

Anneaux et modules

Cours de Bachelor

Table des matières

1	Introduction	2
2	Anneaux et modules	4
2.1	Rappels sur les anneaux	4
2.2	Modules	8
2.3	Suites exactes	12
2.4	Modules libres et projectifs	14
2.5	La propriété du rang unique	19
2.6	Anneaux et modules noethériens	21
3	Catégories de modules	24
3.1	Catégories, foncteurs, transformations naturelles et adjoints	24
3.2	Catégories de modules : les foncteurs Hom et \otimes	30
3.3	Le théorème d'équivalence de Morita	33
4	Le foncteur $K_0(-)$	37
4.1	Définition de $K_0(-)$ et résultats immédiats	37
4.2	Le groupe K_0 réduit	40
4.3	Anneaux de Dedekind	41
4.4	$K_0(R)$ lorsque R est un anneau de Dedekind	45
5	Le foncteur $K_1(-)$.	48
5.1	Matrices élémentaires et le lemme de Whitehead	48
5.2	$K_1(R)$ lorsque R est un anneau commutatif	50
5.3	$K_1(R)$ lorsque R est un anneau euclidien	51

1 Introduction

13.03.2006

Rappelons qu'un espace vectoriel est un groupe abélien sur lequel agit un corps. Si l'on remplace ce corps par un anneau quelconque, on obtient la notion de *module*. Nous verrons que certains résultats classiques d'algèbre linéaire ne sont pas vrais pour les modules. Par exemple, on ne peut pas leur assurer l'existence d'une base. Les modules pour lesquels une base existe sont appelés *libres*. Nous verrons aussi que certaines propriétés des anneaux et des modules sont liées. Par exemple, tout sous-module d'un module libre sur un anneau principal est lui-même libre. De façon générale, quels sont les résultats que l'on peut récupérer de l'algèbre linéaire et appliquer aux modules ? La K-théorie permet de répondre partiellement à cette question.

La K-théorie est un domaine des mathématiques relativement nouveau qui apparut à la fin des années cinquante avec certains travaux de A. Grothendieck. D'une certaine façon, la K-théorie est une généralisation de l'algèbre linéaire sur les anneaux. Elle associe à tout anneau R une suite de groupes abéliens, notés $K_n(R)$, $n \geq 0$. Les deux premiers groupes de K-théorie, $K_0(R)$ et $K_1(R)$, peuvent être décrits assez concrètement, voire calculés. Les autres sont plus mystérieux !

En algèbre linéaire, le nombre d'éléments constituant une base d'un espace vectoriel, lorsqu'il est fini, est un invariant d'isomorphisme qu'on appelle *la dimension*. Dans la mesure où la notion de module sur un anneau généralise celle d'espace vectoriel sur un corps, il est naturel de se demander si un tel invariant subsiste. En fait, on verra que ce n'est pas le cas, i.e. il existe un anneau R et deux entiers $m, n \in \mathbb{N}$ tels que

$$m \neq n \text{ et pourtant } R^m \cong R^n \text{ comme } R\text{-modules.}$$

Nous verrons que cette situation ne se présente pas lorsque R est un anneau dit *noethérien* (par exemple un anneau principal). Nous verrons également que les modules dit *projectifs de génération finie* admettent une notion analogue de celle de la dimension d'un espace vectoriel. C'est précisément l'étude du premier groupe de K-théorie algébrique, $K_0(R)$. Concrètement, on verra que tout R -module projectif de génération finie définit un élément du groupe abélien $K_0(R)$.

Les matrices jouent un rôle essentiel dans la théorie des espaces vectoriels de dimension finie. Par exemple, lorsque l'on fixe une base B pour un espace vectoriel V de dimension n sur un corps K , on peut alors exprimer toute application linéaire $\varphi \in \text{End}_K(V)$ à l'aide d'une matrice $(\varphi)_B \in M_n(K)$. Si l'on procède à un autre choix de base, disons B' , alors il existe une matrice inversible $D \in M_n(K)$ dite *de changement de base* et telle que

$$(\varphi)_B = D \cdot (\varphi)_{B'} \cdot D^{-1}.$$

On connaît au moins trois invariants de changement de base : la *trace*, le *déterminant* et le *polynôme caractéristique* d'une matrice. On a $\text{tr}((\varphi)_B) = \text{tr}((\varphi)_{B'})$, $\det((\varphi)_B) = \det((\varphi)_{B'})$ et $p_{(\varphi)_B}(t) = p_{(\varphi)_{B'}}(t)$. Rappelons que le déterminant d'une matrice $A = (a_{ij})$ de $M_n(R)$ avec R un anneau commutatif est défini comme suit :

$$\det(A) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}.$$

La commutativité de l'anneau R permet de prouver que $\det(AB) = \det(A)\det(B)$ pour tout $A, B \in M_n(R)$. Peut-on généraliser la notion de déterminant pour les matrices inversibles au cas où l'anneau R n'est pas nécessairement commutatif ?

Pour répondre à cette question, cherchons un groupe G et pour tout $n \geq 1$ une application $D_n : GL_n(R) \rightarrow G$ tels que

1. G est "le plus proche possible" de $GL_n(R)$ (ça va devenir clair plus loin) ;
2. $D_n(I_n) = e_G$ où I_n est la matrice identité de $GL_n(R)$ et e_G l'élément neutre de G ;
3. $D_n(AB) = D_n(A)D_n(B)$;
4. $D_n(ABA^{-1}) = D_n(B)$;
5. $D_{n+1} \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix} = D_n(A)$.

Supposons que l'on ait trouvé de tels homomorphismes de groupes, alors on a le diagramme commutatif suivant :

$$\begin{array}{ccccccc}
 GL_1(R) & \hookrightarrow & \dots & \hookrightarrow & GL_n(R) & \hookrightarrow & GL_{n+1}(R) & \hookrightarrow & \dots & \hookrightarrow & \varinjlim_n GL_n(R) =: GL(R) \\
 & & & & \searrow D_1 & & \searrow D_n & & \searrow D_{n+1} & & \searrow D \\
 & & & & & & & & & & G
 \end{array}$$

L'existence de l'homomorphisme de groupes $D : GL(R) \rightarrow G$ est due à la *propriété universelle* de la limite directe. Remarquons que l'on a $D([A, B]) = D(ABA^{-1}B^{-1}) = D(ABA^{-1})D(B^{-1}) = D(B)D(B^{-1}) = D(BB^{-1}) = e_G$, de sorte que le diagramme suivant commute :

$$\begin{array}{ccc}
 GL(R) & \xrightarrow{D} & G \\
 \text{can.} \downarrow & \nearrow \tilde{D} & \\
 GL(R) & & \\
 \hline
 [GL(R), GL(R)] & &
 \end{array}$$

où $\tilde{D}[A] = D(A)$ pour tout $A \in GL(R)$. Le groupe G le "plus proche" de $GL(R)$ est donc $\frac{GL(R)}{[GL(R), GL(R)]}$. C'est précisément le groupe (abélien !) qui définit le second groupe de K-théorie algébrique, $K_1(R)$. Concrètement, on verra que toute matrice inversible sur R possède un "déterminant" dans $K_1(R)$.

La K-théorie algébrique joue un rôle important dans plusieurs domaines des mathématiques, particulièrement en théorie des nombres, en topologie algébrique, et en géométrie algébrique. Nous en verrons quelques exemples très modestes.

2 Anneaux et modules

2.1 Rappels sur les anneaux

2.1.1 Définition. Un anneau R est un ensemble muni de deux lois de compositions internes appelées multiplication et addition, notées \cdot et $+$ respectivement, et satisfaisant les conditions suivantes :

1. $(R, +)$ est un groupe abélien et on note 0 (parfois 0_R) l'élément neutre pour l'addition,
2. la multiplication est associative, i.e. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$; on se permettra d'écrire xyz pour désigner un tel produit,
3. la multiplication est distributive par rapport à l'addition, i.e. $(x+y)z = xz+yz$ et $z(x+y) = zx+zy$,
4. la multiplication possède un élément neutre, noté 1 (parfois 1_R), qu'on appelle l'unité.

Lorsque la condition 4 n'est pas satisfaite, i.e. lorsqu'il n'y a pas d'élément neutre pour la multiplication, on parle d'anneau non-unital. Un anneau R tel que $1 \neq 0$ et pour lequel tout $x \neq 0 \in R$ possède un inverse multiplicatif, i.e. il existe x^{-1} tel que $xx^{-1} = x^{-1}x = 1$, est appelé un anneau de division (ou encore corps gauche ou corps non-commutatif). Un anneau R est dit commutatif lorsque la multiplication est commutative, i.e. $xy = yx$ pour tout $x, y \in R$. Un corps est un anneau de division commutatif.

Remarques. 1. On a $0x = x0 = 0$ pour tout $x \in R$ [$0x = (0+0)x = 0x+0x$, d'où $0x = 0$].
2. On a $(-x)y = -(xy)$, $x(-y) = -(xy)$ et $(-x)(-y) = xy$ pour tout $x, y \in R$ [$xy + (-x)y = (x + (-x))y = 0y = 0$]; on se permettra d'écrire $-xy$ au lieu de $-(xy)$, $(-x)y$ et $x(-y)$,
3. en particulier on a $(-1)x = x(-1) = -x$ et $(-1)^2 = 1$.
4. Si $1 = 0$ alors $R = \{0\}$ [$x = 1x = 0x = 0$]; pour éviter les situations inintéressantes, on supposera souvent que $1 \neq 0$.

Exemples. 1. On connaît l'anneau des entiers relatifs, noté \mathbb{Z} , ainsi que les rationnels \mathbb{Q} (corps des fractions de \mathbb{Z}). On connaît également l'anneau \mathbb{Z}/n des entiers modulo n (anneau quotient de \mathbb{Z}).
2. Pour tout anneau R et tout entier $n \geq 1$, on a l'anneau des matrices $M_n(R)$ dont les éléments sont les matrices $n \times n$ à coefficients dans R , l'addition et la multiplication sont matricielles, le zéro est la matrice nulle et l'unité est la matrice identité, notée I_n . Dans le cas où R est commutatif, l'anneau des matrices ne l'est pas forcément, par exemple les matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

sont différentes dans $M_2(\mathbb{Z}) \subset M_2(\mathbb{Q})$.

3. L'ensemble des fonctions $\mathbb{R}^{\mathbb{R}}$ (pas nécessairement continues!), muni de l'addition définie par $(f+g)(x) = f(x)+g(x)$ pour tout $x \in \mathbb{R}$ et de la multiplication définie par la composition de fonctions, est un anneau; de façon générale, pour tout groupe abélien G , on peut considérer l'anneau des endomorphismes $\text{End}(G)$.
4. Le sous-ensemble des matrices inversibles de $M_n(R)$ est le sous-groupe noté $GL_n(R)$ et appelé groupe linéaire général de R . Ce n'est pas un anneau parce que la matrice nulle n'est pas inversible.

2.1.2 Définition. Un homomorphisme entre les anneaux R et S est une application $f : R \rightarrow S$ qui vérifie les propriétés suivantes :

1. $f(x + y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$ pour tout $x, y \in R$,
2. $f(1_R) = 1_S$.

Un homomorphisme $f : R \rightarrow S$ est un isomorphisme d'anneaux si f est surjectif et injectif.

Remarques. 1. On a $f(0_R) = 0_S$ [$f(0_R) + f(0_R) = f(0_R + 0_R) = f(0_R)$].

2. On a $f(-x) = -f(x)$ pour tout $x \in R$ [$f(-x) + f(x) = f((-x) + x) = f(0_R) = 0_S$].

3. L'identité id_R sur un anneau R est un isomorphisme d'anneaux.

4. L'unique application $\{0\} \rightarrow R$ est un homomorphisme d'anneaux si et seulement si R est trivial.

5. L'unique application $R \rightarrow \{0\}$ est un homomorphisme d'anneaux.

2.1.3 Définition. Un sous-anneau d'un anneau R est un sous-ensemble $S \subset R$ qui possède les propriétés suivantes :

1. $0_R, 1_R \in S$,
2. si $x, y \in S$ alors $x - y, xy \in S$.

et qui suffisent à lui conférer une structure d'anneau.

2.1.4 Définition. Soit R un anneau. Le centre de R est le sous-anneau commutatif

$$Z(R) = \{z \in R \mid xz = zx \text{ pour tout } x \in R\}.$$

2.1.5 Définition. Soit $f : R \rightarrow S$ un homomorphisme d'anneaux. L'image de f est le sous-anneau

$$\text{im } f = \{f(x) \in S \mid x \in R\} \subset S.$$

2.1.6 Définition. Soit R un anneau. Un sous-ensemble I de R est un idéal à droite (resp. à gauche) s'il vérifie les conditions suivantes :

1. $0_R \in I$,
2. pour tout $a, b \in I$ on a $a - b \in I$,
3. pour tout $a \in I$ et $r \in R$ on a $ar \in I$ (resp. $ra \in I$).

Si I est à la fois un idéal à droite et à gauche, on dit que c'est un idéal bilatère. Un idéal I est dit propre lorsque $I \subsetneq R$.

Remarques. 1. R est un idéal de lui-même.

2. $\{0_R\}$ est un idéal pour tout anneau R que l'on appelle l'idéal nul.

3. Un idéal est un anneau non-unital.

4. L'intersection de deux idéaux est clairement un idéal.

2.1.7 Définition. Soit $f : R \rightarrow S$ un homomorphisme d'anneaux. Le noyau de f est l'idéal

$$\ker f = \{x \in R \mid f(x) = 0_S\} \subset R.$$

2.1.8 Lemme. Soit $f : R \rightarrow S$ un homomorphisme d'anneaux. Alors f est injectif si et seulement si $\ker f$ est trivial.

- Démonstration.* 1. (\implies) Soit $x \in \ker f$, i.e. $f(x) = 0$. On a donc $f(x) = 0 = f(0)$, de sorte que $x = 0$ par injectivité.
2. (\impliedby) Soient $x, y \in R$ tels que $f(x) = f(y)$. On a $f(x) - f(y) = f(x - y) = 0$, i.e. $x - y \in \ker f$, de sorte que $x - y = 0$, i.e. $x = y$.

□

2.1.9 Définition. Soient R un anneau et I un idéal bilatère de R . Le groupe quotient R/I muni du produit $(x + I) \cdot (y + I) = xy + I$ est appelé l'anneau quotient ou l'anneau des résidus de R modulo I .

- Remarques.** 1. L'idéal I est clairement un sous-groupe de R vu comme groupe abélien et on peut donc considérer le groupe quotient R/I . On a ainsi $(x + I) + (y + I) = (x + y) + I$.
2. La multiplication des classes résiduelles est bien définie : soient $x, x', y, y' \in R$ tels que $x + I = x' + I$ et $y + I = y' + I$, de sorte que $x' = x + r$ et $y' = y + s$ pour certains $r, s \in I$, et ainsi $(x'y') + I = ((x + r)(y + s)) + I = (xy + xs + ry + rs) + I = xy + I$, puisque I est bilatère.

2.1.10 Théorème (Premier théorème d'isomorphisme). Soit $f : R \rightarrow S$ un homomorphisme d'anneaux. Alors f induit un isomorphisme $\hat{f} : R/\ker f \xrightarrow{\cong} \text{im } f$ où $\hat{f}[x] = f(x)$ pour tout $x \in R$.

- Démonstration.* 1. (\hat{f} est bien définie) Soient $x, x' \in R$ tels que $[x] = [x'] \in R/\ker f$. On a $x' = x + k$ avec $k \in \ker f$. Ainsi $\hat{f}[x'] = f(x') = f(x + k) = f(x) + f(k) = f(x) = \hat{f}[x]$.
2. (\hat{f} est un homomorphisme) Soient $x, y \in R$. On a $\hat{f}([x] + [y]) = \hat{f}([x + y]) = f(x + y) = f(x) + f(y) = \hat{f}[x] + \hat{f}[y]$.
3. (\hat{f} est surjectif) Clair.
4. (\hat{f} est injectif) Soit $[x] \in \ker \hat{f}$, i.e. $\hat{f}[x] = f(x) = 0$, i.e. $x \in \ker f$. Ainsi $[x] = 0 \in R/\ker f$.

□

2.1.11 Proposition. Soient R un anneau et I un idéal bilatère de R . Les idéaux de R qui contiennent I sont en correspondance biunivoque avec les idéaux de l'anneau quotient R/I via l'application $J \mapsto J/I$.

Démonstration. Exercice.

□

2.1.12 Définition. Un anneau R tel que $1 \neq 0$ est dit simple s'il n'admet que deux idéaux distincts, à savoir l'idéal nul et lui-même.

2.1.13 Définition. Soit R un anneau. Un idéal propre M de R est dit maximal s'il n'existe pas d'idéal propre I tel que $M \subsetneq I \subsetneq R$.

2.1.14 Proposition. Soient R un anneau et M un idéal bilatère de R . L'anneau quotient R/M est simple si et seulement si M est maximal.

Démonstration. C'est un corollaire de la proposition ci-dessus. L'anneau R/M est simple si et seulement s'il ne contient que deux idéaux, i.e. il n'y a que deux idéaux qui contiennent M dans R , à savoir M lui-même et R tout entier, i.e. M est maximal. \square

2.1.15 Proposition. *Un anneau commutatif R est simple si et seulement si R est un corps.*

Démonstration. (\implies) Soit $a \neq 0 \in R$. L'idéal aR doit être R tout entier par simplicité. Il existe donc $b \in R$ tel que $ab = 1$ en particulier, i.e. a possède un inverse.
 (\impliedby) Soit I un idéal non-nul du corps R . Il existe donc $a \neq 0 \in I$. Ainsi $aa^{-1} = 1 \in I$, de sorte que $I = R$. \square

2.1.16 Proposition. *Soient R un anneau commutatif et M un idéal de R . L'anneau quotient R/M est un corps si et seulement si l'idéal M est maximal.*

2.1.17 Théorème (Krull, 1929). *Soit R un anneau commutatif avec $1 \neq 0$. Alors R admet un idéal maximal.*

Démonstration. Cf. [Clé06-1]. \square

2.1.18 Définition. Soient R un anneau et $X \subset R$ un sous-ensemble de R . L'idéal à droite (resp. à gauche, bilatère) engendré par X est déterminé par l'ensemble constitué des sommes finies d'éléments de la forme xr (resp. rx , rxs) avec $x \in X$ et $r \in R$ ($s \in R$). On appelle X l'ensemble des générateurs de cet idéal. Lorsque $X = \{x_1, \dots, x_n\}$ est fini, on écrit $x_1R + \dots + x_nR$ (resp. $Rx_1 + \dots + Rx_n$, $\langle x_1, \dots, x_n \rangle$) l'idéal à droite (resp. à gauche, bilatère) engendré par X . Si $X = \{x\}$ est un singleton, l'idéal engendré est dit principal. Lorsque R est commutatif, on utilise souvent la notation (x_1, \dots, x_n) pour désigner l'idéal (bilatère) engendré par $\{x_1, \dots, x_n\}$.

Remarque. Soient R un anneau et $X \subset R$. Un élément de l'idéal à droite engendré par X est de la forme $x_1r_1 + \dots + x_nr_n$, avec $x_1, \dots, x_n \in X$ et $r_1, \dots, r_n \in R$.

2.1.19 Définition. Soit R un anneau tel que $1 \neq 0$. On dit que R est intègre si pour tout $x, y \in R$ tels que $xy = 0$ on a $x = 0$ ou $y = 0$.

2.1.20 Définition. Un anneau intègre R pour lequel tout idéal (bilatère) (resp. à droite, à gauche) est principal est dit principal (resp. à droite, à gauche).

2.1.21 Proposition. *L'anneau \mathbb{Z} des entiers relatifs est principal.*

Démonstration. Soit I un idéal non-trivial de \mathbb{Z} . Soit d le plus petit entier positif dans I . Pour tout $n \in I$ il existe $q, r \in \mathbb{Z}$ tels que $0 \leq r < d$ et $n = qd + r$. Puisque I est un idéal, $n - qd = r$ est un élément de I , de sorte que $r = 0$ par minimalité de d . \square

Remarque. Soient p et q deux nombres premiers. L'anneau \mathbb{Z}/pq n'est pas principal.

2.2 Modules

20.03.2006

2.2.1 Convention. Dans tout le cours, sauf mention contraire, tous les anneaux sont supposés non-triviaux, i.e. tels que $1 \neq 0$.

Rappel. Soit R un anneau. On note R^{opp} l'anneau opposé à R . Les éléments de R^{opp} sont ceux de R . Comme groupes abéliens, R^{opp} et R sont égaux. Le produit dans R^{opp} est donné par $r_1 \cdot^{\text{opp}} r_2 = r_2 \cdot r_1$ pour tout $r_1, r_2 \in R$.

2.2.2 Définition. Soit R un anneau. Un module à gauche sur R , ou R -module à gauche, est un groupe abélien M (noté additivement) muni d'un homomorphisme d'anneaux $\omega : R \rightarrow \text{End}(M)$, où $\text{End}(M)$ est l'anneau des endomorphismes de M . Pour tout $r \in R$, $m \in M$, on note rm l'élément $(\omega(r))(m)$. On dit que R agit à gauche sur M . Un module à droite sur R , ou R -module à droite, est un module à gauche sur R^{opp} , l'anneau opposé à R .

Remarques. 1. Si R est un anneau commutatif, alors les notions de module à gauche et à droite coïncident puisque $R \cong R^{\text{opp}}$ comme anneaux.

2. Soit M un module à gauche sur R , $m, m_1, m_2 \in M$ et $r, r_1, r_2 \in R$. Les règles suivantes sont vérifiées :

- i) $(r_1 + r_2)m = r_1m + r_2m$,
- ii) $(r_1r_2)m = r_1(r_2m)$,
- iii) $1_R m = m$ et
- iv) $r(m_1 + m_2) = rm_1 + rm_2$.

3. Une loi de composition externe d'un anneau R sur un groupe abélien M qui vérifie les règles i) à iv) ci-dessus définit clairement un homomorphisme d'anneaux $R \rightarrow \text{End}(M)$ qui confère à M une structure de R -module à gauche.

Exemples. 1. Soit R un anneau. L'homomorphisme d'anneaux $\omega : R \rightarrow \text{End}(R)$ défini par $r \mapsto \omega(r) : R \rightarrow R$ et $(\omega(r))(r') = r \cdot r'$ pour tout $r, r' \in R$ (i.e. la multiplication à gauche de R) munit R d'une structure de R -module à gauche.

2. Soit I un idéal à gauche d'un anneau R . De façon analogue à l'exemple précédent, I est un R -module à gauche.

3. Soit A un groupe abélien. L'action de \mathbb{Z} sur A définie par $0 \cdot a = 0_A$, $na = (n-1)a + a$ et $(-n)a = -(na)$ pour tout $n \geq 1$ confère à A une structure de \mathbb{Z} -module.

4. Tout espace vectoriel est un module.

2.2.3 Convention. Pour simplifier, on utilisera le terme *module* au lieu de *module à gauche*.

2.2.4 Définition. Soient M, N deux R -modules. Un homomorphisme de R -modules $f : M \rightarrow N$ est un homomorphisme de groupes abéliens qui vérifie $f(rm) = rf(m)$ pour tout $r \in R$, $m \in M$. Un homomorphisme de R -modules $f : M \rightarrow N$ est un monomorphisme (resp. épimorphisme) s'il est simplifiable à gauche (resp. à droite). C'est un isomorphisme s'il existe un homomorphisme de R -modules $g : N \rightarrow M$ tel que $gf = \text{id}_M$ et $fg = \text{id}_N$.

2.2.5 Convention. On note $M \cong N$ s'il existe un isomorphisme $M \rightarrow N$. On note $M \hookrightarrow N$ (resp. $M \twoheadrightarrow N$) un monomorphisme (resp. épimorphisme).

2.2.6 Définition. Un sous-module d'un R -module M est un sous-groupe M' de M qui vérifie $rm' \in M'$ pour tout $r \in R$ et $m' \in M'$.

2.2.7 Définition. Soit M' un sous-module du R -module M . Le module quotient M/M' est le R -module obtenu en munissant le groupe quotient M/M' de l'action définie par $r[m] = [rm]$ pour tout $r \in R$, $m \in M$.

Remarque. Il faut vérifier que l'action est bien définie, i.e. qu'elle ne dépend pas du choix du représentant de $[m]$: supposons que $[m] = [m_0]$, i.e. $m = m_0 + m'$ pour un certain $m' \in M'$, alors $r[m] = [rm] = [r(m_0 + m')] = [rm_0 + rm'] = [rm_0] = r[m_0]$ puisque $rm' \in M'$.

2.2.8 Définition. Soit $f : M \rightarrow N$ un homomorphisme de R -modules. Le noyau de f est le sous-module de M

$$\ker f = \{m \in M \mid f(m) = 0_N\}.$$

L'image de f est le sous-module de N

$$\operatorname{im} f = \{f(m) \in N \mid m \in M\}.$$

Le conoyau de f est le R -module

$$\operatorname{coker} f = N / \operatorname{im} f.$$

2.2.9 Proposition. Soit $f : M \rightarrow N$ un homomorphisme de R -modules. On a les assertions suivantes :

1. f est injectif si et seulement si $\ker f = \{0\}$,
2. f est surjectif si et seulement si $\operatorname{coker} f = \{[0]\}$,
3. f est un monomorphisme si et seulement si $\ker f = \{0\}$,
4. f est un épimorphisme si et seulement si $\operatorname{coker} f = \{[0]\}$,
5. f est un isomorphisme si et seulement si f est bijectif et
6. en particulier, f est un isomorphisme si et seulement si f est un monomorphisme et un épimorphisme.

Démonstration. 1. (\Leftarrow) Soient $m, m' \in M$ tels que $f(m) = f(m')$. Alors $0 = f(m) - f(m') = f(m - m')$, i.e. $m - m' \in \ker f$, de sorte que $m - m' = 0$ et $m = m'$. (\Rightarrow) Soit $m \in M$ tel que $f(m) = 0$. Alors $f(m) = f(0)$ et $m = 0$ par injectivité de f .

2. Clair.

3. (\Leftarrow) Si f est injectif, alors il est clairement simplifiable à gauche. (\Rightarrow) Supposons que $\ker f \neq \{0\}$. Soit $g : \ker f \subset M$ l'homomorphisme injectif canonique et soit $h : \ker f \rightarrow M$ l'homomorphisme trivial. On a $fg = fh$ avec $g \neq h$, de sorte que f n'est pas un monomorphisme.

4. (\Leftarrow) Si f est surjectif, alors il est clairement simplifiable à droite. (\Rightarrow) Supposons que $\operatorname{coker} f \neq \{[0]\}$. Soit $g : N \rightarrow \operatorname{coker} f$ l'homomorphisme surjectif canonique et soit $h : N \rightarrow \operatorname{coker} f$ l'homomorphisme trivial. On a $gf = hf$ avec $g \neq h$, de sorte que f n'est pas un épimorphisme.

5. (\Leftarrow) Il faut montrer que l'application inverse g de f est un homomorphisme : soient $r, r' \in R$ et $n, n' \in N$. On a $fg(rn + r'n') = \operatorname{id}_N(rn + r'n') = rn + r'n' = r(fg(n)) + r'(fg(n')) = f(rg(n) + r'g(n'))$, de sorte que $g(rn + r'n') = rg(n) + r'g(n')$ puisque f est injectif. (\Rightarrow) Clair.

□

2.2.10 Théorème (Propriété universelle du quotient). *Soit $f : M \rightarrow N$ un homomorphisme de R -modules. Soit M' un sous-module de M tel que $M' \subset \ker f$. Il existe un unique homomorphisme $\tilde{f} : M/M' \rightarrow N$ qui fait commuter le diagramme suivant :*

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \text{can.} \downarrow & \nearrow \tilde{f} & \\ M/M' & & \end{array}$$

De plus, on a $\ker \tilde{f} = \ker f/M'$ et $\text{im } \tilde{f} = \text{im } f$. En particulier, \tilde{f} est un épimorphisme si et seulement si f l'est et \tilde{f} est un monomorphisme si et seulement si $M' = \ker f$.

Démonstration. 1. (existence de \tilde{f}) On pose $\tilde{f}[m] = f(m)$ pour tout $m \in M$. Voyons que c'est bien défini : soit $m_0 \in M$ tel que $[m] = [m_0]$, i.e. $m = m_0 + m'$ pour un certain $m' \in M' \subset \ker f$. On a $\tilde{f}[m] = f(m) = f(m_0 + m') = f(m_0) + f(m') = f(m_0) = \tilde{f}[m_0]$ puisque $m' \in \ker f$.

2. (unicité de \tilde{f}) Supposons qu'il existe un homomorphisme $g : M/M' \rightarrow N$ qui fasse commuter le diagramme ci-dessus. Soit $m \in M$. On a donc $g[m] = f(m)$ par commutativité. Or $f(m) = \tilde{f}[m]$, de sorte que $g[m] = \tilde{f}[m]$. Ainsi $g = \tilde{f}$.

3. ($\ker \tilde{f} = \ker f/M'$) On a $[m] \in \ker \tilde{f}$ si et seulement si $f(m) = 0$, i.e. $m \in \ker f$.

4. ($\text{im } \tilde{f} = \text{im } f$) Clair par définition de \tilde{f} .

□

2.2.11 Corollaire (Premier théorème d'isomorphisme). *Soit $f : M \rightarrow N$ un homomorphisme de R -modules. Alors f induit un isomorphisme $\hat{f} : M/\ker f \xrightarrow{\cong} \text{im } f$ où $\hat{f}[m] = f(m)$ pour tout $m \in M$.*

Démonstration. On prend $N = \text{im } f$ et $M' = \ker f$.

□

2.2.12 Définition. Soit $\{A_i\}_{i \in I}$ une famille de R -modules indexée par l'ensemble I . On définit la **somme directe** $\bigoplus_{i \in I} A_i$ comme le sous-ensemble du produit (ensembliste) $\prod_{i \in I} A_i$ constitué des élément $(a_i)_{i \in I}$ tels que $a_i \neq 0$ pour un nombre fini d'index $i \in I$ (i.e. suites à *support compact*) muni de l'addition terme à terme $(a_i)_{i \in I} + (b_i)_{i \in I} = (a_i + b_i)_{i \in I}$ et de l'action définie par $r(a_i)_{i \in I} = (ra_i)_{i \in I}$, pour tout $r \in R$, $(a_i)_{i \in I}, (b_i)_{i \in I} \in \bigoplus_{i \in I} A_i$.

2.2.13 Théorème (Propriété universelle de la somme directe). Soient M un R -module et $\{f_i : A_i \rightarrow M\}_{i \in I}$ une famille d'homomorphismes de R -modules indexée par l'ensemble I . Il existe un unique homomorphisme $f : \bigoplus_{i \in I} A_i \rightarrow M$ tel que le diagramme suivant commute pour tout $i \in I$:

$$\begin{array}{ccc} A_i & & \\ \text{can.} \downarrow & \searrow f_i & \\ \bigoplus_{i \in I} A_i & \xrightarrow{f} & M. \end{array}$$

Démonstration. 1. (existence de f) On pose $f((a_i)_{i \in I}) = \sum_{i \in I} f_i(a_i)$ pour tout $(a_i)_{i \in I} \in \bigoplus_{i \in I} A_i$. C'est possible puisqu'il n'y a qu'un nombre fini d'index $i \in I$ pour lesquels $a_i \neq 0$.

Soient $j \in I$, $k_j : A_j \hookrightarrow \bigoplus_{i \in I} A_i$ l'inclusion canonique et $a_j \in A_j$. On a $f k_j(a_j) = \sum_{i \in I} f_i((k_j(a_j))_i) = f_j(a_j)$ puisque $(k_j(a_j))_i = a_j$ si $i = j$ et 0 sinon.

2. (unicité de f) Supposons qu'il existe un homomorphisme $g : \bigoplus_{i \in I} A_i \rightarrow M$ qui fasse commuter le diagramme ci-dessus. Soit $(a_i)_{i \in I} \in \bigoplus_{i \in I} A_i$. On a $g((a_i)_{i \in I}) = g(\sum_{i \in I} k_i(a_i)) = \sum_{i \in I} g k_i(a_i) = \sum_{i \in I} f_i(a_i) = f((a_i)_{i \in I})$.

□

2.3 Suites exactes

2.3.1 Définition. Soient $f : A \rightarrow B$ et $g : B \rightarrow C$ des homomorphismes de R -modules. La suite $A \xrightarrow{f} B \xrightarrow{g} C$ est dite **exacte (en B)** si $\text{im } f = \ker g$. Une suite d'homomorphismes de R -modules

$$A_0 \longrightarrow A_1 \longrightarrow \cdots \longrightarrow A_n \longrightarrow A_{n+1}$$

exacte en A_1, \dots, A_n est simplement dite **exacte**. Une suite exacte de la forme

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

est dite **exacte courte**. Pour des raisons évidentes (cf. exemples ci-dessous), on note souvent $A \rightarrowtail B \twoheadrightarrow C$ une telle suite.

- Exemples.**
1. La suite $0 \longrightarrow A \xrightarrow{f} B$ est exacte si et seulement si f est un monomorphisme.
 2. La suite $A \xrightarrow{f} B \longrightarrow 0$ est exacte si et seulement si f est un épimorphisme.
 3. La suite $0 \longrightarrow A \xrightarrow{f} B \longrightarrow 0$ est exacte si et seulement si f est un isomorphisme.
 4. La suite $\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{\text{can.}} \mathbb{Z}/2$ est exacte courte.

2.3.2 Théorème (Lemme du deux sur trois). Soient $A \rightarrowtail B \twoheadrightarrow C$ et $A' \rightarrowtail B' \twoheadrightarrow C'$ deux suites exactes courtes de R -modules et supposons qu'on ait le diagramme commutatif suivant :

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' \end{array}$$

où α, β et γ sont des homomorphismes de R -modules. Si deux des trois homomorphismes α, β et γ sont des isomorphismes, alors le troisième l'est aussi.

Démonstration. On ne va traiter que l'un des trois cas possibles : supposons que α et γ sont des isomorphismes et montrons que β est aussi un isomorphisme. On utilise la méthode dite de *chasse dans les diagrammes*.

1. ($\ker \beta = 0$) Soit $b \in \ker \beta$. Alors $b \in \ker g$ puisque $\gamma g(b) = g' \beta(b) = 0$ et γ est un isomorphisme. Par exactitude il existe $a \in A$ tel que $f(a) = b$. Or $0 = \beta f(a) = f' \alpha(a)$, de sorte que $\alpha(a) = 0$ par injectivité de f' et $a = 0$ puisque α est un isomorphisme. Ainsi $b = f(a) = f(0) = 0$.
2. ($\text{im } \beta = B$) Soit $b' \in B'$. Il existe $b_0 \in B$ tel que $\gamma g(b_0) = g'(b')$ puisque γ est un isomorphisme. On a $g'(b' - \beta(b_0)) = g'(b') - g' \beta(b_0) = g'(b') - \gamma g(b_0) = g'(b') - g'(b') = 0$ par commutativité. Ainsi il existe $a' \in A'$ tel que $f'(a') = b' - \beta(b_0)$ par exactitude. Puisque α est un isomorphisme, il existe $a \in A$ tel que $\alpha(a) = a'$. Posons $b = f(a) + b_0$. On a finalement $\beta(b) = \beta(f(a) + b_0) = \beta f(a) + \beta(b_0) = f' \alpha(a) + \beta(b_0) = f'(a') + \beta(b_0) = (b' - \beta(b_0)) + \beta(b_0) = b'$.

□

Remarque. Ce résultat **n'implique pas** que si $A \hookrightarrow B \twoheadrightarrow C$ et $A' \hookrightarrow B' \twoheadrightarrow C'$ sont des suites exactes courtes avec $A \cong A'$ et $C \cong C'$, alors $B \cong B'$. Il faut vraiment que ces isomorphismes soient compatibles avec un homomorphisme $B \rightarrow B'$ dans le sens où le diagramme ci-dessus commute! Par exemple on a les deux suites exactes courtes $\mathbb{Z}/2 \hookrightarrow \mathbb{Z}/2 \oplus \mathbb{Z}/2 \twoheadrightarrow \mathbb{Z}/2$ et $\mathbb{Z}/2 \hookrightarrow \mathbb{Z}/4 \twoheadrightarrow \mathbb{Z}/2$, mais $\mathbb{Z}/2 \oplus \mathbb{Z}/2 \not\cong \mathbb{Z}/4$.

2.3.3 Définition. Soit $g : B \rightarrow C$ un homomorphisme de R -modules. Une **section** de g est un homomorphisme $\sigma : C \rightarrow B$ tel que $g\sigma = \text{id}_C$ (i.e. σ est un inverse à droite de g). Une suite exacte courte de R -modules $A \hookrightarrow B \twoheadrightarrow C$ est dite **scindée** si $B \twoheadrightarrow C$ possède une section.

2.3.4 Théorème. soit $A \hookrightarrow B \twoheadrightarrow C$ une suite exacte courte scindée. Alors $B \cong A \oplus C$.

Démonstration. Considérons le diagramme suivant :

$$\begin{array}{ccccc} A & \xrightarrow{\text{can.}} & A \oplus C & \xrightarrow{\text{can.}} & C \\ \parallel & & \downarrow \beta & \nearrow \sigma & \parallel \\ A & \xrightarrow{f} & B & \xleftarrow{g} & C \end{array}$$

où $\beta(a, c) = f(a) + \sigma(c)$. Il est commutatif puisque $\beta(a, 0) = f(a) + \sigma(0) = f(a)$ et $g\beta(a, c) = g(f(a) + \sigma(c)) = gf(a) + g\sigma(c) = 0 + c = c$. On conclut à l'aide du lemme du *deux sur trois*. \square

Remarque. L'application β de la preuve est en fait une conséquence de la propriété universelle de la somme directe, comme le montre le diagramme commutatif suivant :

$$\begin{array}{ccc} A & & \\ \text{can.} \downarrow & \searrow f & \\ A \oplus C & \xrightarrow{\beta} & B \\ \text{can.} \uparrow & \nearrow \sigma & \\ C & & \end{array}$$

Exemples. Il existe des suites exactes courtes qui ne sont pas scindées :

1. $\mathbb{Z}/2 \xrightarrow{\cdot 2} \mathbb{Z}/4 \xrightarrow{\text{can.}} \mathbb{Z}/2$ n'est pas scindée,
2. $\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{\text{can.}} \mathbb{Z}/2$ n'est pas scindée et
3. $\mathbb{Z} \xrightarrow{\text{can.}} \mathbb{Q} \xrightarrow{\text{can.}} \mathbb{Q}/\mathbb{Z}$ n'est pas scindée.

2.4 Modules libres et projectifs

27.03.2006

2.4.1 Définition. Soient M un R -module et S un sous-ensemble de M . Le sous-module de M engendré par S est

$$\langle S \rangle = \left\{ \sum_{s \in S} r_s s \mid r_s 0 \in R, r_s \neq 0 \text{ pour un nombre fini de } s \text{ seulement} \right\}.$$

On dit que S **engendre** M (ou S est un **ensemble de générateurs** de M) si $M = \langle S \rangle$. Si M possède un ensemble de générateurs fini, alors M est dit **de génération finie** (ou **de type fini**).

2.4.2 Définition. Soient M un R -module engendré par S . L'ensemble de générateurs S est une **base** de M si les éléments de S sont linéairement indépendants, i.e. si

$$\sum_{\substack{s \in S \\ \text{finie}}} r_s s = 0 \text{ implique que } r_s = 0 \text{ pour tout } s \in S.$$

Si M possède une base S , alors M est dit **libre** (sur S). Si M possède une base S finie, alors on dit que M est de **rang fini** et la cardinalité de S est un **rang** de M .

Remarques. 1. Si M possède une base S , alors pour tout élément $m \in M$ il existe une unique suite $(r_s)_{s \in S}$ telle que $m = \sum_{s \in S} r_s s$.
2. En général, un rang d'un module libre n'est pas unique, i.e. il existe des modules libres admettant des bases de cardinalités différentes (cf. chapitre suivant).

Exemples. 1. Le \mathbb{Z} -module \mathbb{Z} est libre de rang 1.
2. Le \mathbb{Z} -module $\mathbb{Z}/2$ est engendré par $\{[1]\}$ mais n'est pas libre puisque $2[1] = [0]$ et $2 \neq 0 \in \mathbb{Z}$ (c'est un exemple de module de génération finie qui n'est pas de rang fini puisqu'il ne possède pas de base).

2.4.3 Théorème. Si L est un R -module libre sur S , alors $L \cong \bigoplus_{s \in S} R$. Réciproquement, $\bigoplus_{s \in S} R$ est un R -module libre.

Démonstration. 1. Considérons l'homomorphisme $f : L \rightarrow \bigoplus_{s \in S} R$ défini par $m \mapsto (r_s)_{s \in S}$ sachant que $m = \sum_{s \in S} r_s s$ est l'unique décomposition de m dans la base S . Considérons également l'homomorphisme $g : \bigoplus_{s \in S} R \rightarrow L$ défini par $(r_s)_{s \in S} \mapsto \sum_{s \in S} r_s s$. On a ainsi $gf(m) = g(\sum_{s \in S} r_s s) = g((r_s)_{s \in S}) = \sum_{s \in S} r_s s = m$ et $fg((r_s)_{s \in S}) = f(\sum_{s \in S} r_s s) = (r_s)_{s \in S}$, de sorte que f et g sont des isomorphismes.
2. Considérons le sous-ensemble de $\bigoplus_{s \in S} R$ donné par $\{e_s \mid s \in S\}$ avec $e_s = (\delta_{st})_{t \in S}$ ou δ_{st} est le symbole de Kronecker défini par

$$\delta_{st} = \begin{cases} 1_R & \text{si } s = t, \\ 0_R & \text{sinon,} \end{cases}$$

pour tout $s, t \in S$. C'est un ensemble de générateurs puisque pour tout $(r_s)_{s \in S} \in \bigoplus_{s \in S} R$ on a clairement $(r_s)_{s \in S} = \sum_{s \in S} r_s e_s$. De plus on a $\sum_{s \in S} r_s e_s = 0$ si et seulement si pour tout $t \in S$ on a $(\sum_{s \in S} r_s e_s)_t = 0_R$, ce qui implique $r_t = 0_R$. C'est donc une base.

□

2.4.4 Théorème. *Tout R -module est quotient d'un R -module libre.*

Démonstration. Soit M un R -module. On considère le R -module libre $L = \bigoplus_{m \in M} R$ de base $\{e_m \mid m \in M\}$ et l'homomorphisme $f : L \rightarrow M$ défini par $e_m \mapsto m$ pour tout $m \in M$. Par le premier théorème d'isomorphisme, on a $L/\ker f \cong M$ puisque f est clairement surjectif. \square

2.4.5 Théorème. *Soit L un R -module libre. Pour tout épimorphisme $\epsilon : B \twoheadrightarrow C$ et pour tout homomorphisme $\gamma : L \rightarrow C$ il existe un homomorphisme $f : L \rightarrow B$ tel que le diagramme suivant commute :*

$$\begin{array}{ccc} & L & \\ \swarrow f & \downarrow \gamma & \\ B & \xrightarrow{\epsilon} & C \end{array}$$

Démonstration. Soit S une base de L . Par surjectivité de ϵ , pour tout $s \in S$ il existe $b_s \in B$ tel que $\epsilon(b_s) = \gamma(s)$. Pour tout $s \in S$ posons $B_s = \{b \in B \mid \epsilon(b) = \gamma(s)\}$. On a $b_s \in B_s$, de sorte que $B_s \neq \emptyset$. Par l'axiome du choix, il existe une application $\tilde{f} : S \rightarrow \bigcup_{s \in S} B_s \subset B$ telle que $\tilde{f}(s) \in B_s$, i.e. $\epsilon\tilde{f}(s) = \gamma(s)$ pour tout $s \in S$. On étend \tilde{f} à $f : L \rightarrow B$ par linéarité, i.e. pour tout $m = \sum_{s \in S} r_s s \in M$ on pose $f(m) = f(\sum_{s \in S} r_s s) = \sum_{s \in S} r_s \tilde{f}(s)$. On a bien $\epsilon f(m) = \epsilon f(\sum_{s \in S} r_s s) = \epsilon \sum_{s \in S} r_s \tilde{f}(s) = \sum_{s \in S} r_s \epsilon \tilde{f}(s) = \sum_{s \in S} r_s \gamma(s) = \gamma(\sum_{s \in S} r_s s) = \gamma(m)$. \square

2.4.6 Remarque. L'homomorphisme f n'est en général pas unique, comme le prouve l'exemple constitué de \mathbb{Z} -modules suivant :

$$\begin{array}{ccc} & \mathbb{Z} & \\ \swarrow (\cdot 3) & \downarrow \text{can.} & \\ \mathbb{Z} & \xrightarrow{\text{can.}} & \mathbb{Z}/2. \end{array}$$

Nous verrons que cette propriété des modules libres est importante dans la suite de ce cours. On appellera *projectifs* les modules qui en jouissent. On a donc la définition suivante :

2.4.7 Définition. Un R -module P est **projectif** si pour tout épimorphisme $\epsilon : B \twoheadrightarrow C$ et pour tout homomorphisme $\gamma : P \rightarrow C$ il existe un homomorphisme $f : P \rightarrow B$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} & P & \\ \swarrow f & \downarrow \gamma & \\ B & \xrightarrow{\epsilon} & C \end{array}$$

2.4.8 Lemme. *Soit $\{P_i\}_{i \in I}$ une famille de R -modules indexée par l'ensemble I . Les P_i sont projectifs pour tout $i \in I$ si et seulement si $\bigoplus_{i \in I} P_i$ est projectif.*

Démonstration. (\implies) Pour tout $i \in I$ considérons le diagramme suivant :

$$\begin{array}{ccc}
 & P_i & \\
 \text{can.} \downarrow k_i & & \\
 f_i \swarrow & \oplus_{i \in I} P_i & \searrow \gamma \\
 B & \xrightarrow{\epsilon} & C.
 \end{array}$$

Par projectivité de P_i , il existe f_i qui fait commuter le diagramme. Par la propriété universelle de la somme directe, il existe (un unique) $f : \oplus_{i \in I} P_i \rightarrow B$ qui fasse commuter le diagramme suivant pour tout $i \in I$:

$$\begin{array}{ccccc}
 P_i & & & & \\
 \downarrow k_i \text{ can.} & \searrow f_i & \searrow \gamma k_i & & \\
 \oplus_{i \in I} P_i & \xrightarrow{\quad f \quad} & B & \xrightarrow{\epsilon} & C.
 \end{array}$$

Or, pour tout $i \in I$, le diagramme suivant commute :

$$\begin{array}{ccc}
 P_i & & \\
 \downarrow k_i \text{ can.} & \searrow \gamma k_i & \\
 \oplus_{i \in I} P_i & \xrightarrow{\gamma} & C,
 \end{array}$$

et par la propriété universelle de la somme directe, γ est l'unique homomorphisme à avoir cette propriété. Il s'ensuit que $\epsilon f = \gamma$.

(\Leftarrow) Soit $i \in I$, $\gamma : P_i \rightarrow C$ et $\epsilon : B \twoheadrightarrow C$. Pour tout $j \in I$ posons

$$\delta_j = \begin{cases} \gamma & \text{si } i = j, \\ 0 & \text{sinon.} \end{cases}$$

Par la propriété universelle de la somme directe, il existe γ_i tel que le diagramme suivant commute pour tout $j \in I$:

$$\begin{array}{ccc}
 P_j & & \\
 \downarrow \text{can.} & \searrow \delta_j & \\
 \oplus_{i \in I} P_i & \xrightarrow{\gamma_i} & C.
 \end{array}$$

Par projectivité de $\oplus_{i \in I} P_i$ on a le diagramme commutatif suivant :

$$\begin{array}{ccc}
 & P_i & \\
 \text{can.} \swarrow & & \downarrow \gamma \\
 \oplus_{i \in I} P_i & & C \\
 \swarrow & \searrow \gamma_i & \\
 B & \xrightarrow{\epsilon} & C.
 \end{array}$$

□

2.4.9 Théorème. Soit P un R -module. Les assertions suivantes sont équivalentes :

1. P est projectif,
2. pour tout épimorphisme $\epsilon : B \twoheadrightarrow C$, l'homomorphisme induit $\epsilon_* : \text{Hom}(P, B) \rightarrow \text{Hom}(P, C)$ défini par $\epsilon_*(f) = \epsilon f$ est surjectif,
3. toute suite exacte courte $A \hookrightarrow B \twoheadrightarrow P$ est scindée,
4. P est facteur direct dans chaque module dont il est quotient,
5. P est facteur direct d'un module libre.

Démonstration. (1. \implies 2.) Soit $\gamma : P \rightarrow C$. Par projectivité de P on a le diagramme commutatif suivant :

$$\begin{array}{ccc} & P & \\ & \downarrow \gamma & \\ B & \xrightarrow{\epsilon} & C, \end{array} \quad \begin{array}{c} \nearrow f \\ \end{array}$$

et $\epsilon_*(f) = \epsilon f = \gamma$.

- (2. \implies 3.) L'épimorphisme $\epsilon : B \twoheadrightarrow P$ induit l'homomorphisme surjectif $\epsilon_* : \text{Hom}(P, B) \twoheadrightarrow \text{Hom}(P, P)$. Il existe donc $\sigma : P \rightarrow B$ tel que $\epsilon_*(\sigma) = \epsilon\sigma = \text{id}_P$.
- (3. \implies 4.) Supposons que $P \cong B/A$. Alors on a la suite exacte courte scindée $A \hookrightarrow B \twoheadrightarrow P$. Ainsi $B \cong A \oplus P$.
- (4. \implies 5.) Comme tout module, P est quotient d'un module libre.
- (5. \implies 1.) On a $L \cong P \oplus Q$ avec L libre, donc projectif. Par le lemme, P est projectif.

□

Il est clair par définition que tout module libre est projectif. La réciproque est fausse en général, comme le montre l'exemple suivant :

Exemple. Soient $p, q \in \mathbb{Z}$ deux nombres premiers. On a $\mathbb{Z}/p \oplus \mathbb{Z}/q \cong \mathbb{Z}/pq$ (cf. exercices). Par le point 5. du théorème, \mathbb{Z}/p et \mathbb{Z}/q sont des \mathbb{Z}/pq -modules projectifs. Ils ne sont pas libres puisque ils sont de cardinalité inférieure à celle de \mathbb{Z}/pq .

Cependant, on a les résultats suivants :

2.4.10 Théorème. Tout sous-module d'un module libre sur un anneau principal est libre.

2.4.11 Corollaire. Tout module projectif sur un anneau principal est libre. En d'autres termes, sur un anneau principal, il n'y a pas de distinction entre les modules libres et projectifs.

Démonstration. Un module projectif est facteur direct d'un module libre, donc sous-module d'un module libre, donc lui-même libre. □

Démonstration du théorème. Soient $L = \bigoplus_{s \in S} R$ un R -module libre et $M \subset L$ un sous-module. Rappelons que $\{e_s \mid s \in S\}$ est une base de L . Cherchons une base pour M . C'est une conséquence connue du lemme de Zorn de pouvoir supposer S bien ordonné. Pour tout $t \in S$ considérons donc les sous-modules libres de L suivants :

$$L_t^- = \bigoplus_{s < t} R \quad \text{et} \quad L_t = \bigoplus_{s \leq t} R.$$

Soit $m \in M \cap L_t$. On peut clairement écrire $m = m^- + re_t$ avec $m^- \in M \cap L_t^-$. Considérons l'homomorphisme $f_t : M \cap L_t \rightarrow R$ défini par $f_t(m) = r$. On a alors la suite exacte courte suivante :

$$M \cap L_t^- \xrightarrow{\text{can.}} M \cap L_t \xrightarrow{f_t} \text{im } f_t.$$

Comme R est principal, l'idéal $\text{im } f_t$ est engendré par un seul élément, disons r_t . Si $r_t \neq 0$, alors il existe $m_t \in (M \cap L_t) - (M \cap L_t^-)$ tel que $f_t(m_t) = r_t$. Soit $T \subset S$ tel que $t \in T$ si et seulement si $r_t \neq 0$. Alors l'ensemble $B = \{m_t \mid t \in T\}$ constitue une base de M .

1. (les m_t sont linéairement indépendants) Supposons que $\sum_{i=1}^n a_i m_{t_i} = 0$ avec $t_1 < t_2 < \dots < t_n$. On a alors $f_{t_n}(\sum_{i=1}^n a_i m_{t_i}) = a_{t_n} r_{t_n} = 0$. Comme R est intègre et $r_{t_n} \neq 0$, on a $a_{t_n} = 0$. On conclut par récurrence.
2. (B est un ensemble de générateurs) Supposons que B ne soit pas un ensemble de générateurs. Alors il existe $s \in S$ minimal pour lequel $m \in M \cap L_s$ et m ne s'écrit pas comme combinaison linéaire d'éléments de B . Si $s \notin T$, alors $\text{im } f_s = 0$, $M \cap L_s = M \cap L_s^-$ et $m \in M \cap L_s^-$, ce qui contredit la minimalité de s . Si $s \in T$, on a $f_s(m) = ar_s$ pour un certain $a \in R$ puisque $\text{im } f_s = \langle r_s \rangle$. Posons $m' = m - am_s$, de sorte que

$$f_s(m') = f_s(m) - f_s(am_s) = f_s(m) - af_s(m_s) = ar_s - ar_s = 0.$$

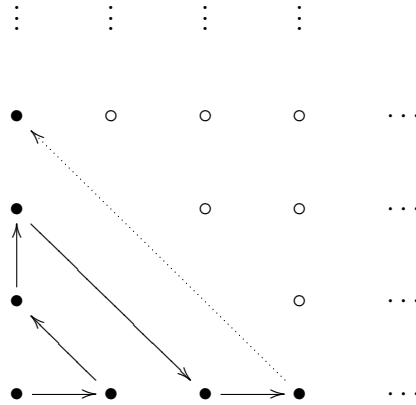
Ainsi $m' \in \ker f_s = M \cap L_s^-$. Or $m' = m - am_s$ ne s'écrit pas comme combinaison linéaire d'éléments de B , ce qui contredit la minimalité de s .

□

2.5 La propriété du rang unique

2.5.1 Proposition. *Il existe un anneau non-trivial R tel que $R \cong R \oplus R$ comme R -modules.*

Démonstration. C'est un fait bien connu que l'ensemble $\mathbb{N} \times \{0\} \cup \{0\} \times \mathbb{N}$ est dénombrable, i.e. il existe une bijection $\varphi = (\varphi_X, \varphi_Y) : \mathbb{N} \rightarrow \mathbb{N} \times \{0\} \cup \{0\} \times \mathbb{N}$. Par exemple on peut prendre la correspondance suivante :



2.5.3 Théorème. *Tout anneau commutatif non-trivial a la propriété du rang unique.*

Démonstration. Soit R un anneau commutatif non-trivial. D'après le théorème de Krull, il existe un idéal maximal M de R . L'anneau quotient $\mathbb{K} = R/M$ est un corps et a donc la propriété du rang unique. Supposons que $\varphi : R^m \cong R^n : \varphi^{-1}$ avec $m, n \in \mathbb{N}$. On a $\varphi \in \text{Hom}_R(R^m, R^n)$ et $\varphi^{-1} \in \text{Hom}_R(R^n, R^m)$. Il existe donc une matrice $A = (a_{ij}) \in M_{m \times n}(R)$ et une matrice $B = (b_{kl}) \in M_{n \times m}(R)$ telles que $AB = I_m$ et $BA = I_n$ (cf. exercices). Soit $p : R \rightarrow \mathbb{K}$ l'homomorphisme surjectif canonique de R -modules. On a clairement $p(A)p(B) = (p(a_{ij}))(p(b_{kl})) = p(AB) = p(I_m) = I_m \in M_m(\mathbb{K})$ et $p(B)p(A) = I_n \in M_n(\mathbb{K})$. Ainsi $\mathbb{K}^m \cong \mathbb{K}^n$ et $m = n$. \square

2.6 Anneaux et modules noethériens

2.6.1 Définition. Un R -module M est **noethérien** s'il satisfait la *condition de chaîne ascendante*, i.e. s'il n'existe pas de suite dénombrable ascendante propre de sous-modules $M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \dots$ de M . En d'autres termes, M est noethérien si toute suite infinie de sous-modules $M_0 \subset M_1 \subset M_2 \dots$ est stationnaire, i.e. il existe $n_0 \in \mathbb{N}$ tel que $M_n = M_{n_0}$ pour tout $n \geq n_0$.

Exemples. 1. Tout espace vectoriel de dimension finie est noethérien.
 2. Tout module fini est noethérien.
 3. Le \mathbb{Z} -module $\mathbb{Z}[X_1, X_2, \dots]$ n'est pas noethérien, puisqu'il contient la chaîne strictement croissante de sous-modules suivante :

$$0 \subsetneq \langle X_1 \rangle \subsetneq \langle X_1, X_2 \rangle \subsetneq \langle X_1, X_2, X_3 \rangle \subsetneq \dots$$

2.6.2 Proposition. *Tout module noethérien est de génération finie.*

Démonstration. Soit M un R -module qui n'est pas de génération finie. Si $S \subset M$ est un sous-ensemble fini de M , alors l'ensemble $M - \langle S \rangle$ est clairement non-vide. Par l'axiome du choix, il existe donc une application $\gamma : \{S \subset M \mid S \text{ fini}\} \rightarrow \bigcup_{S \subset M, S \text{ fini}} (M - \langle S \rangle)$ telle que $\gamma(S) \in M - \langle S \rangle$ pour tout $S \subset M$, S fini. Posons

$$x_0 \in \gamma(\emptyset) \text{ et} \\ x_{n+1} \in \gamma(\{x_0, x_1, \dots, x_n\}) \text{ pour tout } n \geq 0.$$

On a ainsi une chaîne strictement croissante de sous-modules de M donnée par

$$\langle x_0 \rangle \subsetneq \langle x_0, x_1 \rangle \subsetneq \langle x_0, x_1, x_2 \rangle \subsetneq \dots$$

□

Remarque. La réciproque est fausse en général. Par exemple, le $\mathbb{Z}[X_1, X_2, \dots]$ -module libre de rang 1 n'est pas noethérien puisque il contient la chaîne de sous-modules strictement croissante suivante :

$$0 \subsetneq \langle X_1 \rangle \subsetneq \langle X_1, X_2 \rangle \subsetneq \langle X_1, X_2, X_3 \rangle \subsetneq \dots$$

Cette chaîne est différente de celle de l'exemple 3. ci-dessus !

2.6.3 Théorème. *Soit $M' \twoheadrightarrow M \twoheadrightarrow M''$ une suite exacte courte de R -modules. Alors M est noethérien si et seulement si M' et M'' sont noethériens.*

Démonstration. (\implies) Supposons M' (resp. M'') non-noethérien. Alors il existe une suite ascendante propre de sous-modules de M' (M'') dont l'image (la préimage) dans M est aussi une suite ascendante propre de sous-modules de M . Ainsi M est non-noethérien.

(\impliedby) Considérons la suite exacte courte $M' \xrightarrow{f} M \xrightarrow{g} M''$. Soit $M_0 \subset M_1 \subset M_2 \subset \dots$ une suite croissante de sous-modules de M . Montrons qu'elle stabilise. Posons $M'_n = f^{-1}(M_n)$ et $M''_n = g(M_n)$ pour tout $n \in \mathbb{N}$. On a clairement les suites croissantes $M'_0 \subset M'_1 \subset M'_2 \subset \dots$ et $M''_0 \subset M''_1 \subset M''_2 \subset \dots$, qui stabilisent puisque M' et M'' sont noethériens.

De plus, pour tout $n \in \mathbb{N}$ on a la suite exacte courte $M'_n \xrightarrow{f} M_n \xrightarrow{g} M''_n$. Ainsi il existe $n_0 \in \mathbb{N}$ tel que pour tout $n \geq n_0$ on ait le diagramme commutatif suivant :

$$\begin{array}{ccccc} M'_{n_0} & \twoheadrightarrow & M_{n_0} & \twoheadrightarrow & M''_{n_0} \\ = \downarrow \text{incl.} & & \downarrow \text{incl.} & & = \downarrow \text{incl.} \\ M'_n & \twoheadrightarrow & M_n & \twoheadrightarrow & M''_n. \end{array}$$

Ainsi $M_0 \subset M_1 \subset M_2 \subset \dots$ stabilise par le lemme des deux sur trois.

□

2.6.4 Corollaire. *Toute somme directe finie de modules noethériens est noethérienne.*

2.6.5 Définition. Un anneau R est **noethérien à gauche** (resp. **à droite**) s'il est noethérien comme R -module à gauche (resp. à droite). Un anneau R est **noethérien** s'il est noethérien à gauche et à droite.

Exemples. 1. Tout corps est noethérien.
2. L'anneau $\mathbb{Z}[X_1, X_2, X_3, \dots]$ n'est pas noethérien.

2.6.6 Corollaire. *Tout module de génération finie sur un anneau noethérien à gauche est noethérien.*

Démonstration. Soit M un R -module de génération finie avec R noethérien à gauche. Il existe un épimorphisme $R^n \twoheadrightarrow M$ pour un certain $n \in \mathbb{N}$, avec R^n noethérien par le corollaire. Ainsi M est noethérien par le théorème. □

2.6.7 Proposition. *Tout anneau principal à gauche est noethérien à gauche.*

Démonstration. Soit R un anneau principal à gauche. Soit $I_0 \subset I_1 \subset I_2 \subset \dots$ une suite croissante de sous-modules de R vu comme R -module. Ce sont clairement des idéaux à gauche de R . L'idéal $I = \bigcup_{i \in \mathbb{N}} I_i$ est principal et il existe $x \in R$ tel que $I = Rx$. Ainsi il existe $n_0 \in \mathbb{N}$ tel que $x \in I_{n_0}$ et donc $I_n = I_{n_0} = I$ pour tout $n \geq n_0$. □

Exemple. L'anneau \mathbb{Z} est noethérien.

2.6.8 Corollaire. *Tout module de génération finie sur un anneau principal à gauche est noethérien. En particulier, les groupes abéliens de type fini sont noethériens.*

Remarque. En fait, comme pour les groupes abéliens de type fini, il y a un résultat plus général qui explicite la structure de tels modules. Si M est un module de génération finie sur un anneau principal R , alors on peut montrer qu'on a un isomorphisme

$$M \cong R^n \oplus T$$

pour un certain $n \in \mathbb{N}$ et où T est un R -module dit *de torsion*, i.e. pour tout $m \in T$ il existe $r \neq 0 \in R$ tel que $rm = 0$.

2.6.9 Lemme. Soit M un module noethérien et $f : M \rightarrow M$ un endomorphisme surjectif. Alors f est un isomorphisme.

Démonstration. Considérons la suite croissante $\ker f \subset \ker f^2 \subset \ker f^3 \subset \dots$ de sous-modules de M . Cette suite stabilise et il existe $n_0 \in \mathbb{N}$ tel que $\ker f^n = \ker f^{n_0}$ pour tout $n \geq n_0$. Soit $m \in \ker f$. Il existe $m' \in M$ tel que $m = f^{n_0}m'$ par surjectivité de f^{n_0} . On a $0 = f(m) = f^{n_0+1}m'$, i.e. $m' \in \ker f^{n_0+1} = \ker f^{n_0}$, et $m = f^{n_0}m' = 0$. Ainsi $\ker f$ est trivial. \square

2.6.10 Théorème. Soit R un anneau principal ou noethérien à gauche. Alors R a la propriété du rang unique.

Démonstration. Supposons que $R^m \cong R^n$ avec $n \geq m$. On a une suite exacte courte évidente :

$$R^{n-m} \hookrightarrow R^n \xrightarrow{f} R^n$$

où f étend l'isomorphisme ci-dessus. Par le lemme, f est un isomorphisme. Ainsi R^{n-m} est trivial, i.e. $n = m$. \square

Remarque. Les résultats qui viennent d'être établis restent vrais si l'on supprime chaque occurrence des termes "à gauche".

Remarques. Voici quelques résultats intéressants que nous donnons sans preuve :

1. (Hilbert) Si R un anneau noethérien à gauche, alors l'anneau des polynômes à n indéterminées $R[X_1, \dots, X_n]$ est noethérien à gauche, pour tout $n \geq 1$.
2. (Hopkins-Levitzki) Un module est dit **artinien** si, comme module sur lui-même, il satisfait la *condition de chaîne descendante* qu'on imagine. Un anneau est artinien à gauche si, comme module sur lui-même, il est artinien. Si R est un anneau artinien à gauche, alors R est noethérien à gauche. Attention, ce n'est pas vrai pour les modules. Par exemple, \mathbb{Q}/\mathbb{Z} est un \mathbb{Z} -module artinien qui n'est pas noethérien. En plus la réciproque est fausse. L'anneau $\begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Z} \end{pmatrix}$ est noethérien à gauche, mais pas artinien.
3. (Artin-Wedderburn) Tout anneau simple artinien à gauche est isomorphe à un anneau de matrices sur un anneau de division.
4. Il existe des anneaux qui sont noethérien (resp. artiniens) à gauche mais pas à droite, et vice-versa. Par exemple, $\begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Z} \end{pmatrix}$ est noethérien à gauche, mais pas à droite. L'anneau $\begin{pmatrix} \mathbb{R} & \mathbb{R} \\ 0 & \mathbb{Q} \end{pmatrix}$ est artinien à gauche, mais pas à droite.

3 Catégories de modules

10.04.2006

3.1 Catégories, foncteurs, transformations naturelles et adjoints

La première tentative de fondement des mathématiques est due à Georg Cantor à la fin du 19^e siècle. Il développa une théorie naïve des ensembles qui permit aux mathématiciens de travailler avec des ensembles infinis. Cantor n'axiomatisa pas sa théorie. C'est Gottlob Frege qui le premier dressa une liste d'axiomes pour une théorie des ensembles qui permettait d'interpréter la théorie naïve de Cantor. En 1901, Bertrand Russell découvrit son fameux paradoxe : d'après la théorie de Frege, $R = \{X \mid X \notin X\}$ est un ensemble bien défini, cependant les deux assertions " $R \in R$ " et " $R \notin R$ " impliquent chacune une contradiction et, si l'on croit au principe du tiers exclu, R ne peut pas être un ensemble. Russell écrivit à Frege en juin 1902 pour lui parler de sa découverte. A ce moment, Frege écrivait le second volume de son "Grundgesetze" et il dut y ajouter un appendice en réponse à ce paradoxe. Frege ne parvint jamais à résoudre ce problème et l'on pense qu'il abandonna son travail sur la logique pour cette raison. Russell, en collaboration avec Alfred North Whitehead, entreprit de terminer la tâche de Frege en utilisant une version restreinte de la théorie de ensembles qui aurait permis d'éviter le fameux paradoxe tout en produisant de l'arithmétique. Kurt Gödel prouva plus tard que cette entreprise était impossible.

En 1908, Ernst Zermelo travaillait sur sa version d'une théorie des ensembles basée sur sept axiomes. Il découvrit également le paradoxe de Russell, mais pensant qu'il était trop évident, ne publia jamais quoi que ce soit à ce sujet. Le système de Zermelo évitait le problème grâce à son axiome de séparation. Cet axiome empêche également de concevoir l'ensemble de tous les ensembles.

La théorie des ensembles de Zermelo a été modifiée indépendamment par Abraham Fraenkel et par Thoralf Skolem en 1922. Ils remplacèrent la vague notion de "propriété" de la théorie de Zermelo par une propriété qui peut être formulée par la logique du premier ordre. Les axiomes qui résultent de leur travail (axiome de régularité et schéma d'axiome de remplacement) font aujourd'hui partie intégrante des axiomes standards de la théorie des ensembles, nommée "théorie des ensembles de Zermelo-Fraenkel" (ZF ou ZFC si l'on accepte l'axiome du choix). A noter que l'histoire est ici injuste, puisque c'est la version de Skolem qui a finalement été retenue et que son nom ne figure pas dans la dénomination de cette théorie. A noter encore que ZF et ZFC contiennent une infinité d'axiomes.

Il existe encore bien d'autres systèmes d'axiomes pour la théorie des ensembles, par exemple : von Neumann-Bernays-Gödel (NBG), Kripke-Platek (KP), Kripke-Platek avec "urelements" (PKU), Morse-Kelley, New Foundations et théorie positive des ensembles.

La théorie des ensembles que nous allons utiliser pour définir les catégories et les notions qui s'y rapportent est celle de von Neumann-Bernays-Gödel (NBG). Elle a l'avantage sur ZFC de ne contenir qu'un nombre fini d'axiomes, de fournir les mêmes résultats que ZFC et par exemple de permettre de considérer formellement la collection de tous les ensembles à l'aide de la notion de "classe". Formulée tout d'abord par John von Neumann dans les années 1920, cette théorie a été modifiée par Paul Bernays en 1937 et finalement simplifiée par Kurt Gödel en 1940.

Nous n'allons pas étudier cette théorie, mais juste indiquer que la notion d'ensemble est dérivée de celle de classe. En fait, un ensemble est défini comme un élément d'une classe et l'on peut considérer la classe de tous les ensembles. Notons toutefois que les axiomes NBG ne permettent pas de considérer la classe de toutes les classes, ni l'ensemble de tous les ensembles.

3.1.1 Définition. Une **catégorie** \mathcal{C} est une classe munie d'une application de classes \circ , appelée **composition**, définie d'une sous-classe de $\mathcal{C} \times \mathcal{C}$ dans \mathcal{C} et vérifiant les propriétés suivantes :

1. si $h \circ (g \circ f)$ ou $(h \circ g) \circ f$ est défini pour $f, g, h \in \mathcal{C}$, alors l'autre est défini et ils sont égaux,
2. pour tout $f \in \mathcal{C}$ il existe $e_L, e_R \in \mathcal{C}$ tels que $f \circ e_R, e_L \circ f$ soient définis et $f = f \circ e_R = e_L \circ f$; un élément $e \in \mathcal{C}$ tel que $e \circ f = f$ et $f \circ e = f$ pour tout f pour lequel la composition est définie, est appelé une **identité**,
3. si $g \circ e$ et $e \circ f$ sont définis avec e une identité, alors $g \circ f$ est défini.

Si la catégorie \mathcal{C} est un ensemble, elle est dite **petite**. La classe des **objets** de la catégorie \mathcal{C} est la classe $\text{ob } \mathcal{C}$ constituée de toutes les identités. Soit $f \in \mathcal{C}$. Le **domaine** de f est l'unique objet (i.e. identité) $\text{dom}(f) \in \text{ob } \mathcal{C}$ tel que $f \circ \text{dom}(f) = f$. Le **codomaine** de f est l'unique objet $\text{cod}(f) \in \text{ob } \mathcal{C}$ tel que $\text{cod}(f) \circ f = f$. Pour tout $A, B \in \text{ob } \mathcal{C}$ on définit la classe des **morphismes** de domaine A et de codomaine B comme la classe

$$\text{Hom}_{\mathcal{C}}(A, B) = \{f \in \mathcal{C} \mid \text{dom}(f) = A \text{ et } \text{cod}(f) = B\}.$$

On note très souvent $f : A \rightarrow B$ un morphisme de $\text{Hom}_{\mathcal{C}}(A, B)$. La catégorie \mathcal{C} est dite **localement petite** si $\text{Hom}_{\mathcal{C}}(A, B)$ est un ensemble pour tout couple d'objets (A, B) .

Convention. Sauf mention du contraire, les catégories que nous considérerons seront localement petites.

Remarques.

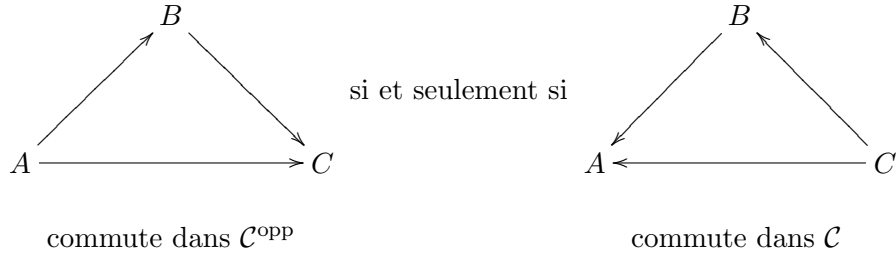
1. Le domaine d'un morphisme $f \in \mathcal{C}$ est bien unique : supposons que l'identité e soit telle que $f \circ e = f$, alors $f \circ e = (f \circ \text{dom}(f)) \circ e = f \circ (\text{dom}(f) \circ e)$, de sorte que $\text{dom}(f) \circ e$ est défini et $\text{dom}(f) = e$ puisque $\text{dom}(f)$ et e sont des identités. Idem pour le codomaine de f .
2. Le morphisme $g \circ f$ est défini pour $f, g \in \mathcal{C}$ si et seulement si $\text{cod}(f) = \text{dom}(g)$. De plus, $\text{dom}(g \circ f) = \text{dom}(f)$ et $\text{cod}(g \circ f) = \text{cod}(g)$. En résumé, pour tout $A, B, C \in \text{ob } \mathcal{C}$ on a une fonction de composition $\text{Hom}_{\mathcal{C}}(B, C) \times \text{Hom}_{\mathcal{C}}(A, B) \rightarrow \text{Hom}_{\mathcal{C}}(A, C)$ définie par $(g, f) \mapsto g \circ f$.
3. Pour tout $f \in \text{Hom}_{\mathcal{C}}(A, B)$, $g \in \text{Hom}_{\mathcal{C}}(B, C)$ et $h \in \text{Hom}_{\mathcal{C}}(C, D)$ on a $h \circ (g \circ f) = (h \circ g) \circ f$.
4. Pour tout $A \in \text{ob } \mathcal{C}$ on a clairement $A \in \text{Hom}_{\mathcal{C}}(A, A)$. On note souvent id_A ou 1_A cet élément distingué que l'on appelle l'**identité** sur A . Avec cette notation on a $f \circ \text{id}_A = f = \text{id}_B \circ f$ pour tout $f \in \text{Hom}_{\mathcal{C}}(A, B)$.

Exemples.

1. La catégorie **Set** des ensembles est la classe de toutes les applications d'ensembles munie de la composition d'applications. Cette catégorie n'est pas petite (puisque la classe de tous les ensembles n'est pas un ensemble), mais elle est localement petite (on peut considérer l'ensemble de toutes les applications entre deux ensembles donnés).
2. La catégorie **Top** des espaces topologiques est la classe de toutes les applications continues entre espaces topologiques.
3. La catégorie **Grp** des groupes est la classe de tous les homomorphismes de groupes.
4. La catégorie **Ring** des anneaux est la classe de tous les homomorphismes d'anneaux.
5. Pour un anneau donné R , la catégorie **$R\text{-Mod}$** (resp. **$\text{Mod-}R$**) des R -modules à gauche (resp. à droite) est la classe de tous les homomorphismes de R -modules à gauche (resp. à droite).
6. Pour un corps donné \mathbb{K} , la catégorie **$\mathbb{K}\text{-Vect}$** des espaces vectoriels sur le corps \mathbb{K} est la classe de toutes les applications linéaires.
7. Si \mathcal{C} et \mathcal{D} sont des catégories, alors la classe produit $\mathcal{C} \times \mathcal{D}$, munie de la composition évidente, est une catégorie.

3.1.2 Définition. Soit \mathcal{C} une catégorie avec la composition donnée par \circ . La catégorie **duale** \mathcal{C}^{opp} de \mathcal{C} est donnée par la classe \mathcal{C} munie de la composition \circ' définie par $g \circ' f = f \circ g$. On a ainsi $\text{ob } \mathcal{C}^{\text{opp}} = \text{ob } \mathcal{C}$, $\text{dom}_{\mathcal{C}^{\text{opp}}}(f) = \text{cod}_{\mathcal{C}}(f)$, $\text{cod}_{\mathcal{C}^{\text{opp}}}(f) = \text{dom}_{\mathcal{C}}(f)$ et $\text{Hom}_{\mathcal{C}^{\text{opp}}}(A, B) = \text{Hom}_{\mathcal{C}}(B, A)$ pour tout $A, B \in \text{ob } \mathcal{C}$.

Exemple.



3.1.3 Définition. Un morphisme $f : A \rightarrow B$ d'une catégorie \mathcal{C} est un **monomorphisme** (resp. **épimorphisme**) s'il est simplifiable à gauche (resp. à droite), et on note souvent $A \rightarrowtail B$ (resp. $A \twoheadrightarrow B$). C'est un **isomorphisme** s'il existe un morphisme $g : B \rightarrow A$ tel que $g \circ f = \text{id}_A$ et $f \circ g = \text{id}_B$.

Exemples.


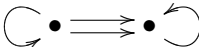
1. Dans la catégorie des **R -Mod**, les monomorphismes sont les homomorphismes injectifs, les épimorphismes sont les homomorphismes surjectifs et les isomorphismes sont les homomorphismes injectifs et bijectifs.
2. Dans la catégorie **Ring**, les monomorphismes sont les homomorphismes injectifs, les homomorphismes surjectifs sont des épimorphismes, mais les épimorphismes ne sont pas tous surjectifs.
3. Un monomorphisme (resp. épimorphisme, isomorphisme) dans \mathcal{C}^{opp} est un épimorphisme (resp. monomorphisme, isomorphisme) dans \mathcal{C} .

3.1.4 Définition. Soit \mathcal{C} une catégorie. S'il existe un objet $0 \in \text{ob } \mathcal{C}$ tel que pour tout $A \in \text{ob } \mathcal{C}$ les ensembles $\text{Hom}_{\mathcal{C}}(A, 0)$ et $\text{Hom}_{\mathcal{C}}(0, A)$ sont des singletons, alors 0 est appelé un **objet nul**. Dans ce cas, on dit que \mathcal{C} est une catégorie *avec objet nul* et pour tout $A, B \in \text{ob } \mathcal{C}$ on a le morphisme distingué $0 : A \rightarrow 0 \rightarrow B$ qu'on appelle le **morphisme nul**.

Remarques.

1. Un objet nul est clairement unique à isomorphisme près [on a forcément $0 \rightarrow 0' \rightarrow 0 = \text{id}_0$ et $0' \rightarrow 0 \rightarrow 0' = \text{id}_{0'}$, i.e. $0 \cong 0'$].
2. Si \mathcal{C} est une catégorie avec objet nul, alors \mathcal{C}^{opp} est une catégorie avec objet nul.

Exemples.

1. N'importe quel singleton est un objet nul de **Grp** ou **R -Mod**.
2. Les catégories **Set** et **Top** n'ont pas d'objet nul [$\text{Hom}(X, \emptyset) = \emptyset$].
3. Les catégories  et  n'ont pas d'objet nul.

Définition. Soit \mathcal{C} une catégorie avec objet nul. Un **noyau** d'un morphisme $f \in \text{Hom}_{\mathcal{C}}(A, B)$ est la donnée d'un objet $\ker f$ et d'un morphisme $k \in \text{Hom}_{\mathcal{C}}(\ker f, A)$ tels que $f \circ k = 0$ et qui vérifient la propriété universelle suivante : pour tout morphisme $k' \in \text{Hom}_{\mathcal{C}}(K, A)$ tel que $f \circ k' = 0$ il existe un unique morphisme $q \in \text{Hom}_{\mathcal{C}}(K, \ker f)$ satisfaisant $k' = k \circ q$, i.e. tel que le diagramme suivant commute :

$$\begin{array}{ccccc} & K & & & \\ & \searrow 0 & & & \\ q \downarrow & & k' \searrow & & \\ \ker f & \xrightarrow{k} & A & \xrightarrow{f} & B. \end{array}$$

Remarques. 1. L'objet $\ker f$ est unique à (un seul) isomorphisme près.

2. On définit le **conoyau** comme le noyau dans la catégorie duale.

Exemples. 1. Dans **Grp**, **Ring** et **R-Mod**, le noyau d'un homomorphisme avec l'inclusion canonique est un noyau catégoriel.

2. On ne peut pas parler de noyau dans la catégorie **Set** qui n'a pas d'objet nul.

3.1.5 Définition. Soient \mathcal{C} et \mathcal{D} deux catégories. Un **foncteur covariant** (resp. **contravariant**) est une application de classes $F : \mathcal{C} \rightarrow \mathcal{D}$ qui vérifie les propriétés suivantes :

1. pour tout $A \in \text{ob } \mathcal{C}$ on a $F(A) \in \text{ob } \mathcal{D}$ (en d'autres termes, $F(\text{id}_A) = \text{id}_{F(A)}$),
2. pour tout $f \in \text{Hom}_{\mathcal{C}}(A, B)$ et $g \in \text{Hom}_{\mathcal{C}}(B, C)$ on a $F(g \circ f) = F(g) \circ F(f)$ (resp. $F(g \circ f) = F(f) \circ F(g)$).

Remarques. 1. Un foncteur contravariant de \mathcal{C} dans \mathcal{D} est un foncteur covariant de \mathcal{C}^{opp} dans \mathcal{D} . On écrira donc souvent *foncteur* à la place de *foncteur covariant*.

2. On définit très souvent les foncteurs sur les objets de la catégorie, sans préciser leur effet sur les autres morphismes.

Exemples. 1. L'application de classes $1_{\mathcal{C}} : \mathcal{C} \rightarrow \mathcal{C}$ définie par $1_{\mathcal{C}}(f) = f$ pour tout $f \in \mathcal{C}$ est un foncteur ; on l'appelle le **foncteur identité**.

2. L'application de classes $\text{Hom}_{\mathcal{C}}(A, -) : \mathcal{C} \rightarrow \mathbf{Set}$ définie par $\text{Hom}_{\mathcal{C}}(A, -)(B) = \text{Hom}_{\mathcal{C}}(A, B)$ pour tout $B \in \text{ob } \mathcal{C}$ et $\text{Hom}_{\mathcal{C}}(A, -)(g : B \rightarrow B') : \text{Hom}_{\mathcal{C}}(A, B) \rightarrow \text{Hom}_{\mathcal{C}}(A, B')$, $f \mapsto g \circ f$ pour tout $f \in \text{Hom}_{\mathcal{C}}(A, B)$ et $g \in \text{Hom}_{\mathcal{C}}(B, B')$, est un foncteur (covariant).

3. L'application de classes $\text{Hom}_{\mathcal{C}}(-, B) : \mathcal{C} \rightarrow \mathbf{Set}$ définie par $\text{Hom}_{\mathcal{C}}(-, B)(A) = \text{Hom}_{\mathcal{C}}(A, B)$ pour tout $A \in \text{ob } \mathcal{C}$ et $\text{Hom}_{\mathcal{C}}(-, B)(g : A \rightarrow A') : \text{Hom}_{\mathcal{C}}(A', B) \rightarrow \text{Hom}_{\mathcal{C}}(A, B)$, $f \mapsto f \circ g$ pour tout $f \in \text{Hom}_{\mathcal{C}}(A', B)$ et $g \in \text{Hom}_{\mathcal{C}}(A, A')$, est un foncteur contravariant.

4. L'application de classes $\text{Hom}_{\mathcal{C}}(-, -) : \mathcal{C}^{\text{opp}} \times \mathcal{C} \rightarrow \mathbf{Set}$ définie par $\text{Hom}_{\mathcal{C}}(-, -)(A, B) = \text{Hom}_{\mathcal{C}}(A, B)$ pour tout $A, B \in \text{ob } \mathcal{C}$ et $\text{Hom}_{\mathcal{C}}(-, -)(f : A \rightarrow A', g : B \rightarrow B') : \text{Hom}_{\mathcal{C}}(A', B) \rightarrow \text{Hom}_{\mathcal{C}}(A, B')$, $h \mapsto g \circ h \circ f$ pour tout $f \in \text{Hom}_{\mathcal{C}}(A, A')$, $g \in \text{Hom}_{\mathcal{C}}(B, B')$ et $h \in \text{Hom}_{\mathcal{C}}(A', B)$, est un foncteur.

5. L'application de classes $\mathcal{F} : \mathbf{Set} \rightarrow \mathbf{R-Mod}$ qui associe à tout ensemble S le R -module à gauche libre sur S est un foncteur ; on l'appelle le **foncteur libre**.

6. L'application de classes $U : \mathbf{R-Mod} \rightarrow \mathbf{Set}$ qui associe à tout R -module à gauche son ensemble sous-jacent est un foncteur ; on l'appelle le **foncteur d'oubli**.

7. L'application de classes $(-)^{**} : \mathbb{K}\text{-Vect} \rightarrow \mathbb{K}\text{-Vect}$ qui associe à tout espace vectoriel sur \mathbb{K} son double dual est un foncteur.

3.1.6 Définition. Soient $F, G : \mathcal{C} \rightarrow \mathcal{D}$ deux foncteurs. Une **transformation naturelle** entre les foncteurs F et G est une application de classes $\eta : \text{ob } \mathcal{C} \rightarrow \mathcal{D}$, $A \mapsto \eta_A \in \text{Hom}_{\mathcal{D}}(F(A), G(A))$ telle que pour tout $f \in \text{Hom}_{\mathcal{C}}(A, B)$ on ait le diagramme commutatif suivant :

$$\begin{array}{ccc} F(A) & \xrightarrow{\eta_A} & G(A) \\ F(f) \downarrow & & \downarrow G(f) \\ F(B) & \xrightarrow{\eta_B} & G(B). \end{array}$$

La transformation naturelle η est une **équivalence naturelle** si $\eta_A : F(A) \rightarrow G(A)$ est un isomorphisme pour tout $A \in \text{ob } \mathcal{C}$.

- Exemples.**
1. L'application de classes $\text{ob } \mathcal{C} \rightarrow \mathcal{C}$ définie par $A \mapsto \text{id}_A$ est une équivalence naturelle entre les foncteurs identité.
 2. Soit $F : \mathcal{C} \rightarrow \mathcal{D}$ un foncteur. L'application de classes $1_F : \text{ob } \mathcal{C} \rightarrow \mathcal{D}$ définie par $A \mapsto \text{id}_{F(A)}$ est une équivalence naturelle entre le foncteur F et lui-même.
 3. L'application de classes $\eta : \text{ob } \mathbb{K}\text{-}\mathbf{Vect} \rightarrow \mathbb{K}\text{-}\mathbf{Vect}$ définie par $V \mapsto \eta_V : V \rightarrow V^{**}$ est une transformation naturelle entre le foncteur identité et le double dual.

3.1.7 Définition. Soient $F : \mathcal{C} \rightarrow \mathcal{D}$ et $G : \mathcal{D} \rightarrow \mathcal{C}$ deux foncteurs. On dit que F est **adjoint à gauche** de G , et on note $F \dashv G$, s'il existe $\varphi : \text{ob}(\mathcal{C}^{\text{opp}} \times \mathcal{D}) \rightarrow \mathbf{Set}$ une équivalence naturelle entre les foncteurs $\text{Hom}_{\mathcal{D}}(F(-), -), \text{Hom}_{\mathcal{C}}(-, G(-)) : \mathcal{C}^{\text{opp}} \times \mathcal{D} \rightarrow \mathbf{Set}$, i.e. pour tout $A \in \text{ob } \mathcal{C}$ et $B \in \text{ob } \mathcal{D}$ une bijection $\varphi_{A,B} : \text{Hom}_{\mathcal{D}}(F(A), B) \leftrightarrow \text{Hom}_{\mathcal{C}}(A, G(B))$ qui fait commuter le diagramme suivant pour tout $f \in \text{Hom}_{\mathcal{C}^{\text{opp}}}(A, A')$ et $g \in \text{Hom}_{\mathcal{D}}(B, B')$:

$$\begin{array}{ccc} \text{Hom}_{\mathcal{D}}(F(A), B) & \xleftarrow{\varphi_{A,B}} & \text{Hom}_{\mathcal{C}}(A, G(B)) \\ \text{Hom}_{\mathcal{D}}(F(f), g) \downarrow & & \downarrow \text{Hom}_{\mathcal{C}}(f, G(g)) \\ \text{Hom}_{\mathcal{D}}(F(A'), B') & \xleftarrow{\varphi_{A',B'}} & \text{Hom}_{\mathcal{C}}(A', G(B')). \end{array}$$

- Remarques.**
1. Il est facile de voir que $\text{Hom}_{\mathcal{C}}(-, G(-)), \text{Hom}_{\mathcal{D}}(F(-), -) : \mathcal{C}^{\text{opp}} \times \mathcal{D} \rightarrow \mathbf{Set}$ sont des foncteurs.
 2. On dit aussi que G est adjoint à droite de F , et on note $G \vdash F$.
 3. Pour tout $A \in \text{ob } \mathcal{C}$ on a la bijection $\varphi_{A, F(A)} : \text{Hom}_{\mathcal{D}}(F(A), F(A)) \leftrightarrow \text{Hom}_{\mathcal{C}}(A, GF(A))$. Si l'on pose $\eta_A = \varphi_{A, F(A)}(\text{id}_{F(A)}) : A \rightarrow GF(A)$, on obtient en fait une transformation naturelle $\eta : 1_{\mathcal{C}} \rightarrow GF$ que l'on appelle l'unité de l'adjonction $F \dashv G$.
 4. De façon similaire, pour tout $B \in \text{ob } \mathcal{D}$ on peut poser $\epsilon_B = (\varphi_{G(B), B})^{-1}(\text{id}_{G(B)}) : FG(B) \rightarrow B$ et on obtient une transformation naturelle $\epsilon : FG \rightarrow 1_{\mathcal{D}}$ que l'on appelle la counité de l'adjonction $F \dashv G$.
 5. On peut vérifier que la transformation naturelle $\epsilon F \circ F \eta$ est 1_F . De même, $G \epsilon \circ \eta G = 1_G$.
 6. La donnée de transformations naturelles $\eta : 1_{\mathcal{C}} \rightarrow GF$ et $\epsilon : FG \rightarrow 1_{\mathcal{D}}$ qui satisfont les identités $\epsilon F \circ F \eta = 1_F$ et $G \epsilon \circ \eta G = 1_G$ donne lieu à une adjonction $F \dashv G$.

Exemple. Le foncteur libre $\mathcal{F} : \mathbf{Set} \rightarrow R\text{-}\mathbf{Mod}$ est adjoint à gauche du foncteur d'oubli $U : R\text{-}\mathbf{Mod} \rightarrow \mathbf{Set}$ via l'équivalence naturelle $\varphi_{S,M} : \text{Hom}_R(\mathcal{F}(S), M) \leftrightarrow \text{Hom}_{\mathbf{Set}}(S, U(M))$, puisqu'à toute application $f : S \rightarrow M$ correspond un unique homomorphisme de R -modules $\tilde{f} : \bigoplus_S R \rightarrow M$ qui étende f naturellement.

3.1.8 Théorème. Soit $F \dashv G$ une paire de foncteurs adjoints entres catégories avec objet nul. Si F et G préservent l'objet nul, alors F préserve les conoyaux et G préserve les noyaux.

Démonstration. Considérons les foncteurs $F : \mathcal{C} \rightarrow \mathcal{D}$ et $G : \mathcal{D} \rightarrow \mathcal{C}$. Soit $f : A \rightarrow B$ un morphisme de \mathcal{D} et soit $k : \ker f \rightarrow A$ un noyau. Montrons que $Gk : G\ker f \rightarrow GA$ est un noyau de $Gf : GA \rightarrow GB$ (on procède de façon duale pour montrer que F préserve les conoyaux).

1. Montrons que $Gf \circ Gk = 0$. On a $Gf \circ Gk = G(f \circ k) = G(0) = 0$ puisque G préserve le morphisme nul (il préserve l'objet nul).
2. Soit $\tilde{k}' : K \rightarrow GA$ tel que $Gf \circ \tilde{k}' = 0$. Montrons qu'il existe $\tilde{q} : K \rightarrow G\ker f$ tel que $Gk \circ \tilde{q} = \tilde{k}'$. On a la bijection $\varphi : \text{Hom}_{\mathcal{D}}(FK, A) \leftrightarrow \text{Hom}_{\mathcal{C}}(K, GA)$. Posons $k' = \varphi^{-1}(\tilde{k}') \in \text{Hom}_{\mathcal{D}}(FK, A)$. On a $f \circ k' = f \circ \varphi^{-1}(\tilde{k}') = \varphi^{-1}(Gf \circ \tilde{k}') = \varphi^{-1}(0)$ par commutativité du diagramme suivant :

$$\begin{array}{ccc} \text{Hom}_{\mathcal{D}}(FK, A) & \xleftarrow{\varphi} & \text{Hom}_{\mathcal{C}}(K, GA) \\ \text{Hom}_{\mathcal{D}}(F(\text{id}_K), f) \downarrow & & \downarrow \text{Hom}_{\mathcal{C}}(\text{id}_K, Gf) \\ \text{Hom}_{\mathcal{D}}(FK, B) & \xleftarrow{\varphi} & \text{Hom}_{\mathcal{C}}(K, GB). \end{array}$$

On montre facilement que $\varphi(FK \rightarrow 0 \rightarrow B) = K \rightarrow 0 \rightarrow GB$, i.e. que $\varphi^{-1}(0) = 0$. Il existe donc un unique $q : FK \rightarrow \ker f$ tel que $k \circ q = k'$. Posons $\tilde{q} = \varphi(q)$ de sorte que $Gk \circ \tilde{q} = Gk \circ \varphi(q) = \varphi(k \circ q) = \varphi(k') = \varphi(\varphi^{-1}(\tilde{k}')) = \tilde{k}'$ par commutativité du diagramme suivant :

$$\begin{array}{ccc} \text{Hom}_{\mathcal{D}}(FK, \ker f) & \xleftarrow{\varphi} & \text{Hom}_{\mathcal{C}}(K, G\ker f) \\ \text{Hom}_{\mathcal{D}}(F(\text{id}_K), k) \downarrow & & \downarrow \text{Hom}_{\mathcal{C}}(\text{id}_K, Gk) \\ \text{Hom}_{\mathcal{D}}(FK, A) & \xleftarrow{\varphi} & \text{Hom}_{\mathcal{C}}(K, GA). \end{array}$$

3. Montrons que \tilde{q} est unique. Soit $\bar{q} : K \rightarrow G\ker f$ tel que $Gk \circ \bar{q} = \tilde{k}'$. On a donc $k \circ \varphi^{-1}(\bar{q}) = \varphi^{-1}(Gk \circ \bar{q}) = \varphi^{-1}(\tilde{k}') = k'$ par commutativité du diagramme ci-dessus. Ainsi $\varphi^{-1}(\bar{q}) = q$ par la propriété universelle du noyau et $\bar{q} = \varphi(q) = \tilde{q}$.

□

3.1.9 Théorème. Soit $F \dashv G$ une paire de foncteurs adjoints. Alors F préserve les coproduits (i.e. les produits dans la catégorie opposée) et G préserve les produits.

Démonstration. Cf. exercices.

□

3.2 Catégories de modules : les foncteurs Hom et \otimes

3.2.1 Définition. Soient R et S deux anneaux. Un S - R -**bimodule** M est un groupe abélien qui possède une structure de S -module à gauche et une structure de R -module à droite dont les actions commutent, i.e. telles que $(sm)r = s(mr)$ pour tout $m \in M$, $s \in S$ et $r \in R$.

Remarques. 1. Un R -module à droite est un \mathbb{Z} - R -bimodule, de même qu'un R -module à gauche est un R - \mathbb{Z} -bimodule.

2. Soient R, S deux anneaux, A un S - R -bimodule et C un S -module à gauche. On peut munir $\text{Hom}_S(A, C)$ d'une structure de R -module à gauche grâce à la structure de R -module à droite de A en posant $(rf)(a) = f(ar)$ pour tout $f \in \text{Hom}_S(A, C)$, $r \in R$ et $a \in A$.

3.2.2 Définition. Soient R un anneau, A un R -module à droite et B un R -module à gauche. Le **produit tensoriel** de A et B sur R est le groupe abélien $A \otimes_R B$ obtenu comme quotient du groupe libre-abélien (i.e. du \mathbb{Z} -module libre) sur l'ensemble des symboles $\{a \otimes b \mid a \in A \text{ et } b \in B\}$ par le sous-groupe engendré par

$$\begin{aligned} (a_1 + a_2) \otimes b - (a_1 \otimes b + a_2 \otimes b), & \quad a_1, a_2 \in A, b \in B, \\ a \otimes (b_1 + b_2) - (a \otimes b_1 + a \otimes b_2), & \quad a \in A, b_1, b_2 \in B, \\ ar \otimes b - a \otimes rb, & \quad a \in A, b \in B \text{ et } r \in R. \end{aligned}$$

Remarques. 1. Pour tout $a \in A$ et $b \in B$, on notera l'image canonique du symbole $a \otimes b$ dans le produit tensoriel $A \otimes_R B$ par le même symbole $a \otimes b$.

2. On notera $A \otimes B$ au lieu de $A \otimes_{\mathbb{Z}} B$.

3. Le produit tensoriel $A \otimes_R B$ est un \mathbb{Z} -module par définition. Si R est un anneau commutatif, alors $A \otimes_R B$ est aussi un R -module via $r(a \otimes b) = ar \otimes b = a \otimes rb$ pour tout $a \in A$, $b \in B$ et $r \in R$. Si A est un S - R -bimodule pour S un anneau, alors $A \otimes_R B$ est un S -module à gauche via $s(a \otimes b) = sa \otimes b$ pour tout $a \in A$, $b \in B$ et $s \in S$. De même, si B est un R - T -bimodule pour T un anneau, alors $A \otimes_R B$ est un T -module à droite via $(a \otimes b)t = a \otimes bt$ pour tout $a \in A$, $b \in B$ et $t \in T$.

Exemples. 1. On a $A \otimes_R R \xrightarrow{\cong} A$ via l'homomorphisme de groupes $a \otimes r \mapsto ar$ [le noyau de cet homomorphisme est trivial puisque $ar = 0$ implique $a \otimes r = ar \otimes 1 = 0 \otimes 1 = 0 \otimes 0$; la surjectivité est claire puisque $a \otimes 1 \mapsto a$]. De même on a $R \otimes_R B \xrightarrow{\cong} B$ via $r \otimes b \mapsto rb$.

2. On a $\mathbb{Z}/n \otimes \mathbb{Q} = 0$ puisque $[a] \otimes \frac{p}{q} = [a] \otimes \frac{np}{nq} = [a]n \otimes \frac{p}{nq} = 0$.

3. Soit B un R -module à gauche. L'application de classes $- \otimes_R B : \mathbf{Mod}\text{-}R \rightarrow \mathbf{Ab}$ définie par $(f : A \rightarrow A') \mapsto (f_* : A \otimes_R B \rightarrow A' \otimes_R B)$ et $f_*(a \otimes b) = f(a) \otimes b$ pour tout $a \in A$ et $b \in B$ est un foncteur covariant.
4. Soit A un S - R -bimodule. L'application de classes $A \otimes_R - : R\text{-}\mathbf{Mod} \rightarrow S\text{-}\mathbf{Mod}$ définie par $(g : B \rightarrow B') \mapsto (g_* : A \otimes_R B \rightarrow A \otimes_R B')$ et $g_*(a \otimes b) = a \otimes g(b)$ pour tout $a \in A$ et $b \in B$ est un foncteur covariant. Le morphisme induit g_* est bien un homomorphisme de S -modules à gauche puisque $g_*(s(a \otimes b)) = g_*(sa \otimes b) = sa \otimes g(b) = s(a \otimes g(b)) = sg_*(a \otimes b)$ pour tout $a \in A$, $b \in B$ et $s \in S$.

3.2.3 Théorème. Soit A un S - R -bimodule. Le foncteur $A \otimes_R - : R\text{-}\mathbf{Mod} \rightarrow S\text{-}\mathbf{Mod}$ est adjoint à gauche du foncteur $\text{Hom}_S(A, -) : S\text{-}\mathbf{Mod} \rightarrow R\text{-}\mathbf{Mod}$.

Démonstration. La structure de S -module à gauche de $A \otimes_R B$ est induite par la structure de S -module à gauche de A . La structure de R -module à gauche de $\text{Hom}_S(A, C)$ est induite par la structure de R -module à droite de A via $(rf)(a) = f(ar)$ pour tout $f \in \text{Hom}_S(A, C)$, $r \in R$ et $a \in A$. Montrons qu'il existe une transformation naturelle φ telle que pour tout R -module à gauche B et pour tout S -module à gauche C on a

$$\varphi_{B,C} : \text{Hom}_S(A \otimes_R B, C) \leftrightarrow \text{Hom}_R(B, \text{Hom}_S(A, C)).$$

Posons $((\varphi(f))(b))(a) = f(a \otimes b)$ pour tout $f : A \otimes_R B \rightarrow C$, $b \in B$ et $a \in A$. Posons encore $(\varphi^{-1}(\psi))(a \otimes b) = (\psi(b))(a)$ pour tout $\psi : B \rightarrow \text{Hom}_S(A, C)$, $a \in A$ et $b \in B$.

- a) On a $(\varphi^{-1}(\varphi(f)))(a \otimes b) = ((\varphi(f))(b))(a) = f(a \otimes b)$, i.e. $\varphi^{-1}\varphi(f) = f$.
- b) On a $((\varphi(\varphi^{-1}(\psi)))(b))(a) = (\varphi^{-1}(\psi))(a \otimes b) = (\psi(b))(a)$, i.e. $\varphi\varphi^{-1}(\psi) = \psi$.
- c) Soient $\beta : B' \rightarrow B$ et $\gamma : C \rightarrow C'$. Montrons que le diagramme suivant commute :

$$\begin{array}{ccc} \text{Hom}_S(A \otimes_R B, C) & \xleftarrow{\varphi_{B,C}} & \text{Hom}_R(B, \text{Hom}_S(A, C)) \\ \text{Hom}_S(\beta_*, \gamma) \downarrow & & \downarrow \text{Hom}_R(\beta, \gamma_*) \\ \text{Hom}_S(A \otimes_R B', C') & \xleftarrow{\varphi_{B',C'}} & \text{Hom}_R(B', \text{Hom}_S(A, C')) \end{array}$$

Soient $f : A \otimes_R B \rightarrow C$, $b' \in B'$ et $a \in A$. On a d'une part

$$\begin{aligned} ((\text{Hom}_R(\beta, \gamma_*) \circ \varphi(f))(b'))(a) &= ((\text{Hom}_R(\beta, \gamma_*)(\varphi(f)))(b'))(a) \\ &= ((\gamma_* \circ \varphi(f) \circ \beta)(b'))(a) \\ &= ((\gamma_* \circ \varphi(f))(\beta(b')))(a) \\ &= \gamma(((\varphi(f))(\beta(b')))(a)) \\ &= \gamma(f(a \otimes \beta(b'))). \end{aligned}$$

D'autre part on a

$$\begin{aligned} ((\varphi \circ \text{Hom}_S(\beta_*, \gamma)(f))(b'))(a) &= (\varphi(\text{Hom}_S(\beta_*, \gamma)(f))(b'))(a) \\ &= (\varphi(\gamma \circ f \circ \beta_*)(b'))(a) \\ &= \gamma \circ f \circ \beta_*(a \otimes b') \\ &= \gamma(f(a \otimes \beta(b'))). \end{aligned}$$

□

3.2.4 Définition. Un foncteur $F : \mathcal{C} \rightarrow \mathcal{D}$ entre deux catégories de modules est **exact à gauche** (resp. **à droite**) si pour toute suite exacte $0 \rightarrow A' \rightarrow A \rightarrow A''$ (resp. $A' \rightarrow A \rightarrow A'' \rightarrow 0$) de \mathcal{C} , la suite induite $0 \rightarrow FA' \rightarrow FA \rightarrow FA''$ (resp. $FA' \rightarrow FA \rightarrow FA'' \rightarrow 0$) est exacte dans \mathcal{D} . Le foncteur F est dit **exact** s'il est exact à gauche et à droite.

3.2.5 Corollaire. Soit A un S - R -bimodule. Le foncteur $A \otimes_R - : R\text{-Mod} \rightarrow S\text{-Mod}$ est exact à droite et préserve les sommes directes. Le foncteur $\text{Hom}_S(A, -) : S\text{-Mod} \rightarrow R\text{-Mod}$ est exact à gauche et préserve les produits.

Démonstration. Posons $F = \text{Hom}_S(A, -)$ et montrons que F est exact à gauche sachant que F préserve les noyaux. Soit $0 \rightarrow B' \xrightarrow{\beta'} B \xrightarrow{\beta} B''$ une suite exacte. On a $B' \cong \ker \beta$ par exactitude. Cette suite induit la suite $0 \rightarrow FB' \xrightarrow{\beta'_*} FB \xrightarrow{\beta_*} FB''$ où $FB' \cong F \ker \beta \cong \ker \beta_*$ puisque F préserve les noyaux. Ainsi FB' s'injecte dans FB via β'_* et $\text{im } \beta'_* \cong FB' \cong \ker \beta_*$. On procède de façon similaire pour montrer que $A \otimes_R -$ est exact à droite. \square

3.2.6 Corollaire. Soit A un R -module à droite. Le foncteur $A \otimes_R - : R\text{-Mod} \rightarrow \mathbf{Ab}$ est exact à droite et préserve les sommes directes.

3.2.7 Corollaire. Soit A un R -module à gauche. Le foncteur $\text{Hom}_R(A, -) : R\text{-Mod} \rightarrow \mathbf{Ab}$ est exact à gauche et préserve les produits.

3.2.8 Définition. Un R -module A est dit **compact** si le foncteur $\text{Hom}_R(A, -)$ préserve les sommes directes.

Exemples. 1. R est compact comme R -module.

2. Un module de génération finie est compact (cf. exercices).

3. Un module projectif est de génération finie si et seulement s'il est compact (cf. exercices).

4. Soit R un anneau. Le R -module $\bigoplus_{\mathbb{N}} R$ n'est pas compact.

3.2.9 Corollaire. Un R -module P est projectif si et seulement si $\text{Hom}_R(P, -)$ est exact.

Démonstration. On a vu que P est un R -module projectif si et seulement si pour tout épimorphisme $\epsilon : B \twoheadrightarrow C$ l'homomorphisme induit $\epsilon_* : \text{Hom}_R(P, B) \rightarrow \text{Hom}_R(P, C)$ est surjectif. \square

3.3 Le théorème d'équivalence de Morita

3.3.1 Définition. Un foncteur $F : \mathcal{C} \rightarrow \mathcal{D}$ est une **équivalence** de catégories s'il existe un foncteur $G : \mathcal{D} \rightarrow \mathcal{C}$ et deux équivalences naturelles $G \circ F \cong 1_{\mathcal{C}}$ et $F \circ G \cong 1_{\mathcal{D}}$. Dans ce cas, on dit que les catégories \mathcal{C} et \mathcal{D} sont **équivalentes** et on note $\mathcal{C} \simeq \mathcal{D}$.

3.3.2 Définition. Soit R un anneau. Un R -module M est un **générateur** de la catégorie de modules $R\text{-Mod}$ si pour tout R -module N il existe un épimorphisme $\bigoplus_I M \twoheadrightarrow N$ pour un certain ensemble I .

Exemple. L'anneau R est un générateur projectif de génération finie de la catégorie $R\text{-Mod}$ puisque tout module est quotient d'un libre.

3.3.3 Définition. Soit $F : \mathcal{C} \rightarrow \mathcal{D}$ une équivalence de catégories. Une propriété \mathcal{P} est dite **catégorielle** lorsque $f \in \mathcal{C}$ satisfait \mathcal{P} si et seulement si $F(f) \in \mathcal{D}$ satisfait \mathcal{P} .

Exemples. Les propriétés "être un monomorphisme", "être un épimorphisme", "être un isomorphisme", "être une suite exacte (courte)", "être projectif", "être un générateur", lorsqu'elles ont un sens dans les catégories considérées, sont catégorielles.

3.3.4 Théorème (Morita, 1958). Soient R et S deux anneaux. Les assertions suivantes sont équivalentes :

1. $R\text{-Mod} \simeq S\text{-Mod}$,
2. il existe un générateur projectif de génération finie P de $S\text{-Mod}$ tel que $\text{End}_S^{\text{opp}}(P) \cong R$ comme anneaux,
3. il existe un S - R -bimodule M tel que le foncteur $M \otimes_R - : R\text{-Mod} \rightarrow S\text{-Mod}$ est une équivalence de catégories.

Démonstration. (3 \implies 1) Clair.

(1 \implies 2) Soit $F : R\text{-Mod} \rightarrow S\text{-Mod}$ une équivalence de catégories avec $G : S\text{-Mod} \rightarrow R\text{-Mod}$ son inverse, i.e. $\epsilon : FG \cong 1_{S\text{-Mod}}$ et $\eta : 1_{R\text{-Mod}} \cong GF$. Le R -module R est un générateur projectif de génération finie, de sorte que le S -module $P = F(R)$ est aussi un générateur projectif de génération finie (cf. exercices). Montrons qu'on a $\text{End}_S(P) = \text{Hom}_S(F(R), F(R)) \cong \text{Hom}_R(R, R) \cong R^{\text{opp}}$ comme anneaux. Soit $f' : F(R) \rightarrow F(R)$. On a le diagramme commutatif suivant :

$$\begin{array}{ccc} GF(R) & \xrightarrow{G(f')} & GF(R) \\ \eta_R \uparrow \cong & & \cong \uparrow \eta_R \\ R & \xrightarrow{f} & R. \end{array}$$

L'application $\varphi : f' \mapsto f$ est une injection puisque si $G(f') = G(f'')$ alors $FG(f') = FG(f'')$ et on a le diagramme commutatif suivant par naturalité de l'équivalence $\epsilon : FG \rightarrow 1_{S\text{-Mod}}$:

$$\begin{array}{ccccc} F(R) & \xleftarrow{\epsilon} & FGF(R) & \xrightarrow{\epsilon} & F(R) \\ f' \downarrow & & FG(f') \downarrow & & \downarrow f'' \\ F(R) & \xleftarrow{\epsilon} & FGF(R) & \xrightarrow{\epsilon} & F(R). \end{array}$$

Considérons l'application $\psi : f \mapsto F(f)$. On a clairement $\varphi\psi(f) = f$. Ainsi $\varphi\psi\varphi(f') = \varphi(f')$, de sorte que $\psi\varphi(f') = f'$. Il est facile de voir que φ est un homomorphisme d'anneaux. On a donc montré que $\text{End}_S(P) \cong \text{End}_R(R)$ comme anneaux. Montrons que $\text{End}_R(R) \cong R^{\text{opp}}$ comme anneaux. L'isomorphisme est donné par $\Phi : f \mapsto f(1_R)$. On a bien $g \circ f(1) = g(f(1)) = g(f(1) \cdot 1) = f(1)g(1)$, i.e. $\Phi(g \circ f) = \Phi(f)\Phi(g) = \Phi(g) \cdot^{\text{opp}} \Phi(f)$.

(2 \implies 3) Soient P un générateur projectif de génération finie de $S\text{-}\mathbf{Mod}$ et $f : R \xrightarrow{\cong} \text{End}_S^{\text{opp}}(P)$ un isomorphisme d'anneaux. On peut ainsi munir P d'une structure de R -module à droite en posant $xr = f(r)(x)$ pour tout $x \in P$ et $r \in R$. On a bien $(xr)r' = f(r')(xr) = f(r')(f(r)(x)) = f(r') \circ f(r)(x) = f(rr')(x) = x(rr')$ pour tout $r, r' \in R$ et $x \in P$. De plus cette action est compatible avec celle de S puisque $s(xr) = s(f(r)(x)) = f(r)(sx) = (sx)r$ (on a utilisé le fait que $f(r)$ est un S -homomorphisme). On peut donc voir P comme un S - R -bimodule. On a donc un couple de foncteurs adjoints donné par $P \otimes_R - \dashv \text{Hom}_S(P, -)$ où $P \otimes_R - : R\text{-}\mathbf{Mod} \rightarrow S\text{-}\mathbf{Mod}$ et $\text{Hom}_S(P, -) : S\text{-}\mathbf{Mod} \rightarrow R\text{-}\mathbf{Mod}$. Montrons que ces deux foncteurs donnent une équivalence de catégories.

1. Montrons que $\text{Hom}_S(P, P \otimes_R -) \cong 1_{R\text{-}\mathbf{Mod}}$. L'unité de l'adjonction (cf. exercices) fournit une transformation naturelle entre le foncteur identité et $\text{Hom}_S(P, P \otimes_R -)$. En fait, on a $\eta_A : A \rightarrow \text{Hom}_S(P, P \otimes_R A)$ tel que $a \mapsto (x \mapsto x \otimes a)$. Il faut voir que c'est un isomorphisme pour avoir une équivalence naturelle. Soit A un R -module. Il existe un épimorphisme $\epsilon : \bigoplus_I R \twoheadrightarrow A$ pour un certain ensemble I . On a le diagramme commutatif suivant :

$$\begin{array}{ccccc}
 \bigoplus_I R & & (r_i)_{i \in I} & \xrightarrow{\quad} & \epsilon((r_i)_{i \in I}) & & A \\
 \downarrow \cong \text{ via } f & & \downarrow & & \downarrow & & \downarrow \eta_A \\
 \bigoplus_I \text{Hom}_S(P, P) & & (f(r_i))_{i \in I} & & & & \\
 \downarrow \cong \text{ P g.f.} & & \downarrow & & & & \\
 \text{Hom}_S(P, \bigoplus_I P) & & x \mapsto (f(r_i)(x))_{i \in I} & & & & \\
 \downarrow \cong & & \downarrow & & & & \\
 \text{Hom}_S(P, \bigoplus_I (P \otimes_R R)) & & x \mapsto (x \otimes r_i)_{i \in I} & & & & \\
 \downarrow \cong & & \downarrow & & & & \\
 \text{Hom}_S(P, P \otimes_R \bigoplus_I R) & & (x \mapsto x \otimes (r_i)_{i \in I}) \mapsto (x \mapsto x \otimes \epsilon((r_i)_{i \in I})) & & & & \text{Hom}_S(P, P \otimes_R A). \\
 & & \searrow \epsilon_{**} & & & &
 \end{array}$$

Considérons le R -module $\ker \epsilon$. Il existe un épimorphisme $\bigoplus_J R \twoheadrightarrow \ker \epsilon$ pour un certain ensemble J . On a donc le diagramme commutatif suivant :

$$\begin{array}{ccccccc}
 \bigoplus_J R & \twoheadrightarrow & \ker \epsilon & \twoheadrightarrow & \bigoplus_I R & \xrightarrow{\quad \epsilon \quad} & A \\
 \downarrow \eta \cong & & & & \downarrow \eta \cong & & \downarrow \eta_A \\
 \text{Hom}_S(P, P \otimes_R \bigoplus_J R) & \twoheadrightarrow & & & \text{Hom}_S(P, P \otimes_R \bigoplus_I R) & \xrightarrow{\quad \epsilon_{**} \quad} & \text{Hom}_S(P, P \otimes_R A).
 \end{array}$$

La ligne du haut est clairement exacte en $\bigoplus_I R$ et en A . La ligne du bas est aussi exacte puisque $P \otimes_R -$ est exact à droite et $\text{Hom}_S(P, -)$ est exact vu que P est projectif. On conclut que η_A est un isomorphisme à l'aide du lemme des deux sur trois.

2. Pour montrer que $P \otimes_R \text{Hom}_S(P, -) \cong 1_{S\text{-}\mathbf{Mod}}$, il suffit de voir que la counité de l'adjonction est en fait une équivalence naturelle. On procède de la même façon que ci-dessus en utilisant le fait que P est un générateur projectif de génération finie et en suivant consciencieusement les isomorphismes

$$P \otimes_R \text{Hom}_S(P, \bigoplus_I P) \cong P \otimes_R \bigoplus_I \text{Hom}_S(P, P) \cong P \otimes_R \bigoplus_I R \cong \bigoplus_I P.$$

□

3.3.5 Corollaire. Soient S un anneau et $n \geq 1$ un entier. Les catégories de modules $S\text{-Mod}$ et $M_n(S)\text{-Mod}$ sont équivalentes.

Démonstration. S^n est un générateur projectif de génération finie et on a vu aux exercices que $\text{End}_S^{\text{opp}}(S^n) \cong M_n(S)$. □

3.3.6 Corollaire. Soient R et S deux anneaux. Si les catégories de modules $R\text{-Mod}$ et $S\text{-Mod}$ sont équivalentes, alors $Z(R) \cong Z(S)$ comme anneaux.

Démonstration. Cf. exercices □

3.3.7 Corollaire. Soient R et S deux anneaux commutatifs. Les catégories de modules $R\text{-Mod}$ et $S\text{-Mod}$ sont équivalentes si et seulement si $R \cong S$.

4 Le foncteur $K_0(-)$

4.1 Définition de $K_0(-)$ et résultats immédiats

4.1.1 Définition. Soit S un semigroupe (i.e. un ensemble muni d'une loi de composition associative) commutatif. Le **groupe de Grothendieck** associé à S , noté $Gr(S)$, est le groupe libre-abélien (i.e. le \mathbb{Z} -module libre) engendré par l'ensemble des symboles $\{[x] \mid x \in S\}$ et quotienté par le sous-groupe engendré par les éléments $[x] + [y] - [x + y]$ pour tout $x, y \in S$.

Remarque. Pour tout $x \in S$, on notera l'image canonique du symbole $[x]$ dans le groupe de Grothendieck $Gr(S)$ par le même symbole $[x]$.

4.1.2 Proposition. Soit S un semigroupe commutatif. Il existe un homomorphisme de semigroupes $\varphi : S \rightarrow Gr(S)$ tel que pour tout groupe H et pour tout homomorphisme de semigroupes $\psi : S \rightarrow H$ il existe un unique homomorphisme de groupes $\theta : Gr(S) \rightarrow H$ tel que $\psi = \theta \circ \varphi$.

Démonstration. On définit $\varphi : S \rightarrow Gr(S)$ via $x \mapsto [x]$ pour tout $x \in S$. Soit $\psi : S \rightarrow H$. On définit $\theta : Gr(S) \rightarrow H$ sur les symboles via $[x] \mapsto \psi(x)$ pour tout $x \in S$. Cela passe au quotient puisque $\theta([x] + [y] - [x + y]) = \psi(x) + \psi(y) - \psi(x + y) = 0$. On a bien $\theta \circ \varphi(x) = \theta([x]) = \psi(x)$ pour tout $x \in S$. Supposons qu'il existe $\theta' : Gr(S) \rightarrow H$ tel que $\theta' \circ \varphi(x) = \psi(x)$ pour tout $x \in S$. Alors sur les symboles on a $\theta'[x] = \theta' \circ \varphi(x) = \psi(x) = \theta[x]$ pour tout $x \in S$. Ainsi $\theta' = \theta$. \square

Remarques. 1. Le groupe de Grothendieck d'un semigroupe est unique à (un seul) isomorphisme près.
2. On peut rendre cette construction fonctorielle puisque pour tout homomorphisme de semigroupes $f : S \rightarrow S'$ on a le diagramme commutatif suivant :

$$\begin{array}{ccc} S & \xrightarrow{f} & S' \\ \varphi \downarrow & & \downarrow \varphi \\ Gr(S) & \xrightarrow{f_*} & Gr(S') \end{array}$$

où l'existence et l'unicité de l'homomorphisme $f_* : Gr(S) \rightarrow Gr(S')$ sont assurées par la propriété universelle.

3. Si **SemiAb** désigne la catégorie des semigroupes commutatifs, alors on peut résumer la proposition en disant que le foncteur $Gr : \mathbf{SemiAb} \rightarrow \mathbf{Ab}$ est adjoint à gauche du foncteur d'oubli $U : \mathbf{Ab} \rightarrow \mathbf{SemiAb}$.

Exemples. 1. $Gr(\mathbb{N}) \cong \mathbb{Z}$ via $[n] - [m] \mapsto (n - m)$.

2. $Gr(\mathbb{Z}) \cong \mathbb{Z}$ puisque $0 = [n] + [-n] - [n + (-n)] = [n] + [-n]$ i.e. $-[n] = [-n]$.

4.1.3 Définition. Soit R un anneau. On définit le monoïde $\underline{\text{Proj}}(R)$ comme l'ensemble constitué des classes d'isomorphisme de R -modules projectifs de génération finie et muni de l'addition $[P] + [Q] = [P \oplus Q]$ et dont le module trivial est l'élément neutre.

Remarque. On peut rendre cette construction fonctorielle en procédant comme suit. Soient $\varphi : R \rightarrow R'$ un homomorphisme d'anneaux et P un R -module projectif de génération finie. On peut munir R' d'une structure de R -module à droite via φ en posant $r'r = r'\varphi(r)$ pour tout $r \in R$ et $r' \in R'$. On peut donc considérer le groupe abélien $R' \otimes_R P$ qui est un R' -module. Montrons qu'il est projectif de génération finie. On sait qu'il existe un R -module projectif Q tel que $P \oplus Q \cong R^n$ pour un certain $n \geq 1$. On a ainsi

$$(R' \otimes_R P) \oplus (R' \otimes_R Q) \cong R' \otimes_R (P \oplus Q) \cong R' \otimes_R R^n \cong R'^n.$$

4.1.4 Définition. Soit R un anneau. On définit le groupe abélien $\underline{K_0(R)}$ comme le groupe de Grothendieck $Gr(\text{Proj}(R))$.

Remarques. 1. On a $[[P]] + [[Q]] - [[P] + [Q]] = [[P]] + [[Q]] - [[P \oplus Q]]$. Pour alléger la notation, on écrira $[P]$ un élément de $K_0(R)$ au lieu de $[[P]]$.

2. Un élément de $K_0(R)$ s'écrit sous la forme $[P] - [Q]$ où P et Q sont des R -modules projectifs de génération finie.
3. $K_0 : \mathbf{Ring} \rightarrow \mathbf{Ab}$ est un foncteur qui associe à tout homomorphisme d'anneaux $\varphi : R \rightarrow R'$ un homomorphisme de groupes $K_0(R) \rightarrow K_0(R')$ tel que $[P] \mapsto [R' \otimes_R P]$ où R' est vu comme un R -module à droite via φ .

Exemples.

1. Soit \mathbb{K} un corps. Tout \mathbb{K} -module de génération finie est un \mathbb{K} -espace vectoriel de dimension finie. La dimension d'un tel objet est un invariant d'isomorphisme. Ainsi la dimension induit un isomorphisme $\text{Proj}(\mathbb{K}) \cong \mathbb{N}$ et $K_0(\mathbb{K}) \cong \mathbb{Z}$.
2. Soit R un anneau principal. On a vu que tout R -module projectif sur un anneau principal est libre, de sorte que ceux qui sont de génération finie sont de la forme R^n . De plus, R a la propriété du rang unique, ce qui signifie que l'on a un isomorphisme $\text{Proj}(R) \cong \mathbb{N}$ et $K_0(R) \cong \mathbb{Z}$.
3. On a vu qu'il existe un anneau non-trivial R tel que $R \cong R \oplus R$ comme R -modules. Soient P et P' deux R -modules projectifs de génération finie. Il existe donc Q et Q' deux R -modules tels que $P \oplus Q \cong R$ et $P' \oplus Q' \cong R$. On a ainsi les deux suites exactes courtes suivantes :

$$P \oplus P \twoheadrightarrow P \oplus R \twoheadrightarrow P \oplus Q \cong R$$

$$P' \oplus P' \twoheadrightarrow P' \oplus R \twoheadrightarrow P' \oplus Q' \cong R,$$

avec $P \oplus R$ et $P' \oplus R$ projectifs. On peut alors montrer (cf. exercices) que $P \oplus R \oplus P' \oplus P' \cong P' \oplus R \oplus P \oplus P$. Ainsi $R \oplus P' \oplus P' \cong Q \oplus P \oplus R \oplus P' \oplus P' \cong Q \oplus P' \oplus R \oplus P \oplus P \cong R \oplus P' \oplus P$. Ainsi on a $[R] + [P'] + [P'] = [R] + [P'] + [P]$ dans $K_0(R)$, i.e. $[P] = [P']$. Ainsi $K_0(R)$ est trivial.

4.1.5 Théorème. Soient R et S deux anneaux tels que $R\text{-Mod} \simeq S\text{-Mod}$. Alors $K_0(R) \cong K_0(S)$.

Démonstration. D'après le théorème d'équivalence de Morita, il existe un S - R -bimodule M tel que $M \otimes_R - : R\text{-Mod} \xrightarrow{\cong} S\text{-Mod}$ est une équivalence de catégories dont $\text{Hom}_S(M, -)$ est un inverse. Ces foncteurs induisent clairement un isomorphisme de monoïdes $\text{Proj}(R) \cong \text{Proj}(S)$. D'où le résultat. \square

4.1.6 Corollaire. Soient R un anneau et $n \geq 1$ un entier. Alors $K_0(R) \cong K_0(M_n(R))$.

4.2 Le groupe K_0 réduit

4.2.1 Définition. Soit R un anneau. L'unique homomorphisme d'anneaux $\iota : \mathbb{Z} \rightarrow R$ tel que $1 \mapsto 1_R$ induit un homomorphisme de groupes $\iota_* : \mathbb{Z} \rightarrow K_0(R)$. Le **groupe K_0 réduit** de R est le quotient $\tilde{K}_0(R) = K_0(R)/\iota_*(\mathbb{Z}) = \text{coker } \iota_*$.

Remarque. L'image de ι_* est le sous-groupe de $K_0(R)$ engendré par les R -modules libres de génération finie puisque $\mathbb{Z} \cong K_0(\mathbb{Z})$ via $1 \mapsto [\mathbb{Z}]$, de sorte que $\iota_*(1) = [R \otimes_{\mathbb{Z}} \mathbb{Z}] = [R]$. Ainsi $\tilde{K}_0(R)$ mesure la partie non-triviale de $K_0(R)$. On a vu que $\tilde{K}_0(R) = 0$ si R est un anneau principal ou un corps.

4.2.2 Théorème. Soit R un anneau commutatif. Alors $K_0(R) \cong \mathbb{Z} \oplus \tilde{K}_0(R)$.

Démonstration. Si R est un anneau commutatif, alors il possède un idéal maximal M et le quotient R/M est un corps. Soient $\pi : R \rightarrow R/M$ l'homomorphisme canonique et $\pi_* : K_0(R) \rightarrow \mathbb{Z}$ l'homomorphisme induit. On a le diagramme commutatif suivant :

$$\begin{array}{ccccccc}
 & & \iota_* & & \pi_* & & \\
 & \swarrow & & \searrow & & \swarrow & \\
 \mathbb{Z} & \xrightarrow{\cong} & K_0(\mathbb{Z}) & \longrightarrow & K_0(R) & \longrightarrow & K_0(R/M) \xrightarrow{\cong} \mathbb{Z} \\
 n \longmapsto & [\mathbb{Z}^n] \longmapsto & [R \otimes_{\mathbb{Z}} \mathbb{Z}^n] = [R^n] \longmapsto & [R/M \otimes_R R^n] = [(R/M)^n] \longmapsto & n.
 \end{array}$$

Ainsi ι_* est une section de π_* et on a un isomorphisme $K_0(R) \cong \text{im } \iota_* \oplus \ker \pi_* \cong \mathbb{Z} \oplus \tilde{K}_0(R)$. \square

Remarque. On a montré qu'un anneau commutatif R a la propriété du rang unique, i.e. si $R^m \cong R^n$ alors $m = n$. La nomenclature suggère que ce résultat est relié à une notion de rang qui serait définie pour d'autres modules que les modules libres de rang fini. C'est en fait le cas : on peut définir $\text{rk}(P) = \dim_{R/M} R/M \otimes_R P$ pour tout R -module projectif de génération finie P puisque $R/M \otimes_R P$ est un R/M -espace vectoriel de dimension finie. On a $\text{rk}(R^m) = \dim_{R/M} R/M \otimes_R R^m = \dim_{R/M} (R/M)^m = m$ pour tout $m \geq 1$. A l'aide de cette définition, on retrouve très facilement le résultat que R a la propriété du rang unique : si $R^m \cong R^n$, alors $m = \text{rk}(R^m) = \text{rk}(R^n) = n$. En contemplant le diagramme de la preuve ci-dessus, on voit que le rang ainsi défini est une application $\text{rk} : \text{Proj}(R) \rightarrow \mathbb{N}$ qui induit $\pi_* : K_0(R) \rightarrow \mathbb{Z}$. Si P et Q sont des R -modules projectifs de génération finie on a $\text{rk}(P \oplus Q) = \dim_{R/M} R/M \otimes_R (P \oplus Q) = \dim_{R/M} R/M \otimes_R P + \dim_{R/M} R/M \otimes_R Q = \text{rk}(P) + \text{rk}(Q)$.

4.2.3 Définition. Soit R un anneau commutatif et M un idéal maximal de R . On définit le **rang** d'un R -module projectif de génération finie P comme $\dim_{R/M} R/M \otimes_R P$. On obtient ainsi un homomorphisme de monoïdes $\text{rk} : \text{Proj}(R) \rightarrow \mathbb{N}$ qui induit un homomorphisme de groupes $K_0(R) \rightarrow \mathbb{Z}$ qui se scinde et fournit l'isomorphisme $K_0(R) \cong \mathbb{Z} \oplus \tilde{K}_0(R)$.

Remarque. L'homomorphisme de monoïdes $\text{rk} : \text{Proj}(R) \rightarrow \mathbb{N} \subset \mathbb{Z}$ n'est pas le rang le plus "universel" que l'on puisse trouver. En effet, considérons l'homomorphisme de monoïdes canonique $\text{Rk} : \text{Proj}(R) \rightarrow K_0(R)$. D'après la propriété universelle du groupe de Grothendieck, rk se factorise par Rk . Ainsi Rk est "meilleur" que rk . De façon générale, Rk est "meilleur" que n'importe quel autre rang (i.e. tout homomorphisme de monoïdes de la forme $\text{Proj}(P) \rightarrow A$, avec A un groupe abélien, se factorise par Rk). Moralité : le groupe $K_0(R)$ nous permet de définir le "meilleur" rang qui soit pour les R -modules projectifs de génération finie.

4.3 Anneaux de Dedekind

4.3.1 Définition. Un anneau commutatif intègre R tel que pour toute paire d'idéaux $I \subset J \subset R$ il existe un idéal K tel que $I = JK$ est dit **de Dedekind**.

Remarque. L'idéal K de la définition est unique si $I, J \neq 0$. En effet, supposons que $I = JK = JK'$. Soit $a \neq 0 \in J$. Alors $(a) \subset J$ et il existe un idéal L tel que $(a) = JL$. Ainsi $(a)K = JKL = JK'L = (a)K'$. Soit $b \in K$. Alors $ab \in (a)K = (a)K'$ et on peut écrire $ab = \sum_i r_i ab'_i$. Ainsi on a $a(b - \sum_i r_i b'_i) = 0$ et $b = \sum_i r_i b'_i \in K'$ puisque R est intègre. On a prouvé que $K \subset K'$ et on procède de même pour prouver que $K' \subset K$.

Exemples. 1. Tout anneau principal commutatif R est de Dedekind. En effet, si $(a) \subset (b)$, alors $a = bc$ pour un certain $c \in R$ et ainsi $(a) = (b)(c)$.
2. L'anneau des entiers d'un corps de nombres (i.e. la clôture intégrale de \mathbb{Z} dans une extension algébrique finie de \mathbb{Q}) est de Dedekind (cf. [Rot88, Thm. 1.4.18 pp. 22-23]). Par exemple, les entiers de Gauss $\mathbb{Z}[i]$ dans $\mathbb{Q}(i)$, ou les entiers d'Eisenstein dans $\mathbb{Q}(\sqrt{-3})$.

4.3.2 Définition. Soit R un anneau de Dedekind. On définit une relation d'équivalence \sim sur les idéaux non-nuls de R en posant $I \sim J$ si et seulement s'il existe $x, y \neq 0 \in R$ tels que $xI = yJ$. Le **groupe de classes** $C(R)$ de R est le groupe abélien des classes d'idéaux non-nuls de R avec la multiplication. On note $\{I\}$ la classe de l'idéal I dans $C(R)$.

- Remarques.** 1. \sim est bien une relation d'équivalence. La réflexivité et la symétrie sont claires. Si $I \sim K$ et $K \sim L$, alors il existe $x, y, y', z \neq 0 \in R$ tels que $xI = yJ$ et $y'J = zK$, de sorte que $xy'I = yy'J = yzK$, i.e. $I \sim K$.
2. La multiplication des classes est bien définie. En effet, si $I \sim I'$ et $J \sim J'$, alors il existe $x, x', y, y' \neq 0 \in R$ tels que $xI = x'I'$ et $yJ = y'J'$, de sorte que $xyIJ = x'y'I'J'$, i.e. $IJ \sim I'J'$.
3. $C(R)$ est bien un groupe abélien. Les idéaux principaux non-nuls forment une classe puisque on a $b(a) = a(b)$, i.e. $(a) \sim (b)$ pour tout $a, b \neq 0 \in R$. L'élément neutre est la classe des idéaux principaux non-nuls puisque $1(a)I = (a)I = aI$, i.e. $(a)I \sim I$ pour tout $a \neq 0 \in R$. Soient I un idéal non-nul de R et $a \neq 0 \in I$. Alors $(a) \subset I$ et il existe un unique idéal non-nul K tel que $(a) = IK$, de sorte que $\{I\}^{-1} = \{K\}$.

- Exemples.** 1. Le groupe de classes d'un anneau principal commutatif est trivial.
2. Le groupe de classes d'un anneau d'entiers d'un corps de nombres est un groupe abélien fini (cf. [Rot88, Thm. 1.4.19 pp. 23-24]).

4.3.3 Lemme. Soient R un anneau de Dedekind et I un idéal non-nul de R . Alors I est un R -module projectif de génération finie.

Démonstration. Soit $a \neq 0 \in I$. On a $(a) \subset I$, de sorte que $(a) = IK$ pour un idéal non-nul K . On peut donc écrire $a = \sum_{i=1}^m b_i c_i$ avec $b_i \in I$ et $c_i \in K$ pour tout $1 \leq i \leq m$. Soit $x \in I$. Pour tout $1 \leq i \leq m$ on a $xc_i \in IK = (a)$, de sorte que $xc_i = ra$ pour un certain $r \in R$ que l'on va noter $\frac{xc_i}{a}$. Considérons les homomorphismes de R -modules suivants : $\varphi : I \rightarrow R^m$, $x \mapsto (\frac{xc_1}{a}, \dots, \frac{xc_m}{a})$ et $\psi : R^m \rightarrow I$, $(x_1, \dots, x_m) \mapsto \sum_{i=1}^m b_i x_i$. On a $\psi\varphi(x) = \psi(\frac{xc_1}{a}, \dots, \frac{xc_m}{a}) = \sum_{i=1}^m b_i \frac{xc_i}{a} = x$ pour tout $x \in I$. Ainsi $R^m \cong I \oplus \ker \psi$ et I est projectif de génération finie. \square

4.3.4 Théorème. Tout anneau de Dedekind est noethérien.

Démonstration. On a vu aux exercices que R est noethérien si et seulement si tout sous-module de R est de génération finie. Un sous-module de R (R vu comme R -module) est un idéal de R (R vu comme anneau) et on vient de montrer que les idéaux de R sont de génération finie. \square

4.3.5 Définition. Soit R un anneau commutatif. Un idéal propre P de R est dit premier si pour toute paire d'idéaux I, J , $P \supset IJ$ implique $P \supset I$ ou $P \supset J$.

Exemple. Tout idéal maximal M d'un anneau commutatif R est premier. Montrons-le. Soient I et J deux idéaux de R tels que $IJ \subset M$. Si $I \subset M$ alors M est premier. Sinon, soit $a \in I - M$. Pour tout $b \in J$ on a $ab \in IJ \subset M$ avec $a \notin M$, de sorte que $[a][b] = [ab] = 0 \in R/M$ avec $[a] \neq 0 \in R/M$. Par intégrité de R/M qui est un corps, on a $[b] = 0 \in R/M$, i.e. $b \in M$. Ainsi $J \subset M$.

4.3.6 Théorème. Soit R un anneau de Dedekind. Tout idéal propre de R se factorise de manière unique (à l'ordre des termes près) par des idéaux maximaux.

Démonstration. Soit I un idéal propre de R . Posons $I_0 = I$. Par le lemme de Zorn, il existe un idéal maximal M_1 tel que $I = I_0 \subset M_1$. Puisque R est de Dedekind, il existe un idéal I_1 tel que $I = I_0 = M_1 I_1$. Si $I_1 \neq R$, alors il existe un idéal maximal M_2 tel que $I_1 \subset M_2$. Puisque R est de Dedekind, il existe un idéal I_2 tel que $I_1 = M_2 I_2$. Etc. De façon générale, pour tout $n \geq 1$, si $I_{n-1} = R$ alors $I_n = R$, sinon I_n est un idéal tel que $I_{n-1} = M_n I_n$ avec M_n un idéal maximal vérifiant $I_{n-1} \subset M_n$. S'il existe un $n \geq 1$ tel que $I_n = R$, alors $I_{n-1} = M_n I_n = M_n R = M_n$ et on a $I = M_1 I_1 = M_1 M_2 I_2 = \dots = M_1 \dots M_n$. Sinon, la chaîne ascendante d'idéaux $I_0 \subset I_1 \subset \dots$ stabilise puisque R est noethérien. Il existe donc un $n \geq 1$ tel que $I_m = I_n$ pour tout $m \geq n$. En particulier on a $I_{n+1} = I_n = M_{n+1} I_{n+1}$. Soit $a \neq 0 \in I_{n+1}$, alors $(a) \subset I_{n+1}$ et il existe un idéal K tel que $(a) = I_{n+1} K$. Ainsi on a $(a) = I_{n+1} K = M_{n+1} I_{n+1} K = (a) M_{n+1}$. On peut donc écrire $a = \sum_{i=1}^m a r_i m_i$ avec $r_i \in R$ et $m_i \in M_{n+1}$ pour tout $1 \leq i \leq m$, de sorte que $a(1 - \sum_{i=1}^m r_i m_i) = 0$ et $1 = \sum_{i=1}^m r_i m_i \in M_{n+1}$ par intégrité, ce qui est absurde.

Il reste à prouver l'unicité de la décomposition. Supposons que $M_1 \dots M_r = N_1 \dots N_s$ avec $M_1, \dots, M_r, N_1, \dots, N_s$ des idéaux maximaux. On a $M_1 \supseteq M_1 \dots M_r = N_1 \dots N_s$, de sorte que $M_1 \supseteq N_j$ pour un certain $1 \leq j \leq s$ puisque M_1 est premier. Quitte à renuméroter, on peut supposer $M_1 \supseteq N_1$. De plus on a $M_1 = N_1$ par maximalité. On a donc $M_1 M_2 \dots M_r = M_1 N_2 \dots N_s$. Soit $m \neq 0 \in M_1$, alors $(m) \subset M_1$ et il existe un idéal K tel que $(m) = M_1 K$. Ainsi on a $(m) M_2 \dots M_r = M_1 K M_2 \dots M_r = M_1 K N_2 \dots N_s = (m) N_2 \dots N_s$. Soit $n \in N_2 \dots N_s$. On a $mn \in (m) M_2 \dots M_r$ et on peut donc écrire $mn = \sum_{i=1}^l m r_i m_i$ avec $r_i \in R$ et $m_i \in M_2 \dots M_r$ pour tout $1 \leq i \leq l$. Ainsi on a $m(n - \sum_{i=1}^l r_i m_i) = 0$, de sorte que $n = \sum_{i=1}^l r_i m_i \in M_2 \dots M_r$ par intégrité. On a donc $N_2 \dots N_s \subset M_2 \dots M_r$. On prouve de même l'autre inclusion, de sorte que $M_2 \dots M_r = N_2 \dots N_s$. Supposons que $r < s$, alors on obtient $M_r = M_r R = M_r N_{r+1} \dots N_s$, et il s'ensuit que $R = N_{r+1} \dots N_s \subset N_{r+1}$, ce qui est absurde. On a donc forcément $r = s$ et $M_1 = N_1, \dots, M_r = N_r$. \square

4.3.7 Corollaire. Soient R un anneau de Dedekind et M un idéal maximal de R . Alors $M^2 \subsetneq M$.

Démonstration. Clair par unicité des factorisations M et M^2 . \square

4.3.8 Corollaire. Soit R un anneau de Dedekind. Un idéal propre de R est premier si et seulement s'il est maximal.

Démonstration. Soit P un idéal premier de R . On a $P = M_1 \dots M_r$ avec M_1, \dots, M_r des idéaux maximaux. Ainsi $M_i \subset P$ pour un certain $1 \leq i \leq r$. Par maximalité de M_i on a $P = M_i$. \square

4.3.9 Lemme (Théorème chinois). Soient R un anneau commutatif, I et J deux idéaux tels que $I + J = R$. Alors $IJ = I \cap J$ et pour tout $r, s \in R$, il existe $y \in R$ tel que $y \equiv r \pmod{I}$ et $y \equiv s \pmod{J}$, de sorte que $R/IJ \cong R/I \times R/J$. Plus généralement, si I_1, \dots, I_m sont des idéaux tels que $I_i + I_j = R$ pour tout $1 \leq i \neq j \leq m$ et si $x_1, \dots, x_m \in R$, alors il existe un élément $y \in R$ tel que $y \equiv x_i \pmod{I_i}$ pour tout $1 \leq i \leq m$.

Démonstration. Cf. exercices. □

4.3.10 Théorème. Soient R un anneau de Dedekind et I un idéal propre. L'anneau quotient R/I est principal.

Démonstration. On peut écrire $I = M_1^{p_1} \dots M_m^{p_m}$ avec $M_i \neq M_j$ pour tout $1 \leq i \neq j \leq m$. L'ensemble $\mathcal{M} = \{M_1, \dots, M_m\}$ fournit la liste exhaustive de tous les idéaux maximaux qui contiennent I . En effet, si M est un idéal maximal tel que $I = M_1^{p_1} \dots M_m^{p_m} \subset M$, alors $M \supset M_i$ pour un certain $1 \leq i \leq m$ puisque M est premier, de sorte que $M = M_i$ par maximalité. On a vu en exercice que les idéaux de R/I sont en bijection avec les idéaux de R qui contiennent I via l'application $\pi : J \mapsto J/I$. Soit J un idéal de R tel que $I \subset J$, alors il existe un idéal maximal M tel que $J \subset M$, de sorte que $I \subset M$ et $M \in \mathcal{M}$. Montrons que les idéaux $\pi(M)$, $M \in \mathcal{M}$, sont principaux dans R/I , i.e. de la forme $M_i = (y_i) + I$ avec $y_i \in R$. En effet, si c'est bien le cas, alors J est un produit de tels idéaux, donc de la forme $(y) + I$ pour un certain $y \in R$, i.e. $\pi(J)$ est principal dans R/I .

Commençons par montrer que $M_1 = (y_1) + I$ pour un certain $y_1 \in R$. Montrons que pour tout choix de deux idéaux distincts dans $\{M_1^2, M_2, \dots, M_m\}$, ces idéaux sont premiers entre eux.

1. $(M_1^2 + M_i = R, i \geq 2)$ On a $M_i \subset M_1^2 + M_i$ pour tout $2 \leq i \leq m$, or $M_i \neq M_1^2$ par unicité de la factorisation en idéaux maximaux, de sorte que $M_i \not\subset M_1^2 + M_i$ et $M_1^2 + M_i = R$ par maximalité de M_i .
2. $(M_i + M_j = R, i \neq j)$ On a $M_i \subset M_i + M_j$ pour tout $1 \leq i \neq j \leq m$, or $M_i \neq M_j$ par hypothèse, de sorte que $M_i \not\subset M_i + M_j$ et $M_i + M_j = R$ par maximalité de M_i .

Ainsi on peut appliquer le théorème chinois. Soit $x \in M_1 - M_1^2$. Il existe donc $y_1 \in R$ tel que

$$\begin{aligned} y_1 &\equiv x \pmod{M_1^2} \text{ et} \\ y_1 &\equiv 1 \pmod{M_i} \text{ pour tout } 2 \leq i \leq m. \end{aligned}$$

On a $y_1 - x \in M_1^2$ avec $x \in M_1$ et $M_1^2 \subset M_1$, de sorte que $y_1 \in M_1$ et l'idéal $(y_1) + I \subset M_1$ puisque $I \subset M_1$. Supposons qu'on ait $(y_1) + I \subset M_1^2$. Alors $y_1 \in M_1^2$ et $x \in M_1^2$, ce qui est absurde. Supposons qu'on ait $(y_1) + I \subset M_i$ pour $i \geq 2$, alors $y_1 \in M_i$ et $1 \in M_i$, i.e. $M_i = R$, ce qui est absurde. Pour résumer on a

$$\begin{aligned} (y_1) + I &\subset M_1, \\ (y_1) + I &\not\subset M_1^2 \text{ et} \\ (y_1) + I &\not\subset M_i \text{ pour tout } i \geq 2. \end{aligned}$$

Ainsi, M_1^2 et les idéaux maximaux M_2, \dots, M_m ne sont pas des facteurs de $(y_1) + I$. Or les facteurs maximaux de $(y_1) + I$ sont clairement des facteurs de I puisque $I \subset (y_1) + I$ [$I = NK \subset (y_1) + I = ML \subset M$ "implique à l'ordre des facteurs près" $N \subset M$ puisque M est premier, donc $N = M$ par maximalité]. Ainsi $(y_1) + I = M_1^p$ avec $p \geq 1$. Si $p \geq 2$, alors on a $(y_1) + I = M_1^2 M_1^{p-2} \subset M_1^2$, ce qui n'arrive pas. Ainsi $M_1 = (y_1) + I$. L'idéal $\pi(M_1) = \pi((y_1) + I) = (\pi(y_1))$ est donc bien principal dans R/I . On procède de même pour M_2, \dots, M_m . □

4.4 $K_0(R)$ lorsque R est un anneau de Dedekind

4.4.1 Théorème. Soit R un anneau de Dedekind. Alors $K_0(R) = \mathbb{Z} \oplus C(R)$.

4.4.2 Lemme. Soient R un anneau de Dedekind, I et J deux idéaux propres de R . Alors il existe un idéal propre I' de R tel que $I \sim I'$ et $I' + J = R$.

Démonstration. Soit $x \neq 0 \in I$. On a $(x) \subset I$ et il existe un idéal K tel que $(x) = IK$. L'anneau quotient R/JK est principal, de sorte que l'idéal K/JK est principal, i.e. il existe $y \in K$ tel que $K/JK = (y)$ dans R/JK . En d'autres termes on a $K = (y) + JK$. Ainsi $(x) = IK = I(y) + IJK = yI + xJ$. Posons $I' = \frac{yI}{x}$, ce qui a un sens puisque $yI \subset (x)$. On a alors $(x) = xI' + xJ$. En particulier, $x = xa + xb$ avec $a \in I'$ et $b \in J$. Ainsi $x(1 - (a + b)) = 0$ et $1 = a + b$ par intégrité. On a ainsi $I' + J = R$. De plus, $I' \sim I$ puisque $xI' = yI$. \square

4.4.3 Lemme. Soient R un anneau de Dedekind, I et J deux idéaux propres de R . Alors on a un isomorphisme de R -modules $I \oplus J \cong R \oplus IJ$.

Démonstration. Soit I' un idéal tel que $I \sim I'$ et $I' + J = R$. Considérons l'homomorphisme de R -modules $\varphi : I' \oplus J \rightarrow R$ donné par $\varphi(a, b) = a + b$ pour tout $a \in I'$ et $b \in J$. L'homomorphisme de R -modules $I' \cap J \rightarrow \ker \varphi$ tel que $a \mapsto (a, -a)$ est clairement un isomorphisme. Puisque $I' + J = R$ on a ainsi la suite exacte courte suivante :

$$0 \longrightarrow I' \cap J \longrightarrow I' \oplus J \xrightarrow{\varphi} R \longrightarrow 0.$$

Cette suite est scindée puisque R est projectif. Ainsi $I' \oplus J \cong R \oplus I' \cap J$. Or $I \sim I'$ signifie qu'il existe $x, y \neq 0 \in R$ tels que $xI = yI'$ et $I \cong I'$ puisque $a \mapsto \frac{xa}{y}$ est l'inverse de $a' \mapsto \frac{ya'}{x}$. On a donc $I \oplus J \cong I' \oplus J \cong R \oplus I' \cap J = R \oplus I'J \cong R \oplus IJ$. \square

4.4.4 Proposition. Soient R un anneau de Dedekind, I_1, \dots, I_m et J_1, \dots, J_m des idéaux de R tels que $\{I_1 \dots I_m\} = \{J_1 \dots J_m\}$. Alors $I_1 \oplus \dots \oplus I_m \cong J_1 \oplus \dots \oplus J_m$ comme R -modules.

Démonstration. Montrons par récurrence que l'on a $I_1 \oplus \dots \oplus I_m \cong R^{m-1} \oplus I_1 \dots I_m$. Le cas $m = 1$ est clair. Ensuite on a $I_1 \oplus \dots \oplus I_m \cong (R^{m-2} \oplus I_1 \dots I_{m-1}) \oplus I_m \cong R^{m-2} \oplus (I_1 \dots I_{m-1} \oplus I_m) \cong R^{m-2} \oplus (R \oplus I_1 \dots I_m) \cong R^{m-1} \oplus I_1 \dots I_m$ par le lemme précédent. De même, on a $J_1 \oplus \dots \oplus J_m \cong R^{m-1} \oplus J_1 \dots J_m$. De plus $I_1 \dots I_m \sim J_1 \dots J_m$ implique $I_1 \dots I_m \cong J_1 \dots J_m$ comme R -modules. Ainsi $I_1 \oplus \dots \oplus I_m \cong R^{m-1} \oplus I_1 \dots I_m \cong R^{m-1} \oplus J_1 \dots J_m \cong J_1 \oplus \dots \oplus J_m$. \square

4.4.5 Lemme. Soient R un anneau de Dedekind et P un R -module projectif de génération finie. Il existe des idéaux I_1, \dots, I_m de R tels que $P \cong I_1 \oplus \dots \oplus I_m$ comme R -modules.

Démonstration. Soit P un R -module projectif de génération finie. Alors il existe un entier $m \geq 1$ et un R -module Q tels que $R^m \xrightarrow{\varphi} P \oplus Q$, de sorte que P s'injecte dans R^m via $i_m : P \xrightarrow{i} P \oplus Q \xrightarrow{\varphi^{-1}} R^m$. Montrons par récurrence sur m que le monomorphisme $i_m : P \hookrightarrow R^m$ implique le résultat. Si $m = 1$, alors on pose $I_1 = \text{im } i_1$. C'est bien un idéal de R et $P \cong I_1$. Supposons le résultat vrai pour $m - 1$ et supposons que $i_m : P \hookrightarrow R^m$. Posons $\pi : P \xrightarrow{i_m} R^m \xrightarrow{p_m} R$ avec p_m la projection sur le dernier facteur. L'idéal $\text{im } \pi$ est un R -module projectif de génération finie par un lemme précédent. Posons $I_m = \text{im } \pi$. On a donc la suite exacte courte suivante :

$$0 \longrightarrow \ker \pi \longrightarrow P \xrightarrow[p_m \varphi^{-1} i]{\pi} I_m \longrightarrow 0.$$

Cette suite exacte courte est scindée puisque I_m est projectif. Ainsi $P \cong \ker \pi \oplus I_m$. De plus on a $p_m \varphi^{-1} i(\ker \pi) = 0$, i.e. $\varphi^{-1} i(\ker \pi) \subset \ker p_m = R^{m-1}$. Ainsi $\ker \pi \hookrightarrow R^{m-1}$. Par hypothèse de récurrence $\ker \pi \cong I_1 \oplus \dots \oplus I_{m-1}$, et finalement $P \cong I_1 \oplus \dots \oplus I_m$. \square

4.4.6 Proposition. Soient R un anneau de Dedekind, I_1, \dots, I_m et J_1, \dots, J_n des idéaux de R tels que $I_1 \oplus \dots \oplus I_m \cong J_1 \oplus \dots \oplus J_n$ comme R -modules. Alors $m = n$ et $\{I_1 \dots I_m\} = \{J_1 \dots J_n\}$.

Démonstration. Calculons le rang des modules projectifs de génération finie $I_1 \oplus \dots \oplus I_m$ et $J_1 \oplus \dots \oplus J_n$. Soit F le corps des fractions de R (R est intègre). On a $\dim_F F \otimes_R (I_1 \oplus \dots \oplus I_m) = \sum_{i=1}^m \dim_F F \otimes_R I_i = \sum_{i=1}^m \dim_F F = m$ et $\dim_F F \otimes_R (J_1 \oplus \dots \oplus J_n) = n$. Ainsi $m = n$. Considérons l'isomorphisme $\varphi : I_1 \oplus \dots \oplus I_m \xrightarrow{\cong} J_1 \oplus \dots \oplus J_m$. Pour tout $1 \leq i, j \leq m$ posons

$$\varphi_{ij} : I_j \xrightarrow{\iota_j} I_1 \oplus \dots \oplus I_m \xrightarrow{\varphi} J_1 \oplus \dots \oplus J_m \xrightarrow{\pi_i} J_i.$$

Ainsi pour tout $(x_1, \dots, x_m) \in I_1 \oplus \dots \oplus I_m$ et pour tout $1 \leq i \leq m$ on a $\pi_i \varphi(x_1, \dots, x_m) = \pi_i \varphi(\sum_{j=1}^m \iota_j(x_j)) = \sum_{j=1}^m \pi_i \varphi \iota_j(x_j) = \sum_{j=1}^m \varphi_{ij}(x_j)$. Pour tout $\lambda \neq 0 \in F$ on a $\lambda \varphi_{ij}(x_j) = \varphi_{ij}(\lambda x_j) = \varphi_{ij}(\lambda) x_j$, de sorte que $\varphi_{ij}(x_j) = q_{ij} x_j$ pour un certain $q_{ij} \neq 0 \in F$. Ainsi on a

$$\underbrace{\begin{pmatrix} q_{11} & \dots & q_{1m} \\ \vdots & \ddots & \vdots \\ q_{m1} & \dots & q_{mm} \end{pmatrix}}_{Q \in M_m(F)} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$$

où $(y_1, \dots, y_m) = \varphi(x_1, \dots, x_m)$. La matrice Q est inversible puisque φ est un isomorphisme. Montrons qu'on a $\det(Q)I_1 \dots I_m = J_1 \dots J_m$. Soient $x_1 \in I_1, \dots, x_m \in I_m$. Alors

$$\det(Q)x_1 \dots x_m = \det\left(Q \begin{pmatrix} x_1 & & 0 \\ & \ddots & \\ 0 & & x_m \end{pmatrix}\right) = \det\begin{pmatrix} & \vdots & \\ \underbrace{q_{i1}x_1}_{\in J_i} & \cdots & \underbrace{q_{im}x_m}_{\in J_i} \\ & \vdots & \end{pmatrix}$$

et $\det(Q)x_1 \dots x_m \in J_1 \dots J_m$. Ainsi $\det(Q)I_1 \dots I_m \subset J_1 \dots J_m$. On prouve de même que $\det(Q)^{-1}J_1 \dots J_m \subset I_1 \dots I_m$. Finalement $\{I_1 \dots I_m\} = \{J_1 \dots J_m\}$. \square

Démonstration du théorème. Un élément de $K_0(R)$ est de la forme $[P] - [Q]$, où P et Q sont des R -modules projectifs de génération finie. Il existe deux familles d'idéaux non-nuls $\{I_1, \dots, I_m\}$ et $\{J_1, \dots, J_n\}$ telles que $P \cong I_1 \oplus \dots \oplus I_m$ et $Q \cong J_1 \oplus \dots \oplus J_n$ comme R -modules. De plus on sait que si $[P] - [Q] = [P'] - [Q']$, i.e. si $[P] + [Q'] = [P'] + [Q]$, alors $I_1 \oplus \dots \oplus I_m \oplus J'_1 \oplus \dots \oplus J'_{n'} \cong I'_1 \oplus \dots \oplus I'_{m'} \oplus J_1 \oplus \dots \oplus J_n$, de sorte que $m + n' = m' + n$, i.e. $m - n = m' - n'$, et $\{I_1 \dots I_m\}\{J_1 \dots J_n\}^{-1} = \{I'_1 \dots I'_{m'}\}\{J'_1 \dots J'_{n'}\}^{-1}$. Ainsi l'homomorphisme $\varphi : K_0(R) \rightarrow \mathbb{Z} \oplus C(R)$ donné par $[I_1 \oplus \dots \oplus I_m] - [J_1 \oplus \dots \oplus J_n] \mapsto (m - n, \{I_1 \dots I_m\}\{J_1 \dots J_n\}^{-1})$ est bien défini.

Cet homomorphisme est injectif puisque $\varphi([P] - [Q]) = (m - n, \{I_1 \dots I_m\}\{J_1 \dots J_n\}^{-1}) = (m' - n', \{I'_1 \dots I'_{m'}\}\{J'_1 \dots J'_{n'}\}^{-1}) = \varphi([P'] - [Q'])$ implique $m + n' = m' + n$ et $\{I_1 \dots I_m\}\{J'_1 \dots J'_{n'}\} = \{I'_1 \dots I'_{m'}\}\{J_1 \dots J_n\}$. Ainsi $I_1 \oplus \dots \oplus I_m \oplus J'_1 \oplus \dots \oplus J'_{n'} \cong I'_1 \oplus \dots \oplus I'_{m'} \oplus J_1 \oplus \dots \oplus J_n$ et $[P \oplus Q'] = [P' \oplus Q]$, i.e. $[P] - [Q] = [P'] - [Q']$.

Cet homomorphisme est surjectif puisque $\varphi([R^{m-1} \oplus I] - [R^{n-1} \oplus J]) = \varphi(\underbrace{[R \oplus \dots \oplus R \oplus I]}_{(m-1) \text{ termes}} -$

$$\underbrace{[R \oplus \dots \oplus R \oplus J]}_{(n-1) \text{ termes}}) = (m - n, \{R^{m-1}I\}\{R^{n-1}J\}^{-1}) = (m - n, \{I\}\{J\}^{-1}). \quad \square$$

5 Le foncteur $K_1(-)$.

5.1 Matrices élémentaires et le lemme de Whitehead

5.1.1 Définition. Soit R un anneau. Pour tout $n \geq 1$ on considère $GL_n(R)$, le sous-groupe des matrices inversibles de $M_n(R)$. On considère également l'inclusion $GL_n(R) \subset GL_{n+1}(R)$ définie par $A \mapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$. Cela définit ce que l'on appelle un système direct (cf. exercices). On peut ainsi considérer le groupe $GL(R) = \varinjlim GL_n(R)$. Avec l'inclusion ci-dessus, on a $GL(R) = \bigcup_{n \geq 1} GL_n(R)$.

5.1.2 Définition. Soit R un anneau. Pour tout $a \in R$ et $i \neq j$, $1 \leq i, j \leq n$, on définit la matrice élémentaire $e_{ij}(a) \in M_n(R)$ par

$$(e_{ij}(a))_{kl} = \begin{cases} 1 & \text{si } k = l, \\ a & \text{si } k = i \text{ et } l = j, \\ 0 & \text{sinon.} \end{cases}$$

Le sous-groupe de $GL_n(R)$ engendré par les matrices élémentaires est noté $E_n(R)$. Pour tout $n \geq 1$ on peut considérer l'inclusion $E_n(R) \subset E_{n+1}(R)$ définie par $A \mapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$. Le sous-groupe $E(R) = \varinjlim E_n = \bigcup_{n \geq 1} E_n$ de $GL(R)$ est le groupe des matrices élémentaires.

Remarques. 1. La matrice $e_{ij}(a)A$ est la matrice obtenue à partir de A en ajoutant à la i -ème ligne $a \cdot (j$ -ème ligne).

2. La matrice $Ae_{ij}(a)$ est la matrice obtenue à partir de A en ajoutant à la j -ème colonne $a \cdot (i$ -ème colonne).

5.1.3 Lemme. 1. $e_{ij}(a)e_{ij}(b) = e_{ij}(a+b)$, en particulier $e_{ij}(a)^{-1} = e_{ij}(-a)$,

$$2. [e_{ij}(a), e_{kl}(b)] = \begin{cases} 1 & \text{si } i \neq l \text{ et } j \neq k, \\ e_{il}(ab) & \text{si } i \neq l \text{ et } j = k, \\ e_{kj}(-ba) & \text{si } i = l \text{ et } j \neq k, \end{cases}$$

Démonstration. Cf. exercices. □

Remarque. Il n'y a pas de formule simple pour $i = l$ et $j = k$.

5.1.4 Lemme. Toute matrice triangulaire avec des 1 dans la diagonale appartient à $E(R)$.

Démonstration. Cf. exercices. □

5.1.5 Proposition. Soit $A \in GL_n(R)$. Alors $\begin{pmatrix} A & 0 \\ 0 & A^{-1} \end{pmatrix} \in E_{2n}(R)$.

Démonstration.

$$\begin{pmatrix} A & 0 \\ 0 & A^{-1} \end{pmatrix} = \begin{pmatrix} 1 & A \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -A^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & A \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

□

5.1.6 Lemme (Lemme de Whitehead). Soit R un anneau. On a

$$E(R) = [E(R), E(R)] = [GL(R), GL(R)].$$

En particulier, $E(R)$ est un sous-groupe normal de $GL(R)$ et $GL(R)/E(R)$ est un groupe abélien.

Démonstration. On a clairement $[E(R), E(R)] \subset E(R)$. On a vu que $[e_{ij}(a), e_{jl}(1)] = e_{il}(a)$ si i, j et l sont distincts. En d'autres termes, tout générateur de $E(R)$ est un commutateur. Ainsi $E(R) \subset [E(R), E(R)] \subset [GL(R), GL(R)]$. Il reste à montrer que $[GL(R), GL(R)] \subset E(R)$. Soient $A, B \in GL(R)$. On a

$$\begin{pmatrix} ABA^{-1}B^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} AB & 0 \\ 0 & B^{-1}A^{-1} \end{pmatrix} \begin{pmatrix} A^{-1} & 0 \\ 0 & A \end{pmatrix} \begin{pmatrix} B^{-1} & 0 \\ 0 & B \end{pmatrix} \in E(R)$$

par la proposition. □

5.1.7 Définition. Soit R un anneau. On définit le groupe abélien $\underline{K_1(R)}$ comme le groupe $GL(R)/E(R) = GL(R)/[GL(R), GL(R)]$.

Remarques. 1. Un élément de $K_1(R)$ est noté $[A]$ avec $A \in GL(R)$.

2. Notons $A \oplus B$ la matrice $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$. On a $A \oplus B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \begin{pmatrix} AB & 0 \\ 0 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} B^{-1} & 0 \\ 0 & B \end{pmatrix}}_{\in E(R)}$, de

sorte que $[A] \cdot [B] = [AB] = [A \oplus B]$.

3. $[A] = 1$ signifie que l'on peut transformer A en la matrice identité par des opérations élémentaires sur les lignes (ou sur les colonnes). En effet, si $[A] = 1$, alors il existe une matrice élémentaire E telle que $EA = 1$ et $e_{ij}(a)A$ est la matrice obtenue à partir de A en ajoutant à la i -ème ligne $a \cdot (j$ -ème ligne).

4. $K_1 : \mathbf{Ring} \rightarrow \mathbf{Ab}$ est un foncteur qui associe à tout homomorphisme d'anneaux $\varphi : R \rightarrow R'$ un homomorphisme de groupes $K_1(R) \rightarrow K_1(R')$ tel que $[(a_{ij})] \mapsto [(\varphi(a_{ij}))]$.

5.2 $K_1(R)$ lorsque R est un anneau commutatif

Remarque. Si R est un anneau commutatif, alors on peut considérer le déterminant d'une matrice carrée à coefficients dans R . En particulier, pour tout $n \geq 1$ on a $GL_n(R) = \{A \in M_n(R) \mid \det(A) \in R^\times\}$, où R^\times est le groupe des éléments inversibles de R .

5.2.1 Définition. Soit R un anneau commutatif. Pour tout $n \geq 1$ on considère $SL_n(R)$, le groupe multiplicatif des matrices carrées $n \times n$ à coefficients dans R et de déterminant 1. Le groupe spécial linéaire $SL(R)$ est donné par $\varinjlim SL_n(R) = \bigcup_{n \geq 1} SL_n(R)$.

Exemple. $GL_1(\mathbb{Z}) = \{\pm 1\}$ et $SL_1(\mathbb{Z}) = \{+1\}$

5.2.2 Théorème. Soit R un anneau commutatif. On a $K_1(R) \cong R^\times \oplus \underbrace{SL(R)/E(R)}_{SK_1(R)}$.

Démonstration. On a clairement $E(R) \subset SL(R)$, de sorte que $[GL(R), GL(R)] \subset SL(R)$ et $GL(R)/SL(R)$ est abélien. On a donc la suite exacte courte (de groupes) suivante :

$$SL(R) \twoheadrightarrow GL(R) \xrightarrow{\det} R^\times.$$

Cette suite induit la suite exacte courte (de groupes abéliens) suivante :

$$SL(R)/E(R) \twoheadrightarrow GL(R)/E(R) \xrightarrow{\det} R^\times.$$

Cette suite se scinde via $R^\times \cong GL_1(R) \cong GL_1(R)/E_1(R) \subset GL(R)/E(R)$, $a \mapsto [(a)]$. □

5.2.3 Lemme. Soit R un corps. Pour tout $n \geq 1$ on a $SL_n(R) = E_n(R)$.

Démonstration. Il suffit de prouver que $SL_n(R) \subset E_n(R)$. Soit $A \in SL_n(R)$. On sait du cours d'algèbre linéaire que par des opérations élémentaires sur les lignes, A devient diagonale et reste de déterminant 1. En effet, dans la première colonne par exemple, il existe un élément non-nul qui permet de "tuer" tous les autres éléments de la colonne par des opérations élémentaires sur les lignes. A l'aide de matrices de la forme $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \in E(R)$, on peut au besoin "permuter" la ligne qui contient cet élément avec la première ligne. Ainsi on obtient une matrice dont la première colonne est constituée d'un élément non-nul sur la première ligne et de zéros en-dessous. On procède de même sur les autres colonnes pour obtenir une matrice diagonale. Le déterminant reste clairement 1. En multipliant cette matrice à gauche par des matrices de la forme (*) $\text{diag}(1, \dots, 1, a^{-1}, a, 1, \dots, 1)$, on obtient la matrice $\text{diag}(1, \dots, 1, b)$, pour un certain $b \in R^\times$. Or la matrice obtenue doit être de déterminant 1, ce qui force $b = 1$. De plus, les matrices de la forme (*) sont élémentaires puisque $\begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \in E_2(R)$. En résumé, on a montré que A se transforme en la matrice identité par des opérations élémentaires sur les lignes, i.e. il existe une matrice $E \in E_n(R)$ telle que $EA = I_n$. Ainsi $A = E^{-1} \in E_n$. □

5.2.4 Théorème. Soit R un corps. Alors le déterminant induit l'isomorphisme $K_1(R) \cong R^\times = R - \{0\}$.

- Exemples.**
1. $K_1(\mathbb{Q}) = \mathbb{Q} - \{0\}$.
 2. $K_1(\mathbb{R}) = \mathbb{R} - \{0\}$.
 3. $K_1(\mathbb{Z}/2) = 0$.
 4. $K_1(\mathbb{Z}/3) = \mathbb{Z}/2$.

5.3 $K_1(R)$ lorsque R est un anneau euclidien

5.3.1 Définition. Un anneau R est euclidien s'il est commutatif, intègre et s'il existe une norme $|\cdot| : R \rightarrow \mathbb{N}$ telle que

1. $|x| = 0$ si et seulement si $x = 0$, $x \in R$,
2. $|xy| = |x||y|$ pour tout $x, y \in R$,
3. si $x, y \in R$, $y \neq 0$, alors il existe $q, r \in R$ tels que $x = qy + r$ avec $0 \leq |r| < |y|$.

Remarque. $x \in R^\times$ si et seulement si $|x| = 1$.

- Exemples.**
1. \mathbb{Z} muni de la valeur absolue est euclidien.
 2. $\mathbb{Z}[i]$ avec $|a + bi| = a^2 + b^2$ est euclidien.
 3. L'anneau des polynômes $\mathbb{K}[t]$, où \mathbb{K} est un corps et $|f(t)| = 2^{\deg(f)}$ (avec la convention que $\deg(0) = -\infty$) est euclidien.

5.3.2 Théorème. Soit R un anneau euclidien. Alors le déterminant induit l'isomorphisme $K_1(R) \cong R^\times = \{x \in R \mid |x| = 1\}$.

Démonstration. Comme dans le cas d'un corps, il suffit de montrer que $SL_n(R) \subset E_n(R)$. Soit $A = (a_{ij}) \in SL_n(R)$. Considérons la première colonne de A . Il y existe un élément non-nul. Soit $a_{i1} \neq 0$ avec $|a_{i1}|$ minimal. Si $|a_{i1}| = 1$, alors a_{i1} est inversible. Si $|a_{i1}| > 1$, alors (a_{i1}) est un idéal propre de R . Or on a $1 = \det(A) \in (a_{11}, \dots, a_{n1})$, de sorte que $R = (a_{11}, \dots, a_{n1})$. Il existe donc $j \neq i$ tel que $a_{j1} \notin (a_{i1})$. Ainsi on a $a_{j1} = qa_{i1} + r$ avec $|r| < |a_{i1}|$ et $r \neq 0$. Si l'on soustrait $q \cdot (i\text{-ème ligne de } A)$ à la $j\text{-ème ligne de } A$, alors on obtient une matrice A' avec dans la première colonne un élément de norme minimale plus petite que dans A . En itérant la procédure, on obtient une matrice avec un élément inversible dans la première colonne. On peut utiliser cet élément pour "tuer" tous les autres éléments dans la colonne par des opérations élémentaires sur les lignes. Finalement on obtient une matrice diagonale dont les éléments non-nuls sont inversibles et on peut procéder comme dans le cas où R est un corps. \square

Exemple. $K_1(\mathbb{Z}) \cong \{\pm 1\}$.

- Remarques.**
1. Soit R l'anneau des entiers d'un corps de nombres (c'est un anneau de Dedekind). On peut montrer que $SK_1(R)$ est trivial et donc $K_1(R) = R^\times$. L'étude de R^\times est l'objet de la théorie des nombres.
 2. Soit $R = \mathbb{R}[x, y]/(x^2 + y^2 - 1)$ l'anneau des fonctions polynomiales sur le cercle (c'est un anneau de Dedekind). On peut montrer que $SK_1(R)$ n'est pas trivial et contient un élément d'ordre 2.

Références

- [Ar196] D. ARLETTAZ, *Notes de cours*.
- [BK00] A.J. BERRICK AND M.E. KEATING, *An Introduction to Rings and Modules*, Cambridge studies in advanced mathematics 65 (Cambridge University Press, 2000).
- [Clé06-1] A. CLÉMENT, *Applications du lemme de Zorn*, cours "Anneaux et modules", Ecole Polytechnique Fédérale de Lausanne, été 2006.
- [Gol84] R. GOLDBLATT, *Topoi, The Categorical Analysis of Logic*, revised edition, Studies in logic and the foundations of mathematics 98 (North-Holland, 1984).
- [HS96] P.J. HILTON AND U. STAMMBACH, *A course in Homological Algebra*, Graduate Texts in Mathematics 4, 2nd edition (Springer-Verlag, 1996).
- [Ina95] H. INASSARIDZE, *Algebraic K-Theory*, Mathematics and Its Applications (Kluwer Academic Publishers, 1995).
- [Jac89-I] N. JACOBSON, *Basic Algebra I*, 2nd edition (W.H. Freeman and Company, 1989).
- [Jac89-II] N. JACOBSON, *Basic Algebra II*, 2nd edition (W.H. Freeman and Company, 1989).
- [Jea05] A. JEANNERET, *Notes de cours*.
- [Kar78] M. KAROUBI, *K-Theory, An Introduction*, Grundlehren der mathematischen Wissenschaften 226 (Springer-Verlag, 1978).
- [Lam91] T.Y. LAM, *A First Course in Noncommutative Rings*, Graduate Texts in Mathematics 131 (Springer-Verlag, 1991).
- [Mac71] S. MAC LANE, *Categories for the Working Mathematician*, Graduate Texts in Mathematics 5 (Springer-Verlag, 1971).
- [Mat00] M. MATTHEY, *Notes de cours*.
- [Mil71] J. MILNOR, *Introduction to Algebraic K-Theory*, Annals of Mathematics Studies 72 (Princeton University Press and University of Tokyo Press, 1971).
- [Mit65] B. MITCHELL, *Theory of Categories*, Pure and Applied Mathematics (Academic Press, New-York and London, 1965).
- [Ros94] J. ROSENBERG, *Algebraic K-Theory and Its Applications*, Graduate Texts in Mathematics 147 (Springer-Verlag, 1994).
- [Rot88] J.J. ROTMAN, *An Introduction to Algebraic Topology*, Graduate Texts in Mathematics 119 (Springer-Verlag, 1988).
- [ZS58] O. ZARISKI AND P. SAMUEL, *Commutative Algebra, Volume I*, The University Series in Higher Mathematics (D. Van Nostrand, 1958).

Index

$K_0(-)$, 38

$K_1(-)$, 49

$\text{Proj}(-)$, 37

Action

à gauche, 8

Anneau, 4

centre d'un-, 5

commutatif, 4

de Dedekind, 41

de division, 4

des matrices, 4

des résidus, 6

euclidien, 51

homomorphisme, noyau d'un-, 5

intègre, 7

noethérien, 22

noethérien à droite, 22

noethérien à gauche, 22

non-unital, 4

opposé, 8

principal, 7

quotient, 6

simple, 6

sous-, 5

Bimodule, 30

Catégorie, 25

équivalence, 33

duale, 26

localement petite, 25

morphismes d'une-, 25

objet nul, 26

objets d'une-, 25

Centre d'un anneau, 5

Codomaine, 25

Condition de chaîne ascendante, 21

Conoyau

d'un homomorphisme de modules, 9

d'un morphisme, 27

Corps, 4

gauche, 4

non-commutatif, voir corps gauche

Domaine, 25

Epimorphisme, 26

de modules, 8

Equivalence naturelle, 28

Foncteur, 27

adjoint à gauche, 28

contravariant, 27

covariant, 27

d'oubli, 27

exact à droite, 32

exact à gauche, 32

identité, 27

libre, 27

Générateur

d'un idéal, 7

Générateurs

d'un module, 14

Groupe

des matrices élémentaires, 48

linéaire général, 4

spécial linéaire, 50

Groupe de classes, 41

Groupe de Grothendieck, 37

Homomorphisme

d'anneaux, 5

d'anneaux, noyau d'un-, 5

de modules, 8

de modules, conoyau d'un-, 9

de modules, image d'un-, 9

de modules, noyau d'un-, 9

Idéal

à droite, 5

à gauche, 5

bilatère, 5

engendré, 7

générateur(s) d'un-, 7

maximal, 6

premier, 42

principal, 7

propre, 5

Image

d'un homomorphisme d'anneaux, 5

d'un homomorphisme de modules, 9

Isomorphisme, 26

d'anneaux, 5

de modules, 8

Lemme

du *deux sur trois*, 12

Matrice élémentaire, 48

- Module
 - à droite, 8
 - à gauche, 8
 - base d'un-, 14
 - compact, 32
 - de génération finie, 14
 - de rang fini, 14
 - de type fini, 14
 - engendré par un sous-ensemble, 14
 - ensemble de générateurs, 14
 - homomorphisme de modules, 8
 - libre, 14
 - noethérien, 21
 - projectif, 15
 - quotient, 9
 - sous-, 9
- Modules
 - somme directe de modules, 10
- Monomorphisme, 26
 - de modules, 8
- Morphisme
 - nul, 26
- Noyau
 - d'un homomorphisme d'anneaux, 5
 - d'un homomorphisme de modules, 9
 - d'un morphisme, 27
- Opposé
 - anneau-, 8
- Premier théorème d'isomorphisme
 - pour les anneaux, 6
 - pour les modules, 10
- Principal
 - anneau-, 7
 - idéal-, 7
- Produit tensoriel, 30
- Propriété catégorielle, 33
- Propriété du rang unique, 19
- Propriété universelle
 - de la somme directe de modules, 11
 - du quotient de modules, 10
- Quotient
 - module-, 9
- Rang
 - d'un module libre, 14
 - d'un module projectif de génération finie, 40
- Section, 13
 - suite exacte courte scindée, 13
- Somme directe
 - de modules, 10
- Sous-module, 9
- Suite exacte, 12
 - courte, 12
 - courte scindée, 13
- Théorème
 - d'isomorphisme, premier-, 10
- Transformation naturelle, 28