الجمهوريـة الجزائـريـة الديمقراطيـة الشعبيـة
République Algérienne Démocratique et Populaire
وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

N° Réf :……

Centre Universitaire
Abd elhafid boussouf Mila

Institut des sciences et de la technologie **Département de Mathématiques et Informatique**

Mémoire préparé En vue de l'obtention du diplôme de Master

En: Mathématiques

Spécialité: Mathématiques fondamentales

Produit tensoriel

Préparé par : Guemra Osmane

Aya Berkane

Soutenue devant le jury

Mohamed Kecies	**MCB**	**C. U. Abdelhafid Boussouf, Mila**	**Président**
Mounir Boughbina	**MCA**	**C. U. Abdelhafid Boussouf, Mila**	**Rapporteur**
Amina Daoui	**MCA**	**C. U. Abdelhafid Boussouf, Mila**	**Examinatrice**

Année universitaire :2023/2024

Remerciements

Alhamdulillah qui nous a donné la force et le courage pour terminer ce travaille.
Tout d'abord, ce travail ne serait pas aussi riche sans l'aide et l'encadrement de Mr Boughbina Mounir, on le remercie pour sa patience et sa disponibilité durant notre préparation de ce mémoire.
Nos remerciement s'adresse a Madame Daoui Amina pour sa aide, et son soutien moral et ses encouragement.
Nos remerciements sont également anticipés aux membres de jury d'avoir accepté d'évaluer notre travail.
On remercie toutes les personnes qui nous se sont aidées lors de la rédaction de ce mémoire.

Guemra,Aya

Dedicace

Je remercier en premier lieu Allah, le tout puissant de m'avoir donné courage, santé et patience pour achever ce travail.

Je tiens à dédier cet humble travail à:

A ma très chère mère Fahima:

Quoi que je fasse ou que je dise, je ne saurai point te remercier comme il se doit. Ton affection me couvre, ta bienveillance me guide et ta présence à mes côtés a toujours été ma source de force pour affronter les différents obstacles.

A mon très cher père Cherif :

Tu as toujours «été à mes côtés pour me soutenir et m'encourager. Que ce travail traduit ma gratitude et mon affection.

A mes très chers frères :

Ahmed, Mohammed, Moussa, Haroun, Houssam .

ma belle sœur : Kaltoum.

A les femmes de mes frères et leurs enfants :

Hayat Selsabil , Melissa, Ishak, Taim Ellah, Mayar .

A ma binôme: Aya.

A toute les personnes que je connais et que n'ai pas citées, a ceux que j'aime et m'aiment.

Guemra

Dédicace

Ce modest travail est dédié spécailement A ma chére maman (Fatima) ; ma raison de vivre ; en témoignage de ma reconnaisance pour sa patience ; son amour et ses sacrifices.‘
A mon cher papa (Abdeslam)pour son amour cher et son ’evouement. A vous mes parents je dis merci aucune dédicace ne pourra exprimer mes respects.
A mes chéres sœurs Imen et Houyem.
A mon chèr frère Zakaria.
ma réussite est trés important a ses yeux.
Sans oublier la femme de mon oncle (Djamila) et ma chére (Zoubida) et pour leur soitien.
Pour mon fiancé(Yacine), je le remercie chaleureusement surtout pour son soutien moral ininterrompu et ses nombreux conseils encouragements tout le long de ma thèse.
A ma binôme : Guemra.
A mes amies (Zahera, Mimi, Amina, Rayane, Marwa, Nourhane, Oumenia, Ghada, Anaghim, Hanane, Chaima, Salsabil, Racha)et pour ceux qui m’ont donné l’aide un jour pour finir a tout ceux que j’aine et qui m’ainent, je dédie ce mémoire.

Aya

Table des matières

Introduction

Le capitaine James T.Kirk et Monsieur Spoke prirent chacun une place dans le téléporteur, qui en comptait cinq ou six. D'une voix autoritaire le capitaine ordonna "Energie !". Le chef mécanicien Scotty s'executa et poussa une manette sur la console centrale en face de lui. Il vit les corps des deux officiers se dématerialiser et disparaitre petit à petit. Le capitaine et son second venaient d'être téléportés sur la planète autour de laquelle orbitait le vaisseau spatial USS Enterprise.

Tous les amateurs de science fiction, à la Star Trek, se souviennent de cette scène présente dans pratiquement tous les épisodes. Peu d'entre eux savent que cette téléportation est maintenant une possibilité (ne serait-ce que théorique). Il n'est bien sûr pas question de téléporter des objets ou des individus (pas encore) mais il est possible de téléporter l'état de ce qu'on appelle un qubit, un système quantique à deux dimensions. Et encore peu d'entre eux savent que l'ingrédient mathématique essentiel qui rend cette téléportation possible est notre bon vieux produit tensoriel (ici entre espaces vectoriels complexes).

Il est amusant de savoir que la plupart des physiciens ne connaissent ni la définition ni la construction du produit tensoriel. Mais ils savent le manipuler car ses règles de calcul sont assez simples. Le but de ce travail est de remédier a la situation en donnant la définition exacte du produit tensoriel et tous les détails de sa construction. Le cadre naturel de cette définition est la catégorie des R-modules pour R un anneau commutatif. Le produit tensoriel de deux R-modules y est alors défini comme étant un objet de la catégorie qui vérifie une propriété universelle et qui est le seul à la vérifier. En général un tel objet peut ne pas exister mais nous montrons qu'ici le produit tensoriel existe toujours et nous le construisons explicitement sans (que le lecteur se rassure) utiliser le langage catégorique.

Ce mémoire est organisé de la manière suivante. Dans le premier chapitre

on donne la définition d'un R-module pour R un anneau commutatif avec quelques rappels au début du chapitre sur les notions de groupe, d'anneau et de corps. Un soin particulier a été donné à la notion de suite exacte de modules qu'on utilise pour caractériser les modules projectifs comme constituants, dans des sommes directes, de modules libres. Quand l'anneau R est un corps K, un R-module n'est autre chose qu'un K-espace vectoriel et on retrouve ainsi toute l'algèbre linéaire des espaces vectoriels.

Dans le second chapitre, outre la définition du produit tensoriel, on donne aussi une manière générale pour le construire [2, 3, 4]. La définition du produit tensoriel utilise les applications bilinéaires entre modules (et plus généralement les applications multilinéaires). Nous donnons quelques exemples pour illustrer l'utilisation du produit tensoriel.

Mais l'exemple le plus important fait l'objet du troisième chapitre. C'est celui de la téléportation quantique [7]. Ici l'anneau est le corps $\mathbb{C}$ des nombres complexes et les modules sont des espaces vectoriels complexes, plus exactement des espaces de Hilbert (munis donc d'un produit scalaire hermitien). Ces espaces sont ceux donnés par le premier postulat de la mécanique quantique et décrivent donc des systèmes physiques concrets. Aprés le rappel de quelques notions de calcul quantique nous présentons le protocole de téléportation quantique et nous verrons comment le produit tensoriel intervient de manière systématique dans sa formulation.

Chapitre 1

Modules sur un anneau

Dans ce premier chapitre on donne la définition d'un module sur un anneau commutatif R. Quand l'anneau est un corps c'est la définition d'un espace vectoriel. On commence par rappeler les différentes notions dont on aura besoin par la suite, en donnant notamment les définitions et principales propriétés des groupes et anneaux. Nous présentons aussi les modules libres et les modules projectifs qui sont des facteurs de sommes directes dans des modules libres. Cette caractérisation utilise la notion de suite exacte de modules en remarquant qu'une somme directe est une suite exacte particulière. Nos références pour ce chapitre sont [1] et [2]

1.1 Groupes et Anneaux

1.1.1 Groupes

Soit G un ensemble. Une loi de composition interne $*$ sur G est une application $G \times G \longrightarrow G$ qui à deux éléments $x, y \in G$, associe un troisième élément $x * y$. On dit aussi que $*$ est une opération sur G et on parle du couple $(G, *)$. Comme exemple on peut prendre $*$ = addition dans $\mathbb{N}, \mathbb{Z}$ ou $\mathbb{Q}$ ou encore $* = \cup$ ou $\cap$ dans $G = P(A)$, l'ensemble des parties d'un ensemble quelconque A.

La loi $*$ est associative si $x * (y * z) = (x * y) * z, \forall x, y, z \in G$. Elle est commutative si $x * y = y * x, \forall x, y \in G$. Soit $e \in G$. On dit que e est un élément neutre pour $*$ si $x * e = e * x = x, \forall x \in G$. 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 $(G, *)$ ayant un élément neutre est appelé monoide. Par exemple $(\mathbb{N}, +)$ est un monoide d'élément neutre 0.

Soit e un élément neutre de $(G, *)$. Soient x, x' deux éléments de G. 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 $x'' = e * x'' = (x' * x) * x'' = x' * (x * x'') = x' * e = x'$. Par exemple, dans $(\mathbb{N}, +)$, aucun élément autre que 0 n'a de symétrique. Le symétrique de 0 est 0. Dans $(\mathbb{Z}, +)$, tout élément a un symétrique : le symétrique de x est $-x$. Dans $(\mathbb{Z}, \times)$, l'élément neutre est 1 et c'est le seul élément qui ait un symétrique.

Définition 1.1.1. *$(G, *)$ 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.

Par exemple $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ sont des groupes. L'élément neutre est 0 et le symétrique de x est $-x$. L'associativité est évidente. $(\mathbb{N}, +)$ n'est pas un groupe car aucun élément autre que 0 n'a de symétrique. $(\mathbb{Z}, \times)$ 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. $(\mathbb{Q}^* = \mathbb{Q} - \{0\}, \times)$ est un groupe ainsi que $(\mathbb{R}^* = \mathbb{R} - \{0\}, \times)$. L'élément neutre est 1 et le symétrique de x est $x^{-1} = \dfrac{1}{x}$

Définition 1.1.2. *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.*

On note $H < G$. 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 : $e_G = e_H$. Par exemple pour $* = +$, on a des inclusions de sous-groupes : $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$. Pour $* = \times$, on aussi

des inclusions : $\{1\} < \{-1, 1\} < \mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$. 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 1.1.3. *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 $\dfrac{G}{H}$ 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 $*$ et 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 $Ker\phi = H$. Si 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 :

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

Dans la suite un groupe $(G, *)$ sera noté multiplicativement : $* = \cdot$ 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 $-x$.

1.1.2 Anneaux

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

Définition 1.1.4. *On dit que le triplet $(A, +, \cdot)$ est un anneau si :*

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

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

$$(x + y) \cdot z = x \cdot z + y \cdot z$$

Si la loi $\cdot$ est commutative, l'anneau est dit commutatif ou abélien. On notera le plus souvent $x \cdot y = xy$.

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

Définition 1.1.5. *Soit $(A, +, \cdot)$ un anneau soit B une partie de A contenant 1_A et stable pour les lois $+$ et $\cdot$. 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 nécessaire. 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 $(\mathbb{Q}, +, \cdot)$. 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 $xy \in B$.

Définition 1.1.6. *Une partie I d'un anneau A est appelé idéal à gauche (respectivement à droite) si :*

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

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.

Si A est commutatif, les idéaux à gauche et à droite coincident. Remarquer que $\{0_A\}$ et A sont des idéaux de A. Ils sont appelés idéaux triviaux. Les autres idéaux de A sont dits propres. 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 :

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

Dans la suite, on va considérer uniquement des anneaux commutatifs. On dira donc anneau pour anneau commutatif.

Définition 1.1.7. *Soit A un anneau et soit $a \in A$. Alors l'ensemble $I = aA = \{ax, x \in A\}$ 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. Par exemple $(\mathbb{Z}, +, .)$ 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 $\mathbb{Z}$. L'intersection d'un nombre quelconque d'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 $x_k \in G$. 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. Enfin le produit de deux idéaux I et J est l'idéal IJ engendré par les produits xy 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 $y_i \in J$.

Définition 1.1.8. *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 $ab = 0$. 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 $ab = 0$ n'a pas de solution non nulle dans $\mathbb{Z}$ qui est donc un anneau intègre.*

Définition 1.1.9. *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 1.1.1. *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 $d(b + a)bx = b \in I$ (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. □

Proposition 1.1.2. *Une application $f : A \longrightarrow B$ entre deux anneaux est un morphisme si :*

$$f(x + y) = f(x) + f(y)$$
$$f(xy) = f(x)f(y)$$
$$f(1_A) = 1_B$$

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 :

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

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

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

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 $\overline{\cdot}$ en posant : $\overline{x} \ \overline{+} \ \overline{y} = \overline{x + y}$ et $\overline{x} \ \overline{y} = \overline{xy}$. 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 1.1.1. *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 1.1.3. *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 $ab \in I$. 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 $ab \in I$. Donc $\overline{a}\overline{b} = \overline{0}$ 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. □

1.1.3 Corps

Définition 1.1.10. *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 $ab = 0$ et supposons $a \neq 0$. On a alors $a^{-1}ab = b = 0$.

Remarque 1.1.1. *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, $Ker f$ etant un idéal, il doit-être égal à $\{0\}$.*

Proposition 1.1.4. *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 $b + xa = 1$ ou encore $xa = 1 - b \in 1 + I = \overline{1}$. Ce qui veut dire que $\overline{xa} = \overline{1}$ 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 $\overline{y} : \overline{xy} = \overline{1}$. Donc $xy \in 1 + I$ et $1 \in I + xA$. □

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 :

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

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

1.2 Module sur un anneau

1.2.1 Définition

Soit R un anneau unitaire d'élement neutre 1 pour la multiplication et soit M un groupe abélien.

Définition 1.2.1. *On dit que M est un module à gauche sur R si on a une application (une opération à gauche de R sur M)*

$$R \times M \longrightarrow M$$
$$(r, m) \longmapsto rm$$

telle que :

1. *r(m+n)=rm+rn*
2. *(r+s)m=rm+sm*
3. *(rs)m=r(sm)*
4. *1m=m*

pour tous $r, s \in R$ et tous $m, n \in M$.

On dit que M est un module à droite sur R si on a une opération à droite de R sur M :

$$R \times M \longrightarrow M$$
$$(r, m) \longmapsto mr$$

telle que :

1. *(m+n)r=mr+nr*
2. *m(r+s)=mr+ms*
3. *m(rs)=(mr)s*
4. *m1=m*

pour tous $r, s \in R$ *et tous* $m, n \in M$.

Si R est un anneau commutatif, tout module M à gauche sur R est aussi un module à droite sur R en posant :

$$mr = rm$$

Dans la suite de ce mémoire, on travaillera uniquement avec des anneaux commutatifs. On ne fera donc pas de distinction entre module à gauche et module à droite. On parlera tout simplement de module sur un anneau.

Quand $R = K$ est un corps cette définition n'est autre que celle d'un espace vectoriel sur le corps K. C'est ainsi que toute l'algèbre linéaire des espaces vectoriels rentre dans le cadre de la théorie des modules.

Exemple 1.2.1. *1. Tout groupe abélien G est un $\mathbb{Z}$-module avec $\mathbb{Z}$ l'anneau des entiers en posant :*

$$ng = \underbrace{g + g + \cdots + g}_{n fois}$$

pour $n \in \mathbb{Z}$ et $g \in G$, l'addition $+$ est l'addition dans le groupe G.

2. *Tout idéal I d'un anneau R est un R-module. En effet comme I est un idéal de R, on a $ra \in I$ pour tout $r \in R$ et tout $a \in I$ (le multiplication est celle de l'anneau R). Ceci définit une opération de R sur I qui a les propriétés requises.*

3. *Soit S un sous-anneau de R. Soit M est un R-module. En prenant comme opération de S sur M la restriction de l'opération de R sur M, M devient un S-module.*

4. *Soit $\phi : R \longrightarrow S$ un morphisme d'anneaux et soit M un S-module. Alors M devient aussi un R-module en posant :*

$$rm = \phi(r)m$$

5. *Soit $M = R[X]$ l'anneau des pôlynomes à une variable à coefficients dans R. Alors M est un R-module. Si $P = a_0 + a_1X + \ldots + a_nX^n \in R[X]$ avec $a_0, \ldots, a_n \in R$, on pose*

$$rP = ra_0 + ra_1X + \ldots + ra_nX^n$$

La multiplication est celle de l'anneau R.

Définition 1.2.2. *Soit R un anneau et soit M un R-module. Une partie $N \subseteq M$ est appelée un sous-module de M si N est un sous-groupe de M et pour tout $(r, n) \in R \times N$ on a $rn \in N$. Autrement dit N est un sous-groupe de M et N est stable sous l'action de R.*

Si M un R-module et si $N, N^{'}$ sont des sous-modules de M on peut définir leur somme $N + N^{'} = \{x + y / x \in N, y \in N^{'}\}$. C'est un sous-module de M avec l'opération évidente

$$r(x + y) = rx + ry$$

L'intersection de N et $N^{'}$ est aussi un sous-module de M. Plus généralement, une intersection quelconque de sous-module de M est un sous-module de M. L'ensemble des sommes finies d'éléments de la forme ax ou $a \in I$ est un idéal de R et $x \in M$ est aussi un sous-module de M, noté IM. L'opération est ici

$$r(ax) = (ra)x$$

ou

$$r(ax) = a(rx)$$

au choix (c'est le même résultat par le fait que I est un idéal et que R est commutatif).

Si N est un sous-module de M, c'est en particulier un sous-groupe de M. Comme on est dans le cas abélien (où tout sous-groupe est invariant) on peut parler du groupe quotient $\dfrac{M}{N}$ des classes d'équivalence modulo N qui est aussi abélien. On a alors la

Proposition 1.2.1. *Soit M un R-module et soit N un sous-module de M, alors le groupe quotient $\dfrac{M}{N}$ est aussi un R-module.*

Preuve. Soit $\overline{m} = m + N$ la classe de m modulo N. On définit une opération de R sur $\dfrac{M}{N}$ en posant $r\overline{m} = \overline{rm}$. Cette opération est bien définie. En effet supposons $\overline{m} = \overline{m'}$ c'est à dire que $m - m' \in N$, alors an a $rm - rm' = r(m - m') \in N$ puisque N est un sous-module et donc $\overline{rm} = \overline{rm'}$ et on vérifie facilement que cette opération vérifie bien les propriétés de la définition d'un module. □

Définition 1.2.3. *Soient M et N deux R-modules. Un morphisme de modules est une application $\phi : M \longrightarrow N$ qui vérifie :*

1. $\phi(m + m') = \phi(m) + \phi(m')$
2. $\phi(rm) = r\phi(m)$

pour tous $m, m' \in M$ et pour tout $r \in N$.

Quand $R = K$ est un corps c'est la définition d'une application linéaire entre espaces vectoriels.

Le noyau de ϕ est $ker\phi = \{m \in M / \phi(m) = 0_N\}$. C'est un sous-module de M. L'image de ϕ est $Im\phi = \{n \in N / \exists m \in N / n = \phi(m)\}$. C'est aussi un sous-module de N. L'application est injective si et seulement si $ker(\phi) = \{0_M\}$. Remarquer que $\{0_M\}$ est un sous-module de M. De même le morphisme ϕ est surjectif si et seulement si $Im(\phi) = N$. ϕ est un isomorphisme si elle est aussi bijective. Un morphisme induit toujours un isomorphisme comme le montre la proposition suivante

Proposition 1.2.2. *Soit $\phi : M \longrightarrow N$ un morphisme de R-modules, alors on a un isomorphisme canonique*

$$\widetilde{\phi} : \frac{M}{ker\phi} \xrightarrow{\cong} Im\phi$$

$$\overline{m} = m + ker\phi \longmapsto \phi(m)$$

Preuve. $\widetilde{\phi}$ est bien définie. En effet si $\overline{m} = \overline{m'}$, alors $m - m' \in ker\phi$ et donc $\phi(m - m') = \phi(m) - \phi(m') = 0$ et donc $\phi(m) = \phi(m')$. Si $\widetilde{\phi}(\overline{m}) = 0$ alors $\phi(m) = 0$ et donc $m \in ker\phi = \overline{0}$. Ceci montre que $\overline{m} = \overline{0}$ et que $\widetilde{\phi}$ est injective. Soit $n \in Im\phi$. Il existe donc $m \in M$ avec $\phi(m) = n$. Donc $\widetilde{\phi}(\overline{m}) = \phi(m) = n$. Il existe donc $\overline{m} \in \dfrac{M}{ker\phi}$ avec $\widetilde{\phi}(\overline{m}) = n$. Ceci montre que $\widetilde{\phi}$ est surjective. □

1.2.2 Sommes directes et suites exactes

Définition 1.2.4. *Soient M et N deux R-modules. Leur somme directe est :*

$$M \oplus N = \{(m, n), m \in M, n \in N\}$$

avec l'opération de R :

$$r(m, n) = (rm, rn)$$

La proposition suivante caractérise la somme directe par une propriétée universelle.

Proposition 1.2.3. *Soient L, M, N trois R-modules. Alors $L \cong M \oplus N$ si st seulement si il existe des morphismes de R-modules $\pi_1 : L \longrightarrow M$, $i_1 : M \longrightarrow L$, $\pi_2 : L \longrightarrow N$ et $i_2 : N \longrightarrow L$ avec*

1. *$\pi_1 \ o \ i_1 = Id_M$ et $\pi_2 \ o \ i_2 = Id_N$*
2. *$\pi_i \ o \ i_j = 0$ si $i \neq j$*
3. *$i_i \ o \ \pi_1 + i_2 \ o \ \pi_2 = Id_L$*

Preuve. Pour tous R-modules M, N on a des morphismes injectifs (des inclusions) :

$$i_1 : M \longrightarrow M \oplus N$$

envoyant m vers $(m, 0)$ et

$$i_2 : N \longrightarrow M \oplus N$$

envoyant n vers $(0, n)$. On a aussi des projections :

$$\pi_1 : M \oplus N \longrightarrow M$$

envoyant (m, n) vers m et

$$\pi_2 : M \oplus N \longrightarrow N$$

envoyant (m, n) vers n. Ces morphismes verifient les trois propriétées de la proposition. Donc si $\phi : L \xrightarrow{\cong} M \oplus N$ est un isomorphisme, alors $\pi_j \circ \phi$ et $\phi^{-1} \circ i_j$ fournissent ces applications sur L pour $j = 1, 2$.

Inversement étant donnés les π_j et les i_j, on définit

$$\psi : M \oplus N \longrightarrow L$$

en posant

$$\psi((m,n)) = i_1(m) + i_2(n)$$

On vérifie facilement que ce sont des morphismes. De plus on a :

$$\phi \circ \psi((m,n)) = \phi(i_1(m) + i_2(n)) = (m,n)$$

et

$$\psi \circ \phi(x) = \psi(\pi_1(x), \pi_2(x)) = x$$

Ceci montre que ϕ et ψ sont inverses l'une de l'autre. □

La propriété universelle dégagée par cette proposition est la suivante : étant donnés deux R-modules M_1, M_2 et un R-module N avec des morphismes $f_j : M_j \longrightarrow N$, alors il existe un unique R-morphisme $f : M_1 \oplus M_2 \longrightarrow N$ tel que $f_i = f \circ i_j$. L'application f est donnée par $f((m_1, m_2)) = f_1(m_1) + f_2(m_2)$.

Une autre caractérisation des sommes directes utilisé le notion de suite exacte.

Définition 1.2.5. *Soient $M_i, i \in \mathbb{Z}$ des R-modules et soit :*

$$.... \xrightarrow{f_{i-2}} M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} .....$$

Une suite de morphismes de modules. Cette suite est dit exacte en M_i si $Kerf_i = Imf_{i-1}$. La suite est dite exacte si elle est exacte en M_i pour tout i.

Une suite exacte pour laquelle $M_i = 0$ pour $\mid i \mid > 1$ est dite suite exacte courte :

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

L'exactitude vent dire ici que f est injective, g est surjective et que $kerg = Imf$.

Exemple 1.2.2. *1. Toute somme directe $M_1 \oplus M_2$ de deux R-modules fait partie d'un suite exacte courte :*

$$0 \longrightarrow M_1 \xrightarrow{i_1} M_1 \oplus M_2 \xrightarrow{\pi_2} M_2 \longrightarrow 0$$

avec $i_1 : M_1 \longrightarrow M_1 \oplus M_2$ l'inclusion et $\pi_2 : M_1 \oplus M_2 \longrightarrow M_2$ la projection.

2. *Soit N un sous-module d'un R-module M. Alors la suite*

$$0 \longrightarrow N \longrightarrow M \longrightarrow \frac{M}{N} \longrightarrow 0$$

est exacte (le premier morphisme est l'inclusion de N dans M et le second est la surjection canonique de M vers son quotient par N). En posant $N = IM$ pour un idéal I de R on obtient une suite exacte :

$$0 \longrightarrow IM \longrightarrow M \longrightarrow \frac{M}{IM} \longrightarrow 0$$

Définition 1.2.6. *Une suite exacte courte de R-modules :*

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

est scindée s'il existe une morphisme $s : N \longrightarrow M$ tel que $g \circ s = Id_M$. Le morphisme s est appelé le scindage de la suite exacte.

La proposition suivante montre le lien entre suites exactes courtes scindées et sommes directes.

Proposition 1.2.4. *: Soit :*

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0$$

une suite exacte courte scindée, alors

$$M \cong M_1 \oplus M_2$$

Preuve. Soit $s : M_2 \longrightarrow M$ un scindage de la suite exacte courte. On définit des applications :

$$\pi_1 : M \longrightarrow M_1 \qquad m \longmapsto f^{-1}(m - sog(m))$$

$$\pi_2 : M \longrightarrow M_2 \qquad m \longmapsto g(m)$$

$$i_1 : M_1 \longrightarrow M \qquad m_1 \longmapsto f(m_1)$$

$$i_2 : M_2 \longrightarrow M \qquad m_2 \longmapsto s(m_2)$$

On a $g(m - s \circ g(m)) = g(m) - g \circ s \circ g(m) = g(m) - g(m) = 0$. Donc $m - s \circ g(m) \in Kerg = Imf$. Ceci montre que i_1 est bien définie. Ces applications vérfient les propriétés 1, 2 et 3 de la proposition 1.2.3 et font donc de M la somme directe de M_1 et M_2. □

1.3 Modules libres et Modules projectifs

Définition 1.3.1. *: Soit M un R-module et soit $X \subset M$ une partie de M. On dit que X engendre M si :*

$$m = \sum_{i=1}^{k} r_i x_i$$

pour tout $m \in M$, avec $r_i \in R$ et $x_i \in X$. Autrement dit tout élément m de M s'écrit comme combinaison linéaire finie sur R d éléments de X. On dit que M est un modules de type fini s'il est engendre par une partie finie X.

Exemple 1.3.1.

1. *Le $\mathbb{Z}$-module $\mathbb{Z}$ est de type fini engendré par $X = \{1\}$.*
2. *Le $\mathbb{Z}$-module $\mathbb{Z}^n$ est de type fini engendré par $X = \{e_1, e_2, ..., e_n\}$ avec $e_i = (0, ..., 1, ..., 0)$.*
3. *Le $\mathbb{Z}$-module $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est engendré par $X = \{\overline{1}\}$ et aussi par $X = \{\overline{m}\}$ avec $pgcd(m, n) = 1$.*
4. *Si $R = K$ est un corps et $M = V$ un K-espace vectoriel, une partie génératrice de V est une partie génératrice au sens de l'algèbre linéaire.*

Si M un R-module de type fini engendré par $X = \{x_1, x_2, ..., x_n\} \subseteq M$, alors on a une application :

$$\phi : R^n \longrightarrow M \qquad (r_1, .., r_n) \longmapsto \sum_{i=1}^{n} r_i x_i$$

ϕ est un morphisme surjectif de modules. Remarquer que R^n est aussi un R-module engendré par $X = \{e_1, ..., e_n\}$.

Définition 1.3.2. *: Soit M un R-module engendré par $X \subseteq M$. On dit que X est une base de M si tout élément $m \in M$ s'écrit de manière unique comme combinaison linéaire finie (sur R) des éléments de X :*

$$m = \sum_{i=1}^{k} r_i x_i$$

ou de manière équivalente

$$\sum_{i=1}^{n} r_i x_i = 0 \Rightarrow r_i = 0, \forall i$$

pour toute partie finie $\{x_1, x_2, ..., x_n\} \subseteq X$. *Autrement dit* X *est une base de* M *si toute sous-partie finie de* X *est linéairment indépendante sur* R.

Cette définition généralise le notion de base d'un espace vectoriel en algébre linéaire.

Soit R un anneau et soit I un ensemble d'indices. Soit $\{M_i, i \in I\}$ un ensemble de R-modules indexé par I. On définit le module somme directe des M_i noté $\oplus_{i\in I} M_i$ comme étant l'ensemble des tuples $(m_i)_{i\in I}$ avec $m_i \in M_i$ et $m_i = 0$ pour presque tout i. Presque tout i veut dire que tous les m_i sont nuls sauf un nombre fini. L'opération de R sur $\oplus_{i\in I} M_i$ est donnée par $r((m_i)_{i\in I}) = (rm_i)_{i\in I}$. Soit par exemple $R^\infty = \oplus_{n\in\mathbb{N}} R = \oplus_{n=0}^{\infty} R$. Donc ici $I = \mathbb{N}$ et $M_i = R$ pour tout i. R^∞ a une base (infinie) formée des éléments $e_i = \{0, \ldots, 1, \ldots, 0\}$ avec 1 en position $i \in \mathbb{N}$.

Proposition 1.3.1. *: Soit* M *un* R*-module et soit* $X \subseteq M$ *une base de* M*, alors on a un isomorphisme :*

$$M \cong \oplus_{x\in X} R$$

Preuve. On définit une application

$$\phi : \oplus_{x\in X} R \longrightarrow M \qquad (r_x)_{x\in X} \longmapsto \sum_{x\in X} r_x x$$

L'application ϕ est bien définie car $r_x = 0$ pour presque tout x et donc la somme à droite est bien finie. Comme X engendre M, ϕ est surjective. Il nous reste à montrer que ϕ est injective (ϕ est clairement un morphisme de modules). Supposons $\phi((r_x)_{x\in X}) = 0$ donc $\sum_{x\in X} r_x x = 0$. Comme X est une base, on doit avoir $r_x = 0$, pour tout $x \in X$ et donc $(r_x)_{x\in X} = 0$. □

Définition 1.3.3. *Un* R*-module* M *est dit libre s'il a une base* $X \subseteq M$.

Par exemple pour tout $n \geq 1$, le R-module $R^n = R \times R \times ..... \times R$ est libre engendré par $X = \{e_1, e_2, ..., e_n\}$ avec $e_i = (0, \ldots, 1, \ldots, 0)$. La base ici est finie.

Soit M un R-module, alors il existe un R-module libre F et un morphisme surjectif $f : F \longrightarrow M$. En effet Soit X une partie génératrice de M (on peut toujours prendre $X = M$). L'application :

$$f : \oplus_{x\in X} R \longrightarrow M \qquad (r_x)_{x\in X} \longmapsto \sum_{x\in X} r_x.x$$

est bien un morphisme surjectif et $F = \oplus_{x\in X} R$ est libre.

Une classe importante de R-modules est constituée par les modules projectifs.

Définition 1.3.4. *Un R-module P est dit projectif si pour tout R-module M, tout morphisme surjectif $g : M \longrightarrow P$ a un scindage $s : P \longrightarrow M$ et donc $g \circ s = Id_P$.*

Leur interêt provient de le proposition suivante

Proposition 1.3.2. *Soit P un R-module, alors P est projectif si et seulement il existe un R-module Q tel que*

$$P \oplus Q \cong \oplus_{x\in X} R$$

pour un certain ensemble X. Autrement dit un module P est projectif s'il rentre dans une somme directe d'un module libre. Si P est de type fini alors X peut être choisi fini.

Preuve. On sait qu'il existe un module libre F et un morphisme surjectif $g : F \longrightarrow P$. Si X est une partie génératrice de P (par exemple $X = P$), on peut prendre $F = \oplus_{x\in X} R$ et g est l'application qui envoie $(r_x)_{x\in X}$ vers $\sum_{x\in X} r_x x$. Comme P est projectif, il existe un scindage $s : P \longrightarrow F$. Si on pose $Q = Ker g$, on obtient une suite exacte courte scindée

$$0 \longrightarrow Q \longrightarrow F \longrightarrow P \longrightarrow 0$$

et donc $P \oplus Q \cong F$. □

Par exemple tout module libre P est projectif. En effet il suffit de prendre $Q = \{0\}$ le module nul.

Une autre définition des modules projectifs souvent utilisée est donnée par le proposition suivante :

Proposition 1.3.3. *Soit P un R-module, alors P est projectif si pour tous morphismes $f : P \longrightarrow M$ et $g : N \longrightarrow M$ avec g surjective, il existe un morphisme $h : P \longrightarrow N$ tel que $g \circ h = f$.*

Preuve. Supposons P projectif. Il se situe dans une suite exacte scindée

$$0 \longrightarrow Q \longrightarrow F \longrightarrow P \longrightarrow 0$$

Notons $s : P \longrightarrow F$ le scindage de $l : F \longrightarrow P$. Si $g : N \longrightarrow M$ est surjective on obtient une suite exacte courte

$$0 \longrightarrow Kerg \longrightarrow N \longrightarrow M \longrightarrow 0$$

Par surjectivité de g, on peut trouver un morphisme $k : F \longrightarrow N$ tel que $(g \circ k)(x) = (f \circ l)(x)$ pour tout $x \in F$. En effet il existe $y \in N$ tel que $g(y) = f(p)$ (car g est surjective). On pose $k(x) = y$. On définit alors $h : P \longrightarrow N$ en posant $h(p) = k(s(p))$. On a bien $g(h(p)) = g(k(s(p)) = (f(l(s(p)) = f(p)$ et donc $g \circ h = f$. Inversement Soit $g : M \longrightarrow P$ surjective. En appliquant l'hypothèse à $M = N$ et $Id_P : P \longrightarrow P$, on obtient qu'il existe $h = s : P \longrightarrow M$ telle que $g \circ s = Id_P$. C'est la définition d'un module projectif. □

Si M et N sont des R-modules, l'ensemble $Hom_R(M, N)$ des morphismes entre M et N est un groupe abélien pour l'addition des applications :

$$(f + g)(m) = f(m) + g(m)$$

Si M est fixé alors l'application :

$$Hom_R : N \longmapsto Hom_R(M, N)$$

associe à un $R - moduleN$, un groupe abélien. Tout morphisme $\phi : N \longrightarrow L$ de R-modules induit un morphisme de groupes abéliens :

$$\phi_* : Hom_R(M, N) \longrightarrow Hom_R(M, L) \qquad f \longmapsto \phi \circ f$$

En utilisant ces Hom, on peut donner une autre caractérisation des modules projectifs faisant intervenir les suites exactes courtes.

Proposition 1.3.4. *Le R-module P est projectif si et seulement si pour toute suite exacte courte de R-modules :*

$$0 \longrightarrow M \xrightarrow{\phi} N \xrightarrow{\psi} L \longrightarrow 0$$

le suite :

$$0 \longrightarrow Hom_R(P, M) \xrightarrow{\phi_*} Hom_R(P, N) \xrightarrow{\psi_*} Hom_R(P, L) \longrightarrow 0$$

est une suite exacte des groupes abéliens.

Preuve. Il suffit d'utiliser la proposition précédente. Nous laissons les détails au lecteur. □

Chapitre 2

Produit tensoriel de modules

Ce chapitre constitue le coeur de ce travail. On y définit le produit tensoriel de deux modules par une propriété universelle et on construit explicitement ce produit tensoriel en montrant notamment qu'il est unique à isomorphismes prés. L'outil technique utilisé tant dans la définition que la construction est la notion d'application bilinéaire (et multilinéaire) de deux modules vers un troisième module. Nous donnons quelques exemples d'utilisation du produit tensoriel qui peuvent être utiles en Algèbre. Enfin nous mentionnons rapidement les deux opérations importantes de restriction et d'extension des scalaires quand on dispose d'un morphisme d'anneaux $R \longrightarrow S$. Pour ce chapitre nous avons utilisé [2], [3] et [4].

2.1 Applications bilinéaires

Soit R un anneau et soient M, N, P des R-modules.

Définition 2.1.1. *Une application $b : M \times N \longrightarrow P$ est dite bilinéaire si :*

1. $b(m_1 + m_2, n) = b(m_1, n) + b(m_2, n)$ *et* $b(rm, n) = rb(m, n)$ *pour tous* $m_1, m_2, m \in M, n \in N$ *et* $r \in R$.

2. $b(m, n_1 + n_2) = B(m, n_1) + B(m, n_2)$ *et* $b(m, rn) = rb(m, n)$ *pour tous* $m \in M, n_1, n_2, n \in N$ *et* $r \in R$.

Autrement dit $b(m, .)$ est un morphisme (application linéaire) de $N \longrightarrow P$ et $b(., n)$ est un morphisme (application linéaire) de $M \longrightarrow P$ pour tout $m \in M$ et tout $n \in N$. L'ensemble des applications bilinéaires $M \times N \longrightarrow P$ sera noté $Bil(M, N, P)$. Il a une structure naturelle de R-module.

Exemple 2.1.1. *1. Prenons $M = N = P = R$ vu comme module sur lui-même. Alors la multiplication d'anneau :*

$$R \times R \longrightarrow R$$

est une application bilinéaire.

2. *Soit M un R-module. Alors la multiplication par les scalaires :*

$$R \times M \longrightarrow M$$

est bilinéaire (R est vu comme module sur lui-même).

3. *Soit $Hom_R(N, P)$ l'ensemble des morphismes de N vers P. Il a une structure naturelle de R-module. Soit $f : M \longrightarrow Hom_R(N, P)$ un morphisme de R-modules. Alors l'application :*

$$b : M \times N \longrightarrow P \qquad (m, n) \longmapsto f(m)(n)$$

est une application bilinéaire.

Il existe bien sûr des fonctions non bilinéaires. Par exemple si M est un R-module, alors l'addition :

$$M \times M \longrightarrow M \qquad (m_1, m_2) \longmapsto m_1 + m_2$$

n'est pas bilinéaire puisqu'en général :

$$(m_1 + m_2) + m \neq (m_1 + m) + (m_2 + m)$$

Les applications multilinéaires généralisent les applications bilinéaires.

Définition 2.1.2. *Soient $M, M_1, M_2, ..., M_k$ des R-modules. Une application*

$$f : M_1 \times ..... \times M_k \longrightarrow M \qquad (m_1, ..., m_k) \longmapsto f(m_1, ..., m_k)$$

est dite multilinéaire si elle est linéaire en chaque m_i avec les autres variables fixées.

Remarquer que contrairement aux morphismes de modules, les applications bilinéaires (et multilinéaires) n'ont pas de noyau (car $M \times N$ n'est pas un module en général) et leurs images ne forment pas des sous-modules non plus.

2.2 Définition et Construction du produit tensoriel

Définition 2.2.1. *Soient M et N deux R-modules. On appelle produit tensoriel de M et N (sur R) un R-module noté $M \otimes_R N$ muni d'une application bilinéaire $M \times N \xrightarrow{\otimes} M \otimes_R N$ telle que pour toute application bilinéaire $M \times N \xrightarrow{B} P$, il existe un morphisme (application linéaire) unique $M \otimes_R N \xrightarrow{L} P$ tel que $B = L \circ \otimes$.*

Nous allons montrer que le produit tensoriel $M \otimes_R N$ existe toujours et est unique (à isomorphisme prés).

Définition 2.2.2. *Soit X un ensemble. Le groupe abélien libre sur X est le groupe*

$$F(X) = \oplus_{x \in X} \mathbb{Z}$$

C'est l'ensemble des sommes finies

$$\sum_{i=1}^{k} n_i x_i$$

avec $x_i \in X$ et $n_i \in \mathbb{Z}$. Si $Y \subset X$, le sous-groupe de $F(X)$ engendré par Y est l'ensemble des sommes finies

$$\sum_{i=1}^{k} n_i y_i$$

avec $y_i \in Y$ et $n_i \in \mathbb{Z}$.

Si M et N sont deux R-modules, on applique cette définition à $X = M \times N$ pour obtenir le groupe abélien libre $F(M \times N)$. Ses éléments sont les sommes finies

$$\sum_{i=1}^{k} a_i (m_i, n_i)$$

avec $a_i \in \mathbb{Z}$, $m_i \in M$ et $n_i \in N$.

Soit $G \subset F(M \times N)$ le sous-groupe engendré par les éléments de la forme :

- $(m + m', n) - (m, n) - (m', n)$

- $(m, n + n^{'}) - (m, n) - (m, n^{'})$
- $(rm, n) - (m, rn)$

avec $m, m^{'} \in M$, $n, n^{'} \in N$ et $r \in R$. Posons

$$M \otimes_R N \stackrel{def}{=} \frac{F(M \times N)}{G}$$

La classe d'équivalence de (m, n) modulo G sera notée $m \otimes n$:

$$m \otimes n = \overline{(m, n)}$$

L'application quotient sera notée :

$$\pi : F(M \times N) \longrightarrow M \otimes_R N \qquad (m, n) \longmapsto \pi(m, n) = m \otimes n$$

Remarquer que $\pi(G) = 0$.

Proposition 2.2.1. *Le groupe abélien $M \otimes_R N$ est engendré par les éléments de la forme $m \otimes n$ avec $m \in M$ et $n \in N$. Ces éléments satisfont aux relations :*

- $(m + m^{'}) \otimes n = m \otimes n + m^{'} \otimes n$
- $m \otimes (n + n^{'}) = m \otimes n + m \otimes n^{'}$
- $rm \otimes n = m \otimes rn$

De plus $M \otimes_R N$ est un R-module.

Preuve. Les éléments $m \otimes n$ engendrent $M \otimes_R N$ car les éléments (m,n) engendrent $F(M \times N)$ et parce que l'application :

$$F(M \times N) \longrightarrow M \otimes_R N$$

est surjective. Les relations d'écoulent de la définition de G. Par exemple :

$$(m + m^{'}) \otimes n - m \otimes n - m^{'} \otimes n = \pi((m + m^{'}, n) - (m, n) - (m^{'}, n)) = 0$$

car $(m + m^{'}, n) - (m, n) - (m^{'}, n) \in G, \ldots, etc.$ Pour $r \in R$, on pose :

$$r(m \otimes n) = (rm) \otimes n = m \otimes (rn)$$

Ceci définit une opération de R sur $M \otimes_R N$ qui fait de celui-ci un R-module. □

Remarquer qu'on a automatiquement une application bilinéaire :

$$\otimes : M \times N \longrightarrow M \otimes_R N \qquad (m,n) \longmapsto m \otimes n$$

On peut maintenanténoncer le résultat principal de ce chapitre :

Théorème 2.2.1. *Le produit tensoriel de deux R-modules M et N existe et est unique à isomorphisme prés.*

Preuve. On pose

$$M \otimes_R N = \frac{F(M,N)}{G}$$

On a vu que c'est un R-module et qu'il est muni d'une application bilinéaire :

$$\otimes : M \times N \longrightarrow M \otimes_R N \qquad (m,n) \longmapsto m \otimes n$$

Il reste à montrer que pour toute application bilinéaire $M \times N \xrightarrow{B} P$ il existe un unique morphisme

$$L : M \otimes_R N \longrightarrow P$$

tel que $B = L \circ \otimes$. Définissans L par $L(m \otimes n) = B(m,n)$. L est bien définie car B étant bilinéaire, elle s'annule sur $G \subset F(M,N)$ et on a bien :

$$B(m,n) = L \circ \otimes(m,n) = L(m \otimes n)$$

Si $L^{'}$ est un autre morphisme tel que $B = L^{'} \circ \otimes$, on doit avoir $L(m \otimes n) = L^{'}(m,n)$ et donc $L = L^{'}$. Ceci prouve l'unicité de L.

Soient $T, T^{'}$ deux produits tensoriels de M et N (sur R). Nous devons montrer qu'il existe un isomorphisme $f : T \longrightarrow T^{'}$. Par hypothése on a des applications bilinéaires $M \times N \xrightarrow{b} T$ et $M \times N \xrightarrow{b^{'}} T'$ qui vérifient la propriété universelle du produit tensoriel. Pour toutes applications bilinéaires $B : M \times N \longrightarrow P$ et $B^{'} : M \times N \longrightarrow P$, il existe des morphismes uniques $L : T \longrightarrow P$ et $L^{'} : T^{'} \longrightarrow P$ qui vérifient $B = L \circ b$ et $B^{'} = L^{'} \circ b^{'}$. En prenant pour P respectivement T et $T^{'}$ avec $B = b$ et $B^{'} = b^{'}$, on obtient deux morphismes $L^{'} : T^{'} \longrightarrow T$ et $L : T \longrightarrow T^{'}$. De $b = L^{'} \circ b^{'}$ et $b^{'} = L \circ b$, on tire $b = (L^{'} \circ L) \circ b$ et $b^{'} = (L \circ L^{'}) \circ b^{'}$. Par unicité des morphismes de la propriété universelle du produit tensoriel, on doit avoir $L \circ L^{'} = Id_{T'}$ et $L^{'} \circ L = Id_T$. On obtient donc un isomorphisme $L : T \longrightarrow T^{'}$ d'inverse $L^{'}$. □

Exemple 2.2.1. *1. Dans $M \otimes_R N$, on a $m \otimes 0 = 0$ et $0 \otimes m = 0$. En effet on a $m \otimes 0 = m \otimes (0+0) = m \otimes 0 + m \otimes 0$ et donc $m \otimes 0 = 0$. On montre de même que $0 \otimes m = 0$.*

2. Soit A un groupe abélien dont tout élément est d'ordre fini. Regardons A comme un $\mathbb{Z}$-module. Alors on a $\mathbb{Q} \otimes_{\mathbb{Z}} A = 0$. En effet soit $a \in A$ et soit $n \in \mathbb{N}/na = 0$. Alors on a dans $\mathbb{Q} \otimes_{\mathbb{Z}} A$:

$$r \otimes a = n(\frac{r}{n}) \otimes a = \frac{r}{n} \otimes na = \frac{r}{n} \otimes 0 = 0$$

3. $m \otimes n = 0$ si et seulement si toute application bilinéaire sur $M \times N$ s'annule en (m, n).

4. $M \otimes_R N = 0$ si et seulement si toute application bilinéaire sur $M \times N$ est l'application nulle

Pour finir cette section remarquons que le produit tensoriel se généralise à un nombre quelconque de modules. Si $M_1, \ldots, M_k$ sont des R-modules le produit tensoriel $M_1 \otimes_R \ldots \otimes_R M_k$ est un R-module qui vérifie une propriété universelle concernant les applications multilinéaires. L'image de $(m_1, \ldots, m_k)$ est notée $m_1 \otimes \ldots \otimes m_k$. La construction de $M_1 \otimes_R \ldots \otimes_R M_k$ se fait de le même maniére que dans le cas de deux modules.

2.3 Exemples de produit tensoriel

Pour illustrer le théorie générale, on présente ici quelque exemples de produits tensoriels.

2.3.1 Congruences

Soient a et b deux entiers positifs et soit $d = pgcd(a, b)$. Les groupes abéliens de congruences $\frac{\mathbb{Z}}{a\mathbb{Z}}$ et $\frac{\mathbb{Z}}{b\mathbb{Z}}$ peuvent être vus comme des $\mathbb{Z}$-modules et on peut donc parler du produit tensoriel $\frac{\mathbb{Z}}{a\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{b\mathbb{Z}}$. On a alors :

$$\frac{\mathbb{Z}}{a\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{b\mathbb{Z}} \cong \frac{\mathbb{Z}}{d\mathbb{Z}}$$

En particulier $\frac{\mathbb{Z}}{a\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{b\mathbb{Z}} = 0 \iff pgcd(a,b) = 1$. En effet $\frac{\mathbb{Z}}{a\mathbb{Z}}$ et $\frac{\mathbb{Z}}{b\mathbb{Z}}$ sont tous deux engendrés par (la classe de) 1. Donc $1 \otimes 1$ engendre $\frac{\mathbb{Z}}{a\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{b\mathbb{Z}}$ et on a :

$$a(1 \otimes 1) = a \otimes 1 = 0 \otimes 1 = 0$$
$$b(1 \otimes 1) = 1 \otimes b = 1 \otimes 0 = 0$$

Donc l'ordre de $1 \otimes 1$ divise a et b et donc aussi $d = pgcd(a,b)$. Donc l'ordre de $\frac{\mathbb{Z}}{a\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{b\mathbb{Z}}$ est au plus d. Soit l'application bilinéaire :

$$B : \frac{\mathbb{Z}}{a\mathbb{Z}} \times \frac{\mathbb{Z}}{b\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{d\mathbb{Z}} \qquad (x \pmod a, y \pmod b) \longmapsto xy \pmod d$$

Par la propriété universelle du produit tensoriel, il existe un unique

$$f : \frac{\mathbb{Z}}{a\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{b\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{d\mathbb{Z}}$$

tel que $f(x \otimes y) = xy$. En particulier $f(x \otimes 1) = x$ et donc f est surjective. $\frac{\mathbb{Z}}{a\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{b\mathbb{Z}}$ a donc au moins d éléments. Par exemple

$$\frac{\mathbb{Z}}{3\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{5\mathbb{Z}} = 0$$

2.3.2 Anneaux quotients

Soit R un anneau (commutatif) et soient I et J deux ideaux de R. Les anneaux quotient $\frac{R}{I}$ et $\frac{R}{J}$ sont des R-modules de manière naturelle et on a :

$$\frac{R}{I} \otimes_R \frac{R}{J} \cong \frac{R}{I+J} \qquad (\overline{x}, \overline{y}) \longmapsto \overline{xy}$$

En pratique en prenant $I = J = 0$, on a :

$$R \otimes_R R \cong R \qquad x \otimes y \longmapsto xy$$

(Si $R = \mathbb{Z}, I = a\mathbb{Z}$ et $J = b\mathbb{Z}$ on retrouve l'exemple précédent). Ceci se montre comme suit. Soit l'application bilinéaire

$$B : \frac{R}{I} \times \frac{R}{J} \longrightarrow \frac{R}{I+J} \qquad (x \pmod I, y \pmod J) \longmapsto xy \pmod K$$

avec $K = I + J$. Par la propriété universelle du produit tensoriel il existe un unique

$$f : \frac{R}{I} \otimes_R \frac{R}{J} \longrightarrow \frac{R}{I+J}$$

tel que $f(x \pmod I \otimes y \pmod J) = xy \pmod K$. Considérons l'application :

$$g : R \longrightarrow \frac{R}{I} \otimes_R \frac{R}{J} \qquad r \longmapsto r(\overline{1} \otimes \overline{1}) = r(1 \pmod I \otimes 1 \pmod J)$$

g est linéaire. De plus :

1. $r \in I \Rightarrow g(r) = r(\overline{1} \otimes \overline{1}) = \overline{r} \otimes \overline{1} = \overline{0} \otimes \overline{1} = 0$
2. $r \in J \Rightarrow g(r) = r(\overline{1} \otimes \overline{1}) = \overline{1} \otimes \overline{r} = \overline{1} \otimes \overline{0} = 0$

donc $I + J \in Ker g$ et g passe au quotient :

$$g : \frac{R}{I+J} \longrightarrow \frac{R}{I} \otimes_R \frac{R}{J} \qquad r \pmod K \longmapsto r(\overline{1} \otimes \overline{1}) = \overline{r} \otimes \overline{1} = \overline{1} \otimes \overline{r}$$

Montrons que g est l'inverse de f. On a :

$$f(g(r \pmod K)) = f(\overline{r} \otimes \overline{1}) = r \pmod K$$

et donc $f \circ g = Id_{\frac{R}{I+J}}$. Pour calculer $g \circ f$, remarquons que tout tenseur élémentaire $\overline{x} \otimes \overline{y}$ de $\frac{R}{I} \otimes_R \frac{R}{J}$ s'écrit :

$$\overline{x} \otimes \overline{y} = x\overline{1} \otimes y\overline{1} = xy(\overline{1} \otimes \overline{1}) = r(\overline{1} \otimes \overline{1})$$

donc

$$g(f(r(\overline{1} \otimes \overline{1}))) = rg(1 \pmod K) = r(\overline{1} \otimes \overline{1})$$

et donc

$$g \circ f = Id_{\frac{R}{I} + \frac{R}{J}}$$

Ceci montre que :

$$f : \frac{R}{I} \otimes_R \frac{R}{J} \xrightarrow{\cong} \frac{R}{I+J}$$

2.3.3 Modules quotients

Soient R un annueau I un idéal de R. $\dfrac{R}{I}$ est un R-module. Si M est un R-module alors on a un isomorphisme :

$$\frac{R}{I} \otimes_R M \longrightarrow \frac{M}{IM} \qquad \overline{r} \otimes m \longmapsto \overline{rm}$$

En particulier si $I = (0)$, alors $R \otimes_R M \cong M$ par $r \otimes m \longmapsto rm$ et $R \otimes_R R \cong R$ par $r \otimes r^{'} \longmapsto rr^{'}$. En effet soit l'application bilinéaire :

$$B : \frac{R}{I} \times M \longrightarrow \frac{M}{IM} \qquad (\overline{r}, m) \longmapsto \overline{rm}$$

Par la propriété universelle du produit tensoriel, il existe un unique

$$f : \frac{R}{I} \otimes_R M \longrightarrow \frac{M}{IM}$$

tel que $f(\overline{r} \otimes m) = \overline{rm}$. Montrons que f est un isomorphisme. Soit l'application

$$g : M \longrightarrow \frac{R}{I} \otimes_R 0M \qquad m \longmapsto \overline{1} \otimes m$$

g est linéaire en m. IM est engendré par les rm pour $r \in I$ et $m \in M$ et on a :

$$g(rm) = \overline{1} \otimes rm = \overline{r} \otimes m = \overline{0} \otimes m = 0$$

donc g annule IM et passe donc au quotient :

$$g : \frac{M}{IM} \longrightarrow \frac{R}{I} \otimes_R M \qquad \overline{m} \longmapsto \overline{1} \otimes m$$

On a $f(g(\overline{m})) = f(\overline{1} \otimes m) = \overline{1m} = \overline{m}$. Donc $f \circ g = Id_{\dfrac{M}{\overline{IM}}}$. Pour calculer $g \circ f$, remarquons que tout tenseur de $\dfrac{R}{I} \otimes_R M$ est de la forme $\overline{1} \otimes m$, puisque un tenseur élémentaire est de la forme

$$\overline{r} \otimes m = \overline{1} \otimes rm$$

et tout tenseur est somme de tenseurs élémentaires

$$\sum_i \overline{1} \otimes m_i = \overline{1} \otimes \sum_i m_i$$

On a alors

$$g(f(\overline{1} \otimes m)) = g(\overline{m}) = \overline{1} \otimes m$$

et donc

$$g \circ f = Id_{\frac{R}{I} \otimes_R M}$$

2.3.4 Commutativité et associativité

Soient M et N des R-modules. On a un isomorphisme :

$$M \otimes_R N \xrightarrow{\simeq} N \otimes_R M \qquad (m \otimes n) \longmapsto n \otimes m$$

De même si M, N et P sont des R-modules, on a un isomorphisme :

$$(M \otimes_R N) \otimes_R P \xrightarrow{\simeq} M \otimes_R (N \otimes_R P) \qquad (m \otimes n) \otimes p \longmapsto m \otimes (n \otimes p)$$

Pour voir tout cela on procède de la même maniére que dans les exemples précédents utilisant toujours la propriété universelle du produit tensoriel. Ces isomorphismes expriment les propriétés de commutativité et d'associativité du produit tensoriel au niveau des modules. Mais le produit tensoriel n'est pas commutatif au niveau des éléments. En général $m \otimes n \neq n \otimes m$

2.4 Extension de la base

Soit $f : R \longrightarrow S$ un morphisme d'anneaux commutatifs. Soit N un S-module. On peut utiliser f pour regarder N comme un R-module en posant

$$rn = f(r)n \qquad (r, n) \in R \times N$$

En particulier S lui-même est un R-module en posant

$$rs = f(r)s$$

Cette opération du passage d'un S-module à un R-module est souvent appellée la restriction des scalaires et tire son nom du cas particulier oú f est une inclusion (R est un sous-anneau de S) :

$$f : R \hookrightarrow S$$

et on se restreint ainsi de S à R.

Exemple 2.4.1. *En utilisant l'inclusion $\mathbb{R} \hookrightarrow \mathbb{C}$, tout module (espace vectoriel)sur $\mathbb{C}$ est aussi un module (espace vectoriel) sur $\mathbb{R}$.*

Le processus inverse, le passage d'un R-module à un S-module, est appelé l'extension des scalaires ou l'extension de la base. Soit M un R-module. Si $f : R \longrightarrow S$ est un morphisme d'anneaux, S devient un R-module via l'opération $rs = f(r)s$. On peut donc parler du produit tensoriel $S \otimes_R M$ (qui est un R-module). Le groupe additif $S \otimes_R M$ a une unique structure de S-module en posant :

$$s^{'}(s \otimes m) = s^{'}s \otimes m \qquad \forall (s, s^{'}, m) \in S^2 \times M$$

Cette structure de S-module est compatible avec la structure de R-module dans le sens que :

$$rt = f(r)t \qquad \forall s \in R, \forall t \in S \otimes_R M$$

Définition 2.4.1. *$S \otimes_R M$ (en tant que S-module) est appelé l'extension des scalaires de M (de R à S).*

De la même maniére $M \otimes_R S$ est aussi un S-module et on a un isomorphisme :

$$S \otimes_R M \longrightarrow M \otimes_R S \qquad s \otimes m \longmapsto m \otimes s$$

Exemple 2.4.2. *En utilisant toujours l'inclusion $f : \mathbb{R} \hookrightarrow \mathbb{C}$, tout module (espace vectoriel) V sur $\mathbb{R}$ devient un module $V \otimes_R \mathbb{C}$ sur $\mathbb{C}$. Si $V = \mathbb{R}^n$, alors on a :*

$$\mathbb{R}^n \otimes_R \mathbb{C} \cong \mathbb{C}^n$$

Si $M_n(\mathbb{R})$ est l'espace des matrices carrées sur $\mathbb{R}$ d'ordre n, on a

$$M_n(\mathbb{R}) \otimes \mathbb{C} \cong M_n(\mathbb{C})$$

Chapitre 3

Téléportation Quantique

Nous voulions trouver une application spectaculaire du produit tensoriel (quelque chose qui touche à la vie de tous les jours). On ne pouvait pas mieux choisir que la téléportation quantique. Il s'agit ici de téléporter l'état d'un qubit d'un endroit à un autre. Cette technique, qui fait partie du calcul quantique dans le cadre de la théorie de l'information quantique, utlise les lois de la mécanique quantique et en particuliers les propriétés mystérieuses de certains états quantiques dits intriqués. On commence donc par rappeler les postulats de la mécanique quantique qui sont au nombre de quatre. C'est dans le quatrième qu'on voit apparaître le produit tensoriel (ici les modules sont des espaces vectoriels complexes). Nous donnons ensuite les définitions des qubits et des ordinateurs (ou registres) quantiques avec quelques exemples qui montrent les subtilités du calcul quantique. Le protocole de téléportation quantique est présenté à la fin du chapitre. Pour ce dernier chapitre nous avons utilisé [5] et [6] et les articles originaux [7] et [8].

3.1 Notions de Calcul Quantique

3.1.1 Postulats de la mécanique quantique

Postulat 1 : A tout système physique isolé est associé un espace de Hilbert $\mathbb{H}$ sur $\mathbb{C}$ (espace vectoriel complexe muni d'un produit scalaire hermitien, donc linéaire en le second vecteur et antilinéaire en le premier vecteur). $\mathbb{H}$ est l'espace des états du système. Le système est completement determiné par son vecteur d'état qui est un vecteur $\psi \in \mathbb{H}$ tel que $\langle \psi, \psi \rangle = 1$. $\psi \in \mathbb{H}$

est noté $|\psi\rangle$.

Postulat 2 : L'évolution du système dans le temps est décrite par un opérateur unitaire $U : \mathbb{H} \longrightarrow \mathbb{H}$ ou de manière équivalente par un opérateur H (l'hamiltonien) tel que :

$$i\hbar \frac{d\,|\psi\rangle}{dt} = H\,|\psi\rangle$$

avec $\hbar$ la constante de Planck. La relation entre U et H est :

$$U = exp(\frac{-iH}{\hbar}).$$

Si U^* représente l'adjoint de U, alors U unitaire veut dire que $UU^* = U^*U = Id_{\mathbb{H}}$ (en particulier U est inversible). U^* est défini par l'égalité

$$\langle U\psi, \phi\rangle = \langle \psi, U^*\phi\rangle$$

La matrice de U^* est la transposée conjuguée de la matrice de U. Un opérateur unitaire preserve le produit scalaire hermitien. Un opérateur hermitien est un opérateur aut-adjoint et donc égal à son propre adjoint.

Postulat 3 : Toute mesure quantique est décrite par une collection $\{M_m\}$ d'opérateurs hermitiens opérant sur l'espace des états du système. m refère à une mesure possible. Soit $|\psi\rangle$ l'état du système avant la mesure, alors la probabilité qu'on obtienne la mesure m est :

$$P(m) = \langle \psi\,|M_m^* M_m|\,\psi\rangle$$

avec M_m^* l'adjoint de M_m. L'état du système aprés la mesure est :

$$\frac{M_m\,|\psi\rangle}{\sqrt{\langle \psi\,|M_m M_m^*|\,\psi\rangle}} = \frac{M_m\,|\psi\rangle}{\sqrt{P(m)}}.$$

Les M_m ne sont pas quelconques. Ils doivent verifier :

$$\sum_m M_m^* M_m = Id_{\mathbb{H}}$$

ce qui est une autre manière d'écrire $\sum_m P(m) = 1$. Toute mesure est destructrice : si l'état $|\psi\rangle$ est une superposition, la mesure va détruire cette superposition et projeter l'état sur un sous-espace de tout l'espace des états. Si on pose $E_m = M_m^* M_m$, on a $\sum_m E_m = Id$ et on peut utiliser les opérateurs

$\{E_m\}$ pour la mesure. Le plus souvent les E_m sont des projecteurs $E_m = P_m$ ($P_m^2 = P_m, P_m^* = P_m$ et $P_{m'}^* P_m = 0$ pour $m \neq m'$). Dans ce cas la mesure est dite projective ou orthogonale. Par exemple si $|v\rangle$ est un élément d'une base de $\mathbb{H}$ alors P_v= projection sur $|v\rangle$ est un projecteur.

Postulat 4 : L'espace des états d'un système physique composé est le produit tensoriel (sur $\mathbb{C}$) des espaces des états des composants :

$$\mathbb{H} = \mathbb{H}_1 \otimes \mathbb{H}_2 \otimes \ldots \otimes \mathbb{H}_n.$$

L'état $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$ sera le plus souvent écrit $|\psi_1\psi_2 \ldots \psi_n\rangle$. Dans ce dernier postulat le produit tensoriel intervient de manière décisive. Ici on a donc $R = \mathbb{C}$ qui est un corps et le produit tensoriel est celui des espaces vectoriels sur $\mathbb{C}$. On écrira le plus souvent

$$V \otimes_{\mathbb{C}} W = V \otimes W$$

pour V et W deux $\mathbb{C}$-espaces vectoriels en omettant le $\mathbb{C}$.

3.1.2 Qubits et Registres quantiques

Un qubit est une extension naturelle au monde quantique de la notion classique de bit (0 ou 1) qui est à la base de l'informatique.

Définition 3.1.1. *On appelle qubit tout système physique dont l'espace des états a une base orthonormale formée de deux éléments (le chat de Schrodinger par exemple). Donc $\mathbb{H} = \mathbb{C}^2$ et on peut prendre pour base $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.*

Tout état $|\psi\rangle$ du système s'écrit alors comme une superposition :

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

avec a et b, les amplitudes de probabilités, des nombres complexes verifiant $|a|^2 + |b|^2 = 1$ (condition de normalisation). Le produit scalaire hermitien est ici donné par

$$\left\langle \psi, \psi' \right\rangle = \overline{a}a' + \overline{b}b'$$

si

$$\left|\psi'\right\rangle = a'\,|0\rangle + b'\,|1\rangle$$

La condition de normalisation équivaut à $\langle \psi, \psi \rangle = 1$.

D'aprés le troisième postulat la mesure d'un état en mécanique quantique signifie le projeter sur une base. La mesure depend donc de la base choisie. La base $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ est appelée base calculatoire. Mais il existe d'autres bases possibles, par exemple la base $\{|+\rangle, |-\rangle\}$ avec

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

et

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Si aucune base n'est specifiée il sera toujours entendu que la mesure est faite dans la base calculatoire.

Une mesure de $|\psi\rangle$ dans la base calculatoire donnera $|0\rangle$ avec la probabilité $|a|^2$, ou $|1\rangle$ avec la probabilité $|b|^2$. Cette mesure est realisée mathematiquement en utilisant les deux projecteurs P_0 et P_1 associés aux éléments $|0\rangle$ et $|1\rangle$ de la base du qubit :

$$P_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$P_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

On a bien $P_i P_j = \delta_{ij} P_i$ avec $\delta_{ij} = 1$ si $i = j$ et 0 sinon. De plus $P_0 |\psi\rangle = a |0\rangle$ et $P_1 |\psi\rangle = b |1\rangle$. La probabilité de trouver $|\psi\rangle$ à l'état $|0\rangle$ ou $|1\rangle$ est $pr(0) = |P_0 |\psi\rangle|^2 = |a|^2$ ou $pr(1) = |P_1 |\psi\rangle|^2 = |b|^2$.

Aprés la mesure $|\psi\rangle$ devient (avec resultat $|0\rangle$) :

$$\left|\psi'\right\rangle = \frac{P_0 |\psi\rangle}{\sqrt{pr(0)}} = \frac{a |0\rangle}{\sqrt{|a|^2}} = |0\rangle$$

ou (si la mesure est $|1\rangle$)

$$\left|\psi''\right\rangle = \frac{P_1 |\psi\rangle}{\sqrt{pr(1)}} = \frac{b |1\rangle}{\sqrt{|b|^2}} = |1\rangle$$

(Des états $|\psi\rangle$ et $\left|e^{i\theta}\psi\right\rangle$ sont équivalents car ils ont même norme et produisent les mêmes mesures. On dit qu'ils diffèrent par une phase globale).

Ce petit exemple fait apparaitre un des mystères de la mécanique quantique : beaucoup d'information est contenue (ou cachée) dans l'etat. Dés qu'on essaie d'y acceder (par une mesure) toute l'information disparait. Une fois qu'on a effectué la mesure, on ne peut plus récupérer l'etat initial. On le voit d'ailleurs en remarquant que les projecteurs ne sont pas unitaires donc non reversibles.

Définition 3.1.2. *: Un registre quantique ou ordinateur quantique est une collection de n qubits.*

D'aprés le postulat 4, l'espace des états d'un registre quantique est donc :

$$\mathbb{H} = \mathbb{C}^2 \otimes \mathbb{C}^2 \ldots \otimes \mathbb{C}^2 = \mathbb{C}^{2^n}.$$

Par exemple pour $n = 2$, on a $\mathbb{H} = \mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$ avec $|00\rangle, |01\rangle, |10\rangle$ et $|11\rangle$ pour base avec

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

et

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Le produit scalaire de deux états composés est le produit des produits scalaires

$$\left\langle |\psi\rangle |\phi\rangle , \left|\psi'\right\rangle \left|\phi'\right\rangle \right\rangle = \left\langle |\psi\rangle , \left|\psi'\right\rangle \right\rangle . \left\langle |\phi\rangle , \left|\phi'\right\rangle \right\rangle$$

L'information est généralement représentée dans les registres sous forme binaire. Par exemple le nombre 6 est représenté par l'état $|1\rangle \otimes |1\rangle \otimes |0\rangle$ ($6 = 110$

en binaire). De manière générale on pose $|a\rangle = |a_{n-1}\rangle \otimes |a_{n-2}\rangle \otimes \ldots \otimes |a_0\rangle$ si $a = 2^0 a_0 + 2^1 a_1 + \ldots + 2^{n-1} a_{n-1}$. L'état d'un registre quantique s'écrit donc en toute généralité

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle = \sum_{x=0}^{2^n-1} \alpha_x |x\rangle$$

avec $\sum_x |\alpha_x|^2 = 1$. L'écriture $x \in \{0,1\}^n$ veut dire que x parcourt l'ensemble des mots de longueur n qu'on peut former avec les lettres 0 et 1. Les $|x\rangle$ forment donc une base du registre, et on peut utiliser le phénomène de superposition pour stocker plusieurs nombres en même temps dans un registre.

Exemple 3.1.1. *Dans un registre de taille* 3*, on peut représenter des nombres seuls comme* 3 *ou* 7 *:*

$$|3\rangle = |011\rangle = |0\rangle \otimes |1\rangle \otimes |1\rangle$$
$$|7\rangle = |111\rangle = |1\rangle \otimes |1\rangle \otimes |1\rangle$$

Mais on peut aussi les représenter ensemble dans un état superposé :

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}}(|011\rangle + |111\rangle) = \frac{1}{\sqrt{2}}(|3\rangle + |7\rangle)$$

De même :

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$= 2^{-\frac{3}{2}}(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle)$$
$$= 2^{-\frac{3}{2}} \sum_{x=0}^{7} |x\rangle$$

En plus du phénomène de superposition, celui de l'intrication est aussi largement utilisé en calcul quantique : un état est dit intriqué si on ne peut pas l'écrire comme produit tensoriel de deux autres états separés.

Exemple 3.1.2. *Soit l'état* $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$*. Soient* $|\psi_1\rangle = a_1 |0\rangle + b_1 |1\rangle$ *et* $|\psi_2\rangle = a_2 |0\rangle + b_2 |1\rangle$*. Supposons que* $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$*. Donc* $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = a_1 a_2 |00\rangle + a_1 b_2 |01\rangle + b_1 a_2 |10\rangle + b_1 b_2 |11\rangle$ *et* $a_1 b_2 = 0$ *et* $b_1 a_2 = 0$*. Ce qui implique* $a_1 a_2 = 0$ *ou* $b_1 b_2 = 0$*, ce qui est impossible.* $|\psi\rangle$ *représente donc l'état de deux qubits intriqués. On dit que cette paire de qubits est un EPR pour Einstein, Podolsky et Rosen.*

Ces états représentent des situations pour lesquelles il n'y a pas d'analogue classique et pour lesquelles on a aucune intuition. Ils sont aussi à l'origine de l'explosion exponentielle de la taille des registres quantiques quand on rajoute des qubits. Une définition equivalente des états intriqués est en terme de mesure. Deux particules sont non intriquées si la mesure de l'état de l'une n'influe pas sur la mesure de l'état de l'autre. La dimension de l'espace des états d'un registre quantique formé de n qubits est 2^n. Une augmentation linéaire du registre a donc pour conséquence une augmentation exponentielle de la dimension de son espace d'états. C'est là l'un des interêts majeurs du calcul quantique sur le calcul classique.

3.1.3 Portes Quantiques

La dynamique d'un système quantique (et donc d'un qubit ou d'un registre quantique) est, d'aprés le deuxième postulat, régie par l'equation de Schrodinger à travers un opérateur unitaire U qui vérifie donc $U^*U = UU^* = Id$. Un opérateur unitaire est en particulier inversible, ce qui veut dire que le processus physique qu'il décrit est reversible. Le calcul quantique est basé sur le modèle de circuits quantiques qui étend le modèle classique des portes logiques de la logique booléenne. Ainsi toute transformation unitaire sera représentée par un circuit quantique. Les transformations unitaires les plus simples sont celles qui portent sur un seul qubit. En voici quatre données par les matrices correspondantes dans la base calculatoire

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Par exemple Y est la transformation $|0\rangle \longmapsto |-1\rangle$ et $|1\rangle \longmapsto |0\rangle$ et on a bien :

$$Y^*Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = I$$

Un autre exemple important de transformation sur un seul qubit est la transformation de Hadamard H de matrice :

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

On a donc

$$H(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

et

$$H(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Le non-contrôlé est une transformation sur 2 qubits. Elle change le second si le premier est mis à 1 sinon elle ne fait rien :

$$C_{not} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Par exemple

$$C_{not}(|00\rangle) = |00\rangle$$

et

$$C_{not}(|10\rangle) = |11\rangle$$

Un dernier exemple est la transformation de Walsh-Hadamard $H \otimes H \otimes \ldots \otimes H$ avec n facteurs H. Appliquée à $|00\ldots0\rangle$ elle donne :

$$(H \otimes H \otimes \ldots \otimes H)\,|00\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^{n-1}} |x\rangle$$

Autrement dit à partir de $|00\ldots0\rangle$, elle génère une superposition de tous les 2^n états d'un registre quantique comportant n qubits. Le produit tensoriel de deux operateurs A et B est défini par

$$(A \otimes B)(|\psi\rangle \otimes |\phi\rangle) = A\,|\psi\rangle \otimes B\,|\phi\rangle$$

Par exemple pour deux qubits, on a

$$(H \otimes H)\,|00\rangle = H(|0\rangle) \otimes H(|0\rangle)$$

$$= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Exemple 3.1.3. *L'intrication dans l'état* $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ *se voit mieux au moment de la mesure. Supposons qu'on mesure le premier qubit de* $|\psi\rangle$ *et qu'on trouve* 0*. Quel est le nouvel état obtenu aprés la mesure ? Mesurer le premier qubit avec resultat* 0 *équivaut à utiliser l'opérateur* $P_0 \otimes I$ *sur* $|\psi\rangle$ *avec* I *la matrice identité (correspondant donc à ne rien faire au second qubit). Rappelons que*

$$P_0(|0\rangle) = |0\rangle$$

et

$$P_0(|1\rangle) = 0$$

le vecteur nul dans $\mathbb{C}^2$*. On a donc*

$$(P_0 \otimes I)\,|\psi\rangle = \frac{1}{\sqrt{2}}\,|00\rangle$$

La probabilité d'obtenir le resultat 0 *lors de la mesure du premier qubit est donc*

$$pr(0) = |(P_0 \otimes I)\,|\psi\rangle\,|^2 = \frac{1}{2}$$

L'état aprés la mesure est donc

$$|\phi\rangle = \frac{(P_0 \otimes I)\,|\psi\rangle}{\sqrt{pr(0)}} = |00\rangle$$

Donc si on mesure le premier qubit de l'état intriqué $|\psi\rangle$ *et qu'on trouve* 0 *on est certain que la mesure du second qubit donnera aussi* 0*. De même si on mesure le premier qubit à* 1 *on est certain de trouver le second qubit aussi à* 1*.*

3.2 Téléportation quantique

Messaouda veut envoyer un qubit $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ à Kaddour pour des besoins de communication, par exemple en cryptographie quantique. Elle ne connait pas l'état du qubit puisque pour le connaitre elle doit le mesurer et en mécanique quantique la mesure détruit l'état $|\psi\rangle$. Elle ne peut pas non plus le copier ou le cloner à cause de la

Proposition 3.2.1. *[8] Supposons qu'il existe un opérateur unitaire de clonage U. Autremnat dit U est un opérateur sur deux qubits qui copie ou clone le premier qubit en le second*

$$U\left|\psi\right\rangle\left|s\right\rangle = \left|\psi\right\rangle\left|\psi\right\rangle$$

avec $\left|s\right\rangle$ un qubit arbitraire. Alors U ne peut cloner que des états parallèles ou orthogonaux à $\left|\psi\right\rangle$.

Preuve. Soit un autre état $\left|\phi\right\rangle$ avec

$$U\left|\phi\right\rangle\left|s\right\rangle = \left|\phi\right\rangle\left|\phi\right\rangle$$

En prenant le produit scalaire de ces deux équations ensemble on obtient

$$\left\langle U\left|\psi\right\rangle\left|s\right\rangle, U\left|\phi\right\rangle\left|s\right\rangle\right\rangle = \left\langle\left|\psi\right\rangle\left|\psi\right\rangle, \left|\phi\right\rangle\left|\phi\right\rangle\right\rangle$$

et donc

$$\left\langle\left|\psi\right\rangle\left|s\right\rangle, U^*U\left|\phi\right\rangle\left|s\right\rangle\right\rangle = \left\langle\left|\psi\right\rangle\left|\psi\right\rangle, \left|\phi\right\rangle\left|\phi\right\rangle\right\rangle$$

Ce qui donne en utilisant l'unitarité de U

$$\left\langle\left|\psi\right\rangle\left|s\right\rangle, \left|\phi\right\rangle\left|s\right\rangle\right\rangle = \left\langle\left|\psi\right\rangle\left|\psi\right\rangle, \left|\phi\right\rangle\left|\phi\right\rangle\right\rangle$$

ou encore

$$\left\langle\left|\psi\right\rangle, \left|\phi\right\rangle\right\rangle \cdot \left\langle\left|s\right\rangle, \left|s\right\rangle\right\rangle = \left\langle\left|\psi\right\rangle\left|\psi\right\rangle, \left|\phi\right\rangle\left|\phi\right\rangle\right\rangle$$

On obtient donc

$$\left\langle\left|\psi\right\rangle, \left|\phi\right\rangle\right\rangle = \left\langle\left|\psi\right\rangle, \left|\phi\right\rangle\right\rangle^2$$

(Rappelons que $\left\langle\left|s\right\rangle, \left|s\right\rangle\right\rangle = 1$ et que $\left\langle\left|\psi\right\rangle\left|\psi\right\rangle, \left|\phi\right\rangle\left|\phi\right\rangle\right\rangle = \left\langle\left|\psi\right\rangle, \left|\phi\right\rangle\right\rangle \cdot \left\langle\left|\psi\right\rangle, \left|\phi\right\rangle\right\rangle$). On doit donc avoir $\langle\psi, \phi\rangle = 0$ ou 1. Et donc $\left|\phi\right\rangle$ est orthogonal ou parallèle à $\left|\psi\right\rangle$ □

Messaouda ne peut donc pas utiliser un quelconque canal de communication classique pour envoyer le qubit à Kaddour puisqu'elle ne connait pas le qubit et qu'elle ne peut pas le copier ou le cloner. Comment peu-elle donc faire ? Dans un article célèbre [7] de seulement quelques pages quelques spécialistes de la théorie de l'information quantique ont mis au point une technique assez simple ne faisant intervenir que la transformation de Hadamard H et le non-controlé C_{not} qui permet quand même à Messaouda

d'envoyer le qubit à Kaddour. Ils ont appelé cette technique la téléportation quantique.

Messaouda et Kaddour commencent par preparer et partager une paire EPR de deux qubits. Pour cela ils appliquent la transformation $H \otimes I$ au 2-qubit $|00\rangle$

$$\begin{aligned}(H \otimes I)\,|00\rangle &= H\,|0\rangle \otimes I\,|0\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \\ &= \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\end{aligned}$$

Ici I est la matrice unité correspondant donc à l'operateur identité $Id_{\mathbb{C}^2}$ sur $\mathbb{C}^2$. Ils appliquent ensuite un non-controlé sur le premier qubit

$$C_{not}(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

C'est leur EPR paire de qubits partagée. L'etat $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ est ensuite composé avec la paire EPR pour obtenir le 3-qubit

$$|\psi\rangle \otimes (\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle))$$

$$= (a\,|0\rangle + b\,|1\rangle) \otimes (\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$= \frac{1}{\sqrt{2}}(a\,|000\rangle + a\,|011\rangle + b\,|100\rangle + b\,|111\rangle)$$

auquel on applique un non-contrôlé sur le premier et le second qubit

$$(C_{not} \otimes I)(\frac{1}{\sqrt{2}}(a\,|000\rangle + a\,|011\rangle + b\,|100\rangle + b\,|111\rangle))$$

$$= \frac{1}{\sqrt{2}}(a\,|000\rangle + a\,|011\rangle + b\,|110\rangle + b\,|101\rangle)$$

A ce 3-qubit on applique une transformation de Hadamard sur le premier qubit pour obtenir le 3-qubit

$$|\Psi\rangle = (H \otimes I \otimes I)(\frac{1}{\sqrt{2}}(a\,|000\rangle + a\,|011\rangle + b\,|110\rangle + b\,|101\rangle))$$

$$= \frac{1}{2}(a\,|000\rangle + a\,|100\rangle + a\,|011\rangle + a\,|111\rangle + b\,|010\rangle - b\,|110\rangle - b\,|101\rangle + b\,|001\rangle)$$

$$= \frac{1}{2}(|00\rangle\,(a\,|0\rangle + b\,|1\rangle) + |01\rangle\,(a\,|1\rangle + b\,|0\rangle) + |10\rangle\,(a\,|0\rangle - b\,|1\rangle) + |11\rangle\,(a\,|1\rangle - b\,|0\rangle))$$

Ici les deux premiers qubits appartiennent à Messaouda et le troisième qubit appartient à Kaddour. Messaouda a commencé avec les qubits $|\psi\rangle$ et $|0\rangle$ et Kaddour a commencé avec le qubit $|0\rangle$. Les deux qubits $|0\rangle$ ont servi a produire la paire EPR.

Messaouda va maintenant mesurer ses deux (premiers) qubits dans l'etat $|\Psi\rangle$, ne touchant pas au troisième qubit de Kaddour qui, remarquons le, est une superposition. Nous sommes dans un système à trois qubits et on ne veut mesurer que les deux premiers qubits. Cela revient à mesurer dans un système à deux qubits et tensoriser par la matrice identité (2×2) I correspondant à ne rien faire au troisième qubit. La base calculatoire d'un système à deux qubits est formée de $|00\rangle, |01\rangle, |10\rangle$ et $|11\rangle$. Par le troisième postulat de la mécanique quantique, mesurer dans cette base calculatoire revient à operer les operateurs $P_{00} \otimes I, P_{01} \otimes I, P_{10} \otimes I$ et $P_{11} \otimes I$ sur l'état $|\Psi\rangle$. Ici P_{ij} est la projection sur le sous espace engendré par $|ij\rangle$ avec $i = 0$ ou 1 et $j = 0$ ou 1. Par exemple $P_{00}\,|00\rangle = |00\rangle$ et le vecteur nul 0 pour les autres. De même $P_{01}\,|01\rangle = |01\rangle$ et le vecteur nul 0 pour les autres et ainsi de suite. Les mesures possibles sont donc

$$(P_{00} \otimes I)\,|\Psi\rangle = \frac{1}{2}\,|00\rangle\,(a\,|0\rangle + b\,|1\rangle)$$

$$(P_{01} \otimes I)\,|\Psi\rangle = \frac{1}{2}\,|01\rangle\,(a\,|1\rangle + b\,|0\rangle)$$

$$(P_{10} \otimes I)\,|\Psi\rangle = \frac{1}{2}\,|10\rangle\,(a\,|0\rangle - b\,|1\rangle)$$

$$(P_{11} \otimes I)\,|\Psi\rangle = \frac{1}{2}\,|11\rangle\,(a\,|1\rangle - b\,|0\rangle)$$

En mesurant les deux premiers qubits Messaouda va donc obtenir $ij(00, 01, 10, 11)$ avec la probabilité

$$pr(ij) = |(P_{ij} \otimes I)\,|\Psi\rangle\,|^2 = \frac{1}{4}$$

Les etats possibles obtenus aprés la mesure sont donnés par la formule

$$|\Psi_{ij}\rangle = \frac{(P_{ij} \otimes I)\,|\Psi\rangle}{\sqrt{pr(ij)}}$$

et sont donc

$$|\Psi_{00}\rangle = |00\rangle (a|0\rangle + b|1\rangle)$$
$$|\Psi_{01}\rangle = |01\rangle (a|1\rangle + b|0\rangle)$$
$$|\Psi_{10}\rangle = |10\rangle (a|0\rangle - b|1\rangle)$$
$$|\Psi_{11}\rangle = |11\rangle (a|1\rangle - b|0\rangle)$$

remarquer que le qubit de Kaddour est dans l'un des états

$$|\psi_{00}\rangle = a|0\rangle + b|1\rangle$$
$$|\psi_{01}\rangle = a|1\rangle + b|0\rangle$$
$$|\psi_{10}\rangle = a|0\rangle - b|0\rangle$$
$$|\psi_{11}\rangle = a|1\rangle - b|0\rangle$$

Pour savoir dans lequel il suffit à Messaouda de lui envoyer le resultat de sa mesure par un canal classique (par exemple par lettre ou par email).

Si Messaouda mesure 00, Kaddour sait que son qubit est $|\psi_{00}\rangle = a|0\rangle + b|1\rangle$ qui est égal à $|\psi\rangle$ et qui est exactement l'état que Messaouda veut lui envoyer. L'état a donc bien été teleporté.

Si Messaouda mesure 01, Kaddour sait que son qubit est $|\psi_{01}\rangle = a|1\rangle + b|0\rangle$. Il lui applique X et recupere ainsi l'état $|\psi\rangle$

$$X|\psi_{01}\rangle = |\psi\rangle$$

Si Messaouda mesure 10, Kaddour sait que son qubit est $|\psi_{10}\rangle = a|0\rangle - b|1\rangle$. Il lui applique Z et recupere ainsi l'état $|\psi\rangle$

$$Z|\psi_{10}\rangle = |\psi\rangle$$

Si Messaouda mesure 11, Kaddour sait que son qubit est $|\psi_{11}\rangle = a|1\rangle - b|0\rangle$. Il lui applique ZX et recupere ainsi l'état $|\psi\rangle$

$$ZX|\psi_{11}\rangle = |\psi\rangle$$

Remarquer que Messaouda n'a plus l'état $|\psi\rangle$, qui n'a donc pas été cloné. Cette technique ne contredit pas le principe de la relativité restreinte qui stipule que rien ne peut voyager à une vitesse supérieure à celle de la lumière puisque Messaouda doit envoyer son résultat à Kaddour par un canal de communication classique.

Conclusion

Dans ce travail nous avons défini le produit tensoriel dans son cadre le plus naturel et le plus général, Celui des modules sur un anneau commutatif. Le produit tensoriel de deux modules est un autre module qui vérifie une certaine propriété universelle et qui est le seul à la vérifier. Cette unicité est clairement mise en evidence lors de sa construction que nous avons détaillée et illistrée à travers quelques exemples. L'exemple de la téléportation quantique, que nous donnons en dernier, montre clairement l'utilité du produit tensoriel.

Résumé : Le produit tensoriel est trés utile et largement utilisé tant en Mathématiques qu'en Physique. Nous définission ici dans un cadre trés général, celui des modules sur un anneau commutatif. Quand l'anneau est un corps on retrouve toute l'algèbre linéaire des espaces vectoriels. Quand l'anneau est l'anneau des entiers on retrouve toute la théorie des groups abéliens. Suivant Bourbaki, nous montrons comment construire le produit tensoriel de deux modules. Nous illustrons son utilisation à travers l'exemple de la téléportation quantique qui utilise des espaces vectoriels complexes de dimension finie munis d'un produit scalaire hermitien (des espaces de Hilbert).

ABSTRACT : The tensor product is very useful and widely used in both Mathematics and Physics. We define it here in a very general framework, that of modules on a commutative ring, When the ring is a field we find all the linear algebra of vector space. When the ring is the ring of integers we find the whole theory of abelian groups. Following Bourbaki, We show how to construct the tensor product of two modules. We illustrate its use through the example of quantum teleportation which uses complex finite-dimensional vector spaces equipped with a Hermitian scalar product (Hilbert spaces).

ملخص : يعتبر الموتر مفيدا جدا ويستخدم على نطاق واسع في كل من الرياضيات والفيزياء. نحن نحددها هنا في اطار عام جدا, وهو اطار الوحدات الموجودة على حلقة تبادلية. عندما تكون الحلقة مجالا نجد كل الجبر الخطي للمسافات المتجهة. عندما تكون الحلقة هي حلقة الاعداد الصحيحة نجد النظرية الكاملة للمجموعات الابيلية باتباع بورباكي, نعرض كيفية بناء المنتج الموتر لوحدتين. نوضح استخدامه من خلال مثال النقل الاني الكمي الذي يستخدم مساحات متجهة معقدة ذات ابعاد محدودة ومجهزة بمنتج عددي هيرميت (فضاءات هيلبرت).

Bibliographie

[1] M. Atiyah, and I. MacDonald, Introduction to commutative algebra, Addison-Wesley-Longman, (1969).

[2] Serge Lang, Algebra, Addison-Wesley, 1971.

[3] Nicolas Bourbaki, Algèbre, Hermann, 1973.

[4] Roger Godement, Cours d'Algèbre, Hermann, 1963.

[5] Nielsen, M. A. and Chuang, I. L. (2000). Quantum Computation and Quantum Information. Cambridge Univ. Press, Cambridge.

[6] Colin P.Williams ; Scott H.Clearwater, Explorations in Quantum Computing, Springer Verlag, 1998.

[7] Bennett, Charles H. ; Brassard, Gilles ; Crpeau, Claude ; Jozsa, Richard ; Peres, Asher ; Wootters, William K. (29 March 1993). "Teleporting an Unknown Quantum State via Dual Classical and EinsteinPodolskyRosen Channels". Physical Review Letters. 70 (13).

[8] William Wooters, Wojciech Zurek, A single quantum cannot be cloned, Nature 299 (1982).