleftrightarrow xy^{-1} \in \mathrm{Ker}(f)$$

Ainsi, si $x, y \in G$ sont dans la même classe modulo $\mathrm{Ker}(f)$ alors $f(x) = f(y)$. Ceci permet de définir une application

$$\begin{array}{rccc} \varphi : & \dfrac{G}{\mathrm{Ker}(f)} & \longrightarrow & \mathrm{Im}(f) \\ & \overline{x} & \longmapsto & f(x) \end{array}$$

qui est visiblement surjective. Soient $\overline{x}, \overline{y} \in G/\mathrm{Ker}(f)$, comme $\overline{x.y} = \overline{x}.\overline{y}$, on en déduit que

$$\varphi(\overline{x}.\overline{y}) = \varphi(\overline{x.y}) = f(xy) = f(x)f(y) = \varphi(\overline{x})\varphi(\overline{y})$$

et donc que φ est un morphisme de groupe. Si $\overline{y} \in \mathrm{Ker}(\varphi)$, alors $f(y) = e^{'}$ et donc $y \in \mathrm{Ker}(f)$. Ceci justifie que $\mathrm{Ker}(\varphi) = \{\mathrm{Ker}(f)\}$ (qui est le neutre de $G/\mathrm{Ker}(f)$) et donc que φ est injectif.

□

Etant donnés une suite finie $G_0, \cdots, G_n$ de groupes et pour tout $i = 0, \cdots, n-1$ un homomorphisme de groupe $f_i : G_i \longrightarrow G_{i+1}$, on dit que la suite

$$G_0 \xrightarrow{f_0} G_1 \xrightarrow{f_1} \cdots \xrightarrow{f_{n-1}} G_n$$

est exacte si pour tout $i = 0, \cdots n-2$, on a $\mathrm{Ker}(f_{i+1}) = \mathrm{Im}(f_i)$.

Si l'on note 1 le groupe trivial, alors dire que l'on a la suite exacte

$$1 \longrightarrow N \xrightarrow{f} G$$

est juste dire que le morphisme f est injectif. De même, dire que l'on a la suite exacte

$$G \xrightarrow{f} H \longrightarrow 1$$

est juste dire que le morphisme g est surjectif. Ainsi, quand on a une suite exacte

$$1 \longrightarrow N \xrightarrow{f} G \xrightarrow{s} H \longrightarrow 1$$

on a $\mathrm{Ker}(s) = \mathrm{Im}(f)$ et comme s est surjective, on a $H \simeq G/\mathrm{Im}(f)$. Comme f est injective, les groupes N et $\mathrm{Im}(N)$ sont isomorphes, c'est pour cela que souvent on écrit $H \simeq G/N$.

Réciproquement, si N est un sous-groupe distingué de G, alors on a la suite exacte

$$1 \longrightarrow N \xrightarrow{f} G \xrightarrow{s} G/N \longrightarrow 1$$

où f est l'injection canonique de N dans G et s la surjection canonique de G dans son quotient modulo N.

c) Le centre $Z(G)$ d'un groupe G est distingué dans G. On alors :

Proposition.— *Soit G un groupe. Les groupes* $\mathrm{Int}(G)$ *et* $\dfrac{G}{Z(G)}$ *sont isomorphes.*

Preuve : Considérons l'application

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

Par définition de $\mathrm{Int}(G)$, l'application θ est surjective. Soit maintenant $g, g' \in G$, l'application $\sigma_{gg'}$ est définie pour tout $x \in G$ par

$$\sigma_{gg'}(x) = (gg')x(gg')^{-1} = gg'xg'^{-1}g^{-1} = g(\sigma_{g'}(x))g^{-1} = \sigma_g(\sigma_{g'}(x)) = (\sigma_g \circ \sigma_{g'})(x)$$

L'application θ est donc un épimorphisme de groupe et par application du premier théorème d'isomorphisme, les groupes $\mathrm{Im}(f) = \mathrm{Int}(G)$ et $G/\mathrm{Ker}(f)$ sont isomorphes. Soit $g \in G$, on a

$$\begin{array}{rcl} g \in \mathrm{Ker}(f) & \iff & \sigma_g = Id \iff \forall x \in G,\ gxg^{-1} = x \\ & \iff & \forall x \in G,\ gx = xg \iff g \in Z(G) \end{array}$$

et donc $\mathrm{Ker}(f) = Z(G)$.

□

Par ailleurs, on peut caractériser l'abélianité de G, grâce au groupe quotient $G/Z(G)$:

Proposition.— *Soit G un groupe de $Z(G)$ son centre. Les propriétés suivantes dont équivalentes :*

i) G est abélien,

ii) $Z(G) = G$,

iii) $G/Z(G)$ est trivial (i.e. réduit à un seul élément),

iv) $G/Z(G)$ est monogène.

Preuve : $i) \Rightarrow ii)$ Si G est abélien et $x \in G$, alors pour tout $y \in G$, on a $xy = yx$ et donc $x \in Z(G)$.

$ii) \Rightarrow iii)$ Si $G = Z(G)$ alors $G/Z(G) = \{Z(G)\} = \{\overline{e}\}$.

$iii) \Rightarrow iv)$ Un groupe trivial est évidement monogène.

$iv) \Rightarrow i)$ Si $G/Z(G)$ est monogène, il existe $a \in G$ tel que

$$G/Z(G) = <\overline{a}> = \{\overline{a}^n / \ n \in \mathbb{Z}\}$$

Soit $x, y \in G$,il existe donc $n, m \in \mathbb{Z}$ tels que $\overline{x} = \overline{a}^n$ et $\overline{y} = \overline{a}^m$ et par suite, il existe $z_x, z_y \in Z(G)$ tels que $x = a^n z_x$ et $y = a^m z_y$. On a donc

$$xy = a^n z_x a^m z_y = a^{n+m} z_x z_y = a^m a^n z_y z_x = a^m z_y a^n z_x = yx$$

et donc G est abélien.

□

d) Le sous-groupe $\mathrm{Int}(G)$ est distingué dans $\mathrm{Aut}(G)$. Le groupe quotient $\dfrac{\mathrm{Aut}(G)}{\mathrm{Int}(G)}$ s'appelle le groupe des automorphisme extérieur et se note $\mathrm{Ext}(G)$.

e) Soit A est une partie d'un groupe G et $H = <A>$. Si pour tout $g \in G$ et tout $a \in A$, on a $gag^{-1} \in H$, alors H est distingué dans G (Exercice). En particulier, si dans un groupe G un élément $x \in G$ vérifie que pour tout $g \in G$, il existe $n \in \mathbb{Z}$ tel que $gxg^{-1} = x^n$, alors le sous-groupe monogène $< x >$ est distingué dans G.

f) On considère le groupe S_3. On a vu que S_3 était engendré par les deux éléments $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. On a

$$S_3 = \{e, \sigma, \sigma^2, \tau, \sigma \circ \tau, \tau \circ \sigma\}$$

et $\sigma^2 \circ \tau = \tau \circ \sigma$ et $\tau \circ \sigma^2 = \sigma \circ \tau$.

On note $N =< \sigma >$ et $T =< \tau >$. On a vu que $o(N) = 3$ et que $o(T) = 2$ et d'après la formule des indices, il y a exactement deux classes à droite et à gauche modulo N. Ce sont

$$\left\{ \begin{array}{lcl} N & = & \{e, \sigma, \sigma^2\} \\ N\tau & = & \{\tau, \sigma \circ \tau, \tau \circ \sigma\} \end{array} \right. \qquad \left\{ \begin{array}{lcl} N & = & \{e, \sigma, \sigma^2\} \\ \tau N & = & \{\tau, \tau \circ \sigma, \sigma \circ \tau\} \end{array} \right.$$

On voit qu'elles coincident, donc N est distingué dans S_3. De même,il y a exactement trois classes à droite et à gauche modulo N. Ce sont

$$\left\{ \begin{array}{lcl} T & = & \{e, \tau\} \\ T\sigma & = & \{\sigma, \tau \circ \sigma\} \\ T\sigma^2 & = & \{\sigma^2, \sigma \circ \tau\} \end{array} \right. \qquad \left\{ \begin{array}{lcl} T & = & \{e, \tau\} \\ \sigma T & = & \{\sigma, \sigma \circ \tau\} \\ \sigma^2 T & = & \{\sigma^2, \tau \circ \sigma\} \end{array} \right.$$

On voit qu'elles ne coincident pas, donc T n'est pas distingué dans S_3.

g) (Groupe dérivé) Etant donné un groupe G et $x, y \in G$, on appelle commutateur de x et de y dans G l'élement $[x, y] = x^{-1}y^{-1}xy$. On appelle groupe dérivé de G le sous-groupe $D(G)$ de G engendré par l'ensemble des commutateurs (on voit que G est abélien si et seulement si $D(G) = \{e\}$). Le sous-groupe $D(G)$ est distingué dans G et on a

Proposition.— *Pour tout sous-groupe distingué N de G, les propriétés suivantes sont équivalentes :*

i) G/N est abélien,

ii) $D(G) \subset N$.

En particulier, $G/D(G)$ est abélien.

Preuve : $i) \Rightarrow ii)$ Soit $x, y \in G$, on a $\overline{x}.\overline{y} = \overline{y}.\overline{x}$ et donc

$$\overline{x^{-1}}.\overline{y^{-1}}.\overline{x}.\overline{y} = \overline{e}$$

mais comme $\overline{x^{-1}}.\overline{y^{-1}}.\overline{x}.\overline{y} = \overline{x^{-1}y^{-1}xy}$, on en déduit que $[x, y] \in N$. On a donc $D(G) \subset N$.

$ii) \Rightarrow i)$ Pour $x \in G$, on note $\overline{x}$ la classe de x modulo N. Pour tout $x, y \in G$, on a

$$\overline{x^{-1}}.\overline{y^{-1}}.\overline{x}.\overline{y} = \overline{x^{-1}y^{-1}xy} = \overline{e}$$

puisque par hypothèse, $[x, y] \in N$. On en déduit donc que $\overline{x}.\overline{y} = \overline{y}.\overline{x}$ c'est-à-dire que G/N est abélien.

□

h) Si H est un sous-groupe d'indice 2 d'un groupe G, alors H est distingué dans G. En effet, si $[G : H] = 2$ alors les ensembles $\left(\frac{G}{H}\right)_d$ et $\left(\frac{G}{H}\right)_g$ sont composé de 2 éléments. Soit $x \in G$ tel que $x \notin H$, on a donc $xH \neq H$ et donc $G = H \cup xH$ et $H \cap xH = \emptyset$. On a de même $G = H \cup Hx$ et $H \cap Hx = \emptyset$. On en déduit que $xH = Hx$ et donc H est distingué dans G.

i) Soit A et B deux groupes. Les sous-groupes $A \times \{e\}$ et $\{e\} \times B$ sont distingués dans le groupe produit $A \times B$. Cette propriété est, plus généralement, vraie pour tous les sous-groupes $q_i(G_i)$ d'un produit cartésien quelconque $\prod_{i \in I} G_i$.

Attention : Soit G un groupe et H, K deux sous-groupes de G tels que $H \leq K$.

a) Si $H \triangleleft G$ alors $H \triangleleft K$. La réciproque de cette propriété est fausse, il suffit de prendre $H = K$ et H non distingué dans G.

b) Si H est distingué dans G alors K n'est pas forcément distingué dans G (prendre $H = \{e\}$), de même si K est distingué dans G alors H ne l'est pas forcément dans G (prendre $K = G$).

c) Si H est distingué dans K et K est distingué dans G alors H n'est pas forcément distingué dans G. Nous verrons, sur un exemple, ce fait au paragraphe 2.3.

Proposition.— *Soit G un groupe et $\{H_i\}_{i \in I}$ une famille de sous-groupes distingués de G. Le sous-groupe $\bigcap_{i \in I} H_i$ est distingué dans G.*

Preuve : Soit $x \in \bigcap_{i\in I} H_i$ et $g \in G$, comme $H_i \triangleleft G$, on a $gxg^{-1} \in H_i$ pour tout $iu \in I$ et, par suite, $gxg^{-1} \in \bigcap_{i\in I} H_i$.

□

Proposition.— *Soit $G, G^{'}$ deux groupes et $f \in \mathrm{Hom}(G, G^{'})$.*

a) Si $H \triangleleft G$ alors $f(H) \triangleleft f(G)$, en particulier, si f est un épimorphisme alors $f(H)$ est distingué dans $G^{'}$.

b) Si $H^{'} \triangleleft G^{'}$ alors $f^{-1}(H^{'}) \triangleleft G$.

Preuve : a) Soit $h^{'} \in f(H)$, $g^{'} \in f(G)$ et $h \in H$, $g \in G$ tels que $h^{'} = f(h)$ et $g^{'} = f(g)$. Par hypothèse, on a $ghg^{-1} \in H$ donc

$$g^{'}h^{'}g^{'-1} = f(g)f(h)f(g)^{-1} = f(g)f(h)f(g^{-1}) = f(ghg^{-1}) \in H$$

et par suite $f(H) \triangleleft f(G)$.

b) Soit $h \in f^{-1}(H^{'})$ et $g \in G$. On a $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} \in H^{'}$ (car $f(h) \in H^{'}$). On en déduit donc que $ghg^{-1} \in f^{-1}(H^{'})$ et par suite que ce sous-groupe est bien distingué dans G.

□

Proposition.— *Soit H, K deux sous-groupes d'un groupe G.*

a) Si $H \triangleleft G$ alors $H \cap K \triangleleft K$.

b) Si $H \triangleleft G$ alors HK est un sous-groupe de G et $H \triangleleft HK$.

Preuve : a) Soit $x \in H \cap K$ et $y \in K$, on a $yxy^{-1} \in K$ car $x \in K$ et $yxy^{-1} \in H$ car $x \in H$ et $H \triangleleft G$, donc $yxy^{-1} \in H \cap K$ et par suite $H \cap K \triangleleft K$.

b) Soit $k \in K$ et $h \in H$, on a $kh = khk^{-1}k$ et comme $H \triangleleft G$, on a $khk^{-1} \in H$ et par suite $kh \in HK$. De même, on montre que $hk \in KH$, c'est-à-dire que $HK = KH$ et donc que HK est un sous-groupe de G. Par ailleurs, comme HK est un sous-groupe de G qui contient H, si $H \triangleleft G$, alors évidemment $H \triangleleft HK$.

□

Normalisateur

Définition.— *Soit G un groupe, $\mathcal{P}(G)$ son ensemble de parties. On dit que deux éléments $S, S^{'} \in \mathcal{P}(G)$ sont conjuguées s'il existe $g \in G$ tel que*

$$S^{'} = gSg^{-1} = \{gsg^{-1} / \ s \in S\}$$

On vérifie immédiatement que la relation "être conjuguée à" est une relation d'équivalence sur $\mathcal{P}(G)$, que l'on appelle relation de conjugaison. La classe d'équivalence d'une partie S modulo la relation de conjugaison est l'ensemble

$$\{gSg^{-1} / \ g \in G\}$$

on l'appelle classe de conjugaison de S.

Définition.— *Soit G un groupe et S une partie non vide de G. On appelle normalisateur de S dans G l'ensemble*

$$N_G(S) = \{g \in G / \ gSg^{-1} = S\}$$

et l'on appelle centralisateur de S l'ensemble

$$C_G(S) = \{g \in G / \ \forall s \in S, \ gsg^{-1} = s\}$$

Proposition.— *Les ensembles $N_G(S)$ et $C_G(S)$ sont des sous-groupes de G et $C_G(S) \triangleleft N_G(S)$.*

Preuve : Exercice.

□

On constate qu'un sous-groupe H d'un groupe G est distingué si et seulement si $N_G(H) = G$. En fait, la proposition suivante montre qu'en toute généralité, le sous-groupe $N_G(H)$ est le plus gros sous-groupe de G dans lequel H est distingué :

Proposition.— *Soit G un groupe.*

a) Pour tout sous-groupe H de G, on a $H \triangleleft N_G(H)$.

b) Si $H \leq K$ sont deux sous-groupes de G, alors si $H \triangleleft K$, on a $K \leq N_G(H)$.

c) Si $K \leq N_G(H)$, alors HK est un sous-groupe de G et $H \triangleleft HK$.

Preuve : a) Soit $x \in H$ et $y \in N_G(H)$, on a par définition $yxy^{-1} \in H$, donc $H \triangleleft N_G(H)$.

b) Si $H \triangleleft K$, alors pour tout $x \in K$, on a $xHx^{-1} = H$ et donc $x \in N_G(H)$.

c) Comme $H \triangleleft N_G(H)$, si $K \leq N_G(H)$ on a vu que HK était alors un sous-groupe de $N_G(H)$ (et donc de G) et que $H \triangleleft HK$.

□

1.3.4 Propriétés des groupes quotients, théorèmes d'isomorphisme

Propriété universelle

Théorème.— *Soit G un groupe, H un sous-groupe distingué de G et*

$$s : G \longrightarrow G/H$$

la surjection canonique. Si G' est un groupe et $f : G \longrightarrow G'$ un morphisme de groupes tel que $H \subset \mathrm{Ker}(f)$, alors il existe un unique morphisme

$$\varphi : G/H \longrightarrow G'$$

tel que $\varphi \circ s = f$.

Preuve : Existence. Soit $x, y \in G$ tel que $s(x) = s(y)$ (i.e. $xy^{-1} \in H$). Comme $\mathrm{Ker}(f) \subset N$, on a donc $xy^{-1} \in \mathrm{Ker}(f)$ et par suite $f(xy^{-1}) = e$ c'est-à-dire $f(x) = f(y)$. Cette remarque montre que si l'on pose, pour tout $\overline{x} \in G/H$

$$\varphi(\overline{x}) = f(x)$$

alors cette définition ne dépend pas du choix du représentant de la classe $\overline{x}$, et par suite φ définit une application de G/H dans G'. Il est alors évident que $\varphi \circ s = f$.

Reste à voir que φ est un morphisme de groupe, mais par définition, pour tout $\overline{x}, \overline{y} \in G/H$, on a

$$\varphi(\overline{x}.\overline{y}) = \varphi(\overline{xy}) = f(xy) = f(x)f(y) = \varphi(\overline{x})\varphi(\overline{y})$$

ce qui prouve bien que φ est un morphisme.

Unicité. Supposons avoir deux morphismes $\varphi, \varphi' : G/H \longrightarrow G'$ tels que $\varphi \circ s = f = \varphi' \circ s$. Comme s est surjective, l'égalite $\varphi \circ s = \varphi' \circ s$ implique $\varphi = \varphi'$.

□

Remarques : a) Dans le théorème ci-dessus, on voit que si f est surjectif alors φ l'est aussi puisque $\varphi \circ s = f$. De même, si $H = \mathrm{Ker}(f)$ alors φ est injective car si $\overline{x}$ est tel que $\varphi(\overline{x}) = e'$, alors $f(x) = e'$ et donc $x \in \mathrm{Ker}(f) = H$ et par suite $\overline{x} = H = \overline{e}$.

b) Ce théorème est une généralisation du 1er théorème d'isomorphisme. En effet, si $f : G \longrightarrow G'$ est un morphisme de noyau $\mathrm{Ker}(f)$, alors le théorème et la remarque précédente appliqués à $H = \mathrm{Ker}(f)$ montre qu'il existe un unique isomorphisme $\varphi : G/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}(f)$ tel que $\varphi \circ s = f$. Ceci permet de définir ce que l'on appelle la décomposition canonique du morphisme f : c'est la donnée des trois applications s, φ, i où $i : \mathrm{Im}(f) \longrightarrow G'$ désigne l'injection canonique. Elles font commuter le diagramme suivant :

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ {\scriptstyle s}\downarrow & & \uparrow{\scriptstyle i} \\ \dfrac{G}{\mathrm{Ker}(f)} & \xrightarrow{\ \varphi\ } & \mathrm{Im}(f) \end{array}$$

c'est-à-dire que $f = i \circ \varphi \circ s$. Il est à noter que i est injectif, φ bijectif et s surjectif.

Sous-groupes d'un groupe quotient

Proposition.— *Soit G un groupe, H un sous-groupe distingué de G et $s : G \longrightarrow G/H$ la surjection canonique.*

a) Si $\overline{K}$ désigne un sous-groupe de G/H, il existe un unique sous-groupe K de G contenant H tel que $s(K) = \overline{K}$: c'est le sous-groupe $K = s^{-1}(\overline{K})$, de plus on a $s(K) = \dfrac{K}{H}$.

b) Si K_1 est un sous-groupe de G, alors K_1H est un sous-groupe de G contenant H et $s(K_1) = \dfrac{K_1H}{H}$.

Preuve : a) $K = s^{-1}(\overline{K})$ est un sous-groupe de G qui contient $H = s^{-1}(\{\overline{e}\})$ (puisque $\overline{e} \in \overline{K}$, il vérifie visiblement $s(K) = \overline{K}$. Soit $K^{'}$ un sous-groupe de G contenant H et vérifiant $s(K^{'}) = \overline{K}$, on a $K^{'} \subset K$. Soit $\overline{\alpha} \in \overline{K}$ et $x \in K^{'}$ tel que $s(x) = \overline{\alpha}$. Comme $H \leq K^{'}$, on a $xH \subset K^{'}$ et donc $xH = s^{-1}(\overline{\alpha}) \subset K^{'}$. On en déduit donc que $K = s^{-1}(\overline{K}) \subset K^{'}$.

Par ailleurs, comme $H \triangleleft G$ et que $H \leq K \leq G$ on a $H \triangleleft K$ et donc $s(K) = \dfrac{K}{H}$.

b) Comme $H \triangleleft G$, on sait que HK_1 est un sous-groupe de G et que $H \triangleleft HK_1$, il s'ensuit que $s(HK_1) = \dfrac{HK_1}{H}$.

Par ailleurs, $s(K_1)$ est un sous-groupe de G/H et on a, pour $x \in G$,

$$s(x) \in s(K_1) \Longleftrightarrow \exists k_1 \in K_1,\ Hx = Hk_1 \Longleftrightarrow s(x) \in s(HK_1)$$

c'est-à-dire que $s(K_1) = \dfrac{HK_1}{H}$.

□

Cette proposition établit donc une correspondance biunivoque entre les sous-groupes de $\dfrac{G}{H}$ et les sous-groupes de G contenant H. Par exemple, il y a une correspondance entre les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ et les sous-groupes de $\mathbb{Z}$ qui contiennent $n\mathbb{Z}$. On sait que ces derniers sont exactement les $k\mathbb{Z}$ avec k divisant n, on en déduit que les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les $k\mathbb{Z}/n\mathbb{Z}$ avec $k|n$.

Proposition.— *Soit G un groupe, H un sous-groupe distingué de G et $K, K^{'}$ deux sous-groupes de G contenant H. On a :*

a) $K \leq K^{'} \Longrightarrow \dfrac{K}{H} \leq \dfrac{K^{'}}{H}$.

b) $K \triangleleft G \Longleftrightarrow \dfrac{K}{H} \triangleleft \dfrac{G}{H}$.

Preuve : a) Si $K \leq K^{'}$, alors $s(K) \leq s(K^{'})$ et donc $\dfrac{K}{H} \leq \dfrac{K^{'}}{H}$.

b) On a

$$\begin{aligned}
K \triangleleft G &\iff \forall (k,x) \in K \times G,\ xkx^{-1} \in K \\
&\Longrightarrow \forall (k,x) \in K \times G,\ s(xkx^{-1}) \in \frac{K}{H} \\
&\iff \forall (s(k), s(x)) \in \frac{K}{H} \times \frac{G}{H},\ s(x)s(k)s(x)^{-1} \in K \\
&\iff \frac{K}{H} \triangleleft \frac{G}{H}
\end{aligned}$$

L'implication réciproque de la deuxième ligne se démontre ainsi : si $\forall (k,x) \in K \times G,\ s(xkx^{-1}) \in \dfrac{K}{H}$, alors pour tout $x \in G$, le groupe xKx^{-1} est un sous-groupe de G qui contient H (puisque $H \subset K$ et que $H \triangleleft G$) dont l'image par s est $\dfrac{K}{H}$. La proposition précédente montre que $xKx^{-1} = K$, d'où l'implication réciproque.

□

2eme et 3eme théorèmes d'isomorphisme

Lemme.— *Soient G, $G^{'}$ deux groupes, $H \triangleleft G$, $H^{'} \triangleleft G^{'}$ deux sous-groupes distingués et $s : G \longrightarrow G/H$, $s^{'} : G^{'} \longrightarrow G^{'}/H$ les surjections canoniques. Si $f \in \mathrm{Hom}(G, G^{'})$ est tel que $f(H) \subset H^{'}$ alors il existe un unique $\overline{f} \in \mathrm{Hom}\left(\dfrac{G}{H}, \dfrac{G^{'}}{H^{'}}\right)$ tel que le*

diagramme suivant

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle s}\downarrow & & \downarrow{\scriptstyle s'} \\ \dfrac{G}{H} & \xrightarrow{\overline{f}} & \dfrac{G'}{H'} \end{array}$$

commute (i.e. $\overline{f} \circ s = s' \circ f$*).*

Preuve : On vérifie (exercice) que $\mathrm{Ker}(s' \circ f) = f^{-1}(H)$. La propriété universelle du groupe quotient montre alors qu'il existe un unique $\overline{f} \in \mathrm{Hom}\left(\dfrac{G}{H}, \dfrac{G'}{H'}\right)$ tel $\overline{f} \circ s = s' \circ f$.

□

Remarques : a) Si $s' \circ f$ est surjectif alors $\overline{f}$ l'est aussi, mais on notera que $s' \circ f$ peut être surjectif sans que f le soit.

b) La condition $\mathrm{Ker}(s' \circ f) = H$ équivaut à $f^{-1}(H') = H$, cette condition implique $\overline{f}$ injectif.

Théorème.— (2ème théorème d'isomorphisme) *Soient G un groupe et H un sous-groupe distingué de G. Pour tout sous-groupe K de G, les groupes quotients* $\dfrac{K}{H \cap K}$ *et* $\dfrac{HK}{H}$ *existent et sont isomorphes.*

Preuve : D'après ce qui précède comme $H \triangleleft G$, on sait que $H \cap K \triangleleft K$ et que $H \triangleleft HK$, ce qui justifie l'existence des groupes quotients $\dfrac{K}{H \cap K}$ et $\dfrac{HK}{H}$.

Considérons l'injection canonique

$$j : K \longrightarrow HK$$

et notons

$$s : K \longrightarrow \frac{K}{H \cap K} \text{ et } s' : HK \longrightarrow \frac{HK}{H}$$

les surjections canoniques. Comme par définition on a $j(H \cap K) = H \cap K \subset H$, il existe un unique morphisme $\varphi \in \mathrm{Hom}\left(\dfrac{K}{H \cap K}, \dfrac{HK}{K}\right)$ tel que le diagramme suivant

$$\begin{array}{ccc} K & \xrightarrow{j} & HK \\ {\scriptstyle s}\downarrow & & \downarrow{\scriptstyle s'} \\ \dfrac{K}{H \cap K} & \xrightarrow{\varphi} & \dfrac{HK}{H} \end{array}$$

commute. Montrons que φ est un isomorphisme : le morphisme $s' \circ j$ est surjectif, car

$$s' \circ j(K) = s'(K) = \frac{KH}{H}$$

et comme $s' \circ j = \varphi \circ s$, on en déduit que $\varphi \circ s$, et donc φ, sont surjectifs.

On a

$$(s' \circ j)^{-1}(\{e\}) = j^{-1}(s'^{-1}(\{e\})) = j^{-1}(H) = K \cap H$$

donc

$$s^{-1}(\varphi^{-1}(\{e\})) = (\varphi \circ s)^{-1}(\{e\}) = K \cap H$$

il s'ensuit que $\varphi^{-1}(\{e\}) = \{e\}$ et donc que φ est injective.

□

Remarque : Dans le cas de notation additive, on a donc $\dfrac{K}{H \cap K} \simeq \dfrac{H + K}{H}$. Dans le cas où H et K sont en somme directe, ce théorème justifie que $\dfrac{H \oplus K}{H} \simeq K$, puisque, par définition, $H \cap K = \{0\}$.

Théorème.— (3ème théorème d'isomorphisme) *Soient G un groupe et H, K deux sous-groupes distingués de G tels que $H \subset K$. On a*

$$\frac{G}{K} \simeq \frac{\frac{G}{H}}{\frac{K}{H}}$$

Preuve : On sait que, comme $K \triangleleft G$, on a $\frac{K}{H} \triangleleft \frac{G}{H}$ et par suite, le groupe quotient $\frac{G/H}{K/H}$ existe bien. Notons

$$s_H : G \longrightarrow \frac{G}{H},\ s_K : G \longrightarrow \frac{G}{K},\ \text{et } \pi : \frac{G}{H} \longrightarrow \frac{G/H}{K/H}$$

les surjections canoniques. On a $s_H(K) = \frac{K}{H}$, car $H \leq K$ et donc, il existe un unique $\varphi \in \mathrm{Hom}\left(\frac{G}{K}, \frac{G/H}{K/H}\right)$ tel que le diagramme suivant

$$\begin{array}{ccc} G & \xrightarrow{s_H} & \frac{G}{H} \\ {\scriptstyle s_K}\downarrow & & \downarrow{\scriptstyle \pi} \\ \frac{G}{K} & \xrightarrow{\varphi} & \frac{G/H}{K/H} \end{array}$$

commute. On vérifie (exercice) qu'alors φ est bien un isomorphisme.

□

Chapitre 2

Etude de quelques familles usuelles de groupes

2.1 Groupes monogènes et cycliques

2.1.1 Caractérisation

On rappelle qu'un groupe est dit monogène s'il est engendré par un de ses éléments, il est dit cyclique si, de plus, il est fini. Si G est un groupe monogène et $x \in G$ est un générateur de G, alors on a

$$G = \{x^k,\ k \in \mathbb{Z}\}$$

Notons que, dans ces conditions, l'application

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

est un épimorphisme de groupe (exercice). On voit aussi que si $f : G \longrightarrow G^{'}$ est un morphisme de groupe et que si G est monogène alors $\mathrm{Im}(f)$ est un groupe monogène (on remarqu'alors l'image d'un générateur de G est un générateur de $\mathrm{Im}(f)$).

Proposition.— *Soit G un groupe monogène.*

- *Si G est infini, alors $G \simeq \mathbb{Z}$.*
- *Si G est fini alors $G \simeq \mathbb{Z}/n\mathbb{Z}$ où $n = o(G)$.*

Preuve : Considérons l'épimorphisme $\varphi : \mathbb{Z} \longrightarrow G$ introduit plus haut. D'après le premier théorème d'isomorphisme, on a $G \simeq \mathbb{Z}/Ker(\varphi)$. Or, nous avons vu que les sous-groupes de $\mathbb{Z}$ était de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$, donc il existe n tel que $Ker(\varphi) = n\mathbb{Z}$.

- si $n = 0$, alors $Ker(\varphi) = \{0\}$ et par suite $G \simeq \mathbb{Z}$ et donc G est infini.
- si $n \neq 0$, alors $G \simeq \mathbb{Z}/n\mathbb{Z}$ et par suite G est fini et son ordre est celui de $\mathbb{Z}/n\mathbb{Z}$ c'est-à-dire n.

□

Corollaire.— *Deux groupes monogènes sont isomorphes si et seulement s'ils ont le même cardinal.*

Preuve : Immédiat.

□

Exemples : Le groupe μ_n des racines complexes de l'unité est cyclique d'ordre n.

2.1.2 Sous-groupes d'un groupe monogène

Proposition.— *Tout sous-groupe non trivial d'un groupe monogène infini est un groupe monogène infini. Tout sous-groupe d'un groupe cyclique est cyclique.*

Preuve : Les sous-groupes non triviaux de $\mathbb{Z}$ sont les $k\mathbb{Z}$ qui sont monogènes infinis et ceux de $\mathbb{Z}/n\mathbb{Z}$ sont les $k\mathbb{Z}/n\mathbb{Z}$ (pour $k|n$) qui sont cycliques. La proposition s'obtient alors en considérant, suivant le cas, un isomorphisme du groupe avec $\mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$.

□

Prenons $n \geq 1$. Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les sous-groupes $k\mathbb{Z}/n\mathbb{Z}$ avec $k|n$. On remarque que $o(k\mathbb{Z}/n\mathbb{Z}) = \frac{n}{k}$ et donc, en particulier, pour $d|n$ il n'y a qu'un seul sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d : c'est le sous-groupe $(n/d)\mathbb{Z}/n\mathbb{Z}$. On a de manière générale :

Théorème.— (Réciproque du théorème de Lagrange pour les groupes cycliques) *Soit $G =< x >$ un groupe cyclique d'ordre n. Pour tout diviseur d de n il existe un unique sous-groupe de G d'ordre d et ce sous-groupe est engendré par l'élément $x^{n/d}$.*

Preuve : Exercice.

□

Exemple : Soit $\mu_n = \{\exp(2ik\pi/n)/\ k \in \mathbb{Z}\}$ le groupe des racines complexes n-ième de l'unité. On voit que $\xi = \exp(2i\pi/n)$ est un générateur. Pour $d|n$, l'unique sous-groupe d'ordre d de μ_n est donc $< \xi^{n/d} >= \mu_d$ (exercice).

Proposition.— *Soit G un groupe. Si $x \in G$ est d'ordre n, alors pour tout $a \in \mathbb{Z}^*$, on a*

$$o(x^a) = \frac{n}{\text{p.g.c.d.}(a,n)} = \frac{\text{p.p.c.m.}(a,n)}{a}$$

Preuve : La deuxième égalité provient du fait que

$$an = \text{p.g.c.d.}(a,n).\text{p.p.c.m.}(a,n)$$

Notons $l = \text{p.g.c.d.}(a,n)$. Comme l divise a, on voit que an/l est un multiple de n et donc, par suite, $(x^a)^{(n/l)} = e$. Soit maintenant un entier $i \in \mathbb{N}$ tel que $(x^a)^i = e$. Puisque x est d'ordre n, il existe $k \in \mathbb{N}$ tel que $ia = kn$. Maintenant $ia = kn$ est visiblement un multiple de a et de n, donc de $q = \text{p.p.c.m.}(a,n)$ et par suite, on a $ia = k^{'}q$ avec $k^{'} \in \mathbb{N}$ et donc $i = k^{'}n/l$ ce qui montre bien que x^a est d'ordre n/l.

□

2.1.3 Générateurs

Proposition.— *Soit $G =< x >$ un groupe monogène.*

• *Si G est infini, alors les seuls générateurs de G sont x et x^{-1}.*

• *Si G est cyclique d'ordre $n \geq 2$ alors l'ensemble des générateurs de G est formé par les x^k avec $k \in \mathbb{Z}$ tel que $(n,k) = 1$.*

Preuve : • L'isomorphisme canonique $\mathbb{Z} \longrightarrow G$ fait correspondre biunivoquement les générateurs de ces deux groupes. Or (exercice) il n'y a que deux générateurs de $\mathbb{Z}$: ± 1 qui correspondent à x et x^{-1}.

• Les éléments de G sont les x^k avec $k \in \mathbb{Z}$ et x^k est un générateur ssi $o(x^k) = n$. Or $o(x^k) = \dfrac{n}{\text{p.g.c.d.}(n,k)}$, donc x^k est un générateur ssi $\text{p.g.c.d.}(n,k) = 1$.

□

Remarque : Soit $G =< x >$ cyclique d'ordre $n \geq 2$. Si $k \in \mathbb{Z}$ est premier à n, alors en effectuant la division euclidienne de k par n, on trouve qu'il existe $k^{'} \in \mathbb{Z}$ et $s \in \{1, \cdots, n-1\}$ tel que

$$k = k^{'}n + s$$

et donc $x^k = x^{k^{'}n+s} = x^{nk^{'}}x^s = x^s$. Par ailleurs, si on prend

$$s, s^{'} \in E(n) = \{k \in \{1, \cdots, n-1\}/\ (k,n) = 1\}$$

tel que $s \neq s^{'}$ alors $x^s \neq x^{s^{'}}$. Et par suite on voit qu'il y a une bijection entre les éléments de $E(n)$ et les générateurs de G. D'où :

Proposition-Définition.— *Soit G un groupe cyclique d'ordre $n \geq 2$, le nombre de générateurs de G est égal à*

$$\varphi(n) = \sharp E(n)$$

La fonction $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ définie par $\varphi(1) = 1$ et pour tout $n \geq 2$, $\varphi(n) = \sharp E_n$ s'appelle l'indicateur d'Euler.

2.1.4 Décomposition en produit cartésien d'un groupe cyclique

Décomposition

Un produit de groupes cycliques n'est par forcément un groupe cyclique. En effet considérons le groupe de Klein $\mathbb{Z} : 2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, on vérifie facilement que tout élément non trivial de ce groupe est d'ordre 2, doncil ne peut pas être cyclique car, étant d'ordre 4, alors il existerait un élément d'ordre 4. Nous allons, dans cette partie, regarder à quelles conditions le produit cartésien de deux groupe cyclique reste cyclique et nous en déduirons, pour un groupe cyclique quelconque, une décomposition en produit de groupes cycliques.

Lemme.— *Soient n, m deux entier positifs non nuls. On a $n\mathbb{Z} \cap m\mathbb{Z} = l\mathbb{Z}$ avec $l = \text{p.p.c.m.}(n, m)$. En particulier, les propriétés suivantes sont équivalentes :*

i) $(n, m) = 1$,

ii) $n\mathbb{Z} \cap m\mathbb{Z} = nm\mathbb{Z}$.

Preuve : L'ensemble $n\mathbb{Z} \cap m\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, il est donc de la forme $a\mathbb{Z}$ avec $a \geq 1$. On a $a\mathbb{Z} = n\mathbb{Z} \cap m\mathbb{Z} \subset \mathbb{Z}/n\mathbb{Z}$ et $a\mathbb{Z} \subset \mathbb{Z}/m\mathbb{Z}$, il s'ensuit que $n|a$ et $m|a$ et donc que $l|a$ c'est-à-dire $a\mathbb{Z} \subset l\mathbb{Z}$. Réciproquement, on a $n|l$ et $m|l$ donc $l\mathbb{Z} \subset n\mathbb{Z}$ et $l\mathbb{Z} \subset m\mathbb{Z}$ et donc $l\mathbb{Z} \subset n\mathbb{Z} \cap m\mathbb{Z} = a\mathbb{Z}$.

□

Théorème.— *Soient n, m deux entier positifs non nuls. Les propriétés suivantes sont équivalentes :*

i) $(n, m) = 1$,

ii) $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z}$.

Preuve : $i) \Rightarrow ii)$ Notons respectivement

$$\sigma : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \quad \pi : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

les surjections canonique et considérons le morphisme

$$\begin{array}{rccc} f : & \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & a & \longmapsto & (\sigma(a), \pi(a)) \end{array}$$

On a $a \in Ker(f)$ ssi $\sigma(a) = 0$ et $\pi(a) = 0$ c'est-à-dire ssi $a \in Ker(\sigma) \cap Ker(\pi) = n\mathbb{Z} \cap m\mathbb{Z} = nm\mathbb{Z}$ (d'après le lemme). Ainsi $Ker(f) = nm\mathbb{Z}$ et donc, d'après le premier théorème d'isomorphisme, on en déduit que $\text{Im}(f) \simeq \mathbb{Z}/nm\mathbb{Z}$. Par ailleurs l'ordre de $\mathbb{Z}/nm\mathbb{Z}$ (donc de $\text{Im}(f)$) est nm qui est égal à celui de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Donc f est surjective et $Im(f) = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

non $i) \Rightarrow$ *non* $ii)$ Supposons que $(n, m) = a \neq 1$. Comme $a|n$ et $a|m$, il existe un élément $x \in \mathbb{Z}/n\mathbb{Z}$ et un élément $y \in \mathbb{Z}/m\mathbb{Z}$ d'ordres a. Les éléments $(x, 0)$ et $(0, y)$ engendrent des sous-groupes distincts qui sont tous deux d'ordre a dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ ce qui empeche (à cause de la réciproque du théorème de Lagrange pour les groupes cycliques) $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ d'être cyclique, donc, en particulier d'être isomorphe à $\mathbb{Z}/nm\mathbb{Z}$.

□

Corollaire.— *Le produit direct de deux groupes cycliques est cyclique si et seulement si les ordres des deux groupes sont premiers entre eux.*

Preuve : Soit C_n et C_m deux groupes cycliques d'ordres respectifs n et m. Les groupe C_n et C_m sont respectivement isomorphes à $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$, donc le groupe produit $C_n \times C_m$ est isomorphe à $\mathbb{Z}/n \times \mathbb{Z}/m$. Si $(n, m) = 1$ alors, d'après ce qui précède, on a

$$C_n \times C_m \simeq \mathbb{Z}/n \times \mathbb{Z}/m \simeq \mathbb{Z}/nm\mathbb{Z}$$

et donc $C_n \times C_m$ est cyclique.

Si $(n, m) \neq 1$ et si $C_n \times C_m$ était cyclique, comme c'est un groupe d'ordre nm il serait isomorphe à $\mathbb{Z}/nm\mathbb{Z}$ et, par suite, on aurait $\mathbb{Z}/n \times \mathbb{Z}/m \simeq \mathbb{Z}/nm\mathbb{Z}$ ce qui est absurde d'après ce qui précède.

□

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

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{\alpha_n}\mathbb{Z}$$

Preuve : S'obtient par récurrence.

□

Calcul de $\varphi(n)$

Théorème.— *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.— *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.— *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

2.2 Groupes symétriques

2.2.1 Rappels, propriétés

Pour un entier $n \geq 1$, le groupe S_n est le groupe (pour la composition) des bijections de l'ensemble $\{1, \cdots, n\}$. C'est un groupe fini et son ordre est $o(S_n) = n!$. Si $n > 2$ alors S_n est un groupe non commutatif. Etant donné un élément $\sigma \in S_n$, on écrit

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

Les éléments de S_n sont appelés des permutations. L'identité, qui est le neutre de S_n sera noté e plutot que Id. L'usage veut aussi que l'on s'autorise à noter la composition dans S_n par l'absence de notation comme dans un groupe quelconque.

Si E désigne un ensemble à n éléments, alors les groupes $(\text{Perm}(E), \circ)$ et S_n sont isomorphes. (Exercice).

Si $n \leq m$, alors l'application $f : S_n \longrightarrow S_m$ qui à σ associe $\widetilde{\sigma}$ définie par

$$\widetilde{\sigma}(i) = \sigma(i) \text{ pour tout } i = 1, \cdots, n \text{ et } \widetilde{\sigma}(i) = i \text{ pour tout } i = n+1, \cdots, m$$

est un monomorphisme de groupe. On l'appelle le plongement canonique de S_n dans S_m.

Soit G un groupe et $x \in G$. L'application t_x "translation à gauche" par $x : g \longmapsto xg$ définit une bijection de G dans lui-même. Ainsi, étant donné un groupe fini G d'ordre n, que nous noterons $G = \{x_1, \cdots, x_n\}$, on définit une application

$$\begin{array}{rccc} \theta : & G & \longrightarrow & S_n \\ & x & \longmapsto & \sigma_x = ind \circ t_x \circ ind^{-1} \end{array}$$

où ind désigne l'application de G dans $\{1, \cdots, n\}$ qui à x_i associe i. Ainsi, on a $\sigma_x(i) = j$ ssi $xx_i = x_j$

Proposition-Définition.— *L'application θ est un monomorphisme de groupe. On l'appelle plongement canonique de G dans S_n.*

Preuve : Soit $x, y \in G$ tels que $\theta(x) = \theta(y)$. On a donc pour tout $i = 1, \cdots, n$, $ind \circ t_x \circ ind^{-1}(i) = ind \circ t_y \circ ind^{-1}(i)$ c'est-à-dire puisque ind est une bijection que pour tout $i = 1, \cdots, n$, $xx_i = yx_i$, on en déduit donc que $x = y$ et donc que θ est injective.

Soit $x, y \in G$ et $i \in \{1, \cdots, n\}$. On a $\theta(xy)(i) = ind \circ t_{xy}(x_i) = ind(xyx_i)$, or $yx_i = x_j$ où $j = \sigma_x(i)$ et $xx_j = x_k$ où $k = \sigma_y(j)$, on en déduit que $xyx_i = x_k$ où $k = \sigma_x \circ \sigma_y(i)$. Ceci étant valable pour tout $i = 1, \cdots, n$, on a bien $\theta(xy) = \theta(x) \circ \theta(y)$.

□

Cette proposition montre que tout groupe d'ordre n est isomorphe à un sous-groupe de S_n. Ceci suggère la grande richesse du groupe S_n et nous invite à étudier plus précisément ce groupe.

On remarque que l'on peut plonger G dans S_n non pas en utilisant la translation à gauche t_x mais celle à droite. Certains auteurs le font et le plongement obtenu, bien que différent est aussi appelé plongement canonique...

2.2.2 σ-orbite

Définition.—*Soit $\sigma \in S_n$, on appelle support de σ l'ensemble*

$$\text{Supp}(\sigma) = \{i \in \{1, \cdots, n\} / \ \sigma(i) \neq i\}$$

Remarques : (exercice)

a) On a $\text{Supp}(\sigma) = \emptyset \Longleftrightarrow \sigma = e$.

b) Quelle que soit $\sigma \in S_n$, $\sigma \neq e$, la restriction de σ à $\text{Supp}(\sigma)$ est un élément de $\text{Perm}(\text{Supp}(\sigma))$.

c) Quelle que soit $\sigma \in S_n$ et $k \in \mathbb{Z}$, on a $\text{Supp}(\sigma^k) \subset \text{Supp}(\sigma)$. Notons que cette inclusion peut être stricte. Toutefois, on a $\text{Supp}(\sigma^{-1}) = \text{Supp}(\sigma)$.

Proposition.— *Soit $\sigma, \sigma' \in S_n$. Si $\text{Supp}(\sigma) \cap \text{Supp}(\sigma') = \emptyset$ alors $\sigma\sigma' = \sigma'\sigma$.*

Preuve : Exercice.

□

Définition.— *Soit $\sigma \in S_n$ et $i \in \{1, \cdots, n\}$. On appelle σ-orbite de i l'ensemble*

$$\Omega_\sigma(i) = \{\sigma^r(i) / \ r \in \mathbb{Z}\}$$

Remarques : a) Si, sur l'ensemble $\{1, \cdots, n\}$, on définit la relation (d'équivalence) $\mathcal{R}_\sigma$ suivante :

$$i\mathcal{R}_\sigma k \Longleftrightarrow \exists r \in \mathbb{Z},\ \sigma^r(i) = k$$

on voit que la σ-orbite de i, $\Omega_\sigma(i)$ n'est rien d'autre que la classe d'équivalence de i modulo $\mathcal{R}_\sigma$.

b) Soit $\sigma \in S_n$ avec $\sigma \neq e$. Posons $k = o(\sigma)$, on a alors

$$< \sigma >= \{e, \sigma, \cdots, \sigma^{k-1}\}$$

il s'ensuit que pour tout $i = 1, \cdots, n$, on a

$$1 \leq \sharp\Omega_\sigma(i) \leq k$$

On remarqu'alors on a $\sharp(\Omega_\sigma(i)) = 1 \Longleftrightarrow i \notin \text{Supp}(\sigma)$ (on dit que la σ-orbite est ponctuelle). Ainsi, si $i \in \text{Supp}(\sigma)$, on a

$$2 \leq \sharp\Omega_\sigma(i) \leq k$$

c) Si $\{i_1, \cdots, i_m\}$ désigne une classe de représentants des σ-orbite de $\{1, \cdots, n\}$, c'est-à-dire une classe de représentants de l'ensemble quotient $\{1, \cdots, n\}/\mathcal{R}_\sigma$, alors les sous-ensembles $\{\Omega_\sigma(i_q)\}_{1 \leq q \leq m}$ forment une partition de $\{1, \cdots, n\}$, on a donc

$$n = \sum_{q=1}^{m} \sharp\Omega_\sigma(i_q)$$

Par exemple, pour $n = 6$ et $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$, on a

$$\Omega_\sigma(1) = \{1, 5, 3\},\ \Omega_\sigma(2) = \{2\},\ \Omega_\sigma(4) = \{4, 6\}$$

2.2.3 Cycles et transposition

Définition.— *Dans S_n on appelle cycle de longueur r ($1 \leq r \leq n$) ou alors r-cycle, toute permutation $\sigma \in S_n$ telle qu'il existe r entiers distincts deux à deux de $\{1, \cdots, n\}$, $j_1, \cdots, j_r$ tels que*

$$\sigma(j_1) = j_2, \sigma(j_2) = j_3, \cdots, \sigma(j_{r-1}) = j_r, \sigma(j_r) = j_1 \text{ et } \forall k \notin \{j_1, \cdots, j_r\},\ \sigma(k) = k$$

Un tel r-cycle sera noté $(j_1, \cdots, j_r)$ (son support est alors égal à $\{j_1, \cdots, j_r\}$).

On appelle transposition tout cycle de longueur 2.

On appelle permutation circulaire la permutation

$$\sigma = (1\ 2 \cdots n) = \begin{pmatrix} 1 & 2 & \cdots & n \\ 2 & 3 & \cdots & 1 \end{pmatrix}$$

Exemples : a) Tout cycle de longueur 1 est l'identité.

b) On a $S_2 = \{e, \tau\}$ où τ est la transposition (1 2). S_3 n'est composé que de cycles : e de longueur 1, trois transpositions $\tau_1 = (1\ 2)$, $\tau_1 = (2\ 3)$ et $\tau_3 = (1\ 3)$, et deux 3-cycles $\mu_1 = (1\ 2\ 3)$ (la permutation circulaire) et $\mu_2 = (1\ 3\ 2)$. On remarque qu'un n-cycle n'est pas forcément la permutation circulaire (pour $n = 3$ comparer μ_1 et μ_2).

Remarque : Une transposition est donc un élément de S_n qui échange deux éléments de $\{1, \cdots, n\}$ et laisse invariant les autres. Il y a donc une correspondance biunivoque entre les transpositions dans S_n et les paires d'éléments de $\{1, \cdots n\}$. On en déduit qu'il y a exactement $C_n^2 = \dfrac{n(n-1)}{2}$ transpositions dans S_n.

Proposition.— *Dans le groupe S_n, un r-cycle est un élément d'ordre r. En particulier, toute transposition est une involution (i.e. un élément égal à son propre inverse).*

Preuve : Soit $\sigma = (j_1\ j_2 \cdots j_r)$ un r-cycle. Il s'agit de montrer que $\sigma^r = e$ et que $\sigma^k \neq e$ pour $k = 1, \cdots r-1$.

Soit $k \in \{1, \cdots, r-1\}$, on a $\sigma^k(j_1) = j_{k+1} \neq j_1$ et donc $\sigma^k \neq e$. Maintenant, pour tout $l = 1, \cdots, r$, on a $\sigma^{r-l+1}(j_l) = j_1$

et donc $\sigma^r(j_l) = (\sigma^{l-1}\sigma^{r-l+1})(j_l) =) = \sigma^{l-1}(j_1) = j_l$. Par ailleurs comme $\sigma(k) = k$ pour tout $k \notin \{j_1, \cdots, j_l\}$, on a $\sigma^r(k) = k$ et, par suite, $\sigma^r = e$.

□

Remarque : L'inverse d'un r-cycle est un r-cycle, puisque

$$(j_1\ j_2\ \cdots j_r)^{-1} = (j_r\ j_{r-1}\ \cdots j_1)$$

Cependant un produit de r-cycle n'est pas forcément un cycle. Par exemple, dans S_4, si $\sigma = (1\ 2\ 3\ 4)$ désigne la permutation cicruclaire alors

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

qui n'est visiblement pas un cycle.

Proposition.— *Dans le groupe S_n, le conjugué d'un r-cycle est un r-cycle et réciproquement, deux r-cycles sont conjugués.*

Preuve : Soit $\gamma = (j_1\ \cdots\ j_r)$ un r-cycle et $\sigma \in S_n$. On a (exercice)

$$\sigma\gamma\sigma^{-1} = (\sigma(j_1)\ \cdots\ \sigma(j_r))$$

ce qui justifie que le conjugué d'un r-cycle est encore un r-cycle. Par ailleurs, si

$$\gamma = (j_1\ \cdots\ j_r)\ et\ \mu = (i_1\ \cdots\ i_r)$$

sont deux r-cycles, alors comme les ensembles $\{j_1, \cdots, j_r\}$ et $\{i_1, \cdots, i_r\}$ sont deux sous-ensembles de $\{1, \cdots, n\}$ de même cardinal, il existe un élément (éventuellement plusieurs) $\sigma \in S_n$ tel que $\sigma(j_l) = i_l$ pour tout $l = 1, \cdots, r$. On a alors, d'après ce qui précède, $\sigma\gamma\sigma^{-1} = \mu$.

□

Proposition.— *Soit $\sigma \in S_n$ telle que $\sigma \neq e$. Les propositions suivantes sont équivalentes :*

i) σ est un cycle,

ii) dans la partition en σ-orbites de $\{1, \cdots, n\}$, il n'existe qu'une seule σ-orbite non-ponctuelle (le cardinal de celle-ci est alors égal à la longueur du cyle σ).

Preuve : $i) \Rightarrow ii)$ Soit $\sigma = (j_1\ j_2\ \cdots j_r)$ un r-cycle, c'est un élément d'ordre r et l'on a

$$\Omega_\sigma(j_1) = \left\{j_1, \sigma(j_1), \cdots, \sigma^{r-1}(j_1)\right\} = \{j_1, j_2, \cdots, j_r\}$$

Par ailleurs, si $i \notin \mathrm{Supp}(\sigma)$, on a $\Omega_\sigma(i) = \{i\}$ et par suite il n'existe qu'une seule σ-orbite non ponctuelle et son cardinal est bien r.

$ii) \Rightarrow i)$ Si σ est une permutation ne possédant qu'une seule σ-orbite non ponctuelle de cardinal r :

$$\Omega_\sigma(j) = \{j, \sigma(j), \cdots, \sigma^{r-1}(j)\}$$

en posant $j_1 = j$, $j_2 = \sigma(j)$, $\cdots$, $j_r = \sigma^{r-1}(j)$, on voit que σ coincide avec le r-cycle $(j_1\ j_2\ \cdots\ j_r)$.

□

2.2.4 Générateurs

On dira de deux cycles qu'ils sont disjoints si leurs supports le sont.

Théorème.— *Soit $\sigma \neq e$ un élément de S_n. Il existe un unique entier $s \geq 1$ et une unique collection de cycles disjoints deux à deux $\gamma_1, \cdots, \gamma_s$ tous différents de e telle que*

$$\sigma = \gamma_1 \cdots \gamma_s$$

Preuve : Soit $\sigma \neq e$ dans S_n; le support de σ étant non vide, il existe au moins une σ-orbite non ponctuelle et toute σ-orbite non ponctuelle $\Omega_\sigma(i)$ permet de définir un cycle, en posant, si

$$\Omega_\sigma(i) = \{i, \sigma(i), \cdots, \sigma^{r-1}(i)\}$$

$\gamma = (j_1\ j_2\ \cdots\ j_r)$ où $j_k = \sigma^{k-1}(i)$ pour $k = 1, \cdots, r$. Le cycle γ associé à $\Omega_\sigma(i)$ a alors pour support $\Omega_\sigma(i)$ et la restriction de σ à $\Omega_\sigma(i)$ est égale à γ.

Notons $\{\Omega_q\}_{1\leq q\leq s}$ l'ensemble des σ-orbites non ponctuelles et notons $\{\gamma_q\}_{1\leq q\leq s}$ la collection des cycles associés. Les σ-orbites Ω_q étant disjointes deux-à-deux il s'ensuit que les cycles γ_q le sont également et par suite qu'ils commutent deux à deux. Posons

$$\mu = \gamma_1 \cdots \gamma_s$$

Si $i \notin \bigcup_{q=1}^{s} \Omega_q$, alors la σ-orbite de i est ponctuelle et donc $\sigma(i) = i$. Par ailleurs, pour tout $q = 1, \cdots, s$, on a $\gamma_q(i) = i$, ce qui montre que $\mu(i) = \sigma(i)$.

Si maintenant, $i \in \bigcup_{q=1}^{s} \Omega_q$, alors il existe un unique q tel que $i \in \Omega_q$ et pour tout $q \neq q^{'}$, on a $i \notin \Omega_{q^{'}}$. On a donc, pour $q^{'} \neq q$, $\gamma_{q^{'}}(i) = i$ et $\gamma_q(i) = \sigma(i)$ et par suite, comme

$$\mu = \gamma_q \gamma_1 \cdots \gamma_{q-1} \gamma_{q+1} \cdots \gamma_s$$

on a $\sigma(i) = \mu(i)$. Donc $\sigma = \mu$.

Supposons que

$$\sigma = \gamma_1^{'} \cdots \gamma_r^{'}$$

soit une autre décomposition eux cycles disjoints deux à deux tous différents de e. Les σ-orbites non ponctuelles correspondent à la réunion des uniques $\gamma_q^{'}$-orbites non ponctuelles, mais comme la décomposition en σ-orbites de l'ensemble $\{1, \cdots, n\}$ est unique, on en déduit donc que $r = s$. Par ailleurs, chaque σ-orbite correspond à un unique γ_q et un unique $\gamma_{q^{'}}^{'}$ et comme la restriction de σ sur sa σ-orbite correspond au cycle concerné, on voit que $\gamma_q = \gamma_{q^{'}}^{'}$. La correspondance se faisant visiblement bi-univoquement, on a $\{\gamma_q\}_{1\leq q\leq s} = \{\gamma_q^{'}\}_{1\leq q\leq s}$.

□

Remarques : a) Le fait que les cycles soient disjoints, implique qu'ils commutent deux à deux. Ainsi l'écriture de σ obtenue dans la théorème est unique à l'ordre près des facteurs. On parle alors de la décomposition canonique de σ en produit de cycles.

b) Ce théorème assure notamement que le groupe S_n est engendré par ses cycles.

Exemple : Si l'on reprend la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$ de S_6, la décomposition en σ-orbite $\Omega_\sigma(1) = \{1, 5, 3\}$, $\Omega_\sigma(2) = \{2\}$, $\Omega_\sigma(4) = \{4, 6\}$ de $\{1, 2, 3, 4, 5, 6\}$ implique que

$$\sigma = (1\ 5\ 3)(4\ 6)$$

Proposition.— *Si $\sigma \neq e$ désigne un élément de S_n et*

$$\sigma = \gamma_1 \cdots \gamma_s$$

sa décomposition canonique en produit de cycles, alors l'ordre de σ est égal au p.p.c.m. *des ordres des cycles γ_i (c'est-à-dire au* p.p.c.m. *des longueurs des γ_i).*

Preuve : Posons $l = \text{p.p.c.m.}(o(\gamma_i))$. Pour tout $i = 1, \cdots, s$, on a $l = k_i o(\gamma_i)$ avec $k_i \in \mathbb{N}^*$, et comme les γ_i commutent deux à deux, on en déduit que

$$\sigma^l = \gamma_1^l \cdots \gamma_s^l = (\gamma_1^{o(\gamma_1)})^{k_1} \cdots (\gamma_s^{o(\gamma_s)})^{k_s} = e$$

et donc si $v = o(\sigma)$, on a $v|l$.

D'autre part, si $\Omega_q = \text{Supp}(\gamma_q)$, alors $\sigma_{|\Omega_q} = \gamma_{q|\Omega_q}$ et donc, puisque $\sigma_{|\Omega_q}^v = Id$, on en déduit que $v|o(\gamma_q)$. Ceci étant valable pour tout $q = 1, \cdots, s$, on a $v|l$. Donc $v = l$.

□

Théorème.— *Toute permutation $\sigma \neq e$ de S_n se décompose (de manière non-unique) comme produit (non permutable en général) de transpositions.*

Preuve : En vertu du théorème de décomposition en cycle d'une permutation, pour montrer ce théorème, il faut et il suffit de le montrer dans le cas où σ est un r-cycle, mais si $\sigma = (j_1\ j_2\ \cdots j_r)$, on voit que

$$(j_1\ j_2\ \cdots j_r) = (j_1\ j_2)(j_2\ j_3) \cdots (j_{r-1}\ j_r)$$

ce qui achève la preuve.

□

Exemples : Si l'on reprend la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$ de S_6, on a vu que

$$\sigma = (1\ 5\ 3)(4\ 6)$$

et donc par suite, une décomposition possible en transposition de σ est

$$\sigma = (1\ 5)(5\ 3)(4\ 6)$$

Proposition.— *Soit $n \geq 2$, on a*

$$S_n = \left\langle \{(1,i)\}_{2\leq i\leq n} \right\rangle = \left\langle \{(i,i+1)\}_{1\leq i\leq n-1} \right\rangle$$

Preuve : Pour ces propriétés, il suffit donc, en vertu de ce qui précède, de montrer que toute transposition appartient à $\left\langle \{(1,i)\}_{2\leq i\leq n} \right\rangle$ et $\left\langle \{(i,i+1)\}_{1\leq i\leq n-1} \right\rangle$.

Comme, pour tout $j,k \in \{1,\cdots,n\}$, on a $(j,k) = (1,j)(1,k)(1,j)$, on en déduit que

$$S_n = \left\langle \{(1,i)\}_{2\leq i\leq n} \right\rangle$$

Considérons p et q tels que $1 \leq p < q \leq n$ et montrons par récurrence sur $q-p$ que $(p,q) \in \left\langle \{(i,i+1)\}_{1\leq i\leq n-1} \right\rangle$:
Pour $q-p = 1$ c'est évident car $(p,q) = (p,p+1)$.
Si la propriété est vraie pour $q-p \geq 1$, alors au rang $q-p+1$, on voit que

$$(p,q) = (q-1,q)(p,q-1)(q-1,q)$$

et donc par application de l'hypothèse de récurrence, on a

$$(p,q) \in \left\langle \{(i,i+1)\}_{1\leq i\leq n-1} \right\rangle$$

□

2.2.5 Signature d'une permutation

Définition.— *Soit $\sigma \in S_n$. On appelle nombre d'inversions de σ, le nombre de paires $\{i,j\} \in \{1,\cdots,n\}$ telles que la restriction de σ à $\{i,j\}$ soit décroissante (i.e. si $i > j$ alors $\sigma(i) < \sigma(j)$ et si $i < j$ alors $\sigma(i) > \sigma(j)$). On note ν_σ cet entier.*

Exemple : Dans S_5, on considère $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$. Les paires $\{i,j\}$ où il y a inversion sont $\{1,2\}$, $\{1,3\}$, $\{1,4\}$, $\{1,5\}$, $\{2,3\}$, $\{2,4\}$ et $\{3,4\}$. Ainsi, on a $\nu_\sigma = 7$.

Lemme.— *Soit $\sigma \in S_n$ et $a_1,\cdots a_n$ des nombres réels distincts deux à deux. On pose pour tout $i = 1,\cdots,n$, $b_i = a_{\sigma(i)}$. On a*

$$(-1)^{\nu_\sigma} = \prod_{1\leq i<j\leq n} \frac{b_j - b_i}{a_j - a_i}$$

Preuve : L'ensemble des couples (i,j) tels $1 \leq i < j \leq n$ décrit exactement l'ensemble des paires $\{i,j\}$. Comme σ est une permutation il s'ensuit que l'ensemble des couples $(\sigma(i),\sigma(j))$ tels que $1 \leq i < j \leq n$ décrit lui aussi exactement l'ensemble des paires $\{i,j\}$. Par ailleurs, comme on a

$$\prod_{1\leq i<j\leq n} \frac{b_j - b_i}{a_j - a_i} = \frac{\displaystyle\prod_{1\leq i<j\leq n} b_j - b_i}{\displaystyle\prod_{1\leq i<j\leq n} a_j - a_i}$$

on voit que ce produit est de module 1. Maintenant, si sur le couple $\{i,j\}$ la permutation σ présente une inversion, le facteur $b_j - b_i$ au numérateur sera égal à l'opposé d'un facteur $a_{j'} - a_{i'}$ du dénominateur, au contraire, si σ ne

présente pas d'inversion sur la paire $\{i,j\}$ alors le facteur au dénominateur le facteur $b_j - b_i$ au numérateur sera égal à un facteur $a_{j'} - a_{i'}$ au dénominateur. Le produit considéré est donc égal à $(-1)^m$ où m est le nombre de paires où σ présente une inversion, c'est à dire à $(-1)^{\nu_\sigma}$.

□

Définition.— *Soit $\sigma \in S_n$. On appelle signature de σ l'entier (égal à ± 1) $\epsilon_\sigma = (-1)^{\nu_\sigma}$. On dira que σ est pair (resp. impaire) si $\epsilon_\sigma = 1$ (resp. si $\epsilon_\sigma = -1$).*

Corollaire.— *L'application*

$$\begin{array}{rccc} \epsilon : & S_n & \longrightarrow & \{1,-1\} \\ & \sigma & \longmapsto & \epsilon_\sigma \end{array}$$

est un morphisme de groupe (l'ensemble $\{1,-1\}$ étant considéré comme sous-groupe multiplicatif de $(\mathbb{Q}^*,.)$).

Preuve : Soit $\sigma, \sigma^{'} \in S_n$. Prenons des réels $a_1, \cdots, a_n$ distincts deux à deux. Posons pour tout $i = 1, \cdots, n$, $b_i = a_{\sigma(i)}$ et $c_i = b_{\sigma'}(i)) = a_{\sigma'\sigma(i)}$. Par application de la proposition précédente, on a

$$\begin{aligned} \epsilon_{\sigma'\sigma} &= \frac{\prod\limits_{1\le i<j\le n} c_j - c_i}{\prod\limits_{1\le i<j\le n} a_j - a_i} \\ &= \frac{\prod\limits_{1\le i<j\le n} c_j - c_i}{\prod\limits_{1\le i<j\le n} b_j - b_i} \cdot \frac{\prod\limits_{1\le i<j\le n} b_j - b_i}{\prod\limits_{1\le i<j\le n} a_j - a_i} \\ &= \epsilon_{\sigma'}.\epsilon_\sigma \end{aligned}$$

□

Proposition.— *Toute transposition est impaire, en particulier, si $n \geq 2$ alors l'application ϵ est un épimorphisme.*

Preuve : Comme pour tout $l, k \in \{1, \cdots, n\}$ distincts, on a $(l\ k) = (1\ l)(1\ k)(1\ l)$ et que ϵ est un morphisme, il suffit de montrer cette proposition dans le cas d'une transposition du type $(1\ l)$ pour $l \geq 2$. Les inversions de $(1\ l)$ sont $\{1,2\}, \{1,3\}, \cdots, \{1,l\}$ et $\{2,l\}, \{3,l\}, \cdots, \{l-1,l\}$ (si $l \geq 3$). Il y en a donc $l - 1 + l - 2 = 2l - 3$ et donc

$$\epsilon_{(1\ l)} = (-1)^{2l-3} = -1$$

□

Corollaire.— *Si $\sigma \in S_n$ est le produit de k transpositions, alors $\epsilon_\sigma = (-1)^k$.*

Preuve : Immédiat.

□

2.2.6 Le groupe alterné A_n

Définition.— *On appelle groupe alterné de degré n le sous-ensemble A_n de S_n constitué des permutations paires.*

Proposition.— *Pour $n \geq 2$, l'ensemble A_n est un sous-groupe de S_n d'ordre $\frac{n!}{2}$. On a $A_n \triangleleft S_n$ et $\frac{A_n}{S_n} \simeq \mathbb{Z}/2\mathbb{Z}$.*

Preuve : Ces résultats sont immédiats une fois que l'on a constaté que A_n est le noyau du morphisme signature

$$\epsilon : S_n \longrightarrow \{1,-1\}$$

□

Si $n \geq 3$ et si $\sigma = (i\ j\ k)$ désigne un 3-cycle de S_n on constate (exercice) que $\epsilon_\sigma = 1$, c'est-à-dire que $\sigma \in A_n$. Les 3-cycles jouent un rôle essentiel dans A_n :

Théorème.— *Pour $n \geq 3$, le sous-groupe de S_n engendré par les 3-cycles est égal à A_n.*

Preuve : Pour tout $i, j, k, l \in \{1, \cdots, n\}$, on a

$$(i\ j)(k\ l) = (i\ j\ k)(j\ k\ l)$$

Par ailleurs, un élément de A_n est le produit d'un nombre pair de transpositions, ce qui justifie le résultat.

□

2.3 Groupes diédraux

On considère dans ce paragraphe le plan affine et euclidien $\mathcal{P}$ rapporté à un repère orthonormé $(O, \vec{i}, \vec{j})$. Pour tout entier $n \geq 2$ on considère un polygone régulier P_n à n sommets, centré en O et tel que l'un de ses sommets soit sur l'axe Ox. On considère alors D_n, l'ensemble des isométries du plan $\mathcal{P}$ qui conserve P_n (c'est-à-dire des isométries σ vérifiant $\sigma(P_n) = P_n$. On voit immédiatement que D_n est un groupe pour la composition.

Définition.— *Pour tout $n \geq 2$, le groupe D_n s'appelle le groupe diédral de degré n.*

Proposition.— *Pour $n \geq 2$, D_n est un groupe fini d'ordre $2n$.*

Preuve : Notons $A_1, \cdots, A_n$ les n sommets de P_n énumérés dans le sens trigonométrique en prenant $A_1 \in Ox$. On constate que si l'on regarde $\cap P$ comme le plan complexe, alors les A_k correspondent aux racines n-ième de l'unité, plus précisément, on a pour tout $k = 1, \cdots, n$

$$A_k = \exp\left(\frac{2i(k-1)\pi}{n}\right)$$

Pour tout $k = 0, \cdots, n-1$, on note ρ_k la rotation de centre O et de rayon $2ik\pi/n$. On voit que $\rho_k = \rho_1^k$ et par suite que l'ensemble de ces rotations forme un sous-groupe cyclique Γ_n de D_n d'ordre n.

Notons σ la symétrie d'axe Ox. On voit que $\sigma \in D_n$ et plus spécialement que $\sigma(A_1) = A_1$ et que pour tout $k \in \{2, \cdots, n\}$ on a

$$\sigma(A_k) = A_{n-k+2}$$

Il est clair que $\sigma \notin \Gamma_n$ car $\sigma \neq Id$ et $\sigma(A_1) = A_1$ or pour tout $k = 1, \cdots, n-1$ on a $\rho_1^k(A_1) = A_{1+k}$. Par ailleurs, pour tout $k = 0, \cdots, n-1$, on a $\rho_1^k \circ \sigma \notin \Gamma_n$, sinon, comme Γ_n est un sous-groupe on aurait $\sigma \in \Gamma_n$. Enfin les éléments $\rho_1^k \circ \sigma$ sont distincts deux à deux pour $k \in \{0, \cdots, n-1\}$.

Tout ceci montre que D_n contient au moins $2n$ éléments qui sont

$$\{Id, \rho_1, \cdots, \rho_1^{n-1}, \sigma, \rho_1 \circ \sigma, \cdots, \rho_1^{n-1} \circ \sigma\}$$

Pour $n = 2$ on vérifie sans mal que D_2 compte deux éléments. Si $n \geq 3$, on remarque qu'une isométrie f présevant P_n est entièrement déterminée par l'image des sommets de P_n. Ainsi donc, il y a n choix possible pour $f(A_1)$, mais comme f est une isométrie, on a $d(A_1, A_2) = d(f(A_1), f(A_2))$ et donc il n'y a que deux choix possibles pour $f(A_2)$. Enfin, une fois fixé $f(A_1)$ et $f(A_2)$, toujours parce que f est une isométrie, on voit qu'il n'y a qu'un seul choix possible pour $f(A_k)$ pour $k = 3, \cdots, n$. Ceci justifie donc que $\sharp D_n \leq 2n$.

□

Remarques : (Exercices) On conserve les notations de la preuve.

a) On remarque que pour tout $k = 0, \cdots, n-1$, on a $\sigma \circ \rho_h \circ \sigma = \sigma \circ \rho_h \circ \sigma^{-1} = \rho_h^{-1}$. En particulier, on constate que pour $n \geq 3$, D_n n'est pas abélien.

b) Pour $n = 2$, on voit que D_2 est isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. pour $n = 3$, le groupe D_3 est isomorphe au groupe S_3. De manière générale, on voit que D_n est isomorphe à un sous-groupe de S_n. Le groupe D_4 n'est pas isomorphe au groupe Q_8 car Q_8 n'a qu'un seul élément d'ordre 2 alors que D_4 en a 5.

c) On a $\Gamma_n \triangleleft D_n$. Plus exactement, on a la suite exacte

$$1 \longrightarrow \Gamma_n \xrightarrow{i} D_n \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

d) Pour $n \geq 2$ et tout $k = 1, \cdots, n-1$, les éléments $\rho_k \circ \sigma$ et $\sigma \circ \rho_h$ sont distincts et d'ordre 2.

Théorème.— *Si G est un groupe engendré par deux éléments a et b vérifiant $o(a) = n \geq 2$, $o(b) = 2$ et $o(ab) = 2$, alors G est isomorphe à D_n.*

Preuve : Comme $o(a) = n$ on voit que G contient un sous-groupe cyclique d'ordre n qui est $\{e, a, \cdots, a^{n-1}\}$. Par ailleurs, comme $o(ab) = 2$, on a $a(bab) = e$ et donc $bab = a^{-1}$ et par suite $ba^k b = ba^k b^{-1} = a^{n-k}$ (puisque $b = b^{-1}$). On en déduit, comme on l'a fait pour D_n, que les éléments $\{e, a, \cdots, a^{n-1}, b, ab, \cdots, a^{n-1}b\}$ sont distinct deux à deux.

Comme $G =< a, b >$, tout élément de G s'écrit comme un produit formel de puissance de a et de b, mais comme $ba^k = a^{n-k}b$, on en déduit par récurrence que tout élément de G s'écrit sous la forme $a^i b^j$ avec $i, j \in \mathbb{Z}$, mais comme $o(a) = n$ et $o(b) = 2$, on voit que l'on peut prendre $i = 0, \cdots, n-1$ et $j = 0, 1$. Ainsi, on a

$$G = \{e, a, \cdots, a^{n-1}, b, ab, \cdots, a^{n-1}b\}$$

On voit alors que l'application $\varphi : G \longrightarrow D_n$ définie par

$$\varphi(a^i b^j) = \rho_1^i \circ \sigma^j$$

est un isomorphisme de groupe.

□

Un contre-exemple à l'implication $H \triangleleft K \triangleleft G \Longrightarrow H \triangleleft G$: On considère le groupe $G = D_4$ et l'on note $\rho = \rho_1$. Soit $H = \{e, \sigma\}$ et $K = \{e, \sigma, \rho^2, \sigma\rho^2\}$. On vérifie facilement que $H \leq K \leq G$. Maintenant, pour des raisons de cardinalité évidente, on a $[G : K] = 2$ et $[K : H] = 2$. Il s'ensuit que $H \triangleleft K \triangleleft G$. Et pourtant, H n'est pas distingué dans G : en effet, on a

$$\rho \circ \sigma \circ \rho^{-1} = \rho \circ \sigma \circ \sigma \circ \rho \circ \sigma = \rho^2 \circ \sigma \notin H$$

2.4 Groupes simples

Définition.— *Un groupe G est dit simple s'il ne possède pas d'autres sous-groupes distingués que $\{e\}$ et lui-même.*

Proposition.— *Un groupe abélien est simple si et seulement s'il est cyclique d'ordre premier.*

Preuve : Exercice.

□

Remarques : a) Si G est un groupe simple, on ne peut rien dire sur la simplicité de ses sous-groupes et de ses quotients. Ils peuvent l'être ou pas...

b) Un groupe fini d'ordre p^n avec p premier et $n \geq 2$ n'est jamais simple. En effet, s'il est commutatif il possède un sous-groupe d'ordre p (exercice) qui est donc normal et non trivial. Si G n'est pas commutatif, on sait que $Z(G)$ n'est pas trivial, étant distingué dans G, G n'est pas simple.

Théorème.— *Pour $n \geq 5$, le groupe alterné A_n est simple.*

Preuve : Considérons un sous-groupe $H \triangleleft A_n$ différent de $\{e\}$. Comme H est distingué, si H possède un 3-cycle, il les possède tous (car les 3-cycles sont conjugués deux à deux dans S_n mais aussi dans A_n (exercice)) et, par suite, comme les 3-cycles engendrent A_n, on en déduit que $H = A_n$. Ainsi, pour montrer la simplicité de A_n, il suffit de montrer que H contient un 3-cycle.

Considérons $\tau \in H$, $\tau \neq e$ et $i \in \mathrm{Supp}(\tau)$. Posons $j = \tau(i)$ et prenons un $k \in \{1, \cdots, n\} - \{i, j, \tau^{-1}(i)\}$. Posons $l = \tau(k)$ et considérons l'élément

$$\sigma = \alpha^{-1}\tau\alpha\tau^{-1} \text{ avec } \alpha = (i\ j\ k)$$

Comme H est distingué dans A_n, on a $\sigma \in H$. Le calcul de σ donne :

$$\sigma = (i\ j\ k)^{-1}\tau(i\ j\ k)\tau^{-1} = (k\ j\ i)(\tau(i)\ \tau(j)\ \tau(k)) = (k\ j\ i)(j\ m\ l)$$

avec $m = \tau(j)$. On en déduit que $\sharp\mathrm{Supp}(\sigma) \leq 5$. Les entiers i, j, k sont visiblement distincts deux à deux. L'entier l ne peut être égal à i ou à j. On a donc deux cas :

1) $l \neq k$. L'entier m est forcément différent de l et de j. Il y a donc, a priori, trois possibilités : a) $m \notin \{i, j, k, l\}$, b) $m = i$, c) $m = k$.

1.a) On a $\sigma = (k\ j\ i)(j\ m\ l) = (i\ k\ j\ m\ l)$. Posons $\beta = (i\ k\ j)$, on a alors

$$\beta^{-1}\sigma\beta\sigma^{-1} = (j\ k\ i)(i\ k\ j\ m\ l)(i\ k\ j)(l\ m\ j\ k\ i) = (i\ j\ m)$$

qui est un 3-cycle, mais comme H est distingué dans A_n, on a $\beta^{-1}\sigma\beta\sigma^{-1} \in H$.

1.b) On a $\sigma = (k\ j\ i)(j\ i\ l) = (i\ l)(j\ k)$. Comme $n \geq 5$, il existe $p \in \{1, \cdots, n\} - \{i, j, k, l\}$. Posons $\beta = (i\ k\ p)$, on a alors

$$\beta^{-1}\sigma\beta\sigma^{-1} = (p\ k\ i)(i\ l)(j\ k)(i\ k\ p)(i\ l)(j\ k) = (i\ p\ l\ j\ k)$$

qui est dans H. En appliquant le même raisonement qu'au 1.a), on en déduit que H possède un 3-cycle.

1.c) On a $\sigma = (k\ j\ i)(j\ k\ l) = (i\ k\ l)$, et σ est donc un 3-cycle.

2) $l = k$. L'entier m étant différent de l et de j, il y a donc, a priori, deux possibilités : a) $m = i$, b) $m \notin \{i, j, k\}$.

2.a) On a donc $\sigma = (k\ j\ i)(j\ i\ k) = (i\ j\ k)$ et donc σ est un 3-cycle.

2.b) On a donc $\sigma = (k\ j\ i)(j\ m\ k) = (i\ k)(j\ m)$. En appliquant le même raisonement qu'au 1.b), on trouve que H possède un 3-cycle.

Dans tous les cas H possède un 3-cycle et donc que $H = A_n$.

□

2.5 Groupes résolubles

2.5.1 Suites de composition

Définition.— *Soit G un groupe, on appelle suite de composition (ou suite normale) de G toute suite finie*

$$\{e\} = G_0 \leq G_1 \leq \cdots \leq G_n = G$$

de sous-groupes tels que, pour tout $i = 0, \cdots, n-1$ on ait $G_i \triangleleft G_{i+1}$. L'entier n s'appelle alors la longueur de la suite et les groupes $\dfrac{G_{i+1}}{G_i}$ sont appelés les quotients de la suite.

Exemples : a) Pour tout groupe G, la suite $\{e\} \leq G$ est une suite de composition.

b) Considérons le groupe symétrique S_4 et les sous-groupes

$$H = \{e, (1\ 2)(3\ 4)\} \text{ et } K = \{e, (1\ 2)(3\ 4), (1\ 4)(2\ 3)\}$$

La suite

$$\{e\} \leq H \leq K \leq A_4 \leq S_4$$

est une suite de composition (exercice).

Définition.— *Un groupe G est dit résoluble s'il existe une suite de composition*

$$\{e\} = G_0 \leq G_1 \leq \cdots \leq G_n = G$$

telle que, pour tout $i = 0, \cdots, n-1$, le quotient $\dfrac{G_{i+1}}{G_i}$ soit abélien.

Exemples : a) Tout groupe abélien est résoluble.

b) Les groupes diédraux D_n sont résolubles. En effet, le sous-groupe Γ_n de D_n composé des rotations est un sous-groupe distingué et donc, la suite

$$\{e\} \triangleleft \Gamma_n \triangleleft D_n$$

est une suite de composition à quotients abéliens, puisque ces derniers sont respectivement $\dfrac{\Gamma_n}{\{e\}} = \Gamma_n$ et $\dfrac{D_n}{\Gamma_n} \simeq \mathbb{Z}/2\mathbb{Z}$ qui sont des groupes cycliques.

c) S_4 est résoluble. En effet, le suite de composition de l'exemple précédent est à quotients abéliens (exercice).

d) Les seuls groupes simples résolubles sont les groupes cycliques d'ordre premier. En particulier le groupe alterné A_n n'est pas résoluble pour $n \geq 5$.

2.5.2 Propriétés et caractérisation

Rapelons qu'étant donné un groupe G, on appelle groupe dérive de G le sous-groupe $D(G)$ de G engendré par les commutateurs. On sait qu'alors $D(G) \triangleleft G$. Pour tout entier $n \geq 0$, on définit par récurrence les sous-groupe $D_n(G)$ par

$$D_0(G) = G,\ \forall n \geq 0,\ D_{n+1}(G) = D(D_n(G))$$

On voit alors que la suite $(D_n(G))_n$ vérifie :

$$\cdots \triangleleft D_n(G) \triangleleft D_{n-1}(G) \triangleleft \cdots \triangleleft D_0(G)$$

Théorème .— *Soit G un groupe, les propositions suivantes sont équivalentes :*

i) G est résoluble,

ii) Il existe $n \in \mathbb{N}$ tel que $D_n(G) = \{e\}$.

Preuve : $i) \Rightarrow ii)$ Soit

$$\{e\} = H_0 \triangleleft \cdots \triangleleft H_n = G$$

un suite de composition de G à quotients abéliens. Comme $\dfrac{G}{H_{n-1}}$ est abélien, on en déduit que $D_1(G) \leq H_{n-1}$. Mais maintenant, comme $D_1(G) \leq H_{n-1}$, on a $D_2(G) \leq D(H_{n-1})$ et par suite, comme $\dfrac{H_{n-1}}{H_{n-2}}$ est abélien, on a $D(H_{n-1}) \leq H_{n-2}$ et donc $D_2(G) \leq H_{n-2}$. Par récurence, on montre de cette manière que pour tout $i = 1, \cdots, n$ on a $D_i(G) \leq H_{n-i}$. En particulier, on a $D_n(G) \leq H_0 = \{e\}$ et donc $D_n(G) = \{e\}$.

$ii) \Rightarrow i)$ Puisque, de manière générale, pour un groupe H le quotient $\dfrac{H}{D(H)}$ est abélien, la suite de composition

$$\{e\} = D_n(G) \triangleleft D_{n-1}(G) \triangleleft \cdots \triangleleft D_0(G) = G$$

est à quotients abéliens. Donc G est résoluble.

□

Remarque : La suite

$$D_0(G) \geq D_1(G) \geq \cdots \geq D_n(G) \geq \cdots$$

est décroissante. Si pour un entier k, on a $D_k(G) = D_{k+1}(G)$, alors pour tout $n \geq k$, on a $D_n(G) = D_k(G)$. Ainsi, s'il existe deux terme consécutif de cette suite identique, alors il exite un entier $k \geq 0$ tel que

$$D_0(G) > D_1(G) > \cdots > D_k(G) = D_{k+1}(G) = \cdots$$

(la suite est strictement décroissante jusqu'au rang k puis stationnaire). Les groupes résolubles satisfont cette propriété, mais il est à noté qu la seule condition d'être stationnaire à partir d'un certain rang pour cette suite ne caractérise pas les groupes résolubles (en effet tous les groupes finis ont cette propriété).

Théorème .— *Tout sous-groupe et tout quotient d'un groupe résoluble est résoluble.*

Preuve : Soit G un groupe résoluble et H un sous-groupe de G. Il existe un entier n tel que $D_n(G) = \{e\}$. Comme $H \leq G$, on a, pour tout entier $k \geq 0$, $D_k(H) \leq D_k(G)$. Ainsi, pour $k = n$, on a $D_n(H) \leq D_n(G) = \{e\}$ et par suite $D_n(H) = \{e\}$ et donc H est résoluble.

Soit $N \triangleleft G$ et $\varphi : G \longrightarrow \dfrac{G}{N}$ la surjection canonique. Comme pour tout $x, y \in G$, on a

$$\overline{x}^{-1}.\overline{y}^{-1}.\overline{x}.\overline{y} = \overline{xyx^{-1}y^{-1}}$$

on en déduit que $D\left(\dfrac{G}{N}\right) = \varphi(D(G))$ et par suite, pour tout entier $k \geq 0$, on a

$$D_k\left(\frac{G}{N}\right) = \varphi(D_k(G))$$

et donc, pour $k = n$, on a

$$D_n\left(\frac{G}{N}\right) = \varphi(D_n(G)) = \varphi(\{e\}) = \{\overline{e}\}$$

et donc $\frac{G}{N}$ est résoluble.

□

Théorème .— *Soit G un groupe et H un sous-groupe normal de G. Si H et $\frac{G}{H}$ sont résolubles alors G l'est aussi.*

Preuve : Considérons deux suites de composition

$$\{e\} = H_0 \leq H_1 \leq \cdots \leq H_r = H \text{ et } \{\overline{e}\} = \frac{G_0}{H} \leq \frac{G_1}{H} \leq \cdots \leq \frac{G_s}{H} = \frac{G}{H}$$

dont les quotients sont abéliens. Comme, pour tout $i = 0, \cdots, s-1$, on a

$$\frac{\frac{G_{i+1}}{H}}{\frac{G_i}{H}} \simeq \frac{G_{i+1}}{G_i}$$

et que ce dernier groupe est, par hypothèse, abélien, on en déduit que la suite de composition

$$\{e\} = H_0 \leq H_1 \leq \cdots \leq H_r = H = G_0 \leq G_1 \leq \cdots \leq G_s = G$$

est à quotients abéliens et donc que G est résoluble.

□

Corollaire.— *a) Pour tout entier $n \geq 5$, S_n n'est pas résoluble.*

b) Tout groupe fini d'ordre p^n (avec p premier) est résoluble.

Preuve : a) On a vu que pour $n \geq 5$, A_n n'était pas résoluble. Comme il est sous-groupe de S_n, ce dernier ne peut être résoluble.

b) Par récurrence sur n : pour $n = 1$, le groupe G est abélien car cyclique, donc il est résoluble.

Si au rang $n-1 \geq 1$ tout groupe d'ordre p^k (avec $1 \leq k \leq n-1$) est résoluble, alors au rang n, si G désigne un groupe d'ordre p^n, on sait que le centre $Z(G)$ de G est un sous-groupe distingué qui n'est pas trivial. On a donc $o(Z(G)) \geq p$ et donc $o(G/Z(G)) \leq p^{n-1}$. L'hypothèse de récurrence assure que $G/Z(G)$ est résoluble et comme $Z(G)$ est abélien, il est résoluble, donc d'après le théorème, G est résoluble.

□

Chapitre 3

Théorie de Sylow

3.1 Groupe opérant sur un ensemble

3.1.1 Généralités

Définition.— *Etant donnés un groupe G de neutre e et un ensemble non vide E, on appelle action à gauche du groupe G sur l'ensemble E toute loi de composition externe à gauche sur E à opérateurs dans G, c'est-à-dire toute application*

$$\begin{array}{ccc} G\times E & \longrightarrow & E \\ (g,x) & \longmapsto & g.x \end{array}$$

satisfaisant aux deux conditions suivantes :

$$\begin{array}{l} 1/\ \forall (g_1,g_2)\in G,\ \forall x\in E,\ (g_1g_2).x = g_1.(g_2.x) \\ 2/\ \forall x\in E,\ e.x = x \end{array}$$

Si E est muni d'une action à gauche de G, on dira que le groupe G opère à gauche sur l'ensemble E et que l'ensemble E est un G-ensemble à gauche.

Remarque : On définit de manière analogue la notion d'action à droite. Dans la suite quand nous ne préciserons pas si l'action est à droite ou à gauche c'est qu'elle sera toujours à gauche.

Proposition.— *Soit G un groupe oéprant sur un ensemble E. Pour tout $g\in G$, l'application*

$$\begin{array}{rccc} \gamma_g: & E & \longrightarrow & E \\ & x & \longmapsto & g.x \end{array}$$

est une bijection (i.e. un élément de $\mathrm{Perm}(E)$). L'application

$$\begin{array}{rccc} \gamma: & G & \longrightarrow & \mathrm{Perm}(E) \\ & g & \longmapsto & \gamma_g \end{array}$$

est un morphisme de groupes (dont le noyau est appelé noyau de l'action de G sur E).

Preuve : L'application γ_g est surjective car pour tout $y\in E$, on a $y=\gamma_g(g^{-1}y)$. De même elle est injective car si $x,y\in E$ sont tels que $\gamma_g(x)=\gamma_g(y)$ alors on a $g.x=g.y$ et par suite $g^{-1}.(g.x)=g^{-1}.(g.y)$, c'est-à-dire $x=y$.

Pour tout $g_1,g_2\in G$ et tout $x\in E$, on a

$$\gamma_{g_1}\circ\gamma_{g_2}(x) = g_1.(g_2.x) = (g_1g_2).x = \gamma_{g_1g_2}(x)$$

ce qui justifie que $\gamma_{g_1}\circ\gamma_{g_2}=\gamma_{g_1g_2}$.

□

Remarques : A toute action de G sur E, on peut donc associer un élément de $\mathrm{Hom}(G,\mathrm{Perm}(E))$. Réciproquement, à tout élément $\lambda\in\mathrm{Hom}(G,\mathrm{Perm}(E))$, on peut associer une action de G sur E par

$$\begin{array}{ccc} G\times E & \longrightarrow & E \\ (g,x) & \longmapsto & \lambda(g)(x) \end{array}$$

(exercice). Il y a donc une correspondance bi-univoque entre les actions du groupe G sur l'ensemble E et les éléments de $\mathrm{Hom}(G, \mathrm{Perm}(E))$, c'est-à-dire que l'on aurait pu prendre pour définition de l'action : être élément de $\mathrm{Hom}(G, \mathrm{Perm}(E))$.

Exemples : a) Tout groupe G opère sur tout ensemble non vide E par :

$$\begin{array}{ccc} G \times E & \longrightarrow & E \\ (g, x) & \longmapsto & x \end{array}$$

Cette action s'appelle l'action triviale.

b) G opère sur lui-même par translation à gauche (exercice)

c) G opère sur lui-même par conjugaison ($(g, x) \mapsto gxg^{-1}$) (exercice)

d) G opère sur $\mathcal{P}(G)$ par translation à gauche et par conjugaison (exercice).

e) Soit un sous-groupe H de G. G opère par translation à gauche sur l'ensemble quotient $\left(\frac{G}{H}\right)_g$ (exercice).

f) $\mathrm{Perm}(E)$ agit de manière naturelle sur E (exercice).

3.1.2 Stabilisateurs et orbites

Définitions

Définition.— *Etant donné un groupe G opérant sur un ensemble E, on appelle stabilisateur (ou sous-groupe d'isotropie) de l'élément $x \in E$ l'ensemble*

$$G_x = \{g \in G / \ g.x = x\}$$

On vérifie facilement (exercice) que G_x est bien un sous-groupe de G. Si l'on considère sur E la relation binaire ρ_G définie par

$$x \rho_G y \Longleftrightarrow \exists g \in G, \ y = g.x$$

on voit (exercice) que ρ_G est une relation d'équivalence sur E.

Définition.— *Etant donné un G-ensemble E et un élément $x \in E$, on appelle orbite de x suivant G (ou G-orbite) de x, la classe d'équivalence de x modulo ρ_G.*

La G-orbite d'un élément $x \in E$ sera notée Ω_x, elle est égale à

$$\Omega_x = \{g.x / \ g \in G\}$$

Exemples : a) Si G opère par translation à gauche sur lui-même alors pour tout $x \in G$, on a $G_x = \{e\}$ et $\Omega_x = G$.

b) Si G opère sur G (resp. sur $\mathcal{P}(G)$) par conjugaison, alors pour tout $x \in G$ (resp. tout $S \in \mathcal{P}(G)$), on a

$$G_x = \{g \in G / \ gxg^{-1} = x\} = C_G(x) \text{ le centralisateur de } x \text{ dans } G$$

$$(resp. \ G_S = \{g \in G / \ gSg^{-1} = S\} = N_G(S) \text{ le normalisateur de } S \text{ dans } G)$$

et

$$\Omega_x = \{gxg^{-1} / \ g \in G\} = \text{ la classe de conjugaison de } x \text{ dans } G$$

$$(resp. \ \Omega_x = \{gSg^{-1} / \ g \in G\} = \text{ la classe de conjugaison de } S \text{ dans } \mathcal{P}(G))$$

En particulier, on voit que, dans ce cas, ρ_G est la relation de conjugaison dans G (resp. dans $\mathcal{P}(G)$).

c) Si H est un sous-groupe de G et si G opère par translation à gauche sur $\left(\frac{G}{H}\right)_g$, pour toute classe à gauche xH on a

$$G_{xH} = xHx^{-1}$$

Proposition.— *Soit G un groupe et H un sous-goupe de G. Le noyau de l'action de translation à gauche de G sur $\left(\frac{G}{H}\right)_g$, est le sous-groupe $\bigcap_{x \in G} xHx^{-1}$ et c'est le plus grand sous-groupe normal de G contenu dans H.*

Preuve : Le noyau de l'action est donc le noyau du morphisme

$$\begin{array}{rccc} \gamma : & G & \longrightarrow & \mathrm{Perm}\Big((G/H)_g\Big) \\ & g & \longmapsto & \gamma_g \end{array}$$

avec $\gamma_g(xH) = gxH$ pour tout $xH \in \left(\frac{G}{H}\right)_g$. Ainsi, on a $g \in \mathrm{Ker}(\gamma)$ ssi pour tout $x \in G$, $gxH = xH$ c'est-à-dire ssi $g \in \bigcap_{x\in G} G_{xH}$. Etant donné que pour cette action on a $G_{xH} = xHx^{-1}$, on trouve bien que $\mathrm{Ker}(\gamma) = \bigcap_{x\in G} xHx^{-1}$.

Notons $\Delta = \bigcap_{x\in G} xHx^{-1}$. Comme Δ est le noyau d'un morphisme, on a $\Delta \triangleleft G$. Il est clair que $\Delta \subset H$ (prendre $x = e$). Soit maintenant un sous-groupe $N \triangleleft G$ contenu dans H. Pour tout $x \in G$, on a $xNx^{-1} \subset xHx^{-1}$, mais comme $N = xNx^{-1}$, on en déduit que $N \subset \bigcap_{x\in G} xHx^{-1} = \Delta$.

□

Propriétés des stabilisateurs et des orbites

Proposition.— *Soit E un G-ensemble. Quels que soient $x, y \in E$, on a*

$$x\rho_G y \Longrightarrow G_x \text{ et } G_y \text{ conjugués dans } \mathcal{P}(G)$$

Preuve : Si $x\rho_G y$ alors il existe $g \in G$ tel que $y = g.x$. Soit $g' \in G_y$, on a $g'.y = y$ et donc $(g'g).x = g.x$ c'est-à-dire $x = (g^{-1}g'g).x$, ce qui implique donc que $g^{-1}g'g \in G_x$ et par suite $g' \in gG_xg^{-1}$. On a donc $G_y \subset gG_xg^{-1}$.

Réciproquement, Soit $g' \in gG_xg^{-1}$, on a $x = (g^{-1}g'g).x$ et par suite $g.x = g'.(g.x)$, c'est-à-dire $y = g'.y$ ce qui implique $g' \in G_y$. On a donc $gG_xg^{-1} \subset G_y$, ce qui, au final, assure que $G_y = gG_xg^{-1}$.

□

Théorème.— *Soit E un G-ensemble, pour tout $x \in E$, on a*

$$\sharp\Omega_x = [G : G_x]$$

Preuve : Il faut et il suffit de montrer qu'il existe une bijection entre les ensembles Ω_x et $\left(\frac{G}{G_x}\right)_g$. A cet effet, considérons l'application

$$\begin{array}{rccc} \psi : & \Omega_x & \longrightarrow & \left(\frac{G}{G_x}\right)_g \\ & g.x & \longmapsto & gG_x \end{array}$$

(qui est bien définie car si $g.x = g'.x$ alors $g^{-1}g' \in G_x$ et par suite $gG_x = g'G_x$). L'application ψ est, par définition, surjective. Elle est aussi injective car

$$g_1G_x = g_2G_x \Longrightarrow g_1^{-1}g_2 \in G_x \Longrightarrow (g_1^{-1}g_2).x = x \Longrightarrow g_1.x = g_2.x$$

ce qui assure qu'elle est, pour finir, bijective.

□

Corollaire.— *Soit G un groupe considéré comme opérant sur $\mathcal{P}(G)$ par conjugaison. Pour tout $S \in \mathcal{P}(G)$, on a*

$$\sharp\Omega_S = [G : N_G(S)]$$

Preuve : Immédiat.

□

Corollaire.— *Soit E un G-ensemble fini et $\{x_i\}_{1\leq i\leq n}$ une classe de réprésentants des G-orbites. On a*

$$\sharp E = \sum_{i=1}^{n} [G : G_{x_i}]$$

Preuve : Immédiat, compte tenu du fait que la famille $\{\Omega_i\}_{1\leq i\leq n}$ forme une partition de E.

□

Corollaire.— (Equation des classes) *Soit G un groupe fini opérant sur lui-même par conjugaison. Si $\{x_i\}_{1\leq i\leq n}$ désigne une classe de réprésentants des classes de conjugaison dans G, alors on a*

$$o(G) = \sum_{i=1}^{n} [G : C_G(x_i)]$$

où $C_G(x_i)$ désigne le centralisateur de x_i dans G.

Preuve : Immédiat.

□

Définition.— *Soit E un G-ensemble, une G-orbite est dite ponctuelle si elle est réduite à un seul élément.*

Exemple : Si l'on considère un groupe G (de centre $Z(G)$) opérant sur lui-même par conjugaison, on voit que (exercice)

$$x \in Z(G) \Longleftrightarrow \Omega_x = \{x\} \Longleftrightarrow C_G(x) = G$$

Théorème.— *Soit G un groupe fini de centre $Z(G)$. Si $\{x_i\}_{1\leq i\leq n}$ désigne une classe de réprésentants des classes de conjugaison non ponctuelle dans G, alors on a*

$$o(G) = o(Z(G)) + \sum_{i=1}^{n} [G : C_G(x_i)]$$

Preuve : On a remarqué, dans l'exemple précédent, que les classes de conjugaison ponctuelles correspondent bi-univoquement aux éléments de $Z(G)$ et que pour $x \in Z(G)$, on a $C_G(x) = G$. Fort de cette remarque, on applique le corollaire précédent.

□

Théorème.— *Soit G un groupe fini d'ordre p^n avec p premier et $n \geq 1$ entier. Le centre $Z(G)$ de G n'est pas trivial.*

Preuve : Si G est abélien le résultat est clair. Si G n'est pas abélien, en appliquant le théorème précédent, on trouve que

$$o(Z(G)) = p^n - \sum_{i=1}^{n} [G : C_G(x_i)]$$

où les x_i sont des représentants des classes de conjugaison non ponctuelle de G. On a donc pour tout $i = 1, \cdots, n$, $[G : C_G(x_i)] > 1$, mais comme chaque indice $[G : C_G(x_i)]$ divise $o(G) = p^n$, on en déduit que p divise chaque $[G : C_G(x_i)]$, donc $\sum_{i=1}^{n} [G : C_G(x_i)]$ et par suite $o(Z(G))$. Ainsi $Z(G)$ ne peut être trivial (son ordre est au moins p).

□

Corollaire.— *Tout groupe d'ordre p^2 avec p premier est abélien.*

Preuve : Supposons que $Z(G) \neq G$, on a alors, en vertu du théorème précédent, $1 < o(Z(G)) < p^2$, mais comme $o(Z(G))|p^2$ on a donc $o(Z(G)) = p$ et par suite $o\left(\dfrac{G}{Z(G)}\right) = p$, ce qui implique que $\dfrac{G}{Z(G)}$ est cyclique et par suite que G est abélien, ce qui est absurde.

□

Définition.— *Soit E un G-ensemble. On dit que l'action de G sur E est transitive, si*

$$\forall x, y \in E,\ \exists g \in G,\ g.x = y$$

On dit alors que E est un G-ensemble homogène ou que G est transitif sur E.

On dit que l'action est fidèle sur E, si pour tout $g \in G$, on a

$$\forall x \in E,\ g.x = x \Longrightarrow g = e$$

Remarques : a) On voit qu'un groupe G opère transitivement sur un ensemble E ssi E n'a qu'une seule G-orbite ssi pour tout $x \in E$, $\Omega_x = E$.

b) Pour un groupe G, la propriété d'opérer fidèlement sur un ensemble E est équivalente à dire que le morphisme $G \longrightarrow \mathrm{Perm}(E)$ associé canoniquement à l'action est un monomorphisme. En particulier, quand G opère fidèlement sur E, G est isomorphe à un sous-groupe de $\mathrm{Perm}(E)$.

Exemples.— (Exercice) a) G opère transitivement et fidèlement sur lui-même par translation à gauche.

b) Si G n'est pas trivial alors G n'opère pas transitivement sur lui-même par conjugaison. Par ailleurs, on voit que l'action de conjugaison sur un groupe G est fidèle ssi $Z(G) = \{e\}$.

c) Si E désigne un G-ensemble alors G opère transitivement sur toute les G-orbites de E.

Proposition.— *Soit G un groupe et H un sous-groupe de G. L'action de G sur $\left(\frac{G}{H}\right)_g$ par translation à gauche est transitive.*

Réciproquement, si E désigne un G-ensemble homogène, alors il existe un sous-groupe H de G tel que E soit équipotent à $\left(\frac{G}{H}\right)_g$.

Preuve : On a $\left(\frac{G}{H}\right)_g = \{gH/\ g \in G\}$. L'action d'un élément $g \in G$ sur H est $H^g = gH$, donc l'orbite de H sous l'action de G est

$$\Omega_H = \{gH/\ g \in G\} = \left(\frac{G}{H}\right)_g$$

il n'y a donc qu'une seule orbite pour cette action ce qui assure que l'action est transitive.

Soit E un G-ensemble homogène. On a donc pour tout $x \in E$, $\Omega_x = E$, mais on a vu que Ω_x était équipotent à $\left(\frac{G}{G_x}\right)_g$.

□

3.1.3 Points fixes

Définition.— *Etant donné un G-ensemble E, on appelle point fixe de E tout élément $x \in E$ tel que*

$$\forall g \in G,\ g.x = x$$

L'ensemble des points fixes de E sera noté E_G.

On voit qu'un élément $x \in E$ est un point fixe si et seulement si sa G-orbite est ponctuelle. On a donc

$$E_G = \{x \in E/\ \Omega_x = \{x\}\} = \{x \in E/\ G_x = G\}$$

Exemples : a) Si G opère transitivement sur E, alors $E_G = \emptyset$.

b) Si G opère sur lui-même par conjugaison alors $G_G = Z(G)$ (exercice).

Voici maintenant deux lemmes trés importants qui nous servirons dans la partie suivante pour la démonstration des théorèmes de Sylow.

Lemme.— *Soit G un groupe d'ordre p^n avec p premier et $n \geq 1$ entier. Si G opère sur un ensemble fini E, alors*

$$\sharp E_G \equiv \sharp E\ mod(p)$$

Preuve : On a $x \in E_G$ ssi $\Omega_x = \{x\}$, ainsi, si $\{\Omega_{x_i}\}_{1 \leq i \leq k}$ désigne les orbites non ponctuelles de E, alors on a

$$\sharp E = \sharp E_G + \sum_{i=1}^{k} \sharp \Omega_{x_i}$$

Pour tout $i = 1, \cdots, k$, on a $\sharp \Omega_{x_i} = [G : G_{x_i}]$ et $\sharp \Omega_{x_i} > 1$. Il s'ensuit que p divise $\sharp \Omega_{x_i}$ et par suite $\sharp E - \sharp E_G$.

□

Lemme.— *Soient H et K deux sous-groupes d'un groupe G. On suppose que $[G:H]=r$ et que $o(K)=p^n$ où p est un nombre premier ne divisant pas r et $n\geq 1$ est un entier. Le sous-groupe K est contenu dans un conjugué du sous-groupe H.*

Preuve : Le groupe K opère par translation à gauche sur l'ensemble $\left(\frac{G}{H}\right)_g$. Notons E l'ensemble des points fixes. D'après le lemme précédent, on a

$$\sharp E \equiv r(p)$$

mais comme p ne divise pas r, on en déduit que $E\neq\emptyset$. Soit donc xH un élément de E. Si G_{xH} désigne le stabilisateur de xH sous l'action de G tout entier sur $\left(\frac{G}{H}\right)_g$ on a alors visiblement $K\leq G_{xH}$ mais comme $G_{xH}=xHx^{-1}$, on en déduit que K est bien contenu dans un conjugué de H.

□

3.1.4 Produit semi-direct

Produit semi-direct de deux groupes

Soient H et N deux groupes $\varphi\in\mathrm{Hom}(H,\mathrm{Perm}(N))$ une action du groupe H sur le groupe N. Pour $h\in H$ et $x\in N$, on notera plus volontier x^h à la place de $\varphi(h)(x)$ l'action de l'élément h sur l'élement x. On voit donc qu'avec ces notations, on a

$$(1)\quad \forall h_1,h_2\in H,\ \forall x\in N,\ (x)^{h_1h_2}=(x^{h_2})^{h_1}$$
$$(2)\quad \forall x\in N,\ x^e=x$$

On s'intéresse aux actions qui respectent la structure de groupe de N c'est-à-dire qui vérifie

$$(3)\ \forall h\in H,\ \forall x,y\in N,\ (xy)^h=x^hy^h$$

Lemme.— *Avec les notations précédentes, une action $\varphi\in\mathrm{Hom}(H,\mathrm{Perm}(N))$ vérifie la condition* (3) *si et seulement si* $\mathrm{Im}(\varphi)\in\mathrm{Aut}(N)$*, c'est-à-dire si et seulement si pour tout $h\in H$, $\varphi(h)$ est un automorphisme du groupe N.*

Preuve : Exercice.

□

Par exemple, si G opère sur lui-même par conjugaison alors l'action vérifie la condition (3). Par contre s'il opère par translation à gauche, ce n'est pas le cas.

Etant donné deux groupes H et N et une action $\varphi\in\mathrm{Hom}(H,\mathrm{Perm}(N))$, on considère sur l'ensemble $H\times N$ la loi de composition suivante : pour tout $(h,x),(k,y)\in H\times N$,

$$(h,x)(k,y)=(hk,xy^h)$$

Lemme-Définition.— *Avec les notation précédente, si* $\mathrm{Im}(\varphi)\in\mathrm{Aut}(N)$ *(i.e. l'action vérifie la condition* (3)*) alors l'ensemble $H\times N$ muni de cette loi est un groupe. On le note $H\times_\varphi N$ (ou parfois $H\ltimes N$ si l'action φ est sous-entendue) et on l'appelle le produit semi-direct du groupe N par le groupe H relativement à l'action φ.*

Preuve : • Neutre. Pout tout $(h,x)\in H\times_\varphi N$, on a $(h,k)(e_H,e_N)=(he_H,ke_N^h)$ mais comme l'action vérifie (3), on a $e_N^h=(e_Ne_N)^h=e_N^he_N^h$ et donc $e_N^h=e_N$. Par suite, on a $(h,k)(e_H,e_N)=(h,k)$. Inversement, on a $(e_H,e_N)(h,k)=(e_Hh,e_Nk^{e_H})=(e_H,e_N)$. Ainsi le couple (e_H,e_N) est un neutre bilatère.

• Existence d'un inverse. Soit $(h,x)\in H\times_\varphi N$. Puisque, pour h fixé, l'application $t\mapsto t^h$ est un automorphisme de N, il existe $y\in N$ tel que $y^h=x^{-1}$. On a alors

$$(h,x)(h^{-1},y)=(hh^{-1},xy^h)=(hh^{-1},xx^{-1})=(e_H,e_N)$$

Par ailleurs puisque $y^h=x^{-1}$ on faisant agir h^{-1} on trouve $y=(x^{-1})^{h^{-1}}$, mais comme $t\mapsto t^{h^{-1}}$ est un automorphisme du groupe N, on trouve que $y^{-1}=x^{h^{-1}}$. Ainsi on a

$$(h^{-1},y)(h,x)=(h^{-1}h,yx^{h^{-1}})=(h^{-1}h,yy^{-1})=(e_H,e_N)$$

et donc $(h,x)^{-1}=(h^{-1},y)$. On remarque, au passage, que l'on a montré que $y=(x^{-1})^{h^{-1}}$.

• Associativité. Soit $(h,x),(k,y),(l,z) \in H \times_\varphi N$. On a

$$\begin{array}{rcl}[(h,x)(k,y)](l,z) & = & (hk, xy^h)(l,z) = (hkl, xy^h z^{hk}) \\ & = & (hkl, x(yz^k)^h) = (h,x)(kl, yz^k) \\ & = & (h,x)[(k,y)(l,z)]\end{array}$$

La loi de composition est donc associative.

□

Exemple : Si φ est l'action triviale on voit immédiatement que $H \times_\varphi N = H \times N$.

Théorème.— *Soit $G = H \times_\varphi N$. Les applications*

$$\alpha : \begin{array}{ccc} H & \longrightarrow & G \\ h & \longmapsto & (e_G, h) \end{array} \quad et \quad \beta : \begin{array}{ccc} N & \longrightarrow & G \\ x & \longmapsto & (x, e_H) \end{array}$$

sont des monomorphismes de groupes et si l'on identifie H à $\alpha(H)$ et N à $\alpha(N)$ dans G, on a alors

a) $\forall h \in H$, $\forall x \in N$, $x^h = hxh^{-1}$,

b) $N \triangleleft G$,

c) $G = HN = NH$,

d) $H \cap N = \{e\}$.

Réciproquement, si G désigne un groupe contenant deux sous-groupes H et N vérifiants les conditions b),c),d) précédente alors G est isomorphe au produit semi direct $H \times_\varphi N$ où φ est l'action de conjugaison de H sur N. (On dit alors que G est le produit semi-direct de N par H.)

Preuve : Le fait que α et β soient des monomorphismes est laissé en exercice.

a) Soit $h \in H$ et $x \in N$, on a

$$hxh^{-1} = (h, e_G)(e_H, x)(h^{-1}, e_G) = (h, x^h)(h^{-1}, e_G) = (e_H, x^h) = x^h$$

b) Soit $(h,x) \in G$, on a $(h,x)^{-1} = (h^{-1}, (x^{-1})^{h^{-1}})$ et donc pour tout $(e_H, y) \in N$, on a

$$(h,x)(e_H,y)(h,x)^{-1}) = (h, xy^h)(h^{-1}, (x^{-1})^{h^{-1}}) = (e_H, xy^h x^{-1}) \in N$$

et donc $N \triangleleft G$.

c) Soit $(h,x) \in G$, on a $(h,x) = (h,e_G)(e_H, x^{h^{-1}}) \in HN = NH$ (puisque $N \triangleleft G$.

d) Evident.

Réciproquement, si un groupe G possède deux sous-groupes vérifiant les conditions b),c),d), alors le groupe H agit sur le groupe N par conjugaison. Pour cette action, considérons le produit semi-direct $H \ltimes N$ et l'application

$$\psi : \begin{array}{ccc} H \ltimes N & \longrightarrow & G \\ (h,x) & \longmapsto & xh \end{array}$$

C'est un morphisme de groupe. En effet, on a

$$\psi((h,x)(g,y)) = \psi((hg, xhyh^{-1}) = xhyh^{-1}hg = xhyg = \psi((h,x))\psi((g,y))$$

Par ailleurs, il est surjectif d'après c). Il est aussi injectif, car si $(h,x) \in \mathrm{Ker}(\psi)$, alors on a $xh = e$ et donc $x = h^{-1} \in H \cap N = \{e\}$ (d'après la condition d)). Ainsi $x = h = e$ et $(h,x) = (e,e)$, ψ est bien injectif.

□

Exemple : L'exemple typique est le groupe diédral D_n. En effet, si l'on note N le sous-groupe de D_n constitué des rotations (isomorphe à $\mathbb{Z}/n\mathbb{Z}$) et H le sous-groupe engendré par la symétrie s (isomorphe à $\mathbb{Z}/2\mathbb{Z}$), alors on a vu que $H \cap N = \{e\}$, $N \triangleleft D_n$ et $G = HN$. C'est-à-dire que D_n est isomorphe au produit semi-direct $\mathbb{Z}/2 \ltimes \mathbb{Z}/n$ où l'action de l'élement non trivial de $\mathbb{Z}/2$ sur $\mathbb{Z}/n$ est le passage à l'inverse (exercice).

Proposition.— *Soit $G = H \ltimes N$ un produit semi-direct de groupes. Si on identifie N à son image canonique dans G alors N est distingué et $\dfrac{H \ltimes N}{N} \simeq H$.*

Preuve : On a vu précédement que $N \triangleleft G$, $NH = G$ et que $N \cap H = \{e_G\}$, le deuxième théorème d'isomorphisme assure alors que

$$\frac{G}{N} = \frac{HN}{N} \simeq \frac{H}{H \cap N} = H$$

□

Suite exacte scindée

On rappelle qu'étant donné trois groupes N, G, H, et des morphismes $\alpha : N \longrightarrow G$ et $f : G \longrightarrow H$, dire que la suite de groupes

$$1 \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{f} H \longrightarrow 1$$

est exacte, revient à dire que α est injectif, f surjectif et $\mathrm{Ker}(f) = \mathrm{Im}(\alpha)$. Dans ces condition, si l'on identifie N à $\mathrm{Im}(\alpha)$, alors on a $H \simeq G/N$.

Définition.— *Une suite exacte de groupes*

$$1 \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{f} H \longrightarrow 1$$

est dite scindée s'il existe un morphisme $s : H \longrightarrow G$ tel que $f \circ s = Id$. On dit alors que s est une section.

Théorème.— *Si une suite exacte de groupes*

$$1 \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{f} H \longrightarrow 1$$

est scindée par une section $s : H \longrightarrow G$ alors G est isomorphe au produit semi-direct $H \times_\varphi N$ où φ est l'action de H sur N donnée par

$$\forall h \in H,\ \forall x \in N,\ x^h = \alpha^{-1}(s(h)\alpha(x)s(h^{-1}))$$

Réciproquement, si un groupe G est isomorphe à un produit semi-direct $H \times_\varphi N$, alors il existe une suite exacte de groupes

$$1 \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{f} H \longrightarrow 1$$

qui est scindée.

Preuve : Notons $N_0 = \alpha(N)$ et $H_0 = s(H)$. Le groupe N_0 est distingué dans G, puisque c'est le noyau de f. Si $x \in N_0 \cap H_0$ alors on a $f(x) = e_H$ car $N_0 = \mathrm{Ker}(f)$, mais comme $x = s(h)$ pour un certain $h \in H$, on a $e_H = f(s(h)) = h$ et donc $x = s(e_H) = e_G$ puisque s est un morphisme. On a donc $H_0 \cap N_0 = \{e_G\}$. Enfin, soit $x \in G$ et $x' = s(f(x))$, puisque $f(x') = f(x)$, il existe $h \in \mathrm{Ker}(f) = N_0$ tel que $x = x'h$ et donc $x \in H_0 N_0$.

Ainsi, le groupe G est le produit semi-direct des sous-groupes H_0 et N_0, il est donc isomorphe à $H_0 \ltimes N_0$ où l'action d'un élément $h_0 \in H_0$ sur un élément $x_0 \in N_0$ est $x_0^{h_0} = h_0 x_0 h_0^{-1}$. Les isomorphismes $\alpha : N \longrightarrow N_0$ et $s : H \longrightarrow H_0$ permettent alors de définir une action de H sur N définie, pour $h \in H$ et $x \in N$, par

$$x^h = \alpha^{-1}((\alpha(x))^{s(h)}) = \alpha^{-1}(s(h)\alpha(x)s(h^{-1}))$$

et l'on constate alors que, pour ces actions, les groupes $H_0 \ltimes N_0$ et $H \ltimes N$ sont isomorphes.

La réciproque est laissée en exercice.

□

Exemple : Pour tout entier $n \geq 1$, on a donc une suite exacte scindée

$$1 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow D_n \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

3.2 Théorèmes de Sylow et applications

3.2.1 Les théorèmes de Sylow

Lemme.— *Soit p un nombre premier, s un entier premier à p, n un entier non nul et $r \in \{1, \cdots, n\}$. Il existe un entier λ premier à p tel que*

$$C_{sp^n}^{p^r} = \lambda p^{n-r}$$

Preuve : On a

$$C_{sp^n}^{p^r} = \frac{(sp^n)!}{p^r!(sp^n-p^r)!} = \frac{sp^n(sp^n-1)\cdots(sp^n-p^r+1)}{1.2.\cdots.p^r}$$

Dans le produit $sp^n(sp^n-1)\cdots(sp^n-p^r+1)$ seuls les facteurs de la forme sp^n-ph sont divisible par p, si bien que, il existe un entier λ_0, premier à p, tel que

$$\begin{aligned} sp^n(sp^n-1)\cdots(sp^n-p^r+1) &= \lambda_0.sp^n.(sp^n-p).(sp^n-2p).\cdots(sp^n-(p-1)p^{r-1}) \\ &= \lambda_0.sp^n.\prod_{k=1}^{r-1}\prod_{i=1}^{p-1}(sp^n-ip^k) \end{aligned}$$

Pour $k=1,\cdots,r-1$ et $i=1,\cdots,p-1$ fixés, on remarque que $(sp^n-ip^k)=p^k(sp^{n-k}-i)$ avec $sp^{n-k}-i$ premier à p. Donc, pour tout $k=1,\cdots,r-1$, il existe un entier λ_k, premier avec p, tel que

$$\prod_{i=1}^{p-1}(sp^n-ip^k) = \lambda_k p^{k(p-1)}$$

et, par suite, on a

$$sp^n(sp^n-1)\cdots(sp^n-p^r+1) = \lambda_0.\lambda_1.\cdots.\lambda_{r-1}p^{n+(p-1)+2(p-1)+\cdots+(r-1)(p-1)}$$

De même, dans le produit $1.2.\cdots.p^r$ seuls les termes de la forme hp ne sont pas premiers avec p. Il existe donc un entier μ_0, premier avec p, tel que

$$\begin{aligned} 1.2.\cdots.p^r &= \mu_0.p.(2p).\cdots.p^{r-1}p \\ &= \mu_0.\left(\prod_{k=1}^{r-1}\prod_{i=1}^{p-1} ip^k\right)p^r \end{aligned}$$

Pour tout $k=1,\cdots,r-1$, il existe un entier μ_k, premier avec p tel que

$$\prod_{i=1}^{p-1} ip^k = \mu_k.p^{k(p-1)}$$

(en fait $\mu_k = 1.2.\cdots.(p-1) = (p-1)!$). On en déduit que

$$1.2.\cdots.p^r = \mu_0.\mu_1.\cdots.\mu_{r-1}.p^{r+(p-1)+2(p-1)+\cdots+(r-1)(p-1)}$$

Ainsi, on peut écrire :

$$C_{sp^n}^{p^r} = \frac{sp^n(sp^n-1)\cdots(sp^n-p^r+1)}{1.2.\cdots.p^r} = \frac{\lambda_0.\lambda_1.\cdots.\lambda_{r-1}}{\mu_0.\mu_1.\cdots.\mu_{r-1}}p^{n-r}$$

mais comme $C_{sp^n}^{p^r}$ est entier et que les entiers $\lambda_0,\cdots,\lambda_{r-1},\mu_0,\cdots,\mu_{r-1}$ sont tous premiers avec p, on en déduit que $\lambda = \frac{\lambda_0.\lambda_1.\cdots.\lambda_{r-1}}{\mu_0.\mu_1.\cdots.\mu_{r-1}}$ est un entier premier avec p.

□

Théorème.— (Premier théorème de Sylow) *Soit G un groupe fini et p un nombre premier. Si $o(G) = sp^n$ avec n et s entiers, alors pour tout entier $k=0,\cdots,n$, il existe un sous-groupe de G d'ordre p^k.*

Preuve : Si $k=0$ c'est clair, on suppose donc $k\geq 1$. Par ailleurs, on peut supposer, dans cette preuve que s est premier à p.

Notons $\mathcal{F}$ l'ensemble des parties de G de cardinal p^k. On a, d'après le lemme précédent,

$$\sharp\mathcal{F} = C_{sp^n}^{p^k} = \lambda p^{n-k}$$

avec λ premier à p. Puisque pour tout $A\in\mathcal{F}$, on a $\sharp gA = \sharp A$, on voit que G opère sur $\mathcal{F}$ par translation à gauche. Il s'ensuit que

$$\sharp\mathcal{F} = \sum_{i=1}^{m}[G:G_{A_i}] = \lambda p^{n-k}$$

où pour tout $\{A_i\}_{1\leq i\leq m}$ désigne une famille de représentants des G-orbites distinctes de $\mathcal{F}$ et où G_{A_i} désigne le stabilisateur de A_i dans G. Il s'en suit qu'il existe au moins un $h\in\{1,\cdots,m\}$ tel que p^{n-k+1} ne divise pas $[G:G_{A_h}]$. Notons $H=G_{A_h}$. Comme $o(G)=sp^n$, que $o(G)=o(H)[G:H]$ et que p^{n-k+1} ne divise pas $[G:H]$, on en déduit qu'il existe un entier $s^{'}$ divisant s et un entier $\alpha\in\{0,\cdots,n-k\}$ tels que

$$[G:H]=s^{'}p^{\alpha}$$

En posant $s=s^{'}s^{''}$, on trouve que $o(H)=s^{''}p^{n-\alpha}$ mais comme $k\leq n-\alpha\leq n$, on voit que p^k divise $o(H)$ et donc que $p^k\leq o(H)$.

Par définition de G_{A_h}, pour tout $g,g^{'}\in G_{A_h}$, on a $gA_h=g^{'}A_h=A_h$ et si $g\neq g^{'}$, alors pour tout $x\in A_h$, on a $gx\neq g^{'}x$. Cela implique, en particulier, que $\sharp H=\sharp G_{A_h}\leq\sharp A_h=p^k$. On a donc $o(H)\leq p^k$ et, par suite, $o(H)=p^k$.

□

Définition.— *Un groupe fini est appelé p-groupe (avec p premier), si son ordre est une puissance de p.*

Soit G un groupe fini d'ordre divisible par un premier p (disons $o(G)=sp^n$ avec s premier à p et $n\geq 1$). On appelle p-sous-groupe de G (resp. p-sous-groupe de Sylow) tout sous-groupe de G d'ordre p^k avec $k=1,\cdots,n$ (resp. d'ordre p^n).

Lemme.— *Soit G un groupe fini. Si S est un p-sous-groupe de Sylow de G, alors S est l'unique p-sous-groupe de Sylow de $N_G(S)$.*

Preuve : Posons $o(G)=p^ns$ avec s premier à p. On remarque que S est un p-sous-groupe de Sylow de tout sous-groupe de G le contenant, en particulier de $N_G(S)$.

On a $o(N_G(S))=p^ns^{'}$ avec $s^{'}$ premier à p et si K est un p-sous-groupe de Sylow de $N_G(S)$ alors $o(K)=p^ns^{'}$. On sait, par la partie précédente, que K est contenu dans un conjugué de S, donc il existe $x\in N_G(S)$ tel que $K\leq xSx^{-1}$, mais comme $xSx^{-1}=S$ et que $o(S)=o(K)$, on en déduit que $K=S$.

□

Théorème.— (Deuxième théorème de Sylow) *Soit G un groupe fini et p un premier divisant $o(G)$.*

- *Tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow de G.*
- *Les p-sous-groupes de Sylow de G sont conjugués.*
- *Le nombre de p-sous-groupes de Sylow de G est un entier qui divise $o(G)$ et qui est congru à 1 modulo p.*

Preuve : Posons $o(G)=p^ns$ avec s premier à p.

• Soit H un p-sous-groupe de G et S un p-sous-groupe de sylow de G. D'après la partie précédente, il existe $x\in G$ tel que $H\leq xSx^{-1}$, mais comme $o(xSx^{-1})=o(S)=p^n$, on en déduit que xSx^{-1} est aussi un p-sous-groupe de Sylow de G.

• Soient $S,S^{'}$ deux p-sous-groupes de Sylow. Le raisonnement au dessus, montre que $S^{'}\leq xSx^{-1}$ pour un certain $x\in G$. Mais le calcul des ordres de $S^{'}$ et xSx^{-1} montre que $xSx^{-1}=S^{'}$.

• Soit $\mathcal{S}$ l'ensemble des p-sous-groupes de Sylow de G. D'après le résultat précédent, G opère transitivement par conjugaison sur $\mathcal{S}$. Il n'y a donc qu'une seule classe de conjugaison et si $S\in\mathcal{S}$ alors on a

$$\sharp\mathcal{S}=\sharp\Omega_S=[G:N_G(S)]$$

et donc $\sharp\mathcal{S}$ divise $o(G)$. Plus précisément, $\sharp\mathcal{S}$ divise s puisque $s=[G:S]=[G:N_G(S)][N_G(S):S]$. Par ailleurs, S opère sur $\mathcal{S}$ par conjugaison, et donc si $\mathcal{S}_S$ désigne l'ensemble des points fixes du S-ensemble $\mathcal{S}$, alors on a

$$\sharp\mathcal{S}\equiv\sharp\mathcal{S}_S(p)$$

Or, on a

$$S^{'}\in\mathcal{S}_S\Longleftrightarrow\forall y\in S,\ S^{'}=ySy^{-1}\Longleftrightarrow S\leq N_G(S^{'})$$

D'après le lemme précédent, $N_G(S^{'})$ ne contient qu'un seul p-sous-groupe de Sylow : $S^{'}$. On en déduit donc que $\sharp\mathcal{S}_S=1$ et donc que $\sharp\mathcal{S}\equiv 1(p)$.

□

En résumé, si $o(G)=p^ns$ avec s premier à p, on retiendra que le nombre n_p de p-sous-groupes de Sylow de G divise s et vérifie $n_p\equiv 1(p)$.

Corollaire.— *Un groupe fini G a un unique p-sous-groupe de Sylow si et seulement si ce dernier est distingué dans G. En particulier, si G est abélien il n'existe qu'un seul p-sous-groupe de Sylow de G.*

Preuve : Immédiat.

□

3.2.2 Applications aux groupes finis

Théorème.— *Soit G un groupe d'ordre pq où p et q sont deux nombres premiers distincts tels que $q \not\equiv 1(p)$, alors G a un unique p-sous-groupe de Sylow.*

Preuve : Soit n_p le nombre de p-sous-groupes de Sylow de G. On sait que n_p divise q, donc, puisque q est premier, que $n_p = 1$ ou q. Par ailleurs, on a $n_p \equiv 1(p)$ et comme $q \not\equiv 1(p)$, on en déduit que $n_p \neq q$ et, par suite, $n_p = 1$.

□

Corollaire.— *Un groupe fini d'ordre pq, avec p et q deux nombres premiers distincts, n'est pas simple.*

Preuve : On peut supposer que $p > q$ et donc p ne divise pas $q-1$, ce qui implique, d'après le théorème précédent, que G possède un unique p-sous-groupe de Sylow. Ce dernier est normal et est non trivial. Donc G n'est pas simple.

□

Corollaire.— *Soient p et q deux nombres premiers distincts tels que $q \not\equiv 1(p)$, et $p \not\equiv 1(q)$. Tout groupe d'ordre pq est cyclique.*

Preuve : D'après le théorème précédent, G à un unique p-sous-groupe de Sylow (donc normal et cyclique car d'ordre p) $H_p =< x >$ et un unique q-sous-groupe de Sylow (donc normal et cyclique car d'ordre q) $H_q =< y >$.

Pour des raisons évidentes d'ordre, on a $H_p \cap H_q = \{e\}$ et comme H_pH_q est un sous-groupe de G contenant H_p qui est d'ordre p, son ordre est $> p$ et comme q est premier, on a $o(H_pHq) = pq$. Donc $G = H_pH_q$.

Puisque le commutateur $[x,y] = x^{-1}y^{-1}xy$ peut respectivement s'écrire

$$[x,y] = (x^{-1}y^{-1}x)y = x^{-1}(y^{-1}xy)$$

il est donc élément de H_q et de H_p puisque ces deux sous-groupes sont normaux. Ainsi $[x,y] = e$ et par suite, $xy = yx$. On en déduit que quelque que soit $a \in H_p$ et $b \in H_q$, on a $ab = ba$.

On en conclue que

$$G \simeq H_p \times H_q \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$$

et donc que G est cyclique.

□

Théorème.— *Soit p un nombre premier impair. Si G est un groupe d'ordre $2p$, alors G est soit cyclique soit isomorphe au group diédral D_p.*

Preuve : Comme p est premier, on a $2 \not\equiv 1(p)$ et donc G a un unique p-sous-groupe de Sylow S (qui étant de cardinal p est isomorphe à $\mathbb{Z}/p$). Soit n_2 le nombre de 2-sous-groupes de Sylow de G. On sait que $n_2 \equiv 1(2)$ et que $n_2|p$, on a donc $n_2 = 1$ ou p.

• Si $n_2 = 1$, notons H l'unique 2-sous-groupe de Sylow de G. Il est clair que $S \cap H = \{e\}$ (sinon $S \cap H = H \subset S$). Les sous-groupes S et H sont distingués dans G (puisque ce sont, respectivement, les uniques p-sous-groupe et 2-sous-groupe de Sylow de G) ainsi SH est un sous-groupe de G et, pour des raisons évidentes d'ordre, on a $o(SH) = 2p$ c'est-à-dire $G = SH$. Enfin, si $s \in S$ et $h \in H$, on a $shs^{-1} = h$, car si $h \neq e$, alors $shs^{-1} \in H$ et $shs^{-1} \neq e$. On en déduit que $sh = hs$ et donc que $G \simeq H \times S \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/2p\mathbb{Z}$.

• Si $n_2 = p$, soit a un générateur de S et $b \in G - S$. On a $o(b) = 2$, en effet l'ordre de b est soit 2, soit p, soit $2p$. S'il était d'ordre $2p$, G serait cyclique et ne possèderait donc qu'un seul 2-sous-groupe de Sylow, ce qui est contraire à l'hypothèse. Si b était d'ordre p alors G possèderait au moins deux p-sous-groupes de Sylow ce qui est absurde. L'élément ab n'est pas dans S (car a y étant, on aurait alors $b \in S$), il est donc lui aussi d'ordre 2. On en déduit que le sous-groupe $< a,b >$ est isomorphe au groupe diédral D_p, mais comme ce dernier est d'ordre $2p$, on déduit finalement que $G =< a,b > \simeq D_p$.

□

Théorème.— *Soit G un groupe fini d'ordre $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Si pour tout $i = 1, \cdots, k$ le groupe G possède un unique p_i-sous-groupe de Sylow P_i, alors*

$$G = P_1 \cdots P_k \simeq P_1 \times \cdots \times P_k$$

Preuve : Puisque les P_i sont uniques, ils sont distingués et, par suite, $P_1 \cdots P_k$ est un sous-groupe de G. Pour des raisons évidentes d'ordre, on voit que $G = P_1 \cdots P_k$.

Si $i \in \{1, \cdots, k\}$, on a

$$o(P_1 \cdots P_{i-1} P_{i+1} \cdots P_k) = p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_k^{\alpha_k}$$

et, pour des raisons d'ordre, on en déduit que $P_1 \cdots P_{i-1} P_{i+1} \cdots P_k \cap P_i = \{e\}$.

Soient $i \neq j$ et $x_i \in P_i$ et $x_j \in P_j$. Puisque $P_i, P_j \triangleleft G$, on a $[x_i, x_j] \in P_i \cap P_j = \{e\}$ et donc $x_i x_j = x_j x_i$. Tout ceci permet alors d'affirmer que $P_1 \cdots P_k \simeq P_1 \times \cdots \times P_k$.

□

Corollaire.— *Soit G un groupe abélien d'ordre $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Le groupe G est la somme directe de ses uniques p_i-sous-groupes de Sylow.*

Preuve : Immédiat.

□

Corollaire.— *Soit p et q deux nombres premiers distincts tels que $p^2 \not\equiv 1(q)$ et $q \not\equiv 1(p)$. Tout groupe d'ordre $p^2 q$ est abélien.*

Preuve : Soit H_p (resp. H_q) un p-sous-groupe de Sylow (resp. un q-sous-groupe de Sylow) de G. Notons n_p et n_q le nombre respectif de p et q-sous-groupes de Sylow de G. On sait que n_p divise q, donc $n_p = 1$ ou q, mais comme $n_p \equiv 1(p)$ et $q \not\equiv 1(p)$, on en déduit que $n_p = 1$ et par suite que H_p est l'unique p-sous-groupe de G (et donc normal dans G). De même, on sait que n_q divise p^2, donc $n_p = 1, p$ ou p^2, mais comme $n_q \equiv 1(q)$ et $p^2 \not\equiv 1(q)$ (et par suite $p \not\equiv 1(q)$, on en déduit que $n_q = 1$ et par suite que H_q est l'unique q-sous-groupe de G (et donc normal dans G).

Le théorème précédent montre alors que $G \simeq H_p \times H_q$ et est donc abélien puisque, pour des raisons d'ordre, H_p et H_q le sont.

□

Proposition.— *Soit p un nombre premier et G un groupe d'ordre p^2. G est soit isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ soit à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Preuve : Supposons que G ne soit pas cyclique. D'après Sylow, il existe un sous-groupe $H =< x >$ de G d'ordre p. Considérons un élément $y \in G - H$. Comme G n'est pas cyclique y n'est pas d'ordre p^2 et comme $y \neq e$, il n'est pas d'ordre 1 non plus. On en déduit que $o(y) = p$.

Maintenant le groupe $< x > \cap < y >= \{e\}$ car c'est un sous-groupe de $< x >$ et de $< y >$ qui sont distincts et d'ordre p premier tous deux. Par ailleurs, pour des raisons d'ordres, on voit que $< x, y >= G$. Comme G est abélien, puisque d'ordre p^2, par application des résultat sur les produits directs de groupes, on trouve que $G \simeq < x > \times < y > \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

□

3.2.3 Classification des groupes finis d'ordre ≤ 10.

On se propose, dans ce paragraphe, d'appliquer les résultats du précédent pour classifier les groupes finis G, à isomorphisme près, jusqu'à l'ordre $n = 10$.

- $n = 1$. Il n'y a que le groupe trivial.
- $n = 2$. C'est un nombre premier donc G est cyclique et $G \simeq \mathbb{Z}/2\mathbb{Z}$.
- $n = 3$. C'est un nombre premier donc G est cyclique et $G \simeq \mathbb{Z}/3\mathbb{Z}$.
- $n = 4$. $4 = 2^2$, donc $G \simeq \mathbb{Z}/4\mathbb{Z}$ ou $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- $n = 5$. C'est un nombre premier donc G est cyclique et $G \simeq \mathbb{Z}/5\mathbb{Z}$.
- $n = 6$. On a $6 = 2.3$ et 3 premier impair, donc G est soit isomorphe à $\mathbb{Z}/6\mathbb{Z}$ soit à $D_3 = S_3$.
- $n = 7$. C'est un nombre premier donc G est cyclique et $G \simeq \mathbb{Z}/7\mathbb{Z}$.
- $n = 8$. 1/ Supposons que G soit abélien.

a) Si G a un élément d'ordre 8 alors G est cyclique et donc $G \simeq \mathbb{Z}/8\mathbb{Z}$.

b) Si G n'a pas d'élément d'ordre 8 mais un d'ordre 4. Notons $H =< x >$ où $o(x) = 4$ et prenons un élément $y \notin H$.

. Si $o(y) = 2$, alors H et $< y >$ sont en somme direct et donc, pour des raisons d'ordre, on a $G = H \oplus < y > \simeq \mathbb{Z}/4Z \times \mathbb{Z}/2\mathbb{Z}$.

. Si $o(y) = 4$ alors $o(y^2) = 2$. Si $y^2 \notin H$, alors pour les mêmes raisons que précédement on a $G = H \oplus < y^2 > \simeq \mathbb{Z}/4Z \times \mathbb{Z}/2\mathbb{Z}$. Si $y^2 \in H$ alors l'élément $z = xy$ est d'ordre 2, car dans H il n'y a qu'un seul élément d'ordre 2 : $x^2 = y^2$ et donc $z^2 = x^2y^2 = e$. Maintenant $z \notin H$, donc pour les mêmes raisons que précédement on a $G = H \oplus < z > \simeq \mathbb{Z}/4Z \times \mathbb{Z}/2\mathbb{Z}$.

On a donc $G \simeq \mathbb{Z}/4Z \times \mathbb{Z}/2\mathbb{Z}$.

c) Il n'existe pas d'élément d'ordre 4. Donc tous les éléments non triviaux de G sont d'ordre 2. Soit $a \neq e$ et $b \notin < a >$, notons $H =< a, b >$. C'est un groupe d'ordre 4 isomorphe à $< a > \times < b >$ (même raisonnement qu'avant). Soit $c \notin H$, $< c >$ étant d'ordre 2, on voit que $< c > \cap H = \{e\}$ et donc comme G est abélien, on a $< a, b, c > \simeq H \times < c > \simeq < a > \times < b > \times < c >$. Pour des raisons d'ordre, on a $G =< a, b, c > \simeq \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$.

2/ Supposons G non abélien. Si pour tout $x \in G$, on a $x^2 = e$, alors pour $x, y \in G$, on a $(xy)^2 = e = xyxy$ et donc $xy = x^2yxy^2$ c'est-à-dire $xy = yx$, donc G est abélien. Ainsi, il existe un élément a d'ordre 4 dans G.

Posons $N =< a >$, comme N est d'indice 2 dans G, on a donc $N \triangleleft G$. Notons alors $s : G \to G/N$ la surjection canonique. Le groupe G/N est d'ordre 2 et si $b \in G - N$, on a $s(b) \neq \overline{e}$ et $s(b^2) = (s(b))^2 = \overline{e}$, on a donc $b^2 \in N$.

Plus précisément, comme b^2 ne peut pas être d'ordre 4 (sinon b serait d'ordre 8 et G serait cyclique), on a $b^2 = e$ ou $b^2 = a^2$ (car sinon $b^2 = a$ ou a^3 qui sont d'ordre 4).

a) Si $b^2 = e$. Notons $H =< b >= \{e, b\}$, on a donc $H \cap N = \{e\}$. Comme N est distingué, on a $bab^{-1} \in N$, et comme a est d'ordre 4, on a $bab^{-1} = a$ ou $a^3 = a^{-1}$. Si $bab^{-1} = a$ alors tout élément de H commute avec tout élément de N et, pour des raisons évidentes, d'ordre, on a $HN = G$, ce qui implique que $G \simeq H \times N$ ce qui est absurde puisque G n'est pas commutatif. On a donc $bab^{-1} = a^{-1}$. On voit alors que l'action par conjugaison du groupe H sur le groupe N est le passage à l'inverse, ce qui justifie que $G = NH$ est isomorphe au groupe D_3.

b) Si $b^2 = a^2$, posons $c = ab$, $d = ba$. Il est clair que ni b ni b^3 ni c ni d ne sont dans N (sinon $b \in N$). De même, les éléments b, b^3, c, d sont distincts deux à deux. En effet, b est visiblement distincts de c et de d (car sinon $a = e$) et de b^3 (sinon b n'est plus d'ordre 3). b^3 est distinct de c et de d (sinon $a = a^2$). Et enfin, $c \neq d$ sinon a et b commuttent et comme ils engendrent G, G serait abélien.

On a donc $G = \{e, a, a^2, a^3, b, b^3, ab, ba\}$. On a $aba = b$ et $bab = a$ (tester toutes les possibilités), et donc, on en déduit que la table de Cayley du groupe G est :

$+$	e	a	a^2	a^3	b	b^3	ab	ba
e	e	a	a^2	a^3	b	b^3	ab	ba
a	a	a^2	a^3	e	ab	ba	b^3	b
a^2	a^2	a^3	e	a	b^3	b	ba	ab
a^3	a^3	e	a	a^2	ba	ab	b	b^3
b	b	ba	b^3	ab	a^2	e	a	a^3
b^3	b^3	ab	b	ba	e	a^2	a^3	a
ab	ab	b	ba	b^3	a^3	a	a^2	e
ba	ba	b^3	ab	b	a	a^3	e	a^2

On voit alors que la correspondance

$$e \longleftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad a \longleftrightarrow \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$
$$a^2 \longleftrightarrow \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \qquad a^3 \longleftrightarrow \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$
$$b \longleftrightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad b^3 \longleftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$
$$ab \longleftrightarrow \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \qquad ba \longleftrightarrow \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

définit un isomorphisme entre G et Q_8.

- $n = 9$. $9 = 3^2$, donc $G \simeq \mathbb{Z}/9\mathbb{Z}$ ou $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
- $n = 10$. On a $6 = 2.5$ et 5 premier impair, donc G est soit isomorphe à $\mathbb{Z}/10\mathbb{Z}$ soit à D_5.

ordre	groupes abéliens	nb	groupes non abéliens	nb	total
1	$\{0\}$	1		0	1
2	$\mathbb{Z}/2$	1		0	1
3	$\mathbb{Z}/3$	1		0	1
4	$\mathbb{Z}/4$, $\mathbb{Z}/2\times\mathbb{Z}/2$	2		0	2
5	$\mathbb{Z}/5$	1		0	1
6	$\mathbb{Z}/6$	1	D_3	1	2
7	$\mathbb{Z}/7$	1		0	1
8	$\mathbb{Z}/8$, $\mathbb{Z}/2\times\mathbb{Z}/4$, $(\mathbb{Z}/2)^3$	3	D_4, Q_8	2	5
9	$\mathbb{Z}/9$, $\mathbb{Z}/3\times\mathbb{Z}/3$	2		0	2
10	$\mathbb{Z}/10$	1	D_5	1	2

Chapitre 4

Généralités sur les anneaux

4.1 Anneaux et morphismes

4.1.1 Anneau

Définition.— *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 bilatère, 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.— *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.— *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.— *Soit A un anneau unitaire. Le magma $(U(A),.)$ 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) Sur $\mathbb{Z}/n\mathbb{Z}$ on définit une multiplication par : $\overline{a}.\overline{b} = \overline{ab}$. On vérifie que la définition de cette loi ne dépend pas du choix des représentants des classes. Alors $(\mathbb{Z}/n\mathbb{Z},+,.)$ est un anneau commutatif et unitaire et on a $U(\mathbb{Z}/n\mathbb{Z}) = \{\overline{a} / \ a \in \mathbb{Z} \text{ premier avec } n\}$.

g) Si $\{A_i\}_{i\in I}$ désigne un ensemble d'anneaux, l'anneau produit $\prod_{i\in I} A_i$ en considérant les deux lois de compositions

$$(a_i)_{i\in I} + (b_i)_{i\in I} = (a_i + b_i)_{i\in I}$$
$$(a_i)_{i\in I}.(b_i)_{i\in I} = (a_i.b_i)_{i\in I}$$

On vérifie sans mal que l'anneau produit $\prod_{i\in I} A_i$ est commutatif (resp. unitaire) ssi tous les A_i le sont. Par ailleurs, si l'anneau produit est unitaire alors on a

$$U\left(\prod_{i\in I} A_i\right) = \prod_{i\in I} U(A_i)$$

Il est à noter que si $\sharp I \geq 2$ alors $\prod_{i\in I} A_i$ n'est jamais intègre.

h) 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.— *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.— *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.

□

Soit A un anneau commutatif intègre. Sur l'ensemble $A \times (A - \{0\})$, on considère la relation binaire $\mathcal{R}$ définie par $(a,b)\mathcal{R}(c,d) \Longleftrightarrow ad = bc$. C'est une relation d'équivalence (exercice). Sur l'ensemble quotient $K = A \times (A - \{0\})/\mathcal{R}$, on définit les lois de composition suivante :

$$\begin{aligned} \overline{(a,b)} + \overline{(c,d)} &= \overline{(ad+bc, bd)} \\ \overline{(a,b)}.\overline{(c,d)} &= \overline{(ac, bd)} \end{aligned}$$

Ces définitions ne dépendent pas des représentants des classes d'équivalences. En effet soit $(a,b), (a',b'), (c,d), (c',d') \in A \times A - \{0\}$ tels que $\overline{(a,b)} = \overline{(a',b')}$ et $\overline{(c,d)} = \overline{(c',d')}$. On a alors

$$(ad+bc)b'd' = ab'dd' + cd'bb' = a'bdd' + c'dbb' = (a'd' + b'c')bd$$

et par suite $\overline{(ad+bc, bd)} = \overline{(a'd' + b'c', b'd')}$. De même, on a

$$(ac)(b'd') = ab'cd' = a'bc'd = (a'c')(bd)$$

et par suite $\overline{(ac, bd)} = \overline{(a'c', b'd')}$.

Théorème-Définition.— *Soit A un anneau commutatif et intègre. L'ensemble $(K, +, .)$ précédement défini est un corps commutatif. On l'appelle corps des fractions de A et on le note* $\mathrm{Frac}(A)$. *Un élément de K de représentant $(a,b) \in A \times A - \{0\}$ se note $\dfrac{a}{b}$.*

Si A est unitaire, alors il existe un monomorphisme naturel de A dans K.

Preuve : • $(K, +)$ est un groupe abélien.

Commutativité : $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{cb+da}{db} = \frac{c}{d} + \frac{a}{b}$.

Associativité : $\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{adf+bcf+bde}{bdf} = \frac{a}{b} + \frac{cf+de}{df} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right)$

Neutre : $\frac{0}{x} + \frac{a}{b} = \frac{0b+xa}{xb} = \frac{xa}{xb} = \frac{a}{b}$.

Opposé : $\frac{a}{b} + \frac{-a}{b} = \frac{ab-ab}{b^2} = \frac{0}{b^2}$.

• $(K, +, .)$ est un corps commutatif.

Commutativité : $\frac{a}{b}.\frac{c}{d} = \frac{ac}{bd} = \frac{cb}{db} = \frac{c}{d}.\frac{a}{b}$.

Associativité : $\left(\frac{a}{b}.\frac{c}{d}\right).\frac{e}{f} = \frac{ac}{bd}.\frac{e}{f} = \frac{ace}{bdf} = \frac{a}{b}.\frac{ce}{df} = \frac{a}{b}.\left(\frac{c}{d}.\frac{e}{f}\right)$.

Distibutivité : $\frac{a}{b}.\left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b}\frac{cf+de}{df} = \frac{acf+ade}{bdf} = \frac{ad+bc}{bd}.\frac{e}{f} = \left(\frac{a}{b} + \frac{c}{d}\right).\frac{e}{f}$.

Neutre : $\frac{x}{x}.\frac{a}{b} = \frac{xa}{xb} = \frac{a}{b}$.

Existence d'un inverse pour . : $\frac{a}{b}\frac{b}{a} = \frac{ab}{ba} = \frac{ab}{ab}$.

Supposons que A soit unitaire. Et considérons l'application

$$\begin{array}{rccc} \varphi : & A & \longrightarrow & \mathrm{Frac}(A) \\ & a & \longmapsto & \frac{a}{1} \end{array}$$

On a pour tout $a, b \in A$,

$$\begin{aligned} \varphi(a+b) &= \tfrac{a+b}{1} = \tfrac{a}{1} + \tfrac{b}{1} = \varphi(a) + \varphi(b) \\ \varphi(a.b) &= \tfrac{a.b}{1} = \tfrac{a}{1}.\tfrac{b}{1} = \varphi(a).\varphi(b) \end{aligned}$$

Par ailleurs $\varphi(1) = \frac{1}{1} = 1_K$ et donc φ est un morphisme d'anneaux unitaires. On a $x \in \mathrm{Ker}(\varphi)$ si et seulement si $\frac{x}{a} = \frac{0}{a}$ c'est-à-dire ssi $xa = a0$, ssi $x = 0$. Donc φ est injectif.

□

Par exemple, si $A = \mathbb{Z}$, alors $\mathrm{Frac}(A) = \mathbb{Q}$. Si $A = K[X]$ avec K un corps, alors $\mathrm{Frac}(K[X]) = K(X)$ (ensemble des fractions rationnelles).

4.1.2 Morphisme

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

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

Preuve : Exercice.

□

4.1.3 Caractéristique

On considère un anneau A unitaire et l'application

$$\begin{array}{rccc} \varphi : & \mathbb{Z} & \longrightarrow & A \\ & n & \longmapsto & n.1_A \end{array}$$

Il s'agit visiblement d'un morphisme d'anneau, son noyau est donc un sous-groupe de $\mathbb{Z}$, c'est-à-dire un ensemble de la forme $r\mathbb{Z}$ avec $r \in \mathbb{N}$.

Définition.— *L'entier r précédement défini s'appelle la caractéristique de l'anneau A. On le note* $\text{car}(A)$.

Si $\text{car}(A) = 0$ alors $\mathbb{Z}$ peut être vu comme un sous-anneau de A. Si $r = \text{car}(A) > 0$, l'entier r est donc le plus petit entier non nul tel que $r.1_A = 0_A$. En particulier, si n est un entier multiple de r, alors pour tout $a \in A$, on a $n.a = 0_A$ (exercice).

Exemple : a) L'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n.

b) Les anneaux $\mathbb{Z}, \mathbb{Z}[X]$ sont de caractéristique 0.

c) L'anneau $(\mathcal{P}(E), \Delta, \cap)$ est de caractéristique 2.

Proposition.— *Soit A un anneau unitaire de caractéristique p un nombre premier. Pour tout $a, b \in A$ tel que $ab = ba$, on a*

$$(a+b)^p = a^p + b^p$$

Preuve : La formule du binôme de Newton dit que $(a+b)^p = \sum_{k=0}^{p} C_p^k a^k b^{n-k}$. Maintenant, puisque p est premier, pour tout $k = 1, \cdots, p-1$, on a $p | C_p^k$ (exercice) et donc $C_p^k a^k b^{n-k} = 0$.

□

On voit immédiatement que, par récurrence, on a dans cette situation

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$

pour tout entier $n \geq 0$.

4.2 Idéaux et anneaux quotients

4.2.1 Idéaux et sous-anneaux

Définition.— *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.— *Dans un anneau commutatif A un idéal I est dit principal s'il est de la forme $I = aA (= Aa)$. Un anneau A est 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.— *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.

□

Lemme-Définition.— *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. En particulier, si X est une partie non vide de A, il existe un plus petit idéal de A contenant X. On l'appelle idéal engendré par X et on le note (X).*

Preuve : Exercice.

□

Si I et J sont deux idéaux d'un anneau commutatif A alors l'idéal engendré par $I \cup J$ est l'idéal $I + J = \{x + y/\ x \in I, y \in J\}$ (exercice). On l'appelle l'idéal somme des idéaux I et J. Plus généralement, si $\{I_k\}_{k\in K}$ désigne une famille d'idéaux de A, note $\sum_{k\in K} I_k$ l'idéal de A engendré par $\bigcup_{k\in K} I_k$. On voit alors que

$$\sum_{k\in K} I_k = \left\{ \sum_{j\in J} x_j/\ J \subset K\ fini,\ \forall j \in J\ x_j \in I_j \right\}$$

L'idéal $I.J$ de A engendré par les élément de la forme $x_i x_j$ avec $x_i \in I$ et $x_j \in J$ s'appelle l'idéal produit des idéaux I et J. Si I est un idéal de A et $(J_k)_k$ une famille d'idéaux de A alors on a $I.\left(\sum_k J_k\right) = \sum_k I.J_k$ (exercice).

On voit immédiatement que $I.J \subset I \cap J \subset I, J \subset I + J$. Il est à noter que ces inclusions sont strictes en général.

Proposition.— *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 $\mathrm{Ker}(f)$ *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).

Définition.— *Soit A un anneau commutatif et unitaire et I un idéal de A. On dit que I est*

- *premier, si pour tout $x, y \in A$, $xy \in I \Longrightarrow x \in I$ ou $y \in I$.*
- *maximal, si $I \neq A$ et si pour tout idéal $N \neq A$ de A on a $I \subset N \Longrightarrow I = N$.*

Remarque : On voit, par récurrence, que si I est un idéal premier d'un anneau A et si $x_1, \cdots, x_n$ sont des éléments de A qui ne sont pas dans I, alors le produit $x_1 \cdots x_n$ n'est pas dans I.

Théorème.— (Krull) *Soit A un anneau unitaire et I un idéal de A. Il existe un idéal maximal M de A qui contient I. En particulier tout anneau unitaire possède des idéaux maximaux.*

Preuve : Considérons l'ensemble $\mathcal{I}$ des idéaux stricts de A contenant I. L'ensemble $\mathcal{I}$ n'est visiblement pas vide puisqu'il contient I. L'ensemble ordonné $(\mathcal{I}, \subset)$ est inductif. En effet, considérons une chaine $\{I_x\}_{x \in X}$ d'éléments de $\mathcal{I}$. Comme cette famille est totalement ordonnée, l'ensemble $N = \bigcup_{x \in X} I_x$ est un idéal de A (qui contient I). Maintenant $N \neq A$ sinon on aurait $1 \in A$ et par suite, il existerait $x \in X$ tel que $1 \in I_x$ ce qui impliquerait que $I_x = A$. On en déduit donc que $N \in \mathcal{I}$ et donc que la chaine $\{I_x\}_{x \in X}$ admet un majorant.

D'après l'axiome de Zorn, il existe un élément maximal M dans $\mathcal{I}$. Il vérifie alors les propriétés du théorème.

□

Proposition.— (Théorème d'évitement) *Soit A un anneau commutatif.*

a) Soient $P_1, \cdots, P_n$ des idéaux premiers de A et I un idéal de A tel que $I \subset \bigcup_{i=1}^{n} P_i$. Il existe $i \in \{1, \cdots, n\}$ tel que $I \subset P_i$.

De plus, si dans cette situation on a $I = \bigcup_{i=1}^{n} P_i$ alors il existe $i \in \{1, \cdots, n\}$ tel que $I = P_i$.

b) Soient $I_1, \cdots, I_n$ des idéaux de A et P un idéal premier de A tel que $\bigcap_{i=1}^{n} I_i \subset P$. Il existe $i \in \{1, \cdots, n\}$ tel que $I_i \subset P$.

De plus, si dans cette situation on a $P = \bigcap_{i=1}^{n} I_i$ alors il existe $i \in \{1, \cdots, n\}$ tel que $I_i = P$.

Preuve : a) Quitte à retirer des P_i de la réunion, on peut supposer que $P_i \neq P_j$ pour tout $i \neq j$. Ainsi, pour tout $i \neq j$, notons x_{ij} un élément de P_j qui n'est pas dans P_i. Considérons alors pour tout $i = 1, \cdots, n$ l'élément $x_i = \prod_{j \neq i} x_{ij}$. Puisque P_i est premier et qu'aucun x_{ij} n'est dans P_i, on en déduit que $x_i \notin P_i$. Par contre, pour $j \neq i$, comme P_j est un idéal et que $x_{ij} \in P_j$, on voit que $x_i \in P_j$.

Supposons que I ne soit inclus dans aucun des P_i, c'est-à-dire que pour tout $i = 1, \cdots, n$, il existe $a_i \in I$ tel que $a_i \notin P_i$. Considérons l'élément

$$x = x_1 a_1 + \cdots + x_n a_n$$

Comme I est un idéal, et que $a_i \in I$ pour tout $i = 1, \cdots, n$, on a que $x \in I$ et, par suite, il existe un indice $i_0 \in \{1, \cdots, n\}$ tel que $x \in P_{i_0}$. Maintenant, pour tout $i \neq i_0$ on a $x_i \in P_{i_0}$ et donc, comme P_{i_0} est un idéal, on a

$$a_1 x_1 + \cdots + a_{i_0-1} x_{i_0-1} + a_{i_0+1} x_{i_0+1} + \cdots + a_n x_n \in P_{i_0}$$

et donc $a_{i_0} x_{i_0} \in P_{i_0}$, mais ceci est absurde car ni a_{i_0} ni x_{i_0} ne vit dans P_{i_0} et P_{i_0} est premier.

Supposons que $I = \bigcup_{i=1}^{n} P_i$. D'après ce qui précède, il existe $i_0 \in \{1, \cdots, n\}$ tel que $I \subset P_{i_0}$. Si $I \neq P_{i_0}$, alors comme $P_{i_0} \subset \bigcup_{i=1}^{n} P_i$, on ne peut pas avoir $I = \bigcup_{i=1}^{n} P_i$. Donc $I = P_{i_0}$.

b) Supposons que pour tout $i = 1, \cdots, n$, il existe $x_i \in I_i$ tel que $x_i \notin P$. Considérons l'élément $x = x_1 \cdots x_n$, comme les I_i sont des idéaux, on a $x \in I_i$ pour tout $i = 1, \cdots, n$ et donc $x \in P$. Comme P est premier, $x_1(x_2 \cdots x_n) \in P$ et $x_1 \notin P$, on a $x_2 \cdots x_n \in P$. On en déduit, par récurrence, que $x_n \in P$, ce qui est absurde.

Supposons que $P = \bigcap_{i=1}^{n} I_i$. D'après ce qui précède, il existe $i_0 \in \{1, \cdots, n\}$ tel que $I_{i_0} \subset P$. Si $I_{i_0} \neq P$, alors comme $\bigcap_{i=1}^{n} I_i \subset I_{i_0}$, on ne peut pas avoir $P = \bigcap_{i=1}^{n} I_i$. Donc $I_{i_0} = P$.

□

4.2.2 Anneaux quotients

Etant donné un anneau A et un idéal I de A, si l'on considère sur A la relation d'équivalence $x \mathcal{R} y \Longleftrightarrow x - y \in I$, on sait que $\mathcal{R}$ est compatible pour la structure de groupe additif de A et donc que l'ensemble quotient $A/\mathcal{R}$ a naturellement une structure de groupe en posant $\overline{x} + \overline{y} = \overline{x+y}$. On définit sur $A/\mathcal{R}$ une autre loi de composition en posant $\overline{x}.\overline{y} = \overline{x.y}$. On vérifie (exercice) que cette définition ne dépend pas du choix du représentant de la classe d'équivalence et que $(A/\mathcal{R}, +, .)$ est un anneau.

Définition.— *L'anneau $(A/\mathcal{R}, +, .)$ défini précédement s'appelle l'anneau quotient de A par l'idéal I et se note $\frac{A}{I}$.*

Remarque : a) Il est à noté que si $s : A \longrightarrow A/I$ désigne la surjection canonique, alors s est un morphisme d'anneaux et que si A est unitaire, alors A/I l'est aussi et s est un morphisme d'anneaux unitaires.

b) Tout anneau quotient de A peut s'écrire $A/\mathrm{Ker}(f)$ où f est un morphisme d'anneau et de manière générale, on voit que si $f : A \longrightarrow B$ désigne un morphisme d'anneaux alors les anneaux $\mathrm{Im}(f)$ et $A/\mathrm{Ker}(f)$ sont isomorphes (exercice).

Théorème.— *Soit $f : A \longrightarrow B$ un morphisme d'anneaux et I un idéal bilatère de A. Si $I \subset \mathrm{Ker}(f)$, alors il existe un unique morphisme d'anneau $\tilde{f} : A/I \longrightarrow B$ tel que $f = \tilde{f} \circ s$ où $s : A \longrightarrow A/I$ est l'épimorphisme canonique.*

Preuve : Exercice.

□

Remarque : Comme dans le cas des groupes, on voit que si f est surjective, alors $\tilde{f}$ l'est aussi.

Théorème.— *Soit A un anneau et I, J deux idéaux bilatères de A tels que $I \subset J$. Il existe un épimorphisme $f : A/I \longrightarrow A/J$ naturel qui envoit une classe de A modulo I sur son unique classe modulo J.*

Preuve : Exercice.

Théorème.— *Soit A un anneau et I, J deux idéaux bilatères de A. On a les isomorphismes d'anneaux suivants :*

a) $\frac{I}{I \cap J} \simeq \frac{I+J}{J}$.

b) Si $I \subset J$, alors $\frac{J}{I}$ est un idéal bilatère de $\frac{A}{I}$ et $\frac{\frac{A}{I}}{\frac{J}{I}} \simeq \frac{A}{J}$.

Par ailleurs, il existe une bijection entre les idéaux bilatères de l'anneau quotient $\frac{A}{I}$ et les idéaux bilatères de A contenant I.

Preuve : Exercice.

□

Proposition.— *Soit A un anneau commutatif et unitaire et I un idéal de A. L'idéal I est maximal (resp. premier) si et seulement si l'anneau quotient A/I est un corps (resp. intègre).*

Preuve : L'anneau A/I est commutatif et unitaire, c'est donc un corps si et seulement s'il n'a pas d'autres idéaux que A/I et $\{0\}$. Ces idéaux correspondant bijectivement à tous les idéaux de A qui contienne I, on en déduit que A/I est un corps si et seulement si I n'est contenu que dans les idéaux I et A, c'est-à-dire si et seulement si I est maximal.

Notons $s : A \longrightarrow A/I$ la surjection canonique. Supposons A/I intègre et prenons $x, y \in A$ tels que $xy \in I$. On a donc $s(xy) = 0$ mais comme $s(xy) = s(x)s(y)$ on en déduit que soit $s(x) = 0$ et donc $x \in I$, soit $s(y) = 0$ et donc $y \in I$. Ainsi I est bien premier.

Réciproquement, supposons I premier. Prenons $x, y \in A$ tels que $s(x)s(y) = 0$, alors $s(xy) = 0$ et donc $xy \in I$. Ainsi soit $x \in I$ et $s(x) = 0$, soit $y \in I$ et $s(y) = 0$. L'anneau A/I est bien intègre.

□

Corollaire.— *Soit A un anneau commutatif et unitaire. Tout idéal maximal de A est premier.*

Preuve : Immédiat.

□

Remarque : La réciproque de cette proposition est fausse. En effet, dans $\mathbb{Z}[X]$ l'idéal (X) est premier mais non maximal (exercice).

Théorème.— (dit des restes chinois) *Soit A un anneau unitaire, $I_1, \cdots, I_n$ des idéaux de A tels que pour tout $j \neq k$ on ait $I_j + I_k = A$ et $b_1, \cdots, b_n \in A$. Il existe un élément $b \in A$ tel que $b \equiv b_j \ mod\ I_j$ pour tout $j = 1, \cdots, n$. De plus, l'élément b est déterminé de facon unique modulo l'idéal $I_1 \cap \cdots \cap I_n$.*

Preuve : Procédons par récurrence sur l'entier n.

Pour $n = 2$ Soit $b_1, b_2 \in A$ et $(a_1, a_2) \in I_1 \times I_2$ tels que $a_1 + a_2 = 1$. Posons $b = a_2 b_1 + a_1 b_2$. On a

$$b - b_1 = (a_2 - 1)b_1 + a_1 b_2 = a_1(b_2 - b_1) \in a_1 A \subset I_1$$

De même, on a $b - b_2 \in I_2$.

Supposons que pour $n - 1 \geq 2$ la proposition soit vraie. Alors au rang n, posons $J = \bigcap_{k=1}^{n-1} I_k$. Pour tout $j = 1, \cdots n-1$ considérons des éléments $a_j \in I_j$ et $a_j^{'} \in I_n$ tels que $a_i + a_i^{'} = 1$. En développant la relation $\prod_{j=1}^{n-1}(a_i + a_i^{'}) = 1$, on obtient $a_1 \cdots a_{n-1} + b = 1$ avec $b \in I_n$, mais visiblement on a $a_1 \cdots a_n \in I_1 \cap \cdots \cap I_{n-1}$ et donc, par suite, on a $I_1 \cap \cdots \cap I_{n-1} + I_n = A$.

Soit $b_1, \cdots, b_n \in A$, par hypothèse de récurrence, il existe $b_0 \in A$ tel que $b_0 - b_j \in I_j$ pour tout $j = 1, \cdots, n-1$. mais en appliquant la proposition au rang $n = 2$ pour les idéaux $I_1 \cap \cdots \cap I_{n-1}$ et I_n, on trouve qu'il existe $b \in A$ tel que $b - b_0 \in I_1 \cap \cdots \cap I_{n-1}$ et $b_n - b_0 \in I_n$. Comme pour tout $j = 1, \cdots, n-1$ on a $b - b_0 \in I_j$ et $b_0 - b_j \in I_j$, on a finalement $b - b_j \in I_j$.

Par ailleur, si $b^{'} \in A$ est un autre élément vérifiant $b^{'} - b_j \in I_j$ pour tout $j = 1, \cdots, n$. En soustrayant les relations, on a alors, $b - b^{'} \in I_j$ pour tout $j = 1, \cdots, n$, c'est-à-dire $b - b^{'} \in I_1 \cap \cdots \cap I_n$.

□

Si I et J sont deux idéaux d'un anneau A tels que $I \subset J$, on voit que l'on peut définir une application naturelle $f : \dfrac{A}{I} \longrightarrow \dfrac{A}{J}$ de la manière suivante : si $s_I : A \longrightarrow A/I$ et $s_J : A \longrightarrow A/J$ désignent les surjections canonique, on pose pour tout $a \in A$, $f(s_I(a)) = s_J(a)$. On vérifie sans mal que la définition de f ne dépend pas du choix de a modulo I et que f est alors un morphisme d'anneau. On dit que f est le morphisme naturel.

En particulier, si $I_1, \cdots, I_n$ sont des idéaux de A, pour tout $j = 1, \cdots, n$ on peut considérer le morphisme naturel

$$f_j : \frac{A}{I_1 \cap \cdots \cap I_n} \longrightarrow \frac{A}{I_j}$$

et par suite l'application naturelle

$$\begin{array}{rccc} \theta : & \dfrac{A}{I_1 \cap \cdots \cap I_n} & \longrightarrow & \dfrac{A}{I_1} \times \cdots \times \dfrac{A}{I_n} \\ & x & \longmapsto & (f_1(x), \cdots, f_n(x)) \end{array}$$

Ce morphisme est alors injectif, en effet, si $x \in A$ est tel que $s_{I_1 \cap \cdots \cap I_n}(x) \in \mathrm{Ker}(\theta)$ alors $f_j(s_{I_j}(x)) = 0$ pour tout $j = 1, \cdots, n$ et donc $x \in I_j$. Ainsi, $x \in I_1 \cap \cdots \cap I_n$, c'est-à-dire $s_{I_1 \cap \cdots \cap I_n}(x) = 0$. Le théorème des restes chinois permet d'en dire plus sur le monomorphisme θ :

Corollaire.— *Soit A un anneau unitaire, $I_1, \cdots, I_n$ des idéaux de A tels que pour tout $j \neq k$ on ait $I_j + I_k = A$. Le monomorphisme naturel*

$$\theta : \frac{A}{I_1 \cap \cdots \cap I_n} \longrightarrow \frac{A}{I_1} \times \cdots \times \frac{A}{I_n}$$

est un isomorphisme.

Preuve : Il s'agit donc de montrer que θ est surjectif, mais si $b_1, \cdots, b_n \in A$, le théorème des restes chinois affirme qu'il existe $b \in A$ tel que $b \equiv b_j \bmod I_j$ pour tout $j = 1, \cdots, n$. On a donc $\theta(s_{I_1 \cap \cdots \cap I_n}(b)) = (s_{I_1}(b_1), \cdots, s_{I_n}(b_n))$ et donc θ est surjective.

□

4.3 Anneaux euclidiens, principaux, factoriels

Dans cette partie tous les anneaux considérés seront commutatifs et unitaires.

4.3.1 Arithmétique des anneaux

Définition.— *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.— *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, $u, v \in U(A)$.

□

Définition.— *Soit A un anneau commutatif et unitaire et $c \in A$ un élément non nul et non inversible. On dit que c est*

- *irréductible, si pour tout $a, b \in A$, $c = ab \Longrightarrow a$ ou b inversible.*
- *premier, si pour tout $a, b \in A$, $c|ab \Longrightarrow c|a$ ou $c|b$.*

Exemples : (Exercice)

a) $A = \mathbb{Z}$. On a p premier ssi p irréductible.

b) $A = \mathbb{Z}/6\mathbb{Z}$. L'élément $\overline{2}$ est premier mais n'est pas irréductible.

c) $A = \mathbb{Z}[\sqrt{-10}] = \{a + ib\sqrt{10} / \ a, b \in \mathbb{Z}\}$. L'élement 2 est irréductible mais pas premier.

Proposition.— *Soit A un anneau commutatif unitaire intègre et $a \in A$.*

a) a est premier si et seulement si (a) est un idéal premier non nul.

b) a est irréductible si et seulement si (a) est un idéal maximal non nul dans l'ensemble des idéaux principaux stricts de A.

c) Si a est premier alors a est irréductible.

d) Si a est irréductible alors les seuls diviseurs de a sont les unités et les associés de a.

Preuve : a) On a $(a) = aA$. Si a est premier et si $b, c \in A$ sont tels que $bc \in aA$, alors il existe $x \in A$ tel que $bc = xa$. On en déduit que $a|bc$, donc $a|b$ (et dans ces conditions $b \in aA$) ou $a|c$ (et dans ces conditions $c \in aA$). Ainsi (a) est bien premier.

Réciproquement, supposons que (a) soit premier et considérons $b, c \in A$ tel que $a|bc$. On a donc $bc = ax$ pour un certain $x \in A$ et donc $bc \in (a)$. Donc on a $b \in (a) = aA$ (et donc $a|b$) ou $c \in (a) = aA$ (et donc $a|c$).

b) Supposons a irréductible et prenons un idéal principal strict $I = bA$ ($b \in A$), tel que $(a) = aA \subset I = bA$. On a donc $a \in bA$ et par suite $b|a$. Il existe donc $x \in A$ tel que $a = xb$, mais comme a est irréductible, on a soit $x \in U(A)$ soit $b \in U(A)$. La deuxième hypothèse est impossible car alors on aurait $I = A$. On a donc $x \in U$, donc $a|b$ et par suite $b \in aA$ et donc $bA \subset aA$. On en conclu que $aA = bA$ et donc que aA est bien maximal.

Réciproquement, supposons aA est maximal dans l'ensemble des idéaux principaux stricts de A et $a = bc$ avec $b, c \in A$. Si ni b ni c ne sont des unités, comme on a $(a) \subset (b)$ et $(a) \subset (c)$, on en déduit, par hypothèse de maximalité, que $(a) = (b)$ et $(a) = (c)$. Ainsi, il existe $u, v \in U(A)$ tel que $a = ub$ et $a = vc$ et donc $uva = a^2$. Comme A est intègre, on a $a = uv \in U(A)$ ce qui implique $aA = A$ et ce dernier point est contraire aux hypothèses.

c) Supposons a premier et $b, c \in A$ tels que $a = bc$. On a donc $a|bc$ et donc $a|b$ ou $a|c$ (disons $a|b$). Il existe donc $d \in A$ tel que $b = ad$ et par suite on a $a = adc$. Comme A est intègre, on a donc $dc \in U(A)$ et donc $c \in U(A)$.

d) Immédiat.

□

Définition.— *Soit A un anneau et $\{a_i\}_{i\in I}$ une famille non vide d'éléments de A. Un élément $a \in A$ est appelé plus grand commun diviseur (noté en abrégé p.g.c.d.) de la famille $\{a_i\}_{i\in I}$ (resp. plus petit commun multiple (noté en abrégé p.p.c.m.) de la famille $\{a_i\}_{i\in I}$) si $a|a_i$ pour tout $i \in I$ et si $b \in A$ est tel que $b|a_i$ pour tout $i \in I$ alors $b|a$ (resp. $a_i|a$ pour tout $i \in I$ et si $b \in A$ est tel que $a_i|b$ pour tout $i \in I$ alors $a|b$).*

On dit que les éléments de $\{a_i\}_{i\in I}$ sont premiers entre eux (dans leur ensemble) s'ils admette 1 pour p.g.c.d.

Remarques : a) (Exercice) Notons $\mathcal{B}_A$ l'ensemble des idéaux principaux de A. Dire que la famille $\{a_i\}_{i\in I}$ admet un p.g.c.d. (resp. un p.p.c.m.) équivaut à dire que la famille d'idéaux $\{(a_i)\}_{i\in I}$ admet une borne supèrieure (resp. inférieure) $\mathcal{M}$ dans $\mathcal{B}_A$. On remarque alors que les p.g.c.d. (resp. les p.p.c.m.) de la famille $\{a_i\}_{i\in I}$ sont exactement les $d \in A$ tel que $\mathcal{M} = dA$.

b) On remarque que tous les p.g.c.d. (resp. les p.p.c.m.) d'une famille $\{a_i\}_{i\in I}$ (s'il en exsite au moins un) sont associés.

c) On peut reformuler de manière équivalente, pour les éléments d'une famille $\{a_i\}_{i\in I}$, le fait d'être premiers entre eux en disant que les seuls $d \in A$ vérifiants $d|a_i$ pour tout $i \in I$ sont les éléments de $U(A)$.

4.3.2 Anneaux factoriels

Définition.— *Un anneau A est dit factoriel s'il vérifie les propriétés suivantes :*

1/ A est commutatif, unitaire et intègre.

2/ Tout élément non nul et non inversible de A se décompose comme un produit fini d'éléments irréductibles.

3/ Une telle décomposition est unique, à l'ordre et aux unités près. i.e. si $p_1, \cdots, p_n$ et $q_1, \cdots, q_m$ sont des irréductibles tels que

$$p_1 \cdots p_n = q_1 \cdots q_m$$

alors $n = m$ et il existe $\sigma \in S_n$ et pour tout $i = 1, \cdots, n$, $u_i \in U(A)$ tels que $p_i = u_i q_{\sigma(i)}$.

Exemple.— Les anneaux $\mathbb{Z}$ et $\mathbb{Z}[X]$ sont factoriels.

Proposition.— *Soit A un anneau factoriel et $a \in A$. L'élément a est irréductible si et seulement s'il est premier.*

Preuve : Puisque A est intègre, on sait déjà que si a est premier, il est irrécutible. Réciproquement supposons a irréductible et suposons que a divise un produit xy. On a donc $xy = ab$ avec $b \in A$. Soit $x = p_1.\cdots.p_n$, $y = q_1.\cdots.q_m$ et $b = l_1.\cdots.l_k$ des décompositions en facteurs irréductibles. On a donc

$$p_1 \cdots p_n.q_1 \cdots q_m = a.l_1 \cdots l_k$$

mais comme par le 3/ la décomposition est unique à l'odre et aux unités près, on a soit $a = up_i$ pour un certain i et une certaine unité u soit $a = uq_i$ pour un certain i et une certaine unité u et donc soit $a|x$ soit $a|y$.

□

Etant donné un anneau factoriel A, on note $\mathrm{Irr}(A)$ l'ensemble des éléments irréductibles de A. Sur $\mathrm{Irr}(A)$ on considère la relation d'équivalence $\mathcal{R}$ "être associé à". Si l'on considère une classe de représentants $\mathcal{C}$ dans A de l'ensemble quotient $\mathrm{Irr}(A)/\mathcal{R}$ fixée une fois pour toute, alors on voit que pour tout élément $a \in A - \{0\}$ on peut associer un unique $u \in U(A)$ et une unique famille d'entiers positifs $(v_p(a))_{p\in\mathcal{C}}$ presque partout nulle (i.e. $v_p(a) \neq 0$ pour on nombre fini de $p \in \mathcal{C}$) telle que

$$a = u \prod_{p\in\mathcal{C}} p^{v_p(a)}$$

et réciproquement. L'entier $v_p(a)$ s'appelle la p-valuation de a. On a alors

Proposition.— *Pour tout $x, y \in A - \{0\}$, on a*

1/ $x|y$ si et seulement si $\forall p \in \mathcal{C}$, $v_p(x) \leq v_p(y)$.

2/ $v_p(xy) = v_p(x) + v_p(y)$.

3/ $v_p(x+y) \geq \min(v_p(x), v_p(y))$ et il y a égalité si $v_p(x) \neq v_p(y)$.

Preuve : Exercice.

□

Théorème.— *Soit A un anneau factoriel. Toute famille $\{a_i\}_{i\in I}$ non vide d'éléments de A admet un p.g.c.d. et, si I est fini, admet un p.p.c.m. Par ailleurs, un p.g.c.d. est*

$$d = \prod_{p\in\mathcal{C}} p^{\alpha_p} \text{ où } \alpha_p = \min_{i\in I}(v_p(a_i))$$

et un p.p.c.m. est

$$m = \prod_{p\in\mathcal{C}} p^{\beta_p} \text{ où } \beta_p = \sup_{i\in I}(v_p(a_i))$$

Preuve : Exercice.

□

Proposition.— *Soit A un anneau factoriel et $a, b, c, b_1, \cdots, b_n \in A$.*

1/ Si $a|bc$ et que a est premier avec b, alors $a|c$. ("Théorème de Gauss")

2/ Si a est premier avec chaque b_i alors a est premier avec $b_1 \cdots b_n$.

3/ Si $b_1, \cdots, b_n$ sont deux à deux premiers entre eux et que $b_i|a$ pour tout $i = 1, \cdots, n$ alors $b_1 \cdots b_n|a$. En particulier, dans cette situation, $b_1 \cdots b_n$ est un p.p.c.m. de la famille $\{b_i\}_{i=1,\cdots,n}$.

4/ L'élément b est un p.p.c.m. de la famille $\{b_i\}_{i=1,\cdots,n}$ si et seulement si $b_i|b$ pour tout $i = 1, \cdots, n$ et les élements $\dfrac{b}{b_i}$ sont premiers entre eux dans leur ensemble.

Preuve : Exercice.

□

4.3.3 Anneaux principaux

On rappelle qu'un anneau A est dit principal s'il est commutatif, intègre, unitaire et si tout idéal de A est principal. L'exemple standard d'anneau principal est l'anneau $\mathbb{Z}$.

Théorème.— *Soit A un anneau principal et $(a_i)_{i\in I}$ une famille non vide d'éléments non nul de A. La famille $(a_i)_{i\in I}$ admet un p.g.c.d. et les p.g.c.d. de cette famille sont exactement les $d \in A$ tels que $dA = \sum_{i\in I} a_i A$.*

Si l'ensemble I est fini, la famille $(a_i)_{i\in I}$ admet un p.p.c.m. et les p.p.c.m. de cette famille sont exactement les $d \in A$ tels que $dA = \bigcap_{i\in I} a_i A$.

Preuve : Soit $d \in A$ tel que $dA = \sum_i a_i A$. On a $a_i \in dA$ et par suite $d|a_i$ pour tout $i \in I$. Soit $d' \in A$ tel que $d'|a_i$ pour tout $i \in I$. On a donc $a_i \in d'A$ et donc $a_iA \subset d'A$ pour tout $i \in I$. Ceci implique que $dA = \sum_i a_i A \subset d'A$ et donc que $d'|d$. Ainsi, d est bien un p.g.c.d. de la famille $(a_i)_{i\in I}$.

Par ailleurs, si d et d' sont deux p.g.c.d. de la famille $\{a_i\}_{i=1,\cdots,n}$, alors ils sont associés et donc $dA = d'A$.

Soit $d \in A$ tel que $dA = a_1A \cap \cdots \cap a_nA$. On a donc $d \in a_iA$ et donc $a_i|d$ pour tout $i = 1, \cdots, n$. Soit $d' \in A - 0$ tel que $a_i|d'$ pour tout $i = 1, \cdots, n$, on a donc $d' \in a_iA$ pour tout $i = 1, \cdots, n$ et donc $d' \in a_1A \cap \cdots \cap a_nA = dA$ et donc $d'|d$. Ainsi, d est un p.p.c.m. des a_i.

Par ailleurs, si d et d' sont deux p.p.c.m. de la famille $\{a_i\}_{i=1,\cdots,n}$, alors ils sont associés et donc $dA = d'A$.

□

Remarque : Pour une famille infinie l'existence d'un p.p.c.m. reste indécise. Par exemple, pour $A = \mathbb{Z}$, aucune famille infinie n'admet de p.p.c.m. Par contre, pour $A = \mathbb{Q}[X]$, la famille $\{r(X-1)\}_{r\in\mathbb{Q}^*}$ est infinie et admet $X-1$ pour p.p.c.m.

Corollaire.— (Théorème dit de Bezout) *Dans les conditions du théorème précédent, les a_i sont premiers entre eux dans leur ensemble si et seulement si il existe une famille d'éléments de A, $(\lambda_i)_{i\in I}$, presque partout nulle telle que $\sum_{i\in I} \lambda_i a_i = 1$.*

Preuve : Immédiat.

□

Remarque : Le théorème de Bezout n'est pas valable dans les anneaux factoriels. En effet, prenons par exemple $A = K[X, Y]$ où K désigne un corps. Les éléments X et Y sont visiblement premiers entre eux et pourtant $(X)+(Y) \neq A$.

Corollaire.— *Soit A un anneau principal, $a, b, c \in A$ et $b_1, \cdots, b_n \in A$.*

a) ("Théorème de Gauss") Si $a|bc$ et si a est premier avec b alors $a|c$.

b) Si a est premier avec chaque b_i alors a est premier avec $B = b_1 \cdots b_n$.

c) Si les b_i sont deux à deux premiers entre eux alors $b_1 \cdots b_n$ est un p.p.c.m. de la famille $\{b_i\}_{i=1,\cdots,n}$.

d) Si les b_i sont deux à deux premiers entre eux alors les éléments

$$B_1 = B/b_1, \cdots, B_n = B/b_n$$

(avec $B = b_1 \cdots b_n$) sont premiers entre eux dans leur ensemble.

e) Si pour tout $i = 1, \cdots, n$, on a $b_i|b$ alors b est un p.p.c.m. de la famille $\{b_i\}_{i=1,\cdots,n}$ si et seulement si les b/b_i sont premiers entre eux.

Preuve : a) On écrit la relation de Bezout : il existe $u, v \in A$ tel que $au + bv = 1$ et comme par hypothèse on a $bc = xa$ pour un certain $x \in A$, on a $acu + bcv = c = acu + axv = a(cu + xv)$ on en déduit que $a|c$.

Les énoncés b),c),d),e) s'obtiennent comme le a), en utilisant Bezout et sont laissés en exercice.

□

Proposition.— *Soit A un anneau principal et $p \in A$ non nul. Les proposition suivantes sont équivalentes :*

i) p est premier,

ii) p est irréductible,

iii) pA est un idéal maximal.

Preuve : $i) \Rightarrow ii)$ Imédiat.

ii) $\Rightarrow$ *iii*) On sait que pA est maximal dans l'ensemble des idéaux principaux, mais comme tout idéal est pricipal dans A, pA est bien maximal.

iii) $\Rightarrow$ *i*) Si pA est maximal, alors il est premier puisque A est commutatif et unitaire et par suite p l'est aussi puisque A est intègre.

□

Théorème.— (des restes chinois) *Soit A un anneau principal et $a_1, \cdots, a_n$ une famille d'éléments de A deux à deux premiers entre eux. Posons $a = a_1 \cdots a_n$, il existe un isomorphisme naturel*

$$\theta : \frac{A}{aA} \longrightarrow \frac{A}{a_1 A} \times \cdots \times \frac{A}{a_n A}$$

qui a tout $x \in \dfrac{A}{aA}$ de représentant $t \in A$ associe $(t_1, \cdots, t_n)$ où t_i est la calsse de t modulo $a_i A$ pour tout $i = 1, \cdots, n$.

Preuve : C'est un application du théorème des restes chinois général. Il suffit de vérifier que $a_i A + a_j A = A$ pour tout $i \neq j$ (ceci est immédiat par Bezout) et que $a_1 A \cap \cdots \cap a_n A = aA$. Ce dernier point a été vu précédement.

□

Théorème.— *Tout anneau principal est factoriel.*

Preuve : Nous procéderons par étapes pour cette preuve. Soit A un anneau principal qui n'est pas un corps (sinon la proposition est triviale).

Etape I : *Toute suite croissante (pour l'inclusion) d'idéaux de A est stationnaire* (en termes savants, on dit que A est noethérien). En effet, soit $(I_n)_n$ une suite croissante d'idéaux de A. La réunion $I = \bigcup_{n \in \mathbb{N}} I_n$ est donc un idéal et puisque A est principal, il existe $a \in A$ tel que $I = aA$. Mais comme $a \in I$, il existe $n \in \mathbb{N}$ tel que $a \in I_n$. On a donc $aA \subset I_n$, mais comme $I_n \subset aA$, on a $I_n = aA$ et, par suite, $I_m = aA$ pour tout $m \geq n$.

Etape II : *Toute famille non vide d'idéaux de A admet un élément maximal.* En effet, sinon on peut par récurrence construire à partir de cette famille une suite strictement croissante d'idéaux, ce qui est exclu d'après l'étape I.

Etape III : *Il existe dans A au moins un élément irréductible.* Considérons la famille des idéaux de A non triviaux. Cette famille n'est pas vide car A n'est pas un corps. D'après l'étape II, il existe un élément maximal dans cette famille, et cet élément est de la forme pA avec $p \in A$ non nul et non inversible. L'idéal pA est maximal dans l'ensemble des idéaux principaux de A donc p est irréductible.

Etape IV : *Existence d'une factorisation.* Soit $\mathcal{C}$ une classe de représentants des éléments irréductibles de A. Cette classe n'est pas vide d'après l'étape III. Notons $\mathcal{E}$ l'ensemble des éléments de la forme

$$u \prod_{p \in \mathcal{C}} p^{\alpha_p}$$

où $u \in U(A)$ et $(\alpha_p)_{p \in \mathcal{C}}$ désigne une famille presque partout nulle. Il s'agit de montrer que $\mathcal{E} = A - \{0\}$.

Supposons le contraire et considérons la famille $\{xA\}_{x \notin \mathcal{E}}$. Cette famille n'est pas réduite à l'idéal $\{0\}$ par hypothèse, elle possède donc un élément maximal non trivial, d'après l'étape II. Notons aA un tel idéal. L'élément a ne peut pas être irréductible (puisque les irréductibles vivent dans $\mathcal{E}$, puisqu'ils sont tous associés à des éléments de $\mathcal{C}$), il s'écrit donc sous la forme $a = bc$ avec b et c non inversibles. L'idéal aA est donc strictement inclus dans bA et cA et, par hypothèse de maximalité, on en déduit que $b, c \in \mathcal{E}$. Mais comme l'ensemble $\mathcal{E}$ est visiblement stable pour le produit, on en déduit, pour finir, que $a = bc \in \mathcal{E}$, ce qui est absurde.

Etape V : *Unicité de la factorisation.* Supposons que l'on ait

$$u \prod_{p \in \mathcal{C}} p^{\alpha_p} = v \prod_{p \in \mathcal{C}} p^{\beta_p}$$

avec $u, v \in U(A)$ et $(\alpha_p)_{p \in \mathcal{C}}$ et $(\beta_p)_{p \in \mathcal{C}}$ presque partout nulles.

S'il existe $p_0 \in \mathcal{C}$ tel que $\alpha_{p_0} \neq \beta_{p_0}$ (par exemple $\alpha_{p_0} > \beta_{p_0}$) alors, en divisant par $p_0^{\beta_{p_0}}$, on a

$$u \prod_{p \in \mathcal{C}} p^{\alpha_p'} = v \prod_{p \in \mathcal{C}} p^{\beta_p'}$$

avec $\alpha'_{p_0} = \alpha_{p_0} - \beta_{p_0}$, $\beta'_{p_0} = 0$ et $\alpha'_p = \alpha_p$ et $\beta'_p = \beta_p$ pour $p \neq p_0$. Par suite p_0 divise $G = u\prod_{p\in\mathcal{C}} p^{\alpha'_p}$, mais comme p_0 est premier avec tout $p \neq p_0$, il est donc premier avec $D = v\prod_{p\in\mathcal{C}} p^{\beta'_p}$ (théorème de Gauss) et donc ne peut diviser D, ce qui est absurde.

On a donc $\alpha_p = \beta_p$ pour tout $p \in \mathcal{C}$ et donc, puisque A est intègre et que $D = G \neq 0$, on a $u = v$.

□

4.3.4 Anneaux euclidiens

Définition.— *Soit A un anneau commutatif, on appelle stathme euclidien sur A toute application $s : A - \{0\} \longrightarrow \mathbb{N}$ vérifiant :*

a) $\forall a, b \in A - \{0\}$, $a|b \Longrightarrow s(a) \leq s(b)$.

b) $\forall a \in A$, $\forall b \in A - \{0\}$, $\exists q, r \in A$ tels que $a = bq + r$ et $r = 0$ ou $s(r) < s(b)$.

L'anneau A est dit euclidien s'il est intègre et s'il possède un stathme euclidien s (on précise alors que A est euclidien pour le stathme s).

Remarques : a) Un anneau euclidien A peut trés bien posséder plusieurs stathmes euclidiens, par exemple si s est un stathme euclidien de A, alors ks en est aussi un pour tout $k \in \mathbb{N}$.

b) Dans un anneau euclidien A, écrire $a = bq + r$ et $r = 0$ ou $s(r) < s(b)$ pour deux éléments a et b s'appelle "effectuer la division euclidienne de a par b. L'élement q s'appelle le quotient de la division euclidienne et r le reste. Il est à noter que le couple (q, r) n'a aucune raison d'être unique (voir exemple plus bas).

Exemple : a) L'anneau $\mathbb{Z}$ est euclidien pour le stathme $|.|$. Pour ce stathme, le quotient et le reste d'une division euclidienne ne sont pas uniques, par exemple, on a

$$5 = 1.3 + 2 = 2.3 - 1$$

Une facon de palier à cela est d'imposer à ce que le reste r soit une quantité positive. Dans ces conditions il y a unicité, c'est-à-dire :

$$\forall a \in \mathbb{Z},\ \forall b \in \mathbb{Z} - \{0\},\ \exists!(q, r) \in \mathbb{Z} \times \mathbb{N} \text{ tels que } a = bq + r \text{ et } r < |b|$$

(Exercice)

b) L'anneau $K[X]$ quand K est un corps est euclidien pour le stathme d° et, dans cette situation, il y a unicité du quotient et du reste dans une division euclidienne (voir chapitre suivant).

c) Considérons le sous-anneau $\mathbb{Z}[i] = \{a + ib/\ a, b \in \mathbb{Z}\}$ de $\mathbb{C}$ et l'application $s : \mathbb{Z}[i] \longrightarrow \mathbb{N}$ définie par

$$N(a + ib) = |a + ib|^2 = a^2 + b^2$$

L'application N est multiplicative (i.e. $N(xy) = N(x)N(y)$), il s'ensuit que si $x|y$ dans $\mathbb{Z}[i]$ alors $N(x) \leq N(y)$.

Soit $x, y \in \mathbb{Z}[i]$ avec $y \neq 0$. Dans $\mathbb{C}$, on a $xy^{-1} = u + iv$ avec $u, v \in \mathbb{Q}$ et donc pour tout$q = a + ib \in \mathbb{Z}[i]$, on a $N(xy^{-1} - q) = (u - a)^2 + (v - b)^2$. On peut choisir $a \in \mathbb{Z}$ (resp. $b \in \mathbb{Z}$) tel que $|u - a| \leq 1/2$ (resp. $|v - b| \leq 1/2$), il suffit, selon la situation de prendre $a = E(u)$ ou $a = E(u) + 1$ (resp. $b = E(v)$ ou $b = E(v) + 1$). Pour un tel choix de a et de b, on a donc

$$N(xy^{-1} - q) = (u - a)^2 + (v - b)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{4} < 1$$

en posant alors $r = x - qy$, on a $x = qy + r$ et comme $N(r)N(y^{-1}) = N(ry^{-1}) = N(xy^{-1} - q) < 1$, on en déduit que $N(r) < N(y)$ et donc que N est un stathme euclidien sur $\mathbb{Z}[i]$.

Théorème.— *Tout anneau euclidien est principal (et donc, en particulier, factoriel).*

Preuve : Soit (A, s) un anneau euclidien et I un idéal non nul de A. COnsidérons l'ensemble

$$\mathcal{E} = \{s(x)/\ x \in I\}$$

c'est un ensemble non vide d'entiers, il possède donc un plus petit élément n. Soit $a \in I$ tel que $s(a) = n$ et soit $b \in I$. Effectuons la division euclidien de b par a :

$$b = aq + r \text{ avec } r = 0 \text{ ou } s(r) < s(a)$$

Si $r \neq 0$, alors $r = b - aq \in I$ et $s(r) < s(a)$. Ceci est absurde puisque n est minimal dans $\mathcal{E}$. Ainsi, on a $r = 0$, donc $b = aq = \in aA$ et, par suite, $I = aA$.

□

Comme corollaire, on obtient que si x, y sont deux éléments non nuls d'un anneau euclidien A alors ils admettent un p.g.c.d. Dans le cas des anneaux euclidiens, on possède un algorithme (dit algorithme d'Euclide) pour déterminer un p.g.c.d. de deux éléments :

Considérons donc un anneau euclidien (A, s) et deux éléments non nuls $x, y \in A$. Effectuons la division euclidienne D_1 de x par y, $x = q_1 y + r_1$. Si r_1 est non nul, effectuons la division euclidienne D_2 de y par r_1, $q_1 = q_2 r_1 + r_2$. Si $r_2 \neq 0$ effectuons la division euclidienne D_3 de r_1 par r_2. Et ainsi de suite, si, au rang k le reste r_k de la division euclidienne D_k effectuée est non nul on effectue la division euclidienne D_{k+1} du reste r_{k-1} de la division euclidienne D_{k-1} par le reste r_k de la division euclidienne D_k . On obtient donc une suite de restes non nuls (r_k). Compte tenu du fait que $s(r_1) > s(r_2) > \cdots$ et qu'il s'agit là d'une suite d'entiers positifs, il existe donc un rang n tel que $r_{n+1} = 0$. On se retrouve donc avec une suite de $n+1$ divisions euclidiennes :

$$\begin{array}{lcllcl}
D_1 & : & x & = & q_1 y & + & r_1 \\
D_2 & : & y & = & q_2 r_1 & + & r_2 \\
D_3 & : & r_1 & = & q_3 r_2 & + & r_3 \\
 & & & \vdots & & & \\
D_n & : & r_{n-2} & = & q_n r_{n-1} & + & r_n \\
D_{n+1} & : & r_{n-1} & = & q_{n+1} r_n & &
\end{array}$$

Proposition.— *Avec les notations précédentes, l'élément r_n (le dernier reste des divisions euclidiennes successives) est un p.g.c.d. des éléments x, y.*

Preuve : Comme $r_{n-1} = q_{n+1} r_n$ on a $r_n | r_{n-1}$ mais comme $r_{n-2} = q_n r_{n-1} + r_n$, on a aussi $r_n | r_{n-2}$. Par récurrence, on en déduit que $r_n | r_k$ pour tout $k = 1, \cdots, n$ et donc que $r_n | y$ et $r_n | x$.

Réciproquement, soit $a \in A$ tel que $a | x$ et $a | y$. Puisque $x = q_1 y + r_1$, on a donc $a | r_1$ et par récurrence, on trouve $a | r_n$. Ainsi r_n est bien un p.g.c.d. des éléments a et b.

□

Chapitre 5

Anneaux de polynômes

5.1 Polynômes en une variable

5.1.1 Généralités

Définition.— *Etant donné un anneau commutatif A, on appelle polynôme (en une variable) à coefficients dans A toute suite $(a_n)_n$ à coefficients dans A presque partout nulle (i.e. $a_n = 0$ pour n assez grand). On note $A[X]$ l'ensemble des polynômes en une variables à coefficients dans A.*

Notations : Si k désigne un entier positif et a un élément de a, on note aX^k la suite $(\chi_k)_n$ définie par $\chi_k(n) = 0$ si $n \neq k$ et $\chi_k(k) = a$. On dit que X est la variable de l'anneau de polynômes.

On écrit alors formellement tout polynôme $(a_n)_n \in A[X]$ sous la forme

$$\sum_{k\geq 0} a_k X^k$$

Si le polynôme $P = (a_n)_n$ n'est pas la suite nulle, il existe un plus grand entier n_0 et un plus petit entier n_1 tels que $a_{n_0} \neq 0$ et $a_n = 0$ pour tout $n > n_0$ et $a_{n_1} \neq 0$ et $a_n = 0$ pour tout $n < n_1$. Les entiers n_0 et n_1 s'appelle respectivement la valuation et le degré du polynôme P, on les note respectivement $v(P)$ et $d^\circ(P)$. Si $0 = (a_n)_n$ désigne la suite nulle, on convient que $v(0) = +\infty$ et $d^\circ(0) = -\infty$. Avec ces notations, on voit que l'on peut écrire, un polynôme $P = (a_n)_n$ non nul de $A[X]$ sous la forme

$$P(X) = \sum_{k=v(P)}^{k=d^\circ P} a_k X^k$$

L'élément a_{n_1} où $n_1 = d^\circ P$ est appelé terme de plus haut degré du polynôme P. Dans le cas où A est unitaire et que cet élément vaut 1, on dit que P est unitaire ou normalisé.

Un polynôme non nul $P \in A[X]$ vérifiant $v(P) = d^\circ P$ est appellé monôme (c'est donc un polynôme de la forme aX^n avec $a \in A - \{0\}$ et $n \geq 0$).

Arithmétique sur $A[X]$: On définit sur $A[X]$ deux lois de compositions internes + et . définies, pour $P(X) = \sum_{n\geq 0} a_n X^n$ et $Q(X) = \sum_{n\geq 0} b_n X^n$ dans $A[X]$, par :

$$(P+Q)(X) = \sum_{n\geq 0}(a_n + b_n)X^n$$
$$(P.Q)(X) = \sum_{n\geq 0} c_n X^n \text{ avec } c_n = \sum_{i+j=n} a_i b_j$$

Ces deux lois sont bien internes, car si $k_1 = d^\circ P$ et $k_2 = d^\circ Q$, on voit que pour tout $n > \sup(k_1, k_2)$, on a $a_n + b_n = 0$. De même, si $n > k_1 + k_2$ et si (i, j) est un couple d'entiers tel que $i + j = n$, alors on a $i > k_1$ ou $j > k_2$ et donc soit $a_i = 0$ soit $b_j = 0$, ce qui, dans les deux cas, assure que $c_n = 0$.

Théorème.— *Muni des lois + et ., $A[X]$ est un anneau commutatif qui contient A comme sous-anneau. Si A est unitaire (resp. intègre) alors $A[X]$ l'est aussi et, dans le cas où $A[X]$ est unitaire et intègre, on a $U(A[X]) = U(A)$.*

Preuve : Exercice.

□

Si l'on considère un élément $a \in A - \{0\}$ et un entier $n \in \mathbb{N}$, le produit aX^n s'appelle un monome. On constate alors que la notation formelle de tout à l'heure, pour un polynôme P :

$$P(X) = \sum_{k=v(P)}^{k=d^\circ P} a_k X^k$$

correspond en fait à une somme de monomes.

Si B est un anneau (quelconque) et A un sous-anneau commutatif de B, pour tout polynôme $P(X) = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$ et tout élément $b \in B$, on appelle évaluation du polynôme P en b, l'élément

$$P(b) = a_0 + a_1.b + \cdots + a_n.b^n \in B$$

Ainsi, si $b = 0$, on a donc $P(0) = a_0$ (cette évalutation s'appelle le terme constant de P). Une fois fixé l'élément $b \in B$, l'application

$$\begin{array}{rccc} \varphi_b : & A[X] & \longrightarrow & B \\ & P(X) & \longmapsto & P(b) \end{array}$$

est un morphisme d'anneaux. On l'appelle le morphisme d'évaluation en b. Les éléments de $\mathrm{Ker}(\varphi_b)$ s'appelle les "polynômes annulateurs" (dans $A[X]$) de l'élément b. Ce morphisme joue, dans des situations précises, un grand rôle en arithmétique.

Proposition.— *Soit A un anneau intègre. Pour tous $P, Q \in A[X]$, on a :*

a) $d^\circ P.Q = d^\circ P + d^\circ Q$.

b) $d^\circ(P+Q) \leq \sup(d^\circ P, d^\circ Q)$ *et il y a égalité si* $d^\circ P \neq d^\circ Q$.

c) $d^\circ P = 0 \Longleftrightarrow P \in A - \{0\}$.

d) $v(P.Q) = v(P) + v(Q)$.

e) $v(P+Q) \geq \inf(v(P), v(Q))$ *et il y a égalité si* $v(P) \neq v(Q)$.

Avec les conventions suivantes $+\infty + n = +\infty$, $-\infty + n = -\infty$ *pour tout entier* $n \geq 0$.

Preuve : Exercice.

□

Remarque : On fera bien attention que ces relation ne sont valables que dans le cas d'un anneau intègre. Par exemple, dans $\mathbb{Z}/4\mathbb{Z}[X]$, on a $\overline{2}X.\overline{2}X = 0$.

Etant donné un morphisme d'anneaux unitaires $f : A \longrightarrow B$, on peut définir l'application

$$\begin{array}{rccc} \tilde{f} : & A[X] & \longrightarrow & B[X] \\ & \sum_{i=0}^{n} a_i X^i & \longmapsto & \sum_{i=0}^{n} f(a_i) X^i \end{array}$$

On vérifie sans mal (exercice) que $\tilde{f}$ est un morphisme d'anneau et que si f est injectif (resp. surjectif) alors $\tilde{f}$ l'est aussi. Le morphisme $\tilde{f}$ est appelé le morphisme des anneaux de polynômes associé au morphisme f.

5.1.2 Propriétés de l'anneau $A[X]$

Théorème.— *Soit A un anneau commutatif et intègre. Les propositions suivantes sont équivalentes :*

i) $A[X]$ *est euclidien (pour le stathme* d°*),*

ii) $A[X]$ *est principal,*

iii) A *est un corps.*

Preuve : $i) \Rightarrow ii)$ est évident.

$ii) \Rightarrow iii)$ Considérons l'idéal $I = (X)$ engendré par X. Il est premier. En effet si $P, Q \in A[X]$ sont tels que $PQ \in I$ cela veut dire que $v(PQ) \geq 1$ et comme A est intègre, cela implique que $v(P) + v(Q) \geq 1$, c'est-à-dire que $v(P) \geq 1$ ou $v(Q) \geq 1$ (i.e. $P \in (X)$ ou $Q \in (X)$). Maintenant comme $A[X]$ est supposé principal, (X) est donc maximal et, par

suite, l'anneau quotient $\frac{A[X]}{(X)}$ est un corps.

Considérons l'épimorphisme canonique $s : A[X] \longrightarrow \frac{A[X]}{(X)}$ et sa restriction $\tilde{s}$ à A. On a $\mathrm{Ker}(\tilde{s}) = A \cap (X) = \{0\}$, donc $\tilde{s}$ est injectif. Soit $P \in A[X]$ de coefficient constant $a = P(0)$. On a $P(X) - a \in (X)$ et donc $s(P) = s(a)$, ce qui justifie que $\tilde{s}$ est surjectif et par suite que $\tilde{s}$ est un isomorphisme d'anneaux entre A et $\frac{A[X]}{(X)}$. Ainsi, A est un corps.

iii) $\Rightarrow$ *i*) Supposons que A soit un corps, prenons M et N deux polynômes de $A[X]$ avec N non nul et cherchons deux polynôme $Q, R \in A[X]$ tels que $M = QN + R$ et $d^\circ R < d^\circ N$.

• Si $d^\circ M < d^\circ N$, alors $Q = 0$ et $R = M$ conviennent.

• $d^\circ M \geq d^\circ N$, posons $n = d^\circ N$ et $m = d^\circ M$ et

$$N(X) = a_n X^n + \cdots + a_0 \text{ et } M(X) = b_m X^m + \cdots + b_0$$

Posons $q_1 = (b_m/a_n)X^{m-n}$ et $M_1 = M - q_1 N$. On a $d^\circ M_1 < d^\circ M$. Si $d^\circ M_1 < d^\circ N$ alors on pose $Q = q_1$ et $R = M_1$. Sinon, par le même procédé, il existe un polynôme $q_2 \in A[X]$ tel que le polynôme $M_2 = M_1 - q_2 N$ vérifie $d^\circ M_2 < d^\circ M_1$. Par récurrence, on construit deux suites finies $q_1, \cdots, q_n$ et $M_1, \cdots, M_n$ telles que

$$M_k = M_{k-1} - N q_k,\ d^\circ M_k < d^\circ M_{k-1}$$

pour tout $k = 2, \cdots, n$ et $d^\circ M_n < d^\circ M$. L'entier n existe bien puisque la suite $(d^\circ M_k)_k$ est strictement décroissante. On pose alors $Q = q_1 + \cdots + q_n$ et $R = M_n$.

□

Remarques : a) En particulier, l'anneau $\mathbb{Z}[X]$ n'est pas principal bien que $\mathbb{Z}$ le soit.

b) Si A est un corps, alors la division euclidienne d'un polynôme M par un polynôme N non nul, est unique (i.e. le quotient et le reste). En effet, si l'on peut écrire $M = Q_1 N + R_1$ et $M = Q_2 N + R_2$ avec $d^\circ R_1, d^\circ R_2 < d^\circ N$ alors on a $(R_1 - R_2) = (Q_2 - Q_1)N$ et donc $d^\circ(R_1 - R_2) = d^\circ(Q_1 - Q_2) + d^\circ N$, mais comme $d^\circ(R_1 - R_2) \leq \sup(d^\circ R_1, d^\circ R_2) < N$, on en déduit que la seule possibilité est $d^\circ(R_1 - R_2) = d^\circ(Q_1 - Q_2) = -\infty$ c'est-à-dire $R_1 = R_2$ et $Q_1 = Q_2$.

c) L'algorithme présenté dans la preuve pour prouver que $A[X]$ est euclidien si A est un corps s'appelle la division suivant les puissances décroissantes du polynôme M par le polynôme N.

Applications : Considérons un corps K et un anneau (quelconque) A qui contient K comme sous-anneau. Fixons un élément $a \in A$ et considérons

$$\begin{array}{rccc} \varphi_a : & K[X] & \longrightarrow & A \\ & P(X) & \longmapsto & P(a) \end{array}$$

le morphisme d'évaluation en a. Le noyau $\mathrm{Ker}(\varphi_a)$ (l'ensemble des polynômes annulateurs de a) est un idéal de $K[X]$, il est donc principal, et, par suite, il existe un polynôme $P \in K[X]$ tel que $\mathrm{Ker}(\varphi_a) = (P)$. Si l'on choisit P unitaire (ce qui est possible), alors P est unique pour cette propriété. On appelle le polynôme P, le polynôme minimal de a sur K et on le note $\mathrm{Min}_K(a)$.

L'exemple classique d'application est le cas où $A = \mathcal{M}_n(K)$ est l'algèbre des matrices carrées à coefficients dans K. Etant donnée une matrice $M \in \mathcal{M}_n(K)$, le théorème de Cayley-Hamilton affirme que le polynôme caractéristque $\mathrm{Car}(M)(X) = \det(M - XI)$ est un polynôme annulateur de M. Ce qui précède montre alors que $\mathrm{Car}(M)(X)$ est un multiple de $\mathrm{Min}_K(M)(X)$.

5.1.3 Dérivation

Définition.— *Soit A un anneau commutatif et $A[X]$ son anneau de polynôme en une variable. On appelle dérivation usuelle sur $A[X]$ l'application $' : A[X] \longrightarrow A[X]$ définie par*

$$\left(\sum_{k\geq 0} a_k X^k\right)' = \sum_{k\geq 1} k a_k X^{k-1}$$

Si $P \in A[X]$, le polynôme P' s'appelle le polynôme dérivé de P et si $n \geq 0$, on définit par récurrence le polynôme dérivé d'ordre n de P, noté $P^{(n)}$ par : $P^{(0)} = P$ et pour $n \geq 0$, $P^{(n+1)} = (P^{(n)})'$.

Proposition.— *La dérivation usuelle est une application qui vérifie pour $a \in A$, $P, Q \in A[X]$:*

$$(aP + Q)' = aP' + Q' \text{ et } (P.Q)' = P'Q + PQ'$$

Preuve : Exercice.

□

Remarque : On voit facilement que si $n > d^\circ P$ alors $P^{(n)}(X) = 0$. On fera bien attention de ne pas en déduire pour autant que $P^{(n)}(X) \neq 0$ pour tout $n \leq d^\circ P$. Par exemple, dans $\mathbb{Z}/n\mathbb{Z}$, on a $(X^n)^{(k)} = 0$ pour tout $k \geq 1$. Toutefois, si A est de caractéristique nulle et si

$$P(X) = a_n X^n + \cdots + a_0$$

alors pour tout $k = 0, \cdots, n$, on a

$$P^{(k)}(0) = k! a_k$$

et donc, $P^{(k)}(X) \neq 0$.

Proposition.— (Formule de Leibniz) *Soit A un anneau commutatif et $P, Q \in A[X]$. Pour tout entier $n \geq 0$, on a*

$$(P.Q)^{(n)} = \sum_{k=0}^{n} C_n^k . P^{(k)} Q^{(n-k)}$$

(Attention dans cette expression, C_n^k ne désigne nullement un élément de A)

Preuve : Exercice.

□

Théorème.— (Formule de Taylor) *Soit $n \geq 0$ un entier, A un anneau commutatif et unitaire dans lequel pour tout $k = 1, \cdots, n!$, $k.1 \in U(A)$ (e.g. $A = K$ un corps de caractéristique 0), $P \in A[X]$ un polynôme de degré n et $a \in A$. On a*

$$P(X) = \sum_{k=0}^{n} P^{(k)}(a) \frac{(X-a)^k}{k!}$$

(Ici, $\dfrac{1}{k!}$ désigne l'inverse dans A de l'élément $k!.1$.)

Preuve : Par récurrence sur l'entier n. Pour $n = 0$ la proposition est claire. Supposons l'avoir montrée au rang $n - 1 \geq 0$. Alors au rang n considérons un polynôme P de degré n. Si $\alpha \neq 0$ désigne le terme de plus haut degré de P, on voit que $P^{(n)}(X) = n!.\alpha$. Considérons les polynômes

$$H(X) = P^{(n)}(a) \frac{(X-a)^n}{n!} \text{ et } Q(X) = P(X) - H(X)$$

Comme le terme de degré n de $H(X)$ vaut α, on en déduit que le polynôme Q est de degré $\leq n - 1$. En appliquant l'hypothèse de récurrence, on trouve que

$$\begin{aligned} Q(X) &= \sum_{k=0}^{n-1} Q^{(k)}(a) \frac{(X-a)^k}{k!} \\ &= \sum_{k=0}^{n-1} P^{(k)}(a) \frac{(X-a)^k}{k!} - \sum_{k=0}^{n-1} H^{(k)}(a) \frac{(X-a)^k}{k!} \end{aligned}$$

Maintenant, pour $k = 0, \cdots, n-1$, on a $H^{(k)}(X) = P^{(n)}(a) \dfrac{(X-a)^{n-k}}{(n-k)!}$, on en déduit que $H^{(k)}(a) = 0$, et ainsi,

$$P(X) = \sum_{k=0}^{n-1} P^{(k)}(a) \frac{(X-a)^k}{k!} + P^{(n)}(a) \frac{(X-a)^n}{n!} = \sum_{k=0}^{n} P^{(k)}(a) \frac{(X-a)^k}{k!}$$

□

5.1.4 Composition

Soit A un anneau commutatif, comme $A[X]$ est un sous-anneau de $A[X]$, pour tout polynôme $Q \in A[X]$ on peut considérer le morphisme d'évalution en Q :

$$\begin{array}{rccc} \varphi_Q : & A[X] & \longrightarrow & A[X] \\ & P(X) & \longmapsto & P(Q(X)) \end{array}$$

Définition.— *Avec les notations précédentes, pour $P, Q \in A[X]$ on appelle composée du polynôme Q par le polynôme P, le poynôme $\varphi_Q(P)$. On le note $P \circ Q$.*

Proposition.— *Soit A un anneau commutatif et $P, Q \in A[X]$.*

1/ Si A est intègre alors $d^\circ P \circ Q = d^\circ P.d^\circ Q$.

2/ $(P \circ Q)^{'}(X) = Q^{'}(X).(P^{'} \circ Q)(X)$.

Preuve : Exercice.

□

Exercice : Examiner la valuation d'une composée. Que devient le 1/ de la proposition précédente si A n'est pas intègre?

5.1.5 Irréductibilité

Dans tout ce paragraphe, on suppose donné un anneau A factoriel et l'on note K son corps de fractions. Comme A s'injecte canoniquement dans K, on voit que $A[X]$ peut-être vu comme un sous-anneau de $K[X]$.

Définition.— *Soit $P(x) = a_n X^n + \cdots + a_0 \in A[X]$ un polynôme non nul. On appelle contenu du polynôme P un p.g.c.d. de la famille $\{a_0, \cdots, a_n\}$ et on le note $c(P)$ (il est unique aux inversibles près). On dit que le polynôme P est primitif, s'il est de degré ≥ 1 et si son contenu vaut* 1.

Remarque : Si $P \in A[X]$, on voit que $P = c(P)P_1$ avec $P_1 \in A[X]$ et $c(P_1) = 1$. Par ailleurs, si $P \in K[X]$, on peut écrire

$$P(X) = \frac{a_n}{b_n} X^n + \cdots + \frac{a_0}{b_0}$$

avec $a_0, \cdots, a_n, b_0, \cdots, b_n \in A$, on a donc

$$P(X) = \frac{1}{b_0 \cdots b_n} \left(a_n \prod_{i \neq n} b_i X^n + \cdots + a_0 \prod_{i \neq 0} b_i \right)$$

où le polynôme $P_1(X) = (a_n \prod_{i \neq n} b_i X^n + \cdots + a_0 \prod_{i \neq 0} b_i)$ est un élément de $A[X]$

Proposition.— (Lemme de Gauss) *Soit $P, Q \in A[X]$ deux polynôme non nuls. On a (aux inversible près) $c(PQ) = c(P)c(Q)$.*

Preuve : Supposons pour commencer que $c(P) = c(Q) = 1$. Si $C(PQ) \neq 1$, considérons un élément irréductible $p \in A$ tel que $p | c(PQ)$, ainsi p divise tous les coefficients du polynôme PQ. Considérons alors l'anneau quotient $B = A/pA$, la surjection canonique $s : A \longrightarrow A/pA$ et $\tilde{s} : A[X] \longrightarrow B[X]$ le morphisme des anneaux de polynômes associé au morphisme s.

Puisque p est irrèductible il est premier et donc l'anneau quotient B et donc $B[X]$ est intègre. Comme p divise tous les coefficients de PQ, on a $\tilde{s}(PQ) = 0$ mais comme $\tilde{s}(PQ) = \tilde{s}(P)\tilde{s}(Q) = 0$ et que $B[X]$ est intègre, on en déduit que $\tilde{s}(P) = 0$ ou $\tilde{s}(Q) = 0$, c'est-à-dire que p divise tous les coefficients de P ou de Q et donc $p | c(P)$ ou $p | c(Q)$ ce qui est absurde par hypothèse.

De manière générale, on écrit $P = c(P)P_1$ et $Q = c(Q)Q_1$ où P_1, Q_1 sont des polynômes primitifs de $A[X]$. On a alors $c(PQ) = c(P)c(Q)c(P_1Q_1) = c(P)c(Q)$ d'après ce qui précède.

□

Corollaire.— *a) Soient $P, Q \in A[X]$ tels que $P|Q$ dans $K[X]$ et que $c(P)|c(Q)$ dans A, alors $P|Q$ dans $A[X]$.*

b) Soit $P \in A[X]$ primitif et $Q, R \in K[X]$ tel que $P = QR$ dans $K[X]$. Il existe deux éléments $u, v \in K$ et deux polynômes primitifs $R_1, Q_1 \in A[X]$ tels que $P = Q_1R_1$ et $Q_1 = uQ$ et $R_1 = vR$ (en particulier $uv = 1$).

c) Si $P \in A[X]$ unitaire, $Q \in K[X]$ unitaire et $R \in K[X]$ sont tels que $P = QR$ dans $K[X]$, alors Q et R sont dans $A[X]$.

Preuve : a) Supposons avoir un polynôme $R \in K[X]$ tel que $Q = PR$. Il existe un élément $\alpha \in A$ et un polynôme $R_1 \in A[X]$ tels que $R(X) = \frac{1}{\alpha}R_1(X)$. On a donc $\alpha Q = PR_1$ et par application du lemme de Gauss, on a $\alpha c(Q) = c(P)c(R_1)$ mais comme $c(P)|c(Q)$ dans A, on en déduit que $c(R_1)$ est un multiple dans A de α et, par suite, que $R(X) = \frac{1}{\alpha}R_1(X) \in A[X]$.

b) Soit $\alpha, \beta \in A$ et $Q_0, R_0 \in A[X]$ tels que $\alpha Q = Q_0$ et $\beta R = R_0$. On a donc $\alpha\beta P = Q_0R_0$ et par application du lemme de Gauss, $\alpha\beta = c(Q_0)c(R_0)$. Soit $Q_1, R_1 \in A[X]$ primitifs tels que $Q_0 = c(Q_0)Q_1$ et $R_0 = c(R_0)R_1$. On a

$$\begin{aligned} Q &= \frac{1}{\alpha}Q_0 = \frac{c(Q_0)}{\alpha}Q_1 \\ R &= \frac{1}{\beta}R_0 = \frac{c(R_0)}{\beta}R_1 \end{aligned}$$

on a donc $QR = Q_1R_1$ et $Q_1 = uQ$ et $R_1 = vR$ avec $u = \dfrac{\alpha}{c(Q_0)}$ et $u = \dfrac{\beta}{c(R_0)}$.

c) C'est une application directe du b) en remarquant que puisque P est unitaire, il est primitif.

□

Proposition.— *Les éléments irréductibles de $A[X]$ sont exactement les éléments irréductibles de A et les polynômes irréductibles primitifs.*

Preuve : Soit $P \in A[X]$ irréductible. Si $P \notin A$, alors P est clairement primitif, sinon $c(P)$ n'est pas une unité et donc $P = c(P)P_1$ avec P_1 primitif et donc non inversible.

Si $P \in A$, alors P est clairement irréductible dans A. Réciproquement, si $P \in A$ est irréductible dans A, alors supposons que $P = P_1Q$ avec $P_1, Q \in A[X]$. Comme A est intègre, si P_1 et ou Q n'est pas constant, alors $d^\circ P_1Q > 0$ ce qui est absurde. Donc $P_1, Q \in A$ et comme P est irréductible, un des deux polynôme P_1 ou Q est une unité.

□

Théorème.— *Soit $P \in A[X]$ un polynôme.*

a) Si P est irréductible dans $A[X]$ et $d^\circ P \geq 1$, alors il est irréductible dans $K[X]$.

b) Si P est irréductible dans $K[X]$ alors P est irréductible dans $A[X]$ si et seulement si P est primitif.

Preuve : Exercice.

□

Théorème.— *Soit A un anneau. Si A est factoriel, alors $A[X]$ l'est aussi.*

Preuve : A étant factoriel il est intègre et par suite $A[X]$ l'est aussi.

Puisque K est un corps, $K[X]$ est euclidien et donc factoriel. Ainsi, si $P \in A[X]$ est non nul, il existe des polynômes $Q_1, \cdots, Q_n \in K[X]$ irréductibles tels que

$$P(X) = Q_1(X) \cdots Q_n(X)$$

Comme précédement, on trouve qu'il existe des polynômes primitifs $\widetilde{Q_1}, \cdots, \widetilde{Q_n} \in A[X]$ associés respectivement aux polynômes $Q_1, \cdots, Q_n$ et un élément $u \in A$ tels que

$$P(X) = u\widetilde{Q_1}(X) \cdots \widetilde{Q_n}(X)$$

En appliquant le lemme de Gauss, on voit que $u = c(P) \in A$. Par ailleurs, pour $i = 1, \cdots, n$ le polynôme $\widetilde{Q_i}(X)$ étant associé à $Q_i(X)$ est irréductible dans $K[X]$, comme il est dans $A[X]$ et primitif, il est irréductible dans $A[X]$. Enfin, A étant factoriel, u est lui aussi un produit d'élément irréductibles dans A donc dans $A[X]$. Ceci montre que tout polynôme de $A[X]$ est un produit d'éléments irréductibles de $A[X]$.

Reste à montrer l'unicité de la décomposition. Supposons avoir $\mathcal{C}_1$ une classe de représentants des éléments irréductibles de A et $\mathcal{C}_2$ une classe de représentants des éléments irréductibles de $A[X]$ qui ne sont pas dans A (i.e. les éléments de $\mathcal{C}_2$ qui ont un degré ≥ 1).Supposons avoir

$$\prod_{p \in \mathcal{C}_1} p^{\alpha_p} \prod_{Q \in \mathcal{C}_2} Q^{\beta_Q} = \prod_{p \in \mathcal{C}_1} p^{\alpha'_p} \prod_{Q \in \mathcal{C}_2} Q^{\beta'_Q}$$

où $\{\alpha_p\}_{\in\mathcal{C}_1}$, $\{\alpha_p^{'}\}_{\in\mathcal{C}_1}$, $\{\beta_Q\}_{\in\mathcal{C}_2}$ et $\{\beta_Q^{'}\}_{\in\mathcal{C}_2}$ sont des familles d'entiers positifs presque partout nulles. Les polynômes $Q \in \mathcal{C}_2$ sont irréductibles dans $K[X]$ et visiblement non associés deux à deux. Ainsi, dans $K[X]$, on a

$$\prod_{Q\in\mathcal{C}_2} Q^{\beta_Q} = u \prod_{Q\in\mathcal{C}_2} Q^{\beta_Q^{'}}$$

où $u = \prod_{p\in\mathcal{C}_1} p^{\alpha_p^{'}-\alpha_p} \in K$ est une unité. Comme $K[X]$ est factoriel, on déduit que $\beta_Q = \beta_Q^{'}$ pour tout $Q \in \mathcal{C}_2$. On a donc

$$\prod_{p\in\mathcal{C}_1} p^{\alpha_p} = \prod_{p\in\mathcal{C}_1} p^{\alpha_p^{'}}$$

dans $A[X]$ et donc dans A, mais comme A est supposé factoriel, on a finalement $\alpha_p = \alpha_p^{'}$ pour tout $p \in \mathcal{C}_1$.

□

Théorème.— (Critère d'Eisenstein) *Soit A un anneau factoriel, K son corps de fractions et $P(X) = a_nX^n + \cdots + a_0$ un polynôme de $A[X]$ de degré $n \geq 1$. S'il existe un élément irréductible $\pi \in A$ tel que $\pi \not| a_n$, $\pi | a_i$ pour tout $i = 0, \cdots, n-1$ et $\pi^2 \not| a_0$ alors P est irréductible dans $K[X]$.*

Preuve : Supposons P primitif et supposons qu'il existe $Q, R \in A[X]$ avec

$$Q(X) = b_mX^m + \cdots + b_0 \text{ et } R(X) = c_lX^l + \cdots + c_0$$

avec $m > 0$ et $l > 0$. On a $a_0 = b_0c_0$ mais comme $\pi | a_0$ et que $\pi^2 \not| a_0$, on en déduit que π divise un des b_0, c_0 mais pas l'autre. Disons par exemple $\pi | b_0$ et $\pi \not| c_0$. Comme $a_n = b_mc_l$ et que $\pi \not| a_n$ on en déduit que $\pi \not| b_m$.

On a, $a_1 = b_1c_0 + b_0c_1$ et comme π divise a_1 et b_0 il divise b_1c_0 mais comme il ne divise pas c_0, on a $\pi | b_1$. Par récurrence, on montre que pour tout $i = 0, \cdots, m$, $\pi | b_i$ puisque

$$a_i = b_ic_0 + b_{i-1}c_1 + \cdots + b_0c_i$$

et que $\pi \not| c_0$. Ainsi $\pi | b_m$ ce qui est absurde d'après ce qui précède. Donc P est irréductible dans $A[X]$ et donc dans $K[X]$.

Si P n'est plus supposé primitif, alors on peut écrire $P = c(P)P_1$ avec $P_1 \in A[X]$ primitif. Vu que $\pi \not| a_n$, on en déduit que $\pi \not| c(P)$ et, par suite, que le polynôme P_1 vérifie les hypothèses du théorème et est donc, d'après ce qui précéde, irrèductible dans $K[X]$. Ceci assure finalement que P est aussi irrèductible dans $K[X]$, puisque $c(P)$ est une unité de $K[X]$.

□

5.1.6 Racines

Définition.— *Soit A un anneau commutatif et $P \in A[X]$ un polynôme non nul. Un élément $a \in A$ est dit racine de P si $P(a) = 0$.*

Théorème.— *Soit A un anneau commutatif unitaire et $P \in A[X]$ un polynôme de degré $d > 0$. Si $a \in A$ est racine de P, il existe un polynôme $Q \in A[X]$ de degré $d-1$ tel que $P(X) = (X-a)Q(X)$.*

Preuve : On montre facilement, par récurrence, que pour tout $n \geq 1$ entier et tout $a \in A$, on a

$$X^n - a^n = (X-a)(X^{n-1} + aX^{n-2} + \cdots + a^{n-2}X + a^{n-1})$$

Il s'ensuit que si $P(X) = \sum_{n=0}^{d} a_nX^n$ on a

$$\begin{aligned} P(X) - P(a) &= \sum_{n=0}^{d} a_nX^n - \sum_{n=0}^{d} a_na^n = \sum_{n=0}^{d} a_n(X^n - a^n) \\ &= \sum_{n=1}^{d} a_n(X-a)\sum_{k=0}^{n-1} a^{n-1-k}X^k = (X-a)Q(X) \end{aligned}$$

avec $Q(X) = \sum_{n=1}^{d} a_n \sum_{k=0}^{n-1} a^{n-1-k}X^k$ qui est visiblement de degré $d-1$, puisque son terme de degré $d-1$ vaut $a_d \neq 0$.

□

Corollaire.— *Soit A un anneau commutatif unitaire intègre. Un polynôme $P \in A[X]$ de degré $d > 0$ possède au plus d racines dans A. En particulier, un polynôme de $A[X]$ qui possède une infinité de racines est nécessairement nul.*

Preuve : Supposons que P possède $d+1$ racines distinctes $a_1, \cdots, a_{d+1}$. Par application du théorème précédent, il existe $P_1 \in A[X]$ de degré $d-1$ tel que $P(X) = (X-a_1)P_1(X)$. En évaluant cette égalité en a_2, on trouve que $0 = P(a_2) = (a_1 - a_2)P_1(a_2)$. Comme $a_1 - a_2 \neq 0$ et que A est intègre, on en déduit que $P_1(a_2) = 0$. Ainsi, il existe un polynôme $P_2 \in A[X]$, de degré $d-2$ tel que $P_1(X) = (X-a_2)P_2(X)$. Et ainsi de suite, par récurrence, on construit une suite finie de polynômes $P_1, \cdots, P_{d+1}$ tel que $P_i(X) = (X - a_{i+1})P_{i+1}(X)$ et $d^\circ P_i = d - i$ pour tout $i = 0, \cdots, d$. Le polynôme P_{d+1} est donc de degré -1 ce qui est absurde.

Corollaire.— *Soit A un anneau commutatif unitaire intègre et $P \in A[X]$ un polynôme de degré d. Si $a_1, \cdots, a_n \in A$ sont des racines distinctes deux à deux de P, il existe un polynôme $Q \in A[X]$ de degré $d-n$ tel que $P(X) = (X-a_1)\cdots(X-a_n)Q(X)$.*

Preuve : Exercice.

□

Remarque : Si A n'est pas intègre, ces résultats sont faux. Par exemple, dans $\mathbb{Z}/6\mathbb{Z}[X]$ le polynôme $P(X) = X^2 - \overline{5}X$ (qui est de degré 2) possède 4 racines : $\overline{0}, \overline{2}, \overline{3}, \overline{5}$.

On voit immédiatement grace au théorème qu'un polynôme $P \in A[X]$ possède une racine $a \in A$ si et seulement si le polynôme $(X-a)$ divise $P(X)$ dans $A[X]$.

Définition.— *Soit A un anneau commutatif unitaire et $a \in A$ une racine d'un polynôme $P \in A[X]$. On appelle multiplicité de a comme racine de P, le plus grand entier $n \geq 1$ tel que $(X-a)^n | P(X)$. Si la multiplicité n de a comme racine de P est 1, on dit que a est une racine simple, sinon on dit qu'elle est multiple d'ordre n.*

Proposition.— *Soit A un anneau commutatif unitaire intègre, $P \in A[X]$ et $a \in A$ une racine de P. Les propositions suivantes sont équivalentes :*

i) a est racine multiple de P,

ii) $P(a) = P'(a) = 0$.

Si, de plus, on suppose que A est caractéristique nulle, alors les propositions suivantes sont équivalentes :

i) a est racine d'ordre n de P,

ii) $P(a) = P'(a) = \cdots = P^{(n-1)}(a) = 0$ et $P^{(n)}(a) \neq 0$.

Preuve : $i) \Longrightarrow ii)$ On a $P(X) = (X-a)^2 Q(X)$ avec $Q(X) \in A[X]$. On a donc $P'(X) = 2(X-a)Q(X) + (X-a)^2 Q(X)$ et donc $P'(a) = 2(a-a)Q(a) + (a-a)^2 Q'(a) = 0$.

$ii) \Longrightarrow i)$ Comme $P(a) = 0$, on a $P(X) = (X-a)Q_0(X)$ avec $Q_0(X) \in A[X]$. On a $P'(X) = Q_0(X) + (X-a)Q_0'(X)$ et donc $0 = P'(a) = Q_0(a)$. Ainsi il existe $Q \in A[X]$ tel que $Q_0(X) = (X-a)Q(X)$ et ainsi $P(X) = (X-a)^2 Q(X)$.

Supposons maintenant $car(A) = 0$.

$i) \Longrightarrow ii)$ Supposons que $P(X) = (X-a)^n Q(X)$ avec $Q \in A[X]$ tel que $Q(a) \neq 0$. En appliquant la formule de Leibniz pour $k = 0, \cdots, n-1$, on a

$$P^{(k)}(X) = \sum_{i=0}^{k} C_k^i \left((X-a)^n\right)^{(i)} Q^{(k-i)}(X)$$

Or, pour $i = 0, \cdots, n-1$, on a $\left((X-a)^n\right)^{(i)} = \dfrac{n!}{(n-i)!}(X-a)^{n-i}$ et donc, puisque $i < n-1$, on a $\left((X-a)^n\right)^{(i)}(a) = 0$. Ainsi $P^{(k)}(a) = 0$. Pour $k = n$, on a

$$P^{(n)}(a) = \sum_{i=0}^{n} C_n^i \frac{n!}{(n-i)!}(X-a)^{n-i}(a)Q^{(k-i)}(a) = n!Q(a)$$

Comme $car(A) = 0$ et que $Q(a) \neq 0$, on a $P^{(n)}(a) = n!Q(a) \neq 0$.

$ii) \Longrightarrow i)$ On considère le corps des fractions $K = Frac(A)$ et on regarde P comme élément de $K[X]$. En appliquant

la formule de Taylor, on trouve

$$P(X) = \sum_{k=0}^{d^\circ P} P^{(k)}(a)\frac{(X-a)^k}{k!} = \sum_{k=n}^{d^\circ P} P^{(k)}(a)\frac{(X-a)^k}{k!}$$

On a donc

$$P(X) = (X-a)^n Q(X) \text{ avec } Q(X) = \sum_{k=n}^{d^\circ P} P^{(k)}(a)\frac{(X-a)^{k-n}}{k!}$$

On voit alors que $Q(a) = P^{(n)}(a)/n! \neq 0$ et donc que a est d'ordre n dans $K[X]$. On en déduit (exercice) que a est aussi d'ordre n dans $A[X]$.

Remarque : La deuxième équivalence est fausse en caractéristique $\neq 0$. Par exemple dans $\mathbb{Z}/p\mathbb{Z}[X]$ (p premier) le polynôme $P(X) = X^p$ possède $\overline{0}$ comme racine d'ordre p, mais pour tout entier $n \in \mathbb{N}$, $P^{(n)}(\overline{0}) = \overline{0}$.

Toutefois, on voit bien dans la preuve que si l'on retire l'hypothèse sur la caractéristique, il reste quand même le résultat suivant : si a est racine d'ordre n de P alors $P(a) = P'(a) = \cdots = P^{(n-1)}(a) = 0$.

5.1.7 Fonctions polynômiales

Soit A un anneau, considérons l'ensemble

$$\mathcal{F}(A,A) = A^A = \{f : A \longrightarrow A\}$$

l'ensemble des applications de A dans lui-même. On peut munir A d'une structure d'anneaux (exercice) en considérant les deux lois de compositions internes $+, .$, définies, pour $f, g \in \mathcal{F}(A,A)$, par

$$\begin{array}{lcl} \forall x \in A,\ (f+g)(x) & = & f(x)+g(x) \\ \forall x \in A,\ (f.g)(x) & = & f(x).g(x) \end{array}$$

Si A est commutatif (resp. unitaire) alors $\mathcal{F}(A,A)$ l'est aussi. Si A désigne un anneau commutatif, on considère l'application

$$\varphi : A[X] \longrightarrow \mathcal{F}(A,A)$$

qui à un polynôme $P \in A[X]$ associe sa "fonction polynomiale" associée $f : A \longrightarrow$ définie pour $x \in A$ par $f(x) = P(x)$. L'application φ est un morphisme d'anneau (exercice).

Définition.— *On appelle anneau des fonctions polynomiales sur A, le sous-anneau* $\mathrm{Im}(\varphi)$. *On le note* $\mathrm{Pol}(A)$.

L'étude algébrique de l'anneau des fonctions polynomiales sur A peut s'avérer délicate si l'anneau A est "exotique". Toutefois, dans la grande majorité des cas, les choses se passent bien :

Théorème.— *Soit A un anneau commutatif intègre infini. Les anneaux $A[X]$ et* $\mathrm{Pol}(A)$ *sont isomorphes.*

Preuve : Il suffit de montrer que φ est injectif. Soit $P \in \mathrm{Ker}(\varphi)$. On a donc pour tout $x \in A$, $P(x) = 0$. Le polynôme P admet donc une infinité de racine, il est par conséquent nul.

□

Proposition.— *Soit A un anneau commutatif intègre fini (disons, par exemple, $A = \{a_1, \cdots, a_n\}$) et soit $\Omega(X) = (X - a_1)\cdots(X - a_n)$. Les anneaux $A[X]/(\Omega)$ et* $\mathrm{Pol}(A)$ *sont isomorphes.*

Preuve : Soit $P \in \mathrm{Ker}(\varphi)$. On a donc pour tout $x \in A$, $P(x) = 0$, c'est-à-dire $P(a_i) = 0$ pour tout $i = 1, \cdots, n$. Le théorème de factorisation montre alors que $P(X) = \Omega(X)Q(X)$ avec $Q \in A[X]$. On voit donc que $\mathrm{Ker}(\varphi) = (\Omega)$.

□

5.2 Polynômes en plusieurs variables

5.2.1 Définitions, propriétés

On considère un entier $n \geq 1$ et un anneau commutatif unitaire A, on appelle polynôme en n variables à coefficients dans A toute application $P : \mathbb{N}^n \longrightarrow A$ presque partout nulle (i.e. P est nulle sauf sur un sous-ensemble fini de $\mathbb{N}^n$).

Etant donné $(\alpha_1,\cdots,\alpha_n)\in\mathbb{N}^n$ et $a\in A$, on note $aX_1^{\alpha_1}\cdots X_n^{\alpha_n}$ le polynôme $P:\mathbb{N}^n\longrightarrow A$ qui à $(\alpha_1,\cdots,\alpha_n)$ associe a et associe 0 partout ailleurs. Un tel polynôme est appelé un monôme (à plusieurs variables).

On note $A[X_1,\cdots,X_n]$ l'ensemble des polynômes en n variables à coefficients dans A. Les éléments $X_1,\cdots,X_n$ sont appellées les variables de l'anneau de polynômes. Etant donné un $P\in A[X_1,\cdots,X_n]$, on écrit formellement

$$P(X_1,\cdots,X_n)=\sum_{(\alpha_1,\cdots,\alpha_n)\in\mathbb{N}^n}\lambda_{\alpha_1,\cdots,\alpha_n}X_1^{\alpha_1}\cdots X_n^{\alpha_n}$$

où $\lambda_{\alpha_1,\cdots,\alpha_n}\in A$ est la valeur de la fonction P en $(\alpha_1,\cdots,\alpha_n)\in\mathbb{N}^n$.

Sur $A[X_1,\cdots,X_n]$ on définit deux lois de composition internes, + et ., en posant pour les polynômes

$$\left\{\begin{array}{l}P(X_1,\cdots,X_n)=\displaystyle\sum_{(\alpha_1,\cdots,\alpha_n)\in\mathbb{N}^n}\lambda_{\alpha_1,\cdots,\alpha_n}X_1^{\alpha_1}\cdots X_n^{\alpha_n}\\ Q(X_1,\cdots,X_n)=\displaystyle\sum_{(\alpha_1,\cdots,\alpha_n)\in\mathbb{N}^n}\mu_{\alpha_1,\cdots,\alpha_n}X_1^{\alpha_1}\cdots X_n^{\alpha_n}\end{array}\right.\in A[X_1,\cdots,X_n]$$

$$\begin{array}{rcl}(P+Q)(X_1,\cdots,X_n) & = & \displaystyle\sum_{(\alpha_1,\cdots,\alpha_n)\in\mathbb{N}^n}(\lambda_{\alpha_1,\cdots,\alpha_n}+\mu_{\alpha_1,\cdots,\alpha_n})X_1^{\alpha_1}\cdots X_n^{\alpha_n}\\ (P.Q)(X_1,\cdots,X_n) & = & \displaystyle\sum_{(\alpha_1,\cdots,\alpha_n)\in\mathbb{N}^n}\nu_{\alpha_1,\cdots,\alpha_n}X_1^{\alpha_1}\cdots X_n^{\alpha_n}\end{array}$$

$$\left(\text{où }\nu_{\alpha_1,\cdots,\alpha_n}=\sum_{(i_1,\cdots,i_n),(j_1,\cdots,j_n)\in\mathbb{N}^n/\ \forall k=1,\cdots,n\ i_k+j_k=\alpha_k}\lambda_{i_1,\cdots,i_n}\mu_{j_1,\cdots,j_n}\right)$$

(on vérifie (exercice) qu'il s'agit bien de lois de composition internes). On voit que si $n=1$, alors $(A[X_1],+,.)$ est l'anneau de polynômes en une variable à coefficients dans A.

Proposition.— *Avec les notations précédentes, le triplet $(A[X_1,\cdots,X_n],+,.)$ est un anneau commutatif unitaire et l'application $A\longrightarrow A[X_1,\cdots,X_n]$ qui à $a\in A$ associe $aX_1^0\cdots X_n^0$ est un monomorphisme d'anneaux (on peut donc voir A comme un sous-anneau de $A[X_1,\cdots,X_n]$).*

Preuve : Exercice.

□

Remarque : On voit de même que pour tout couple $k\leq n$ d'entiers non nuls, on a un monomorphisme canonique $A[X_1,\cdots,X_k]\longrightarrow A[X_1,\cdots,X_n]$.

Théorème.— *Soient $n\geq 2$ un entier et A un anneau commutatif. Les anneaux $A[X_1,\cdots,X_n]$ et $A[X_1,\cdots,X_{n-1}][X_n]$ sont isomorphes.*

Preuve : Considérons les monomorphismes canoniques

$$\begin{array}{rccc}\varphi: & A[X_n] & \longrightarrow & A[X_1,\cdots X_n]\\ \psi: & A[X_1,\cdots,X_{n-1}] & \longrightarrow & A[X_1,\cdots X_n]\end{array}$$

et l'application $\Theta:A[X_1,\cdots,X_{n-1}][X_n]\longrightarrow A[X_1,\cdots,X_n]$ définie par

$$\Theta\left(\sum_{i=0}^{d}Q_i(X_1,\cdots,X_{n-1})X_n^d\right)=\sum_{i=1}^{d}\psi(Q_i(X_1,\cdots,X_{n-1}))\varphi(X_n^d)$$

L'application Θ est visiblement un monomorphisme d'anneaux. Le fait que Θ soit surjective est laissé en exercice.

□

Corollaire.— *Soient $n\geq 1$ un entier et A un anneau commutatif et unitaire.*

a) Si A est intègre, $A[X_1,\cdots,X_n]$ l'est aussi et $U(A[X_1,\cdots,X_n]=U(A)$.

b) Si A est factoriel, $A[X_1,\cdots,X_n]$ l'est aussi.

c) Si A est intègre alors X_i est premier dans $A[X_1,\cdots,X_n]$, pour tout $i=1,\cdots,n$.

Preuve : a) et b) sont conséquences immédiates de ce qui précède. Pour le c), constatons que si B est un anneaux intègre, alors X est premier dans $B[X]$. En effet, si $X|P(X)Q(X)$, alors $P(0)Q(0) = 0$ et donc, par intégrité, on a $P(0) = 0$ (et alors $X|P(X)$) ou $Q(0) = 0$ (et alors $X|Q(X)$). On applique alors ce résultat pour $X = X_i$ et $B = A[X_1, \cdots, X_{i-1}, X_{i+1}, \cdots, X_n]$.

□

Théorème.— *Soient $n \geq 1$ un entier et $\varphi : A \longrightarrow B$ un morphisme d'anneaux commutatifs unitaires. Soit $f : \{X_1, \cdots, X_n\} \longrightarrow B$ une application quelconque. Il existe un unique morphisme d'anneau $\tilde{f} : A[X_1, \cdots, X_n] \longrightarrow B$ tel que $\tilde{f}(a) = \varphi(a)$ pour tout $a \in A$ (on regarde A comme sous-anneau de $A[X_1, \cdots, X_n]$) et tel que $\tilde{f}(X_i) = f(X_i)$ pour tout $i = 1, \cdots, n$.*

Preuve : Existence : L'application $\tilde{f} : A[X_1, \cdots, X_n] \longrightarrow B$ définie par

$$\tilde{f}\left(\sum_{(\alpha_1,\cdots,\alpha_n)} \lambda_{\alpha_1,\cdots,\alpha_n} X_1^{\alpha_1} \cdots X_n^{\alpha_n}\right) = \sum_{(\alpha_1,\cdots,\alpha_n)} \varphi(\lambda_{\alpha_1,\cdots,\alpha_n}) f(X_1)^{\alpha_1} \cdots f(X_n)^{\alpha_n}$$

fait l'affaire.

Unicité : Soit $\tilde{f}'$ un autre morphisme ayant les mêmes propriétés. On a alors

$$\begin{aligned}
\tilde{f}\left(\sum_{(\alpha_1,\cdots,\alpha_n)} \lambda_{\alpha_1,\cdots,\alpha_n} X_1^{\alpha_1} \cdots X_n^{\alpha_n}\right) &= \sum_{(\alpha_1,\cdots,\alpha_n)} \tilde{f}(\lambda_{\alpha_1,\cdots,\alpha_n}) \tilde{f}(X_1)^{\alpha_1} \cdots \tilde{f}(X_n)^{\alpha_n} \\
&= \sum_{(\alpha_1,\cdots,\alpha_n)} \varphi(\lambda_{\alpha_1,\cdots,\alpha_n}) f(X_1)^{\alpha_1} \cdots f(X_n)^{\alpha_n} \\
&= \sum_{(\alpha_1,\cdots,\alpha_n)} \tilde{f}'(\lambda_{\alpha_1,\cdots,\alpha_n}) \tilde{f}'(X_1)^{\alpha_1} \cdots \tilde{f}'(X_n)^{\alpha_n} \\
&= \tilde{f}'\left(\sum_{(\alpha_1,\cdots,\alpha_n)} \lambda_{\alpha_1,\cdots,\alpha_n} X_1^{\alpha_1} \cdots X_n^{\alpha_n}\right)
\end{aligned}$$

□

Remarque : Soit B un anneau commutatif unitaire et A un sous-anneau unitaire de B. Considérons un entier $n \geq 1$ et $\alpha_1, \cdots, \alpha_n \in A$. D'après le théorème précédent, il existe un unique morphisme d'anneaux $f : A[X_1, \cdots, X_n]$ tels que $f(a) = a$ pour tout $a \in A$ et $f(X_i) = \alpha_i$ pour tout $i = 1, \cdots, n$. On note $A[\alpha_1, \cdots, \alpha_n]$ le sous-anneau de B égal à $\mathrm{Im}(f)$. On voit alors que

$$A[\alpha_1, \cdots, \alpha_n] = \{P(\alpha_1, \cdots, \alpha_n) / \ P \in A[X_1, \cdots, X_n]\}$$

c'est-à-dire que $A[\alpha_1, \cdots, \alpha_n]$ est l'ensemble des évaluations du n-uplet $(\alpha_1, \cdots, \alpha_n)$ en les polynômes de $A[X_1, \cdots, X_n]$. On constate, par ailleurs, que $A[\alpha_1, \cdots, \alpha_n]$ est le plus petit sous-anneaux de B qui contienne A et les α_i. On l'appelle le "sous-anneau de B engendré par les α_i sur A".

En jouant sur la position des variables, on voit donc que, étant donné un polynôme $P(X_1, \cdots, X_n)$ ($n \geq 2$) et un indice $i \in 1, \cdots, n$, on peut écrire

$$P(X_1, \cdots, X_n) = P_i(X_i) \text{ avec } P_i \in A[X_1, \cdots, X_{i-1}, X_{i+1}, \cdots, X_n][X_i]$$

On appelle alors degré (resp. la valuation) relatif à la variable X_i du polynôme P, le degré (resp. la valuation) du polynôme P_i et on le note $d^\circ_{X_i} P$ (resp $v_{X_i}(P)$).

On peut aussi définir le degré (global) du polynôme

$$P(X_1, \cdots, X_n) = \sum_{(\alpha_1,\cdots,\alpha_n) \in \mathbb{N}^n} \lambda_{\alpha_1,\cdots,\alpha_n} X_1^{\alpha_1} \cdots X_n^{\alpha_n}$$

en posant

$$d^\circ P = \sup_{(\alpha_1,\cdots,\alpha_n) \in \mathbb{N}^n} \{\alpha_1 + \cdots + \alpha_n / \ \lambda_{\alpha_1,\cdots,\alpha_n} \neq 0\}$$

si $P \neq 0$ et $d^\circ P = -\infty$ si $P = 0$. De même, on définit sa valuation, en posant

$$v(P) = \inf_{(\alpha_1,\cdots,\alpha_n) \in \mathbb{N}^n} \{\alpha_1 + \cdots + \alpha_n / \ \lambda_{\alpha_1,\cdots,\alpha_n} \neq 0\}$$

si $P \neq 0$ et $v(P) = +\infty$ si $P = 0$. On a alors :

Théorème.— *Soient $n \geq 1$ un entier et A un anneau. Si $P, Q \in A[X_1, \cdots, X_n]$, on a :*

a) $d^\circ PQ \leq d^\circ P + d^\circ Q$ (et il y a égalité si A est intègre).

b) $d^\circ(P+Q) \leq \sup(d^\circ P, d^\circ Q)$ (et il y a égalité si $d^\circ P \neq d^\circ Q$).

c) $v(PQ) \geq v(P) + v(Q)$ (et il y a égalité si A est intègre).

d) $v(P+Q) \leq \inf(v(P), v(Q))$ (et il y a égalité si $v(P) \neq v(Q)$).

Preuve : Exercice.

□

Définition.— *Un polynôme $P \in A[X_1, \cdots, X_n]$ est dit homogène, si $d^\circ P = v(P)$.*

Remarque : Un polynôme est donc homogène si et seulement si tous ses monômes non nuls sont de même degré. On constate alors (exercice) que si P est homogène, alors pour tout $\lambda \in A$, et tout $a_1, \cdots, a_n \in A$, on a $P(\lambda a_1, \cdots, \lambda a_n) = \lambda^d P(a_1, \cdots, a_n)$ avec $d = d^\circ P$. Il est à noter que cette propriété ne caractérise pas les polynômes homogènes (exercice).

5.2.2 Polynômes symétriques

On considère un anneau commutatif et unitaire A et un entier $n \geq 1$. On note S_n le groupe symétrique de degré n. Pour tout $P(X_1, \cdots, X_n) \in A[X_1, \cdots, X_n]$ et tout $\sigma \in S_n$, on pose

$$P^\sigma(X_1, \cdots, X_n) = P(X_{\sigma(1)}, \cdots, X_{\sigma(n)})$$

Par exemple, si $P(X, Y, Z) = X + XYZ^2 \in A[X, Y, Z]$ et si $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$, on a $P^\sigma(X, Y, Z) = Y + X^2YZ$.

Lemme.— *Avec les notations précédentes, pour tout $P, Q \in A[X_1, \cdots, X_n]$ et tout $\sigma, \mu \in S_n$, on a : a) $(P+Q)^\sigma = P^\sigma + Q^\sigma$, $(PQ)^\sigma = P^\sigma Q^\sigma$.*

b) $(P^\sigma)^\mu = P^{\mu \circ \sigma}$.

(le groupe S_n agît sur l'anneau $A[X_1, \cdots, X_n]$.)

Preuve : Exercice.

□

Définition.— *On appelle polynôme symétrique de $A[X_1, \cdots, X_n]$ tout polynôme P tel que $P^\sigma = P$ pour tout $\sigma \in S_n$. On note $\mathrm{Sym}_n(A)$ l'ensemble des polynômes symétriques de $A[X_1, \cdots, X_n]$*

Exemple : Le polynôme $X^2 + XY + Y^2$ est symétrique dans $\mathbb{Z}[X, Y]$, mais $X - Y$ ne l'est pas.

Proposition.— *L'ensemble $\mathrm{Sym}_n(A)$ est un sous-anneau de $A[X_1, \cdots, X_n]$.*

Preuve : Exercice

□

Définition.— *Soit A un anneau commutatif et unitaire et $n \geq 1$ un entier. Pour tout $k = 1, \cdots, n$, on appelle k-ième polynôme symétrique élémentaire, le polynôme*

$$\sigma_k^n(X_1, \cdots, X_n) = \sum_{1 < i_1 < \cdots < i_k < n} X_{i_1} \cdots X_{i_k} \in A[X_1, \cdots, X_n]$$

Par exemple, pour $n = 4$, on a

$$\begin{aligned}
\sigma_1^4(X_1, X_2, X_3, X_4) &= X_1 + X_2 + X_3 + X_4 \\
\sigma_2^4(X_1, X_2, X_3, X_4) &= X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4 \\
\sigma_3^4(X_1, X_2, X_3, X_4) &= X_1X_2X_3 + X_1X_2X_4 + X_1X_3X_4 + X_2X_3X_4 \\
\sigma_4^4(X_1, X_2, X_3, X_4) &= X_1X_2X_3X_4
\end{aligned}$$

On vérifie aisément que $\sigma_k^n(X_1, \cdots, X_n) \in \mathrm{Sym}_n(A)$ pour tout $k = 1, \cdots, n$.

Lemme.— *Soit $n \geq 2$ un entier. Pour tout $k = 2, \cdots, n$, on a*

$$\sigma_k^{n+1}(X_1, \cdots, X_{n+1}) = \sigma_k^n(X_1, \cdots, X_n) + X_{n+1}\sigma_{k-1}^n(X_1, \cdots, X_n)$$

En particulier, on a $\sigma_k^{n+1}(X_1, \cdots, X_n, 0) = \sigma_k^n(X_1, \cdots, X_n)$ pour tout $k = 1, \cdots, n$.

Preuve : Exercice

□

Théorème.— *Soit A un anneau commutatif intègre unitaire et*

$$P(X) = X^n + a_1X^{n-1} + \cdots + a_n \in A[X]$$

un polynôme unitaire de degré $n \geq 1$ possédant n racines $\alpha_1, \cdots, \alpha_n$ (éventuellement multiples) dans A. Pour tout $k = 1, \cdots, n$, on a

$$a_k = (-1)^k\sigma_k^n(\alpha_1, \cdots, \alpha_n)$$

Preuve : Montrons la propriété par récurrence sur l'entier n. Pour $n = 1, 2$ la propriété semble claire. Supposons la vraie pour $n \geq 2$ et donnons nous un polynôme $P(X) = X^{n+1} + a_1X^n + \cdots + a_{n+1} \in A[X]$ unitaire de degré $n+1$ possédant $n+1$ racines $\alpha_1, \cdots, \alpha_{n+1}$. Puisque A est commutatif et intègre, on a

$$P(X) = (X - \alpha_1)\cdots(X - \alpha_{n+1})$$

Considérons le polynôme

$$Q(X) = (X - \alpha_1)\cdots(X - \alpha_n) = X^n + b_1X^{n-1} + \cdots + b_n$$

Par hypothèse de récurrence, on pour tout $k = 1, \cdots, n$, on a

$$b_k = (-1)^k\sigma_k^n(\alpha_1, \cdots, \alpha_n)$$

Maintenant, en développant, on trouve

$$P(X) = X^{n+1} + (b_1 - \alpha_{n+1})X^n + (b_2 - \alpha_{n+1}b_1) + \cdots + (b_n - \alpha_{n+1}b_{n-1})X - \alpha_{n+1}b_n$$

On en déduit donc que

$$a_{n+1} = -\alpha_{n+1}b_n = -(-1)^n\alpha_{n+1}\sigma_n^n(\alpha_1, \cdots, \alpha_n) = (-1)^{n+1}\sigma_{n+1}^{n+1}(\alpha_1, \cdots, \alpha_{n+1})$$

et

$$a_1 = b_1 - \alpha_{n+1} = (-1)^1\sigma_1^n(\alpha_1, \cdots, \alpha_n) - \alpha_{n+1} = (-1)^1\sigma_1^{n+1}(\alpha_1, \cdots, \alpha_{n+1})$$

Par ailleurs, pour tout $k = 2, \cdots, n$, on a, par hypothèse de récurrence,

$$\begin{array}{rcl} a_k & = & (b_k - \alpha_{n+1}b_{k-1}) = (-1)^k\sigma_n^k(\alpha_1, \cdots, \alpha_n) - (-1)^{k-1}\sigma_n^{k-1}(\alpha_1, \cdots, \alpha_n) \\ & = & (-1)^k(\sigma_n^k(\alpha_1, \cdots, \alpha_n) + \sigma_n^{k-1}(\alpha_1, \cdots, \alpha_n)) \end{array}$$

et que, d'après le lemme, on a

$$\sigma_k^{n+1}(X_1, \cdots, X_{n+1} = \sigma_k^n(X_1, \cdots, X_n) + X_{n+1}\sigma_{k-1}^n(X_1, \cdots, X_n)$$

on en déduit donc que

$$a_k = (-1)^k\sigma_k^{n+1}(\alpha_1, \cdots, \alpha_{n+1})$$

pour tout $k = 2, \cdots, n$.

□

Théorème.— *Soit A un anneau factoriel et $n \geq 1$ un entier. Pour tout $P \in \mathrm{Sym}_n(A)$, il existe un polynôme $f \in A[T_1, \cdots, T_n]$ tel que*

$$P(X_1, \cdots, X_n) = f\left(\sigma_1^n(X_1, \cdots, X_n), \cdots, \sigma_n^n(X_1, \cdots, X_n)\right)$$

(on dit que les polynômes symétriques élémentaires engendre l'anneau des polynômes symétriques.

Preuve : On procède par récurrence sur n:

Pour $n = 1$, les polynômes symétriques de $A[X_1]$ sont tous les polynômes et $\sigma_1^1(X_1) = X_1$. Il suffit donc de prendre $f = P$.

Supposons pour $n \geq 1$ que si $P(X_1, \cdots, X_n) \in \mathrm{Sym}_n(A)$, alors il existe un polynôme $f(T_1, \cdots, T_n) \in A[T_1, \cdots, T_n]$ tel que

$$P(X_1, \cdots, X_n) = f(\sigma_1^n(X_1, \cdots, X_n), \cdots, \sigma_n^n(X_1, \cdots, X_n))$$

Prenons alors $P(X_1, \cdots, X_{n+1}) \in A[X_1, \cdots, X_{n+1}]$, un polynôme symétrique de degré d et montrons par récurrence sur d que P peut s'écrire:

$$P(X_1, \cdots, X_{n+1}) = f_d(\sigma_1^{n+1}(X_1, \cdots, X_{n+1}), \cdots, \sigma_{n+1}^{n+1}(X_1, \cdots, X_{n+1}))$$

avec $f_d(T_1, \cdots, T_{n+1}) \in A[T_1, \cdots, T_{n+1}]$.

Pour $d = 0$, la proposition est trivialement vraie.

Supposons la proposition vraie pour $d \geq 0$. Si $P(X_1, \cdots, X_{n+1})$ désigne un polynôme symétrique de $A[X_1, \cdots, X_{n+1}]$ de degré $d+1$, remarquons qu'alors $P(X_1, \cdots, X_n, 0)$ est un polynôme symétrique de $A[X_1, \cdots, X_n]$. D'après l'hypothèse de récurrence (sur n), il existe $g_1(T_1, \cdots, T_n) \in A[T_1, \cdots, T_n]$ tel que:

$$P(X_1, \cdots, X_n, 0) = g_1(\sigma_1^n(X_1, \cdots, X_n), \cdots, \sigma_n^n(X_1, \cdots, X_n))$$

Le degré du polynôme $g_1(\sigma_1^{n+1}(X_1, \cdots, X_{n+1}), \cdots, \sigma_n^{n+1}(X_1, \cdots, X_{n+1}))$ est inférieur à $d+1$. Maintenant le polynôme $P_1(X_1, \cdots, X_{n+1})$, qui est égal à

$$P(X_1, \cdots, X_{n+1}) - g_1(\sigma_1^{n+1}(X_1, \cdots, X_{n+1}), \cdots, \sigma_n^{n+1}(X_1, \cdots, X_{n+1}))$$

est clairement symétrique de degré inférieur à $d+1$. Comme

$$P_1(X_1, \cdots, X_n, 0) = 0$$

et que P_1 est symétrique, on peut écrire:

$$P_1(X_1, \cdots, X_{n+1}) = X_1 \cdots X_{n+1} P_2(X_1, \cdots, X_{n+1})$$

(ceci car $A[X_1, \cdots X_n]$ est factoriel et que X_i, qui est visiblement irréductible, divise P_1 pour tout $i = 1, \cdots, n+1$).

Le polynôme P_2 est clairement symétrique et de degré inférieur à $d - n$. Par hypothèse de récurrence, il existe $g_2 \in A[T_1, \cdots, T_{n+1}]$ tel que

$$P_2(X_1, \cdots, X_{n+1}) = g_2(\sigma_1^{n+1}(X_1, \cdots, X_{n+1}), \cdots, \sigma_{n+1}^{n+1}(X_1, \cdots, X_{n+1}))$$

On a alors

$$P(X_1, \cdots, X_{n+1}) = g_1(\sigma_1^{n+1}(X_1, \cdots, X_{n+1}), \cdots, \sigma_n^{n+1}(X_1, \cdots, X_{n+1})) + \sigma_{n+1}^{n+1}(X_1, \cdots, X_{n+1}) g_2(\sigma_1^{n+1}(X_1, \cdots, X_{n+1}), \cdots, \sigma_{n+1}^{n+1}(X_1, \cdots, X_{n+1}))$$

ce qui achève la preuve.

□

Il n'est généralement pas facile, étant donné P, de trouver f. Par exemple, pour $n = 2$, considérons le polynôme $P(X_1, X_2) = X_1^3 + X_2^3$ et cherchons f. On part de l'égalité :

$$(X_1 + X_2)^3 = X_1^3 + X_2^3 + 3X_1^2 X_2 + 3X_1 X_2^2$$

On a donc $P = (X_1 + X_2)^3 - 3X_1 X_2 (X_1 + X_2) = (\sigma_1^2)^3 - 3\sigma_1^2 \sigma_2^2$ et donc $f(T_1, T_2) = T_1^3 - 3T_1 T_2$.

Théorème.— *Soit A un anneau commutatif unitaire intègre et $n \geq 1$ un entier. Si $P \in A[T_1, \cdots, T_n]$ est tel que*

$$P(\sigma_1^n(X_1, \cdots, X_n), \cdots, \sigma_n^n(X_1, \cdots, X_n)) = 0$$

alors $P = 0$ (on dit que les polynômes symétriques élémentaires sont algériquement indépendants).

Preuve : Montrons la propriété par récurrence sur n :

Pour $n = 1$, la propriété est claire puisque $\sigma_1^1 = X_1$.

Si pour $n > 1$ la propriété est vraie pour $n-1$, alors au rang n, considérons un polynôme non nul $P(T_1, \cdots, T_n) \in A[T_1, \cdots, T_n]$ de degré minimal tel que:

$$P(\sigma_1^n(X_1, \cdots, X_n), \cdots, \sigma_n^n(X_1, \cdots, X_n)) = 0$$

On regarde maintenant $A[T_1, \cdots, T_n]$ comme l'anneau $A[T_1, \cdots, T_{n-1}][T_n]$ et on note

$$P(T_1, \cdots, T_n) = P_0(T_1, \cdots, T_{n-1}) + \cdots + P_d(T_1, \cdots, T_{n-1})T_n^d$$

Le polynôme P_0 ne peut pas être nul sinon

$$P(T_1, \cdots, T_n) = T_n Q(T_1, \cdots, T_n)$$

avec $Q(T_1, \cdots, T_n) \in A[T_1, \cdots, T_n]$, on aurait donc

$$\sigma_n^n(X_1, \cdots, X_n)Q(\sigma_1^n(X_1, \cdots, X_n), \cdots, \sigma_n^n(X_1, \cdots, X_n)) = 0$$

c'est à dire $Q(\sigma_1^n(X_1, \cdots, X_n), \cdots, \sigma_n^n(X_1, \cdots, X_n)) = 0$, mais alors il vient $d^\circ Q < d^\circ P$, ce qui contredit l'hypothèse de minimalité sur P.

En prenant $X_n = 0$ dans l'équation:

$$P_0(\sigma_1^n(X_1, \cdots, X_n), \cdots, \sigma_{n-1}^n(X_1, \cdots, X_n)) + \cdots + P_d(\sigma_1^n(X_1, \cdots, X_n), \cdots, \sigma_{n-1}^n(X_1, \cdots, X_n))\sigma_n^n(X_1, \cdots, X_n)^d = 0$$

on trouve alors:

$$P_0(\sigma_1^{n-1}(X_1, \cdots, X_{n-1}), \cdots, \sigma_{n-1}^{n-1}(X_1, \cdots, X_{n-1})) = 0$$

Par hypothèse de récurrence on en déduit que $P_0 = 0$ ce qui est absurde.

□

Les deux derniers théorèmes combinés, peuvent se ré-écrire en disant que pour tout $P \in \mathrm{Sym}_n(A)$, il existe un unique polynôme $f \in A[T_1, \cdots, T_n]$ tel que

$$P(X_1, \cdots, X_n) = f(\sigma_1^n, \cdots, \sigma_n^n)$$

De manière équivalente, ces théorèmes signifient

$$\mathrm{Sym}_n(A) = A[\sigma_1^n, \cdots, \sigma_n^n] \simeq A[X_1, \cdots, X_n]$$

Chapitre 6

Arithmétique des entiers

6.1 Présentation axiomatique des entiers naturels

6.1.1 Axiomatique

Dans ce qui suit, E désigne un ensemble et $\leq$ un ordre sur E. On considère les axiomes suivants :

S.0. L'ensemble E est non vide.

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

S.2. Toute partie majorée non vide de E possède un plus grand élément.

S.3. E ne possède pas de plus grand élément.

Premières remarques : Si $(E, \leq)$ vérifie les axiomes S.1. alors $\leq$ est un ordre total sur E. Par ailleurs si $(E, \leq)$ vérifie S.0,2,3. alors E est un ensemble infini. Enfin, si E vérifie S.0,1. alors E possède un plus petit élément.

Dans la suite on considère un ensemble ordonné $(E, \leq)$ vérifiant les axiomes S.1,2,3. On note 0 le plus petit élément de E.

Les fonctions successeur et prédécesseur : Considérons un élément $n \in E$ et $F = \{m \in E / \ m > n\}$. D'après ce qui précède F n'est pas vide (sinon E posséderait un plus grand élément). On appelle successeur de n l'élément noté $s(n)$ égal au plus petit élément de l'ensemble F.

Considérons un élément $n \in E - \{0\}$ et $F = \{m \in E / \ m < n\}$. D'après 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 $p(n)$ égal au plus grand élément de l'ensemble F.

Propriété.— *a) Pour tout $n \in E$ on a $s(n) > n$ et pour tout $m \in E$ on a $m > n \iff m \geq s(n)$.*

b) Pour tout $n \in E - \{0\}$ on a $p(n) < n$ et pour tout $m \in E$ on a $m < n \iff m \leq p(n)$.

c) La fonction s est strictement croissante et la fonction p est strictement décroissante.

d) Pour tout $n \in E - \{0\}$ on a $s \circ p(n) = n$.

Preuve : a,b,c) Exercices.

d) 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.— (appelé principe de récurrence) *Soit A une partie de E. Si A vérifie*

- $0 \in A$.
- $\forall n \in E,\ n \in A \Longrightarrow s(n) \in A$.

alors $A = E$.

Preuve : Raisonnons par l'absurde en supposant que $A \neq E$. On considère alors l'ensemble $F = E - A$ 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.

□

Théorème.— *L'application s est une bijection de E sur E − {0}. Son application réciproque est la fonction p*

Preuve : • Prouvons que s est bien à valeur dans $E - \{0\}$. Supposons qu'il existe $n \in E$ 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 E.

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

□

Théorème.— *Un ensemble non vide ordonné $(E, \leq)$ vérifie les axiomes S.0,1,2,3. si et seulement si l'ensemble E vérifie les axiomes (dits de Peano) suivants :*

P.0. *il existe un élément $0 \in E$ et une application $s : E \to E$.*

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

P.2. *Toute partie A de E vérifiant $0 \in A$ et $s(A) \subset A$ est égale à E.*

Preuve : $S.0, 1, 2, 3. \Longrightarrow P.0, 1, 2.$ est clair, la fonction s à considérer étant la fonction successeur. La réciproque est admise. Un des ingrédients de la preuve consiste dans le fait que l'ordre $\leq$ que l'on recherche sur E se définit de manière non-équivoque par les deux propriétés suivantes : 1/ $\forall x \in E$, $0 \leq x$. 2/ $\forall x, y \in E$, $x \leq y \Longleftrightarrow s(x) \leq s(y)$.

□

Théorème.— *Soient $(E, \leq)$ et $(E', \leq')$ deux ensembles ordonné vérifiant les axiomes S.0,1,2,3. Il existe une unique bijection croissante de E sur E'.*

Preuve : Notons 0 (resp. $0'$) le plus petit élément de E (resp. de E').

• Unicité. Soient f et g deux bijections croissantes de E sur E'. L'application $g^{-1} \circ f$ est donc une bijection croissante de E dans lui-même. Une telle application est nécessairement égale à l'identité (exercice).

• Existence. Admise.

□

En conclusion, tous les ensembles ordonnés vérifiant les axiomes S.0,1,2,3. sont isomorphes en tant qu'ensembles ordonnés, leurs propriétés pour cette structures sont donc les mêmes. Dans la suite on choisira $\mathbb{N}$ un tel ensemble (l'existence d'un tel ensemble est consécutive d'axiomes de la théorie des ensembles). On l'appelera "ensemble des entiers naturels".

6.1.2 Arithmétique sur $\mathbb{N}$

Addition.

Théorème.— *Sur $\mathbb{N}$ il existe une unique loi de composition interne + appelée addition telle que :*

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

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

Preuve : Admise.

□

Proposition.— *Le magma $(\mathbb{N}, +)$ est associatif, commutatif et unitaire. Le seul élément symétrisable de $\mathbb{N}$ est 0.*

Preuve :

□

Théorème.— *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 :

□

Multiplication

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

Théorème.— *Sur* $\mathbb{N}$ *il existe une unique loi de composition interne . appelée multiplication telle que :*

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

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

Preuve : Admise.

□

Proposition.— *Le magma* $(\mathbb{N}, .)$ *est associatif, commutatif et unitaire. La multiplication est distributive sur l'addition.*

Preuve :

□

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 $x, y, z \in \mathbb{N}$. Montrer que si $x \leq y$ alors $x + z \leq y + z$ et que $xz \leq yz$. Que devient cette propriété si l'on remplace $\leq$ par $<$?

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

6.2.1 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.— *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.— *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.— *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

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

Théorème.— *$(\mathbb{Z},+,.)$ 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.— *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.— *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.— *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 $x\leq y\Longleftrightarrow y-x\in\mathbb{N}$ 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 petit (resp. un plus grand) 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.

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

Théorème.— *Soit $a,b\in\mathbb{Z}$ 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.

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

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 $r := r - b$, $q := q + 1$.

Nous savons que dans la hiérarchie des anneaux, les anneaux euclidiens sont les plus élevés. En particulier le fait que $\mathbb{Z}$ soit euclidien implique qu'il est principal et factoriel. Ainsi les théorèmes de Gauss et de Bezout y sont vérifié. Nous allons, dans les parties suivantes retrouver ces faits, mais sans utiliser les théorèmes généraux d'arithmétique des anneaux.

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

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

Proposition.— *Les éléments premiers de l'anneau $\mathbb{Z}$ sont exactement les nombres premiers et leurs opposés. Deux premiers distincts sont associés si et seulement si ils sont opposés, si bien que $\mathcal{P}$ constitue une classe de représentants des éléments premiers de $\mathbb{Z}$ pour la relation d'équivalence "être associé à".*

Lemme.— *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.— (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.— (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 le résultat suivant : 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.— *1/ Soit p un nombre premier. Montrer que*

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

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

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

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

i) $x|y$,

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

Preuve : Exercice.

□

Etant donné deux entiers $x, y \in \mathbb{Z}^*$ les *p.g.c.d.* (resp. les *p.p.c.m.*) de x et de y sont associés. Il y en a donc 2 qui sont opposés l'un de l'autre. Dans $\mathbb{Z}$ on appelle LE *p.g.c.d.* (resp. LE *p.p.c.m.*) de x et de y, celui des deux qui est positif. On le note $p.g.c.d.(x, y)$ (resp. $p.p.c.m.(x, y)$) ou parfois $x \wedge y$ (resp. $x \vee y$) ou encore (x, y).

Proposition.— *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 p.g.c.d. (resp. le p.p.c.m) de x et de y.*

2/ Soient $x, y \in \mathbb{Z}^*$. Posons $d = p.g.c.d.(x, y)$ et $m = p.p.c.m.(x, y)$. 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 $x, y, z \in \mathbb{Z}^*$ 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 *p.g.c.d.* (resp. *p.p.c.m.*) d'une famille finie d'entiers non nuls : si $x_1, \cdots, x_n \in \mathbb{Z}^*$ on pose $p.g.c.d.(x_1, \cdots, x_n) = x_1 \wedge \cdots \wedge x_n$ (resp. $p.p.c.m.(x_1, \cdots, x_n) = x_1 \vee \cdots \vee x_n$).

Proposition.— *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 p.g.c.d. (resp. le p.p.c.m) des entiers x_i.

2/ Posons $d = p.g.c.d.(x_1, \cdots, x_n)$ et $m = p.p.c.m.(x_1, \cdots, x_n)$. 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.— *Soit $a, b \in \mathbb{Z}^*$ et $a = bq + r$ la division euclidienne de a par b. Si $r \neq 0$ alors $p.g.c.d.(a, b) = p.g.c.d.(b, r)$. Si $r = 0$ alors $p.g.c.d.(a, b) = b$.*

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 $r_N = p.g.c.d.(a,b)$ (exercice). On dit que le dernier reste non nul de l'algorithme d'Euclide est égal au *p.g.c.d.*.

Complexité : Le fait que $0 = r_{N+1} < r_N < \cdots < r_0 = b$ montre que $N(a,b) \leq b$. Il y a donc au maximum b divisions euclidiennes a effectuer pour trouver le *p.g.c.d.* de a et b. En fait, on peut majorer beaucoup mieux ce nombre de divisions euclidiennes :

Proposition.— *Soit a,b deux entiers naturels non nuls. On a*

$$N(a,b) < 2\log_2 b + 1$$

Preuve : Soit $i \in \{0,\cdots,N-2\}$. Si $r_{i+1} \leq \frac{r_i}{2}$ alors $r_{i+2} < \frac{r_i}{2}$. Si maintenant $r_{i+1} > \frac{r_i}{2}$ alors $r_i = r_{i+1}q_{i+2} + r_{i+2} > \frac{r_i}{2} + r_{i+2}$ et donc $r_{i+2} < \frac{r_i}{2}$ dans tous les cas.

Supposons que $N = 2k$ soit pair. On a donc

$$b = r_0 > 2r_2 > 4r_4 > \cdots > 2^k r_{2k} \geq 2^k$$

et donc $k \leq \log_2 b$, ce qui implique $N < 2\log_2 b + 1$.

Supposons maintenant que $N = 2k+1$ soit impair. On a donc

$$b = r_0 > r_1 > 2r_3 > 4r_5 > \cdots > 2^k r_{2k+1} \geq 2^k$$

et donc $k \leq \log_2 r_1 < \log_2 b$, ce qui implique là encore que $N < 2\log_2 b + 1$.

□

Exercice : (On garde les notations précédentes)

a) Que représente l'entier $r_{N(a,b)}$ pour le couple (a,b)?

b) Comparer $N(b,a)$ et $N(a,b)$.

c) Soit $a = bq + r$ la division euclidienne de a par b. Expliciter $N(b,r)$ en fonction de $N(a,b)$ quand $r \neq 0$.

d) Prouver que si a' désigne un entier strictement positif tel que $a \equiv a' \bmod(b)$ alors $N(a,b) = N(a',b)$.

e) Expliquer comment, grâce aux questions précédentes on peut, sans faire le calcul, dresser le tableau à double entrées des valeurs de $N(a,b)$ pour $a,b \in \mathbb{N}^*$. Dresser ce tableau pour $a,b \in \{1,\cdots,10\}$.

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

2/ Décrire des algorithmes qui permettent de calculer le *p.g.c.d.* de deux entiers.

Lemme.— *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.

□

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

Preuve : Exercice.

□

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

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

i) $x|y$,

ii) $y\mathbb{Z} \subset x\mathbb{Z}$.

En conséquence de quoi si d (resp. m) est un entier naturel non nul, les propriétés suivantes sont équivalentes :

i) $d = p.g.c.d.(x,y)$ (resp. $m = p.p.c.m.(x,y)$),

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

Preuve : La première équivalence est évidente.

Soit $d = p.g.c.d.(x,y)$. 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 $m = p.p.c.m.(x,y)$ est laissé en exercice.

□

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

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

i) x et y sont premiers entre eux,

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

Preuve : Soit $d = p.g.c.d.(x,y)$. 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 $d = 1$.

□

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

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 $d = p.g.c.d.(a,b)$. 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

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

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

$a=bq_0+r_0$
$b=r_0q_1+r_1$
$r_0=r_1q_2+r_2$
$\vdots$
$r_{n-2}=r_{n-1}q_n+d$
$r_{n-1}=r_nq_{n+1}$.

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 $d=p.g.c.d.(-91,56)$. Utilisons l'algorithme d'Euclide :

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

On a donc $p.g.c.d.(-91,56)=d=7$. 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 $p.g.c.d.$ 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 $(x, y) \in \mathbb{Z}^2$:

$$\begin{aligned} ax + by = c &\iff a^{'}x + b^{'}y = h \\ &\iff \begin{cases} a^{'}x + b^{'}y = h \\ a^{'}x_0 + b^{'}y_0 = h \end{cases} \\ &\iff a^{'}(x - x_0) = b^{'}(y_0 - y) \\ &\iff \exists k \in \mathbb{Z},\ k = \frac{(x - x_0)}{b^{'}} = \frac{(y_0 - y)}{a^{'}} \text{ (par application du théorème de Gauss)} \\ &\iff \exists k \in \mathbb{Z},\ \begin{cases} x = x_0 + b^{'}k \\ y = y_0 - a^{'}k \end{cases} \end{aligned}$$

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 $\mathbb{Z}$.

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

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

L'anneau $\mathbb{Z}$ est euclidien pour le stathme $|.|$, il est donc principal et ses idéaux sont les $n\mathbb{Z}$ pour $n \in \mathbb{N}^*$. On va étudier dans ce paragraphe l'anneau $\mathbb{Z}/n\mathbb{Z}$. C'est un anneau commutatif et unitaire, dans la suite de ce texte on notera $(\mathbb{Z}/n\mathbb{Z})^*$ le groupe multiplicatif $U(\mathbb{Z}/n\mathbb{Z})$.

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

Proposition.— *Soit $n \in \mathbb{N}^*$, les propositions suivantes sont équivalentes :*

i) n est premier,

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

ii) $\mathbb{Z}/n\mathbb{Z}$ est intègre.

Preuve : $i) \Rightarrow ii)$ L'entier n étant premier, il est irréductible et donc $n\mathbb{Z}$ est un idéal maximal de $\mathbb{Z}$ et donc $\mathbb{Z}/n\mathbb{Z}$ est un corps.

$ii) \Rightarrow iii)$ Evident.

$iii) \Rightarrow i)$ Si $\mathbb{Z}/n\mathbb{Z}$ est intègre, alors $n\mathbb{Z}$ est un idéal premier et donc n est premier.

□

Proposition.— *Soit $n \in \mathbb{N}^*$, et $k \in \mathbb{Z}$. On note $\overline{k}$ la classe de k dans $\mathbb{Z}/n\mathbb{Z}$. Les propositions suivantes sont équivalentes :*

i) $\overline{k}$ engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$,

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 : $i) \Leftrightarrow ii)$ a déjà été vu dans la partie sur les groupes.

$ii) \Rightarrow iii)$ 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 $d = p.g.c.d.(n, k) > 1$ 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.

□

Corollaire.— *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.— *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.— *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*

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

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

Proposition.— *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

$$l = k + n \prod_{p\ premier,\ p \leq nm,\ p \nmid k} p$$

convient.

□

Théorème.— *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 $p^{f+1} \nmid N$. 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.— *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.— *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.— *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.— *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.— *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 $\left(\frac{\mathbb{Z}}{24\mathbb{Z}}\right)^* \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$.

6.3.2 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.— 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.

Chapitre 7

Introduction à la théorie des corps

7.1 Généralités

7.1.1 Anneaux et corps

On rappelle qu'un corps est un anneau unitaire A tel que $U(A) = A - \{0\}$. Si A est commutatif, on parle de corps commutatif, dans le cas contraire, on parle de corps gauche. Dans tout ce qui suit, les corps que l'on considérera seront commutatifs.

Proposition.— *Soit k un corps et A un anneau. Tout morphisme non trivial d'anneau $f : k \to A$ est injectif.*

Preuve : • Le corps k étant, en particulier un anneau, le noyau $\mathrm{Ker}(f)$ de f est un idéal de k. Il vaut donc k ou $\{0\}$. La première hypothèse est exclue puisque f est non trivial.

□

On rappelle que pour $n \in \mathbb{N}^*$ donné, il y a équivalence entre :

i) n est premier,

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

iii) $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Si p désigne un nombre premier, on note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Définition.— *Soit $(K, +, .)$ un corps. On appelle sous-corps de K, toute partie k de K stable par $+$ et $.$ telle que $(k, +, .)$ soit un corps.*

Lemme.— *Soit K un corps et $(k_i)_i$ une famille de sous-corps de K. Alors $\bigcap_i k_i$ est un sous-corps de K.*

Preuve : Exercice.

□

Si k est un sous-corps de K et A une partie de K, l'intersection des sous-corps de K contenant k et A est donc un sous-corps de K (l'intersection ne se fait pas sur un ensemble vide car K contient A et k). Ce corps est le plus petit sous-corps (au sens de l'inclusion) de K contenant k et A.

Définition.— *On appelle corps engendré dans K par A sur k le plus petit sous-corps (au sens de l'inclusion) de K contenant k et A. On le note $k(A)$.*

Proposition.— *Soit $k \subset K$ deux corps et $A \subset K$. On a*

$$\begin{aligned} k(A) &= \left\{ \frac{P(a_1, \cdots, a_n)}{Q(b_1, \cdots, b_m)} / \; n, m \in \mathbb{N};\; P \in k[X_1, \cdots, X_n], \right. \\ &\quad Q \in k[X_1, \cdots, X_m]; \\ &\quad \left. (a_1, \cdots, a_n) \in A^n, (b_1, \cdots, b_m) \in A^m;\; Q(b_1, \cdots, b_m) \neq 0 \right\} \\ &= \left\{ \frac{\sum_{i \in I} \lambda_i \prod_{k_i \in J_i} a_{k_i}}{\sum_{i' \in I'} \lambda_{i'} \prod_{k_{i'} \in J_{i'}} b_{k_{i'}}} / \; I, I', J_i, J_{i'} \; finis, \right. \\ &\quad \left. a_{k_i}, b_{k_{i'}} \in A;\; \lambda_i, \lambda_{i'} \in k \right\} \end{aligned}$$

Preuve: Exercice.

□

Définition.— *Soit K un corps et k_0 et k_1 deux sous-corps de K. On appelle compositum dans K des corps k_0 et k_1 le corps $k_0 \bullet k_1 = k_0(k_1) = k_1(k_0)$. Par extension, si $(k_i)_i$ désigne une famille de sous-corps de K, on appelle compositum des corps k_i dans le corps K, le plus petit sous-corps de K contenant k_i pour tout i. On note ce corps $\bullet_i k_i$.*

Lemme.— *La caractéristique d'un corps K est soit nul, soit égale à un nombre premier.*

Preuve : Considérons le morphisme $f : \mathbb{Z} \to K$ défini par $f(n) = 1 + \cdots + 1$ (n fois). Son noyau est donc de la forme $n\mathbb{Z}$ avec $n = \mathrm{car}(K)$. Si $n \neq 0$, alors par le théorème d'isomorphisme $\mathrm{Im}(f)$ s'identifie à $\mathbb{Z}/n\mathbb{Z}$, mais comme $\mathrm{Im}(f)$ est un sous-anneau de K qui est un corps, alors $\mathrm{Im}(f)$ est intègre, donc $\mathbb{Z}/n\mathbb{Z}$ l'est aussi et par suite n est un nombre premier.

□

Définition.— *Un corps est dit premier s'il ne possède pas d'autre sous-corps que lui-même. Soit K un corps, on appelle sous-corps premier de K l'intersection de tous ces sous-corps. Le sous-corps premier d'un corps est donc un corps premier.*

Proposition.— *Un corps premiers est isomorphe soit à $\mathbb{Q}$ soit à un $\mathbb{Z}/p\mathbb{Z}$ pour p premier. Si K est un corps et F sont sous-corps premier. On a:*

$$\mathrm{car}(K) = 0 \iff F \simeq \mathbb{Q} \text{ et } \mathrm{car}(K) = p \iff F \simeq \mathbb{F}_p$$

Preuve : Exercice.

□

7.1.2 Polynômes

On rappelle qu'étant donné un corps K commutatif, l'anneau $K[X]$ est euclidien (donc en particulier principal).

Proposition.— *Soit K un corps commutatif et k un sous-corps de K. Soit $P, Q \in k[X] \subset K[X]$. Le p.g.c.d de P et Q est le même dans $k[X]$ et dans $K[X]$.*

Preuve : Puisqu'il y a unicité, le résultat de la division euclidienne de deux polynômes de $k[X]$ est le même dans $k[X]$ et dans $K[X]$. L'algorithme d'euclide qui donne le p.g.c.d. de P et Q étant une suite de divisions euclidiennes, on en déduit qu'il est le même dans $k[X]$ et dans $K[X]$.

□

On rappelle que si A est un anneau commutatif et $P \in A[X]$ est un polynôme de degré $n \geq 1$ alors si $\alpha \in A$ est racine de P, il existe $Q \in A[X]$ de degré $n-1$ tel que $P(X) = (X - \alpha)Q(X)$. En conséquence de quoi, si A est intègre (en particulier si A est un corps commutatif), un polynôme $P \in A[X]$ de degré $n \geq 1$, possède au maximum n racines.

Ainsi, si $P \in K[X]$ un polynôme et $\alpha \in K$ une racine de P, il existe un polynôme $Q \in K[X]$ et un entier $d > 0$ tel que $P(X) = (X - \alpha)^d Q(X)$ et $Q(\alpha) \neq 0$. On rappelle que l'on dit alors que α est racine de P d'ordre d.

On dit qu'un polynôme $P \in K[X]$ est totalement décomposé si ses seuls facteurs irréductibles sont de degré 1, ce qui revient à dire que la somme des ordres de ses racines est égale à son degré.

Lemme.— *Soit K un corps commutatif, les propositions suivantes sont équivalentes :*

i) Tout polynôme $P \in K[X]$ de degré ≥ 1 admet une racine,

ii) tout polynôme $P \in K[X]$ est totalement décomposé.

Preuve: S'obtient par récurrence finie.

□

Définition.— *On dit qu'un corps commutatif K est algébriquement clos, s'il satisfait au propriétés du lemme précédent.*

7.2 Extensions

7.2.1 Généralités

Définition.— *Soit k un corps. On appelle extension du corps k, toute paire (K, φ) où K est un corps et $\varphi : k \to K$ un morphisme de corps.*

Si K est un corps k un sous-corps de K, alors l'injection canonique de k dans K définie une extension du corps k. Réciproquement, si K est une extension d'un corps k (par un morphisme φ), alors $\varphi(k)$ est un sous-corps de K isomorphe à k. On identifie alors souvent k et $\varphi(k)$. L'extension se note alors K/k.

Définition.— *Soit K_1/k et K_2/k deux extensions d'un même corps (pour fixé les idées notons $\varphi_1 : k \to K_1$ et $\varphi_1 : k \to K_2$ les morphismes associés). On appelle k-isomorphisme (ou k-plongement) de K_1 vers K_2 tout morphisme de corps $\psi : K_1 \to K_2$ tel que pour tout $x \in k$, on ait $\psi \circ \varphi_1(x) = \varphi_2(x)$. On note $\mathrm{Isom}_k(K_1, K_2)$ l'ensemble des k-isomorphisme de K_1 vers K_2.*

Définition.— *Soit K/k une extension et $\varphi : k \to K$ le morphisme associé. On appelle extension intermédiaire de K/k tout sous-corps K_0 de K contenant $\varphi(k)$. K_0/k est alors une extension.*

Proposition.— *Soit K un corps de caractéristique p premier (resp. 0). On a l'extension $K/\mathbb{F}_p$ (resp. $K/\mathbb{Q}$).*

Preuve: Exercice.

□

Si K/k désigne une extension de corps, le corps K a naturellement une structure de k-espace vectoriel. On peut donc parler de la dimension de K en tant que k-e.v.

Définition.— *Soit K/k une extension de corps. On appelle degré de l'extension K/k la dimension $\dim_k(K)$. On note ce nombre (éventuellement égal à $+\infty$) $[K : k]$. Si $[K : k] < +\infty$, on dit que K/k est finie.*

Si M/L et L/K sont deux extensions, alors M/K est une extension. On a alors :

Proposition.— $[M : K] = [M : L].[L : K]$.

Preuve: Si l'une des deux extensions est infinie le résultat est clair. Supposons $[L : K] = n$ et $[M : L] = m$ et notons $(a_1, \cdots, a_n)$ une K-base de L et $(b_1, \cdots, b_m)$ une L-base de M. Soit $x \in M$, il existe donc $\beta_1, \cdots, \beta_m$ des éléments de L tels que

$$x = \beta_1 b_1 + \cdots + \beta_m b_m$$

Maintenant, pour tout $i = 1, \cdots m$, il existe des éléments $\alpha_{i1}, \cdots, \alpha_{in}$ de K tels que

$$\beta_i = \alpha_{i1} a_1 + \cdots + \alpha_{in} a_n$$

et par suite

$$x = \sum_{i,j} \alpha_{ij} b_i a_j$$

donc la famille $(b_i a_j)_{ij}$ est une famille K-génératrice de M. Montrons qu'elle est K-libre. Supposons donné une famille (λ_{ij}) d'éléments de K tels que

$$\sum_{i,j} \lambda_{ij} b_i a_j = 0$$

En posant

$$\omega_i = \lambda_{i1} a_1 + \cdots + \lambda_{in} a_n \in L$$

on a $\omega_1 b_1 + \cdots + \omega_m b_m = 0$ et comme la famille $(b_1, \cdots, b_m)$ est une L-base de M, on en déduit que $\omega_i = 0$ pour tout i, c'est-à-dire

$$\lambda_{i1} a_1 + \cdots + \lambda_{in} a_n = 0$$

mais comme $(a_1, \cdots, a_n)$ est une K-base de L, on en déduit que $\lambda_{ij} = 0$ pour tout i et tout j.

□

Corollaire.— *Soit K/k une extension et K_0 une extension intermédiaire. Alors $[K : k]$ est divisible par $[K : K_0]$ et $[K_0 : k]$. En particulier, si $[K : k] = p$ premier, alors les seuls sous-extensions de K/k sont K et k.*

Définition.— *Soit K/k une extension et P une partie de K. L'ensemble des extensions intermédiaires de K/k qui contiennent P admet, au sens de l'inclusion, un plus petit élément (l'intersection). On la note $k(P)$ et on l'appelle la sous-extension de K/k engendré par P. Lorsque $P = \{a_1, \cdots, a_n\}$, on note plus volontier $k(\{a_1, \cdots, a_n\}) = k(a_1, \cdots, a_n)$.*

Définition.— *Une extension K/k est dite de type fini s'il existe une partie $P \subset K$ finie telle que $K = k(P)$. On dit que K/k est monogène s'il existe $\alpha \in K$ tel que $K = k(\alpha)$. On dit alors que α est un élément primitif de l'extension K/k.*

Remarque : Si K/k est une extension de degré premier, alors K/k est monogène. De manière plus précise, tout élément $\alpha \in K - k$ est primitif.

7.2.2 Extensions algébriques

Définition.— *Soit K/k une extension et $\alpha \in K$. On dit que α est algébrique sur k, s'il existe un polynôme $P \in k[X]$ tel que $P(\alpha) = 0$. Dans le cas contraire, on dit que α est transcendant sur k.*

Si tout élément de K est algébrique sur k, on dit que K/k est une extension algébrique, dans le cas contraire, on dit que K/k est transcendante.

Soit K/k une extension et $a \in K$. On considère l'application $\Phi_a : k[X] \to K$ définie par :

$$\Phi_a(P(X)) = P(a)$$

L'application Φ_a est un morphisme de k-algèbre. On note $k[a]$ son image. $k[a]$ est donc le sous-k-espace vectoriel de K engendré par la famille $(a^n)_{n\in\mathbb{N}}$. On remarque que le sous-corps $k(a)$ de K est constitué des éléments de la forme $P(a)/Q(a)$ où $P, Q \in k[X]$ et $Q(a) \neq 0$, c'est-à-dire que $k(a) = Frac(k[a])$.

Proposition.— *Soit K/k une extension et $\alpha \in K$. Les propositions suivantes sont équivalentes :*

i) α est algébrique,

ii) $\dim_k k[\alpha] < +\infty$,

iii) Φ_α n'est pas injectif.

Preuve: $i) \Rightarrow ii)$ Soit $P(X) = \sum_{i=0}^{d} a_i X^i \neq 0$ un polynôme annulateur de α. Montrons par récurrence que pour tout $n \geq d$, α^n est combinaison linéaire sur k de $1, \alpha, \cdots, \alpha^{d-1}$.
Pour $n = d$, on a $\alpha^d = -\sum_{i=0}^{d-1} a_i \alpha^i$
Supposons la propriété vérifiée au rang $n \geq d$. On a donc

$$\alpha^n = \sum_{i=0}^{d-1} \lambda_i \alpha^i$$

avec $\lambda_i \in k$. On a alors

$$\begin{array}{rcl} \alpha^{n+1} & = & \alpha.\alpha^n \\ & = & \sum_{i=0}^{d-1} \lambda_i \alpha^{i+1} \\ & = & \sum_{i=1}^{d-1} \lambda_{i-1} \alpha^i + \lambda_{d-1} \alpha^d \\ & = & \sum_{i=1}^{d-1} \lambda_{i-1} \alpha^i - \sum_{i=0}^{d-1} \lambda_{d-1} a_i \alpha^i \end{array}$$

La proposition est donc vérifiée et par suite $(1, \cdots, \alpha^{d-1})$ est une famille génératrice de $k[\alpha]$ qui est donc de dimension $\leq d$ sur k.

$ii) \Rightarrow iii)$ La famille $(\alpha^i)_i$ est k-liée puisqu'infinie. Il existe donc un entier n et des éléments $a_0, \cdots, a_n$ de k tel que

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

c'est à dire $P \in \mathrm{Ker}(\Phi_\alpha)$ avec

$$P(X) = \sum_{i=0}^{n} a_i X^i \neq 0$$

donc Φ_α n'est pas injectif.

$iii) \Rightarrow i)$ Soit $P \in \mathrm{Ker}(\Phi_\alpha)$ non nul, alors $P(\alpha) = 0$ et par suite α est algébrique.

□

Soit $\alpha \in K$ algébrique. Le noyau de Φ_α (c'est-à-dire l'ensemble des polynômes qui admettent α pour racine) est donc un idéal non nul de $k[X]$. Comme $k[X]$ est principal, il existe un et un seul polynôme normalisé $\mathrm{Min}_k(\alpha)(X) \in k[X]$, tel que $\mathrm{Ker}\ \Phi_\alpha =< \mathrm{Min}_k(\alpha)(X) >$. On appelle ce polynôme, le polynôme minimal de α. On a alors :

Proposition.— *Soit K/k une extension, $\alpha \in K$ un élément algébrique et P un polynôme de $k[X]$. Les propositions suivantes sont équivalentes :*

i) $P = \mathrm{Min}_k(\alpha)$,

ii) P est irréductible, unitaire et $P(\alpha) = 0$.

Preuve: $i) \Rightarrow ii)$ Il faut montrer que P est irréductible. Si ce n'est pas le cas, alors $P = P_1 P_2$ avec $d^\circ P_i > 0$ et comme $P(\alpha) = 0$ on a $P_1(\alpha) = 0$ ou $P_2(\alpha)$, mais comme $d^\circ P_i < d^\circ P$, ceci contredit la minimalité de P.

$ii) \Rightarrow i)$ On a $P \in \mathrm{Ker}(\Phi_\alpha)$ et comme ce dernier est engendré par $\mathrm{Min}_k(\alpha)$ on en déduit que $\mathrm{Min}_k(\alpha)|P$, mais comme P est irréductible et que $\mathrm{Min}_k(\alpha)$ n'est pas constant, on en déduit que $P|\mathrm{Min}_k(\alpha)$. Ces deux polynômes étant unitaire, on a bien $P = \mathrm{Min}_k(\alpha)$.

□

Corollaire.— *Soit K/k une extension et $\alpha \in K$. Les propositions suivantes sont équivalentes :*

i) α *est algébrique,*

ii) $[k(\alpha) : k] < +\infty$,

iii) $k(\alpha) = k[\alpha]$.

Preuve: $i \Rightarrow iii$ On a $k[\alpha] \subset k(\alpha)$. Le corps $k(\alpha)$ est le sous-corps de K constitué des éléments $P(\alpha)/Q(\alpha)$ avec $P, Q \in k[X]$ et $Q(\alpha) \neq 0$. Soit M le polynôme minimal de α. Les polynômes M et Q sont premiers entre eux, donc, d'après Bezout, il existe $U, V \in k[X]$ tel que $UM + VQ = 1$ et par suite $1/Q(\alpha) = V(\alpha) \in k[\alpha]$ et donc $P(\alpha)/Q(\alpha) \in k[alpha]$ c'est-à-dire $k(\alpha) \subset k[\alpha]$.

$iii \Rightarrow i$ Il existe un entier n et des éléments non tous nul $a_0, \cdots, a_n$ de k tel que $\alpha^{-1} = a_0 + \cdots + a_n \alpha^n$. On a donc

$$a_n \alpha^{n+1} + \cdots + a_0 \alpha - 1 = 0$$

ce qui prouve que α est algébrique sur k.

$iii \Rightarrow ii$ On sait que $(i) \Leftrightarrow iii)$) α est algébrique, donc que $\dim_k k[\alpha] < +\infty$. On a donc $[k(\alpha) : k] < +\infty$.

$ii \Rightarrow i$ Comme $k[\alpha]$ est un sous-k-espace vectoriel de $k(\alpha)$ on a donc $\dim_k k[\alpha] < +\infty$ et par suite, α est algébrique sur k.

□

Proposition.— *Soit K/k une extension et $\alpha \in K$ un élément algébrique. On a $[k(\alpha) : k] = d^\circ \mathrm{Min}_k(\alpha) = n$ et la famille $(1, \alpha, \cdots, \alpha^{n-1})$ est une k-base de $k(\alpha)$.*

Preuve: On sait que $k(\alpha) = k[\alpha]$. La même preuve que pour la proposition ???, montre que la famille $(1, \alpha, \cdots, \alpha^{n-1})$ est k-génératrice de $k[\alpha]$. Supposons qu'il existe une équation de dépendance linéaire non trivial pour cette famille

$$\lambda_0 + \cdots + \lambda_{n-1} \alpha^{n-1} = 0$$

Le polynôme $P(X) = \sum_{i=0}^{n-1} \lambda_i X^i \neq 0$ est alors anulateur de α ce qui contredit la minimalité de $\mathrm{Min}_k(\alpha)$.

□

Définition.— *Soit K/k une extension et $\alpha \in K$ un élément algébrique. On appelle degré de α, le degré de son polynôme minimal.*

Si M/K désigne une extension et $M/L/K$ une extension intermédiaire, alors tout élément de M algébrique sur K est algébrique sur L et son degré sur L est plus petit que son degré sur K.

Proposition.— *Toute extension finie est algébrique. De manière plus précise, si L/K est une extension de degré n, alors tout élément de K a un degré $\leq n$ sur k.*

Preuve: Soit $\alpha \in K$. La famille $1, \cdots, \alpha^n$ comptant $n+1$ éléments est liée dans K, donc il existe des éléments non tous nuls $a_0, \cdots, a_n \in k$ tel que

$$a_0 + a_1 \alpha + \cdots + a_n \alpha^n = 0$$

Le polynôme $P(X) = a_0 + \cdots + a_n X^n \in k[X]$ est donc annulateur de α et par suite $\mathrm{Min}_k(\alpha)$ divise P donc le degré de α est plus petit que n.

□

Lemme.— *Soit L/K une extension et $A \subset L$. On a alors* $K(A) = \bigcup_{J \subset A \ finie} K(J)$.

Preuve: Il est clair que $\bigcup_{J\subset A\ finie} K(J) \subset K(A)$. Maintenant, il est clair aussi que $A \subset \bigcup_{J\subset A\ finie} K(J)$. Pour montrer notre résultat, il suffit de prouver que $\bigcup_{J\subset A\ finie} K(J)$ est un corps. Soit $x, y \in \bigcup_{J\subset A\ finie} K(J)$ $(y \neq 0)$, il existe donc $J_x \subset A$ et $J_y \subset A$ finies telles que $x \in K(J_x)$ et $y \in K(J_y)$. Alors $J_x \cup J_y$ est une partie finie de A et comme $x - y$ et xy^{-1} sont dans $K(J_x \cup J_y) \subset \bigcup_{J\subset A\ finie} K(J)$ on en déduit bien que $\bigcup_{J\subset A\ finie} K(J)$ est un corps.

□

Corollaire.— *Soit L/K une extension et $A \subset L$. Les propriétés suivantes sont équivalentes :*

i) $K(A)/K$ est algébrique,

ii) $\forall \alpha \in A$, α est algébrique sur K.

Preuve: $i) \Rightarrow ii)$ Evident.

$ii) \Rightarrow i)$ Soit $J \subset A$ une partie finie. Posons $J = \{\alpha_1, \cdots, \alpha_n\}$. On a $[K(\alpha_1) : K] < +\infty$. Comme α_2 est algébrique sur K, il l'est sur $K(\alpha_1)$ et donc $[K(\alpha_1, \alpha_2) : K(\alpha_1)] < +\infty$, comme $[K(\alpha_1, \alpha_2) : K] = [K(\alpha_1, \alpha_2) : K(\alpha_1)].[K(\alpha_1) : K]$ on en déduit que $[K(\alpha_1, \alpha_2) : K] < +\infty$. Par récurrence finie, on en déduit que $K(J)/K$ est une extension finie et par suite algébrique. Pour finir, il suffit de remarquer que $K(A) = \bigcup_{J\subset A\ finie} K(J)$.

□

Corollaire.— *Soit $L = K(\alpha_1, \cdots, \alpha_n)$ une extension de type finie d'un corps K. Les propositions suivantes sont équivalentes :*

i) L/K est algébrique,

ii) $[L : K] < +\infty$,

iii) α_i est algébrique pour tout $i = 1, \cdots, n$.

Preuve: $i) \Rightarrow ii)$ Par transitivité des degré, on a

$$[L : K] = [L : K(\alpha_1, \cdots, \alpha_{n-1})].\cdots.[K(\alpha_1) : K]$$

comme toutes ces dimensions sont finies, on en déduit bien le résultat.

$ii) \Rightarrow iii)$ Immédiat.

$iii) \Rightarrow i)$ C'est une conséquence de la proposition précédente.

□

Corollaire.— *Soient M/L et L/K deux extensions. Les propositions suivantes sont équivalentes :*

i) M/K est algébrique,

ii) M/L et L/K sont algébriques.

Preuve: $i) \Rightarrow ii)$ Evident.

$ii) \Rightarrow i)$ Soit $\alpha \in M$ et $P(X) = \sum_{i=0}^{n} a_i X^i = \mathrm{Min}_L(\alpha)$. Les éléments a_i sont algébriques sur K, donc le corps $K' = K(a_0, \cdots, a_n)$ est de dimension fini sur K. Le polynôme $P \in K'[X]$ est annulateur de α, donc α est algébrique sur K'. Donc $K'(\alpha)/K'$ est fini et par transitivité des degré $K'(\alpha)/K$ est fini et comme $K(\alpha) \subset K'(\alpha)$ on en déduit que α est algébrique sur K.

□

7.2.3 Clôture algébrique

Proposition.— *Soit K/k une extension. L'ensemble A des éléments de K algébriques sur k forme un corps, extension algébrique de k. On l'appelle clôture algébrique de k dans K. Si K est algébriquement clos alors A l'est aussi.*

Preuve: On a $A \subset K$, pour montrer que A est un sous-corps de K, il suffit de prouver que si $x, y \in A$ avec $y \neq 0$ alors $x - y \in A$ et $xy^{-1} \in A$. Maintenant, par hypothèse x et y sont algébrique sur k, donc $[k(x, y) : k] < +\infty$ donc $k(x, y)/k$ est une extension algébrique et comme $x - y \in k(x, y)$ et $xy^{-1} \in k(x, y)$ on en déduit bien que $x - y \in A$ et $xy^{-1} \in A$. Le fait que A/k soit une extension algébrique est immédiat.

Si K est supposé algébriquement clos, montrons que A l'est aussi. Soit $P(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ un polynôme non constant. Posons $K_0 = k(a_0, \cdots, a_n)$. Comme les a_i sont algébriques sur k, on en déduit que $[K_0 : k] < +\infty$. Soit

maintenant $\alpha \in K$ tel que $P(\alpha) = 0$. L'élément α est donc algébrique sur K_0 et par suite $[K_0(\alpha) : K_0] < +\infty$ et donc $[K_0(\alpha) : k] < +\infty$ et donc α est algébrique sur k, donc $\alpha \in A$.

□

Proposition.— *Soit K/k une extension telle que K soit algébriquement clos. Les propositions suivantes sont équivalentes :*

i) K/k est algébrique,

ii) K/k ne possède pas d'extension intermédiaire stricte qui soit algébriquement close.

Preuve: $i) \Rightarrow ii)$ Soit K_0 un sous-corps strict de K. Il existe donc $\alpha \in K$ tel que $\alpha \notin K_0$. Comme K/K_0 est une extension algébrique, α possède un polynôme minimal sur K_0, $P \in K_0[X]$. Le polynôme P est de degré > 1 sinon, α serait dans K_0. Le polynôme P étant irréductible n'est pas totalement décomposé sur K_0 ce qui montre bien que ce corps n'est pas algébriquement clos.

$ii) \Rightarrow i)$ Supposons K/k transcendante. Le corps A obtenu dans la proposition précédente est une extension intermédiaire de K algébriquement close et différente de K car A/k est une extension algébrique.

□

Définition.— *Soit K/k une extension. On dit que K est une clôture algébrique de k si K vérifie les deux propriétés équivalentes de la proposition précédente.*

Lemme.— *Soit K un corps et $P \in K[X]$ un polynôme irréductible de degré ≤ 1. Le corps $K[X]/(P)$ est une extension finie de K dans laquelle P admet une racine.*

Preuve: Puisque P est irréductible, l'anneau $K[X]/(P)$ est bien un corps et l'injection canonique $K \to K[X]$ se factorisant, on en déduit que $K[X]/(P)$ est une extension de K. Posons $n = d^\circ P$ et $\alpha = \overline{X}$. Il est clair que $1, \alpha, \cdots, \alpha^{n-1}$ forment une base de $K[X]/(P)$ vu comme K-espace vectoriel. Par ailleurs, il est aussi clair que $P(\alpha) = 0$.

□

Proposition.— *Soit K/k une extension. Les propositions suivantes sont équivalentes :*

i) K est une clôture algébrique de k,

ii) K/k est une extension algébrique maximale,

iii) K/k est algébrique et tout polynôme non constant de $k[X]$ admet toutes ses racines dans K.

Preuve: $i) \Rightarrow ii)$ K/k est algébrique. Si K/k n'est pas maximale, alors il existe une extension K_0/K stricte et par suite tout élément $\alpha \in K_0 - K$ fournit un polynôme $(\mathrm{Min}_K(\alpha))$ de $K[X]$ de degré ≥ 2 n'ayant pas de racine dans K, donc K n'est pas algébriquement clos.

$ii) \Rightarrow iii)$ Soit $P \in k[X]$ ne possédant pas toutes ses racines sur K. P vu dans $K[X]$ possède donc un facteur irréductible Q de degré ≥ 2. Le corps $K_Q = K[X]/(Q)$ est une extension algébrique stricte de K, mais alors K_Q/k est algébrique ce qui contredit la maximalité du K/k.

$iii) \Rightarrow i)$ Il faut montrer que K est algébriquement clos. Si ce n'est pas le cas, alors il existe $P \in K[X]$ sans racine dans K. Soit Q un facteur irréductible de P de degré ≤ 2. Le corps de $K_Q = K[X]/(Q)$ est une extension stricte de K. Soit $\alpha \in K_Q - K$. Comme K_Q/K et K/k sont algébriques, α est algébrique sur k. Le polynôme minimal $\mathrm{Min}_k(\alpha)$ ne peut pas être totalement décomposé sur K, sinon on aurait $\alpha \in K$, d'où l'absurdité.

□

Si K/k est une extension avec K algébriquement clos, la clôture algébrique A de k dans K est donc une clôture algébrique de k. Ainsi tout corps contenu dans un corps algébriquement clos possède une clôture algébrique. En fait, de manière générale, on a :

Théorème.— (Steiniz) *Tout corps k admet une clôture algébrique.*

Preuve: (D'après Lang) On considère l'anneau $D = K[X_f]$ des polynômes à coefficients dans K en les variables X_f où f parcourt l'ensemble des polynômes de $K[X]$ de degré ≤ 1. Soit I l'idéal de D engendré par les polynômes $f(X_f)$ pour f parcourant $K[X]$.

• L'idéal I est strict. En effet, $1 \notin I$, sinon il existerait des indices $f_1, \cdots, f_n$ et des polynômes $g_1, \cdots, g_n \in D$ tels que

$$\sum_{i=1}^{n} g_i f_i(X_{f_i}) = 1$$

Maintenant, il existe une extension L/K telle que chaque polynôme $f_i(X_{f_i})$ admette une racine. En évaluant l'égalité en un uplet contenant ces racines, on a alors $0 = 1$ ce qui est absurde.

• Le théorème de Krull assure qu'il existe un idéal maximal $\overline{I}$ contenant I. Considérons le corps $E = D/\overline{I}$. C'est une extension de K. En effet, la surjection canonique $s : D \to E$ induit un morphisme de corps de K sur E. Notons $x_f = s(X_f)$ et considérons le corps $E_1 = K(x_f)_f$. Chaque x_f est algébrique sur K, donc E_1/K est algébrique. Par ailleurs, tout polynôme $f \in K[X]$ admet une racine dans E_1 (à savoir x_f).

On construit de la même facon une extension algébrique E_2/E_1 telle que tous polynôme $f \in E_1[X]$ admette une racine dans E_2 et, par réccurence, on construit une suite d'extension $(E_n)_n$ telle que pour tout n, E_{n+1}/E_n est algébrique et tout polynôme $f \in E_n$ admet une racine dans E_{n+1}.

• Considérons alors le corps $L = \bigcup_n E_n$. L/K est algébrique et tout polynôme $f \in L[X]$ appartient à $E_n[X]$ pour un certain n, donc admet une racine dans $E_{n+1} \subset L$. L est bien algébriquement clos.

□

Proposition.— *Soit L/K et M/K deux extension de corps et $\alpha \in L$ et $\beta \in M$ deux élements algébriques sur K. Les propositions suivantes sont équivalentes :*

i) $\mathrm{Min}_K(\alpha) = \mathrm{Min}_K(\beta)$,

ii) il existe un (unique) K-isomorphisme $\sigma \in \mathrm{Isom}_k(K(\alpha), K(\beta))$ tel que $\sigma(\alpha) = \beta$.

Preuve: *i)* $\Rightarrow$ *ii)* Commencons par montrer l'unicité. Soit σ_1 et σ_2 deux K-isomorphismes de $\mathrm{Isom}_k(K(\alpha), K(\beta))$ tels que $\sigma_i(\alpha) = \beta$ pour $i = 1, 2$. On sait que $1, \alpha, \cdots, \alpha^{n-1}$ est une base du K-espace vectoriel $K(\alpha)$. Comme σ_1 et σ_2 sont des morphismes de corps et que $\sigma_1(\alpha) = \sigma_2(\alpha)$, on en déduit que $\sigma_1(\alpha^d) = \sigma_2(\alpha^d)$ pour tout $d = 0, \cdots, n-1$ et comme σ_1 et σ_2 sont en particulier des applications K-linéaires, on en déduit bien que $\sigma_1 = \sigma_2$.

Montrons maintenant l'existence de σ. Considérons le polynôme

$$P = \sum_{i=0}^{n} a_i X^i = \mathrm{Min}_K(\alpha) = \mathrm{Min}_K(\beta)$$

On sait que $1, \alpha, \cdots, \alpha^{n-1}$ et $1, \beta, \cdots, \beta^{n-1}$ forment des bases de $K(\alpha)$ et de $K(\beta)$. Définissons σ de la manière suivante : si $x \in K(\alpha)$ alors il existe un unique n-uplet $\lambda_0, \cdots, \lambda_{n-1} \in K$ tel que $x = \lambda_0 + \cdots + \lambda_{n-1}\alpha^{n-1}$. On pose alors

$$\sigma(x) = \lambda_0 + \cdots + \lambda_{n-1}\beta^{n-1}$$

On a bien $\sigma(\alpha) = \beta$ et σ est une application K-linéaire. Reste à vérifier que σ est bien un morphisme de corps. Puisque σ est K-linéaire, il suffit pour cela de montrer que l'image d'un produit de deux éléments de la K-base $1, \alpha, \cdots, \alpha^{n-1}$ est le produit des images de ces éléments, c'est-à-dire finalement que pour tout entier d, $\sigma(\alpha^d) = \beta^d$. Cette propriété est visiblement vraie pour $d = 0, \cdots, n-1$. Montrons la pour $d \geq n$.
Pour $d = n$, on a $\alpha^n = \alpha^n - P(\alpha) = -\sum_{i=0}^{n-1} a_i \alpha^i$ et donc

$$\begin{array}{rcl} \sigma(\alpha^n) & = & -\sum_{i=0}^{n-1} a_i \sigma(\alpha^i) \\ & = & -\sum_{i=0}^{n-1} a_i \beta^i \\ & = & \beta^n - P(\beta) \\ & = & \beta^n \end{array}$$

Supposons la propriété vraie au rang $d \geq n$. Alors $\sigma(\alpha^d) = \beta^d$. Soit $\lambda_0, \cdots, \lambda_{n-1} \in K$ tels que

$$\alpha^d = \lambda_0 + \cdots + \lambda_{n-1}\alpha^{n-1}$$

on a alors

$$\beta^d = \lambda_0 + \cdots + \lambda_{n-1}\beta^{n-1}$$

On a donc

$$\begin{array}{rcl} \alpha^{d+1} & = & \lambda_0\alpha + \cdots + \lambda_{n-1}\alpha^n \\ & = & \lambda_0\alpha + \cdots - \lambda_{n-1}\sum_{i=0}^{n-1} a_i\alpha^i \end{array}$$

et ainsi,

$$\begin{array}{rcl} \sigma(\alpha^{d+1}) & = & \lambda_0\beta + \cdots + \lambda_{n-1}\sigma(\alpha^n) \\ & = & \lambda_0\beta + \cdots - \lambda_{n-1}\sum_{i=0}^{n-1} a_i\beta^i \\ & = & \lambda_0\beta + \cdots + \lambda_{n-1}\beta^n \\ & = & \beta^{d+1} \end{array}$$

ce qui achève la preuve.

$ii) \Rightarrow i)$ Soit $P_1 = \mathrm{Min}_K(\alpha)$ et $P_2 = \mathrm{Min}_K(\beta)$. Comme $P_1(\alpha) = 0$ et que $\sigma(P_1(\alpha)) = P_1(\sigma(\alpha)) = P_1(\beta) = 0$, on en déduit que P_1 est un polynôme annulateur de β, donc $P_2|P_1$. Maintenant, il est clair que σ est bijectif puisqu'il envoie la base $1, \cdots, \alpha^{n-1}$ sur la base $1, \cdots, \beta^{n-1}$. En appliquant le même raisonnement que précédement à σ^{-1}, on en déduit que $P_1|P_2$ et comme ces deux polynômes sont unitaires, on trouve finalement $P_1 = P_2$.

□

Définition.— *Deux éléments algébriques d'une extension K/k sont dit conjugués, s'ils ont le même polynôme minimal.*

Proposition.— *Soit L/K une extension algébrique et $\sigma \in \mathrm{Isom}_K(L,L)$. Si $\alpha \in L$, on note $\mathcal{C}_\alpha$ l'ensemble des conjugués de α sur K dans L. La restriction de l'application σ à $\mathcal{C}_\alpha$ est une bijection de $\mathcal{C}_\alpha$ dans lui-même. En particulier, σ est un automorphisme de corps. On note alors* $\mathrm{Isom}_K(L,L) = \mathrm{Aut}_K(L)$. *Cet ensemble est un groupe pour la composition.*

Preuve: L'ensemble $\mathcal{C}_\alpha$ est fini puisque $P = \mathrm{Min}_K(\alpha)$ ne possède qu'un nombre fini de racines dans L. Soit $\beta \in \mathcal{C}_\alpha$. On alors $0 = \sigma(P(\beta)) = P(\sigma(\beta))$ donc $\sigma(\beta) \in \mathcal{C}_\alpha$ ce qui justifie bien que l'image de $\mathcal{C}_\alpha$ par σ est incluse dans $\mathcal{C}_\alpha$. Maintenant σ est injective et comme $\mathcal{C}_\alpha$ est fini on en déduit bien que σ restreinte à $\mathcal{C}_\alpha$ est bijective.

On sait que σ est injective, montrons qu'elle est surjecive. Soit $\alpha \in L$. On a $\alpha \in \mathcal{C}_\alpha$, et comme σ est une bijection sur $\mathcal{C}_\alpha$, il existe $\beta \in \mathcal{C}_\alpha \subset L$ tel que $\sigma(\beta) = \alpha$, ce qui prouve bien la surjectivité de σ.

□

Proposition.— *Soit L/K une extension monogène ($L = K(\alpha)$), M/K une extension quelconque. Pour tout $\sigma \in \mathrm{Isom}_K(L,M)$, $\sigma(\alpha)$ est une racine de* $\mathrm{Min}_K(\alpha)$ *et réciproquement, si β est une racine de* $\mathrm{Min}_K(\alpha)$ *dans M, il existe un unique $\sigma \in \mathrm{Isom}_K(L,M)$ tel que $\sigma(\alpha) = \beta$. Il y a donc une correspondance bijective entre les éléments de* $\mathrm{Isom}_K(L,M)$ *et les racines de* $\mathrm{Min}_K(\alpha)$ *dans L.*

Preuve: Il est clair que si $\sigma \in \mathrm{Isom}_K(L,M)$, alors $0 = \sigma(P(\alpha)) = P(\sigma(\alpha))$, donc $\sigma(\alpha)$ est bien une racine de P dans M.

Soit $\beta \in M$ une racine, une des propositions précédentes montre qu'il existe un unique élément $\sigma \in \mathrm{Isom}_k(k(\alpha), k(\beta))$ tel que $\sigma(\alpha) = \beta$, donc il existe bien un élément $\mu \in \mathrm{Isom}_k(L,M)$ tel que $\mu(\alpha) = \beta$. Comme $\mu(\alpha) = \beta$, on a $\mu(k(\alpha)) \subset k(\beta)$, on a nécessairement $\mu = \sigma$.

□

Théorème.— (Steiniz) *Soit k un corps et $\overline{k}$ une clôture algébrique. Soit K/k une extension algébrique et $\sigma \in \mathrm{Isom}_k(K,\overline{k})$. Si L/K est une extension algébrique, alors il existe $\widetilde{\sigma} \in \mathrm{Isom}_k(L,\overline{k})$ tel que $\widetilde{\sigma}_{|K} = \sigma$.*

Preuve: Examinons pour commencer le cas monogène $L = K(a)$. Soit $P = \mathrm{Min}_K(a)$ et soit $\alpha \in overlinek$ une racine du polynôme $\sigma(P) \in \overline{k}[X]$. On vérifie alors, comme dans la prop ???, que l'application $\widetilde{\sigma} : K(a) \to \overline{k}$ donnée par $\widetilde{\sigma}(x) = \sigma(x)$ pour $x \in K$ et $\widetilde{\sigma}(a) = \alpha$ définie bien l'élément $\widetilde{\sigma} \in \mathrm{Isom}_k(L,\overline{k})$ recherché.

Pour le cas général, considérons l'ensemble $\mathcal{E}$ des couples $(K_0, \widetilde{\sigma}_{K_0})$ où K_0 est une extension intermédiaire de L/K et $\widetilde{\sigma}_{K_0} \in \mathrm{Isom}_k(K_0,\overline{k})$ tel que la restriction de $\widetilde{\sigma}_{K_0}$ à K soit égale à σ. On ordonne $\mathcal{E}$ de la manière suivante, $(K_0, \widetilde{\sigma}_{K_0}) \leq (K_1, \widetilde{\sigma}_{K_1})$ ssi $K_0 \subset K_1$ et la restriction de $\widetilde{\sigma}_{K_1}$ à K_0 vaut $\widetilde{\sigma}_{K_0}$. L'ensemble ordonné $(\mathcal{E}, \leq)$ est alors inductif. En effet, prenons $(K_i, \widetilde{\sigma}_{K_i})_i$ une chaîne dans $\mathcal{E}$ et considérons $M = \bigcup_i K_i$. L'ensemble M est un corps (puisqu'il s'agit d'une chaine) et c'est une extension intermédiaire de L/K. Sur M définissons $\widetilde{\sigma}$ par :

$$\widetilde{\sigma}(x) = \widetilde{\sigma}_{K_i}(x) \text{ si } x \in K_i$$

L'application $\widetilde{\sigma}$ est bien définie puisque $(K_i, \widetilde{\sigma}_{K_i})_i$ est une chaîne, c'est un élément de $\mathrm{Isom}_k(M,\overline{k})$ dont la restriction à K est σ. Ainsi le couple $(M, \widetilde{\sigma}) \in \mathcal{E}$ est un majorant de la chaîne $(K_i, \widetilde{\sigma}_{K_i})_i$, c'est-à-dire que $\mathcal{E}$ est inductif. Le lemme de Zorn affirme alors qu'il existe dans $\mathcal{E}$ un élément $(K_0, \widetilde{\sigma}_{K_0})$ maximal. Si $K_0 \neq L$ alors il existe $a \in L - K_0$ et d'après le cas monogène, il existe un élément $\mu \in \mathrm{Isom}_k(K_0(a),\overline{k})$ tel que $\mu_{|K_0} = \widetilde{\sigma}_{K_0}$. Mais alors, $\mu_{|K} = \sigma$ et donc $(K_0(a), \mu) \in \mathcal{E}$ et $(K_0, \widetilde{\sigma}_{K_0}) < (K_0(a), \mu)$ ce qui contredit la maximalité de $(K_0(a), \mu)$.

□

Si K_1 et K_2 sont deux extensions d'un même corps k, on dira que K_1 et K_2 sont k-isomorphes s'il existe un k-isomorphisme bijectif de K_1 sur K_2.

Corollaire.— (Steiniz) *Si K_1 et K_2 sont deux clôtures algébriques d'un même corps k, alors K_1 et K_2 sont k-isomorphes.*

Preuve: D'après ce qui précède, il existe des éléments$\sigma_1 \in \mathrm{Isom}_k(K_1,K_2)$ et $\sigma_2 \in \mathrm{Isom}_k(K_2,K_1)$. Comme $\sigma_2 \circ \sigma_1 \in \mathrm{Isom}_k(K_1,K_1) = \mathrm{Aut}_k(K_1)$ on a donc σ_2 surjective et, par suite, σ_2 définit un k-isomorphisme bijectif de K_2 sur K_1.

□

Les clôtures algébriques d'un corps K donnée sont donc toutes K-isomorphes. C'est pour ceci que l'on parlera de *la clôture algébrique*, $\overline{K}$, de K pour désigner un choix arbitraire d'une clôture.

Corollaire.— *Soit L/K une extension algébrique. Toute clôture algébrique de K est une clôture algébrique de L et réciproquement.*

Preuve: Exercice.

□

7.2.4 Extensions transcendantes

On rappelle que, si K désigne un corps, le corps $K(X)$ est défini comme étant le corps des fractions de l'anneau de polynômes $K[X]$.

Proposition.— *Soit K/k une extension et $\alpha \in K$. Les propositions suivantes sont équivalentes :*

i) α *est transcendant,*

ii) $[k(\alpha) : k] = +\infty$,

iii) $\dim_k k[\alpha] = +\infty$,

iv) $k(\alpha) \neq k[\alpha]$,

v) Φ_α *est injectif,*

vi) $k(\alpha)$ *est k-isomorphe à $k(X)$.*

Preuve: L'équivalence des propriétés i) à v) est juste la reformulation du théorème de caractérisation de l'algébricité.

$v) \Rightarrow vi)$ Comme Φ_α est injective et que $k[\alpha]$ est engendré par les α^n on en déduit que Φ_a est un k-isomorphisme de $k[X]$ sur $k[\alpha]$ qui induit donc un k-isomorphisme bijectif de $k(X)$ sur $k(\alpha)$.

$vi) \Rightarrow ii)$ Soit φ un k-isomorphisme bijectif de $k(X)$ dans $k(\alpha)$. C'est en particulier un isomorphisme de k-espaces vectoriels, donc $\dim_k k(\alpha) = \dim_k k(X) = +\infty$.

□

Un argument de cardinalité permet de montrer que dans l'extension $\mathbb{C}/\mathbb{Q}$ il existe des nombres transcendants. En effet, $\mathbb{Q}$ est dénombrable, donc pour tout $n \geq 0$, l'ensemble $\mathbb{Q}_n[X]$ des polynômes rationnels de degré $\leq n$ est dénombrable puisque ce dernier ensemble est équipotent à un produit fini $\mathbb{Q} \times \cdots \times \mathbb{Q}$ ($n+1$ fois) d'ensembles dénombrables. Maintenant comme $\mathbb{Q}[X]$ est la réunion dénombrable des ensembles $\mathbb{Q}_n[X]$, il est lui-même dénombrable.

Chaque polynôme $P \in \mathbb{Q}[X]$ a un nombre fini de racines, donc l'ensemble des complexe qui sont algébriques sur $\mathbb{Q}$ est dénombrable. Or $\mathbb{C}$ ne l'est pas, donc il existe des nombres complexes transcendants sur $\mathbb{Q}$.

On remarque que la "quantité" de nombres complexes transcendants sur $\mathbb{Q}$ est "colossale" (puisque indénombrable). Une facon de mieux voir cette idée est de considérer les nombres réels algébriques sur $\mathbb{Q}$, comme ils sont dénombrables ils forment un ensemble de mesure nulle au sens de Lebesgue sur $\mathbb{R}$. Ainsi, si l'on prend un réel au hazard, il est transcendant...

7.2.5 Corps de rupture et corps de décomposition

Définition.— *Soit k un corps et $P \in k[X]$ un polynôme irréductible. On appelle corps de rupture de P toute extension K/k telle que :*

- *K/k algébrique,*
- *P admet une racine dans K,*
- *P n'admet aucune racine dans les extensions intermédiaires strictes de K/k.*

Proposition.— *Soit k un corps et $P \in k[X]$ un polynôme irréductible. On a :*

- *$k[X]/(P)$ est un corps de rupture de P,*
- *une corps K est un corps de rupture de P ssi il existe $\alpha \in K$ tel que $P(\alpha) = 0$ et $K = k(\alpha)$,*
- *deux corps de ruptures de P sont k-isomorphes.*

Preuve: • Puisque P est irréductible, l'anneau $k[X]/(P)$ est bien un corps et l'injection canonique $k \to k[X]$ se factorisant, on en déduit que $k[X]/(P)$ est une extension de k. Posons $n = d^\circ P$ et $\alpha = \overline{X}$. Il est clair que $1, \alpha, \cdots, \alpha^{n-1}$ est une base de $k[X]/(P)$ vu comme k-espace vectoriel. Par ailleurs, il est aussi clair que $P(\alpha) = 0$.

Supposons qu'il existe une sous-extension stricte M de $k[X]/(P)$ admettant une racine β de P. On a $[M : k] < n$ et donc $d^\circ \mathrm{Min}_k(\beta) < n$, mais comme P est annulateur de β on a alors que $\mathrm{Min}_k(\beta)$ divise P strictement ce qui est absurde puisque P est irréductible et que $\mathrm{Min}_k(\beta)$ n'est pas constant.

• Soit K/k une extension et $\alpha \in K$ tel que $P(\alpha) = 0$ et $K = k(\alpha)$. Pour montrer que K est un corps de rupture, il suffit de montrer que P n'a pas de racine dans unze sous-extension stricte. Supposons donnée une telle sous-extension M avec $\beta \in M$ tel que $P(\beta) = 0$. Comme $[M : k] < [K : k] = d^\circ P$, on en déduit que $d^\circ \mathrm{Min}_k(\beta) < d^\circ$, ce qui, comme précédement, est absurde.

Réciproquement, soit K un corps de rupture. Il existe donc $\alpha \in K$ tel que $P(\alpha) = 0$. Si $K \neq k(\alpha)$, alors $k(\alpha)$ est une sous-extension stricte de K/k où P possède une racine ce qui est contraire au fait que K est un corps de rupture.

• Soit K/k un corps de rupture de P et $\alpha \in K$ une racine de P. On sait donc que $K = k(\alpha) = k[\alpha]$. Considérons l'application $\varphi : k[X] \to K$ donnée par $\varphi(Q) = Q(\alpha)$. Le morphisme φ est surjectif et son noyau est précisément (P), on en déduit donc que $K = k(\alpha) = k[\alpha] \simeq k[X]/(P)$, le dernier isomorphisme étant visiblement un k-isomorphisme. Donc tout les corps de ruptures sont k-isomorphes à $k[X]/(P)$.

□

Corollaire.— *Soit k un corps, K/k une extension et $P \in k[X]$ un polynôme irréductible. Dans K, il y a au plus n corps de ruptures où n désigne le nombre de racines de P dans K.*

Preuve: Immédiat.

□

Définition.— *Soit k un corps et $P \in k[X]$ un polynôme. On appelle corps de décomposition (ou corps des racines) de P toute extension K/k telle que :*

• *K/k algébrique,*

• *P est totalement décomposé dans K,*

• *P n'est totalement décomposé dans aucune extensions intermédiaires strictes de K/k.*

Proposition.— *Soit k un corps, $\overline{k}$ une clôture algébrique de k et $P \in k[X]$ un polynôme irréductible. Dans $\overline{k}$, P ne possède qu'un seul corps de décomposition, c'est le corps $K = k(\alpha_1, \cdots, \alpha_n)$ où $\alpha_1, \cdots, \alpha_n \in \overline{k}$ sont tels que $P(X) = a(X - \alpha_1) \cdots (X - \alpha_n)$ dans $\overline{k}[X]$.*

Preuve: Soit K un corps de décomposition de P dans $\overline{k}$. On a donc $k(\alpha_1, \cdots, \alpha_n) \subset K$, comme dans $k(\alpha_1, \cdots, \alpha_n)$, P se décompose totalement, on en déduit bien que $K = k(\alpha_1, \cdots, \alpha_n)$.

□

Corollaire.— *Soit k un corps et $P \in k[X]$ un polynôme irréductible. Tous les corps de décomposition de P sont k-isomorphes et si K désigne un tel corps alors $[M : k] \leq n!$ avec $n = d^\circ P$.*

Preuve: Soit K_1 et K_2 deux corps de décompositions de P et $\overline{K_1}$ et $\overline{K_2}$ des clôtures algébriques de K_1 et K_2. Puisque K_1/k et K_2/k sont des extensions algébriques, on en déduit que $\overline{K_1}$ et $\overline{K_2}$ sont des clôtures algébriques de k et par le théorème de Steiniz, $\overline{K_1}$ et $\overline{K_2}$ sont k-isomorphes. Soit $\varphi : \overline{K_1} \to \overline{K_2}$, un k-isomorphisme (bijectif). Le corps $\varphi(K_1)$ est un sous-corps de $\overline{K_2}$ où P se décompose totalement, donc $K_2 \subset \varphi(K_1)$. De même, on a $K_1 \subset \varphi^{-1}(K_2)$, mais comme $[K_1 : k] = [\varphi(K_1) : k]$ et $[K_2 : k] = [\varphi^{-1}(K_2) : k]$, donc $K_2 = \varphi(K_1)$ et $K_1 = \varphi^{-1}(K_2)$, ce qui montre bien que K_1 et K_2 sont k-isomorphes.

Soit $K = k(\alpha_1, \cdots, \alpha_n)$ un corps de décomposition de P. On a $[k(\alpha_1) : k] = n$. Le polynôme minimal de α_2 sur $k(\alpha_1)$ est un diviseur de P, c'est forcément un diviseur strict puisque P n'est plus irréductible sur $k(\alpha_1)$. Donc $[k(\alpha_1, \alpha_2) : k(\alpha_1)] \leq n - 1$, et par récurrence, on en déduit que pour tout $i = 1, \cdots, n-1$, $[k(\alpha_1, \cdots, \alpha_{i+1}) : [k(\alpha_1, \cdots, \alpha_i)] \leq n - i$. Maintenant, comme

$$[k(\alpha_1, \cdots, \alpha_n) : k] = [k(\alpha_1, \cdots, \alpha_n) : k(\alpha_1, \cdots, \alpha_{n-1})]. \cdots . [k(\alpha_1) : k]$$

on trouve bien $[K : k] \leq 2.3. \cdots .n = n!$.

□

7.3 Corps finis

7.3.1 Théorème de Wedderburn

Pour tout entier $n \in \mathbb{N}^*$, on note $\Phi_n(X) = \prod_{\xi}(X-\xi)$ (ξ parcourt l'ensemble des racines primitives n-ième de l'unité) le n-ième polynôme cyclotomique. On rappelle que $\Phi_n(X)$ est un polynôme irréductible de $\mathbb{Z}[X]$.

Lemme.— *Soit n et d deux entiers. Les propositions suivantes sont équivalentes :*

i) d divise n,

ii) $X^d - 1$ *divise* $X^n - 1$ *dans* $\mathbb{Z}[X]$.

et dans cette situation, si $d < n$ *alors* $\Phi_n(X)$ *divise* $\dfrac{X^n-1}{X^d-1}$ *dans* $\mathbb{Z}[X]$.

Preuve: Si $n = kd$, alors

$$X^n - 1 = (X^d - 1)(1 + X^d + X^{2d} + \cdots + X^{(k-1)d})$$

Donc $X^d - 1$ divise $X^n - 1$ dans $\mathbb{Z}[X]$.

Réciproquement, si $X^d - 1$ divise $X^n - 1$, en particulier, les racines de $X^d - 1$ dans $\mathbb{C}$ sont des racines de $X^n - 1$. Soit ξ une racine primitive d-ième de l'unité, $\xi^d - 1 = 0$ donc $\xi^n - 1 = 0$ donc $n = kd$.

Soit ξ une racine primitive n-ième de l'unité. Comme $d < n$, $\xi^d - 1 \neq 0$, donc ξ est racine de $\dfrac{X^n-1}{X^d-1}$. Ceci étant valable pour toutes les racines primitives n-ièmes de l'unité et comme $\Phi_n(X)$ et $\dfrac{X^n-1}{X^d-1}$ sont des polynômes normalisés, $\Phi_n(X)$ divise $\dfrac{X^n-1}{X^d-1}$ dans $\mathbb{Z}[X]$.

□

Lemme.— *Soit p un nombre premier et* $k \in \mathbb{N}^*$. *Posons* $q = p^k$. *Si n et d sont deux entiers alors les propositions suivantes sont équivalentes :*

i) d divise n,

ii) $q^d - 1$ *divise* $q^n - 1$.

Preuve: Si $n = kd$, d'après le lemme précèdant, en évaluant les polynômes en $X = q$, on a $q^d - 1$ divise $q^n - 1$ dans $\mathbb{Z}$.

Réciproquement supposons que $q^d - 1$ divise $q^n - 1$ dans $\mathbb{Z}$. On a donc $q^n \equiv 1[q^d - 1]$. Effectuons la division euclidienne de n par d: on a $n = kd + r$ avec $k \in \mathbb{N}$ et $0 \leq r < d$. Supposons que $r \neq 0$, on a $q^n = q^{kd}.q^r$, mais comme $q^{kd} \equiv 1[q^d - 1]$ on a $q^n = q^{kd}.q^r \equiv q^r[q^d - 1]$ et donc $q^r \equiv 1[q^d - 1]$. Mais $q^d - 1$ ne peut pas diviser $q^r - 1$ car $q^r - 1 < q^d - 1$. Donc $r = 0$ et d divise n.

□

Théorème.— (Wedderburn) *Tout corps fini est commutatif.*

Preuve: Soit F un corps fini et $Z = Z(F)$ son centre. Le corps F est donc un Z-espace vectoriel et si $q = \sharp Z$ alors $\sharp F = q^n$ avec $n = \dim_Z F$.

Sur F^*, on définit la relation d'équivalence $\simeq$ par:

$$\forall (x, x') \in F^*,\ x \simeq x' \Longleftrightarrow \exists y \in F^* / \ x' = yxy^{-1}$$

Pour $x \in F^*$, on pose $N(x) = \{y \in F / \ yx = xy\}$.

$N(x)$ est un sous-corps de F contenant Z. Donc, on a $\sharp N(x) = q^{\delta(x)}$ avec $\delta(x) = \dim_Z N(x)$ (on a $\delta(x) = n$ si et seulement si $x \in Z^*$).

Soit $x \in F^*$. On note $\bar{x}$ la classe d'équivalence de x modulo $\simeq$. Il est clair que l'on a $\bar{x} = \{yxy^{-1} / \ y \in F^*\}$. Sur F^* on introduit la relation d'équivalence $\equiv$ définie par

$$y \equiv y' \text{ ssi } yxy^{-1} = y'xy'^{-1}$$

Il est clair que $\sharp \bar{x} = \sharp(F^* / \equiv)$. Maintenant

$$y \equiv y' \Longleftrightarrow y'^{-1} y \in N(x)'^*$$

Par conséquent le cardinal des classes d'équivalences de $\equiv$ vaut exactement $\sharp N(x)^*$, et par suite on a $\sharp\bar{x} = \dfrac{\sharp F^*}{\sharp N(x)^*}$. En particulier, comme $\sharp N(x)^* = q^{\delta(x)} - 1$ et que $\sharp F^* = q^n - 1$, on a $q^{\delta(x)} - 1$ divise $q^n - 1$, ce qui implique d'après le lemme que $\delta(x)$ divise n.

Les classes d'équivalence définissent une partition, donc on a:

$$\sharp F^* = \sum_{i=1}^{h} \sharp\bar{x}_i$$

et donc:

$$q^n - 1 = \sum_{i=1}^{h} \frac{q^n - 1}{q^{\delta(x_i)} - 1}$$

Si $x_k \in Z^*$, alors $\bar{x}_k = Z^*$. Alors x_k est le seul des x_i pour lequel $\delta(x_k) = n$. Dans ce cas $\sharp x_k = \sharp Z^* = q - 1$. On en déduit donc que:

$$q^n - 1 = q - 1 + \sum_{i/\ \delta(x_i)<n} \frac{q^n - 1}{q^{\delta(x_i)} - 1}$$

D'après le lemme

$$\Phi_n(q) \text{ divise } q^n - 1 \text{ et } \frac{q^n - 1}{q^{\delta(x_i)} - 1}$$

pour $\delta(x_i) < n$. On déduit que $\Phi_n(q)$ divise $q - 1$.

Si ξ est une racine primitive n-ième de l'unité alors si $n > 2$, $\xi \notin \mathbb{R}$. Posons $\xi = \alpha + i\beta$, avec $(\alpha, \beta) \in \mathbb{R}^2$. On a

$$\begin{array}{rcccl} |q-\xi|^2 & = & (q-\alpha)^2 + \beta^2 & = & q^2 + \alpha^2 + \beta^2 - 2\alpha q \\ & = & q^2 + 1 - 2\alpha q & > & q^2 + 1 - 2q \\ & = & |q-1|^2 & & \end{array}$$

ceci parce que $|\xi_n| = 1 = \alpha^2 + \beta^2$ et que $\alpha < 1$ (sinon ξ est réel). Ainsi $|q - \xi| > |q - 1|$ et par suite $|\Phi_n(q)| > |q - 1|$, donc

$$\frac{|q-1|}{|\Phi_n(q)|} < 1$$

ce qui est absurde car ce nombre est un entier positif non nul.

Si $n = 2$, alors $\xi_2 = -1$ et à nouveau $|q - \xi_2| > |q - 1|$ ce qui est absurde pour les mêmes raisons que précédemment.

On en déduit que $n = 1$ et donc que $F = Z$, c'est à dire que F est commutatif.

7.3.2 Corps finis

Si F désigne un corps fini alors sa caractéristique est un nombre premier p et par suite $\sharp F = p^n$ avec $n = \dim_{\mathbb{Z}/p\mathbb{Z}} F$. Réciproquement:

Théorème.— *Pour tout nombre premier p et tout entier $n \in \mathbb{N}$, il existe un unique corps fini (à isomorphisme près) de cardinal $q = p^n$. On note $\mathbb{F}_q$ ce corps.*

Preuve: Montrons tout d'abord qu'un tel corps existe. Notons $\overline{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{Z}/p\mathbb{Z}$ (elle est unique à isomorphes près, d'après le théorème de Steiniz). Le polynôme $P(X) = X^q - X$ a une dérivée égale à

$$P'(X) = qX^{q-1} - 1 = -1$$

(nous sommes en caractéristique p). Sa dérivée étant égale à une constante, P est premier avec sa dérivée. Donc P n'a que des racines simples dans $\overline{\mathbb{F}}_p$. Soit F l'ensemble de ces racines. Il est clair que F est un corps, car: si $(x, y) \in F^2$ alors $(x.y)^q = x^q.y^q = x.y$ donc $x.y \in F$, si $x \neq 0$ alors

$$(x^{-1})^q = (x^q)^{-1} = x^{-1}$$

et donc $x^{-1} \in F$,

$$(-x)^q = -x^q = -x$$

donc $-x \in F$ et enfin

$$(x+y)^q = \sum_{k=0}^{q} C_q^k x^k + y^{q-k} = x^q + y^q = x + y$$

(car C_q^k est divisible par p donc nul dans $\overline{\mathbb{F}}_p$ pour $k = 1, \cdots, q-1$) et donc $(x+y) \in F$.

Comme $\sharp F = q$, F est bien un corps à q éléments. Notons au passage que c'est le corps de décomposition dans $\overline{\mathbb{F}}_p$ du polynôme $X^q - X$.

Prenons maintenant un corps F' de cardinal q. Grâce au théorème de Wedderburn, on sait que F' est commutatif. Il est de caractéristique p, sa clôture algébrique est isomorphe à $\overline{\mathbb{F}}_p$, il est donc isomorphe à un sous-corps de $\overline{\mathbb{F}}_p$. On peut donc le voir directement comme un sous corps de $\overline{\mathbb{F}}_p$ (ceci veut dire qu'une fois choisie $\overline{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$, F' est isomorphe, modulo le choix d'un isomorphisme entre $\overline{\mathbb{F}}_p$ et $\overline{F}'$, à un sous-corps de $\overline{\mathbb{F}}_p$).

Maintenant, pour tout $x \in F'$, $x^q = x$. En effet, F étant un corps, F^* est un groupe multiplicatif d'ordre $q-1$. D'après le théorème de Lagrange, si $x \in F^*$, alors $x^{q-1} = 1$ et par suite $x^q = x$. Il est clair que $x = 0$ vérifie aussi cette égalité.

Comme $\sharp F = q$ il s'ensuit que F' est le corps de décomposition du polynôme $X^q - X$ dans $\overline{\mathbb{F}}_p$. Mais comme il y a unicité du corps de décomposition on en déduit que $F' = F = \mathbb{F}_q$.

□

Proposition.— *Soit p un nombre premier et $n, m \in \mathbb{N}^*$. Posons $q = p^n$ et $q' = p^m$. Les propositions suivantes sont équivalentes :*

i) $\mathbb{F}_{q'}$ est une extension de $\mathbb{F}_q$,

ii) il existe $k \in \mathbb{N}^*$ tel que $m = kn$.

Preuve: $i) \Rightarrow ii)$ $\mathbb{F}_{q'}$ étant une extension de $\mathbb{F}_q$, on peut le voir comme $\mathbb{F}_q$-espace vectoriel, sa dimension $k > 0$ sur $\mathbb{F}_q$ est finie sinon le corps serait infini. On a donc $q' = q^k$, c'est à dire que $m = kn$.

$ii) \Rightarrow i)$ Supposons $m = kn$. Si $x \in \mathbb{F}_q$ alors $x^q = x$ et donc par récurrence, $x^{q^k} = x$ c'est-à-dire $x^{q'} = x$ c'est-à-dire $x \in \mathbb{F}_{q'}$.

□

Proposition.— *Le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique. De manière générale, si K est 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.

□

Proposition.— *Un corps fini n'est jamais algébriquement clos.*

Preuve: Soit $F = \{x_1, \cdots, x_n\}$ un corps fini. Considérons le polynôme $P(X) = (X - x_1) \cdots (X - x_n) + 1$, c'est un polynôme de degré n et qui vérifie $P(x) = 1 \neq 0$ pour tout $x \in F$. Donc F n'est pas algébriquement clos.

□

7.4 Notion de séparabilité

Définition.— • *Soit k un corps et $P \in k[X]$ un polynôme irréductible. On dit que P est séparable si P ne possède que des racines simples dans $\overline{k}$.*

• *Un élément algébrique α d'une extension L/K est dit séparable, si $\mathrm{Min}_K(\alpha)$ est un polynôme séparable.*

• *Une extension algébrique L/K est dite séparable si tout les éléments de L sont séparables.*

Proposition.— *Soit k un corps et $P \in k[X]$ un polynôme irréductible non constant. Les propositions suivantes sont équivalentes :*

i) P est séparable,

ii) $P' \neq 0$.

Preuve: $ii) \Rightarrow i)$ Si $P' \neq 0$ alors comme P est irréductible et que $d^\circ P' < d^\circ P$, P et P' sont premier entre eux, donc n'ont pas de racine commune dans $\overline{k}$, donc P est à racines simples.

$i) \Rightarrow ii)$ Si $P' = 0$, alors $car(k) = p \neq 0$. Il existe donc un polynôme $Q \in k[X]$ tel que $P(X) = Q(X^p)$. Le polynôme Q étant non constant possède dans $\overline{k}$ une racine α. On a donc $P(X) = (X^p - \alpha)Q_1(X^p)$. Soit maintenant β une racine dans $\overline{k}$ de $X^p - \alpha$. On a $X^p - \alpha = X^p - \beta^p = (X - \beta)^p$ et donc β est racine d'ordre au moins p de P, c'est-à-dire que P n'est pas séparable.

□

Corollaire.— *Soit k un corps et $P \in k[X]$ un polynôme irréductible.*

• *Si $car(k) = 0$ alors P est séparable. En particulier, toute extension algébrique en caractéristique nulle est séparable.*

• *Si $car(k) = p$, alors il existe un entier n et un polynôme $Q \in k[X]$ irréductible et séparable tel que $P(X) = Q(X^{p^n})$. En particulier, les racines de P dans $\overline{k}$ ont toutes la même multiplicité.*

Preuve: • c'est évident.

• Si P est séparable, alors on prend $Q = P$ et $n = 0$. Sinon, il existe $P_1 \in k[X]$ tel que $d^\circ P_1 \geq 1$ et tel que $P(X) = P_1(X^p)$. Le polynôme P_1 est irréductible, sinon P ne le serait pas. Si le polynôme P_1 est séparable, on prend $Q = P_1$ et $n = 1$, sinon on recommence : il existe $P_2 \in k[X]$ irréductible tel que $d^\circ P_2 \geq 1$ et tel que $P_1(X) = P_2(X^p)$ etc. Cette récurence est finie, car $d^\circ P_{i+1} = d^\circ P_i - p$ et chaque P_i est non constant. Soit n l'indice pour lequel P_n est séparable, on prend alors $Q = P_n$ et on a bien $P(X) = Q(X^{p^n})$ avec Q irréductible et séparable.

Soit $\alpha_1, \cdots, \alpha_m$ les racines de Q dans $\overline{k}$. Elles sont distinctes deux à deux. Pour tout $i = 1, \cdots, m$ prenons β_i une racine de $X^{p^n} - \alpha_i$. Les β_i sont distinctes deux à deux et on a:

$$\begin{aligned} P(X) &= Q(X^{p^n}) = A\prod_{i=1}^{m}(X^{p^n} - \alpha_i) = A\prod_{i=1}^{m}(X^{p^n} - \beta_i^{p^n}) \\ &= A\prod_{i=1}^{m}(X - \beta_i)^{p^n} = A\left(\prod_{i=1}^{m}(X - \beta_i)\right)^{p^n} \end{aligned}$$

ce qui justifie que les β_i sont les racines de P et que leur ordre est p^n pour tout $i = 1, \cdots, m$.

□

Exemples : a) Considérons un nombre premier p et le corps $k = \mathbb{F}_p(T)$. Le polynôme $P(X) = X^p - T$ est irréductible dans $k[X]$ par application du critère d'Eisenstein. On voit que $P' = 0$ et par suite, P ne possède qu'une seule racine dans $\overline{k}$ (que l'on peut, par exemple, noter $T^{1/p}$ ou $\sqrt[p]{T}$) qui est donc d'ordre p.

Dans le même ordre d'idée, si l'on prend un entier $k \geq 1$ premier avec p et un entier $l \geq 1$ et que l'on considère le polynôme $P(X) = X^{kp^l} - T \in k[X]$, on voit que P est irréductible et qu'il possède k racines distinctes d'ordre p^l.

b) Une extension algébrique L/K de caractéristique 0 est toujours séparable, puisque tous les polynômes irréductibles de $K[X]$ sont séparables.

c) L'extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ est toujours séparable. En effet, un élément $x \in \mathbb{F}_{q^n}$ non nul est racine du polynôme $P(X) = X^{q^n-1} - 1$ qui est à racines simples puisque $P'(X) = -X^{q^n-2}$ ne s'annule qu'en 0. Comme $\mathrm{Min}_{\mathbb{F}_q}(x)$ est un diviseur de P, il est lui-même à racines simples et donc x est séparable.

Lemme.— *Soit K un corps et $\overline{K}$ sa clôture algébrique. L'ensemble E des éléments de $\overline{K}$ séparables sur K est un sous-corps de $\overline{K}$.*

Preuve: Admis.

□

Définition.— *L'ensemble des éléments séparables sur K s'appelle la clôture séparable de K et se note K^{sep}. Le corps K est dit parfait si $K^{sep} = \overline{K}$.*

Proposition *Soit K un corps de caractéristique p. Les propositions suivantes sont équivalentes:*

i) K est parfait,

ii) l'endomorphisme $x \mapsto x^p$ est surjectif.

Preuve: $i) \Rightarrow ii)$: Soit $a \in K$. Considérons le polynôme $P(X) = x^p - a$ et L son corps de décomposition sur K. Comme K est parfait, L/K est séparable et par suite galoisienne. Soit $b \in L$ une racine de P. Comme $P(b) = 0$, son polynôme minimal divise donc $P(X) = (X-b)^p$ et comme b est séparable, ce polynôme est $X - b$ ce qui prouve que $b \in K$.

$ii) \Rightarrow i)$: Soit $P \in K[X]$ un polynôme irréductible et inséparable. On a alors $P(X) = \sum_{i=0}^{n} a_i X^{ip}$. Soit $b_i \in K$ tel que $a_i = b_i^p$, on a donc:

$$P(X) = \sum_{i=0}^{n} (b_i X^i)^p = \left(\sum_{i=0}^{n} b_i X^i \right)^p$$

ce qui est contraire à l'irréductibilité de P.

□

Exemples : a) Tout corps de caractéristique nulle est parfait.

b) Les corps finis sont parfaits.

c) Le corps $\mathbb{F}_p(T)$ n'est pas parfait.