Chapitre 1

Introduction, définitions, exemples

1.1 Introduction

Remarques 1.1.1. Ces notes sont évolutives...Elles vont se construire en même temps que le cours.

Un bref aperçu historique du développement de la théorie des anneaux a été donné en cours. Quelques noms peuvent servir de points de repères : Hamilton, Molien, Wedderburn, Cartan, E. Noether, E. Artin, Jacobson, Hopkins, Levitzki, Goldie, Martindale, Amitsur, Cohn, Goodearl,...

Les buts du cours : la version optimiste est la suivante :

a) Développer la théorie des anneaux et modules semi-simples donner le théorème d'Artin-Wedderburn, donner quelques applications en représentations des groupes finis.

b) Etude de la localisation de Ore, théorème de Goldie, dimension uniforme, théorème de Posner, autres types d'anneaux quotients.

c) Questions de plongement exemple de Malcev, corps des fractions et corps universels des fractions (théorèmes de P.M.Cohn)

d) Simplifications de modules et anneaux de von Neumann réguliers.

1.2 Définitions et exemples

Définitions 1.2.1. Soit R un anneau (toujours supposé unitaire). Un R-module à gauche est un groupe abélien $M,+$ muni d'une application $R\times M \longrightarrow M : (r,m) \mapsto r.m$ telle que

a) $(r_1 + r_2).m = r_1.m + r_2.m \quad \forall(r_1,r_2,m) \in R \times R \times M.$

b) $r.(m_1 + m_2) = r.m_1 + r.m_2 \quad \forall(m_1,m_2,r) \in M \times M \times R.$

c) $(r_1r_2).m = r_1.(r_2.m) \quad \forall(r_1,r_2,m) \in R \times R \times M.$

d) $1.m = m \quad \forall m \in M.$

Un R-module à droite est un groupe abélien $M,+$ muni d'une application $M \times R \longrightarrow M : (m,r) \mapsto m.r$ telle que

a) $m.(r_1 + r_2) = m.r_1 + m.r_2 \quad \forall (r_1,r_2,m) \in R \times R \times M$.
b) $(m_1 + m_2).r = m_1.r + m_2.r \quad \forall (m_1,m_2,r) \in M \times M \times R$.
c) $m.(r_1 r_2) = (m.r_1).r_2 \qquad \forall (r_1,r_2,m) \in R \times R \times M$.
d) $m.1 = m \quad \forall m \in M$.

Si R et S sont des anneaux, un (R,S) bimodule est un R-module à gauche qui est simultanément un S-module à droite tel que pour tout $r,m,s \in R \times M \times S,(r.m).s = r.(m.s)$

Exemples 1.2.2. 1. $\mathbb{H}(R)$ le corps ds quaternions d'Hamilton sur $\mathbb{R}$.

2. $M_n(R)$, où R est un anneau et $n \in \mathbb{N}$. R^n (les colonnes) est alors naturellement un $M_n(R)$-module à gauche.
3. $R \times S$ où R et S sont des anneaux.
4. $T_n(R) = \{A = (a_{ij}) \in M_n(R) \mid a_{ij} = 0 \text{ si } j < i\}$.
5. $B_3(R) = \{A \in T_n(R) \mid a_{12} = 0\}$.
6. $C_3(R) = \{A \in B_3(R) \mid a_{23} = 0\}$.
7. $\mathbb{C}[x; -]$, où $-$ désigne la conjugaison complexe. Les éléments de cet anneau sont les polynômes de la forme $\sum_{i=0}^{n} c_i x^i$, $c_i \in \mathbb{C}$. La loi de commuattion $xa = \overline{a}x$ pour $a \in \mathbb{C}$.
8. Si σ est un endomorphisme d'un anneau R et δ est une σ-dérivation de R (i.e. $\delta(a+b) = \delta(a)+\delta(b)$ et $\delta(ab) = \sigma(a)\delta(b)+\delta(a)b$ pour tout $a,b \in R$). Si $\sigma = id.$ on obtient la définition d'une dérivation (usuelle) sur R. Si $a \in R$, l'application
$$\delta_{a,\sigma} : R \longrightarrow R : x \mapsto ax - \sigma(x)a$$
est une σ-dérivation appelée dérivation interne.
On peut alors considérer l'anneaux des polynômes gauches (aussi appelé extension de Ore) $R[x; \sigma,\delta]$ dont les éléments sont les polynômes $\sum_{i=0}^{n} a_i x^i$, $a_i \in R$ et la multiplication est basée sur la loi de commutation
$$xa = \sigma(a)x + \delta(a) \quad \text{pour } a \in R$$
9. On peut aussi considérer les polynômes de Laurent $R[x,x^{-1}; \sigma]$, les séries formelles $R[[x; \sigma]]$.
10. Si R et S sont des anneaux et M est un (R,S) bimodule on peut considérer l'anneau
$$\begin{pmatrix} R & M \\ 0 & S \end{pmatrix}$$

11. Si G est un groupe et R est un anneau on peut former l'anneau de groupe RG. On verra l'utilité de cet anneau lors de la théorie des représentations des groupes finis.

Définition 1.2.3. Un anneau R est dit simple si les seuls idéaux bilatères de R sont (0) et R.

Les corps sont évidemment des anneaux simples. Les anneaux simples serviront de "briques" lors de la description des anneaux semi-simples donnés par le théorème d'Artin-Wedderburn. Le théorème suivant montre, en particulier, que les anneaux de matrices sur des corps sont des anneaux simples.

Théorème 1.2.4. *Soit R un anneau et $M_n(R)$ l'anneau des matrices $n \times n$ sur R. Les idéaux de R sont de la forme $M_(I)$ où I est idéal bilatère de R. En particulier, si R est simple alors $M_n(R)$ est simple.*

Démonstration. Il est clair que si I est un idéal de R alors $M_n(I)$ est un idéal de $M_n(R)$.

D'autre part si J est un idéal de $M_n(R)$ on définit $I := \{a \in R \,|\, a$ est le coefficient M_{11} d'une matrice $M \in J\}$. On montre que $J = M_n(I)$. On remarque tout d'abord que

$$\forall M \in M_n(R),\, e_{ij}Me_{kl} = M_{jk}e_{il}.$$

Si $M \in J$,$e_{1i}Me_{kl} = M_{ij}e_{11} \in J$ donc $M_{ij} \in I$. D'autre part, si $A \in M_n(I)$ et $1 \leq i{,}l \leq n$ on choisit $M \in J$ tel que $M_{11} = A_{il}$ on alors $A_{il}e_{il} = M_{11}e_{il} = e_{i1}Me_{1l} \in J$ et donc $A \in J$. □

Voici une autre source importante d'anneaux simples :

Théorème 1.2.5. *Soit A une $\mathbb{Q}$-algèbre et δ une dérivation sur A. $R = A[x; id.,\delta]$ est un anneau simple si et seumlement si A est δ-simple (les seuls idéaux bilatères de A stable par δ sont (0) et R) et δ n'est pas une dérivation interne.*

Démonstration. □

Chapitre 2

Conditions de Chaînes; radicaux

2.1 Modules noethériens, artiniens

Définition 2.1.1. Soit R un anneau, un module ${}_RM$ est noetherien (resp. artinien) si toute chaîne ascendante (resp. descendante) de sous modules de M est stationnaire. Un anneau R est noethérien à gauche (resp. artinien) si ${}_RR$ est noethérien (resp. artinien). De même R est noethérien (resp. artinien) à droite si R_R l'est. Un R-module à gauche (resp. à droite) non nul ${}_RM$ (resp. M_R) est simple si les seuls sous modules de M sont $\{0\}$ et M.

Proposition 2.1.2. *Soit ${}_RM$ un R-module, les affirmations suivantes sont équivalentes :*

1. *${}_RM$ est noetherien.*
2. *Toute chaîne strictement ascendante de sous-modules de M est finie.*
3. *Les sous-modules de ${}_RM$ possède la condition maximale i.e. tout ensemble non vide de sous modules de M admet un élément maximal.*
4. *Tout sous-module de ${}_RM$ est finiment engendré.*

De même on a aussi :

Proposition 2.1.3. *Soit ${}_RM$ un R-module, les affirmations suivantes sont équivalentes :*

1. *${}_RM$ est artinien.*
2. *Toute chaîne strictement décroissante de sous-modules de M est finie.*
3. *${}_RM$ possède la condition minimale i.e. tout ensemble non vide de sous ensembles de M admet un élément minimal.*

Remarque 2.1.4. Les analogues des deux propositions ci-dessus sont évidemment aussi vraies pour des modules à droite.

Exercices 2.1.5.
1. L'anneau $\mathbb{Z}$ est il noethérien? artinien?
2. Montrer que l'anneau $\begin{pmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}$ est noethérien à droite mais pas à gauche.
3. Montrer qu'un anneau artinien intègre est un corps.

4. Montrer qu'un endomorphisme injectif d'un module artinien est un automorphisme.

Le théorème suivant porte le nom de théorème de la base d'Hilbert.

Théorème 2.1.6. *Si R est un anneau noethérien à droite (resp. à gauhe), il en est de même pour $R[X]$. En particulier si k est un corps alors $k[x_1,\dots,x_n]$ est noethérien.*

Démonstration. Soit I un idéal à droite de $R[X]$. On va montrer que I est finiment engendré. On pose

$$\forall n \in \mathbb{N}, I_n := \{\text{coefficients dominants des polynomes de } I \text{ de degre } n\} \cup \{0\}.$$

Il est clair que pour tout $n \in \mathbb{N}$, I_n est un idéal à droite de R. Puisque $f(X) \in I$ implique $f(X)X \in I$, on a

$$I_0 \subseteq I_1 \subseteq I_2 \cdots \subseteq I_n \subseteq \dots$$

Par conséquent il existe $l \in \mathbb{N}$ tel que $I_r = I_{r+1}$ si $r \geq l$. Pour $0 \leq i \leq l$ soient $a_{i1},a_{i2},\dots,a_{in_i}$ des générateurs de l'idéal à droite I_i et pour $1 \leq j \leq n_i$, $f_{ij} \in I$ des polynômes de degré i dont le coefficient dominant est a_{ij}. On montre par induction que $I = \sum f_{ij}R[X]$. Soit $f(X) \in I$ on pose $d := \deg(f)$ et on note $a \in I_d$ le coefficient dominant de f. Si $d = 0$ alors $f = a \in \sum a_{0i}R \subseteq \sum f_{0i}R[X]$. Si $d > 0$ on distingue 2 cas:

Si $d > l$ alors que $a \in I_d = I_l$ et on écrit $a = \sum a_{li}r_i$. Le polynôme $g(X) = f(X) - \sum f_{li}r_iX^{d-l}$ est un polynôme de I dont le degré est strictement inférieur à d, l'hypothèse d'induction permet alors de conclure.

Si $d \leq l$ $a \in I_d$ donc on peut écrire $a = \sum a_{dj}s_j$ et le polynôme $g(X) = f(X) - \sum f_{dj}s_j$ appartient à I et est de degré strictement inférieur à d.... □

Proposition 2.1.7. *Soit ${}_RM$ un R-module et un N un sous module de M. ${}_RM$ est noethérien (resp. artinien) si et seulement si N et M/N le sont.*

Démonstration. Il est clair que si M est noethérien alors N et M/N le sont aussi. Réciproquement supposons N et M/N noethériens et soit $(M)_i$ une chaîne ascendante de sous modules de M. Il existe $l \in \mathbb{N}$ tel que $M_i \cap N = M_{i+1} \cap N$ et $M_{i+1} + N = M_i + N$ pour $i \geq l$. Pour un tel i, si $x \in M_{i+1} \subseteq M_{i+1} + N = M_i + N$ on écrit $x = y + z$, où $y \in M_i$ et $z \in N$. Donc $z = x - y \in N \cap M_{i+1} = N \cap M_i$ et on conclut $x = y + z \in M_i$. □

Proposition 2.1.8. *a) Soient ${}_RM$ et ${}_RN$ deux R-modules à gauche noethériens. $M \oplus N$ est aussi noethérien.*

b) Tout module à gauche ${}_RM$ finiment engendré sur un anneau noethérien à gauche est noethérien.

Démonstration. a) On a $\frac{M\oplus N}{N} \cong M$. La proposition précédente 2.1.7 permet alors de conclure.

b) On écrit $M = \sum_{i=1}^{n} Rx_i$ et on considère le morphisme de R-modules: $\varphi : R^n \longrightarrow M$ défini par $\varphi((r_1,\dots,r_n)) = \sum r_i x_i$. On a $M \cong R^n/ker\varphi$. L'affirmation a) ci-dessus montre que le module R^n est noéthérien à gauche et il en est donc de même de M. $\square$

Définitions 2.1.9. 1. Une série de composition pour un module ${}_RM$ est une suite de sous modules de M :

$$\{0\} = M_0 \subset M_1 \subset \cdots \subset M_n = M.$$

telle que chaque facteur M_{i+1}/M_i est un module simple. Ces facteurs sont appelés les facteurs de composition. Un module est de longueur fini s'il admet une série de composition. La longueur de la suite ci-dessus est n et est appelée la longueur de composition.

2. Si $N_0 \subseteq N_1 \subseteq N_2 ... \subseteq N_m$ est une suite de sous modules d'un module M, on appelle raffinement de cette suite toute suite obtenue a partir de celle-là en introduisant un nombre fini de nouveaux sous modules.
3. deux suites de sous modules $0 \subseteq L_1 \subseteq L_2 ... \subseteq L_s = M$ et $0 \subseteq M_1 \subseteq M_2 ... \subseteq M_n = M$ sont dites équivalentes si $s = n$ et s'il existe une permutation $\sigma \in \mathcal{S}_n$ telle que $M_{i+1}/M_i \cong L_{\sigma(i)+1}/L_{\sigma(i)}$.

Quand un module admet une série de composition ses différentes chaînes de composition ont même longueur et cela débouche sur la notion de longueur pour ce module. Rappelons le lemme suivant (loi modulaire) dont on laisse la démonstration en exercice :

Lemma 2.1.10. *Soit M un module et A,B,C, des sous modules de M tels que $A \subseteq C$. Alors*

$$A + (B \cap C) = (A + B) \cap C$$

Commençons par le lemme de Zassenhaus :

Lemma 2.1.11. *Soit M un module et $N' \subseteq N$ $L' \subseteq L$ des sous modules d'un module M. Alors :*

$$\frac{N' + (L \cap N)}{N' + (L' \cap N)} \cong \frac{N \cap L}{(N' \cap L) + (N \cap L')} \cong \frac{L' + N \cap L}{L' + N' \cap L}.$$

Démonstration. $\frac{N'+(L\cap N)}{N'+(L'\cap N)} \cong \frac{N'+(L'\cap N)+(L\cap N)}{N'+(L'\cap N)} \cong \frac{(L\cap N)}{(N'+(L'\cap N))\cap(L\cap N)}$. En utilisant le lemme 2.1.10 on obtient $\frac{(L\cap N)}{(N'+(L'\cap N))\cap(L\cap N)} \cong \frac{(L\cap N)}{(L'\cap N)+(N'\cap(L\cap N))} \cong \frac{N\cap L}{(N'\cap L)+(N\cap L')}$. $\square$

Théorème 2.1.12. *Si*

$$N = L_0 \subseteq L_1 \subseteq L_2 ... \subseteq L_s = L$$

et

$$N = N_0 \subseteq N_1 \subseteq N_2 ... \subseteq N_m = L$$

sont des suites de sous modules d'un même module M, ces suites admettent des raffinements équivalents.

Démonstration. Il s'agit en fait d'introduire des sous modules L_{ij} définis de la manière suivante :

$$L_{ij} := (N_j \cap L_{i+1}) + L_i \qquad i = 0, \ldots, s-1 \quad j = 0, \ldots, m.$$

On obtient ainsi une chaîne de sous modules :

$$N = L_{00} \subseteq L_{01} \subseteq L_{O2} \subseteq \cdots \subseteq L_{0m} = L_1 \subseteq L_{11} \subseteq \cdots \subseteq L_{s-1\,m} = L_s = L$$

De même on introduit les sous modules :

$$N_{ij} = (N_{i+1} \cap L_j) + N_i \qquad i = 0, \ldots, m-1 \quad j = 0, \ldots, s$$

On obtient ainsi une deuxième chaîne de sous modules :

$$N = N_{00} \subseteq N_{01} \subseteq \cdots \subseteq N_{0s} = N_1 \subseteq \cdots \subseteq N_{m-1\,s} = N_m = L$$

Le lemme 2.1.11 montre que $L_{i\,j+1}/L_{ij} \cong N_{j\,i+1}/N_{ji}$. Ceci montre que les deux raffinements obtenus sont équivalents. □

On en déduit le théorème de Jordan-Hölder :

Théorème 2.1.13. *Si un module M admet une série de composition alors toute chaîne de sous-modules sans répétition admet un raffinement en une série de composition. En particulier, toutes les séries de composition de M ont même longueur.*

Notation 2.1.14. Si M admet une série de compositio, on notera $l(M)$ la longueur d'une série de composition. $l(M)$ est indépendant de la série de composition choisie, $l(M)$ ne dépend que de M.

La proposition suivante justifie le traitement des modules de longueur fini dans cette section.

Proposition 2.1.15. *Pour tout module M les affirmations suivantes sont équivalentes :*

1. *M possède une série de composition.*
2. *Toute chaîne de sous modules dans M sans répétition peut être raffinée en une série de composition.*
3. *M est à la fois noethérien et artinien.*

Démonstration. (1) $\Longrightarrow$ (2) Ceci se déduit du théorème 2.1.13.
(2) $\Longrightarrow$ (3) Si on considère une chaîne strictement croissante de sous modules, elle peut être, par hypothèse, raffinée en une série de composition, qui est clairement finie. la chaîne originale l'était donc aussi. Ceci montre dons que M est noethérien. De même on montre que M est artinien.
(3) $\Longrightarrow$ (1) Soit M_1 un sous module maximal de M ensuite, si $M_1 \neq 0$, soit M_2 un sous module maximal de M_1, On continue de cette manière ... Les quotients obtenus sont clairement simples et le processus s'arrête car le module M est artinien. □

Exercice 2.1.16.

Montrer que l'anneau $\begin{pmatrix} \mathbb{Q} & \mathbb{R} \\ 0 & \mathbb{R} \end{pmatrix}$ est artinien à droite mais pas à gauche. (Aide : construire une série de composition à droite)

Proposition 2.1.17. *Soit ${}_RA$ un R-module à gauche et ${}_RB$ un R-sous module de A. On a :*

$$l(A) = l(B) + l(A/B)$$

Exemple 2.1.18. Soit $m = p_1 \dots p_s$ la décomposition de $m \in \mathbb{N}$ en produit de nombres premiers. la suite

$$\mathbb{Z}/(m) \supseteqq (p_1)/(m) \supseteqq (p_1p_2)/(m) \supseteqq \cdots \supseteqq 0$$

est une série de composition.

Notons aussi le résultat suivant :

Proposition 2.1.19. *Tout sous-module propre d'un module ${}_RM$ finiment engendré est plongeable dans un sous module maximal.*

Démonstration. Soit $M = Rx_1 + Rx_2 + \cdots + Rx_n$ un module finiment engendré et N un sous module propre de M. On considère la famille $\mathcal{C}$ des sous-modules propres de M qui contiennent N. Le fait que M soit finiment engendré permet de conclure qu'une union croissante de modules propres est encore propre. Le lemme de Zorn permet alors de conclure que cette famille admet un élément maximal N'. Il est clair que N' est alors un sous-module maximal. □

Corollaire 2.1.20. *Tout idéal à droite (resp. à gauche) d'un anneau est contenu dans un idéal à droite (resp. à gauche) maximal.*

Démonstration. Il suffit de rappeler que ${}_RR$ est finiment engendré car $1 \in R$. □

2.2 Radical de Jacobson

Définition 2.2.1. Soit R un anneau, l'intersection des idéaux maximaux à gauche de R est appelé le radical de Jacobson de R et est noté $Jac(R)$. On dit qu'un anneau est semi-primitif si $Jac(R) = 0$.

Lemma 2.2.2. *Pour tout $y \in R$, les affirmations suivantes sont équivalentes:*

1. $y \in Jac(R)$
2. $1 - xy$ *est inversible à gauche pour tout* $x \in R$.
3. $yM = 0$ *pour tout module simple à gauche* M.
4. $1 - xyz$ *est inversible pour tout* $x,z \in R$.

Démonstration. □

Corollaire 2.2.3.

1. $Jac(R) = \cap annM$ *où* M *parcourt l'ensemble des modules à gauche simples. En particulier,* $Jac(R)$ *est un idéal de* R.
2. $Jac(R)$ *est le plus grand idéal à gauche* I *tel que* $1 + I \subseteq U(R)$.
3. *Les radicaux de Jacobson à gauche et à droite coincident.*

Exercices 2.2.4.

1. Montrer que si I est un idéal de R contenu dans $Jac(R)$ alors $Jac(R/I) = Jac(R)/I$. En particulier $R/Jac(R)$ est semiprimitif.
2. Montrer qu'un R-module à gauche simple M est aussi un $R/Jac(R)$-module à gauche simple et réciproquement.
3. Montrer qu'un élément $x \in R$ est inversible à gauche dans Rsi et seulement si $\overline{x} \in R/Jac(R)$ est inversible à gauche.
4. Montrer que $Jac(R)$ contient tout ideéal à gauche (resp. à droite) nil (Un sous ensemble $X \subseteq R$ est dit nil si pour tout $x \in X$, il existe un naturel $n \in \mathbb{N}$ tel que $x^n = 0$).
5. Si D est un corps calculer $Jac(D[[x]])$.
6. Si D est un corps calculer $Jac(T_2(D))$ où $T_2(D)$ est l'anneau des matrices triangulaires supérieures 2×2 sur D.

Théorème 2.2.5. *Si R est artinien à gauche (resp. à droite), $Jac(R)$ est le plus grand idéal à gauche nilpotent. C'est aussi le plus grand idéal à droite nilpotent.*

Démonstration. L'exercice ci-dessus montre que tout idéal nil, et à fortiori tout idéal nilpotent, est contenu dans le radical de Jacobson. Il suffit donc de montrer que ce dernier est nilpotent lorsque l'anneau est artinien. Posons $J := Jac(R)$. La condition de chaîne décroissante montre qu'il existe $l \in \mathbb{N}$ tel que $J^l = J^{l+1} = ...$ Montrons que $J^l = 0$ Si $J^l \neq 0$, parmi les idéaux $\mathfrak{A}$ tels que $J^l\mathfrak{A} \neq 0$, choississons en un qui est minimal: $\mathfrak{A}_0$. Soit $a \in \mathfrak{A}_0$ tel que tel que $J^l a \neq 0$. On a alors

$$J^l.(J^l a) = J^{2l} a = J^l a \neq 0\,.$$

La minimalité de $\mathfrak{A}_0$ implique alors que $J^l a = \mathfrak{A}_0$. En particulier il existe $y \in J^l \subseteq Jac(R)$ tel que $a = ya$. Mais puisque $(1-y)$ est inversible (2.2.2), on conclut que $a = 0$. Cette contradiction montre que $Jac(R)$ est nilpotent.

□

Corollaire 2.2.6. *Dans un anneau artinien à gauche, tout idéal à gauche nil est nilpotent.*

Le théorème suivant est dû à Amitsur:

Théorème 2.2.7. *Si R est un anneau sans idéaux nils non nuls, alors $R[t]$ est semiprimitif.*

Ce théorème peut être précisé (Amitsur) :

Théorème 2.2.8. *Soit R un anneau et $T = \{t_i \,|\, i \in I\}$ un ensemble non vide d'indéterminées (commutatives). Alors, $Jac(R[T]) = N[T]$ où $N = R \cap Jac(R)$.*

Terminons ce paragraphe par le résultat suivant connu sous le nom de lemme de Nakayama

Proposition 2.2.9. *Soit L un idéal à gauche de R. Les affirmations suivantes sont équivalentes:*

i) $L \subseteq Jac(R)$

ii) Pour tout R-module à gauche finiment engendré M, $LM = M$ implique $M = 0$.

iii) Pour tout sous R-module à gauche N d'un R-module à gauche M tel que M/N est finiment engendré $N + LM = M$ implique $N = M$.

Démonstration. i) $\Longrightarrow$ ii) Supposons $M \neq 0$ et parmi tous les sous modules propres (i.e. $\neq M$) de M le lemme de Zorn montre que l'on peut en trouver un maximal N (car M est finiment engendré). En particulier, le module M/N est simple et donc $L.(M/N) = 0$, c'est-à-dire $L.M \subseteq N$. En particulier $L.M \neq M$.

ii) $\Longrightarrow$ iii) Il suffit d'appliquer ii) au module quotient M/N

iii) $\Longrightarrow$ i) Supposons qu'un élément $y \in L$ but $y \notin Jac(R)$. Alors $y \notin M$ pour un certain idéal à gauche maximal M de R. On a $M + L = R$ donc, à fortiori, $M + L.R = R$ et *iii)* montre que $M = R$, une contradiction. □

Exercices 2.2.10. 1. Soit R un anneau. Montrer que les affirmation suivantes sont équivalentes :

i) Pour tout $a \in R$, il existe un $x \in R$ tel que tel que $a = axa$.

ii) Tout idéal principal à gauche est engendré par un idempotent.

iii) Tout idéal principal à gauche est est un sommant direct de ${}_R R$.

iV) Tout idéal à gauche finiment engendré est engendré par un idempotent.

V) Tout idéal à gauche finiment engendré est un sommant direct de ${}_R R$.

Un anneau satisfaisant aux conditions équivalentes ci-dessus est dit régulier de Von Neumann.

2. Montrer qu'un anneau régulier de Von Neumann est semi-primitif.
3. Montrer qu'un anneau R est régulier de von Neumann si et seulement si pour tout idéal à droite I et tout idéal à gauche J de R on a $IJ = I \cap J$.

2.3 Autres radicaux

Définitions 2.3.1. 1. Un idéal propre I d'un anneau R est premier si A,B sont des idéaux de R tels que $AB \subseteq P$ alors $A \subseteq P$ ou $B \subseteq P$. Remarquer qu'un idéal premier doit être propre (i.e. $\neq R$).

2. Un idéal I de R est dit semi-premier si pour tout idéal J de R, $J^2 \subseteq I$ implique $J \subseteq I$.
3. Un anneau R est dit premier (resp. semi-premier) si $\{0\}$ est un idéal premier (resp. semi-premier).
4. Un idéal (bilatère) P est dit primitif à droite si P est l'annulateur d'un module à droite simple.
5. Un R-module à droite est fidèle si $ann_R M = 0$ (i.e. si $Mr = 0$ implique $r = 0$).
6. Un anneau R est dit primitif à droite si 0 est un idéal primitif à droite i.e. s'il existe un R-module à droite M tel que $ann_R M = 0$.

Proposition 2.3.2. *Soit P un idéal d'un anneau R, les affirmations suivantes sont équivalentes:*

1. *P est un idéal premier.*
2. *Pour a,$b \in R$, $(a)(b) \subseteq P$ implique $a \in P$ ou $b \in P$.*
3. *Pour a,$b \in R$, $aRb \subseteq P$ implique $a \in P$ ou $b \in P$.*
4. *Si des idéaux à gauche A,B de R sont tels que $AB \subseteq P$, alors $A \subseteq P$ ou $B \subseteq P$.*
5. *Si des idéaux à droite A,B de R sont tels que $AB \subseteq P$, alors $A \subseteq P$ ou $B \subseteq P$.*

Exemples 2.3.3. 1. Un anneau commutatif est premier si et seulement si il est intègre.

2. Un anneau de matrices $M_n(R)$ sur un anneau premier R est un anneau premier.
3. Si R est un anneau premier et si σ est un automorphisme de R et δ est une σ-dérivation, alors $R[x;\sigma,\delta]$ est un anneau premier.
4. Tout ideal maximal $\mathcal{M}$ est premier.
5. Tout idéal primitif est premier.
6. $T_2(R)$ n'est pas premier.

Proposition 2.3.4. *Tout idéal premier contient un idéal premier minimal.*

Démonstration. Soit P un idéal premier d'un anneau R et $\mathcal{P}$ l'ensemble des idéaux premiers de R contenus dans P. On ordonne partiellement $\mathcal{P}$ via $Q' \preceq Q$ ssi $Q' \supseteq Q$ pour $PQ', Q \in \mathcal{P}$. On peut utiliser le lemme de Zorn a condition de montrer que toute chaîne dans $\mathcal{P}$ admet une borne supérieure. Soit donc $\mathcal{C}$ une telle chaîne. L'ensemble $Q := \cap_{C\in\mathcal{C}} C$ est un idéal de R inclus à P. Montrons que c'est un idéal premier : Soit donc $x,y \in R$ tels que $xRy \subseteq Q$ mais $x \notin Q$. Alors $x \notin P'$ pour un certain idéal $P' \in \mathcal{C}$. Remarquons que P' étant premier et $xRy \subseteq Q \subseteq P'$, on a $y \in P'$. Pour tout $P'' \in \mathcal{C}$ on a soit $P'' \subseteq P'$ soit $P' \subseteq P''$. Dans le premier cas on a $x \notin P''$ et $xRy \subseteq Q \subseteq P''$ donc $y \in P''$. Dans le second cas on a $y \in P' \subseteq P''$ donc on a à nouveau $y \in P''$. P'' étant quelconque dans $\mathcal{C}$ on conclut $y \in Q$ et donc Q est bien un idéal premier. Il est clair que $Q \in \mathcal{P}$ est une borne supérieure pour $\mathcal{C}$. Le lemme de Zorn s'applique et fournit un élément maximal dans $\mathcal{P}$ et cet élément est un idéal premier minimal de R.

□

Théorème 2.3.5. *Dans un anneau noethérien à droite (resp. à gauche), il existe un nombre fini d'idéaux premiers minimaux et il existe un produit fini d'idéaux premiers minimaux qui est nul.*

Démonstration. Il suffit de montrer qu'il existe des idéaux premiers $P_1, \dots, P_n$ de R tels que $P_1 P_2 \cdots P_n = 0$ (justifier). Supposons qu'aucun produit d'idéaux premiers de R ne soit nul. Soit Z l'ensemble des idéaux de R qui ne contiennent pas un produit fini d'idéaux premiers. L'idéal nul étant dans Z, on a $Z \neq \emptyset$. L'hypothèse de noethériennité montre qu'il existe un élément maximal $M \in Z$. Aucun produit fini d'idéaux premiers n'est contenu dans M ($M \in Z$) mais tout idéal non nul contenant M contient un produit fini d'idéaux prmiers (maximalité de M dans Z). En particulier M lui même n'est pas premier donc il existe des idéaux I,J de R tels que $(I+M)(J+M) \subseteq M$ et $M \subsetneq I+M, M \subsetneq J+M$. La maximalité de M montre qu'il existe des idéaux premiers $P_1, \dots, P_n$ et $Q_1, \dots, Q_l$ tels que $P_1 \cdots P_n \subseteq I+M$ et $Q_1 \cdots Q_l \subseteq J+M$. On conclut que $P_1 \cdots P_n Q_1 \cdots Q_l \subseteq M$ ce qui contredit... □

Définitions 2.3.6.

1. Un ensemble non vide $S \subseteq R$ est un m-système si pour tout couple $(a,b) \in S^2$ il existe $r \in R$ tel que $arb \in S$.
2. Soit I un idéal d'un anneau R. On note
$$\sqrt{I} := \{s \in R |\text{ tout } m-\text{systeme contenant } s \text{ rencontre } I\}$$
3. $\sqrt{0}$ est noté $radR$ et est appelé le radical premier de R.

Proposition 2.3.7. *1. Un idéal $P \subseteq R$ est premier si et seulement si $R \backslash P$ est un m-système.*

2. *Soit $S \subseteq R$ un m-système et soit P un idéal maximal parmi les idéaux de R disjoints de S. Alors P est un idéal premier.*
3. *Si I est un idéal alors $\sqrt{I} \subseteq \{s \in R | s^n \in I$ pour un certain $n \geq 1\}$. Si R est commutatif, l'égalité est vérifiée.*

Démonstration. 1. Ceci est une conséquence immédiate de la caractérisation (3) donnée en 2.3.2.

2. Supposons $a \notin P$ et $b \notin P$ mais $(a)(b) \subseteq P$. Il exite $s \in P + (a)$ et $s' \in P + (b)$ (maximalité de P). Soit $r \in R$ tel que $srs' \in S$, on a alors $srs' \in (P+(a))R(P+(b)) \subseteq P+(a(b)) \subseteq P$. Cette contradiction montre que P est premier.
3. L'inclusion est évidente puisque les puissances de s forment un m-système. Supposons maintenant que R soit commutatif, et soit $s \in R$ tel que $s^n \in I$. Soit S un m-système contenant s. Il existe donc $r \in R$ tel que $s^n r \in S$. Donc S rencontre I en $s^n r$ et $s \in \sqrt{I}$.

□

Théorème 2.3.8. *Soit I un idéal d'un anneau R.*

1. *$\sqrt{I}$ est l'intersection des idéaux premiers de R contenant I.*
2. *$\sqrt{I}$ est un idéal de R.*
3. *$Rad(R)$ est l'intersection de tous les idéaux premiers de R.*
4. *$Rad(R/Rad(R)) = 0$.*
5. *$Rad(R)$ est un idéal nil.*
6. *$Rad(R) \subseteq Jac(R)$.*

Démonstration. 1) Soit $s \in \sqrt{I}$ et P un idéal premier contenant I. Le m-système $R \setminus P$ ne peut contenir s (sinon il rencontre I et donc aussi P). On a donc $s \in P$.
Réciproquement si $s \notin \sqrt{I}$. Il existe donc un m-système S contenant s qui est disjoint de . Le lemme de Zorn montre qu'il existe un idéal $P \supseteq I$ qui est maximal parmi les idéaux de R disjoints de S. P est un idéal premier et $s \notin P$.
2) est clair d'après 1).
3) C'est une conséquence évidente de 2.3.7 3).
4) On sait que $Jac(R)$ contient tous les idéaux nils(Cf. 2.2.4). □

Définition 2.3.9. On appelle n-système un sous ensemble N de R tel que si $a \in N$, il existe un $r \in R$ tel que $ara \in N$.

Lemma 2.3.10. *Si $a \in R$ est un élément d'un n-système N, montrer qu'il existe un m-système $M \subseteq N$ tel que $a \in M$.*

Démonstration. Il suffit de définir $M := \{a_1, a_2, \dots\}$ via $a_1 = a, a_2 = a_1 r_1 a_1, a_3 = a_2 r_2 a_2, \dots, a_{i+1} = a_i r_i a_i, \dots$ où les $r_i \in R$ sont tels que $a_i \in N$ pour tout $i \geq 1$. On vérifie alors que M est un m-système, il est clairement contenu dans N. □

Exercices 2.3.11. 1. Soit I un idéal d'un anneau R. Montrer que les affirmations suivantes sont équivalentes :

   (a) I est semi-premier.
   (b) Pour $a \in R$, $(a)^2 \subseteq I$ implique $a \in I$.
   (c) Pour $a \in R$, $aRa \subseteq I$ implique $a \in I$.
   (d) Pour tout idéal à gauche A de R, $A^2 \subseteq I$ implique $A \subseteq I$.
   (e) Pour tout idéal à droite A de R, $A^2 \subseteq I$ implique $A \subseteq I$.
   (f) I est une intersection d'idéaux premiers.
   (g) $I = \sqrt{I}$.

2. Montrer que les affirmations suivantes sont équivalentes:
   (a) R est un anneau semi-premier.
   (b) $rad(R) = 0$.
   (c) R ne possède aucun ideal bilatère non nul nilpotent.
   (d) R ne possède aucun idéal à gauche non nul nilpotent.

3. Montrer qu'un anneau primitif à droite est premier.

Théorème 2.3.12. *Soit R un anneau. Alors :*

1. $Rad(R[t]) = rad(R)[t]$.
2. *Pour tout* $n \geq 1$, $Rad(M_N(R)) = M_n(Rad(R))$.

Lemma 2.3.13. *1. Si A est un idéal à droite nil et B un idéal bilatère nil de R, $A + B$ est un idéal à gauche nil.*

2. *La somme de de tous les idéaux (bilatères) nils est un idéal nil. C'est le plus grand idéal nil de R.*

Définition 2.3.14. On note $Nil(R)$ la somme des idéaux bilatères nils. C'est le radical nil supérieur.

Remarques 2.3.15. La conjecture de Koethe affirme que la somme de deux idéaux à gauche nils est encore un idéal nil. Cette conjecture date de 1930 et reste ouverte à ce jour. De nombreuses formulations équivalentes en ont été données et elle est vraie dans de nombreuses classes d'anneaux (par ex. noethériens ou à I.P.). Des résultats récents ont été obtenus pour des questions proches de cette conjecture (par exemple A. Smoktunowitch a donné un exemple d'un anneau nil R tel que $R[x]$ est non nil. Cet exemple est à rapprocher de celui donné par Golod et Shafarevitch (1964) d'une algèbre nil non localement nilpotente). A titre indicatif mentionnnons, dans le théorème suivant, quelques affirmations équivalentes à la conjecture de Koethe :

Théorème 2.3.16. *Les affirmations suivantes sont équivalentes :*

1. *La somme de deux idéaux à gauche nil d'un anneau R est un idéal nil.*
2. $Jac(R[t]) = Nil(R)[t]$.
3. *Si R est nil alors $M_2(R)$ est aussi nil.*

Terminons cette section par le

Corollaire 2.3.17. *Si R est un anneau artinien à droite (resp. à gauche), alors $Nil(R) = Jac(R)$.*

Chapitre 3

Anneaux semi-simples

On reprend et développe ici le premier chapitre des notes du cours consacré à la théorie des représentations.

3.1 Semi-simplicité

Définition 3.1.1. Soit R un anneau (unitaire) et $0 \neq_R M$ R-module.

1. $0 \neq M$ est simple si les seuls sous-modules de M sont $\{0\}$ et M.
2. ${}_R M$ est semi simple si tout R-sous module N de M est un sommant direct, i.e. s'il existe ${}_R N'$ tel que $N \oplus N' = M$.

Proposition 3.1.2. *Si M est un module semi-simple tout sous module de M est aussi semi-simple. Tout module quotient M/N, où N est un sous module de M, est aussi semi-simple.*

Démonstration. Soit N est un sous module de M et $X \subseteq N$ un sous module de N. La semi-simplicité de M montre qu'il existe un sous module U de M tel que $X \oplus U = M$. Puisque $X \subseteq N$ la loi modulaire (2.1.10) montre que

$$N = N \cap M = N \cap (X \oplus U) = X + (N \cap U)$$

En fait, cette dernière somme est directe car $N \cap U \subseteq U$. Ainsi X est un sommant direct de N et N est semi-simple.
Si N est un sous module de M, la semi simplicité de M implique que N est un sommant direct de M, i.e. il existe n' tel que $M = N \oplus N'$ et donc $M/N \cong N'$. Ce qui précède montre que le sous module N' est semi simple, il en est donc de même de M/N. □

Exemples 3.1.3. Les $\mathbb{Z}$ modules simples sont les groupes abéliens simples. Ce sont donc les groupes $\mathbb{Z}/p\mathbb{Z}$, où p est premier. Les $\mathbb{Z}$ modules semi-simples sont donc des sommes directes de ces modules. En particulier, le théorème chinois montre que $\mathbb{Z}/(n\mathbb{Z})$ est semi-simple dès que n est sans carré.

Lemma 3.1.4. *Tout module semi-simple non nul contient un sous module simple.*

Démonstration. Soit $0 \neq m \in M$ et $Rm \cong R/L$ où $L = ann_R m$ est un idéal à gauche. Soit I un idéal à gauche maximal contenant L (2.1.20). Alors I/L est un sous-module maximal de R/L. L'isomorphisme $R/L \cong Rm$ applique I/L sur Im qui est donc un sous module maximal de Rm. Puisque M est semi-simple $M = Im \oplus P$ pour un certain sous-module P. On a alors

$$Rm = Im \oplus (P \cap Rm) .$$

Puisque Im est un sous module maximal de Rm, il est clair que $P \cap Rm$ est un module simple; c'est donc un sous module simple de M.

□

Lemma 3.1.5. *Soit $M = \sum_{i \in I} M_i$ une somme non nécessairement directe de sous modules simples. Alors il existe un sous ensemble $J \subseteq I$ tel que $M = \oplus_{j \in J} M_j$.*

Démonstration. On considère $\mathcal{F} := \{E \subseteq I \mid \sum_{i \in E} M_i$ est une somme directe$\}$. Bien sur pour tout $i \in I, \{i\} \in \mathcal{F}$. En particulier, $\mathcal{F} \neq \emptyset$. On montre que $\mathcal{F}$ est un inductif: Soit $(I_\lambda)_{\lambda \in \Lambda}$ une chaîne dans $\mathcal{F}$. Montrons que $J = \cup_{\lambda \in \Lambda} I_\lambda$ est aussi un élément de $\mathcal{F}$: si $j_0 \in J$ et $x \in M_{j_0} \cap \sum_{i \in J \setminus \{j_0\}} M_i$, alors $x = x_{i_1} + x_{i_2} + ... + x_{i_l} \in M_{j_0}$ où $i_j \in J \setminus \{j_0\}$ et $x_{i_j} \in M_{i_j}$. Il existe $\mu \in \Lambda$ tel que $\{j_0, i_1, \ldots, i_l\} \subseteq I_\mu$. Mais alors $\sum_{s \in I_\mu} M_s$ est une somme directe donc $x = 0$. On conclut que la somme $\sum_{j \in J} M_j$ est directe et donc que $J \in \mathcal{F}$. Le lemme de Zorn montre qu'il existe $K \subseteq I$ maximal tel que $\sum_{k \in K} M_k$ est directe. Montrons maintenant que pour tout $i \in I, M_i \subseteq \sum_{k \in K} M_k$; M_i étant simple on a $M_i \cap \sum_{k \in K} M_k$ est soit le module nul soit égal à M_i. Mais la première possibilité contredit la maximalité de K... On doit donc avoir $M_i \cap \sum_{k \in K} M_k = M_i$ ce qui montre que $M_i \subseteq \sum_{j \in J} M_j$. Ainsi $M = \sum_{i \in I} M_i = \oplus_{k \in K} M_k$ □

Théorème 3.1.6. *Soit ${}_R M$ un R-module à gauche. Les affiramtions suivantes sont équivalentes :*

1. *M est semi-simple.*
2. *M est la somme d'une famille de sous modules simples.*
3. *M est la somme directe d'une famille de sous modules simples.*

Démonstration. 1) $\Rightarrow$ 2) Soit M_1 la somme des sous modules simples de M, $M = M_1 \oplus M_2$. Si $M_2 \neq 0$, le lemme 3.1.4 montre M_2 contient un sous module simple ce qui contredit la définition de M_1.

2) $\Rightarrow$ 3) c'est une conséquence imméditate du lemme 3.1.5.

3) $\Rightarrow$ 1) Supposons $M = \oplus_{i \in I} M_i$, M_i simple et soit $N < M$ $(N \neq M)$. On considère $\mathcal{F} := \{J \subseteq I \mid \oplus_{j \in J} M_j \cap N = 0\}$. □

On aura besoin du résultat suivant, connu sous le nom de lemme de Schur :

Proposition 3.1.7. *Si $_RM$ est un R-module simple, $End_R(M)$ est un corps.*

Démonstration. Il suffit de noter que tout le noyau d'un endomorphisme non nul est un sous module propre de M, puisque M est simple on doit donc avoir un noyau nul. De même puisque l'image d'un endomorphisme non nul est un sous module non nul, on conclut que tout endomorphisme doit être surjectif. □

3.2 Théorème de Wedderburn

On a besoin de quelques résultats relatifs aux homomorphismes entre somme directes de modules. Si R est un anneau, $n \geq 1$ et M est un R-module, on note $M^{(n)}$ le module $M \oplus M \oplus \cdots \oplus M$ où figure n facteurs M.

Soit A une k algèbre (k un anneau commutatif), $M_1, \ldots, M_n$ et $N_1, \ldots, N_s$ des A-modules à droite. On considère H l'ensemble des matrices $s \times n$ dont les entrées sont des morphismes de A-modules $f_{ij} : M_j \longrightarrow N_i$. On munit H d'une structure de k-module via

$$(f_{ij}) + (g_{ij}) = (f_{ij} + g_{ij})$$

$$\alpha(f_{ij}) = (\alpha f_{ij}) , \alpha \in k$$

Si $n = s$ et $N_i = M_i$ pour tout $i = 1, \ldots, n$ alors H est muni d'une structure de k-algèbre via

$$((f_{ij})(g_{ij}))_{ij} = (\sum_{k=1}^{n} f_{ik} g_{kj})$$

Lemma 3.2.1. *Avec les définitions précédentes*

1. *H est un k-module isomorphe à $Hom_A(\oplus M_j, \oplus N_i)$.*
2. *Si $n = s$, et $N_i = M_i$ pour $i = 1, \ldots, n$ alors H est une k-algèbre isopmorphe à $End_A(\oplus_{j=1}^{n} M_j)$.*

Démonstration. 1) Il est facile de vérifier que H est un k-module. On considère

$$\varphi : Hom_A(\oplus M_j, \oplus N_i) \longrightarrow H : f \mapsto (p_i^N f q_j^M)_{ij}$$

Où $q_j^M : M_j \longrightarrow \oplus_{i=1}^{n} M_l$ est l'injection canonique et $p_i^N : \oplus N_i \longrightarrow N_i$ est la projection canonique. On montre que φ est un morphisme de k-modules. (exercice).

Montrons que φ est injective : si $\varphi(f) = 0$ alors $p_i^N f q_j^M = 0$ pour tout (i,j). En remarquant que $\sum_i q_i^M p_i^M = id_{\oplus M_i}$ on a, pour $x \in \oplus M_j$, $f(x) = f((\sum_j q_j^M p_j^M)(x)) = \sum_j f(q_j^M(p_j^M(x))) = \sum_{ij}(q_i^N p_i^N f q_j^M p_j^M)(x) = 0$ Donc $f \in ker\varphi \Longrightarrow f = 0$.

Montrons que φ est surjective : Soit $(f_{ij} \in H)$ Posons $f = \sum_{ij} q_i^N f_{ij} p_j^M$ on a $\varphi(f) = (p_k^N f q_l^M)_{kl} = (p_k^N (\sum_{ij} q_i^N f_{ij} p_j^M) q_l^M)_{kl}$ et en remarquant que $p_j^M q_l^M = \delta_{jl} id_{M_l}$, on a $\varphi(f) = (p_k^N \sum q_i^N f_{il} id_{M_l})_{kl} = \cdots = (f_{kl})$ Donc φ est surjective.
2) Laissée au lecteur. □

Corollaire 3.2.2. *Soit R un anneau et M,M_1,M_2,...,M_n des R-modules à droite.*

1.
$$End_R(M^{(n)}) \cong M_n(End_R(M)) \quad .$$

2. *Si pour $i \neq j, Hom_R(M_i,M_j) = 0$, alors*
$$End_R(\bigoplus_{i=1}^{n} M_i) \cong \prod_{i=1}^{n} End_R(M_i) \quad .$$

Les isomorphismes étant des isomorphismes d'anneaux.

Voici maintenant un résultat fondamental,classique et très facile à démontrer.

Lemma 3.2.3. *(Lemme de Schur)*

Soient M_1 et M_2 des R-modules à gauche simples.

1. *Si $M := M_1 = M_2$, alors $End_R(M)$ est un corps.*
2. *Si $M_1 \ncong M_2$, alors $Hom_R(M_1,M_2) = 0$.*

Démonstration. Pour la preuve il suffit de se rappeler le fait que le noyau et l'image d'un morphisme sont des sous-modules et les seuls sous modules d'un module simple... □

Remarque Si $M_2 \overset{\phi}{\cong} M_1$, alors $Hom_R(M_1,M_2)$ est aussi un corps pour le produit défini par $f.g := f \circ \phi \circ g$...(exercice).

Définition 3.2.4. Un anneau R est semi-simple à droite si le R-module R_R est semi-simple.

Remarque 3.2.5. On verra bientôt que R_R est semi-simple si et seulement si ${}_RR$ est semi-simple.

Lemma 3.2.6. *Soit R un anneau semi-simple à droite. Un module M_R est simple si et seulement si M_R est isomorphe à un idéal à droite minimal de R.*

Démonstration. Un idéal à droite minimal est toujours simple. Réciproquement si R_R est semi simple et M_R est simple alors il existe un idéal à droite maximal $\mathcal{M}$ de R tel que $M_R \cong R/\mathcal{M}$ Puisque R_R est semi-simple, on a $R = \mathcal{M} \oplus I$ et I est alors un idéal à droite minimal de R. On a en outre $M_R \cong R/\mathcal{M} \cong I$. □

Théorème 3.2.7. *(théorème d'Artin Wedderburn)*

Soit R un anneau, les assertions suivantes sont équivalentes :

1. *R_R est semi-simple.*
2. *Tout R-module simple à droite est semi-simple.*
3. *Tout idéal à droite de R est un facteur direct de R.*
4. *$R \cong \prod_{i=1}^{t} M_{n_i}(K_i)$, où les K_i sont des corps (éventuellemnt non commutatifs) et l'isomorphisme est un isomorphise d'anneaux.*

Démonstration. 1) $\Longrightarrow$ 2) Si R_R est semi-simple, tout R-module à droite libre est semi-simple. Or tout R-module àdroite est quotient d'un R-module à droite libre. L'exercice **??** permet alors de conclure.

2) $\Longrightarrow$ 1) C'est clair !

1) $\Longleftrightarrow$ 3) C'est aussi clair !!

1) $\Longrightarrow$ 4) R_R est par hypothèse une somme directe de R-module simple : $R_R = \bigoplus_{\lambda\in\Lambda} S_\lambda$ où les S_λ sont simples. On peut donc écrire $1 = \sum_{i=1}^{l} e_{\lambda_i}$ et on a $S_{\lambda_i} = e_{\lambda_i}R$. Pour tout $a \in R$ on a alors $a = 1.a = \sum_{i=1}^{l} e_{\lambda_i}a$, ce qui montre que l'on a en fait $R_R = \bigoplus_{i=1}^{l} S_{\lambda_i} = \bigoplus_{i=1}^{t}(\bigoplus_{k=1}^{n_i} S_{k,i})$ avec $\sum_{i=1}^{t} n_i = l$ et où l'on a regroupé les modules simples isomorphes : $S_{ki} \cong S_{k'i}$, pour tout k,k' et $S_{ki} \ncong S_{k'j}$ si $i \neq j$. On a en particulier $Hom_R(S_{ki},S_{k'j}) = 0$ si $i \neq j$. En posant $M_i := \oplus_{k=1}^{n_i} S_{ki}$, on a $Hom_R(M_i,M_j) = 0$ si $i \neq j$ et $R \cong End(R_R) \cong End_R(\oplus M_i) \cong \prod_{i=1}^{t} End_R(M_i) \cong \prod_{i=1}^{t} M_{n_i}(End_R S_{1i})$. Le lemme de Schur montre alors que les $K_i = End_R S_{1i}$ sont des corps.

4) $\Longrightarrow$ 1) Fixons $i \in \{1,\ldots,t\}$.. On a $M_{n_i}(K_i) = \oplus_{k=1}^{n_i} e_{kk}^{(i)} M_{n_i}(K_i)$ où $e_{kk}^{(i)}$ désigne la matrice à coefficients dans K_i ayant des 0 partout sauf en position kk où elle vaut 1. On montre que $I_k := e_{kk}^{(i)} M_{n_i}(K_i)$ est un $M_{n_i}(K_i)$-module simple et on en déduit facilement que $M_{n_i}(K_i)$ est un anneau semi-simple (il est simple mais tous les anneaux simples ne sont pas semi-simples...donner un exemple) et que $R = \prod_{i=1}^{t} M_{n_i}(K_i)$ est un anneau semi-simple. □

Remarques 3.2.8.
1. La condition 4) du théorème ci-dessus est symétrique on conclut donc que R_R est semi-simple si et seulement si ${}_RR$ est semi-simple.
2. Tout anneau semi-simple est artinien (à gauche et à droite).

Le corollaire suivant est immédiat mais imporaant notamment en théorie des représentations de groupes...

Corollaire 3.2.9. *Soit $R \cong \prod_{i=1}^{t} M_{n_i}(K_i)$ un anneau semi-simple alors, à isomorphisme près, R possède exactement t modules simples à droite (resp. à gauche) qui sont tous des idéaux à droite (resp. à gauche) minimaux de R*

Démonstration. Si V est un R-module simple à droite on a $Hom_R(R,V) \neq 0$ (en effet $V \cong R/\mathcal{M}$ pour un certain idéal à droite maximal $\mathcal{M}$ de R). En reprenant les notations de la preuve du théorème 3.2.7, on a $Hom(S_{k,i}V) \neq 0$ pour un certain (k,i). Donc $S_{1,i} \cong S_{k,i} \cong V$ par le lemme de Schur 3.2.3. □

Théorème 3.2.10. *Soit R un anneau artinien à droite ou à gauche alors R est simple si et seulement si $R \cong M_n(D)$ pour un certain corps D et un ceratain $n \geq 1$.*

Démonstration. A_A est artinien, soit S un idéal à droite minimal de A . Alors AS esun idéal bilatère et donc $AS = \sum aS = A$. Pour $a \in A$, l'application $S \longrightarrow aS : s \mapsto as$ est un épimorphisme de A-mosules à droite. Puisque S est simple, on a soit $as = 0$ soit $aS \approxeq$. Puisque S est simple on a soit $aS = 0$ soit $aS \cong S$. Par conséquent A_A est une somme de modules simples i.e. A_A est semi-simple. Donc $A \cong \prod M_{n_i}(K_i)$ mais puisque A n'a pas d'idéaux bilatères... □

Remarques 3.2.11. 1. Si R est une k-algèbre semi-simple finidimensionnelle alors $R \cong M_{n_1}(D_1) \times \dots M_{n_l}(D_l)$ et $D_i = End(A_i)$ o où ${}_RA_i$ est simple. Donc D_i a aussi une structure de k-algèbre. En fait D_i est un corps qui est une k-algèbre de dimension finie.

Si k est algébriquement clos et R est semi-simple alors $R \cong M_{n_1}(k) \times \dots \times M_{n_s}(k)$.

On va encore donner deux caractérisations des anneaux semi-simples. Donnons d'abord un petit lemme (du a Brauer):

Lemma 3.2.12. *Si I_R est un idéal à droite minimal d'un anneau R, alors soit $I^2 = 0$, soit $I = eR$ où $e^2 = e \in R$.*

Démonstration. Si $I^2 \neq 0$ soit $a \in I$ tel que $aI \neq 0$. On a $0 \neq aI \subseteq I$ et la minimalité de I montre que $aI = I$. Il existe donc $e \in I$ tel que $ae = a$ et $ae^2 = ae = a$, ce qui donne $a(e^2 - e) = 0$. On introduit donc $J := \{i \in I | ai = 0\}$. J est un idéal à droite de R strictement contenu dans I (car $aI \neq 0$), la minimalité de I implique donc que $J = 0$. En particulier $e^2 = e \in I$. Puisque $a \neq 0$, on a $e \neq 0$ et $0 \neq eR \subseteq I$ montre que $eR = I$. □

Théorème 3.2.13. *Un anneau R est semi-simple si et seulement si R est artinien à droite (resp. à gauche) et $Jac(R) = 0$ (i.e. R est artinien à droite et semi-primitif).*

Démonstration. Supposons R semi-simple et écrivons R comme somme directe de R sous modules simples à droite (i.e; d'idéaux à droite minimaux): $R_R = \oplus_{k \in K} I_k$. Puisque $1_R \in R$, il est facile de constater que cette somme est en fait finie: $R_R = \oplus_{k=1}^{n} I_k$. On a alors une série de composition :$\{0\} \subseteq I_1 \subseteq I_1 \oplus I_2 \subseteq \dots \subseteq R$. On conclut que R est artinien et noethérien à droite. D'après 2.2.5, $J := Jac(R)$ est nilpotent et la semi-simplicité de R montre qu'il existe J' un idéal à droite tel que $R = J \oplus J'$. en écrivant $1 = u + v$ avec $u \in J$ et $v \in J'$ on

a $u^2 = u - vu$ mais $vu \in J \cap J' = \{0\}$ et donc $u^2 = u$. Puisque J est nilpotent montre alors que $u = 0$ et $1 = v \in J'$. On conclut que $J' = R$ et $J = 0$.
Réciproquement, supposons R_R artinien et $Jac(R) = 0$. D'après 2.2.5 R ne possède pas d'idéal à droite nilpotent, le lemme montre donc que si I est un idéal à droite minimal alors $I = eR$ où $e = e^2 \in R$. Montrons que tout idéal à droite de R est une somme d'idéaux à droite minimaux. Si ce n'est pas le cas on choisit P minimal dans la famille non vide des idéaux à droite de R qui ne sont pas somme d'idéaux à droite minimaux (artiniennité). $0 \neq P$, soit I un idéal à droite minimal de R contenu dans P. On a vu que $I = eR$ pour un certain idempotent $E \in I$. Soit $I' = (1-e)R)$, on a $R = eR \oplus I'$ et la loi modulaire permet d'écrire $P = eR \oplus (I' \cap P)$. La minimalité de P montre alors que $I' \cap P$ est une somme d'iéaux à droite minimaux mais alors puisque $P = I \oplus (I' \cap P)$, il en est de même de P. Cette contradiction montre que tout idéal à droite de R est une somme d'déaux à droite minimaux de R, c-à-d de sous modules simples. Ceci montre que R est semi-simple. □

Rappelons qu'un anneau est semipremier s'il ne possède aucun idéal bilatère nilpotent non nul. Le lemme suivant est une conséquence immédiate de 3.2.12

Lemma 3.2.14. *Si I est un idéal à gauche minimal d'un anneau semipremier R, alors $I = Re$ où e est un idempotent dans I (i.e. $e^2 = e$)*

Théorème 3.2.15. *Soit R un anneau, les affirmations suivantes sont équivalentes :*

1. *R est semi-simple.*
2. *R est semipremier et artinien à gauche.*
3. *R est semi-premier et saisfait la condition de chaine descendante sur les idéaux principaux à gauche.*

Démonstration. Elle a été donnée au cours et sera transcrite plus tard. □

Une autre caractérisation des algèbres semi-simples fait appel à la notion de module projectif :

Définition 3.2.16. Un R-module à droite P_R est projectif si pour tout morphisme surjectif $A \xrightarrow{\beta} B \longrightarrow 0$ de R-modules à droite et pour tout morphisme $\alpha : P \mapsto B$ il existe un morphisme $\gamma : P \longrightarrow A$ tel que $\alpha = \beta\gamma$.

Théorème 3.2.17. *R est semi-simple si et seulement si tout R-module à droite (resp. à gauche) est projectif.*

Exercice 3.2.18.
1. Montrer qu'un anneau artinien sans élément nilpotent non nul et sans idempotet central non trivial (i.e. $\neq 0{,}1$) est un corps.
2. Soit $R = M_n(D)$ où D est un corps. Montrer que R possède un nombre fini d'idéaux à droite si et seulement si soit $n = 1$ soit D est un corps fini.

3. Soit K un corps commutatif et $R = \begin{pmatrix} k & k \\ 0 & k \end{pmatrix}$. Si $e = e_{1,1}$, montrer que $End(eR)$ est un corps mais que eR n'est pas un R-module simple.

3.3 Théorème de densité de Chevalley-Jacobson

Un théorème important de la théorie des anneaux est le théorème de densité qui affirme que les anneaux primitifs sont les anneaux denses de transformations linéaires d'espaces vectoriels sur des corps (Jacobson-Chevalley).

Si M_R est un module simple alors le lemme de Schur montre que $D := End_R M$ est un corps et M est un (D,R)-bimodule. En particulier, pour $r \in R$, l'application $d_r : M \longrightarrow M$ définie par $d_r(m) = mr$ est un élément de $End_D M$. Ceci permet de définir un morphisme d'anneaux $\varphi : R \longrightarrow End_D M : r \mapsto d_r$. Le noyau de ce morphisme est $Ann_R M$. En particulier si R est primitif à droite et M_R est un module simple et fidèle à droite alors R est plongé dans $End_D M$. Le théorème de Chevalley Jacobson va montrer que R est "assez gros" dans $End_D M$.

Définition 3.3.1. Soit D un corps et M un D-espace vectoriel à gauche sur D. Un sous-anneau R de $End_D M$ est un anneau dense de transformations linéaires si pour toute famille finie D-indépendante $x_1, \dots, x_n$ de M et pour tout sous ensemble $\{y_1, \dots, y_n\} \subseteq M$, il existe un élément $r \in R$ tel que $x_i r = y_i$ pour tout $i = 1, \dots, n$. (On a noté $x_i r$ l'action de r sur x_i)

Théorème 3.3.2. *R est primitif à droite. On note M le module simple et fidèle et $D = End_R M$. R est un anneau dense de transformations linéaires sur ${}_D M$. De plus, si R est artinien à droite, alors $dim_D M < \infty$ et $R \cong M_n(D)$.*

Démonstration. La preuve a été donnée au cours et sera transcrite plus tard. □

3.4 Théorème d'Hopkins-Levitzki et théorème de Maschke

Définition 3.4.1. Un anneau R est semi-primaire si $Jac(R)$ est nilpotent et $R/Jac(R)$ est semi-simple.

Exercice 3.4.2.
1. Tout anneau artnien à droite (resp. à gauche) est semi-primaire.
2. L'anneau $\begin{pmatrix} \mathbb{Q} & \mathbb{R} \\ 0 & \mathbb{Q} \end{pmatrix}$ est semi-primaire mais n'est pas artnien.

Théorème 3.4.3. *R un anneau semi-primaire ${}_R M$ un R-moduke, les affirmations suivantes sont équivalentes:*

1. *M est noethérien.*

2. *M est artinien.*
3. *M possède une série de composition.*

Démonstration. On sait déjà que (3) $\Longrightarrow$ (1) et (3) $\Longrightarrow$ (2). Il suffit donc de montrer que (1) $\Longrightarrow$ (3) et (2) $\Longrightarrow$ (3) si on suppose que R est semi-primaire. On traite ces deux implications simultanément. Supposons que M soit artinien ou noethérien. Soit $n \in \mathbb{N}$ tel que $J^n = 0$. Considérons la suite :

$$0 = J^n M \subseteq J^{n-1} M \dots JM \subseteq M$$

Il suffit de montrer que chaque facteur J^i/J^{i+1} possède une série de composition. Chacun de ces facteurs est noethérien ou artinien sur $\overline{R}$ (Justifier). Or $\overline{R}$ est semi-simple, donc $J^iM/J^{i+1}M$ est une somme directe finie de $\overline{R}$ modules simples, ce qui montre que $J^iM/J^{i+1}M$ possède une suite de composition. □

Corollaire 3.4.4. *Un anneau artinien à gauche est noethérien à gauche. Tout module M finiment engendré sur un anneau artinien à gauche possède une série de composition.*

Soit k un corps commutatif et G un groupe. On considère les applications de G à coefficients dans k à support fini : $kG := \{f : G \longrightarrow k \,|\, |\{x \in G | f(x) \neq 0\}| < \infty\}$. L'addition et la multipliaction étant définie via ces mêmes opérations sur k. Si $f \in kG$ on écrit généralement f sous la forme $f = \sum_{g \in supp(f)} f(g)g$, i.e. $kG = \{\sum_{finie} \alpha_x x\}$. l'addition de deux éléments $f = \sum \alpha_x x \quad g = \sum \beta_y y$ de kG écrits sous cette forme se fait alors en sommant les coeffcients correspondant à $sup(f) \cup sup(g)$ la multiplication se fait de la manière suivante (vérifier qu'elle correspond bien à la multiplication ponctuelle des fonctions)

$$f.g = \sum_{x \in supp(f), y \in supp(g))} \alpha_x \beta_y xy = \sum_z (\sum_{(x,y)|xy=z} \alpha_x \beta_y) z$$

On vérifie que kG est une algèbre appelée algèbre du groupe G sur le corps k. Cette algèbre est intimement liée aux représentations du groupe G. Le théorème suivant montre qu'elle est très souvent semisimple, sa structure sera donc donnée par le théorème d'Artin-Wedderburn.

Théorème 3.4.5. *(théorème de Maschke).*

Soit G ungroupe fini et k un corps commutatif. kG est semisimple si et seulement si $chark$ ne divise pas $|G|$.

3.5 Applications à la théorie des représentations

On va rapidement montrer comment le théorème de Maschke et le théorème de Wedderburn-Artin permettent d'obtenir pas mal de résultats sur la théorie des représentations des groupes finis.

Définitions 3.5.1.

1. Soit V un k-espace vectoriel de dimension finie. Une représentation linéaire d'un groupe G dans V est la donnée d'un morphisme de groupes :

$$\rho : G \longrightarrow GL(V)\,.$$

2. $dimV$ est appelé le degré de la représentation.
3. Si on fixe une base $\mathcal{B}$ de l'espace vectoriel V de dimension n, on obtient une représentation matricielle de G dans $GL_n(k)$ plus explicitement : si $\rho : G \longrightarrow GL(V)$ est une représentation de G, l'application $\mu : G \longrightarrow GL_n(k) : g \mapsto M_{\mathcal{B}}(\rho(g))$ est la représentation matricielle associée.
4. Une représentation sur un espace vectoriel est dite fidèle si l' application ρ ci-dessus est injective. On dit aussi que G agit fidèlement sur V.

Remarques 3.5.2. La donnée d'une représentation d'un groupe G correspond à la donnée d'une action du groupe G sur V : il suffit de noter $g.v = \rho(g)(v)$. On dit aussi que V est un G-module (voir plus loin pour une explication de cette dénomination). On étudiera uniquement les représentations des groupes finis. On considèrera généralement des représentations sur des $\mathbb{C}$-vectoriels de dimension finies (i.e. $k = \mathbb{C}$, dans la définition ci-dessus).

Exemples 3.5.3.

1. La représentaion triviale d'un groupe G sur un vectoriel V est celle qui correspond à l'application triviale :

$$\rho : G \longrightarrow Gl(V) : g \mapsto Id_V\,.$$

Cette représentation n'est évidemment pas fidèle.

2. La représentation régulière reg d'un groupe fini G : on considère le $\mathbb{C}$-vectoriel $V = \oplus_{g \in G} \mathbb{C} e_g$. L'ensemble $\{e_g \,|\, g \in G\}$ est une bas de V. Si $g \in G$, la multiplication par g à gauche définit une permutation sur les éléments de G et $reg(g) \in GL_{\mathbb{C}}(V)$ est défini par $reg(g)(e_h) := e_{gh}$ pour $h \in G$. C'est une représentation fidèle de degré $|G|$.
3. La représentation du groupe $\mathcal{S}_3$ via les idométries d'un triangle équilatérale : On dessine un triangle équlatéral et on fixe un repère tel que les coordonnées des sommets A,B,C de ce triangle soient respectivement $(0,1)$,$(-\sqrt{3}/2, -1/2)$,$(\sqrt{3}/2, -1/2)$. On fait correspondre à la permutation $(1,2)$ la symétrie qui fixe A, et à la permutation $(1,2,3)$ la rotation qui applique A sur B. Puisque les permuations $(1,2)$ et $(1,2,3)$ engendrent $\mathcal{S}_3$ on en déduit une représentation ρ de $\mathcal{S}_3$ caractérisée par :

$$\rho((1,2)) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad \rho((1,2,3)) = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}$$

Cette représentation est fidèle et de degré 2.

On suppose dans la suite que $cark$ ne divise pas $|G|$ de façon à pouvoir appliquer le théorème de Maschke. On a alors $kG \cong \prod_{i=1}^{t} M_{n_i}(D_i)$ où D_i sont des corps. On rappelle que si k est algebriquement clos almos $D_i = k$ pour tout i.

Si $\rho : G \longrightarrow GL(V)$. est une représentation alors V est un kG module à gauche via : $\sum \alpha_g g.v = \sum \alpha_g \rho(g)(v)$.

Deux représentations ρ_1 et ρ_2 sont équivalentes si les k-vectoriels V_1 et V_2 qui leur correspondent sont isomorphes en tant que kG-modules à gauche.

Une représentation est irréductible si le kG-module correspondant est simple.

Le théorème de WA montre immédiatement que toute représentation est somme directe de représentations irréductibles.

Le corollaire 3.2.9 montre qu'il existe un nombre fini de représentations irréductibles d'un groupe fini. Ces représentations sont données par les idéaux minimaux à gauche des différents $M_{n_i}(D_i)$. Il y a donc t représentations irréductibles non équivalentes.

On appelle degré d'une représentation la dimension de l'espace vectoriel associé. Les degrés des représentations irréductibles sont données par les ideaux minimaux à gauche des $M_{n_i}(D_i)$ et sont donc de degré n_i et on a $\sum_{i=1}^{t} n_i^2 = |G|$.

Ceci n'est qu'un bref aperçu de la théorie des représentations. On trouvera quelques informations complémentaires dans le cours sur les représentations des groupes finis et bien sur dans la littérature mentionnée en bibliographie.

Chapitre 4

Anneaux quotients

4.1 Modules projectifs, injectifs et semi-simplicité

Cette section permettra de faire le lien avec le chapitre précédent et préparera les sections suivantes. Commençons par quelques définitions :

Définition 4.1.1. 1. Une suite de morphismes entre R-modules

$$A \xrightarrow{\varphi} B \xrightarrow{\psi} C$$

est exacte en B si $im(\varphi) = ker\psi$. En particulier, si $A = \{0\}$ ceci signifie que φ est injective et si $C = \{0\}$, cela signifie que ψ est injective.

2. Une suite exacte courte est une suite

$$0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$$

exacte en A,B,C. Une telle suite est scindée si et seulement si il existe un morphisme de R-modules $\nu : C \longrightarrow B$ tel que $\psi\nu = Id._C$

3. Un module P est projectif si pour tout diagramme de morphismes de R-modules tel que :

$$\begin{array}{ccc} & P & \\ & \downarrow g & \\ M \xrightarrow{f} & N & \longrightarrow 0 \end{array}$$

(où f est surjective), il existe un morphisme $h : P \longrightarrow M$ tel que $g = fh$.

4. Un module I est injectif si pour tout diagramme de morphismes de R-modules tel que :

$$\begin{array}{ccc} 0 \longrightarrow & A & \xrightarrow{f} B \\ & \downarrow g & \\ & I & \end{array}$$

(où f est injctive) il existe un morphisme $h : B \longrightarrow I$ tel que $g = hf$.

Exercices 4.1.2. 1. Une suite exacte courte

$$0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$$

est scindée si et seulement si il existe un morphisme $h : B \longrightarrow A$ tel que $h\varphi = Id_A$.

2. Si

$$0 \longrightarrow B \xrightarrow{\varphi} B' \xrightarrow{\psi} B''$$

est exacte alors

$$0 \longrightarrow Hom_R(A,B) \xrightarrow{\varphi'} Hom_R(A,B') \xrightarrow{\psi'} Hom_R(A,B'')$$

est exacte (on définira convenablement φ' et ψ').

3. Si

$$B \xrightarrow{\varphi} B' \xrightarrow{\psi} B'' \longrightarrow 0$$

est exacte alors la suite

$$0 \longrightarrow Hom_R(B'',A) \xrightarrow{\psi'} Hom_R(B',A) \xrightarrow{\varphi'} Hom_R(B,A)$$

est exacte (on définira convenablement φ' et ψ').

Lemma 4.1.3. *Soit P un R-module. Si P est libre ou si P est un sommant direct d'un module projectif alors P est projectif.*

Démonstration. On se donne un diagramme

$$\begin{array}{ccc} & P & \\ & \downarrow g & \\ M \xrightarrow{f} & N & \longrightarrow 0 \end{array}$$

où f est surjective et dans les deux cas on doit pouvoir le compléter...

Si P est libre, soit $\{l_i | i \in I\}$ une base de P. Puisque f est surjective, il existe des élémens $m_i \in M$ tels que $g(l_i) = f(m_i)$. On définit $h : P \longrightarrow M : l_i \mapsto m_i$...

Si P est un sommant direct d'un module projectif Q alors (exercice) il eixiste des apllications $\sigma : P \longrightarrow Q$ et $\tau : Q \longrightarrow P$ tels que $\tau\sigma = Id_P$.Puisque Q est projectif et $g\tau : Q \longrightarrow N$ on déduit qu'il existe $\gamma : Q \longrightarrow M$ tel que $f\gamma = g\tau$. On a alors $f(\gamma\sigma) = g(\tau\sigma) = g$ et donc $h = \gamma\sigma$ convient.

□

Exemples 4.1.4. 1. Si k est un corps tout k-module est libre donc projectif.

2. Soients m,n deux entiers premiers entre eux :$(m,n) = 1$. le théorème chinois montre que

$$\frac{\mathbb{Z}}{mn\mathbb{Z}} \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{n\mathbb{Z}}$$

On conclut que $\mathbb{Z}/m\mathbb{Z}$ est un $\mathbb{Z}/mn\mathbb{Z}$ module projectif.

3. Tout $\mathbb{Z}$-module projectif est libre (car tout sous groupe d'un groupe abélien libre est libre)
4. $\mathbb{Q}_{\mathbb{Z}}$ n'est pas projectif (puisqu'il n'est pas libre).
5. Tout module est quotient (=image homomorphe) d'un module projectif.

Proposition 4.1.5. *Soit R un anneau $_RP$ et $_RI$ des R-modules.*

A) Les affirmations suivantes sont équivalentes :

(a) P est projectif.

(b) Toute suite exacte courte

$$0 \longrightarrow A \longrightarrow B \xrightarrow{f} P \longrightarrow 0$$

se terminant par P est scindée.

(c) P est isomorphe à un sommant direct d'un module libre.

B) Les affirmations suivantes sont équivalentes :

(a) Toute suite exacte courte

$$0 \longrightarrow I \longrightarrow A \longrightarrow B \longrightarrow 0$$

commençant par I est scindée.

(b) I est injectif.

Démonstration. On démontre uniquement le A) (a) $\Longrightarrow$ (b) La suite exacte résulte en un diagramme :

$$\begin{array}{l} \qquad P \\ \qquad \downarrow 1_P \\ B \xrightarrow{f} P \longrightarrow 0 \end{array}$$

La projectivité de P montre qu'il existe une application $h : P \longrightarrow B$ telle que $fh = 1_P$...

(b) $\Longrightarrow$ (c)Tout module est un quotient d'un module libre, il existe donc une suite exacte courte

$$0 \longrightarrow M \xrightarrow{i} L \xrightarrow{g} P \longrightarrow 0$$

où L est un module libre. Cette suite est donc scindée c'est à dire qu'il existe un morphisme de modules h tel que $gh = id._P$. On remarque alors que $g(l - h(g(l))) = 0$ et, pour $l \in L$, on peut écrire $l = h(g(l)) + (l - h(g(l)))$. Ce qui montre que $L = i(M) + h(P)$. On vérifie facilement que cette somme est directe.

(c) $\Longrightarrow$ (a) Ceci est une conséquence du lemme 4.1.3. □

Théorème 4.1.6. *Soit R un anneau les affirmations suivantes sont équivalentes :*

1. *R est semi-simple.*

2. *Tout R-module est projectif.*
3. *Toute suite exacte courte de R-modules est scindée.*
4. *Tout R-module est injectif.*

Démonstration. Les équivalences 2) $\Leftrightarrow$ 3) et 3) $\Leftrightarrow$ 4) sont claires d'après le lemme 4.1.3.
Montrons que 1) $\Longrightarrow$ 2) Soit P un R-module. Il existe une suite exacte courte :

$$0 \longrightarrow M \xrightarrow{i} L \xrightarrow{g} P \longrightarrow 0$$

où L est un module libre. Puisque R est semi-simple, tous les R-modules sont semi-simples, en particulier L est semi-simple. On peut donc écrire : $L = i(M) \oplus M'$. La suite ci-dessus est donc scindée (si $j : L \longrightarrow M : l = i(m)+m' \mapsto m$, on a $ji = Id_M$). La projectivité de P en découle.
2) $\Longrightarrow$ 1) Supposons que tout module soit projectif. Si $N \subseteq M$ sont des R-modules on a $0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$ et la projectivité de M/N montre que cette suite exacte courte est scindée c-à-d. $M \cong N \oplus M/N$. Ceci montre que tout sous module d'un module en est un sommant direct. Donc tout R-module est semi-simple...

$\square$

Le théorème suivant porte le nom de critère de Baer :
Théorème 4.1.7. *Un R-module I_R est injectif si et seulement si pour tout idéal à droite $\mathcal{A}$ de R, tout morphisme $f : \mathcal{A} \longrightarrow I$ peut s'étendre en un morphisme $f' : R \longrightarrow I$.*

Démonstration. La condition est clairement nécessaire.
Réciproquement supposons qu'un module I possède cette condition d'extension et soit donné le diagramme suivant (où la ligne supérieure est une suite exacte)

$$\begin{array}{lll} 0 \longrightarrow & A & \xrightarrow{f} B \\ & \downarrow g & \\ & I & \end{array}$$

Considérons $\{(C,h) |\, A \subseteq C \subseteq B$ et $h \in Hom_R(C,I)$ est tel que $h|_A = g\}$. On munit cet ensemble d'un ordre partiel via $(C_1,h_1) \leq (C_2,h_2)$ si et seulement si $C_1 \subseteq C_2$ et $h_1 = h_2|_{C_1}$. Il est facile de voir, en utilisant le lemme de Zorn, que cette famille admet un élément maximal (C,h). Il reste à montrer que $C = B$.

Soit $b \in B$, posons $J := \{r \in R | ar \in C\}$. J est un idéal à droite de R et on définit un R-morphisme $\sigma : J \longrightarrow I : r \mapsto h(ar)$. Par hypothèse σ s'étend en $\sigma' : R \longrightarrow I$. On pose alors $h' : C + bR \longrightarrow I : c + br \mapsto h(c) + \sigma'(r)$. Montrons que h' est bien définie : si $c_1 + br_1 = c_2 + br_2$ où $c_1,c_2 \in C$ et $r_1,r_2 \in R$ alors $b(r_1 - r_2) = c_1 - c_2 \in C$. Donc $r_1 - r_2 \in J$ et $\sigma'(r_1) - \sigma'(r_2) = \sigma'(r_1 - r_2) = \sigma(r_1 - r_2) = h(b(r_1 - r_2)) = h(c_1 - c_2) = h(c_1) - h(c_2)$.

Donc $h(c_1) + \sigma'(r_1) = h(c_2) + \sigma'(r_2)$. Ce qui montre que h' est bien définie. Puisque $(C,h) \leq (C+bR,h')$, la minimalité de (C,h) montre que $b \in C$ et donc $C = B$. □

Exemple 4.1.8. Soit S un anneau intègre principal à droite et $0 \neq b \in S$ tel que $bS = Sb$. L'anneau $R = S/bS$ est tel que R_R est injectif (auto injectif à droite.) En effet si $\mathcal{A}$ est un ideal à droite de R alors $\mathcal{A} = aS/bS$ pour un certain $a \in S$. Le critère de Baer montre qu'il suffit de prouver que tout morphisme de modules à droite $h : \mathcal{A} \longrightarrow R$ peut s'étendre en un morhisme $h* : R \longrightarrow R$. Soit donc $h \in Hom_R(\mathcal{A},R)$ posons $h(\overline{a}) = \overline{s}$ et $b = ac$. On a $\overline{0} = h(\overline{0}) = h(\overline{b}) = h(\overline{ac}) = \overline{sc}$. Ce qui montre que $sc \in bS = Sb$. On peut donc écrire $sc = tb = tac$. Puisque S est intègre on a $s = ta$ et $h(\overline{a}) = \overline{s} = \overline{t}\overline{a}$. On étend alors h à R via $h(\overline{1}) = \overline{t}$.

Remarques 4.1.9. Considérons ce qui se passe dans le cas des idéaux principaux à droite.

a) Si I_R est un R-module et $a \in R$ $f \in Hom_R(aR,I)$ alors si $f(a) = u$ on doit avoir $ann_d(a) \subseteq ann(u)$ où $ann_d(a) = \{x \in R \mid ax = 0\}$.
Réciproquement si $u \in I$ et $a \in R$ sont tels que $ann_r(u) \subseteq ann(u)$, alors $f : aR \longrightarrow I : ar \mapsto ur$ est bien définie et $f \in Hom_R(aR,I)$. On peut donc établir une bijection entre $Hom_R(aR,I)$ et $\{u \in I | ann_d(a) \subset ann(u)\}$.

b) Si I_R est injectif, $a \in R$ et $u \in I$ tel que $ann_d(a) \subseteq ann(u)$ alors $f : aR \longrightarrow I : ar \mapsto ur$ peut s"étendre en $\overline{f} : R \longrightarrow I$ et $u = f(a) = \overline{f}(a) = \overline{f}(1)a \in Ia$. On peut donc conclure que si I_R est injectif alors il est divisible dans le sens précisé ci-dessous.

Définition 4.1.10. Un R-module I_R est divisible si pour tout $u \in I$ et pour tout $a \in R$ tel que $ann_d(a) \subseteq ann(u)$ on a $u \in Ia$ (u est divisible par a.)

On laisse en exercice la preuve de la proposition suivante :

Proposition 4.1.11. *Soit I_R un R-module. Les affirmations suivantes sont équivalentes :*

1. *I est un module divisible.*
2. *Pour tout $a \in R$, $ann_I(ann_d(a)) = Ia$.*
3. *Pour tout $r \in R$, pour tout $f \in Hom_R(aR,I)$, f s'étend à R.*

Exercices 4.1.12.
1. Montrer que si R est un anneau principal à droite alors tout module divisible est injectif.
2. Rappel : un anneau R est Von Neumann régulier si pour tout $a \in R$, $a \in aRa$. Montrer que R est Von Neumann régulier si et seulement si tout R-module à droite est divisible si et seulement si tout R-module cyclique à droite est divisible.

4.2 Enveloppe injective

Proposition 4.2.1. *Tout $\mathbb{Z}$-module se plonge dans un $\mathbb{Z}$-module injectif.*

Démonstration. Soit A un $\mathbb{Z}$-module. Il existe un $\mathbb{Z}$-module libre L et un B un sous module de L tel que $A \cong L/B$. $L \subseteq K$ où K est un $\mathbb{Q}$-vectoriel. Les $\mathbb{Z}$-modules K et K/B sont des $\mathbb{Z}$-modules divisibles (pourquoi?). On a donc $A = L/B \subseteq K/B$ qui est divisible et donc injectif puisque $\mathbb{Z}$ est principal. □

Lemma 4.2.2. *Soit R un anneau et D un groupe abélien divisible (i.e. un $\mathbb{Z}$-module injectif) et ${}_RL$ un R-module a gauche libre. $Hom_{\mathbb{Z}}(L,D)$ est un R-module à droite injectif.*

Démonstration. $Hom_{\mathbb{Z}}(L,D)$ est un R-module àd roite via

$$(f.r)(l) := f(rl) \quad \forall r \in R, \forall l \in L, \forall f \in Hom_{\mathbb{Z}}(L,D)$$

Soit $\{l_j \in L \,|\, j \in J\}$ une base de ${}_RL$, $\mathfrak{A}$ un idéal à droite de R et $\varphi : \mathfrak{A} \longrightarrow Hom_{\mathbb{Z}}(L,R) : a \mapsto \varphi_a$ un morphisme de R-modules à droite. Pour prouver que $Hom_{\mathbb{Z}}(L,R)$ est injectif à droite, il suffit, d'après le critère de Baer 4.1.7, de montreer que φ s'étend en un morphisme défini sur R. On considère $\mathfrak{A}L = \sum \mathfrak{A}l_j$ le sous module de L déterminé par $\mathfrak{A}$ et on défini $\sigma : \mathfrak{A}L \longrightarrow D : \sum_{j\in J} a_jl_j \mapsto \sum_{j\in J} \varphi_{a_j}(l_j)$. On vérifie que σ est un porphisme $\mathbb{Z}$-module et, puisque D est divisible, σ peut s'étendre en $\sigma^* : L \longrightarrow D$. On définit alors $\varphi^* : R \longrightarrow Hom_{\mathbb{Z}}(L,D) : r \mapsto \sigma^*.r$ (on utilise la structure de R-module à droite de $Hom_{\mathbb{Z}}(L,D)$). Il est facile de vérifier que φ^* est un morphisme de R-modules. Montrons que $\varphi^*|_{\mathfrak{A}} = \varphi$:
Soit $a \in \mathfrak{A}, j \in J, r \in R \varphi^*(a)(rl_j) = (\sigma^*)(a)(rl_j) = \sigma^*(arl_j) = \sigma(arl_j) = \varphi_a(rl_j)$ (rappelons que $ar \in \mathfrak{A}$). Ceci montre que φ^* étend bien φ à R et le critère de Baer permet de conclure. □

Théorème 4.2.3. *Tout R-module à droite se plonge dans un module injectif.*

Démonstration. Soit A_R un R-module à droite. D'après 4.2.1 on peut plonger A dans un $\mathbb{Z}$-module injectif M. On a (compléter les détails):

$$A \cong Hom_R(R,A) \subseteq Hom_{\mathbb{Z}}(R,A) \subseteq Hom_{\mathbb{Z}}(R,M)$$

De plus $Hom_{\mathbb{Z}}(R,M)$ est un R-module à droite injectif d'après 4.2.2. □

Donnons maintenant quelques propriétés des modules injectifs :

Proposition 4.2.4.
1. *Si I_R est un module injectif et si A est un sommant direct de I alors A est injecif.*
2. *Si $\{Q_i | i \in I\}$ est une famille de R-modules injectifs alors $\prod_{i\in I} Q_i$ est un R-module injectif.*
3. *Un R module I_R est injectif si et seulement si il est un sommant direct de tout module qui le contient.*

Démonstration. Les preuves sont faciles et on été données en cours...je les transcrirai plus tard...peut être ! □

Définition 4.2.5. Un sous module N_R d'un module M_R est essentiel si tout sous-module non nul de M intersecte N_R non trivialement. Si N est un sous-module essentiel de M on écrira $N \subseteq_e M$.

Proposition 4.2.6. *Un R-module M_R est injectif si et seulement si il ne possède pas d'extension essentielle propre.*

Démonstration. La condition est clairement nécessaire d'après 4.2.4 3).
Réciproquement supposons qu'un module N ne soit sous-module essentiel d'aucun module. Soit I un module injectif tel que $N \subseteq I$ (Cf. 4.2.3). Le lemme de Zorn montrte qu'il existe un module M tel que $N \subseteq M \subseteq I$ maximal tel que $N \cap M = \{0\}$. On a

$$N \cong \frac{N}{N \cap M} \cong \frac{N+M}{M} \subseteq \frac{I}{M}$$

Montrons que cette dernière inclusion est essentielle : Soit $0 \neq \frac{X}{M}$ un sous module de I/M. La maximalité de M montre que $X \cap N \neq 0$ et $X \cap N \nsubseteq M$ (puisque $N \cap M = \{0\}$) donc $M \subsetneq X \cap (N+M)$ et l'inclusion $\frac{N+M}{M} \subseteq \frac{I}{M}$ est bien essentielle. L'hypothèse faite sur $N \cong \frac{N+M}{M}$ montre que $I/M = \frac{N+M}{M}$, donc $N + M = I$ et on conclut que N est un sommant direct de Q, c'est à dire que N est injectif. $\square$

Théorème 4.2.7. *Tout module M_R possède une extension essentielle maximale.*

Démonstration. Soit I un module injectif contenant M (Cf. 4.2.3). On considère l'ensemble :

$$\{N \subseteq I \mid M \subseteq_e N \subseteq I\}$$

Que l'on ordonne par inclusion. Le lemme de Zorn permet de trouver un sous module E maximal tel que $M \subseteq_e E \subset I$. On doit montrer que E est essentiel maximal au dessus de M. Supposons qu'un module E' soit tel que $E \subseteq E'$ et $M \subseteq_e E'$ on a donc aussi $E \subseteq_e E'$. L'injectivité de I montre alors qu'il existe $g : E' \longrightarrow I$ qui étend le plongement de E dans I à E'. Donc $g|_E = Id.$ est injective et puisque M est essentiel dans E', on conclut que g est injective (sinon $0 \neq ker g \cap M \subseteq ker g \cap E = ker(g|_E)$). On a alors $M \subseteq_e E = g(E) \subseteq_e g(E') \subseteq I$. La maximalité de E montre que l'on doit avoir $E = g(E')$ et finalement $E = E'$ ce que l'on voulait montrer. $\square$

Remarque 4.2.8. On a en fait montrer que tout module injectif qui contient un module M contient aussi une extension essentielle maximale de M.

Théorème 4.2.9. *Soit $M_R \subseteq I_R$. Les affirmations suivantes sont équivalentes :*

1. *I est une extension essentielle maximale de M.*

2. *I est injectif et $M \subseteq_e I$.*
3. *I est une extension injective minimale de M.*

Démonstration. 1) $\Longrightarrow$ 2) La transitivité de l'essentialité et la condition 1) montre que I n'admet pas d'extension essentielle propre et 4.2.6 montre que I est un module injectif.
2) $\Longrightarrow$ 3) Soit I' un module injectif tel que $M \subseteq I' \subseteq I$. I' est un sommant direct de dans I (Cf. 4.2.4); on peut donc écrire $I = I' \oplus I''$ et puisque $M \subseteq I'$, on a $I'' \cap M = \{0\}$. Mais $M \subseteq_e I$ donc $I'' = 0$ et $I = I'$.
3) $\Longrightarrow$ 1) Supposons $M \subseteq I$ tel que I soit injectif minimal. La remarque qui précède ce théorème montre que I contient une extension essentielle maximale E de M. L'implication 1) $\Longrightarrow$ 2) ci-dessus montre que E est injectif et la minimalité de I montre que $E = I$. □

Définition 4.2.10. Le module I satisfaisant les propriétés équivalentes du théorème est appelé l'enveloppe injective de M et noté $E(M)$. Le corollaire suivant montre qu'il y a unicité de l'enveloppe injective.

Corollaire 4.2.11. *Soient I,I' deux enveloppes injectives d'un module M. Alors I et I' sont isomorphes et il existe un isomorphisme qui est l'identité sur M.*

Démonstration. La preuve est laissée, une fois encore, en exercice. □

Exercices 4.2.12.
1. Soit R un anneau commutatif intègre et K son corps des fractions.
   a) Montrer que si I est un idéal de R alors $Hom_R(I,K) \cong K$.
   b) Montrer que si M_K est un K-vectoriel à droite alors M_R est injectif.
   c) Montrer que $E(R) = K$.
2. Soient M_j, E_j des R-modules ($j \in J$).
   a) Montrer que $\oplus M_j \subseteq_e \oplus E_j$ ssi $M_j \subseteq_e E_j$ for all $j \in J$.
   b) Montrer que si $|J| < \infty$ then, $E(\oplus M_j) = \oplus E(M_j)$.

Terminons cette section avec une caractérisation des anneaux semi-simples. Pour cela on utilise la notion de socle :

Définition 4.2.13. Soit M un R-module, le socle de M, noté $soc(M)$ est la somme de tous les sous-modules simples de M. C'est donc le plus grand sous-module semi-simple contenu dans M . Soit $\alpha : M \longrightarrow N$ un morphisme de R-modules. Puisque l'image d'un module semi-simple par un morphisme est encore semi-simple, on a $\alpha(Soc(M)) \subseteq Soc(N)$

Lemma 4.2.14. *$Soc(R_R)$ est un idéal de R.*

Démonstration. □

Proposition 4.2.15. *Soit M un R-module. $Soc(M)$ est l'intersection des sous modules essentiels de M.*

Proposition 4.2.16. *Un R-module M est semi-simple si et seulement si il ne possède pas de sous-module propre essentiel.*

4.3 Anneau maximal de quotients

La notion, définie ci-dessous, de sous modules denses généralise celle de sous modules essentiels.

Définitions 4.3.1.
1. Si N_R est un sous module de M_R et $y \in M$ on définit $y^{-1}N = \{r \in R \,|\, yr \in N\}$.
2. Un sous module N d'un module M est dense si pour tout $y \in M$ et pour tout $x \in M \setminus \{0\}$ on a $xy^{-1}N \neq 0$ (i.e. pour tout $y \in M, ann_M(y^{-1}N) = 0$). On notera alors $N \subseteq_d M$.

Les idéaux à droite dense d'un anneau R joueront un role important (essentiel !) dans l'étude de l'anneau des quotients maximaux.

Exercices 4.3.2.

1. Si M_R et N_R sont des sous-modules d'un module L_R et $x \in L$, montrer que :
   a) $x^{-1}N$ est un idéal à droite de R.
   b) $x^{-1}(M \cap N) = (x^{-1}M) \cap (x^{-1}N)$.
2. Montrer qu'un sous module N d'un module M est essentiel si et seulement si pour tout $0 \neq m \in M$, $m.(m^{-1}N) \neq 0$.
3. Si $N \subseteq_d M$ alors $N \subseteq_e M$.
4. $\frac{p\mathbb{Z}}{p^{n+1}\mathbb{Z}}$ est essentiel mais n'est pas dense dans $\frac{\mathbb{Z}}{p^{n+1}\mathbb{Z}}$.
5. Soit R un anneau commutatif, K son corps des fractions et $\{v_i \,|\, i \in I\}$ une base d'un K-vectoriel V_K. Montrer que $W_R := \sum v_i R \subseteq_d V_R$.
6. Pour un idéal à à droite $\mathfrak{A} \subseteq R$ on a $\mathfrak{A} \subseteq_d R$ si et seulement si pour tout $y \in R$, $ann_g(y^{-1}\mathfrak{A}) = 0$.
7. Si $\mathfrak{A}$ est un idéal bilatère de R alors
$$\mathfrak{A} \subseteq_d R_R \text{ si et seulement si } ann_g(\mathfrak{A}) = 0.$$
8. Si $a \in Z(R)$, le centre de R, alors $aR \subseteq_d R_R$.
9. Si R est un idéal premeir alors tout idéal (bilatère) non nul est dense dans R_R et dans ${}_RR$.
10. Si D_R et D'_R sont des sous-modules denses d'un module M_R montrer que :
    a) Tout sous module de M contenant D est dense dans M.

b) Si $x \in M$, alors $x^{-1}M$ est dense dans M.
c) $D \cap D'$ est un sous module dense de M.

11. Soit $N \subseteq M$ des R-modules à droite. Montrer que les affirmations suivantes sont équivalentes :
   (a) $N \subseteq_d M$.
   (b) $Hom_R(M/N,E(M)) = 0$.
   (c) Pour tout sous module P tel que $N \subseteq P \subseteq M$, $Hom_R(P/N,M) = 0$.

Le lemme suivant nous sera utile...

Lemma 4.3.3. *Soit D un idéal à droite de R. Alors D est dense si et seulement si $0 = ann_E D := \{e \in E \mid eD = 0\}$.*

Démonstration. Supposons que D soit dense et soit $0 \neq e \in E$. Puisque $R \subseteq_e E$ il existe $x \in R$ tel que $ex \in R \backslash \{0\}$. Mais,puisque D est dense, $ann_g(x^{-1}D) = 0$, on a $ex.x^{-1}D \neq 0$. Or $x.x^{-1}D \subseteq D$ donc $eD \neq 0$.
Supposons que $ann_E(D) = 0$. Soit $x \in R$ et $a \in ann_g(x^{-1}D)$. On considère l'application $\sigma : D + xR \longrightarrow R \subseteq E : d + xr \mapsto ar$. σ est bien définie : si $d + xr = 0$, alors $xr \in D$, donc $r \in x^{-1}D$ et $ar = 0$. Puisque E est injectif et $D + xR \subseteq R$ donc σ s'étend en $\sigma* : R \longrightarrow E$ et on obtient alors $0 = \sigma(D) = \sigma^*(D) = \sigma^*(1)D$. Ceci montre que $\sigma^*(1) \in ann_E(D) = 0$. C'est pourquoi $\sigma^* = 0$. En particulier $\sigma = 0$ et $0 = \sigma(x) = a$. On conclut que $ann_g(x^{-1}D) = 0$ et donc que D est dense. □

Définition 4.3.4. Soit R un anneau, $E = E(R_R)$ son enveloppe injective, $H := End(E_R)$. E est ainsi un (H,R) bimodule. Le quotient maximal à droite de R est $Q := End({}_H E)$ on le note $Q^r_{max}(R)$.

Remarques 4.3.5.
E est un (H,Q)-bimodule, $R \subseteq Q = Q^r_{max}(R)$. Pour éviter les confusions on notera uR la copie de R_R incluse à E; On a donc $R \cong uR$ via $r \mapsto ur$ et $uR \subseteq_e E$.

Exemples 4.3.6.

1. Si R est un anneau commutatif intègre et K est son corps des fractions alors $Q_{max}(R) = K$.
2. Si R est auto-injectif alors $Q_{max}(R) = R$.

Lemma 4.3.7. *Avec les notations ci-dessus on a :*

1. *$E = Hu$.*
2. *L'application $Q \longrightarrow uQ : q \mapsto uq$ est un isomorphisme de Q-modules.*
3. *Si B_Q est un Q-module et $\beta : B \longrightarrow E$ est un morphisme de R-modules alors β est aussi un morphisme de Q-modules.*

Démonstration.

1) Let $e \in E$ and $\sigma : uR \longrightarrow E : ur \mapsto er$ est un morphisme de R-modules. Puisque E est injectif et $uR \subseteq E$, on peut étendre σ en morphisme de R-modules de E dans E i.e. il existe $h \in H$ tel que $h|_{uR} = \sigma$. On a donc $e = \sigma(u) = h(u) = h.u$ (structure de H-module à gauche de E). On conclut que $e \in Hu$.
2) L'application $\tau : Q \longrightarrow uQ : q \mapsto uq$ est un épimorphisme de Q-modules à droite. de plus, si $uq = 0$ alors $Eq = (Hu)q = 0$ et donc $q = 0$. Ceci montre que τ est un isomorphisme.
3) Soit $b \in B$. On définit $\psi_b : uQ \longrightarrow E : uq \mapsto \beta(bq) - \beta(b)q$. ψ_b est un R-morphisme. L'injectivité de E montre qu'il existe $h_b : E \longrightarrow E$ qui étend ψ_b. Donc $h_b \in H$. D'autre part, $h_b(u) = \psi_b(u) = 0$ et donc $\psi_b(uQ) = h_b(uQ) = h_b(u)Q = 0$ (rappelons que $Q = End({}_HE)$ ce qui signifie que l'action de Q commute avec celle de H). On en déduit $\beta(bq) = \beta(b)q$ pour tout $b \in B$ et $q \in Q$ i.e. β est un morphisme de Q-modules. □

Théorème 4.3.8. *Soit R un anneau, $E = E(R_R)$ et $Q = Q_{max}(R)$. Alors $E_Q \cong E(Q_Q)$ et $Q_{max}(Q) = Q$.*

Démonstration. Montrons que $E_Q \cong E(Q_Q)$. E est un Q-module à droite et $Q \cong uQ \subseteq E$ (l'isomorphisme étant un isomorphisme de Q-modules à droite). $uR \subseteq_e E$ (en tant que R-module à droite). Si $0 \neq X \subseteq E_Q$ alors $X \subseteq E_R$ et donc $X \cap uR \neq 0$. On en déduit que $uQ \subseteq_e E_Q$. Montrons que E_Q est injectif : Soient $A_Q \subseteq B_Q$ des Q-modules et $\varphi : A_Q \longrightarrow E_Q$ un morphisme de Q-modules. φ est aussi un morphisme de R-module à droite donc il existe $\psi : E_R \longrightarrow E_R$ tel que $\psi|_A = \varphi$ (car E_R est injectif). Le point 3) de 4.3.7 montre que ψ est en fait un morphisme de Q-modules.
Montrons maintenant que $Q_{max}(Q) = Q$. R est un sous anneau de Q. $End_Q(E_Q) \subseteq End_R(E_R) = H$. De plus $Q = End_HE$ et ${}_HE_Q$, donc tout élément de H définit un morphisme de E_Q par multiplication à gauche. On a donc finalement $End_Q(E_Q) = H$ et $Q_{max}(Q) = End_HE = Q$. □

On va donner une caractérisation abstraite, indépendante de $E(R_R)$, de l'anneau maximal des quotients. Tout d'abord notons le lemme suivant :

On note $\mathcal{D}(R)$ l'ensemble des idéaux à droite denses dans R.

Lemma 4.3.9. *Soit $q \in Q = Q_{max}(R)$ et soit $D' \in \mathcal{D}(R)$. Alors $D = \{r \in R \,|\, qr \in D'\}$ est aussi un idéal à droite dense de R.*

Démonstration. D est clairement un idéal à droite et il suffit d'après 4.3.3 de montrer que $ann_E(D) = 0$. Si $e \in E$ est tel que $eD = 0$ on définit $\varphi : uD' + uqR \longrightarrow E : ud' + uqr \mapsto er$. Montrons que φ est bien définie : si $ud' + uqr = 0$ alors le 4.3.7 (2) montre que $d' = -qr$ i.e. $r \in D$ et donc $er = 0$. φ est un morphisme de R-modules et l'injectivité de E_R implique que φ s'étend en un morphisme de $h \in End_R(E)$. D'autre part on a $\varphi(uD') = 0$, donc $(hu)D' = 0$ et,puisque D' est dense, 4.3.3 montre que $hu = 0$. Donc $e = h(uq) = (hu)q = 0$ et on conclut que $ann_E(D) = 0$. $\square$

Théorème 4.3.10. *L'anneau maximal des quotients $Q = Q_{max}(R_R)$ satisfait les propriétés suivantes :*

1. *$R \subseteq Q$ et $1_Q = 1_R$ (Q et R ont même unité).*
2. *Si $q \in Q$, alors il existe $D \in \mathcal{D}(R)$ tel que $qD \subseteq R$.*
3. *Si $q \in Q$ et $D \in \mathcal{D}(R)$, alors $qD = 0$ implique $q = 0$.*
4. *Si $D \in \mathcal{D}(R)$ et $\varphi : D \longrightarrow R$ est un morphisme de R-modules à droite, alors il existe $q \in Q$ tel que $\varphi d = qd$ pour tout $d \in D$.*

De plus, si Q' est un anneau satisfaisant ces quatre conditions, alors Q' est isomorphe à Q par un isomorphisme qui est l'identité sur R.

Démonstration. Montrons que Q possède ces propriétés. (1) est clair.
(2) Pour $x \in R$, $x^{-1}R = R$ et donc $ann_g(x^{-1}R) = 0$. ce qui montre que R_R est dense. Le lemme 4.3.9 montre alors $D = \{r \in R \,|\, qr \in R\}$ est un idéal dense et on a $qD \subseteq R$.
(3) Si $qD = 0$ alors $EqD = 0$ et donc $Eq = 0$ (4.3.3) et donc $Huq = 0$. Or $Id_E \in H$, et on obtient $uq = 0$ c'est à dire $q = 0$.
(4) Soit $\varphi : D \longrightarrow R$ donné. Posons $\varphi' : D \longrightarrow E : d \mapsto u\varphi(d)$. φ' est un morphisme de R-modules et l'injectivité de E montre qu'il s'étend en un R-morphisme $\varphi'' : R \longrightarrow E$. Remarquons que si $h \in H$ et $d \in D$, alors

$$h\varphi''(1)d = h\varphi''(d) = h\varphi'(d) = hu\varphi(d).$$

En particulier, Si $hu = 0$, alors $h\varphi"(1)D = 0$ et 4.3.3 implique que $h\varphi''(1) = 0$. On a $E = Hu$. L'application q définie par $(hu)q = h\varphi''(1)$ est bien définie. Donc q est un morphisme de H-modules de E, i.e. $q \in Q$ et pour tout $d \in D$, on a $huqd = h\varphi''(1)d = h\varphi''(d) = h\varphi'(d) = hu\varphi(d)$. Ceci montre que $E(qd - \varphi(d)) = 0$ et on obtient que $qd = \varphi(d)$.
Pour montrer l'unicité, supposons que $Q' \supseteq R$ satsisfasse aussi les conditions 1 à 4 ci-dessus. Soit $q \in Q$ et, grace à 2, soit $D \in \mathcal{D}(R)$ tel que $qD \subseteq R$. L'application $\sigma_q : D \longrightarrow R : d \mapsto qd$ est un morphisme de R-modules, donc 4 appliqué à Q' montre qu'il existe $q' \in Q'$ tel que $q'd = \sigma_q d = qd$ pour tout $d \in D$. En outre, 3 (appliqué a q') montre que, q étant fixé, q' est unique. D'autre part si on avait choisi un autre module dense D_1 tel que $qD_1 \subseteq R$ et si q'_1 était l'élément de Q' correspondant, on aurait $q'_1 d = qd = q'd$ pour tout $d \in D \cap D_1$. Or $D \cap D_1$ est aussi dense et on a donc $q'_1 = q'$ par l'hypothèse 3. En d'autres termes q' est déterminé de manière unique par q et l'équation $q'd = qd$ pour tout $d \in D$ (indépendance par rapport au choix de D). On a donc une application bien définie : $\psi : Q \longrightarrow Q' : q \mapsto q'$et $\psi|_R = Id_R$. On montre que cette application est en fait un isomorphisme d'anneaux. $\square$

4.4 Anneau total des quotients, théorèmes de Goldie

Définitions 4.4.1. 1. On dit qu'un anneau Q est un anneau de quotients à droite de R s'il existe T un ensemble multiplicatif d'éléments réguliers de R tel que :

   (a) Q est un anneau contenant R $(1_Q = 1_R)$.

   (b) Tout élément de T est inversible dans Q.

   (c) Tout élément de Q est de la forme rt^{-1} où $r \in R$ et $t \in T$.

   On dit que Q est un localisé à droite de R par rapport à T.

2. Un ensemble multiplicatif d'éléments réguliers de R est un ensmble de dénominateurs à droite si pour tout $r \in R$ et $t \in T$, il existe $r_1 \in R$ et $t_1 \in T$ tel que $rt_1 = tr_1$.

Lemma 4.4.2. *Soit T un ensemble multiplicatif d'éléments réguliers de R.*

1. *S'il existe un localisé à droite pour T, alors T est un ensemble de dénominateurs à droite de R.*

2. *Si T est un ensemble de dénominateurs à droite et S est un anneau contenant R dans lequel tous les éléments de T sont inversibles alors*

   (a) l'ensemble $RT^{-1} = \{rt^{-1} \in S \mid r \in R, t \in T\}$ est sous anneau de S contenant $T^{-1}R$.

   (b) La structure d'anneau de RT^{-1} est indépendante de celle de S.

   (c) Tout ensemble fini d'éléments de RT^{-1} admet un dénominateur commun.

Théorème 4.4.3. *Si T est un ensemble de dénominateurs à droite dans l'anneau R, alors l'anneau des quotients RT^{-1} (que l'on notera aussi R_T) existe et est unique à R-isomorphisme près. (i.e. l'isomorphisme est l'identité sur R.)*

Démonstration. Le lemme 4.4.2 ci dessus montre qu'il suffit de trouver une extension $R \subseteq S$ dans laquelle tous les éléments de T sont inversibles. Soit $S := Q^r_{max}(R)$. On posera, comme auparavent, $E = E(R_R)$, $H := End_R(E_R)$ on a donc $Q_{max}(R) = End_H({}_HE)$. Soit aussi $t \in T$. Si $r \in R$ et $t \in T$ il existe $r_1 \in R$ et $t_1 \in T$ tels que $rt_1 = tr_1 \in tR$. Donc $t_1 \in r^{-1}(tR)$ et, puisque, t_1 est régulier, on conclut que $ann_g(r^{-1}(tR)) = 0$ pour tout $r \in R$. Ceci montre que tR est un idéal à droite dense de R et le lemme 4.3.3 signifie que $ann_E(tR) = 0$. An particulier $ann_g(t) = 0$.
D'autre part soit $e \in E$ un élément quelconque. Puisque $ann_d(t) = 0$, l'application $\sigma : tR \longrightarrow E : tr \mapsto er$ est un R morphisme bien défini. Puisque E est injectif, σ s'étend en $\overline{\sigma} : R \longrightarrow E$ et donc $e = \sigma(t) = \overline{\sigma}(t) = \overline{\sigma}(1)t \in Et$. On a donc $E = Et$.
Puisque $E = Et$ et $ann_E(t) = 0$, l'application $q : E \longrightarrow E : et \mapsto e$ est bien définie et est un endomorphisme de H-module de E. Donc $q \in Q_{max}(R) = S$.

En outre on a, pour tout $e \in E$ $etq = e$ et, pour tout $f \in Et = E$, $fqt = f$. On en déduit que $tq = qt = 1$ et donc $t^{-1} = q \in S$. □

Si l'ensemble des éléments réguliers $\mathcal{C}$ de R forme un ensemble de dénominateurs à droite on dit que R est un anneau de Ore. l'anneau $R\mathcal{C}^{-1}$ est alors appelé l'anneau total des fractions ou encore (l'anneau classique des fractions à droite) et noté $Q^d_{cl}(R)$. Si en outre R est un domaine on dit que R est un domaine de Ore et $Q^d_{cl}(R)$ est alors un corps.

Corollaire 4.4.4. *Soit R un anneau.*

1. *R est un anneau de Ore à droite si et seulement si $Q^d_{cl}(R)$ existe.*
2. *R est un domaine de Ore à droite si et seulement si $Q^d_{cl}(R)$ est un corps (appelé corps des fractions à droite).*
3. *Si $Q^d_{cl}(R)$ existe, alors il est unique à isomorphisme fixant R près.*

Exercices 4.4.5. 1. Montrer qu'un anneau intègre qui est de Ore à droite est un domaine de Ore.

2. Soit $R = \mathbb{Q}[x][t;\sigma]$ où $\sigma : x \mapsto x^2$.
   (a) Montrer que R est un anneau intègre principal à gauche.
   (b) Montrer que R n'est pas un domaine de Ore à droite.
   (c) Montrer que R admet un corps de fractions à gaucje mais pas à droite.

Définitions 4.4.6. Soit T un ensemble de dénominateurs à droite d'un anneau R. A tout idéal à droite I de R on fait correspondre l'idéal $I_T := IT^{-1} = \{rs^{-1} \,|\, r \in I\}$; On dit que l'idéal I est saturé pour T si $xt \in I$ et $t \in T$ implique $x \in I$. (on utilisera la notation allégée R_T au lieu de RT^{-1})

On a alors les résultats suivants dont on laisse la démonstration en exercice:

Proposition 4.4.7.

1. *$(I + J)_T = I_T + J_T$.*
2. *$(I \cap J)_T = I_T \cap J_T$.*
3. *Si I est un idéal essentiel à droite de R alors I_T est un idéal essentiel de R_T.*
4. *Si $I_1 \oplus \dots I_n$ est une somme directe dans R alors $(I_1)_T \oplus \dots (I_n)_T$ est directe dans R_T.*
5. *Si Si X est un idéal à droite de R_T, alors $X \cap R$ est un idéal à droite de R et $X = (X \cap R)_T = (X \cap R)(R_T)$.*
6. *Si X est un idéal essentiel à droite dans R_T alors $X \cap R$est un idéal essentiel de R.*
7. *Si $X_1 \oplus \dots X_n$ est une somme directe d'idéaux à droite de R_T, alors $(X_1 \cap R) \oplus \dots (X_n \cap R)$ est une somme directye d'déaux à droite dans R.*
8. *L'application $I \mapsto I_T$ est un isomorphisme du treills des idéaux à droite saturés de R sur le treillis des idéaux à droite de R_T.*

Définition 4.4.8. Un anneau R est un anneau de Goldie à droite si R satisfait les conditions suivantes :

a) Les annulateurs des éléments de R vérifient la condition de chaîne ascendante.

b) Il n'existe pas de famile infinie d'idéaux à droite dont la somme soit directe.

Lemma 4.4.9. *Soit T un ensemble de dénominateurs à droite d'un anneau R. Si R_T est est soit noethérien soit artinien alors R est de Goldie à droite.*

Démonstration. Le théorème d'Hopkins-Levitzki montre qu'il suffit de prouver le lemme lorsque R_T est noethérien à droite. R_T ne peut alors contenir de somme directe infinie d'idéaux à droite non nuls. Supposons que $\oplus_{j\in J} I_i$ soit une somme directe d'idéaux à droite de R alors $\oplus_{j\in J}(I_j)_T$ est une somme directe d'idéaux à droite de R. Cette somme doit donc être finie.
Supposons maintenat que $ann_d(x_1) \subseteq ann_d(x_2) \subseteq \dots$ soit une chaîne ascendante d'annulateurs à droite d'éléments de R. Posons $X := \{x_n, x_{n+1} \dots\}$. On a $ann_d(x_n) = ann_d(X_n)$. Posons $S = R_T$. Puisque $X_n \supseteqq X_{n+1}$, on a $ann_d^S(X_1) \subseteq ann_d(X_{n+1})^S \subseteq \dots$ et la noetheriennité de S implique que cette chaîne est sationnaire. Mais $ann_d^S(X_n) \cap R = ann_d^R(X_n) = ann_d^R(x_n)$ et on conclut que la chaîne $ann_d^R(x_1) \subseteq ann_d^R(x_2) \dots$ est aussi stationnaire. □

Lemma 4.4.10. *Soit R un anneau semi-premier satisfaisant la condition de chaîne ascendante sur les annulateurs à droite d'éléments de R. Alors R ne possède aucun idéal à droite ou à gauche nil.*

Démonstration. Supposons que R possède un idéal non nul nil I (à droite ou à gauche). Il suffit de démontrer le lemme dans le cas ou I est monogène c'est à dire de la forme $I = rR$ ou $I = Rr$ pour un certain $r \in R$. Comme d'autre part Rr est un idéal nil si et seulement si rR est un idéal nil, il suffit de considérer le cas $I = Rr$. Soit $b \in I$ tel que $ann_d(b)$ est maximal parmi les annulateurs à droite des éléments non nuls de I. Montrons que $bRb = 0$. Soit $r \in R$. Si $rb = 0$ alors $brb = 0$. Sinon $0 \neq rb$ est nilpotent et il existe $n > 0$ tel que $(rb)^n \neq 0$ mais $(rb)^{n+1} = 0$. Puisque $ann_d(b) \subseteq ann_d(rb)^n$, la maximalité de $ann_d(b)$ implique que l'on a $ann_d(b) = ann_d(rb)^n$. Mais $rb \in ann_d(rb)^n = ann_d(b)$. On a donc $brb = 0$. L'élément $r \in R$ étant quelconque, on conclut que $bRb = 0$ ce qui contredit le fait que R est semi-premier. □

Théorème 4.4.11. *(Théorème de Goldie)*

Soit R un anneau et T les éléments réguliers de R. R admet un anneau total des quotients à droite R_T qui est semi-simple si et seulement si R est semi-premier de Goldie à droite.

Démonstration. Montrons d'abord que "la condition est nécessaire". Si R_T est semi-simple on vient de montrer dans le lemme 4.4.9 ci-dessus que R est de

Goldie à droite. D'autre part si N est un idéal bilatère nilpotent de R alors $B := ann_g^R(N)$ est un idéal bilatère de R. Montrons que B est essentiel dans R : Soit X un idéal non nul a droite de R et soit $n \in \mathbb{N}$ maximal tel que $XN^n \neq 0$. Alors $xN^n \subseteq B$. Donc $0 \neq XN^n \subseteq X \cap B$ ce qui montre que B est essentiel dans R. On en déduit que B_T est essentiel à droite dans R_T. Puisque R_T est semi-simple il ne possède pas d'idéal à droite essentiel propre ce qui montre que $1 \in B_T$, et donc $B \cap T$ est non vide. Puisque $(B \cap T)N = 0$ on conclut que $N = 0$. Ceci montre que R ne possède pas d'déaux bilatères nilpotents non nuls c'est à dire que R est semi-simple.
Montrons maintenant que la condition est suffisante. On montre d'abord que :

1. Soit $r \in R$, il existe un entier $n > 0$, tel que $r^n R \oplus ann_d^R(r^n)$ soit un idéal à doite essentiel de R. En effet il existe un entier n tel que $p > n \Longrightarrow ann_d(a^n) = ann_d(a^p)$ (condition b)). Donc $a^n R \cap ann_d(a^n) = 0$. Soit I un idéal à droite de R tel que $I \cap (a^n R \oplus ann_d(a^n)) = 0$, la somme $I + a^n I + a^{2n} I \ldots a^{pn} I + \ldots$ est directe et la condition c) implique que $I = 0$.
2. Soit $s \in R$ tel que $ann_d(s) = 0$ alors $ann_g(s) = 0$ et sR est un idéal à droite essentiel dans R. Ceci est laissé au lecteur.
3. Tout idéal à droite I de R qui est essentiel contient un élément régulier. En effet, d'après le lemme 4.4.10 précédent on sait que I n'est pas un nil idéal. La condition a) de 4.4.8 montre qu'il existe un élément $0 \neq a_1 \in I$ (car I est essentiel) tel que $ann_d(a_1) = ann_d(a_1^2)$ donc $a_1 R + ann_d(a_1)$ est directe. Si $ann_d(a_1) \neq 0$, on peut trouver un élément $0 \neq a_2 \in ann_d(a_1) \cap I$ tel que $ann_d(a_2) = ann_d(a_1^2)$. Remarquons qu'alors $a_2 R + (ann_d(a_1) \cap ann_d(a_2) \cap I)$ est une somme directe contenue dans $ann_d(a_1) \cap I$ et la somme $a_1 R + a_2 R + (ann_d(a_1) \cap ann_d(a_2) \cap I)$ est directe. Si $ann_d(a_1) \cap ann_d(a_2) \neq 0$, on peut trouver un élément $0 \neq a_3 \in ann_d(a_1) \cap ann_d(a_2) \cap I$ tel que $ann_d(a_3) = ann_d(a_3^2)$ et tel que la somme $a_1 R + a_2 R + a_3 R + (ann_d(a_1) \cap ann_d(a_2) \cap ann_d(a_3) \cap I)$ est une somme directe. On obtient ainsi une suite d'éléments a_k tels que la somme
$$a_1 R + \cdots + a_k R + (ann_d(a_1) \cdots \cap ann_d(a_3) \cap I)$$
est directe. La condition b) 4.4.8] montre qu'il existe p tel que $ann_d(a_1) \cap \ldots ann_d(a_p) \cap I = 0$. Posons $c = \sum_{i=1}^p a_i \in I$. remarquons que c n'est pas un diviseur de zéro (si $cx = 0$ la somme directe ci-dessus montre que $a_i x = 0$ pour tout $i = 1, \ldots, p$ et donc $x \in \cap_i (ann_d(a_i)) = 0$). La propriété 2) ci-dessus montre alors que c est non diviseur de zéro.

On peut maintenat donner la preuve du théorème de Goldie. Soit $r \in R$ et $t \in T$. La propriété 2) montre que tR est tR est un idéal essentiel à droite. De même $r^{-1}tR$ est essentiel. D'après la propriété 3) il existe un élément $t' \in T \cap r^{-1}tR$. Ceci montre que la condition de Ore est satisfaite et R admet un anneau total des quotients $Q^d_{cl}(R)$. Soit I est idéal à droite de R il existe un idéal à droite I' de R tel que $I \oplus I'$ soit essentiel dans R et la propriété 3) montre que $I \oplus I' \cap T \neq \emptyset$. On en déduit alors grâce à 4.4.7 que tout idéal à droite de $R_T = Q_c l^d(R)$ est un sommant direct, ce que l'on voulait démontrer. $\square$

Bibliographie

1. P.M. Cohn, Skew Fields, Cambridge University Press.
2. Mc Connell et Robson, Noncommutative Noetherian rings, Wiley.
3. K.R. Goodearl, R.B. Warfield, An introduction to noncommutative Noetherian rings, London Math. Soc., Student texts **16**.
4. T.Y.Lam, A first course in non commutative rings, GTM **131**.
5. T.Y.Lam, Lectures on Modules and Rings, GTM **189**.
6. G. Renault, Algèbre non commutative, Gauthier-Villars, 1975.
7. L. Rowen, Ring theory, Vol 1 et 2 Academic Press.
8. D. Passman, A course in Ring Theory, AMS, 2004.