UNIVERSITE SIDI MOHAMED BEN ABDELLAH

FACULTE DES SCIENCES ET TECHNIQUES

Département des Mathématiques

Licence Sciences et Techniques (LST)

Mathématiques et Applications

MEMOIRE DE FIN D'ETUDES

Pour l'obtention du Diplôme de Licence Sciences et Techniques

Titre

Anneaux, Idéaux, corps et quaternions

Présenté par :

- *Mounir Souita*

Encadré par :

- *Pr Najib mahdou (FST)*
- *Pr Hassan oukili (FST)*

Soutenu Le 15 Juin 2015 devant le jury composé de:

- Pr Najib Mahdou

- Pr Aziza Rahmouni Hassani

-Pr Hassan oukili

Stage effectué à FST FES

Année Universitaire 2014 / 2015

FACULTE DES SCIENCES ET TECHNIQUES FES – SAISS

B.P. 2202 – Route d'Imouzzer – FES

212 (0)5 35 61 16 86 – Fax: 212 (0)5 35 60 82 14

Site web: http://www.fst-usmba.ac.ma

REMERCIEMENTS

Nous tenons avant d'aborder le développement de ce rapport, à Remercier mon encadrant, monsieur **Hassan Oukili** *de ma voir proposé ce thème.*

Nos remerciements vont aussi aux membres du jury **Pr Najib Mahdou et Pr Aziza Rahmouni Hassani** *qui nous ont honorés par leur présence.*

J'adresse également mes remerciements à toutes les professeures du Département Mathématiques qui ont contribué à mon formation pendant ces trois années de l'étude à FST de Fès

Enfin, je remercie tous ceux qui ont contribué à faciliter la tâche de notre travail, en prodiguant généralement leur aide accompagnée de sympathie et d'encouragements qu'ils trouvent ici l'expression de notre sincère gratitude

DEDICACE

Nous dédions ce modeste travail à nos pères et nos mères, qui nous ont supportés depuis le jour où ils nous ont eux au monde, qui nous ont initiées à l'art de vivre avec tout notre amour et respect.

A nos familles qui sont, et resteront toujours l'inspiration Joies et de la motivation de nos efforts.

A nos frères et nos sœurs, qui ont été nos meilleurs amis et nos Inséparables complices.

12 juin 2015

Table des matières

Chapitre 1

Anneaux, anneaux intègres

1.1 Anneaux

Définition. *Un anneau est un ensemble A muni de deux lois de composition internes, une notée additivement et l'autre multiplicativement telles que :*

i) *$(A,+)$ est un groupe commutatif ;c'est à dire que la loi de composition interne $+$ est associative, admet un élément neutre, et tout élément est symétrisable et commutatif dans A.*

ii) *$\times$ est une loi de composition interne associative dans A.*

iii) *$\times$ est distributive par rapport à la loi $+$.*

Exemple 1.1. *$(\mathbb{Z},+,.)$, $(\mathbb{Q},+,.)$, $(\mathbb{R},+,.)$, $(\mathbb{C},+,.)$ sont des anneaux commutatifs.*

Soit A un anneau, on a les proprietés suivantes :

a) Pour tout $a \in A$, $0a = 0$ (on dit que 0 est absorbant pour la multiplication)

b) si $e \in A$ est un élément tel que pour tout $a \in A$, $ea = a$, alors $e = 1$ (unicité de l'élément neutre pour la multiplication)

c) pour tout $a \in A$, on a $(-1)a = -a$.

d) Si $1 = 0$ dans A, alors $A = \{0\}$, on dit que A est l'anneau nul.

e) pour tout $a \in A$ et pour tous entiers $m, n \geq 0$, on a $a^{m+n} = a^m a^n$.

f) La formule du binome est valide : si a et $b \in A$ et $n \geq 0$, on a

$(a+b)^n = \sum_k^n \binom{n}{k} a^k b^{n-k}$

Définition. *Soit A un anneau et soit a un élément de A.*
On dit que a est inversible, ou que a est unité de A, s'il existe $b \in A$ tel que $ab = 1$. Un tel b est nécessairement unique, c'est l'inverse de a, on le note a^{-1}.
On dit que a est diviseur de zéro s'il existe $b \in A$, $b \neq 0$ tel que $ab = 0$.
On dit que a est simplifiable s'il n'est pas diviseur de zéro, c'est-à-dire si la relation $ab = 0$ avec $b \in A$ implique $b = 0$.
On dit enfin que a est nilpotent s'il existe $n \geq 1$ tel que $a^n = 0$.

Proposition. *L'ensemble des éléments inversibles d'un anneau A est un groupe pour la multiplication, on le note $U(A)$, c'est le groupe des unités de A.*

Démonstration. –Soit a et b deux éléments de A, d'inverses a^{-1} et b^{-1}. Alors
$(ab)(a^{-1}b^{-1}) = (aa^{-1})(bb^{-1}) = 1$, si bien que ab est inversible d'inverse $a^{-1}b^{-1}$. La multiplication de A définit ainsi une loi interne sur $U(A)$. De plus, 1 est inversible et est un élément neutre pour cette loi. Enfin, si $a \in U(A)$, son inverse pour cette loi n'est autre que a^{-1}. Ainsi, U(A) est un groupe pour la multiplication. □

Définition. *Soit A un anneau non nul.*
*On dit que A est **intègre** si : $\forall x, y \in A$, $xy = 0 \Longrightarrow x = 0$ ou $y = 0$.*
*On dit que A est **réduit** si 0 est le seul élément nilpotent de A.*
*On dit que A est un **corps** si tout élément non nul de A est inversible.*

Définition. *On dit que deux éléments a et b d'un anneau A sont **associés** s'il existe un élément inversible $u \in U(A)$ tel que $a = bu$.*

Proposition. *Soit A un anneau fini intègre. Alors, A est un corps.*

Démonstration. –Soit a un élément non nul de A. On doit prouver que a est inversible dans A . soit $\phi : A \to A$ l'application telle que $\phi(b) = ab$. Alors ϕ *est injective* : si $\phi(b) = \phi(b')$, on a $ab = ab'$, donc $a(b - b') = 0$. Comme A est intègre est $a \neq 0$,$(b - b') = 0$. Par suite, le cardinal de $\phi(A)$ est égale au cardinal de A. Comme $\phi(A)$ est une partie de A, $\phi(A) = A$. Ainsi, ϕ est surjective et il existe $b \in A$ tel que $ab = 1$. □

1.2 Sous-anneaux

Définition. *Soit A un anneau. Un sous-anneau de A est une partie $B \subset A$ contenant 0 , 1, stable par addition, passage à l'opposé et multiplication.*

Définition. *soit (A,+,×) un anneau et B un sous ensemble de A. Le sous ensemble B est dit un sous anneau de A si (B,+,×) est un anneau Ceci revient à :*

i) *(B, +) est un sous-groupe de (A, +), c'est-à-dire* $0 \in B$ *et* $\forall x, y \in B$ $(x - y) \in B)$

ii) *B stable pour la multiplication :* $\forall x, y \in B$, $xy \in B$.

iii) $1 \in B$.

Exemple 1.2. $\mathbb{Z}$ *est un sous-anneau de* $\mathbb{R}$.

Exemple 1.3. $\mathbb{Z}[i]$=*{a+ib,a,b* $\in \mathbb{Z}$*} est un sous-anneau de (*$\mathbb{C}$*,+,.)*

Remarque 1.1. ***1)*** *Le seul sous-anneau de* $\mathbb{Z}$ *est* $\mathbb{Z}$ *lui-même. En effet, si B est un sous-anneau de* $\mathbb{Z}$*, alors* $1 \in B$, $2 = 1 + 1 \in B$ *et* $\forall n \in \mathbb{N}^*$, $n = 1 + ... + 1 \in B$. $0 = 1 - 1 \in B$, *aussi* $\forall n \in \mathbb{N}^*$, $-n = 0 - n \in B$ *et ainsi* $B = \mathbb{Z}$.
2) *En général, un anneau B contenu dans un anneau A n'est pas nécessairement un sous-anneau de A (au sens des anneaux unitaires). L'anneau* $B = \{\overline{0}, \overline{2}, \overline{4}\}$ *n'est pas un sous-anneau de l'anneau* $A = \mathbb{Z}/6\mathbb{Z}$ *(au sens des anneaux unitaires) car* $1_A = \overline{1} \notin B$.
3) *sous-anneau d'un anneau intègre est intègre.*

1.3 Anneaux intègres

Définition. *Un anneau A est dit* ***intègre*** *si et seulement si :*

1) *A est commutatif.*

2) *A n'admet aucun diviseur de zéro.*

3) $A \neq \{0\}$.

Définition. *Soit A un anneau non nul. A est un anneau intègre si :*
$\forall x,y \in A, xy = 0 \Rightarrow x=0$ *ou* $y=0$.

Exemple 1.4. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *sont des anneaux intègres.*

Exemple 1.5. $(\mathbb{Z}/4\mathbb{Z}, +, .)$ *n'est pas intègre car* $\overline{2}.\overline{2} = \overline{4} = \overline{0}$ *mais* $\overline{2} \neq \overline{0}$.

1.4 Caractéristique d'un anneau

Définition. *Soit $(A,+,.)$ un anneau. Pour $n \in \mathbb{Z}$ et $a \in A$, on définit*

$$na=\begin{cases} \overbrace{a+\ldots+a}^{n fois} \text{ si } n>0 \\ 0 \text{ si } n=0 \\ \overbrace{(-a)+\ldots,(-a)}^{-n fois} \text{ si } n<0 \end{cases}$$

Si $n,m \in \mathbb{Z}$ et $a \in A$ alors $(n+m).a = na+ma$ et $(nm)a = n(ma)$. On définit ***la caractéristique d'un anneau*** *A comme étant le plus petit entier $n > 0$ tel que $n.1_A = 0_A$ si un tel entier existe. Sinon (i.e., si $\forall n \in \mathbb{N}^*$: $n.1_A \neq 0_A$), on dit que la caractéristique de l'anneau A est nulle. La caractéristique de l'anneau A est notée car(A).*

Exemple 1.6. ***1)*** *$car(\mathbb{Z}) = 0$*

2) *Si $n \geq 2$, $car(\mathbb{Z}/n\mathbb{Z}) = n$.*

1.5 Morphismes d'anneaux

Définition. *Soit A et B deux anneaux. Un homomorphisme d'anneaux $f : A \longrightarrow B$ est une application vérifiant les propriétés suivantes :*

- *on a $f(0) = 0$ et $f(1) = 1$.*

- *pour tous a et b dans A, on a $f(a+b) = f(a)+f(b)$ et $f(ab) = f(a)f(b)$.*

Le mot ***homomorphisme*** *est un synonyme pour morphisme. Si A est un anneau, l'application identique $Id_A : A \longrightarrow A$ est un morphisme d'anneaux. La* ***composition*** *de deux morphismes d'anneaux est encore un morphisme d'anneaux. cela permet de définir la* CATÉGORIE DES ANNEAUX.
Conformément aux définitions de théorie des catégories, on dit qu'un morphisme d'anneaux $f : A \longrightarrow B$ est un ***isomorphisme*** *s'il existe un morphisme d'anneaux $g : B \longrightarrow A$ tel que $f \circ g = Id_B$ et $g \circ f = Id_A$. Le morphisme g est alors appelé morphisme réciproque de f. On note $f : A \xrightarrow{\sim} B$ pour signifier que le morphisme $f : A \longrightarrow B$ est un isomorphisme ; si A et B sont isomorphes, c'est-à-dire s'il existe un isomorphisme de A dans B, on écrit $A \simeq B$.*

Exemple 1.7. *Soient $\mathbb{Z}[\sqrt{2}]$ et $\mathbb{Z}[\sqrt{3}]$ les sous-anneaux de $\mathbb{C}$ engendrés par $\mathbb{Z}$, et respectivement par $\sqrt{2}$ et $\sqrt{3}$.*

a) *On a $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2}; a,b \in \mathbb{N}\}$ et $\mathbb{Z}[\sqrt{3}] = \{a+b\sqrt{3}; a,b \in \mathbb{N}\}$.*

b) *Il n'existe pas de morphisme d'anneaux de* $\mathbb{Z}[\sqrt{2}]$ *dans* $\mathbb{Z}[\sqrt{3}]$.

En effet

a) *On démontre que tout élément de* $\mathbb{Z}[\sqrt{2}]$ *s'écrit d'une maniére unique sous la forme* $a+b\sqrt{2}$, *pour* a *et* $b \in \mathbb{N}$. *En effet, comme*
$(a+b\sqrt{2})+(a'+b'\sqrt{2}) = (a+a')+(b+b')\sqrt{2}$ *et*
$(a+b\sqrt{2})(a'+b'\sqrt{2}) = aa'+ba'\sqrt{2}+ab'\sqrt{2}+2bb' = (aa'+2bb')+(ab'+a'b)\sqrt{2}$, *l'ensemble des* $a+b\sqrt{2}$ *est un sous-anneau de* $\mathbb{C}$, *donc égal à* $\mathbb{Z}[\sqrt{2}]$. *L'unicité de la décomposition résulte du fait que* $\sqrt{2} \notin \mathbb{Q}$. *On aurait si non deux entiers non tous deux nuls* a *et* b *tels que* $a+b\sqrt{2}=0$. *On peut supposer* a *et* b *premiers entre eux, et en particulier* $a^2 = 2b^2$. *Ainsi , a est pair; on écrit donc* $a = 2a'$, *d'où* $2a'^2 = b^2$, *ce qui implique que* b *est pair, contrairement au fait que* a *et* b *étaient supposés premiers entre eux.*
De même, tout élément de $\mathbb{Z}[\sqrt{3}]$ *s'écrit de maniére unique sous la forme* $a+b\sqrt{3}$.

b) *Supposons donné un homomrphisme d'anneaux* $f : \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Z}[\sqrt{3}]$. *Alors, il existe* a *et* b *tels que* $f(\sqrt{2}) = a+b\sqrt{3}$. *Alors* $f(2) = f(1+1) = 2f(1) = 2$ *mais* $f(2) = f(\sqrt{2}\sqrt{2}) = f(\sqrt{2})^2 = (a+b\sqrt{3})^2 = a^2+3b^2+2ab\sqrt{3}$. *Il faut donc résoudre le systéme d'équations :*

$$\begin{cases} a^2+3b^2 &= 2 \\ 2ab &= 0 \end{cases}$$

Ainsi, soit $a=0$, *soit* $b=0$. *Si* $a=0$, *on trouve* $3b^2=2$, *ce qui est impossible (*$b=0$ *ne convient pas, et si* $b \neq 0$, $3b^2 \geq 3$*). Si* $b=0$, *on trouve* $a^2=2$ *qui n'a pas de solution entiere. Ainsi,* f *n'existe pas.*

Proposition. *Un morphisme d'anneaux est un isomorphisme si et seulement si il est bijectif.*

Démonstration. Si $f : A \longrightarrow B$ est un isomorphisme, son morphisme réciproque est en particulier une bijection réciproque de f, donc f est bijectif. Réciproquement, supposons que f est bijectif et notons g sa bijection réciproque. Il nous faut alors prouver que g est un morphisme d'anneaux de B dans A.
Comme $f(0)=0$, $g(0)=0$. Si a et $b \in B$

$f(g(a+b)) = a+b = f(g(a))+f(g(b)) = f(g(a)+g(b))$. et

$f(g(ab)) = ab = f(g(a))f(g(b)) = f(g(a)g(b))$.

Comme f est bijectif, $g(a+b) = g(a)+g(b)$ et $g(ab) = g(a)g(b)$. □

Proposition. *Soit K un corps et $l : \mathbb{Z} \longrightarrow K$ l'homomrphisme canonique. Alors, K contient un plus petit sous-corps k_0.*

- *si l est injectif, K_0 est isomorphe à $\mathbb{Q}$.*

- *si l n'est pas injectif, il existe un unique nombre premier p tel que $Kerl = (p)$ et K_0 est de cardinal p.*

Démonstration. L'intersection $L = \cap K_i$ d'une famille (k_i) de sous-corps de K est un sous-corps de K : comme $1 \in K_i$ pour tout i, $1 \in L$. Si x et y sont dans L, $x - y$ est dans tout K_i donc dans K. Si de plus $y \neq 0$, x/y appartient à chaque K_i donc $x/y \in L$. Lintersection de tous les sous-corps de K est donc un sous-corps de K. On le note K_0.
Supposons maintenant que l est injectif et construisons un homomorphisme de corps $\widetilde{l} : \mathbb{Q} \longrightarrow K$. Pour cela, si a/b est une fraction d'entier avec $b \neq 0$, $l(b) \neq 0$ dans K et on pose $\widetilde{l}(a/b) = l(a)/l(b)$. Cela ne dépend pas de la fraction choisie :
si $a/b = c/d$, on a $ad = bc$ dans $\mathbb{Z}$, donc
$l(a)l(d) = l(ad) = l(bc) = l(b)l(c)$ et $l(a)/l(b) = l(c)/l(d)$.
C'est un homomorphisme de corps : pour la somme de deux éléments,

$$\widetilde{l}(a/b)+\widetilde{l}(c/d) = \frac{l(a)}{l(b)}+\frac{l(c)}{l(d)} = \frac{l(a)l(d)+l(b)l(c)}{l(b)l(d)} = \frac{l(ad+bc)}{l(bd)} = \widetilde{l}(\frac{ad+bc}{bd})$$
$$= \widetilde{l}((a/b)+(c/d))$$

et pour le produit ,

$$\widetilde{l}(a/b)\widetilde{l}(c/d) = \frac{l(a)}{l(b)}\frac{l(c)}{l(d)} = \frac{l(a)l(c)}{l(b)l(d)} = \frac{l(ac)}{l(bd)} = \widetilde{l}(ac/bd) = \widetilde{l}((a/b)(c/d)).$$

Par suite, $\widetilde{l}$ est un homomrphisme de corps $\mathbb{Q} \longrightarrow K$. Il est nécessairement injectif et définit donc un isomorphisme de $\mathbb{Q}$ sur un sous-corps K_0' de K.Nécessairement, $K_0 \subset K_0'$. Réciproquement, comme K_0 contient 1, il contient $l(\mathbb{Z})$ puis toutes les fractions $l(a)/l(b)$ avec $b \neq 0$. Par suite, $K_0 = K_0'$.

Supposons maintenant que l n'est pas injectif. Son noyau est un idéal (n) de $\mathbb{Z}$, où n est défini comme le plus petit entier strictement positif tel que $l(n) = 0$. Soit p un facteur premier de n. On peut écrire $n = pm$ avec $1 \leq m < n$. On a donc $0 = l(n) = l(p)l(m)$. Par minimalité de n, $l(m) \neq 0$ donc $l(p) = 0$. Cela implique $p \geq n$, donc $n = p$.
L'image $l(\mathbb{Z})$ de $\mathbb{Z}$ par l'homomrphisme l est un sous-anneau de K. En fait, on a $l(\mathbb{Z}) = \{l(0), ..., l(p-1)\}$: si $n \in \mathbb{Z}$, la division euclidienne de n par p s'écrit $n = pq + r$ avec $0 \leq r < p-1$ et $l(n) = l(p)l(q) + l(r) = l(r)$. En particulier, le cardinal de $l(\mathbb{Z})$ est exactement p. Ainsi, $l(\mathbb{Z})$ est un sous-anneau

fini d'un anneau intégre. Donc est un corps. Par minimalité de K_0, ce corps contient K_0, mais réciproquement K_0 contient 1, donc il contient $l(\mathbb{Z})$. $\square$

Chapitre 2

Idéaux

2.1 Idéal

Définition. *On appelle idéal d'un anneau A tout sous-groupe $I \subset A$ tel que pour tout $a \in A$ et tout $b \in I$, $ab \in I$.*

Remarque 2.1. *Un idéal est un sous anneau, mais la réciproque est fausse. Par exemple $\mathbb{Z}$ est un sous-anneau de ($\mathbb{R}$,+, .) qui n'est pas un idéal ($1 \times \sqrt{2} = \sqrt{2} \notin \mathbb{Z}$).*

Remarque 2.2. *{0} es A sont des idéaux de A.*

Propriétés. *Soit I un idéal d'un anneau $(A, +, .)$, si I contient un élément inversible, alors $I = A$.*

Démonstration. –On a par définition $I \subseteq A$, soit $x \in I$ inversible dans A c'est à dire $x^{-1} \in A$, soit $a \in A$, on a $a = xx^{-1}a \in I \Longrightarrow$A $\subseteq I$. □

Pour prouver qu'une partie I de A est un idéal, il suffit d'établir les faits suivants :

__ $0 \in I$

__ si $a \in I$ et $b \in I$, $a + b \in I$.

__ si $a \in A$ et $b \in I$, $ab \in I$.

Exemple 2.1. *Si K est un corps, les seuls idéaux de K sont {0} et K. En effet, soit I un idéal de K distinct de {0} et soit a un élément non nul de I. Soit $b \in K$. Comme $a \neq 0$, on peut considérer l'élément $\frac{b}{a}$ de K et par définition d'un idéal $(\frac{b}{a})a \in I$. On a donc $b \in I$, d'où $I = K$.*

Exemple 2.2. *Si I est un idéal de $\mathbb{Z}$, alors il existe un unique entier $n \geq 0$ tel que I=(n).*

En effet

–Si $I = (0)$, n=0 convient.
Supposons maintenant $I \neq (0)$. Soit I un idéal de $\mathbb{Z}$ et n le plus petit entier naturel non nul de I. Alors on a $n\mathbb{Z} \subset I$.
Soit $m \in I$; la division euclidienne de m par n montre qu'il existe $a \in \mathbb{N}$; $r \in \mathbb{N}$ tel que :
$m = an + r$ et $0 \leq r < n$. Comme on a $r = m - an \in I$, $0 \leq r < n$, et n le plus petit entier naturel non nul appartenant à I, alors on a necessairement $r = 0$ et $m = an \in I$. D'où on a : $I = nZ = (n)$.

Proposition. *Le noyau d'un morphisme d'anneaux $f : A \longrightarrow B$ est l'ensemble des $a \in A$ tels que $f(a) = 0$. C'est un idéal de A noté $Kerf$.*

Démonstration. –Un morphisme d'anneaux étant un morphisme de groupe abéliens, $Kerf$ est un sous-groupe de A. De plus, si $x \in Kerf$ et si $a \in A$, on a $f(ax) = f(a)f(x) = f(a)0 = 0$ donc $ax \in Kerf$. Il en résulte que $Kerf$ est un idéal de A. □

Proposition. *(**Image, image réciproque.**)–Soit $f : A \longrightarrow B$ un morphisme d'anneaux. Plus généralement, si J est un idéal de B, l'image réciproque*
$f^{-1}(J) = \{a \in A; f(a) \in J\}$ est un idéal de A.

Démonstration. –Comme $f(0) = 0 \in J$, $0 \in f^{-1}(J)$. Si a et $b \in f^{-1}(J)$, $f(a + b) = f(a) + f(b) \in J$ puisque $f(a)$ et $f(b) \in J$ et J est un idéal de B. Enfin, si $a \in A$ et $b \in f^{-1}(J)$, on a $f(ab) = f(a)f(b) \in J$ puisque $f(b) \in J$. □

Remarque 2.3. *L'image d'un idéal par un morphisme n'est pas toujour un idéal. En effet :*
Soit f l'application

$$f : \mathbb{Z} \longrightarrow \mathbb{Q}$$

$$x \longmapsto x$$

$f(2\mathbb{Z}) = 2\mathbb{Z}$ n'est pas un idéal de $\mathbb{Q}$ (car $2 \in 2\mathbb{Z}$, $1/2 \in \mathbb{Q}$ mais $2.1/2 \notin 2\mathbb{Z}$).

Définition. ***(Nilradical)****–Le nilradical d'un anneau A est l'ensemble de ses éléments nilpotents . C'est un idéal de A.*
Plus généralement, on définit le radical I de A par la formule :
$\sqrt{I} = \{a \in A; il\ existe\ n \geq 1, a^n \in I\}$.
C'est un idéal de A qui contient I. Par définition même, le nilradical de A est donc égal au radical de l'idéal nul.

Démonstration. –Comme $0^1 = 0 \in I$, $0 \in I$. Si $a \in \sqrt{I}$ et $b \in \sqrt{I}$, choisissons n et $m \geq 1$ tels que $a^n \in I$ et $b^m \in I$. Alors, on a d'après la formule du binôme :

$(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k}$
Dans cette somme, tous les termes appartiennent à I : c'est vrai de ceux correspondant à $k \geq n$ puisque $a^k = a^n a^{k-n}$ et $a^n \in I$; de même, si $k \leq n$, $n+m-k \geq m$ et $b^{n+m-k} = b^m b^{n-k}$ appartient à I. On a donc $(a+b)^{n+m} \in I$, d'où $a+b \in \sqrt{I}$. Enfin, si $a \in \sqrt{I}$ et $b \in A$, choisissons $n \geq 1$ tel que $a^n \in I$. Alors $(ba)^n = b^n a^n \in I$ et $ba \in \sqrt{I}$. □

2.2 Intersection, réunion d'idéaux

Intersection : Si I et J sont deux idéaux de A, l'ensemble $I \bigcap J$ est encore un idéal de A. Plus généralement, l'intersection d'une famille (non vide) d'idéaux de A est encore un idéal de A.

Démonstration. –Soit $(I_s)_s$ une famille d'idéaux de A et posons $I = \bigcap_s I_s$. L'intersection d'une famille de sous-groupes est encore un sous-groupe, donc I est un sous-groupe de A. Soit maintenant $x \in I$ et $a \in A$ arbitraires et montrons que $ax \in I$. Pour tout s, $x \in I_s$ et I_s étant un idéal ; on a donc $ax \in I_s$. Par suite, ax appartient à tous les I_s, donc $ax \in I$. □

Réunion : Soit I et J des idéaux de A.
Alors $I \bigcup J$ est un idéal de $A \Longleftrightarrow$I $\subset J$ ou $J \subset I$.

Démonstration. –($\Leftarrow$)*évident.*
($\Rightarrow$)I $\bigcup J$ est un idéal de $A \Rightarrow$I $\bigcup J$ est un sous-groupe de $(A, +)$. Or la réunion des deux sous-groupes n'est un sous-groupe que si l'un des sous-groupes est contnue dans l'autre. □

2.3 Idéal engendré par une partie

Définition. *Soit A un anneau et B une partie non vide de A. L'idéal engendré par B, qu'on note (B) est le plus petit idéal de A qui contient B.*

Proposition. $(B) = \bigcap_{I\ idéal\ de\ A} I$, *tel que* $B \subset I$.

Démonstration. –On pose :
$J = \bigcap_{I \text{ idéal de } A} I$ tel que $B \subset I$, J est un idéal de A qui contient B. Donc $(B) \subset J$. On montre que $J \subset (B)$:
Comme J est l'intersection de tous les idéaux qui contiennent B et (B) est un idéal qui contient B, alors $J \subset (B)$. □

Proposition. *(B)=*$\{a_1b_1 + ... + a_kb_k, a_i \in A,\ b_i \in B,\ k \geq 1\}$

Démonstration. –On pose :
$I = \{a_1b_1 + ... + a_kb_k, a_i \in A, b_i \in B, k \geq 1\}$
On montre que I est un idéal qui contient B.

i) $B \neq \emptyset \Longrightarrow \exists b \in B$, on a $0_A = 0_A b \in I$.

ii) Soit $x, y \in I$, on montre que $x + y \in I$. On pose :
$x = a_1b_1 + ... + a_kb_k, a_i \in A$,$\mathrm{b}_i \in B$
$y = a'_1b'_1 + ... + a'_kb'_k, a'_i \in A$,$\mathrm{b'}_i \in B$
Alors :
$x + y = a_1b_1 + ... + a_kb_k + a'_1b'_1 + ... + a'_kb'_k \in I$

iii) Soit $x \in I$ et $a \in A$. On montre que $ax \in I$. On pose
$x = a_1b_1 + ... + a_kb_k, a_i \in A$,$\mathrm{b}_i \in$B,k ≥ 1:
$ax = a(a_1b_1 + ... + a_kb_k) = (aa_1)b_1 + ... + (aa_k)b_k \in I$

iv) Soit $b \in B$ alors $b = 1_A b \in I$.
Donc $B \subset I$. Comme I est un idéal de A qui contient B et (B) est le plus petit idéal de A qui contient B, $(B) \subset I$.
On montre que $I \subset (B)$. Soit $x \in I$ alors x s'écrit :
$x = a_1b_1 + ...a_kb_k$ avec $a_i \in A$, $b_i \in B$, $k \geq 1$
Comme (B) contient B, $b_i \in (B)$. Or (B) est un idéal donc :
$a_1b_1 + ... + a_kb_k \in (B)$ □

Exemple 2.3. $< \emptyset >= \{0\}$ *et* $< \{1\} >= A$.
Si A est commutatif et $x \in A$, *alors* $< \{x\} >= Ax = \{ax/a \in A\}$ *et est noté* $< x >$ *ou* (x).

Proposition. *Soient A et B deux anneaux et* $f : A \longrightarrow B$ *un homomorphisme d'anneaux. Pour tout idéal I de A, on note* $f_*(I)$ *l'idéal de B engendré par* $f(I)$ *et on l'appelle extension de I dans B. Pour tout idéal J de B, on appelle contraction de J l'idéal* $f^{-1}(J)$.
Etant donné un idéal I de A et un idéal J de B, on a les assertions suivantes :

a) *I est contenu dans $f^{-1}(f_*(I))$ et J contient $f_*(f^{-1}(J))$.*

b) *$f^{-1}(J) = f^{-1}(f_*(f^{-1}(J)))$ et $f_*(I) = f_*(f^{-1}(f_*(I)))$.*

Soit ζ l'ensemble des idéaux de A qui sont des contractions d'idéaux de B et ξ l'ensemble des idéaux de B qui sont des extensions d'idéaux de A.

c) *$\zeta = \{I; I = f^{-1}(f_*(I))\}$ et $\xi = \{J; f_*(f^{-1}(J))\}$.*

d) *l'application f_* définit une bijection de ζ sur ξ d'inverse f^{-1}.*

En effet :

a) *Soit $x \in I$, $f(x) \in f(I) \subset f_*(I)$, d'où $x \in f^{-1}(f_*(I))$.*
Soit $y \in f_*(f^{-1}(J))$. On peut donc écrire $y = \sum_{i=1}^{n} b_i f(x_i)$, pour $b_i \in B$ et $x_i \in f^{-1}(J)$. Ainsi, $f(x_i) \in J$ et $y \in J$.

b) *La premiere inclusion de a) appliquée à $I = f^{-1}(J)$ donne $f^{-1}(J) \subset f^{-1}(f_*(f^{-1}(J)))$. En appliquant f^{-1} à la seconde, on obtient l'égalité souhaitée. Si l'on applique f_* à la premiere inclusion de a) , on obtient $f_*(I) \subset f_*(f^{-1}(f_*(I)))$. Si l'on applique la seconde inclusion de a) à l'idéal $J = f(I)$, on obtient que $f_*(I)$ contient $f_*(f^{-1}(f_*(I)))$, d'où l'égalité.*

c) *D'aprés la premiere égalité de b), tout élément I de ζ vérifie $I = f^{-1}(f_*(I))$, tandis qu'il est clair que tout idéal I vérifiant $I = f^{-1}(f_*(I))$ est un contracté : c'est le contracté de $f_*(I)$.*
D'autre part, tout idéal J de ξ vérifie $J = f_*(f^{-1}(J))$ (appliquer la seconde égalité de b) à un idéal I tel que $J = f_*(I)$, tandis que si un idéal J vérifie $J = f_*(f^{-1}(J))$, c'est l'extension de $f^{-1}(J)$, donc un élément de ξ.

d) *L'application f_* envoie bien idéaux contractions d'idéaux de B dans les idéaux qui sont extensions d'idéaux de A et l'application f^{-1} envoie les idéaux qui sont extensions d'idéaux de A dans ceux qui sont contractés d'idéaux de B. Montrons que $f_* f^{-1} : \xi \longrightarrow \xi$ est l'identité. C'est en fait la seconde égalité de b). De même, la premiere égalité de b) entraine que $f^{-1} f_* : \zeta \longrightarrow \zeta$ est l'identité. Ainsi, f_* est bijective, de bijection réciproque f^{-1}.*

2.4 Somme d'idéaux

Soit I et J deux idéaux de A. L'ensemble des sommes $a+b$ avec $a \in I$ et $b \in J$ est un idéal de A, noté $I+J$. C'est aussi l'idéal de A engendré par la partie $I \cup J$. Plus généralement, si $(I_s)_{s\in S}$ est une famille d'idéaux de A, l'ensemble des sommes (presque nulles) $\sum_s a_s$, où pour tout s, $a_s \in I_s$, est un idéal de A noté $\sum_s I_s$. C'est aussi l'idéal de A engendré par la partie $\bigcup_s I_s$.

Démonstration. –Comme $0 = \sum_s 0$ et comme $0 \in I_s$ pour tout s, $0 \in \sum_s I_s$. En suite, si $a = \sum_s a_s$ et $b = \sum_s b_s$ sont deux éléments de $\sum_s I_s$, on a $a+b = \sum_s (a_s + b_s)$ où pour tout s, $a_s + b_s \in I_s$. Donc $a+b \in \sum_s I_s$. Finalement, si $a = \sum_s a_s$ appartient à I_s et $b \in A$, on a $ba = \sum_s (ba_s)$. Pour tout s, $ba_s \in I_s$, donc $ba \in \sum_s I_s$. Ainsi, $\sum_s I_s$ est bien un idéal de A.
Pour montrer que c'est l'idéal de A engendré par la partie $\cup_s I_s$, nous devons établir deux inclusions. Tout d'abord, si $t \in S$ et $a \in I_t$, on a $a = \sum_s a_s$ avec $a_s = 0$ si $t \neq s$ et $a_t = a$.Donc $a \in \sum_s I_s$ et l'idéal $\sum_s I_s$ contient I_t. Par définition de l'idéal $< \cup_s I_s >$ (Plus petit idéal qui contient la partie $\cup_s I_s$), on a ainsi
$< \cup_s I_s > \subset \sum_s I_s$.
Dans l'autre sens, si I est un idéal contenant $\cup_s I_s$, montrons que I contient $\sum_s I_s$. Soit alors $a = \sum_s a_s$ un élément de $\sum_s I_s$. Tous les termes de cette somme appartiennent à I. Par définition d'un idéal, a appartient à I et I contient $\sum_s I_s$. □

2.5 Produit d'idéaux

Définition. *Soit I et J deux idéaux de A. L'ensemble des produits ab avec $a \in I$ et $b \in J$ n'est pas forcément un idéal de A. L'idéal IJ est par définition l'idéal engendré par ces produits. C'est ainsi l'ensemble des combinaisons linéaires finies $\sum a_s b_s$ avec $a_s \in I$ et $b_s \in J$.*

Proposition. *Soit A un anneau, soit I et J deux idéaux de A. Alors, $IJ \subset I \cap J$.*
Si de plus si $I + J = A$, auquel cas on dit que les idéaux I et J sont comaximaux, alors on a l'égalité : $IJ = I \cap J$.

Démonstration. –Si $a \in I$ et $b \in J$, ab appartient à I (c'est un multiple de $a \in I$) et appartient à J (c'est un multiple de $b \in J$). Donc $ab \in I \cap J$. Puisque les produits ab avec $a \in I$ et $b \in J$ appartiennent à l'idéal $I \cap J$,

l'idéal IJ qui engendré par ces produits est contenu dans $I \cap J$.
Si $I + J = A$, il existe $x \in I$ et $y \in J$ tels que $x + y = 1$. Soit alors $a \in I \cap J$,écrivons
$a = a1 = a(x + y) = ax + ay$.
Comme $a \in I$ et $y \in J$, $ay \in IJ$; comme $a \in J$ et $x \in I$, $ax \in IJ$. Par suite, leur somme $ax + ay$ appartient à IJ et $a \in IJ$. Il en résulte que si I et J sont comaximaux, on a $I \cap J \subset IJ$, donc, compte-tenu de l'autre inclusion, $I \cap J = IJ$. □

Proposition. *Soient I,J et L des idéaux de A.,Alors on a les assertions suivantes :*

a) *$I.J$ est contenu dans $I \cap J$.*

b) $(I.J) + (I.L) = I.(J + L)$.

c) *$(I \cap J) + (I \cap L)$ est contenu dans $I \cap (J + L)$.*

d) *si J est contenu dans I, on a $J + (I \cap L) = I \cap (J + L)$.*

En effet :

a) *Soit $x \in I.J$: x s'écrit sous la forme $x = \sum_{i=1}^{n} \alpha_i \beta_i$ avec $\alpha_i \in I$ et $\beta_i \in J$. Pour chaque i on a donc $\alpha_i \beta_i \in I \cap J$, d'où $x \in I \cap J$.*

b) *On a $I.J \subset I.(J+L)$ et $I.L \subset I.(J+L)$, donc $I.J+I.L$ est inclus dans $I.(J+L)$. Réciproquement, soit $x \in I(J+L)$. On a donc $x = \sum_{i=1}^{n} \alpha_i(\beta_i + \gamma i)$, avec $\alpha_i \in I$, $\beta_i \in J$ et $\gamma_i \in L$. Ainsi,*
$x = \sum_{i=1}^{n} \alpha_i \beta_i + \sum_{i=1}^{n} \alpha_i \gamma_i \in I.J + I.L$.

c) *Soit $x = y + z$ avec $y \in I \cap J$ et $z \in I \cap L$. En particulier, $y + z \in I$ et $y + z \in J + L$, d'où $x \in I \cap (J + L)$.*

d) *D'aprés c), on a $J+(I\cap L) \subset I\cap(J+L)$. D'autre part, si $x \in I\cap(J+L)$, alors on peut écrire $x = y + z$, avec $y \in J$ et $z \in L$. En particulier, $z = x - y \in I$, donc $z \in I \cap L$, si bien que $x = y + z \in J + (I \cap L)$.*

Proposition. *Soient I et J deux idéaux de A. On suppose que $I + J = A$. Alors pour tout n, $I^n + J^n = A$.*

Démonstration. Si $I + J = A$, on peut écrire $1 = x + y$ avec $x \in I$ et $y \in J$. Alors on a

$$1 = (x+y)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} x^k y^{2n-k}$$

De plus , pour tout $k \in \{0, ..., 2n\}$, ou bien $x^k \in I^n$, ou bien $y^{2n-k} \in J^n$. Par suite, $1 \in I^n + J^n$ et $I^n + J^n = A$. □

Chapitre 3

Corps

3.1 Corps

Définition. *Soit A un anneau non nul. A est un corps si $U(A) = A - \{0\}$ c'est-à-dire tout élément non nul de A est inversible.*

Exemple 3.1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ *sont des corps.*

Proposition. *Soit A un anneau intègre possédant un nombre fini d'idéaux, alors A est un corps. (Si $x \neq 0$ introduire les idéaux (x^n) pour $n \geq 1$).*

Démonstration. Soit A un anneau intègre et $x \neq 0$ un élément de A qui n'est pas nul. Il faut montrer que x est inversible. On introduit alors les idéaux $(x) \supset (x^2) \supset .... \supset (x^n) \supset ....$ Il y en a une «infinité», et comme A est supposé n'avoir qu'un nombre fini d'idéaux, deux d'entre eux sont égaux, disons $(x^n) = (x^m)$ pour $m > n \geq 1$. Alors, il existe $a \in A$ tel que $x^n = a.x^m$, et $x^n(1 - ax^{m-n}) = 0$. Comme $x \neq 0$, $1 = x^{m-n}$. Ainsi $x.(ax^{m-n-1}) = 1$ et x est inversible. □

Remarque 3.1. *Soient K un corps et A un anneau non nul. Alors tout homomrphisme d'anneax de K dans A est injectif. En effet*

Soit $\phi : K \longrightarrow A$ un homomrphisme d'anneaux. Supposons que ϕ n'est pas injectif et soit $x \in K$ un élément non nul tel que $\phi(x) = 0$. Alors, $\phi(1) = \phi(x/x) = \phi(x)\phi(1/x) = 0$, donc $1 = 0$ dans A, ce qui contredit le fait que A n'est pas l'anneau nul. D'où ϕ est injectif.

3.2 Sous-corps

Définition. *Soit K un corps et K' une partie de K.*
On dit que K' est un sous-corps de K si : K' est un sous-groupe additif de K et $(K')^* = K' - \{0\}$ est un sous-groupe multiplicatif.

Autrement dit : K' est un sous-corps de K si :

* $K' \neq \varnothing$

* $x - y \ \in K'$: $\forall x,y \in K'$

* $xy^{-1} \in (K')^*$: $\forall x,y \in (K')^*$.

3.3 Morphisme de corps

Définition. *Soient K, K' deux corps, $f : K \longrightarrow K'$ un application. Si f est un morphisme (resp endomorphisme, resp isomorphisme, resp automorphisme) d'anneaux, f prend le nom de* ***morphisme*** *(resp* ***endomorphisme****, resp* ***isomorphisme****, resp* ***automorphisme*** *) de corps.*

Exemple 3.2. *$Id_{\mathbb{C}} : \mathbb{C} \longrightarrow \mathbb{C}$ et la conjugaison $\mathbb{C} \longrightarrow \mathbb{C}$ sont des automorphismes du corps $\mathbb{C}$. (pour les lois usuelles).*

Remarque 3.2. *Si $f : K \longrightarrow K'$ est un morphisme de corps, alors pour tout x de $k - \{0\}$:*
$f(x) \neq 0$ et $(f(x))^{-1} = f(x^{-1})$.

3.4 Corps finis

Définition. *Un corps fini est un corps commutatif qui est par ailleurs fini. Il est entièrement déterminé par son cardinal, qui est toujours une puissance d'un nombre premier, ce nombre premier étant sa caractéristique.*

Proposition. *Un corps fini contient un corps $\mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier.*

Démonstration. Soit K un corps fini, et soit π l'application

$$\pi : \mathbb{Z} \longrightarrow K$$

$$n \longmapsto n.1$$

$Ker\pi$ est un idéal de $\mathbb{Z}$, donc de la forme $p\mathbb{Z}$, avec $p \neq 0$ et $p \neq 1$.

Si $p = p_1p_2$, on a $0 = \pi(p) = \pi(p_1p_2) = \pi(p_1)\pi(p_2)$ dans K, donc $\pi(p_1) = 0$ ou $\pi(p_2) = 0 \Longrightarrow$p$_1 \in p\mathbb{Z}$ ou $p_2 \in p\mathbb{Z} \Longrightarrow$p$_1 = p$ ou $p_2 = p$ donc p est premier.

On a donc

$$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \subset K$$

p est le plus petit entier positif tel que $p.1 = 0$ dans K.
p est appelé **la caractéristique du corps.**
$\mathbb{F}_p$ est le plus petit sous-corps de K.
$\mathbb{F}_p$ est l'intersection des sous-corps de K.
$\mathbb{F}_p$ est appelé **corps premier.**
Plus généralement, un corps premier est le plus petit corps contenu dans un corps donné. Il est isomorphe à $\mathbb{Q}$, ou à un des corps $\mathbb{F}_p$ où p est un nombre premier. La caractéristique d'un corps est le nombre 0 si le corps premier est $\mathbb{Q}$, le nombre p si le corps premier est $\mathbb{F}_p$. □

3.5 Nombre d'élément d'un corps fini

Proposition. *Un corps K de caractéristique p admet p^n élément où n est un entier.*

Démonstration. En effet, le nombre n est égal à la dimension de K considéré comme espace vectoriel sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

$$n = dim_{F_p} K$$

□

Proposition. *Si a et b sont deux élément d'un corps K de caractéristique p, alors*

$$(a+b)^p = a^p + b^p.$$

Démonstration. On a $(a+b)^p = \sum_{i=0}^{p} C_p^i a^i b^{p-i}$.
Si $1 \leq i \leq p-1$, on a $C_p^i = \frac{p!}{i!(p-i)!} = p\frac{(p-1)!}{i!(p-i)!}$.
C_p^i est un entier, donc $i!(p-i)!$ divise $p! = p(p-1)!$. Or $i!(p-i)!$ est premier à p, donc divise $(p-1)!$. Donc C_p^i est divisble par p, et est donc nul dans K.
Il reste $(a+b)^p = C_p^0 b^p + C_p^p a^p$.

□

Corollaire 3.1. *Si a et b sont deux éléments d'un corps K de caractéristique p, alors*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

Chapitre 4

Quaternions

4.1 Le corps non-commutatif ($\mathbb{H}$, + , $\times$)

Définition. *Un quaternion est un élément* $(a, b, c, d) \in \mathbb{R}^4$*, on note* $\mathbb{H}$ *l'ensemble des quaternions (l'ensemble* $\mathbb{H}$ *s'identifie à* $\mathbb{R}^4$*, muni des opérations que nous allons définir).*

Addition sur $\mathbb{H}$:
On définit la *somme* de deux quaternions (a, b, c, d) et (a', b', c', d') par : $(a, b, c, d) + (a', b', c', d') = (a + a', b + b', c + c', d + d')$
(c'est l'addition naturelle dans $\mathbb{R}^4$ vu comme $\mathbb{R}$-espace vectoriel).

Multiplication sur $\mathbb{H}$:
On définit également le *produit* $(a, b, c, d) \times (a', b', c', d')$ par l'expression : $(aa' - bb' - cc' - dd', ab' + ba' + cd' - dc', ac' + ca' - bd' + db', da' + ad' + bc' - cb')$.

Théorème 4.1. $(\mathbb{H}, +, \times)$ *est un corps, non commutatif.*

Démonstration. – On vérifie sans problème que $(\mathbb{H}, +)$ est un groupe commutatif, d'élément neutre (0,0,0,0) ; l'opposé d'un élément (a, b, c, d) étant $(-a, -b, -c, -d)$.
–*Non-commutativité de la loi* $\times$ *:*
On a

$$(0, 1, 0, 0) \times (0, 0, 1, 0) = (0, 0, 0, 1)$$

et

$$(0, 0, 1, 0) \times (0, 1, 0, 0) = (0, 0, 0, -1)$$

–*Associativité et distributivité sur* + *:*

Se vérifient en appliquant les propriétés correspondantes des opérations sur $\mathbb{R}$. Attention : il faudrait cette fois démontrer la distributivité à gauche et la distributivité à droite, puisque la multiplication n'est pas commutative.

–*(1,0,0,0) est l'élément neutre de* $\times$ *:*

En appliquant la définition de la loi $\times$, on obtient aisément, pour (a, b, c, d) un quaternion quelconque :
$(1, 0, 0, 0) \times (a, b, c, d) = (a, b, c, d) \times (1, 0, 0, 0) = (a, b, c, d)$

–*Tout élément* $(a, b, c, d) \in \mathbb{H}^* = \mathbb{H} - \{(0, 0, 0, 0)\}$ *est inversible :*

En effet, si (a, b, c, d) est un quaternion non nul, on a $a^2 + b^2 + c^2 + d^2 \neq 0$ (si non les quatre nombres a,b,c,d sont de carré nul, donc tous nuls). Soit alors le quaternion (a_1, b_1, c_1, d_1) défini par :

$$\begin{cases} a_1 &= \dfrac{a}{a^2 + b^2 + c^2 + d^2} \\ b_1 &= \dfrac{-b}{a^2 + b^2 + c^2 + d^2} \\ c_1 &= \dfrac{-c}{a^2 + b^2 + c^2 + d^2} \\ d_1 &= \dfrac{-d}{a^2 + b^2 + c^2 + d^2} \end{cases}$$

En appliquant la définition de la multiplication des quaternions, on vérifie que
$(a, b, c, d) \times (a_1, b_1, c_1, d_1) = (a_1, b_1, c_1, d_1) \times (a, b, c, d) = (1, 0, 0, 0)$ □

Notation : L'opposé (pour la loi $+$) d'un quaternion Z se note $-Z$, et l'on note $Z_1 - Z_2$ la somme $Z_1 + (-Z_2)$.
L'inverse d'un quaternion $Z \neq (0, 0, 0, 0)$ se note $\dfrac{1}{Z}$; et si Z_1 et Z_2 sont deux quaternions avec Z_2 non nul, on note $\dfrac{Z_1}{Z_2}$ le produit $Z_1 \times \dfrac{1}{Z_2}$.

4.2 Plongement de $\mathbb{C}$ dans $\mathbb{H}$

Isomorphisme de $(\mathbb{C}, +, \times)$ **sur un sous-corps de** $(\mathbb{H}, +, \times)$:
Soit $\mathbb{H}'$ l'ensemble des quaternions de la forme $(a, b, 0, 0)$. $\mathbb{H}'$ est non vide, et si $(a, b, 0, 0)$, $(a', b', 0, 0)$ sont des éléments de $\mathbb{H}'$:
-$(a, b, 0, 0) - (a', b', 0, 0) = (a - a', b - b', 0, 0) \in \mathbb{H}'$.
-$(a, b, 0, 0) \times (a', b', 0, 0) = (aa' - bb', ab' + ba', 0, 0) \in \mathbb{H}'$.
-$(1, 0, 0, 0) \in \mathbb{H}'$.

-L'inverse $(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}, 0, 0)$ de $(a, b, 0, 0)$ est encore dans $\mathbb{H}'$.
Donc $(\mathbb{H}', +, \times)$ est un sous-corps de $\mathbb{H}$. Soit l'application :

$$\begin{array}{c} f : \mathbb{C} \longrightarrow \mathbb{H}' \\ a + ib \longmapsto (a, b, 0, 0) \end{array}$$

f est bijective, et l'on vérifie aisément que pour tous complexes z_1 et z_2, on a $f(z_1 + z_2) = f(z_1) + f(z_2)$ et $f(z_1 z_2) = f(z_1) f(z_2)$. Donc f est un isomorphisme de $(\mathbb{C}, +, \times)$ sur $(\mathbb{H}', +, \times)$.

Convention : L'isomorphisme f permet d'identifier $\mathbb{C}$ à $\mathbb{H}'$ (et d'écrire $\mathbb{C} \subset \mathbb{H}$), les lois $+$ et $\times$ sur $\mathbb{H}$ prolongeant alors les opérations déja connues sur $\mathbb{C}$.
Notation : On écrira donc tout élément $(a, b, 0, 0)$ de $\mathbb{H}'$ complexe sous la forme $a + ib$. En particulier 0 est l'élément $(0, 0, 0, 0)$, 1 l'élément $(1, 0, 0, 0)$ et i l'élément $(0, 1, 0, 0)$.
On note par analogie j l'élément $(0, 0, 1, 0)$ et k l'élément $(0, 0, 0, 1)$. La famille $\{1, i, j, k\}$ forme une base de l'ensemble des quaternions vu comme un espace vectoriel sur $\mathbb{R}$, et l'on écrira ainsi $a + bi + cj + dk$ le quaternion (a, b, c, d).

Remarques :

1) Via le plongement de $\mathbb{R}$ dans $\mathbb{C}$, on obtient un plongement de $\mathbb{R}$ dans $\mathbb{H}$ (on peut le décrire explicitement : c'est l'application $x \longmapsto (x, 0, 0, 0)$).

2) Pour tout réel x, on vérifie que le produit d'un quaternion (a, b, c, d) par l'élement $(x, 0, 0, 0)$ (à gauche comme à droite) nous donne le quaternion (ax, bx, cx, dx). Autrement dit, la multiplication dans $\mathbb{H}$ coïncide (sur les réels) avec la multiplication externe sur $\mathbb{R}^4$ vu comme $\mathbb{R}$-espace vectoriel.

3) La notation des quaternions sous la forme $a+bi+cj+dk$ est parfaitement adaptée à l'opération d'addition (la somme de deux quaternions $a+bi+cj+dk$ et $a' + b'i + c'j + d'k$ est $(a + a') + (b + b')i + (c + c')j + (d + d')k$) et de multiplication par un réel. Pour le produit de nos deux quaternion, on obtient en dévloppant l'expression $(a + bi + cj + dk).(a' + b'i + c'j + d'k)$ de façon naturelle, et grâce aux relations :
$i \times j = k = -j \times i$, $j \times k = i = -k \times j$, $k \times i = j = -i \times k$
N.B. Ces formules ressemblent étrangement à celles du produit vectoriel. Si $\vec{u}$ désigne un vecteur de $\mathbb{R}^3$ de coordonnées (x, y, z) et a est un réel, alors on pourra noter $(a, \vec{u})$ le quaternion (a, x, y, z).

Cas particulier : Soient $p = xi + yj + zk$ et $q = x'i + y'j + z'k$ des quaternions purs (i.e sans partie réelle) et $\vec{u}$ et $\vec{v}$ les vecteurs de $\mathbb{R}^3$ de coordonnées (x, y, z) et (x', y', z') respectivement. Alors le produit $pq = (0, \vec{u}).(0, \vec{v})$ est : $p.q = (-xx' - yy' - zz', yz' - zy', -xz' + zx', xy' - yx') = (-\vec{u}.\vec{v}, \vec{u} \wedge \vec{v})$.
Cas général : Soient $p = (a, \vec{u})$ et $q = (b, \vec{v})$ deux quaternions. On a alors :

$$p.q = (a + (0, \vec{u})).(b + (0, \vec{v})) = ab + (0, a\vec{v}) + (0, b\vec{u}) + (-\vec{u}.\vec{v}, \vec{u} \wedge \vec{v})$$

$$= (ab - \vec{u}.\vec{v}, a\vec{v} + b\vec{u} + \vec{u} \wedge \vec{v})$$

4.3 Centre du corps $(\mathbb{H}, +, \times)$

Définition. *Le centre du corps non-commutatif $(\mathbb{H}, +, \times)$ est l'ensemble des éléments de $\mathbb{H}$ commutant pour la loi $\times$ avec tous les éléments de $\mathbb{H}$.*

Théorème 4.2. *Le centre de $(\mathbb{H}, +, \times)$ est l'ensemble des réels.*

Démonstration. Soit $\mathbb{H}_1$ le centre de $(\mathbb{H}, +, \times)$, et (x, y, z, t) un quaternion. $(x, y, z, t) \in \mathbb{H}_1 \iff \forall (a, b, c, d) \in \mathbb{H}$,

$$(x, y, z, t) \times (a, b, c, d) = (a, b, c, d) \times (x, y, z, t)$$

$$\iff \forall a, b, c, d \in \mathbb{R}, \begin{cases} ax - by - cz - dt &= xa - yb - zc - td \\ ay + bx + ct - dz &= ya + xb + zd - tc \\ az + cx - bt + dy &= xc + za - yd + tb \\ dx + at + bz - cy &= ta + xd + yc - zb \end{cases}$$

$$\iff \forall b, c, d \in \mathbb{R}, \begin{cases} ct - dz &= zd - tc \\ -bt + dy &= -yd + tb \\ bz - cy &= yc - bz \end{cases}$$

$$soit (\text{x,y,z,t}) \in \mathbb{H}_1 \iff \forall b, c, d \in \mathbb{R}, \begin{cases} ct - dz &= 0 \\ -bt + dy &= 0 \\ bz - cy &= 0 \end{cases} \iff y = z = t = 0$$

Le quaternion (x, y, z, t) est donc le centre de $\mathbb{H}$ si et seulement si c'est l'image d'une réel par le plongement canonique de $\mathbb{R}$ dans $\mathbb{H}$. □

4.4 Conjugaison dans $\mathbb{H}$; norme sur $\mathbb{H}$

Définition. *Le conjugué d'un quaternion $Z = (a, b, c, d)$ est le quaternion $\overline{Z} = (a, -b, -c, -d)$.*
(cette définition prolonge donc celle du conjugué d'un complexe).

Remarques :

- $Z = \overline{Z} \iff Z \in \mathbb{R}$.

- $Z + \overline{Z} \in \mathbb{R}$.

- En développant le produit $Z \times \overline{Z}$, on trouve
$(a^2+b^2+c^2+d^2, -ab+ba-cd+dc, -ac+ca+bd-db, da-ad-bc+cb) =$
$(a^2+b^2+c^2+d^2, 0, 0, 0) = a^2+b^2+c^2+d^2 \in \mathbb{R}^+$.

Définition. *L'application de $\mathbb{H}$ dans lui-même qui à un quaternion Z associe $\overline{Z}$ s'appelle encore la **conjugaison**. Cette application prolonge la conjugaison définie sur $\mathbb{C}$.*

Théorème 4.3. *La conjugaison est un automorphisme du groupe $(\mathbb{H}, +)$ (mais pas du corps $(\mathbb{H}, +, \times)$).*

Démonstration. Soient $Z = (a, b, c, d)$ et $Z' = (a', b', c', d')$ deux quaternions.

i) $\overline{Z + Z'} = (a+a', -b-b', -c-c', -d-d') = (a, -b, -c, -d)+(a', -b', -c', -d')$

$$= \quad \overline{Z} + \overline{Z'}$$

ii) $\overline{\overline{Z}} = (a, -(-b), -(-c) - (-d)) = (a, b, c, d) = Z$

iii) La conjugaison n'est pas un automorphisme multiplicatif. En effet, si l'on considère les éléments j et k , on a :

$$\overline{jk} = (-j)(-k) = jk = i \text{ et } \overline{jk} = \bar{i} = -i$$

Théorème 4.4. *Soit n l'application de $\mathbb{H}$ dans $\mathbb{R}^+$ définie par $n(Z) = Z\overline{Z}$. Alors n est un **homomorphisme** de $(\mathbb{H}, \times)$ dans $(\mathbb{R}^+, \times)$.*

Démonstration. Soient $Z = (a, b, c, d)$ et $Z' = (a', b', c', d')$ deux quaternions. Alors

$$\begin{aligned} n(ZZ') &= (aa' - bb' - cc' - dd')^2 + (ab' + ba' + cd' - dc')^2 \\ &\quad +(\text{ac'+ca'-bd'+db'})^2 + (da' + ad' + bc' - cb')^2 \\ &= \text{a}^2 n(Z') + b^2 n(Z') + c^2 n(Z') + d^2 n(Z') \end{aligned}$$

Donc :

$$n(ZZ') = n(Z)n(Z')$$

□

Définition. *L'application $Z \longmapsto \sqrt{n(Z)}$ ainsi définie est appelée la **norme** sur le corps des quaternions. On a vu que la norme définit un homomorphisme du groupe $(\mathbb{H}, \times)$ dans $(\mathbb{R}^+, \times)$. Par la suite, on netra G le sous-groupe des quaternions de norme 1, c'est-à-dire le noyau de l'application norme.*

4.5 Représentation matricielle des quaternions

On a vu que l'ensemble $\mathbb{H}$ possède une structure d'algèbre sur $\mathbb{R}$. C'est en particulier un espace vectoriel sur $\mathbb{R}$, de dimension 4, dont on a explicité une base $\{1, i, j, k\}$. Tout quaternion s'écrit alors sous la forme d'une combinaison linéaire des éléments de cette base, c'est-à-dire comme une somme $a.1+b.i+c.j+d.k$, avec a, b, c, d réels.
De par la structure d'algèbre de $\mathbb{H}$, la multiplication (à gauche) par un quaternion q donné, soit l'application $p \longmapsto q.p$, est une application linéaire sur $\mathbb{H}$. Si q s'écrit $a + bi + cj + dk$, cette application a pour matrice, dans la base $1, i, j, k$:

$$\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$$

En fait, on peut définir les quaternions comme l'ensemble des matrices de cette forme : il s'agit manifestement d'un sous-espace vectoriel de $\mathbb{M}_4(\mathbb{R})$. Quant à la multiplication de ces matrices, elle vérifie bien les propriétés voulues de la multiplication des quaternions, d'après l'étude précédente : si l'on note $M(p)$ la matrice associée au quaternion p, alors $M(p)$ est la matrice dans la base $1, i, j, k$ de la multiplication à gauche par p. En composant les applications linéaires, on a donc le résultat suivante : si p_1 et p_2 sont deux quaternions, et $M(p_1)$, $M(p_2)$ les matrices associées, alors $M(p_1)M(p_2)$ est la matrice de la composée des deux applications linéaires «multiplication à gauche par p_2 » et «multiplication à gauche par p_1», c'est-à-dire l'application «multiplication à gauche par $p_1.p_2$»
En fait, on a défini un isomorphisme d'algèbre de $\mathbb{H}$ sur la sous-algèbre de $\mathbb{M}_4(\mathbb{R})$ des matrices de la forme :

$$\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$$

En particulier, la matrice de 1 n'est rien d'autre que la matrice de l'identité, et on a pour i, j, k les matrice :

$$M(i) = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad M(j) = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \quad M(k) = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Cette représentation matricielle des quaternions permet également d'obtenir à moindre effort la propriété suivante :

Propriété La conjugaison sur $\mathbb{H}$ est un anti-automorphisme d'algèbre. (c'est-à-dire une application linéaire du $\mathbb{R}$-espace vectoriel $\mathbb{H}$ dans lui-même, qui vérifie de plus $\overline{p.q} = \overline{p}.\overline{q}$ pour tous p et q).

Démonstration. On a déjà montré que l'application h était un automorphisme du groupe $(\mathbb{H}, +)$. Reste donc à vérifier :
- Pour tout réel x et tout quaternion p, on a $\overline{x.p} = x.\overline{p}$. C'est immédiat en écrivant p sous la forme $a + bi + cj + dk$.
- Pour tous quaternions p et q, on a $\overline{p.q} = \overline{q}.\overline{p}$. On peut bien sur obtenir ceci en revenant aux formes $a + bi + cj + dk$, mais le résultat est beaucoup plus simple d'un point de vue matriciel. En effet, la matrice de $\overline{p}$ n'est autre que la transposée ${}^tM(p)$ *de* $M(p)$. La matrice de $\overline{p.q}$ est de la même façon ${}^tM(p.q) = {}^t(M(p)M(q)) = {}^tM(q){}^tM(p)$. On obtient donc $\overline{p.q} = \overline{q}.\overline{p}$. Notons que le premier point s'en déduit aisément : si x est réel, alors on a $\overline{x.p} = \overline{p}.\overline{x}$. Mais comme $\overline{x} = x$ commute avec tous les quaternions, on a en particulier $\overline{x.p} = x.\overline{p}$. □

Bibliographie

i) **Najib MAHDOU.** ***Introduction à L'Algébre Homologique, (2013)***

ii) **Najib MAHDOU,** ***Cours S5 de structures algébriques enseigné à La Faculté des sciences et Techniques de Fés (2014-2015)***

iii) **Antoine CHAMBERT-LOIR,** ***Algébre Commutative. polycopié du cours enseigné à L'université Pierre et Marie Curie, (2000-2001)***