الجمهورية الجزائرية الديموقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Minstère de l'Enseignement Supérieur et de la Recherche Scientifique

CENTRE UNIVERSITAIRE DE MILA
INSTITUT DES SCIENCES ET DE LA TECHNOLOGIE

Réf. ***/11***

Mémoire de fin d'étude
Présenté pour l'obtention du diplôme de

Licence Académique

Domaine : **Mathématiques et Informatique**
Filière : **Mathématiques**
Spécialité : **Mathématiques Fondamentales**

Thème

Localisation d'un Anneau et Corps de Fractions

Présenté par :

- **Bouayad Aya**
- **Seddiki Assia**

Dirigé par :

- **Mr: Bouguebina Mounir**

Année universitaire 2010-2011

Remerciements

Louange à* dieu *tout puissant de nous avoir aidé, éclairé le chemin pour achever notre travail et nos études.

Nos remerciements à nos très chers parents, frères, sœurs, collègues et amis respectifs qui nous ont encouragés, soutenu durant tout notre parcours.

Un remerciement particulier à notre

encadreur Mr Bouguebina Mounir pour sa présence, son aide et surtout

pour ses précieux conseils qui nous

ont assistés pour l'accomplissement de notre mémoire.

Nous tenons à exprimer nos sincères remerciements à tout le personnel de l'institut de sciences et de la technologie surtout les enseignants qui nous ont enseigné durant toutes nos années d'étude.

Enfin nous remercions toutes les personnes qui ont contribué de prés ou de loin à l'achèvement de ce travail.

Merci bien.

Localisation d'un Anneau et Corps de Fractions

Bouayad Aya et Seddiki Assia

19 mai 2011

Table des matières

Introduction

La localisation est une technique de construction qui généralise la construction du corps des fractions d'un anneau intègre. Si S est un sous-ensemble d'un anneau commutatif A, qui est stable pour la multiplication, alors l'ensemble des fractions formelles (a, s) où a est un élément quelconque de A et s est un élément quelconque de S forme un nouvel anneau commutatif ; l'addition, la soustraction, la multiplication et l'égalité étant définies sur ce nouvel ensemble de la même façon que pour les fractions ordinaires. Le nouvel anneau est noté $S^{-1}A$ et est appelé la localisation de A par rapport à S. Un exemple illustrant ce qui précède est la localisation de l'anneau des nombres entiers au sous-ensemble des nombres entiers impairs stable par multiplication. Le corps des nombres rationnels est la localisation de l'anneau commutatif des nombres entiers à l'ensemble stable par multiplication de nombres entiers non nuls.

Chapitre 1

Groupes, Anneaux et Corps

Dans ce premier chapitre on rapelle brièvement les notions de groupes, d'anneau et de corps dont nous aurons besoin par la suite. Un attention toute particulière est donnée aux idéaux dans un anneau et notamment aux idéaux premiers et maximaux. Les corps qui sont des anneaux particuliers ne feront leur apparition qu'au chapitre 3.

1.1 Loi de Composition interne

Soit E un ensemble. Une loi de composition interne $*$ sur E est une application $E \times E \longrightarrow E$ qui à deux éléments $x, y \in E$, associe un troisième élément $x * y$. On dit aussi que $*$ est une opération sur E et on parle du couple $(E, *)$.

Exemple

1) $* =$ addition dans $\mathbb{N}, \mathbb{Z}$ ou $\mathbb{Q}$.

2) $* = \cup$ ou $\cap$ dans $E = P(A)$, l'ensemble des parties d'un ensemble quelconque A.

Propriétés

1) On dit que $*$ est associative si :

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

2) On dit que $*$ est commutative si :

$$x * y = y * x, \forall x, y \in E.$$

3) Soit $e \in E$. On dit que e est un élément neutre pour $*$ si :

$$x * e = e * x = x, \forall x \in E.$$

Si e existe, il est alors unique. En effet supposons que $e^{'}$ soit un autre élément neutre. On a alors : $e * e^{'} = e$ ($e^{'}$ est élément neutre) et $e * e^{'} = e^{'}$ (e est élément neutre) et donc $e = e^{'}$. Un couple $(E, *)$ ayant un élément neutre est appelé monoide.Par exemple $(\mathbb{N}, +)$ est un monoide d'élément neutre 0.
4) Soit e un élément neutre de $(E, *)$. Soient $x, x^{'}$ deux éléments de E. On dit que $x^{'}$ est le symétrique de x pour la loi $*$ si :

$$x * x^{'} = x^{'} * x = e.$$

Le symétrique , s'il existe, est unique si $*$ est associative. En effet si $x^{'}$ et $x^{''}$ sont deux symétriques de x, on a : $x^{''} = e * x^{''} = (x^{'} * x) * x^{''} = x^{'} * (x * x^{''}) = x^{'} * e = x^{'}$.

Exemple
1) Dans $(\mathbb{N}, +)$, aucun élément autre que 0 n'a de symétrique. Le symétrique de 0 est 0.
2) Dans $(\mathbb{Z}, +)$, tout élément a un symétrique : le symétrique de x est $-x$.
3) Dans $(\mathbb{Z}, \times)$, l'élément neutre est 1 et c'est le seul élément qui ait un symétrique.

1.2 Groupes

Soit $(G, *)$ un ensemble G muni d'une loi de composition interne $*$.

Définition 1 *: $(G, *)$ est un groupe si*
- $*$ *est associative.*
- $*$ *admet un élément neutre e.*
- *tout élément x de G admet un symétrique $x^{'}$ pour $*$.*

Si $*$ est commutative, on dit que $(G, *)$ est un groupe commutatif ou abélien.

Exemple
1) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ sont des groupes. L'élément neutre est 0 et le symétrique de x est $-x$. L'associativité est évidente.
2) $(\mathbb{N}, +)$ n'est pas un groupe car aucun élément autre que 0 n'a de symétrique.
3) $(\mathbb{Z}, \times)$ n'est pas un groupe. La multiplication est associative dans $\mathbb{Z}$

d'élément neutre 1, mais si $x \neq 1$, alors x n'a pas de symétrique.
4) $(\mathbb{Q}^* = \mathbb{Q} - \{0\}, \times)$ est un groupe ainsi que $(\mathbb{R}^* = \mathbb{R} - \{0\}, \times)$. L'élément neutre est 1 et le symétrique de x est $x^{-1} = \frac{1}{x}$

Définition 2 *: Soit $(G, *)$ un groupe et soit H une partie non vide de G. On dit que H est un sous-groupe de G si :*
- *H est stable pour la loi $*$: $x, y \in H \Rightarrow x * y \in H$.*
- *muni de la loi $*$, H est lui-même un groupe.*

Notation : $H < G$
Remarque : En pratique pour montrer que H est un sous-groupe de G, il suffit de vérifier que $x, y \in H \Rightarrow xy^{-1} \in H$. Remarquer aussi que G et H ont même élément neutre : $e_G = e_H$.
Exemple
1) Pour $* = +$, on a des inclusions de sous-groupes : $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$.
2) Pour $* = \times$, on aussi des inclusions : $\{1\} < \{-1, 1\} < \mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$.
3) Tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $n\mathbb{Z}$ pour $n \in \mathbb{N}$. En effet $n\mathbb{Z}$ est clairement un sous-groupe de $\mathbb{Z}$. Inversement soit H un sous-groupe de $\mathbb{Z}$. Soit n le plus petit élément positif non nul de H. Si $x \in H$, la division euclidienne de x par n donne $x = kn + r$ avec $k \in \mathbb{Z}$ et $0 \leq r < n$. Comme H est un sous-groupe, on doit avoir $x - kn = r \in H$. Par définition de n, on doit avoir $r = 0$ et $x = kn$. Donc $H = n\mathbb{Z}$.

Définition 3 *: Soient $(G, *)$ et $(H, \perp)$ deux groupes. Une application $f : G \longrightarrow H$ est un morphisme de groupes si :*

$$f(x * y) = f(x) \perp f(y)$$

$\forall x, y \in G$.

Autrement dit f préserve les structures de groupes de G et H. Si f est bijective, on dit que c'est un isomorphisme. Si $G = H$ et $* = \perp$, on parle d'endomorphisme et d'automorphisme. Noter que $f(e_G) = e_H$. Le noyau du morphisme f est :

$$Kerf = \{x \in G : f(x) = e_H\} = f^{-1}(e_H).$$

C'est un sous-groupe de G. Le noyau est utile pour detecter si f est injective ou non. En effet on a : f injective $\Leftrightarrow$Kerf=$\{e_G\}$. Par exemple le morphisme

$f : \mathbb{Z} \longrightarrow \mathbb{Z}$ donné par $f(x) = 3x$ est injectif puisque $Kerf = \{0\}$ (la loi de groupe est l'addition).

Soit $(G, *)$ un groupe et soit H un sous-groupe de G. On définit une relation sur G par :

$$x \Re y \Leftrightarrow x - y \in H.$$

On vérifie facilement que $\Re$ est une relation d'équivalence. On a donc l'ensemble quotient, ensemble des classes d'équivalence :

$$\frac{G}{\Re} = \frac{G}{H} = \{\overline{x}, x \in G\}.$$

Définissons $\overline{*}$ par $\overline{x} \ \overline{*} \ \overline{y} = \overline{x * y}$. On a donc une loi $\overline{*}$ sur $\frac{G}{H}$ qui devient ainsi un groupe (commutatif si G l'est) appelé le groupe quotient de G par H. En effet :

- l'associativité de $\overline{*}$ découle de celle de $*$ par définition.
- l'élément neutre de $\overline{*}$ est $\overline{e}$ avec e l'élément neutre de $*$.
- le symétrique de $\overline{x}$ est $\overline{x'}$ avec x' le symétrique de x.

On a automatiquement un morphisme surjectif canonique de groupes :

$$\phi : G \longrightarrow \frac{G}{H}$$

qui à x associe $\overline{x}$, de noyau $Ker\phi = H$.

Exemple : On prend $(G, *) = (\mathbb{Z}, +)$ et $H = n\mathbb{Z}$ avec $n \in \mathbb{N}$. On a $x \Re y \Leftrightarrow x - y \in n\mathbb{Z} \Leftrightarrow x \equiv y \ mod(n)$ et :

$$\frac{G}{H} = \frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Convention : Dans la suite un groupe $(G, *)$ sera noté multiplicativement : $* = .$ et $e_G = 1$. Le symétrique x' de x sera noté x^{-1}. Si la loi est commutative, on le notera additivement : $* = +$, $e_G = 0$ et le symétrique x' de x sera noté $-x$.

1.3 Anneaux

Soit A un ensemble muni de deux lois de composition interne $+$ et $.$.

Définition 4 *: On dit que le triplet $(A, +, .)$ est un anneau si :*

- $(A, +)$ *est un groupe abélien d'élément neutre* 0_A.
- *La loi* . *est associative et admet un élément neutre* $1_A \neq 0_A$.
- *La loi* . *est distributive à gauche et à droite par rapport à la loi* + : $\forall x, y, z \in A$, *on a :*

$$x.(y + z) = x.y + x.z$$

$$(x + y).z = x.z + y.z$$

Si la loi . *est commutative, l'anneau est dit commutatif ou abélien.*

Remarque
1) On a appelé ici anneau ce que d'autres appelent anneau unitaire : autrement dit dans la définition d'un anneau, la loi . n'est pas obligée d'avoir un ément neutre 1_A. Comme les anneaux que nous allons rencontrer sont tous unitaires, cela ne pose pas vraiment de problème.
2) Dans un anneau, on a $0_A.x = 0_A$, $\forall x \in A$. En effet : $0_A.x = (x - x).x = x.x - x.x = 0_A$.
Exemple
1) $(\mathbb{Z}, +, .), (\mathbb{Q}, +, .)$ et $(\mathbb{R}, +, .)$ sont des exemples bien connus d'anneaux commutatifs.
2) Soit $A = P(E)$ l'ensemble des parties d'un ensemble E. On prend $+ = \cup$ et $. = \cap$. $(A, +, .)$ est alors un anneau commutatif avec $0_A = \emptyset$ et $1_A = E$.

Définition 5 *: Soit* $(A, +, .)$ *un anneau soit* B *une partie de* A *contenant* 1_A *et stable pour les lois* + *et* . *. On dit que* B *est un sous-anneau de* A *si muni de ces deux lois* B *est lui-même un anneau.*

Remarquer que la condition $1_A \in B$ est necessaire. Par exemple $2\mathbb{Z}$ n'est pas un sous-anneau de $\mathbb{Z}$ car il ne contient pas 1. Par contre $B = \{a + b\sqrt{2}, a, b \in \mathbb{Z}\}$ est un sous-anneau de $(\mathbb{Q}, +, .)$. Dans la pratique pour montrer que B est un sous-anneau de A, il suffit de vérifier que $1_A \in B$ et que $\forall x, y \in B$, on a $x - y$ et $x.y \in B$.

Définition 6 *: Une partie* I *d'un anneau* A *est appelé idéal à gauche (respectivement à droite) si :*

- I *est un sous-groupe de* $(A, +)$.
- $\forall a \in A, \forall x \in I : a.x \in I$ *(respectivement* $x.a \in I$.

Si I *est un idéal à gauche et à droite à la fois de* A*, on dit que c'est un idéal bilatère de* A.

Remarque
1) Si A est commutatif, les idéaux à gauche et à droite coincident.
2) $\{0_A\}$ et A sont des idéaux de A. Ils sont appelés idéaux triviaux. Les autre idéaux de A sont dits propres.
3) Un idéal de A n'est pas forcément un sous-anneau de A, car il ne contient pas en général 1_A. Plus précisément on a :

$$1_A \in I \Leftrightarrow I = A.$$

4) Dans la suite, on va considérer uniquement des anneaux commutatifs. On dira donc anneau pour anneau commutatif.
Exemple
1) Soit A un anneau et soit $a \in A$. Alors l'ensemble $I = aA = \{a.x, x \in A\}$ est un idéal de A. On l'appelle l'idéal principal engendré par a. L'anneau A sera dit principal si tous ses idéaux sont principaux.
2) $(\mathbb{Z}, +, .)$ est un anneau principal. En effet, on a vu que tous les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ pour $n \in \mathbb{N}$ et ce sont donc les seuls idéaux de $\mathbb{Z}$.
3) L'intersection d'un nombre quelconque idéaux est un idéal. Plus généralement l'intersection de tous les idéaux contenant une partie G de A est un idéal. On l'appelle l'idéal engendré par la partie G. Ses éléments sont les sommes finies $\sum_{k=1}^{n} a_k x_k$ avec $a_k \in A$ et $x_k \in G$.
4) la somme de deux idéaux I_1 et I_2 est l'ideal $I_1 + I_2 = \{x+y, x \in I_1, y \in I_2\}$. On peut aussi le définir comme étant l'idéal engendré par$I_1 \cup I_2$. En particulier il contient I_1 et I_2 De manière plus générale la somme $\sum_\lambda I_\lambda$ d'une famille d'idéaux I_λ est le plus petit idéal de A contenat chacun des I_λ
5) Le produit de deux idéaux I et J est l'idéal IJ engeendré par les produits $x.y$ avec $x \in I$ et $y \in J$. Concrètement ses éléments sont les sommes finies $\sum x_i.y_i$ avec $x_i \in I$ et $y\{i \in J$.

Soient $a, b \in A$. On dit que a divise b ou que b est un multiple de a s'il existe $c \in A$ avec $b = ac$. L'idéal $I = aA$ est donc l'ensemble des multiples de a. Remarquer que a divise b si et seulement si $bA \subset aA$. Un élément a est une unité s'il a un inverse a^{-1} pour la multiplication. a est dit premier ou irréductible si $a = bc$ implique que b ou c est une unité. $a \neq 0$ est un diviseur de 0 s'il existe $b \neq 0$ tel que $a.b = 0$. Les anneaux qui n'ont pas de diviseurs de zéro sont appelés des anneaux intègres. Par exemple dans $\mathbb{Z}$, les éléments premiers sont (au signe prés) les nombres premiers p. L'equation $a.b = 0$ n'a pas de solution non nulle dans $\mathbb{Z}$ qui est donc un anneau intègre.

Définition 7 *: Un idéal propre I d'un anneau A est dit premier si $ab \in I$ implique $a \in I$ ou $b \in I$. I est dit maximal s'il n'est contenu dans aucun autre idéal propre de A.*

Proposition 1 *: Un idéal maximal est premier. Les idéaux premiers de $\mathbb{Z}$ sont de la forme $p\mathbb{Z}$ avec p un nombre premier et ils sont tous maximaux.*

Preuve : Soit I un idéal maximal. Soient $a, b \in A$ avec $ab \in I$. Supposons que $a \notin I$. Alors l'idéal $I + aA$ est égal à A, car I est maximal. Il existe alors $d \in I$ et $x \in A$ avec $d + a.x = 1$ et donc $d.b + a.b.x = b \in I$ (rappelons que A est commutatif). Ceci montre que I est premier. Tout idéal propre de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ avec $n \neq 0 \in \mathbb{N}$. Supposons que $n\mathbb{Z}$ premier. $ab \in n\mathbb{Z}$ implique $a \in n\mathbb{Z}$ ou $b \in n\mathbb{Z}$ s'écrit n divise ab implique n divise a ou n divise b, ce qui par le lemme de gauss veut dire que $n = p$ un nombre premier. Enfin $n\mathbb{Z} \subset m\mathbb{Z}$ si et seulement si m divise n. Ceci montre que tout idéal premier de $\mathbb{Z}$ est maximal.

Une application $f : A \longrightarrow B$ entre deux anneaux est un morphisme si :

$$f(x + y) = f(x) + f(y)$$

$$f(x.y) = f(x).f(y)$$

$$f(1_A) = 1_B$$

pour tous $x, y \in A$. Autrement dit f préserve les opérations d'anneau. Si f est de plus bijective, on dit que c'est un isomorphisme entre A et B. Si $A = B$, on parle d'endomorphisme et d'automorphismes, respectivement. Le noyau d'un morphisme f est :

$$Kerf = \{x \in A : f(x) = 0_B\} = f^{-1}(0_B).$$

C'est un idéal de A. L'image de f est :

$$Imf = \{f(x), x \in A\} = f(A).$$

C'est un sous-anneau de B.

Soit A un anneau et soit I un idéal de A. On définit une relation $\Re$ sur A par :

$$x \Re y \Leftrightarrow x - y \in I.$$

On verifie facilement que $\Re$ est une relation d'equivalence sur A. Sur l'ensemble quotient

$$\frac{A}{\Re} = \frac{A}{I} = \{\overline{x}, x \in A\},$$

on définit deux opérations $\overline{+}$ et $\overline{.}$ en posant : $\overline{x} \ \overline{+} \ \overline{y} = \overline{x+y}$ et $\overline{x} \ \overline{.} \ \overline{y} = \overline{x.y}$. Ces deux opérations sont bien définies et font de $\frac{A}{I}$ un anneau. C'est l'anneau quotient de A par I. Remarquer que $\overline{x} = x + I$. En particulier $\overline{0} = I$ est l'élément neutre de $\overline{+}$.

On a un morphisme canonique surjectif d'anneaux :

$$\phi : A \longrightarrow \frac{A}{I}$$

qui à x associe sa classe modulo I, $\overline{x} = x + I$ et de noyau $Ker\phi = I$. De plus il y a une correspondance bijective entre les idéaux J de A qui contiennent I et les idéaux $\overline{J}$ de $\frac{A}{I}$ donnée par $J = \phi^{-1}(\overline{J})$.
Exemple : On prend $A = \mathbb{Z}$ et $I = n\mathbb{Z}$. On a alors $x - y \in n\mathbb{Z} \Longleftrightarrow x \equiv y \ mod(n)$. L'ensemble quotient est donc l'ensemble des classes de congruence modulo n :

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

et les opérations d'anneau sont celles bien connues de l'addition et de la multiplication des congruences.

Proposition 2 *: L'idéal I est premier si et seulement si l'anneau quotient $\frac{A}{I}$ est intègre.*

Preuve : Un anneau est intègre s'il n'a pas de diviseurs de 0. Supposons I premier et soient $\overline{a}$ et $\overline{b}$ tels que $\overline{a}.\overline{b} = \overline{0}$. donc $a.b \in I$. Comme I est premier, cela veut dire que $a \in I$ ou $b \in I$, c'est à dire que $\overline{a} = \overline{0}$ ou que $\overline{b} = \overline{0}$ et donc que l'anneau quotient est intègre. Inversement supposons l'anneau quotient intègre et soient $a, b \in A$ avec $a.b \in I$. Donc $\overline{a}.\overline{b} = 0$ et donc $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$, c'est à dire que $a \in I$ ou $b \in I$. Ceci montre que I est premier.

1.4 Corps

Définition 8 *: Un corps K est un anneau non nul dans lequel tout élément différent de 0 a un inverse pour la multiplication.*

Ainsi $K^* = K - \{0\}$ muni de la loi de multiplication devient un groupe qu'on appelle groupe multiplicatif de K. On a déja rencontré des exemples de corps : $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, etc. Un sous corps de K est une partie L de K stable pour les lois + et . et qui est, pour ces lois, elle-même un corps. Par exemple $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$. Un corps K est automatiquement intègre. En effet soit $a.b = 0$ et supposons $a \neq 0$. On a alors $a^{-1}.a.b = b = 0$.
Remarque : Un corps K n'a pas d'idéal propre. Autrement dit les seuls idéaux de K sont $\{0\}$ et K lui-même. En effet soit I un idéal de K non nul et soit $x \neq 0 \in I$, alors $x^{-1}.x = 1 \in I$ et donc $I = K$. En particulier tout morphisme non nul $f : K \longrightarrow L$ entre deux corps est injectif puisque, $Kerf$ etant un idéal, il doit-être égal à $\{0\}$.

Proposition 3 *: Un idéal I d'un anneau A est maximal si et seulement si l'anneau quotient $\frac{A}{I}$ est un corps.*

Preuve : Supposons I maximal et soit $\overline{x} \neq \overline{0} \in \frac{A}{I}$. Nous devons montrer que $\overline{x}$ a un inverse pour la multiplication. Comme $\overline{x} \neq \overline{0}$, $x \notin I$. L'idéal $I + xA$ doit donc être égal à A car I est maximal. Il existe donc $a \in A$ et $b \in I$ avec $b + x.a = 1$ ou encore $x.a = 1 - b \in 1 + I = \overline{1}$. Ce qui veut dire que $\overline{x}.\overline{a} = \overline{1}$ et donc $\overline{x}$ a un inverse. Inversement supposons que $\frac{A}{I}$ est un corps. Pour montrer que I est maximal, il suffit de montrer que pour tout $x \notin I$, l'idéal $I + xA$ doit être égal à A. Pour cela il faut montrer que $1 \in I + xA$. Or $x \notin I$ équivaut à $\overline{x} \neq 0$ et donc $\overline{x}$ a un inverse $\overline{y}$: $\overline{x}.\overline{y} = \overline{1}$. Donc $xy \in 1 + I$ et $1 \in I + xA$.
Exemple : On a vu que les idéaux maximaux de $\mathbb{Z}$ sont de la forme $p\mathbb{Z}$ avec p un nombre premier. Donc pour tout nombre premier p, les congruences modulo p :

$$\frac{\mathbb{Z}}{pZ} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$$

forment un corps qu'on appelle le corps premier à p éléments et qu'on note $\mathbb{F}_p$.

Chapitre 2

Localisation d'un anneau

La localisation est une technique qui consiste à rendre certains éléments d'un anneau inversibles pour la multiplication. Etant donné un anneau A et une partie S de A, on voudrait construire un autre anneau B dans lequel les éléments de S deviennent inversibles. On voudrait aussi que cette construction soit la meilleure possible, ce qui, on le verra, va s'exprimer sous une forme de propriété universelle concernat A, B et S. Dans ce chapitre, nous allons présenter cette construction, énoncer ses principales propriétés et, surtout, en donner un certain nombre d'exemples pour montrer son utilité.

2.1 Construction de la localisation

Soit A un anneau et soit S une partie de A.

Définition 9 *: La partie S est dite multiplicative si :*
- $x \in S$ *et* $y \in S \Longrightarrow x.y \in S$.
- $1 \in S$.

Une partie S est donc multiplicative si elle est stable pour la multiplication et contient son élément neutre.

Exemple

1) Soit A un anneau et soit S la partie de A formée des éléments qui ne sont pas des diviseurs de 0. S est alors une partie multiplicative. En effet $1 \in S$ et si x et y ne sont pas des diviseurs de 0, leur produit $x.y$ n'est lui aussi pas un diviseur de 0.

2) Soit I un idéal (propre) premier de l'anneau A. La partie $S = A - I$ est

multiplicative. En effet $1 \notin I$ (sinon $I = A$ et I ne serait plus propre), donc $1 \in S$. De plus, comme I est premier, $x \notin I$ et $y \notin I$ implique $x.y \notin I$, ce qui équivaut à $x \in S$ et $y \in S$ implique $x.y \in S$.
3) Soit A un anneau et soit $f \in A$. La partie $S = \{f^n, n = 0, 1, 2, \ldots\}$ est clairement multiplicative.

Sur $A \times S = \{(a, s), a \in A, s \in S\}$, on définit une relation $\Re$ par :

$$(a, s)\Re(b, t) \Longleftrightarrow \exists u \in S : (a.t - b.s).u = 0.$$

Proposition 4 *: La relation $\Re$ est une relation d'équivalence.*

Preuve : Il faut montrer que la relation est réflexive, symétrique et transitive. Soit $(a, s) \in A \times S$. On a $(a.s - s.a).1 = 0$, donc $(a, s)\Re(a, s)$, ce qui montre la reflexivité. Soient $(a, s), (b, t) \in A \times S$ et supposons que $(a.t - b.s).u = 0$. Donc $(b.s - a.t).u = 0$, ce qui montre la symétrie. Supposons maintenant que $(a, s)\Re(b, t)$ et $(b, t)\Re(c, u)$. Il existe donc $v, w \in S$ tels que $(a.t - b.s).v = 0$ et $(b.u - c.t).w = 0$. En multipliant la première égalité par $u.w$ et la deuxième par $s.v$ et en les sommant, on élimine b et on obtient $(a.u - c.s).t.v.w = 0$. Comme $t.v.w \in S$, ceci montre que $(a, s)\Re(c, u)$ et donc la transitivité.

Définition 10 *: L'ensemble quotient $\frac{A}{\Re} = S^{-1}A$ est appelé la localisation de A par S ou encore l'ensemble des fractions de A par S. La classe $\overline{(a, s)}$ sera notée $\frac{a}{s}$ et est appelée la fraction de a par s.*

Sur S^{-1}, on définit une addition et une multiplication par les formules :

$$\frac{a}{s} + \frac{b}{t} = \frac{a.t + b.s}{s.t},$$

$$\frac{a}{s}.\frac{b}{t} = \frac{a.b}{s.t}.$$

Proposition 5 *: Ces deux opérations sont bien définies et font de $S^{-1}A$ un anneau.*

Preuve : Que les deux opérations soient bien définies veut dire qu'elles ne doivent pas dépendre du choix des représentants (a, s) et (b, t) des classes $\frac{a}{s}$ et $\frac{b}{t}$. Soient donc (a', s') et (b', t') deux autres représentant. Il nous faut montrer que

$$\frac{a}{s} + \frac{b}{t} = \frac{a'}{s'} + \frac{b'}{t'},$$

$$\frac{a}{s}.\frac{b}{t} = \frac{a^{'}}{s^{'}}.\frac{b^{'}}{t^{'}}.$$

On sait qu'il existe u, v tels que $(a.s^{'} - a^{'}.s).u = 0$ et $(b.t^{'} - b^{'}.t).v = 0$. Un calcul simple montre que $((a.t + b.s).s^{'}.t^{'} - (a^{'}.t^{'} + b^{'}.s^{'}).s.t).u.v = 0$, ce qui montre la première égalité. La deuxième se démontre de manière analogue. D'autre part on a :

$$\frac{a}{s} + \frac{0}{1} = \frac{a}{s},$$
$$\frac{a}{s}.\frac{1}{1} = \frac{a.1}{s.1} = \frac{a}{s}.$$

Donc $\frac{0}{1}$ est l'élément neutre de l'addition et $\frac{1}{1}$ est lélément neutre de la multiplication. Le symétrique de $\frac{a}{s}$ pour l'addition est $-\frac{a}{s}$. Enfin on vérifie facilement que l'addition et la multiplication sont associatives et commutatives et que la multiplication est distributive par rapport à l'addition.

On a un morphisme d'anneaux $f : A \longrightarrow S^{-1}A$ qui à x associe $\frac{x}{1}$ et qui n'est en général pas injectif. Remarquer que :

$$\frac{s}{1}.\frac{1}{s} = \frac{s.1}{1.s} = \frac{s}{s} = \frac{1}{1} = 1_{S^{-1}A}.$$

C'est dans ce sens qu'on dit que les éléments s de S (qu'on identifie aux fractions $\frac{s}{1}$) deviennent inversibles dans $S^{-1}A$.

L'anneau des fractions vérifie la propriété universelle suivante :

Proposition 6 *: Soit $g : A \longrightarrow B$ un morphisme d'anneau tel que $g(s)$ est une unité de B pour tout $s \in S$. Alors il existe un unique morphisme d'anneaux $h : S^{-1}A \longrightarrow B$ tel que $g = h \circ f$.*

Preuve : Montrons d'abord l'unicité. Si h satisfait les conditions de la proposition, on doit avoir :

$$h(\frac{a}{1}) = h(f(a)) = g(a).$$

Donc :

$$h(\frac{1}{s}) = h((\frac{s}{1})^{-1}) = h(\frac{s}{1})^{-1} = g(s)^{-1}.$$

Et enfin :

$$h(\frac{a}{s}) = h(\frac{a}{1}).h(\frac{1}{s}) = g(a).g(s)^{-1}.$$

Ainsi h est complètement determinée par g et donc unique. Montrons maintenant l'existence. Posons :

$$h(\frac{a}{s}) = g(a).g(s)^{-1}.$$

h sera clairement un morphisme d'anneaux pourvu qu'on montre qu'elle est bien définie, c'est à dire qu'elle ne dépend pas du représentant de la classe $\overline{(a,s)}$. Soient donc (a,s) et $(a^{'},s^{'})$ reliés par la relation $\Re$. Il existe $t \in S$ tel que $(a.s^{'} - a^{'}.s).t = 0$, donc :

$$(g(a).g(s^{'}) - g(a^{'}).g(s)).g(t) = 0.$$

Mais $g(t)$ est une unité dans B, donc :

$$g(a).g(s)^{-1} = g(a^{'}).g(s^{'}).$$

Remarque : Parmi les propriétés de $S^{-1}A$, on peut citer les trois suivantes :
1) $s \in S \Longrightarrow f(s)$ est inversible dans $S^{-1}A$;
2) $f(a) = 0 \Longrightarrow a.s = 0$ pour un certain $s \in S$;
3) Tout élément de $S^{-1}A$ est de la forme $f(a).f(s^{-1})$ pour un certain a et un certain $s \in S$.

En utilisant la proposition précédente, on peut montrer que réciproquement ces propriétés determinent l'anneau $S^{-1}A$ à isomorphisme prés :

Proposition 7 *: Soit $g : A \longrightarrow B$ un morphisme d'anneaux tel que :*

1. *$s \in S \Longrightarrow g(s)$ est une unité de B ;*
2. *$g(a) = 0 \Longrightarrow a.s = 0$ pour un certain $s \in S$;*
3. *Tout élément de B est de la forme $g(a).g(s)^{-1}$;*

alors il existe un unique isomorphisme $h : S^{-1}A \longrightarrow B$ tel que $g = h \circ f$.

Preuve : Par la proposition précédente, nous devons montrer que le morphisme $h : S^{-1}A \longrightarrow B$ défini par :

$$h(\frac{a}{s}) = g(a).g(s)^{-1},$$

est un isomorphisme. Notons d'abord que ce morphisme est bien défini car par la propriété 1) $g(s)$ est inversible. Par la propriété 3) ce morphisme

est clairement surjectif. Reste à montrer qu'il est injectif. Supposons que $h(\frac{a}{s}) = g(a).g(s)^{-1} = 0$. En multipliant à gauche par $g(s)$, on obtient $g(a) = 0$ et donc $a.t = 0$ pour un certain $t \in S$. Ceci veut dire que $(a, s)\Re(0, 1)$. Autrement dit, on a :

$$\frac{a}{s} = \frac{0}{1} = 0$$

dans $S^{-1}A$.

2.2 Etude de $S^{-1}A$

Soit $f : A \longrightarrow B$ un morphisme d'anneau. Soit J un idéal de B. On vérifie facilement que $f^{-1}(J)$ est un idéal de A.

Définition 11 *: L'idéal $f^{-1}(B)$ est appelé la contraction de J par le morphisme f. On le note J^c.*

Si J est premier alors J^c est aussi premier. En effet soient $x, y \in A$ avec $xy \in f^{-1}(J)$. Donc $f(xy) = f(x).f(y) = b \in J$. Comme J est premier, on doit avoir $f(x) \in J$ ou $f(y) \in J$ et donc $x \in f^{-1}(J)$ ou $y \in f^{-1}(J)$.

Si I est un idéal de A, son image $f(I)$ n'est en général pas un idéal de B. Par exemple prenons l'inclusion de $\mathbb{Z}$ dans $\mathbb{Q}$ et I un idéal non nul quelconque de $\mathbb{Z}$. $f(I)$ ne peut pas être un idéal de $\mathbb{Q}$ puisque celui-ci n'a pas d'idéaux propres.

Définition 12 *: L'extension I^e de I est l'idéal de B engendré par $f(I)$: $f(I)B$. C'est l'ensemble des sommes finies $\sum y_i f(x_i)$ avec $x_i \in I$ et $y_i \in B$.*

Si I est premier, I^e ne l'est pas necessairement (en prenant toujours l'exemple de l'inclusion de $\mathbb{Z}$ dans $\mathbb{Q}$, on a $I^e = \mathbb{Q}$ qui n'est pas premier pout tout idéal non nul de $\mathbb{Z}$).

Ces notions de contraction et d'extension vont nous permettre de determiner les idéaux et les idéaux premiers de S^{-1} en utlisant le morphisme canonique $f : A \longrightarrow S^{-1}A$.

Théorème 1 *: On a :*

1. *Tous les idéaux de $S^{-1}A$ sont de la forme $IS^{-1}A = I^e$ pour I un idéal de A.*

2. *Tout idéal premier de $S^{-1}A$ est de la forme $\wp S^{-1}A$ pour $\wp$ un idéal premier de A disjoint de S et inversement pour tout idéal premier $\wp$ de A disjoint de S, $\wp S^{-1}A$ est premier dans $S^{-1}A$*

Preuve : Prouvons d'abord *1.* Soit J un idéal de $S^{-1}A$. Posons $I = J^c$. Si $x = \frac{a}{s} \in J$, alors $x.f(s) = f(a) \in J$ et donc $a \in I$. Ainsi $x = (\frac{1}{s}).f(a) \in IS^{-1}A$. Ceci montre que $J \subset IS^{-1}A$. Comme J est un idéal, l'inclusion inverse $IS^{-1}A \subset J$ est évidente. En définitive on a $J = IS^{-1}A$. Passons maintenant à *2.* Soit P un idéal premier de $S^{-1}A$. Posons $\wp = P^c$. Alors $\wp$ est un idéal premier de A et on a $P = \wp S^{-1}A$. De plus comme P ne contient pas les unités de $S^{-1}A$ (sinon il contiendrait 1 et ne serait donc pas premier), on a $\wp \cap S = \emptyset$. Inversement soit $\wp$ un idéal premier de A disjoint de S. On a donc :

$$\frac{a}{s}.\frac{b}{t} \in \wp S^{-1}A \Longrightarrow r.a.b \in \wp$$

pour $s, t \in S$ et pour un certain $r \in S$. Comme $r \notin \wp$, on doit avoir $a \in \wp$ ou $b \in \wp$, ce qui veut dire que $\frac{a}{s} \in \wp S^{-1}A$ ou $\frac{b}{t} \in \wp S^{-1}A$. Ce qui montre que $\wp S^{-1}A$ est premier.

Le théorème suivant montre que la localisation commute au passage au quotient par les idéaux :

Théorème 2 *: Soit A un anneau et soient S une partie multiplicative de A et I un idéal de A. Notons par $\overline{S}$ l'image de S dans $\frac{A}{I}$. On a alors un isomorphisme :*

$$\frac{S^{-1}A}{IS^{-1}A} \cong \overline{S}^{-1}\frac{A}{I}.$$

Preuve : Les deux membres vérifient la propriété universelle pour les morphismes d'anneaux $g : A \longrightarrow C$ tels que :

- l'image de tout élément de S est une unité dans C.
- l'image de tout élément de I est nulle dans C.

Comme la solution à ce problème universel est unique, on en déduit l'isomorphisme précédent qui est donné explicitement par :

$$\overline{(\frac{a}{s})} \longmapsto \frac{\overline{a}}{\overline{s}},$$

avec $\overline{(\frac{a}{s})}$ la classe de $\frac{a}{s}$ modulo $IS^{-1}A$ et $\overline{a} = a + I$ et $\overline{s} = s + I$.

2.3 Exemples

2.3.1 S=Puissances de f

Soit A un anneau et soit $f \in A$. La partie $S = \{f^n, n \in \mathbb{N}\}$ est une partie multiplicative de A. En effet $1 = f^0 \in S$ et $f^n.f^m = f^{n+m} \in S$.

Définition 13 *: L'anneau $S^{-1}A$ est noté A_f. C'est l'anneau des inverse des puissances de f.*

Le théorème 1 nous permet de determiner les idéaux premiers de A_f :

Proposition 8 *: Les idéaux premiers de A_f correspondent aux idéaux premiers de A qui ne contiennent pas f.*

Preuve : Par le théorème 1 les idéaux premiers de $S^{-1}A$ correspondent aux idéaux premiers de A disjoints de S. Les idéaux de A_f correspondent donc aux idéaux de A disjoints de $S = \{f^n, n = 0, 1, 2, \ldots\}$. Supposons que l'intersection d'un idéal premier I avec S soit non vide. Il existe donc $n \neq 0$ tel que $f^n \in I$. Mais on a :

$$f^n \in I \Longleftrightarrow f \in I,$$

pour tout idéal premier I de A. Autrement dit les idéaux premiers de A non disjoints de S sont exactement ceux qui contiennent f.

Définition 14 *: Un élément f d'un anneau A est dit nilpotent s'il existe un entier $n \neq 0$ tel que $f^n = 0$.*

Si f est un élément nilpotent, l'anneau A_f n'est pas d'une grande utilité. En effet on a :

Proposition 9 *: Si f est nilpotent, l'anneau A_f est l'anneau nul :*

$$A_f = \{0\}.$$

Preuve : Nous allons montrer que de manière générale, si S contient 0 alors $S^{-1}A = \{0\}$. Rappelons que

$$0_{S^{-1}A} = \frac{0}{1} = \overline{(0,1)}.$$

Soit (a, s) un élément de $S \times A$. Nous devons montrer que $\overline{(a, s)} = \overline{(0, 1)}$. Comme S contient un élément $u = 0$, on a :

$$(a.1 - s.0).u = 0,$$

et donc :

$$\frac{a}{s} = \frac{0}{1}.$$

Ceci montre la proposition.

2.3.2 S=A-diviseurs de 0

Soit A un anneau et soit S la partie de A formée des éléments qui ne sont pas des diviseurs de 0. S est une partie multiplicative. En effet $a.1 = 0$ implique que $a = 0$, donc 1 n'est pas un diviseur de 0 et $1 \in S$. Soient $x, y \in S$. Supposons qu'il existe c tel que $x.y.c = 0$. Comme x n'est pas un diviseur de 0, on doit avoir $y.c = 0$ et comme y n'est pas un diviseur de 0, on a forcément $c = 0 =$. Donc $x.y$ n'est pas un diviseur de 0 et $x.y \in S$.

Définition 15 *: L'anneau $S^{-1}A$ est appelé l'anneau quotient total de A ou encore l'anneau des fractions total de A. On le note $K(A)$*

Cette partie S et la plus grande partie multiplicative de A telle que le morphisme canonique $f : A \longrightarrow S^{-1}A$ soit injectif comme le montre la proposition suivante :

Proposition 10 *: Le morphisme canonique $f : A \longrightarrow S^{-1}A$ est injectif si et seulement si S ne contient aucun diviseur de 0.*

Preuve Rappelons que le morphisme f associe à $x \in A$ lélément $\frac{x}{1} \in S^{-1}A$. Supposons f injectif. Soit $u \in S$ avec $a.u = 0$ pour $a \in A$. Donc $(a.1-0.1).u = 0$ et :

$$\frac{a}{1} = \frac{0}{1}.$$

Autrement dit $f(a) = f(0)$. Par injectivité de f, cela donne $a = 0$ et u n'est pas un diviseur de 0. Inversement supposons que S ne contient aucun diviseur de 0. $f(a) = f(b)$ s'écrit :

$$\frac{a}{1} = \frac{b}{1}.$$

Donc il existe $u \in S$ avec $(a.1-b.1).u = 0$. Comme u n'est pas un diviseur de 0, on doit avoir $a-b=0$ et donc $a=b$. Ceci montre que f est un morphisme injectif.
Remarque : On a donc une inclusion :

$$A \hookrightarrow K(A).$$

Si A est intègre (sans diviseurs de 0), On a $S = A^* = A - \{0\}$ et l'anneau $K(A)$ devient le corps de fractions de A. Ce sera le sujet du chapitre 3.

2.3.3 S=A-p

Soit A un anneau et soit $\wp$ un idéal premier de A. La partie $S = A - \wp$ est multiplicative. En effet $1 \in S$ car $1 \notin \wp$ puisque celui-ci est un idéal premier et donc propre. Si x et y n'appartiennent pas à $\wp$ alors $x.y$ n'appartient pas non plus à $\wp$. Donc $x \in S$ et $y \in S$ implique $x.y \in S$.

Définition 16 *: L'anneau $S^{-1}A$ est appelé la localisation de A en l'idéal premier $\wp$. On le note $A_\wp$.*

D'aprés le théorème 1, les idéaux premiers de $A_\wp$ correspondent bijectivement aux idéaux premiers de A disjoints de S et donc aux idéaux premiers de A contenus dans $\wp$.

posons :

$$M = \wp A_\wp = \{\frac{a}{s}, a \in \wp\}.$$

Remarque : Par définition un élément de $\wp A_\wp$ est une somme finie $\sum y_i f(x_i)$ avec $x_i \in \wp$ et $y_i \in A_\wp$. Comme $f(x_i) = \frac{x}{1}$, on a :

$$\sum y_i f(x_i) = \sum \frac{z_i}{t_i}.\frac{x_i}{1} = \sum \frac{z_i.x_i}{t_i}.$$

En réduisant au même denominateur et en utilisant le fait que $\wp$ est un idéal, on arrive à la deuxième égalité.

Proposition 11 *: M est un idéal maximal de $A_\wp$. De plus c'est le seul idéal maximal de $A_\wp$.*

Preuve : D'aprés le théorème 1 $\wp A_\wp$ est un idéal (premier) de $A_\wp$. Redémontrons quand même ce fait. Soient $\frac{a}{s}$ et $\frac{b}{t}$ deux éléments de M. Comme $a, b \in \wp$, on a $a.t - b.t \in \wp$, donc :

$$\frac{a}{s} - \frac{b}{t} = \frac{(a.t - b.s)}{st} \in M.$$

Ceci montre que M est un sous-groupe de $A_\wp$. Soient $\frac{a}{s} \in M$ et $\frac{b}{t} \in A_\wp$. Comme $a.b \in \wp$, on a :

$$\frac{a}{s}.\frac{b}{t} = \frac{a.b}{s.t} \in M.$$

Donc M est bien un idéal de $A_\wp$. Supposons maintenant que :

$$\frac{b}{t} \notin M.$$

Alors $b \notin \wp$ et donc $b \in S$. Cela veut dire que $\frac{b}{t}$ est une unité dans $A_\wp$. Donc si J est un idéal de $A_\wp$ qui n'est pas contenu dans M, alors J contient forcément une unité et donc $J = A_\wp$. Ceci montre du même coup que M est maximal et que c'est le seul idéal maximal de $A_\wp$.

Définition 17 *: On appelle anneau local tout anneau qui a un idéal maximal et un seul.*

Ainsi pour tout idéal premier $\wp$, l'anneau $A_\wp$ est local d'idéal maximal $\wp A_\wp$.

Exemple : On prend $A = \mathbb{Z}$ et $\wp = p\mathbb{Z}$ ave p un nombre premier. Le localisé $\mathbb{Z}_{p\mathbb{Z}}$ est noté $\mathbb{Z}_{(p)}$. Concrètement on a :

$$\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\},$$

et

$$M = \{\frac{a}{b} \in \mathbb{Q} : p \mid a, p \nmid b\}.$$

Remarque :
1) Ne pas confondre $\mathbb{Z}_{(p)}$ et $\mathbb{Z}_p$ qui est l'anneau des entiers p-adiques ensemble des suites (a_n) d'entiers définies modulo p^n et telles que $a_n + p^{n-1}\mathbb{Z} = a_{n-1}$.
2) On peut montrer, mais nous ne le ferons pas ici, qu'il y a un isomorphisme de corps :

$$\frac{\mathbb{Z}_{(p)}}{M} \cong \frac{\mathbb{Z}}{p\mathbb{Z}}.$$

2.4 Le spectre d'un anneau

Définition 18 *: L'ensemble de tous les idéaux premiers d'un anneau A est appelé le spectre de A. On le note $Spec(A)$.*

Soit I un idéal de A. On pose :

$$V(I) = \{\wp \in Spec(A) \mid I \subset \wp\}.$$

Proposition 12 *: On a :*

$$V(I) \cup V(J) = V(IJ),$$

et

$$\bigcap_{\lambda} V(I_\lambda) = V(\sum_{\lambda} I_\lambda).$$

pour tous idéaux I, J de A et pour toute famille d'idéaux $(I_\lambda)_\lambda$ de A.

Preuve : L'idéal IJ est par définition l'idéal engendré par les produits $x.y$ avec $x \in I$ et $y \in J$. C'est l'ensemble de toutes les sommes finies $\sum x_i y_i$ avec $x_i \in I$ et $y_i \in J$. Si $\wp$ contient I et J, il contient evidemment leur produit IJ. Inversement, supposons que $\wp$ contient IJ et supposons que $\wp$ ne contient pas J. Donc il existe $b \in J$ avec $b \notin \wp$. Pour tout $a \in I$, on a $a.b \in \wp$ et donc $a \in \wp$ puisque $\wp$ est premier. Donc $\wp$ contient I. Passons à la deuxième égalité. Rappelons que l'idéal $\sum I_\lambda$ est le plus petit idéal contenant tous les idéaux I_λ. Donc un ideal premier $\wp$ contient la somme des I_λ si et seulement si il contient chaque I_λ.

Ainsi l'ensemble des $V(I)$ pour I un idéal de I est fermé pour les unions finies et les intersections quelconques. On peut donc considérer la topologie sur $Spec(A)$ dont les fermés sont les $V(I)$. Remarquer que :

$$V(0) = SpecA,$$

et

$$V(A) = \emptyset$$

sont des fermés.

Définition 19 *: Cette topologie est appelée la topologie de Zariski de $Spec(A)$.*

On peut aussi décrire cette topologie en termes d'ouverts. Pour $a \in A$, posons :

$$D(a) = \{\wp \in Spec(A) \mid a \notin \wp\}.$$

On a alors :

Proposition 13 *: Les $D(a)$ pour $a \in A$ sont des ouverts et forment une base pour la topologie de Zariski sur $Spec(A)$.*

Preuve : On a $D(a) = Spec(A) - V(aA)$ avec aA l'idéal principal engendré par a. En effet $a \in \wp$ équivaut à $aA \subset \wp$. Donc $D(a)$ est ouvert comme complémentaire d'un fermé. Soit $U = Spec(A) - V(I)$ un ouvert de $Spec(A)$. On peut écrire

$$U = \bigcup_{a \in I} D(a)$$

comme une reunion d'ouverts $D(a)$. Ce qui montre que ces ouverts forment une base pour la topologie de Zariski.

Pour tout ouvert U de $Spec(A)$, on définit $F(U)$ comme étant l'ensemble des fonctions $s : U \longrightarrow \coprod_{\wp \in U} A_\wp$ telles que $s(\wp) \in A_\wp$ pour tout $\wp$ et telles que pour tout $\wp \in U$, il existe un voisinage V de $\wp$ contenu dans U, et des éléments $a, f \in A$, tels que pour tout $q \in V$, $f \notin q$ et $s(q) = \frac{a}{f}$ dans A_q. On vérifie facilement que la somme et le produit des fonctions s font de $F(U)$ un anneau commutatif unitaire (l'élément neutre 1 est la fonction 1 qui vérifie $1(\wp) = 1 \in A_\wp$). De plus si $V \subset U$ est une inclusion d'ouverts, on a un morphisme d'anneaux $F(U) \longrightarrow F(V)$ qui est tout simplement la restriction des fonctions s sur U à V. L'anneau $F(U)$ est souvent appelé l'anneau des fonctions régulières sur U.

Soit $f \in A$ et soit $D(f) = Spec(A) - V(fA)$. La proposition suivante montre qu'en fait $F(D(f))$ est un anneau de fractions :

Proposition 14 *: L'anneau $F(D(f))$ est isomorphe à A_f l'anneau des inverses des puissances de f. En particulier $F(Spec(A)) = A$.*

Preuve : L'isomorphisme ψ cherché est celui qui à $\frac{a}{f^n} \in A_f$ associe la fonction $s \in F(D(f))$ telle que $s(\wp) = \frac{a}{f^n}$ vu comme élément de $A_\wp$ (remarquer que comme $\wp \in D(f)$, $\wp$ ne contient pas f et donc $S = \{f^n, n \in \mathbb{N}\} \subset A - \wp$. Ainsi tout élement de A_f peut-être vu comme un élément de $A_\wp$). L'égalité $F(Spec(A)) = A$ résulte de l'isomorphisme puisque pour $f = 1$, on a $D(f) =$

$Spec(A)$ et donc $F(Spec(A)) = A_1 = A$. Montrons par exemple que ψ est injective. Nous laisserons la surjectivité au lecteur. Supposons que :

$$\psi(\frac{a}{f^n}) = \psi(\frac{b}{f^m}).$$

Donc pour tout $\wp \in D(f)$, il existe $h \in A$ avec $h \notin \wp$ et $(a.f^m - b.f^n).h = 0$ dans A. L'ensemble des annulateurs de $(a.f^m - b.f^n)$, c'est-à-dire des éléments $c \in A$ tels que $(a.f^m - b.f^n).c = 0$ est un idéal I de A. Donc $h \in I$ et $h \notin \wp$, ce qui veut dire que I n'est pas contenu dans $\wp$ pour tout $\wp \in D(f)$. Donc $V(I) \cap D(f) = \emptyset$. Ainsi f appartient à tout idéal premier contenat I. Autrement dit on a :

$$f \in \sqrt{I} = \{x \in A : \exists n \neq 0 : x^n \in I\}.$$

le radical de I. Il existe donc $l \in \mathbb{N}$ avec $f^l \in I$. Par définition de I on a :

$$(a.f^m - b.f^n).f^l = 0,$$

ce qui montre que :

$$\frac{a}{f^n} = \frac{b}{f^m}$$

dans A_f et donc ψ est injective.

Définissons maintenant l'ensemble $F_\wp$ comme étant l'ensemble des paires (U, s) avec U un ouvert de $Spec(A)$ et s un élément de $F(U)$ modulo la relation d'équivalence suivante : Deux paires (U, s) et (V, t) seront dites équivalentes s'il existe un ouvert W contenu dans $U \cap V$ tel que la restriction de s à W soit égale à la restriction de t à W. Un élément de $F_\wp$ est donc une fonction s définie dans un voisinage ouvert de $\wp$. L'addition et la multiplication des fonctions s font aussi de $F_\wp$ un anneau commutatif unitaire.

Définition 20 *: L'anneau $F_\wp$ est appelé l'anneau des germes de fonctions en $\wp$.*

Proposition 15 *: On a un isomorphisme $F_\wp \cong A_\wp$.*

Preuve : Définissons d'abord un morphisme $\phi : F_\wp \longrightarrow A_\wp$ en envoyant $s \in F(U)$ vers sa valeur $s(\wp) \in \mathrm{A}_\wp$. Tout élément de $A_\wp$ s'écrit sous forme

d'une fraction $\frac{a}{f}$ avec $a, f \in A$ et $f \notin \wp$. $D(f)$ est un voisinage ouvert de $\wp$ et on peut définir $s \in F(D(f))$ par :

$$s(\wp) = \frac{a}{f}.$$

Ceci montre que le morphisme ϕ est surjectif. Soit un voisinage ouvert de $\wp$ et soient $s, t \in F(U)$ telles que $s(\wp) = t(\wp)$. Si $s(\wp) = \frac{a}{f}$ et $t(\wp) = \frac{b}{g}$ avec $a, b, f, g \in A$ et $f, g \notin \wp$. On doit donc avoir :

$$\frac{a}{f} = \frac{b}{g}.$$

Cela veut dire qu'il existe $h \notin \wp$ tel que $(a.g - b.f).h = 0$ dans A. Donc l'égalité des deux fractions reste valable dans tout anneau loval A_q tel que $f, g, h \notin q$. L'ensemble de tels idéaux premiers q est l'intersection $D(f) \cap D(g) \cap D(h)$. C'est un ouvert qui contient $\wp$ et $s = t$ dans tout cet ouvert, ce qui montre que ϕ est injective. En conclusion ϕ est bien un isomorphisme.

Chapitre 3

Corps de fractions

Pour A un anneau intègre, la partie $S = A^* = A - \{0\}$ est clairement une partie multiplicative. On va montrer ici que l'anneau des fractions $S^{-1}A$ est en fait un corps qu'on appelle le corps des fractions de A. On va aussi montrer que le morphisme naturel $A \longrightarrow S^{-1}A$ est injectif ce qui permettra de voir A comme un sous-anneau de son corps des fractions. En fait la construction du corps de fractions est beaucoup plus simple que celle d'un anneau de fractions exposée en toute généralité dans le chapitre précédent. C'est pour cela que notre exposition du corps de fractions, bien que constituant un cas particulier du chapitre 2, sera plus directe et plus élémentaire.

3.1 Anneaux intègres

Soit A un anneau intègre (sans diviseur de zéro). On peut simplifier par les éléments de A non nuls : soient $a, b, c \in A$ tels que

$$ab = ac$$

Si $a \neq 0$, cette égalité devient

$$a(b - c) = 0$$

et donc $b - c = 0$ car a n'est pas un diviseur de zéro et on obtient

$$b = c.$$

Ainsi les éléments non nuls de A se comportent comme s'ils avaient des inverses c'est-à-dire comme les éléments d'un corps. On va voir que justement

on peut toujours plonger un anneau intègre dans un corps : son corps de fractions et tout élément non nul de l'anneau devient inversible (pour la multiplication) dans le corps. Remarquer qu'une condition nécessaire pour qu'un anneau soit un sous-anneau d'un corps est qu'il soit intègre (puisque dans un corps il n y a pas de diviseurs de 0).

On peut déja montrer que tout anneau intègre ayant un nombre fini d'éléments est en fait un corps :

Proposition 16 *: Tout anneau intègre A fini est un corps.*

Preuve : Nous devons montrer que tout élément non nul de A a un inverse pour la multiplication. Soit donc $a \neq 0 \in A$. Comme A est fini les éléments $a, a^2, a^3, \ldots$ ne sont pas tous distincts. Il existe donc des entiers naturels m, n tels que $a^m = a^n$ avec disons $m < n$. Donc :

$$a^m - a^n = 0$$

$$a^m - a^m a^{n-m} = 0$$

$$a^m(1 - a^{n-m}) = 0.$$

Comme A n'a pas de diviseurs de zéro et $a^m \neq 0$ on doit avoir

$$1 - a^{n-m} = 0$$

$$a^{n-m} = 1$$

$$a.a^{n-m-1} = 1.$$

Ainsi a^{n-m-1} est un inverse de a.

3.2 Corps de fractions

A partir d'un anneau intgre A on va construire un corps F qui va contenir A comme sous-anneau. Cette construction généralise immédiatement la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$. Pour cela on définit une relation $\Re$ sur $A \times A^*$ par :

$$(a, b)\Re(c, d) \Longleftrightarrow ad = bc.$$

Proposition 17 *: Cette relation est une relation d'équivalence.*

Preuve : On a toujours $ab = ba$ et donc $(a, b)(a, b)$. Ceci montre que la relation est reflexive. Soient $(a, b)\Re(c, d)$. Donc

$$ad = bc$$

$$da = cb$$

$$cb = da$$

et donc $(c, d)\Re(a, b)$. Autrement dit la relation est symétrique. Soient $(a, b), (c, d)et(e, f)$ avec $(a, b)\Re(c, d)$ et $(c, d)\Re(e, f)$. Donc

$$ad = bc \wedge cf = de$$

$$adf = bcf \wedge bcf = bde$$

$$daf = dbe$$

$$d(af - be) = 0.$$

Comme $d \neq 0$, on obtient $af - be = 0$ et $af = be$. Donc $(a, b)\Re(e, f)$ et la relation est transitive.

La classe d'équivalence de (a, b) sera notée :

$$\overline{(a, b)} = \frac{a}{b} = \{(c, d) \mid (a, b)\Re(c, d)\}.$$

et l'ensemble quotient sera noté :

$$F = \frac{A}{\Re} = \{\frac{a}{b}; (a, b) \in A \times A^*\}.$$

Sur F on défint une addition et une multiplication par :

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$\frac{a}{b}.\frac{c}{d} = \frac{ac}{bd}.$$

Remarquer que ces deux opérations sont bien définies c'est-à-dire qu'elles ne dépendent pas du choix des représentants des classes d'équivalence (elles sont d'ailleurs un cas particuliers des mêmes opérations définies dans le chapitre 2).

Théorème 3 *: Muni de ces deux opérations F est un corps commutatif.*

Preuve : L'addition est clairement associative et commutative. Son élément neutre est $\frac{0}{1}$:

$$\frac{a}{b} + \frac{0}{1} = \frac{a.1 + b.0}{b.1} = \frac{a}{b}$$

Le symétrique de $\frac{a}{b}$ est $\frac{-a}{b}$:

$$\frac{a}{b} + \frac{-a}{b} = \frac{a.b + b.(-a)}{b.b} = \frac{0}{b^2} = \frac{0}{1}.$$

La multiplication est clairement associative, commutative et distributive par rapport à l'addition. Son élément neutre est $\frac{1}{1}$:

$$\frac{a}{b}.\frac{1}{1} = \frac{a.1}{b.1} = \frac{a}{b}.$$

Il nous reste à montrer que tout élément non nul de F a un inverse pour la multiplication. Soit

$$\frac{a}{b} \neq \frac{0}{1}$$

dans F. Donc

$$a.1 \neq b.0$$

$$a \neq 0$$

et

$$\frac{b}{a} \in F.$$

De plus on a

$$\frac{a}{b}.\frac{b}{a} = \frac{a.b}{b.a} = \frac{1}{1}.$$

Tout élément non nul de F a donc bien un inverse.

Définition 21 *: Le corps F est appelé le corps de fractions de l'anneau intègre A.*

L'anneau A peut être vu comme un sous-anneau de F dans le sens suivant :

Proposition 18 *: Soit F le corps de fraction de l'anneau intègre A. Alors A est isomorphe à un sous-anneau de F.*

Preuve : Soit $\phi : A \longrightarrow F$ l'application définie par

$$\phi(a) = \frac{a}{1}$$

pour $a \in A$. Nous allons montrer que ϕ est un morphisme injectif. Pour tous $a, b \in A$, on a

$$\phi(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \phi(a) + \phi(b)$$

et

$$\phi(a.b) = \frac{a.b}{1} = \frac{a}{1}.\frac{b}{1} = \phi(a).\phi(b).$$

Donc ϕ est un morphisme d'anneaux. De plus on a

$$Ker\phi = \{a \in A : \phi(a) = 0\}$$

$$= \{a \in A : \frac{a}{1} = \frac{0}{1}\}$$

$$= \{a \in A : a.1 = 1.0\}$$

$$= \{a \in A : a = 0\}$$

$$= \{0\}.$$

Donc ϕ est injective et A s'identifie à son image $Im\phi$ qui est un sous-anneau de F. Autrement dit on identifie l'élément a de A avec l'élément $\frac{a}{1}$ de F :

$$a = \frac{a}{1}.$$

Remarque : Grâce à cette proposition on peut dire que F contient A. De plus on peut montrer que F est le plus petit (au sens de l'inclusion) corps contenant A. En effet soit K un corps contenant A. Pour tous éléments $a, b \in A$ avec $b \neq 0$, on a $b^{-1} \in K$ et aussi $ab^{-1} \in K$. Définissons maintenant une application $\psi : F \longrightarrow K$ par

$$\psi(\frac{a}{b}) = ab^{-1}.$$

ψ est bien définie : Si

$$\frac{a}{b} = \frac{c}{d}$$

on a $ad = bc$ et donc $ad.b^{-1}d^{-1} = bc.b^{-1}d^{-1}$ et $ab^{-1} = cd^{-1}$, ce qui donne

$$\psi(\frac{a}{b}) = \psi(\frac{c}{d}).$$

ψ est un morphisme puisqu'on a :

$$\begin{aligned}\psi(\frac{a}{b} + \frac{c}{d}) &= \psi(\frac{ad+bc}{bd}) \\ &= (ad+bc)(bd)^{-1} \\ &= (ad+bc)d^{-1}b^{-1} \\ &= ab^{-1} + cd^{-1} \\ &= \psi(\frac{a}{b}) + \psi(\frac{c}{d})\end{aligned}$$

et

$$\begin{aligned}\psi(\frac{a}{b}.\frac{c}{d}) &= \psi(\frac{ac}{bd}) \\ &= (ac)(bd)^{-1} \\ &= ac.d^{-1}b^{-1} \\ &= ab^{-1}.cd^{-1} \\ &= \psi(\frac{a}{b}).\psi(\frac{c}{d}).\end{aligned}$$

Un morphisme de corps étant automatiquement injectif, on peut regarder F comme un sous-corps de K.

3.3 Exemples

1) Le corps des nombres rationnels : On prend $A = \mathbb{Z}$. C'est clairement un anneau intègre. Son corps des fractions est le corps $\mathbb{Q}$ des nombres rationnels. Ainsi un nombre rationnel n'est pas vraiment un nombre, c'est plutôt une classe d'équivalence écrite sous forme de fraction :

$$\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}.$$

2) le corps des fractions rationnelles : Pour tout corps commutatif K, les polynômes à coefficients dans K forment un anneau intègre noté $K[X]$. Le corps des fractions de cet anneau estappelé le corps des fractions rationnelles

à coefficients dans K. On le note $K(X)$. Un élément de ce corps s'écrit sous forme d'une fraction :

$$\frac{a_n X^n + \ldots + a_1 X + a_0}{b_m X^m + \ldots + b_1 X + b_0},$$

avec les $a_i, b_j \in K$ et les b_j non tous nuls.

3) Les entiers de Gauss : L'anneau des entiers de Gauss est par définition l'ensemble

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\},$$

muni des restrictions de l'addition et de la multiplication dans $\mathbb{C}$. $\mathbb{Z}[i]$ est un anneau intègre trés utile en arithmétique . On remarque que -1 possède une racine carrée dans $\mathbb{Z}[i]$ et que $\mathbb{Z} \subset \mathbb{Z}[i]$. Le corps des fractions de $\mathbb{Z}[i]$ est donc le plus petit corps contenant $\mathbb{Z}$ et donc aussi $\mathbb{Q}$ et dans lequel -1 possède une racine carrée. C'est donc le corps :

$$\mathbb{Q}(i) = \{a + ib \mid a, b \in \mathbb{Q}\}.$$

Bibliographie

[1] S.Lang, Algebra, third edition, Springer, 2002.

[2] M.F.Atiyah, L.G.Macdonald, Introduction to commutative algebra, Addison-Wesley, 1969.

[3] N.Bourbaki, Eléments de Mathématiques, Algèbre, Hermann, Paris, 1965.

[4] B.L.Van Der Waerden, Modern algebra, Volume I, II, Frederick Ungar publishing Co, New York, 2008.