UNIVERSITÉ DE FRANCHE-COMTÉ

CTU
Besançon

Master

Mathématiques

Unité d'Enseignement « MODULES SUR LES ANNEAUX PRINCIPAUX »

Responsable : J.-R. Belliard.
Centre de Télé-enseignement Universitaire.
Besançon.
belliard@math.univ-fcomte.fr[1]

MMVI

[1]Toute correspondance relative à l'unité « MODULES » (envoi de devoirs, demande de renseignements sur le cours...) est à adresser à :

Université de Franche-Comté.
Télé-enseignement mathématique.
Jean-Robert Belliard.
25030 BESANÇON CEDEX

Cette brochure a été réalisée en LaTeX 2_ε.

Table des matières.

0 Groupes et Anneaux : Rappel de définitions. 1
0.1 Objets, sous-objets, morphismes. 1
0.2 Noyaux, images, quotients 4

1 Modules sur un anneau commutatif : Généralités. 11
1.1 Modules, sous-modules, applications linéaires. 11
1.2 Noyaux, images, produits directs, sommes directes et quotients 15
1.3 Systèmes libres, générateurs, bases, rang. 21
1.4 Suites exactes, torsion. 23

2 Classification des modules de type fini sur les anneaux principaux 27
2.1 Présentation matricielle des modules de type fini 27
2.2 le théorème de la base adaptée : énoncé de résultats 28
2.3 Opérations élémentaires sur les matrices 32
2.4 Équivalences de matrices : l'algorithme de Smith 35
2.5 Démonstration du lemme 2.3 pour les anneaux principaux 37

3 Exercices du chapitre 0. 41
3.2 Exercice 1. 41
3.3 Exercice 2. 41
3.4 Exercice 3. 41
3.5 Exercice 4. 41
3.6 Exercice 5. 41
3.7 Exercice 6. 41
3.8 Exercice 7. 42
3.9 Exercice 8. 42
3.10 Exercice 9. 42
3.11 Exercice 10. 42

4 Exercices du chapitre 1. 43
4.2 Exercice 11. 43
4.3 Exercice 12. 43
4.4 Exercice 13. 43
4.5 Exercice 14. 43
4.6 Exercice 15. 43
4.7 Exercice 16. 44

4.8 Exercice 17. 44
4.9 Exercice 18. 44
4.10 Exercice 19. 44
4.11 Exercice 20. 44
4.12 Exercice 21. 44
4.13 Exercice 22. 44
4.14 Exercice 23. 45
4.15 Exercice 24. 45
4.16 Exercice 25. 45

5 Exercices du chapitre 2. 47
5.2 Exercice 26. 47
5.3 Exercice 27. 47
5.4 Exercice 28. 47
5.5 Exercice 29. 47
5.6 Exercice 30. 48
5.7 Exercice 31. 48

6 Corrigé des exercices du chapitre 0 51
6.1 Exercice 1. 51
6.2 Exercice 2. 51
6.3 Exercice 3. 52
6.4 Exercice 4. 52
6.5 Exercice 5. 52
6.6 Exercice 6. 52
6.7 Exercice 7. 53
6.8 Exercice 8. 53
6.9 Exercice 9. 53
6.10 Exercice 10. 55

7 Corrigé des exercices du chapitre 1 57
7.11 Exercice 11. 57
7.12 Exercice 12. 57
7.13 Exercice 13. 59
7.14 Exercice 14. 59
7.15 Exercice 15. 60
7.16 Exercice 16. 60
7.17 Exercice 17. 60
7.18 Exercice 18. 61
7.19 Exercice 19. 61
7.20 Exercice 20. 61
7.21 Exercice 21. 61
7.22 Exercice 22. 61
7.23 Exercice 23. 62
7.24 Exercice 24. 62
7.25 Exercice 25. 63

8 Corrigé des exercices du chapitre 2 **65**
8.26 Exercice 26. 65
8.27 Exercice 27. 65
8.28 Exercice 28. 67
8.29 Exercice 29. 67
8.30 Exercice 30. 68
8.31 Exercice 31. 69

9 Annales. **71**
9.1 premier devoir 04/05. 71
9.2 solution du premier devoir 04/05. 72
9.3 deuxième devoir 04/05. 73
9.4 solution du deuxième devoir 04/05. 74
9.5 Épreuve principale première session 2005. 77
9.6 Solution de l'épreuve principale première session 2005. 78
9.7 Épreuve complémentaire première session 2005. 80
9.8 Solution de l'épreuve complémentaire première session 2005. 81
9.9 Épreuve principale deuxième session 2005. 82
9.10 Solution de l'épreuve principale deuxième session 2005. 83
9.11 Épreuve complémentaire deuxième session 2005. 84
9.12 Solution de l'épreuve complémentaire deuxième session 2005. 85

Chapitre 0

Groupes et Anneaux : Rappel de définitions.

0.1 Objets, sous-objets, morphismes.

Définition 0.1 : Structure de groupe additif

1. *Un groupe commutatif (additif) est un ensemble G muni d'une loi de composition interne $+$ vérifiant les axiomes :*
   (a) *(existence d'un neutre additif) Il existe $0_G \in G$ tel que pour tout $g \in G$ on ait $0_G + g = g + 0_G = g$*
   (b) *(existence d'un symétrique additif) Pour tout $g \in G$ il existe $(-g) \in G$ tel que $g + (-g) = (-g) + g = 0_G$*
   (c) *(associativité additive) Pour tout a, b, $c \in G$ on a $(a + b) + c = a + (b + c)$.*
   (d) *(commutativité additive) Pour tout a, $b \in G$ on a $a + b = b + a$*
2. *Soit A et B deux groupes (additifs). On appelle morphisme de groupe de A dans B une application $f : A \longrightarrow B$ compatible avec les structures des groupes c'est-à-dire telle que :*
   (a) *Pour tout x, $y \in A$ on ait $f(x + y) = f(x) + f(y)$.*
3. *Soit G un groupe (additif). On appelle sous-groupe de G tout sous-ensemble H de G vérifiant les axiomes*
   (a) *$H \neq \emptyset$*
   (b) *Pour tout a, $b \in H$ on a $a + (-b) \in H$.*

Dans le point 1. ci-dessus, si on se contente des trois premiers axiomes (a), (b) et (c) vous reconnaissez la définition d'un groupe. On parle de groupe commutatif (ou abélien en hommage au mathématicien Abel) lorsqu'en outre le quatrième axiome est vérifié. On n'étudie ici que les groupes commutatifs et on convient de la notation additive en vue de définir la notion d'anneau.
La conjonction des axiomes (a) et (b) du point 3. est équivalente à celle de l'axiome (b) et de l'axiome (a') : $0_G \in H$. En pratique pour montrer qu'un sous-ensemble H est un sous-groupe il est souvent plus commode de vérifier (a'). Si H est un sous-ensemble quelconque de G la restriction de $+ : G \times G \longrightarrow G$ à $H \times H \subset G \times G$ arrive dans G. Si H

vérifie les axiomes de la définition de sous-groupes alors cette restriction définit une loi de composition interne sur H. Muni de cette loi H est un groupe et l'inclusion $H \subset G$ est un morphisme, ce qui justifie l'emploi du terme « sous-groupe ».

Définition 0.2 Anneau
Un anneau A est un groupe additif muni d'une seconde loi de composition interne (multiplication) $\times$ vérifiant les axiomes :

1. *(existence d'un neutre multiplicatif) Il existe $1_A \in A$ tel que pour tout $a \in A$ on ait $1_A \times a = a \times 1_A = a$.*
2. *(associativité multiplicative) Pour tout a, b, $c \in A$ on a $a \times (b \times c) = (a \times b) \times c$.*
3. *(distributivité à gauche et à droite de la multiplication par rapport à l'addition) Pour tout a, b, $c \in A$ on a $(a+b) \times c = (a \times c) + (b \times c)$ et $a \times (b+c) = (a \times b) + (a \times c)$.*

Dans ce cours tous les anneaux vérifieront l'axiome 1 (ils auront un neutre multiplicatif appelé élément unité), ce qui correspond à la norme contemporaine, même si certains ouvrages précisent anneaux unitaires.

Définition 0.3 Anneaux commutatif
Lorsque A est un anneau et que la multiplication est commutative, on dit que A est un anneau commutatif.

Si A est un anneau, l'ensemble A muni de la multiplication n'est pas un groupe, puisqu'on ne suppose pas l'existence d'un inverse multiplicatif (une telle structure est parfois appelée monoïde). De plus (si on exclut le cas trivial $A = \{0\}$) le neutre additif 0_A n'est pas inversible multiplicativement. Lorsque tous les éléments non nuls de A sont inversible on dit que A est un corps.

Définition 0.4
Soit A et B deux anneaux. On appelle morphisme d'anneaux une application $f : A \longrightarrow B$ qui vérifie les axiomes suivants.

1. *f est un morphisme de groupes : Pour tout x, $y \in A$ $\quad f(x+y) = f(x) + f(y)$.*
2. *f est compatible avec la multiplication : Pour tout x, $y \in A$ $\quad f(x \times y) = f(x) \times f(y)$.*
3. *f est un morphisme unitaire : $f(1_A) = 1_B$*

Remarque Il suit de la définition de morphisme de groupes que $f(0_A) = f(0_B)$. Mais cela utilise l'existence des inverses additifs et le point 3. n'est pas redondant. Soit A un anneau commutatif unitaire. Muni de l'addition et de la multiplication composante par composante l'anneau produit $A \times A$ est bien un anneau. Le morphisme de groupes additif $a \mapsto (a, 0)$ de A dans $A \times A$ vérifie les deux premières propriétés mais pas la dernière.

Exemples d'anneaux

1. Les corps des nombres rationnels, réels ou complexes (notés respectivement $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$).
2. L'anneaux des entiers rationnels noté $\mathbb{Z}$.
3. Lorsque A est un anneaux commutatif, l'anneau des polynômes à une indéterminée à coefficients dans A, noté $A[X]$ est un anneau.
4. Lorsque $(A_s)_{s \in S}$ est une famille d'anneaux le produit cartésien $\prod_{s \in S} A_s$ muni des loi de compositions internes composantes par composantes précisées ci-dessous est un

anneau.

$$(a_s)_{s\in S} + (b_s)_{s\in S} = (a_s + b_s)_{s\in S} \quad (a_s)_{s\in S} \times (b_s)_{s\in S} = (a_s \times b_s)_{s\in S}$$

La structure d'anneaux est le cadre naturel pour généraliser les questions de divisibilité (autrement dit d'arithmétique) que chacun a rencontré dans $\mathbb{Z}$. Au contraire dans un corps tous les éléments (non nuls) sont inversibles et se divisent les uns les autres : il n'y a plus de question d'ordre arithmétique. L'algèbre linéaire que vous connaissez suppose que les coefficients appartiennent à un corps (en pratique les auteurs supposent même très souvent le corps des coefficients égal à $\mathbb{R}$ ou $\mathbb{C}$: une perte en généralité regrettable). L'algèbre linéaire classique s'applique a de nombreux domaines des mathématiques, notamment la géométrie ou la théorie des groupes à travers leurs représentations (linéaires). Mais pour la raison évoquée plus haut cette algèbre linéaire ne suffit pas aux applications arithmétiques. Si l'on remplace dans la définition d'espace vectoriel le corps des coefficients par un anneau on obtient une structure de module. L'objet de ce cours sera, tout en rappelant au passage des notions d'algèbre linéaire connues, d'étudier cette structure nouvelle et de cerner les difficultés supplémentaires dues à ce gain en généralité.
Dans une première partie du cours on énoncera des généralités à propos des modules sur un anneau commutatif quelconque. Puis on abordera la classification à isomorphismes près des modules sur les anneaux principaux. Dans l'immédiat on va rappeler d'autres définitions jusqu'à la notion d'anneau principal.

Définition 0.5
Soit A un anneau et I un sous-groupe additif de A. On dit que I est idéal bilatère de A lorsque I est multiplicativement absorbant à gauche et à droite c'est-à-dire lorsque

1. *Pour tout $a \in A$ et tout $i \in I$ on a $a \times i \in I$, et*
2. *Pour tout $a \in A$ et tout $i \in I$ on a $i \times a \in I$.*

Remarque Lorsque seul le point 1. est vérifié, on dit que I est un idéal à gauche. Lorsque seul le point 2. est vérifié on dit que I est un idéal à droite. Lorsque A est commutatif les trois notions sont équivalentes (et on parle d'idéal sans préciser bilatère).

Exemple Soit A un anneau commutatif et $a \in A$. L'ensemble $I = \{x \times a;\ x \in A\}$ est un idéal (forcément bilatère) de A. On dit que I est l'idéal principal engendré par a. (En fait I est le plus petit idéal contenant a c'est donc bien l'idéal ayant pour partie génératrice le singleton $\{a\}$).

Définition 0.6
Soit A un anneau commutatif et $I \subset A$ un idéal de A.

1. *On dit que I est principal lorsqu'il existe $a \in A$ tel que $I = \{x \times a;\ x \in A\}$.*
2. *On dit que A est principal lorsque tous les idéaux de A sont principaux.*

Proposition 0.1 (opérations sur les idéaux) *Soient A un anneau et I et J deux idéaux (à gauche si A n'est pas commutatif) de A.*

1. *$I \cap J$ est un idéal (à gauche) de A.*
2. *L'ensemble noté IJ formé des sommes finies de produit ij où $i \in I$, $j \in J$ est un idéal (à gauche) de A. On l'appelle l'idéal produit de I par J.*

Démonstration : C'est un cas particulier de la proposition 1.2 démontrée dans le chapitre suivant (vous verrez dans la suite que les sous-modules de A sont ces idéaux).
Pour être complet on mentionne la notion de sous-anneau :

Définition 0.7
Soit A un anneau et B un sous-groupe (additif) de A. On dit que B est un sous-anneau de A lorsqu'il satisfait en outre aux axiomes :

1. $1_A \in B$
2. *Pour tout x, $y \in B$ on a $x \times y \in B$.*

Donc un sous-anneau de A est un sous-ensemble B contenant l'unité et stable pour les deux lois : ici aussi l'inclusion $B \subset A$ est un morphisme d'anneaux, et cette propriété caractérise les sous-anneaux de A.

0.2 Noyaux, images, quotients

Proposition 0.2
Soit $f : A \longrightarrow B$ un morphisme de groupes (additifs).

1. *L'ensemble $\{b \in B;\ \exists a \in A \ \text{ tel que } b = f(a)\}$ est un sous-groupe de B.*
2. *L'ensemble $\{a \in A;\ f(a) = 0_B\}$ est un sous-groupe de A.*

Démonstration : Exercice.

Définition 0.8
Soit $f : A \longrightarrow B$ un morphisme de groupes (additifs).

1. *On appelle image de f et on note $\operatorname{Im} f$ le sous-groupe $\operatorname{Im} f = \{b \in B;\ \exists a \in A. \ \text{tel que } b = f(a)\}$.*
2. *On appelle noyau de f et on note $\ker f$ le sous-groupe $\ker f = \{a \in A;\ \text{tel que } f(a) = 0_B\}$.*

Proposition 0.3
Soit $f : A \longrightarrow B$ un morphisme d'anneaux (en particulier de groupes additifs).

1. *L'image $\operatorname{Im} f$ est en outre un sous-anneau de B.*
2. *Le noyau $\ker f$ est en outre un idéal bilatère de A.*

Démonstration : Exercice.

Proposition 0.4
Soit G un groupe additif. la donnée d'un sous-groupe H de G définit une relation d'équivalence sur G comme suit : Si $g \in G$ et $g' \in G$, alors $g \sim_H g'$ si et seulement si $g + (-g') \in H$.

Démonstration On traduit la définition de sous-groupe. H contient l'élément neutre entraîne que $\sim_H$ est reflexive. H contient l'inverse de tout ses éléments entraîne que $\sim_H$ est symétrique. H est stable par $+$ entraîne que $\sim_H$ est transitive. On détaille cette dernière implication et les deux autres sont proposées en exercice. Soit x, y, z, $\in G$ tels que $x \sim_H y$ et $y \sim_H z$. Alors on a $x - y \in H$ et $y - z \in H$. Il suit $x - y + y - z = x - z \in H$, c'est-à-dire $x \sim_H z$.

Définition 0.9
Soit G un groupe additif et H un sous-groupe de G. Soit $\sim_H$ la relation d'équivalence définie par H.

1. *Lorsque $g \sim_H g'$ on dit que g et g' sont dans la même classe d'équivalence modulo H.*
2. *Soit $g \in G$. On note $\overline{g}$ ou $g + H$ ou $\pi_H(g)$ sa classe d'équivalence modulo H. Formellement il s'agit de $\overline{g} = \{x \in G;\ x \sim_H g\}$, c'est un sous-ensemble de G.*
3. *On note G/H l'ensemble des classes d'équivalence pour la relation $\sim_H$. Formellement G/H est un sous-ensemble de l'ensemble des parties de G.*

Pour être formellement correct, on est contraint pendant la définition qui précède de considérer les classes comme des sous-ensembles de G. A l'usage dès qu'on introduit la structure de groupe on doit voir les classes comme les éléments du groupe quotient défini par le théorème qui suit.

Théorème 0.1
Soit G un groupe additif et H un sous-groupe de G. Soit $\pi_H \colon G \longrightarrow G/H$ l'application (surjective) définie par la notation $\pi_H(g)$.

1. *Il existe une unique loi de groupe (additive) sur G/H pour laquelle π_H est un morphisme de groupes.*
2. $\ker \pi_H = H$

Démonstration. Pour le 1., l'unicité suit de la surjectivité de π_H. Quant à l'existence, on doit seulement se convaincre que la loi de composition interne $\overline{x} + \overline{y} := \overline{x + y}$ est bien définie, autrement dit que la classe $\overline{x + y}$ ne dépend pas du choix de x dans $\overline{x}$ ni de celui de y dans $\overline{y}$. Soit $x' \in \overline{x}$ et soit $y' \in \overline{y}$. Alors il existe $h_1 \in H$ et $h_2 \in H$ tels que $x' = x + h_1$ et $y' = y + h_2$. On en déduit $x' + y' = x + y + h_1 + h_2 \in \overline{x + y}$, puisque H est un sous-groupe. D'où l'indépendance relative aux choix requise. Il reste à vérifier que cette loi de composition interne satisfait aux axiomes de la définition des groupes. Il s'agit d'un exercice de routine que je recommande aux lecteurs qui ne seraient pas encore familiers avec la notion de groupe quotient. Concrètement on utilise l'application π_H pour « transporter » de G vers G/H la structure de groupe. Par exemple la classe $\overline{0_G} = \pi_H(0_G)$ est l'élément neutre de G/H. Vous trouverez la fin de la preuve (y compris le 2.) rédigée avec les solutions des autres exercices.

Définition 0.10

1. *On appelle groupe quotient de G par H l'ensemble G/H muni de l'unique structure de groupe du théorème 0.1.*
2. *On appelle surjection canonique le morphisme de groupes $\pi_H \colon G \longrightarrow G/H$ du théorème 0.1.*

Le quotient d'un groupe additif est sensiblement plus simple à définir que celui d'un groupe non commutatif. En effet tous les sous-groupe étant normaux on peut considérer directement les groupes quotients sans s'attarder sur les ensembles de classes à gauche et à droite.

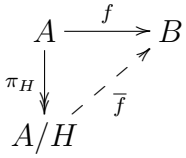
Théorème 0.2
Soit I un idéal bilatère d'un anneau A (en particulier I est un sous-groupe additif de A). Alors il existe sur le groupe quotient A/I une unique structure d'anneau pour laquelle la surjection canonique π_I est un morphisme d'anneaux.

Démonstration Là encore la seule difficulté est de montrer que la multiplication $\overline{x} \times \overline{y} := \overline{x \times y}$ est bien définie. On procède de même que pendant la preuve du théorème 0.1. Soit $x' \in \overline{x}$ et soit $y' \in \overline{y}$. Alors il existe i_1 et i_2 dans I tels que $x' = x + i_1$ et $y' = y + i_2$. Il suit $x' \times y' = (x + i_1) \times (y + i_2) = x \times y + i_1 \times y + x \times i_2 + i_1 \times i_2$. Mais comme I est un idéal bilatère il contient la somme $i_1 \times y + x \times i_2 + i_1 \times i_2$, de sorte que $x' \times y' \in \overline{x \times y}$. Pour conclure il suffit de vérifier que les axiomes de la définition des anneaux se transportent de A à A/I via le morphisme π_I.

Théorème 0.3 factorisation des morphismes

1. *Soit $f\colon A \longrightarrow B$, un morphisme de groupes additifs, et soit H un sous-groupe de A. L'existence d'un morphisme $\overline{f}\colon A/H \longrightarrow B$ tel que $f = \overline{f} \circ \pi_H$ est équivalente à l'inclusion $H \subset \ker f$. Lorsque $\overline{f}$ existe :*
   (a) *$\overline{f}$ est unique.*
   (b) *$\overline{f}$ est surjectif si et seulement si f l'est.*
   (c) *$\overline{f}$ est injectif si et seulement si l'inclusion $H \subset \ker f$ est une égalité.*
2. *Soit $f\colon A \longrightarrow B$, un morphisme d'anneaux, et soit I un idéal de A. L'existence d'un morphisme $\overline{f}\colon A/I \longrightarrow B$ tel que $f = \overline{f} \circ \pi_I$ est équivalente à l'inclusion $I \subset \ker f$. Lorsque $\overline{f}$ existe :*
   (a) *$\overline{f}$ est unique.*
   (b) *$\overline{f}$ est surjectif si et seulement si f l'est.*
   (c) *$\overline{f}$ est injectif si et seulement si l'inclusion $I \subset \ker f$ est une égalité.*

On a sciemment répété en parallèle l'énoncé pour la structure de groupe (additif) et pour la structure d'anneau. Ce théorème et sa preuve fonctionnent avec n'importe quelle structure pour laquelle on dispose des notions de quotients et de noyaux. On verra que c'est le cas pour la structure de module aussi. L'usage est d'illustrer ce phénomène de factorisation par un diagramme triangulaire comme suit.



On parle de diagramme commutatif lorsque les divers morphismes obtenus par compositions (éventuelles) suivant différents chemins coïncident. Dans le cas d'un triangle la seule égalité sous-entendue par la commutativité du diagramme est l'égalité $f = \overline{f} \circ \pi_H$.

Démonstration Le point 2. se démontre comme le premier (en remplaçant partout anneaux par groupe et sous-groupe par idéal). On démontre le point 1. Supposons qu'il existe un morphisme $\overline{f}$ tel que $f = \overline{f} \circ \pi_H$. Montrons que $H \subset \ker f$. Soit $h \in H$. On a $f(h) = \overline{f}(\pi_H(h))$ par hypothèse. Mais puisque $h \in H = \ker \pi_H$ on en déduit $f(h) = \overline{f}(0_{A/H}) = 0_B$ car $\overline{f}$ est un morphisme. Donc $h \in \ker f$ et on a montré l'inclusion

$H \subset \ker f$. Réciproquement supposons que $H \subset \ker f$. La condition $f = \overline{f} \circ \pi_H$ impose $\overline{f}(\overline{a}) = f(a)$ pour tout $a \in A$ d'où l'unicité de $\overline{f}$ si elle existe. Pour établir cette existence on définit $\overline{f}$ à partir de la formule $f = \overline{f} \circ \pi_H$. Soit $x \in A/H$, et soit y, $y' \in A$ tels que $\pi_H(y) = \pi_H(y') = x$. Alors $y - y' \in H \subset \ker f$ et donc $f(y) = f(y')$ ne dépend que de x et pas du choix de y relevant x dans A. En posant $\overline{f}(x) = f(y)$ on définit une application qui est indépendante du choix des $y \in A$ relevant les $x \in A/H$. Cette indépendance montre l'égalité $f = \overline{f} \circ \pi_H$. Soient x, $x' \in A/H$ et y, $y' \in A$ des relevés respectifs. Alors $\overline{f}(x + x') = \overline{f}(\pi_H(y) + \pi_H(y')) = \overline{f}(\pi_H(y + y')) = f(y + y') = f(y) + f(y') = \overline{f}(x) + \overline{f}(x')$. L'application f est donc un morphisme de groupe. L'équivalence entre f surjective et $\overline{f}$ surjective est une conséquence directe de $f = \overline{f} \circ \pi_H$ et de la surjectivité de π_H. Pour montrer l'équivalence entre $\overline{f}$ injective et $H = \ker f$ on va énoncer un lemme un peu plus général.

Lemme 0.1
Soit $f\colon A \longrightarrow B$ un morphisme de groupes additifs et soit H un sous-groupe de $\ker f$. Soit $\overline{f}\colon A/H \longrightarrow B$ le morphisme factorisé de f (on vient de démontrer l'existence et l'unicité de ce morphisme puisque $H \subset \ker f$). Alors $\ker \overline{f}$ est égal au sous-groupe $\ker f/H \subset A/H$. En particulier si $H = \ker f$ alors $\ker \overline{f} = \{0_{G/H}\}$ et $\overline{f}$ est injectif.

Démonstration du lemme : Soit $x \in \ker f$. Alors $\overline{f}(\pi_H(x)) = f(x) = 0_B$. Donc $\pi_H(x) \in \ker \overline{f}$. Cela montre $\ker f/H \subset \ker \overline{f}$. Réciproquement soit $x \in \ker \overline{f}$ et soit $y \in A$ tel que $\pi_H(y) = x$. Alors $f(y) = \overline{f}(\pi_H(y)) = \overline{f}(x) = 0_B$. Donc $y \in \ker f$ et il suit $x \in \pi_H(\ker f) = \ker f/H$. D'où l'égalité.

Définition 0.11
Soit A un anneau commutatif.

1. *On dit qu'un élément $a \in A$ est un diviseur de zéro lorsque $a \neq 0$ et il existe $b \in A, b \neq 0$ tel que $a \times b = 0$ (dans ce cas on dit aussi que b est un codiviseur de zéro de a et vice-versa).*
2. *A est dit intègre s'il ne contient pas de diviseur de zéro.*
3. *Un idéal $I \subset A$ est dit principal lorsqu'il existe un $a \in A$ tel que $I = A \times a := \{x \in A, \exists \alpha \in a$ tel que $x = \alpha \times a\}$.*
4. *On appelle anneau principal un anneau intègre dont tous les idéaux sont principaux.*

Toutes les notions de ce chapitre sont supposées connues et on ne s'est arrêté que sur les démonstrations ré-utilisées dans la suite. Pour démontrer que le rang d'un module est bien défini on utilisera plus tard le théorème de Krull et le fait que $A/\mathfrak{M}$ est un corps si $\mathfrak{M}$ est maximal. On utilisera aussi le « lemme Chinois » qui conclura ce chapitre. On rappelle ces résultats sans en donner la démonstration (celle-ci figure déjà dans le cours sur les anneaux).

Définition 0.12
Soit A un anneau commutatif unitaire.

1. *Un idéal $\mathfrak{P} \subset A$ est dit premier lorsque $\forall x, y \in A \quad xy \in A \implies x \in A$ ou $y \in A$.*
2. *Un idéal $\mathfrak{M} \subset A$ est dit maximal lorsque $\mathfrak{M} \neq A$ et que $\mathfrak{M}$ et A sont les seuls idéaux contenant $\mathfrak{M}$.*

Théorème 0.4
Soit I un idéal d'un anneau commutatif A

1. *I est premier si et seulement si A/I est intègre.*
2. *I est maximal si et seulement si A/I est un corps.*
3. **Théorème de Krull.** *Si $I \neq A$ alors il existe un idéal $\mathfrak{M}$ maximal dans A tel que $I \subset \mathfrak{M}$.*

Les deux premiers points sont classiques et proposés en exercice de révision sur les anneaux. Le troisième est une conséquence immédiate du lemme de Zorn, qui lui-même est équivalent à l'axiome du choix. On n'en dira pas plus dans ces rappels.

Définition 0.13
Soit A un anneau commutatif unitaire, et soient I et J deux idéaux de A.On dit que I et J sont co-maximaux ou étranger lorsque $I + J = A$.

Lemme 0.2
Soient A un anneau commutatif I et J deux idéaux de A co-maximaux , k un entier, et $(I_j)_{j=1}^{j=k}$ une famille de k idéaux de A deux à deux co-maximaux.

1. *$IJ = I \cap J$*
2. *L'ideal I_k est co-maximal à l'idéal produit $\prod_{j=1}^{j=k-1} I_j$. En particulier les idéaux $\prod_{1\leq j\leq k} I_j$ et $\cap_{1\leq j\leq k} I_j$ sont égaux.*

Démonstration :

1. On a la chaîne d'inclusion $IJ \subset I\cap J \subset (I\cap J)A \subset (I\cap J)(I+J) \subset IJ$ d'où l'égalité. (On peut aussi remarquer que l'inclusion $IJ \subset I \cap J$ subsiste en toute généralité).
2. On fait une récurrence sur k. Si $k = 2$ c'est clair. Supposons la proposition vraie pour un certain $k - 1 \geq 2$. Alors par hypothèse et récurrence les trois idéaux I_1, I_k et $J = \prod_{j=2}^{k-1} I_j$ sont deux à deux co-maximaux. Il existe donc des $x_k \in I_k, x'_k \in I_k$, $x_1 \in I_1$ et $j \in J$ tels que $1 = x_k + x_1 = x'_k + j$. En multipliant on obtient $1 = x_k x'_k + x_k j + x'_k x_1 + x_1 j$. Et comme les trois premiers sommants sont dans I_k on en déduit $1 \in I_k + I_1 J = I_k + \prod_{j=1}^{k-1} I_j$ d'où l'hérédité de la propriété à démontrer.

Théorème 0.5 Lemme Chinois
Soient A un anneau commutatif, k un entier et $(I_j)_{j=1}^{j=k}$ une famille de k idéaux de A deux à deux co-maximaux. On a un isomorphisme canonique :

$$\frac{A}{\prod_{j=1}^{j=k} I_j} = \frac{A}{\cap_{j=1}^{j=k} I_j} \cong \prod_{j=1}^{j=k} \frac{A}{I_j}$$

Démonstration : On peut présenter cette démonstration comme une récurrence sur k mais l'hérédité est immédiate en vertu du lemme 0.2. La seule difficulté qui subsiste est le cas particulier $k = 2$ qui est traité dans toutes les référence classiques. On se donne donc I et J deux idéaux comaximaux. On considère le morphisme d'anneaux diagonal $\delta\colon A \longrightarrow A/I \times A/J$ défini par $a \mapsto (a + I, a + J)$. Puisque $I + J = A$ étant donné $(b, c) \in A^2$ il existe $i \in I$ et $j \in J$ tels que $b - c = i + j$ ou encore $b - i = c + j$. Soit

$\alpha = b - i = c + j$, alors $\alpha \equiv b[I]$ et $\alpha \equiv c[J]$, donc α est un antécédent de $(b+I, c+J)$ pour δ qui est surjective. Clairement $\ker \delta = I \cap J$ et on obtient l'isomorphisme annoncé par factorisation de δ. On peut aussi remarquer que le morphisme diagonal se factorise en toute généralité en un morphisme injectif $A/I \cap J \longrightarrow A/I \times A/J$. L'hypothèse de co-maximalité n'est utilisée que pour la surjectivité et l'égalité entre produit et intersection d'idéaux.

Chapitre 1

Modules sur un anneau commutatif : Généralités.

1.1 Modules, sous-modules, applications linéaires.

Soit A un anneau unitaire.

Définition 1.1 structure de A-module
Soit M un groupe additif.

1. *Une opération externe à gauche de A sur M est une application notée $(a, m) \mapsto am$ du produit cartésien $A \times M$ dans M.*
2. *On dit que M est un module à gauche sur A (ou A-module à gauche) lorsqu'il existe une opération externe à gauche de A sur M vérifiant les axiomes (Pour tout $m, m' \in M$ et tout $a, b \in A$) :*
   - *(a)* $a(m + m') = am + am'$
   - *(b)* $(a + b)m = am + bm$
   - *(c)* $1_A m = m$
   - *(g)* $(ab)m = a(bm)$
3. *Soient M et N deux A-module à gauche. On appelle application A-linéaire ou morphisme de A-modules un morphisme de groupes $f : M \longrightarrow N$ compatible avec l'opération de A, autrement dit tel que, pour tout $m \in M$ et tout $a \in A$, on ait $f(am) = af(m)$. On note $\mathrm{Hom}_A(M, N)$ l'ensemble des applications A-linéaires de M dans N.*
4. *Soit M un A-module à gauche, et soit $N \subset M$. On dit que N est un sous-module à gauche de M lorsque N est un sous-groupe de M stable pour l'opération de A, autrement dit lorsque, pour tout $a \in A$ et tout $n \in N$, on a $an \in N$.*

Lorsque A est commutatif l'axiome (g) ci-dessus est équivalent à l'axiome (d) suivant : $(ab)m = b(am)$. Cependant ce dernier axiome se retient mieux en notant l'opération de A comme une opération à droite (une application $(m, a) \mapsto ma$ de $M \times A$ dans M) puisque cela donne alors (d) : $m(ab) = (ma)b$. Pour cette raison, avec des anneaux non commutatif, on distingue les structures de modules à gauche (vérifiant l'axiome (g)) et les structure de module à droite (vérifiant l'axiome (d)). Si A est un anneau, on note A^{op} l'anneau obtenu à partir de A mais avec la nouvelle multiplication $a * b := ba$. Alors tout

A-module à droite est canoniquement muni d'une structure de A^{op}-module à gauche. Pour cette raison si on garde en mémoire que les deux structures existent et sont distinctes, on peut indifféremment étudier la structure de module à gauche ou à droite. Dans ce cours (comme dans la plus part des ouvrages français) on étudie la structure de module à gauche (et on dira « module » plutôt que « module à gauche »).

Par définition un sous-modules $N \subset M$ est un sous-ensemble stable pour les opérations linéaires. Par restriction des opérations de M on définit un loi de composition additive interne à N et une opération externe de A sur N. Le sous-ensemble N est ainsi muni d'une structure de A-module et l'inclusion $N \subset M$ est alors un morphisme de A-modules.

Proposition 1.1 propriétés basiques
Soit M un A-module, $m \in M$, $a \in A$, $N \subset M$, et P un A-module.

1. $0_A m = 0_M$
2. $(-1_A)m = -m$
3. $a0_M = 0_M$
4. *N est un sous-module de M si et seulement si $N \neq \emptyset$ et pour tout $x, y \in N$ et tout $\alpha, \beta \in A$ alors $\alpha x + \beta y \in N$.*
5. *Une application $f\colon M \longrightarrow P$ est A-linéaire si et seulement si pour tout $\alpha, \beta \in A$ et tout $x, y \in M$ on a $f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$.*

Preuve Cela suit de la définition.

1. On a $0_A m + m = (0_A + 1_A)m = (1_A)m = m$. Et comme dans le groupe additif M on peut simplifier par m, on obtient $0_A m = 0_M$.

2. Il s'agit de montrer l'égalité $(-1_A)m + m = 0_M$. Cela suit du 1., car $(-1_A)m + m = (-1_A)m + (1_A)m = (-1_A + 1_A)m = 0_A m = 0_M$.

3. On a $am = a(0_M + m) = a0_M + am$. Pour conclure on simplifie par am dans le groupe additif M.

4. On suppose que N est un sous-module de M. Alors N est un sous-groupe donc non vide. Soient donc $\alpha, \beta \in A$ et $x, y \in N$. Puisque N est un sous-module $\alpha x \in N$ et $\beta y \in N$. Puisque N est un sous-groupe $\alpha x + \beta y \in N$. Cela montre le sens direct de l'équivalence. Réciproquement on suppose N non vide et contenant $\alpha x + \beta y$ pour tout $\alpha, \beta \in A$ et tout $x, y \in N$. En particulier pour $\beta = 0$, on voit que N contient αx pour tout $\alpha \in A$ et tout $x \in N$. Il suffit donc de montrer que N est un sous-groupe de M. Mais N est supposé non vide, et pour tout $x, y \in N$ on a $x - y = 1_A x + (-1_A)y \in N$: cela montre que N est un sous-module de M.

5. Soient $x, y \in M$ et soit $\alpha, \beta \in A$. Si f est A linéaire c'est un morphisme de groupes. Donc $f(\alpha x + \beta y) = f(\alpha x) + f(\beta y)$. Puis comme f est A-linéaire on a $f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$. Cela donne le sens direct de l'équivalence annoncée. Réciproquement on suppose que pour tout $\alpha, \beta \in A$ et tout $x, y \in M$ on ait $f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$. Alors si on prend $\alpha = \beta = 1_A$ dans la formule qui précède on montre que f est un morphisme de groupe. Si on prend $\beta = 0_A$ on montre que f vérifie la seconde propriété des morphismes de A-modules.

Proposition 1.2
Soit M un A-module, soit $(N_s)_{s\in S}$ une famille quelconque de sous-modules de M et P_1 et P_2 deux sous-modules de M.

1. *L'intersection $N = \bigcap_{s\in S} N_s$ est un sous-module de M.*
2. *On note $\sum_{s\in S} N_s$ l'ensemble des sommes finies d'éléments de N_s. C'est un sous-module de M. En particulier lorsque $S = \{1, 2\}$ l'ensemble $N_1 + N_2$ des sommes d'éléments de N_1 et de N_2 est un sous-module de M.*
3. *Si $P_1 \bigcup P_2$ est un sous-module de M alors $P_1 \subset P_2$ ou $P_2 \subset P_1$.*

Démonstration.

1. Soient x, y dans N. Alors pour tout α, β dans A comme chaque N_s est un sous-module contenant x et y il contient $\alpha x + \beta y$. Donc $\alpha x + \beta y \in N$.
2. Toute combinaison linéaire de sommes finies d'éléments de N_s est encore une somme finie d'éléments de N_s.
3. On suppose P_1 et P_2 ne sont pas inclus l'un dans l'autre. Alors il existe $p_1 \in P_1$ et $p_2 \in P_2$ tels que $p_1 \notin P_2$ et $p_2 \notin P_1$. Puisque les P_i sont des sous-modules il vient $p_1 + p_2 \notin P_1$ et $p_1 + p_2 \notin P_2$, alors que p_1 et p_2 appartiennent à la réunion $P_1 \bigcup P_2$.

Exemples

1. Si A est un corps la structure de A-module est identique à celle de A-espace vectoriel.
2. A est un A-module : la multiplication interne tient lieu d'opération externe.
3. Les sous-A-modules de A sont les idéaux de A (à gauche si A n'est pas commutatif).
4. Si M est un A-module il contient les sous-modules triviaux $\{0_M\}$ et M. On dit que M est simple s'il n'en contient pas d'autres (et si $M \neq \{0_M\}$).

Définition 1.2
Soit M et N deux A-modules.

1. *On appelle endomorphisme de M une application A-linéaire de M dans M. On note donc $\mathrm{End}_A(M) = \mathrm{Hom}_A(M, M)$ l'ensemble des endomorphismes de M.*
2. *On appelle isomorphisme de M dans N un morphisme linéaire bijectif.*
3. *On appelle automorphisme de M un isomorphisme de M dans M. On note $\mathrm{Aut}_A(M)$ l'ensemble des automorphismes de M.*

La terminologie « isomorphisme » pour morphisme bijectif est justifiée car la bijection réciproque d'un morphisme linéaire est linéaire :

Proposition 1.3
Soient M et N deux A-modules et soit $f\colon M \longrightarrow N$ un isomorphisme. Alors la bijection réciproque de f est A-linéaire.

Démonstration Soit $\alpha, \beta \in A$ et soit $x, y \in N$. On applique f à $\alpha f^{-1}(x) + \beta f^{-1}(y)$. Par linéarité de f on obtient : $f(\alpha f^{-1}(x) + \beta f^{-1}(y)) = \alpha f(f^{-1}(x)) + \beta f(f^{-1}(y)) = \alpha x + \beta y$. En appliquant f^{-1} à cette égalité il vient $\alpha f^{-1}(x) + \beta f^{-1}(y) = f^{-1}(\alpha x + \beta y)$.

Lemme 1.1
Soit S un ensemble, soient M, N et P des A-modules, soient $f, g \in \mathrm{Hom}_A(M,N)$, et soit $h \in \mathrm{Hom}_A(N,P)$. On note N^S l'ensemble des applications de S dans M

1. *Soit α, $\beta \in N^S$. Alors la formule (valable pour tout $s \in S$) $(\alpha+\beta)(s) = \alpha(s)+\beta(s)$ définit une application $\alpha+\beta \in N^S$. Avec cette loi de composition interne N^S est un groupe additif.*
2. *L'application $f+g \in N^M$ est A-linéaire. En particulier $\mathrm{Hom}_A(M,N)$ est un sous-groupe additif de N^M, donc un groupe.*
3. *Soit $a \in A$ et $\alpha \in N^S$. Alors la formule (valable pour tout $s \in S$) $(a\alpha)(s) = a\alpha(s)$ définit une application $a\alpha \in N^S$. Muni de cette opération externe de A le groupe N^S est un A-module.*
4. *Soit $a \in A$. Si A est commutatif alors l'application $af \in N^M$ est A-linéaire. En particulier $\mathrm{Hom}_A(M,N)$ est un sous-A-module de N^M, donc un A-module.*
5. *L'application composée $h \circ f$ est A-linéaire. En particulier pour $M = N = P$ la composition des applications est une seconde loi interne sur $\mathrm{End}_A(M)$. Muni de cette multiplication $\mathrm{End}_A(M)$ est un anneau (en même temps qu'un A-module si A est commutatif).*

Démonstration.

1. On transporte la structure de groupe de N dans N^S. L'application 0_{N^S} définie par $\forall s \in S \quad 0_{N^S}(s) = 0_N$ est manifestement un neutre additif dans N^S. Si $f \in N^S$ l'application $x \mapsto -f(x)$ est un inverse additif de f. L'associativité et la commutativité dans N^S se déduisent respectivement de l'associativité et de la commutativité dans N.
2. Montrons que $(f+g)$ est A-linéaire. Soient $x, y \in M$ et soient $\alpha, \beta \in A$. Par définition de $(f+g)$ on a $(f+g)(\alpha x+\beta y) = f(\alpha x+\beta y)+g(\alpha x+\beta y)$. Puisque f et g sont A-linéaires on a $(f+g)(\alpha x+\beta y) = \alpha f(x)+\beta f(y)+\alpha g(x)+\beta g(y) = \alpha(f(x)+g(x))+\beta(f(y)+g(y))$. On utilise à nouveau la définition de $f+g$ qui donne $(f+g)(x) = f(x)+g(x)$ et $(f+g)(y) = f(y)+g(y)$ et on conclut à $(f+g)(\alpha x+\beta y) = \alpha(f+g)(x)+\beta(f+g)(y)$.
3. $(a,f) \mapsto af$ telle que défini dans l'énoncé est bien une opération externe de A sur N^S. On transporte la structure de module de N dans N^S : en utilisant les propriétés $(a),(b),(c)$ et (g) dans N on obtient les propriétés analogues pour les images des applications en $s \in S$ fixé quelconque c'est-à-dire pour les applications elles-mêmes.
4. Montrons que af est linéaire. Soient $\alpha, \beta \in A$ et soit $x, y \in M$. Alors par la définition de (af), la linéarité de f et la commutativité de A, on a $(af)(\alpha x+\beta y) = a(f(\alpha x+\beta y)) = a(\alpha f(x)+\beta f(y)) = a\alpha f(x)+a\beta f(y) = \alpha(af)(x)+\beta(af)(y)$.
5. Par définition de $h \circ f$ et linéarité de f et h on a pour tout $\alpha, \beta \in A$ et tout $x, y \in M$:

   $$h\circ f(\alpha x+\beta y) = h(\alpha f(x)+\beta f(y)) = \alpha h(f(x))+\beta h(f(y)) = \alpha(h\circ f)(x)+\beta(h\circ f)(y).$$

   Cela donne la linéarité de $h \circ f$. Dans le 2 on a vu que $\mathrm{End}_A(M)$ est un groupe additif. La composition des applications linéaires admet l'identité comme élément unité et est associative. Soient $f, g, h \in \mathrm{End}_A(M)$. Pour tout $m \in M$, on a $(f+g)\circ h(m) = (f+g)(h(m)) = f(h(m))+g(h(m)) = (f\circ h+g\circ h)(m)$ d'une part, et $(f\circ(g+h))(m) = f((g+h)(m)) = f(g(m))+f(h(m)) = (f\circ g+f\circ h)(m)$ par linéarité

de f d'autre part. Cela donne la distributivité de $\circ$ par rapport à $+$ et montre que $\mathrm{End}_A(M)$ est un anneau. Le plus souvent cet anneau n'est pas commutatif (penser à l'anneau des $\mathbb{K}$-endomorphisme d'un $\mathbb{K}$-espace vectoriel de dimension 2).

Définition 1.3
On appelle A-algèbre un ensemble B qui est à la fois un A-module et un anneau. Les morphismes de A-algèbres sont les morphismes d'anneaux A-linéaires.

Exemples

1. Un groupe additif M est canoniquement un $\mathbb{Z}$-module : voir exercice 12.
2. Se donner une structure de A-module sur un groupe additif M équivaut à se donner un morphisme d'anneau $A \longrightarrow \mathrm{End}_{\mathbb{Z}}(A)$: voir exercice 13.
3. Soit $\mathbb{K}$ un corps (commutatif), V un $\mathbb{K}$-espace vectoriel. Se donner une structure de $\mathbb{K}[X]$-module sur V qui étende la structure de $\mathbb{K}$-espace vectoriel de V équivaut à se donner un morphisme de $\mathbb{K}$-algèbre $\varphi\colon \mathbb{K}[X] \longrightarrow \mathrm{End}_{\mathbb{K}}(V)$. Pour toute $\mathbb{K}$-algèbre B et tout $b \in B$, il existe un unique morphisme de $\mathbb{K}$-algèbre $\varphi\colon \mathbb{K}[X] \longrightarrow B$ tel que $\varphi(X) = b$. En résumé les structures de $\mathbb{K}[X]$-modules sur V compatibles avec la structure de $\mathbb{K}$-espace vectoriel initiale sont en bijection avec $\mathrm{End}_{\mathbb{K}}(V)$: voir exercice 14.

1.2 Noyaux, images, produits directs, sommes directes et quotients

Proposition 1.4
Soit $f\colon M \longrightarrow N$ un morphisme de A-modules (en particulier un morphisme de groupes additifs).

1. *Le noyau de f, $\ker f = \{m \in M;\ f(m) = 0\}$ est un sous-module de M.*
2. *L'image de f, $\mathrm{Im}\, f = \{n \in N;\ \exists m \in M$ tel que $n = f(m)\}$ est un sous-module de N.*

Démonstration.

1. $\ker f$ est un sous-groupe de M par la proposition 0.2. Soit $x \in \ker f$ et soit $\alpha \in A$. Alors on a $f(\alpha x) = \alpha f(x) = \alpha 0 = 0$. Donc $\alpha x \in \ker f$ ce qui montre que $\ker f$ est un sous-module de M.
2. $\mathrm{Im}\, f$ est un sous-groupe de N par la proposition 0.2. Soit $x \in \mathrm{Im}\, f$ et soit $\alpha \in A$. Comme $x \in \mathrm{Im}\, f$, il existe un antécédent $y \in M$ de x, c'est-à-dire tel que $f(y) = x$. Alors par linéarité de f, αy est un antécédent de αx qui appartient donc à $\mathrm{Im}\, f$. Cela montre que $\mathrm{Im}\, f$ est un sous-module de N.

Proposition 1.5
Soit S un ensemble et $(M_s)_{s\in S}$ une famille de A-modules indexée par S. Les lois définies par $(m_s) + (n_s) = ((m+n)_s)$ et $\alpha(m_s) = (\alpha m_s)$ confèrent au produit cartésien $\prod_{s\in S} M_s$ une structure de A-module.

Démonstration : C'est évident.

Définition 1.4
On appelle module produit des $(M_s)_{s\in S}$ et on note $\prod_{s\in S} M_s$ le A-module de la proposition 1.5.

Proposition 1.6
Soit S un ensemble et $(M_s)_{s\in S}$ une famille de A-modules indexée par S. L'ensemble des $(m_s)_{s\in S} \in \prod_{s\in S} M_s$ tels que $m_s = 0$ pour tout $s \in S$ sauf un nombre fini, est un sous-module de $\prod_{s\in S} M_s$.

Démonstration : C'est évident.

Définition 1.5
On appelle somme directe des $(M_s)_{s\in S}$ et on note $\bigoplus_{s\in S} M_s$ le sous-module de $\prod_{s\in S} M_s$ de la proposition 1.6.

Remarques

1. Lorsque S est fini, les modules $\bigoplus_{s\in S} M_s$ et $\prod_{s\in S} M_s$ sont égaux.
2. Lorsque les modules M_s sont tous égaux à M l'application $f \mapsto (f(s))_{s\in S}$ est un isomorphisme de M^S sur $\prod_{s\in S} M$. L'usage est d'identifier ces deux modules. Par cette identification la somme directe $\oplus_{s\in S} M$ s'identifie au sous-module $M^{(S)}$ formé des applications $f\colon S \longrightarrow M$ à support fini (c'est-à-dire telle que $f(s) = 0_M$ pour tout s sauf éventuellement pour un nombre fini de s).
3. Prenons $S = \mathbb{N}$. Le module $A^{(\mathbb{N})}$ est naturellement isomorphe (en tant que module) au module $A[X]$ des polynômes à une indéterminée et à coefficient dans A. Le module $A^{\mathbb{N}}$ est naturellement isomorphe (en tant que module) au module $A[[X]]$ des séries formelles à une indéterminée à coefficients dans A. Pour $A = \mathbb{F}_2$ le corps à deux éléments le module $\mathbb{F}_2^{(\mathbb{N})}$ est dénombrable tandis que $\mathbb{F}_2^{\mathbb{N}}$ est en bijection avec l'ensemble des parties de $\mathbb{N}$, c'est-à-dire en bijection avec $\mathbb{R}$. Il n'existe donc aucune bijection (a fortiori aucun isomorphisme de modules) entre $\mathbb{F}_2^{(\mathbb{N})}$ et $\mathbb{F}_2^{\mathbb{N}}$.

Proposition 1.7
Pour tout $t \in S$, on définit des applications $i_t\colon M_t \longrightarrow \oplus_{s\in S} M_s$ et $p_t\colon \prod_{s\in S} M_s \longrightarrow M_t$ comme suit.

$$\text{Pour } m \in M_t \text{ on pose } i(m) = (i_s(m))_{s\in S} \text{ avec } i_s(m) = \begin{cases} 0 \text{ si } s \neq t \\ m \text{ si } s = t \end{cases}$$
$$\text{Pour } (m_s)_{s\in S} \in \prod_{s\in S} M_s \text{ on pose } p_t((m_s)_{s\in S}) = m_t.$$

On a :

1. *Les applications p_t et i_t sont A-linéaires.*
2. *Soit $\imath\colon \oplus_{s\in S} M_s \longrightarrow \prod_{s\in S} M_s$ l'injection canonique. Alors le morphisme composé $p_t \circ \imath \circ i_t$ est égal à l'identité de M_t.*

Démonstration : C'est évident.

Théorème 1.1
Soit A un anneau et soit $(M_s)_{s\in S}$ une famille de A-modules.

1. *Pour tout A-module M et toute famille de morphismes $f_s\colon M_s \longrightarrow M$, il existe un unique morphisme $f\colon \oplus_{s\in S} M_s \longrightarrow M$ vérifiant $\forall s \in S$, $f \circ i_s = f_s$. On note parfois $\oplus_{s\in S} f_s$ l'unique morphisme qui précède.*
2. *Pour tout A-module M et toute famille de morphismes $g_s\colon M \longrightarrow M_s$, il existe un unique morphisme $g\colon M \longrightarrow \prod_{s\in S} M_s$ vérifiant $\forall s \in S$, $p_s \circ g = g_s$.*

Démonstration.

1. On pose $f((m_s)_{s\in S}) = \sum_{s\in S} f_s(m_s)$. Comme les m_s sont nuls sauf un nombre fini, la somme est finie et ceci définit bien une application $f\colon \oplus_{s\in S} M_s \longrightarrow M$. Cette application vérifie trivialement la condition $\forall s \in S$, $f \circ i_s = f_s$. Pour la linéarité on prend a, $b \in A$ et (m_s), $(n_s) \in \oplus M_s$. En utilisant la définition de f, de la structure de module de la somme directe et la linéarité des f_s on obtient :

$$\begin{aligned} f(a(m_s)_{s\in S} + b(n_s)_{s\in S}) &= f((am_s + bn_s)_{s\in S}) \\ &= \textstyle\sum_s f_s(am_s + bn_s) \\ &= \textstyle\sum_s af_s(m_s) + bf_s(n_s) \\ &= a\textstyle\sum_s f_s(m_s) + b\sum_s f_s(n_s) \\ &= af((m_s)_{s\in S}) + bf((n_s)_{s\in S}) \end{aligned}$$

   Soit f' une application A-linéaire vérifiant $\forall s \in S$, $f' \circ i_s = f_s$. Alors f' et f coïncident sur les images des i_s. Par linéarité ces morphismes sont aussi égaux sur toute combinaisons linéaire d'éléments de ces images c'est-à-dire sur tout élément de la somme directe : on a bien $f = g$.
2. On pose $g(m) = (g_s(m))_{s\in S}$. L'application g est alors A-linéaire par la définition de la structure de A-module du produit, et l'hypothèse de linéarité des g_s. Clairement g vérifie $p_s \circ g = g_s$. Supposons que $g'\colon M \longrightarrow \prod_{s\in S} M_s$ soit une autre morphisme vérifiant cette condition. Si $m \in M$ on note $g'(m) = (g'_s(m))_{s\in S}$ et donc $g'_s(m)$ la composante en M_s de $g'(m)$. la condition $g' \circ p_s = g_s$ impose $g'_s(m) = g_s(m)$. En conséquence les composantes en tout s de $g'(m)$ et $g(m)$ sont égales : on a bien $g' = g$.

Les conditions $f \circ i_t = f_t$ et $p_t \circ g = g_t$ se représentent avec les diagrammes commutatifs ci-dessous.

Les morphismes f et g sont définis "coordonnées par coordonnées" c'est-à-dire au travers des p_s et des i_s et les détails sont expliqués dans la preuve du théorème 1.1. Cette propriété ; de la somme et des injections i_s d'une part, et du produit et des projection p_s d'autre part ; s'appelle la *propriété universelle* de la somme (respectivement du produit) direct. A isomorphismes près il n'y a qu'un seul module qui vérifie cette propriété pour tout M et toute famille de f_s (respectivement g_s).

Théorème 1.2
Soient M un A-module, N un sous-module de M, soit M/N le groupe additif quotient et soit $\pi_N\colon M \longrightarrow M/N$ la projection canonique. Il existe sur M/N une unique structure de A-module pour laquelle π_N est A-linéaire.

Démonstration Il suffit de vérifier que l'opération externe $a\overline{m} = \overline{am}$ est bien définie. Soit m' un autre choix de représentant dans M de la classe $\overline{m}$. Alors il existe $n \in N$ tel que $m' = m + n$. Il vient donc $\overline{am'} = \overline{a(m+n)} = \overline{am + an}$. Et comme $an \in N$ on a bien $\overline{am'} = \overline{am}$. La suite de la démonstration consiste à transporter via π_N la structure de A-module de M sur M/N. Autrement dit on utilise les propriétés $(a), (b), (c)$ et (g) qui sont vraies pour tout $a,\, b \in A$ et tout $m, m' \in M$ pour établir les mêmes propriétés concernant $a, b \in A$ et $\overline{m},\, \overline{m'} \in M/N$.

Théorème 1.3 factorisation des morphismes de modules
Soit $f\colon M \longrightarrow N$, un morphisme de A-modules, et soit P un sous-module de M. L'existence d'un morphisme $\overline{f}\colon M/P \longrightarrow N$ tel que $f = \overline{f} \circ \pi_P$ est équivalente à l'inclusion $P \subset \ker f$. Lorsque $\overline{f}$ existe :

1. *$\overline{f}$ est unique.*
2. *$\overline{f}$ est surjectif si et seulement si f l'est.*
3. *$\overline{f}$ est injectif si et seulement si l'inclusion $H \subset \ker f$ est une égalité.*

Démonstration. Par le théorème de factorisation des morphismes de groupes additifs, il suffit de vérifier que si $P \subset \ker f$ le morphisme de groupe $\overline{f}\colon M/P \longrightarrow N$ est aussi A-linéaire. Soit $a \in A$, soit $x \in M/P$ et soit $m \in M$ tel que $\pi_P(m) = x$. Par définition de la structure de module de M/P on a $ax = \pi_P(am)$. On obtient $\overline{f}(ax) = \overline{f}(\pi_P(am)) = f(am) = af(m) = a\overline{f}(\pi_P(m)) = af(x)$.

Corollaire 1.3.1 premier théorème d'isomorphie de Noether
Soient M et N deux sous-modules d'un même A-module L. On a un isomorphisme naturel

$$\frac{M}{M \cap N} \cong \frac{M+N}{N}.$$

Démonstration Soit $f\colon M \longrightarrow (M+N)/N$ obtenu en composant l'inclusion $M \subset M+N$ avec la projection $\pi_N\colon M + N \longrightarrow (M+N)/N$. Alors f est surjective puisque m est un antécédent de la classe $\overline{m+n} \in (M+N)/N$ pour tout $m \in M$ et tout $n \in N$. Clairement $\ker f = M \cap N$ et on obtient l'isomorphisme annoncé par factorisation de f (c'est-à-dire en appliquant le théorème 1.3).

Corollaire 1.3.2
Soit $(N_s)_{s\in S}$ une famille de sous-modules d'une famille de modules $(M_s)_{s\in S}$. On note $\alpha_s\colon N_s \longrightarrow \oplus_{t\in S} M_t$ le morphisme composé des injections canoniques $N_s \subset M_s$ et des $\imath_s\colon M_s \longrightarrow \oplus_{t\in S} M_t$ et $\alpha = \oplus\alpha_s\colon \oplus_{s\in S} N_s \longrightarrow \oplus_{s\in S} M_s$ le morphisme défini dans le point 2. du théorème 1.1. Le morphisme α est injectif. En identifiant $\oplus_s N_s$ avec $\operatorname{Im}\alpha \subset \oplus_s M_s$, On a un isomorphisme naturel

$$\frac{\oplus_{s\in S} M_s}{\oplus_{s\in S} N_s} \cong \oplus_{s\in S} \frac{M_s}{N_s}$$

Démonstration Soit $(n_s)_{s\in S} \in \ker\alpha \subset \oplus_s N_s$. Alors dans $\oplus_s M_s$ on a $(0)_{s\in S} = (\alpha_s(n_s))_{s\in S}$ et puisque les α_s sont injectifs $n_s = 0$ pour tout s. Cela montre l'injectivité de α. On définit un morphisme $f\colon \oplus_s M_s \longrightarrow \oplus_s M_s/N_s$ en prenant le morphisme somme directe des morphismes obtenus par composition de π_{N_s} avec $\imath_s\colon M_s/N_s \longrightarrow \oplus_{t\in S} M_t/N_t$. Si $(m_s)_{s\in S}$ appartient au noyau $\ker f$ alors pour tout s on a $\overline{n_s} = 0 \in M_s/N_s$, et donc $m_s \in N_s$. On obtient bien $\ker f = \operatorname{Im}\alpha$ puis l'isomorphisme annoncé par factorisation de f.

Proposition 1.8
Soient M un A-module, soit P un sous-module de M et $\pi_P\colon M \longrightarrow M/P$ la projection canonique. L'application $N \mapsto \pi_P(N)$ est une bijection de l'ensemble des sous-module de M contenant P sur l'ensemble des sous-module de M/P. La bijection réciproque est $Q \mapsto \pi_P^{-1}(Q)$.

Démonstration : Soit N un sous-module de M contenant P. Comme π_P est un morphisme $\pi_P(N)$ est un sous-module de M/P. Soit Q un sous-module de M/P alors $\pi_P^{-1}(Q)$ est un sous-module de N contenant $P = \pi_P^{-1}(\{0\})$ puisque Q contient $\{0\}$. Les deux applications de l'énoncé sont donc bien définies et appliquent l'un dans l'autre les ensembles annoncés. Elles sont réciproques l'une de l'autre, donc bijectives.
Remarques : La restriction de π_P au sous-modules N contenant P est un morphisme surjectif $N \longrightarrow \pi_P(N)$. Le noyau de ce morphisme est P, il se factorise donc en un isomorphisme $N/P \cong \pi_P(N)$. On aurait donc pu identifier $\pi_P(N)$ et N/P dans l'énoncé qui précède.

Corollaire 1.3.3 Second théorème d'isomorphie de Noether
Soient $P \subset N$ deux sous-module d'un même A-module M. On a un isomorphisme naturel

$$\frac{M}{N} \cong \frac{M/P}{N/P}.$$

Démonstration On a utilisé la remarque qui précède le corollaire pour identifier N/P avec le sous-module $\pi_P(N) \subset M/P$. C'est pourquoi ce corollaire du théorème 1.3 apparaît ici et non aussitôt après son théorème. On part des morphismes surjectifs $\pi_P\colon M \longrightarrow M/P$ et $\pi_{N/P}\colon \longrightarrow (M/P)/(N/P)$. Soit f le morphisme composé $f = \pi_{N/P} \circ \pi_P$. Alors f est surjectif. Soit $m \in M$ on a les équivalences :

$$m \in \ker f \iff \pi_{N/P}(\pi_P(m)) = 0 \iff \pi_P(m) \in \pi_P(N) \iff \exists n \in N,\ \pi_P(m) = \pi_P(n).$$

Comme $P \subset N$, il suit $\ker f = N$ et on obtient l'isomorphisme annoncé par factorisation de f.

Définition 1.6
Soient M un A-modules, M_1 et M_2 des sous-modules de M.

1. *On dit que M est somme directe interne de M_1 et M_2 lorsque $M = M_1 + M_2$ et $M_1 \cap M_2 = \{0\}$.*
2. *Lorsque M est somme directe interne de M_1 et M_2 on dit que M_1 est facteur direct de M, et que M_2 est un supplémentaire à M_1 dans M.*

Remarque Lorsque A est un corps tout sous-espace vectoriel de tout espace vectoriel sur A admet un (donc des) supplémentaire(s). Ceci est faux en général. Par exemple le sous-module $2\mathbb{Z} \subset \mathbb{Z}$ n'a pas de supplémentaire. En effet si $I \neq \{0\}$ est un idéal de $\mathbb{Z}$ on a $\{0\} \neq 2I$ et $2I \subset I \cap 2\mathbb{Z}$. Et comme $\mathbb{Z} \neq 2\mathbb{Z}$ l'égalité $\mathbb{Z} = I \oplus 2\mathbb{Z}$ est impossible.

Définition 1.7
Soient M un A-module et $(M_i)_{i\in I}$ une famille de sous-modules de M. On dit que M est somme directe interne des M_i lorsque $M = \sum_{i\in I} M_i$ et que pour tout $j \in I$ l'intersection $M_j \cap \sum_{j\neq i} M_i$ est réduite à $\{0\}$.

Proposition 1.9
Soient M un A-module et $(M_i)_{i\in I}$ une famille de sous-modules de M. Soient $f_i \colon M_i \longrightarrow M$ les injections canoniques et soit $f \colon \bigoplus_{i\in I} M_i \longrightarrow M$ le morphisme $\oplus_i f_i$ défini dans le point 2 du théorème 1.1. Les assertions suivantes sont équivalentes :

(1) *M est somme directe interne des M_i.*
(2) *Pour tout $m \in M$ il existe une unique famille finie de $m_i \in M_i$ telle que $m = \sum_i m_i$.*
(3) *f est un isomorphisme.*

Démonstration.

1. On montre l'implication (1) $\implies$ (2). Puisque $M = \sum_{i\in I} M_i$ tout élément de M s'écrit comme une somme finie d'éléments $m_i \in M_i$. Pour l'unicité il suffit de vérifier que si une somme finie d'éléments $m_i \in M_i$ est nulle alors tous les m_i sont nuls. Soient $(m_{i_k})_{1\leq k\leq n}$ une famille finie d'éléments $m_{i_k} \in M_{i_k}$ telle que $\sum_{k=1}^{n} m_{i_k} = 0$. Alors pour tout j avec $1 \leq j \leq n$ le sommant $m_{i_j} = -\sum_{1\leq k\leq n, k\neq j} m_{i_k}$ appartient à l'intersection $M_{i_j} \cap \sum_{k\neq i_j} M_k$. Donc $m_{i_j} = 0$.
2. On montre l'implication (2) $\implies$ (3). Par (2) l'application $\varphi \colon m \mapsto \sum_i \imath_i(m_i)$ est bien définie. Un calcul immédiat montre que f et φ sont réciproques l'une de l'autre : ce sont bien des isomorphismes.
3. On montre l'implication (3) $\implies$ (1). Par définition même le module $\oplus_i M_i$ est somme directe interne des sous-modules $\imath_i(M_i)$. Si f est un isomorphisme on obtient alors que M est somme directe interne des sous-modules $f(\imath_i(M_i)) = M_i$

1.3 Systèmes libres, générateurs, bases, rang.

Dorénavant on suppose en outre que l'anneau unitaire A est commutatif. La notion de rang d'un module libre sur un anneau commutatif unitaire est analogue à la dimension des espaces vectoriels. Elle nécessite cependant (au moins) une étape supplémentaire pour être définie, et ne subsiste pas en toute généralité. On définit ici le rang d'un module libre sur un anneau commutatif unitaire. Signalons qu'il est possible de définir le rang d'un module quelconque sur un anneau intègre et une famille de $\mathfrak{P}$-rangs (a priori distincts) d'un module quelconque indexée par les idéaux premiers $\mathfrak{P}$ de l'anneau A (quelconque). Ces notions ne seront pas définies ici.

Définition 1.8
Soit M un A-module, soit S un ensemble, $T \subset M$ un sous-ensemble de M et $\mathcal{F} = (m_s)_{s\in S}$ une famille d'éléments de M.

1. *On dit que T est un système générateur de M (ou que T engendre M) lorsque pour tout x dans M il existe une famille $(\lambda_t)_{t\in T}$ d'éléments de A tous nuls sauf un nombre fini et tels que $x = \sum_{t\in T} \lambda_t t$.*
2. *On dit que $\mathcal{F}$ est une famille génératrice lorsque le sous-ensemble $\bigcup_{s\in S}\{m_s\} \subset M$ est un système générateur, c'est-à-dire lorsque pour tout x dans M il existe une famille $(\lambda_s)_{s\in T}$ d'éléments de A tous nuls sauf un nombre fini et tels que $x = \sum_{s\in S} \lambda_s m_s$.*
3. *On dit que $\mathcal{F}$ est une famille libre lorsque la seule famille $(\lambda_s)_{s\in S}$ d'éléments de A tous nuls sauf éventuellement un nombre fini et vérifiant $0 = \sum_{s\in S} \lambda_s m_s$ est la famille nulle.*
4. *On dit que $\mathcal{F}$ est une base de M lorsque pour tout x dans M il existe une unique famille $(\lambda_s)_{s\in S}$ d'éléments de A tous nuls sauf un nombre fini et tels que $x = \sum_{s\in S} \lambda_s m_s$.*

Remarques Vous connaissez déjà cette définition dans le cadre des espaces vectoriels. Ces notions en elles-même ne changent pas. Par contre dans le cadre de la théorie des modules sur un anneau qui n'est pas un corps on rencontre un problème d'existence. On ne dispose plus du théorème de la base incomplète. Par exemple dans $\mathbb{Z}$ vu comme module sur $\mathbb{Z}$ l'élément 2 est libre, non générateur mais tout x de $\mathbb{Z}$ est lié à 2 par $2x - x2 = 0$: on ne peut pas compléter 2 en une $\mathbb{Z}$-base de $\mathbb{Z}$. Bien sur $\mathbb{Z}$ admet la $\mathbb{Z}$-base 1, mais par exemple le module $\mathbb{Z}/15\mathbb{Z}$ sur $\mathbb{Z}$ n'admet aucun système libre (en effet pour tout $x \in \mathbb{Z}/15\mathbb{Z}$ on a $15x = 0$). A fortiori il n'existe pas de $\mathbb{Z}$-base de $\mathbb{Z}/15\mathbb{Z}$. Après avoir constaté l'existence de modules qui n'admettent pas de bases on pose la définition :

Définition 1.9
On dit que M est un A module libre (de base B) lorsqu'il existe une famille B d'éléments de M qui soit une base de M.

On rencontre ici la première vraie différence entre la théorie des modules sur un anneau et celle des espaces vectoriels sur un corps : ces derniers sont tous libres. De même on ne peut pas toujours extraire une base d'un système générateur. Par exemple 2 et 3 engendrent $\mathbb{Z}$ mais sont liés par $2 \times 3 = 3 \times 2$, et ni $\{2\}$ ni $\{3\}$ ne sont des systèmes générateurs de $\mathbb{Z}$. Le problème tient à ce que l'on ne peut plus diviser les relations de dépendance linéaire $\lambda_1 x_1 = \sum_{i\neq 1} \lambda_i x_i$ par λ_1 même si λ_1 est non nul. De sorte qu'une telle relation linéaire n'implique pas forcément que x_1 appartient au sous-module engendré par les autres x_i. Vous

pouvez reprendre un cours d'algèbre linéaire sur les corps de seconde année et constater que pratiquement tous les résultats utilisent soit le théorème de la base incomplète soit le principe d'extraction de base à partir de système générateurs. La proposition qui suit fait exception :

Proposition 1.10
Soit S un ensemble et soit $\mathcal{F} = (m_s)_{s\in S}$ une famille d'éléments d'un A-module M.

1. *La famille $\mathcal{F}$ est une A-base de M si et seulement si $\mathcal{F}$ est à la fois libre et génératrice.*
2. *On suppose que $\mathcal{F}$ est une A-base de M. Soit $f\colon A^{(S)} \longrightarrow M$ l'application définie par la formule $f((a_s)_{s\in S}) = \sum a_s m_s$. Alors f est un isomorphisme de A-modules.*
3. *Soit N le plus petit sous-module de M contenant $\mathcal{F}$. Alors $\mathcal{F}$ est une famille génératrice de N.*

Démonstration.

1. Revoir n'importe quel cours d'algèbre linéaire sur un corps : la démonstration n'utilise pas de divisions et s'applique donc encore ici.
2. L'application f est clairement A-linéaire. La définition de A-base montre que tout $x \in M$ admet un et un seul antécédent pour f qui est donc bijective.
3. Avant de commencer la preuve on remarque que l'existence de N est assurée en prenant l'intersection de tous les sous-module de M contenant S. Soit L l'ensemble des combinaisons A-linéaires et finies entre éléments de S. Clairement L est un sous-module de M, et S est un système générateur de L. Puisque $S \subset L$ on a $N \subset L$. Puisque N est un sous-module $L \subset N$. Donc $L = N$ et S engendre N.

Définition 1.10
On reprend les notations de la proposition 1.10.

1. *Le module N du 3 de la proposition 1.10 se note $\langle S\rangle$ et on l'appelle le sous-module de M engendré par S.*
2. *On dit qu'un module M est de type fini lorsqu'il existe un sous-ensemble fini $F \subset M$ tel que $\langle F\rangle = M$.*

Lemme 1.2
Soient S et T deux ensembles. On suppose qu'il existe un isomorphisme $f\colon A^{(S)} \longrightarrow A^{(T)}$. Alors les ensembles S et T ont même cardinal.

Vous connaissez certainement ce résultat lorsque les ensembles S et T sont finis et l'anneau A est un corps : cela revient essentiellement à dire que la dimension des espaces vectoriels de type fini est bien définie. Il se trouve que ce résultat reste vrai en algèbre linéaire classique avec des ensembles S et T quelconques, fait que l'on va admettre dans ce cours.

Lemme 1.3
Le lemme 1.2 est vrai si A est un corps.

Démonstration : admis

On démontre comment étendre ce résultat aux modules sur les anneaux quelconques. Vous pouvez ainsi obtenir une démonstration complète du résultat lorsque S et T sont finis,

ce qui suffit pour la suite du cours. Pour généraliser des espaces vectoriels aux modules cela ne simplifie en rien de supposer S et T fini en on ne le fait pas.

Démonstration du lemme 1.2 Par le théorème de Krull rappelé dans le théorème 0.4 l'anneau A contient (au moins) un idéal maximal, on le note $\mathfrak{M}$. L'idée est de passer au quotient modulo $\mathfrak{M}$ pour retrouver le terrain connu des $A/\mathfrak{M}$-espaces vectoriels. On considère les sous-modules $\mathfrak{M}^{(S)} \subset A^{(S)}$ et $\mathfrak{M}^{(T)} \subset A^{(T)}$. Par le corollaire 1.3.2 on a les isomorphismes de A-modules $A^{(S)}/\mathfrak{M}^{(S)} \cong (A/\mathfrak{M})^{(S)}$ et $A^{(T)}/\mathfrak{M}^{(T)} \cong (A/\mathfrak{M})^{(T)}$. On admet provisoirement l'identité $\mathfrak{M}^{(S)} = f^{-1}(\mathfrak{M}^{(T)})$. Alors par passage au quotient on définit un morphisme A-linéaire (donc $A/\mathfrak{M}$-linéaire) $\overline{f}\colon (A/\mathfrak{M})^{(S)} \longrightarrow (A/\mathfrak{M})^{(T)}$ qui fait commuter le diagramme :

$$\begin{array}{ccc} A^{(S)} & \xrightarrow{\quad f \quad} & A^{(T)} \\ {\scriptstyle \pi_{\mathfrak{M}^{(S)}}}\downarrow & & \downarrow{\scriptstyle \pi_{\mathfrak{M}^{(T)}}} \\ (A/\mathfrak{M})^{(S)} & \xrightarrow{\overline{f}} & (A/\mathfrak{M})^{(T)} \end{array}$$

$\overline{f}$ est bien défini et bijectif car $\pi_{\mathfrak{M}^{(T)}} \circ f$ est surjectif et son noyau vaut $\ker(\pi_{\mathfrak{M}^{(T)}} \circ f) = f^{-1}(\ker \pi_{\mathfrak{M}^{(T)}}) = f^{-1}(\mathfrak{M}^{(T)}) = \mathfrak{M}^{(S)}$. On a donc un isomorphisme entre les $A/\mathfrak{M}$-espaces vectoriels $(A/\mathfrak{M})^{(S)}$ et $(A/\mathfrak{M})^{(T)}$. En d'autres termes ces deux espaces ont même dimension : S et T ont même cardinal.
Pour finir la preuve on doit maintenant montrer l'égalité $\mathfrak{M}^{(S)} = f^{-1}(\mathfrak{M}^{(T)})$. On montre d'abord l'inclusion $f^{-1}(\mathfrak{M}^{(T)}) \subset \mathfrak{M}^{(S)}$. Soit $(e_t)_{t\in T}$ la base canonique de $A^{(T)}$. Clairement le module $\mathfrak{M}^{(T)}$ est engendré par les éléments de la forme me_t si m parcourt $\mathfrak{M}$ et t parcourt T. Mais comme $\mathfrak{M}$ est un idéal les $f^{-1}(me_t) = mf^{-1}(e_t)$ appartiennent à $\mathfrak{M}^{(S)}$. Cela donne l'inclusion $f^{-1}(\mathfrak{M}^{(T)}) \subset \mathfrak{M}^{(S)}$. En appliquant le même raisonnement à f on obtient aussi l'inclusion $f(\mathfrak{M}^{(S)}) \subset (\mathfrak{M}^{(T)})$. Il suit alors $\mathfrak{M}^{(S)} = f^{-1}(f(\mathfrak{M}^{(S)})) \subset f^{-1}(\mathfrak{M}^{(T)})$ d'où l'égalité.

Définition 1.11
Soit M un module libre. On appelle rang de M le cardinal d'une base de M. Le lemme qui précède montre que le rang d'un module libre est bien défini.

Bien entendu si S est un ensemble alors $A^{(S)}$ est un module libre avec sa base canonique. Le rang de $A^{(S)}$ est donc le cardinal de S. Dans le cas particulier où $S = \{1, ..., s\}$ est l'ensemble fini de cardinal s on retrouve la notation standard $A^s = A^S = A^{(S)}$.

1.4 Suites exactes, torsion.

Exemple de suite exacte courte. Soit $N \subset M$ des A-modules. On note $\imath\colon N \longrightarrow M$ et $\pi\colon M \longrightarrow M/N$ les morphismes canoniques. Alors $\imath$ est injectif, π est surjectif, la composée $\pi \circ \imath$ est nulle et on a même l'égalité $\mathrm{Im}(\imath) = \ker(\pi)$. Cette situation se produit très souvent et il est commode de parler dans ce cas de suites exactes de A-modules :

$$0 \longrightarrow N \xrightarrow{\imath} M \xrightarrow{\pi} M/N \longrightarrow 0$$

Dans cette suite de morphismes les applications $\{0\} \longrightarrow N$ et $M/N \longrightarrow \{0\}$ sont les seules possibles et on note 0 le module réduit à $\{0\}$ par abus. Plus généralement on peut parler de suite exacte de longueur quelconque :

Définition 1.12
Soit $(f_n\colon M_n \longrightarrow M_{n+1})_{n\in\mathbb{N}}$ *une famille de morphismes de A-modules.*

1. *On dit que la suite*
$$\cdots \longrightarrow M_{n-1} \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} M_{n+1} \longrightarrow \cdots$$
est exacte en M_n *lorsque* $\mathrm{Im}(f_{n-1}) = \ker(f_n)$.
2. *On dit que la suite*
$$\cdots \longrightarrow M_{n-1} \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} M_{n+1} \longrightarrow \cdots$$
est exacte lorsqu'elle est exacte en M_n *pour tout* n.

Proposition 1.11

1. *Dire que* $M \xrightarrow{\alpha} N \longrightarrow 0$ *est une suite exacte de module revient à dire que* α *est un morphisme de modules surjectif.*
2. *Dire que* $0 \longrightarrow M \xrightarrow{\beta} N$ *est une suite exacte de module revient à dire que* β *est un morphisme de modules injectif.*
3. *Si un module* M *apparaît dans une suite exacte* $0 \longrightarrow M \longrightarrow 0$ *alors le module* M *est nul.*
4. *Dire que* $0 \longrightarrow M \xrightarrow{\gamma} N \longrightarrow 0$ *est une suite exacte revient à dire que* γ *est un isomorphisme.*

Démonstration : C'est immédiat.

Lemme 1.4
Soit $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ *une suite exacte (courte) de A-modules. Les assertions suivantes sont équivalentes :*

(i) *Le sous-module* $\alpha(A)$ *est facteur direct de* B.
(ii) *Il existe un sous-module* $F \subset B$ *tel que la restriction de* β *à* F *soit un isomorphisme* $F \cong C$.
(iii) *Il existe un morphisme* $a\colon B \longrightarrow A$ *tel que* $a \circ \alpha = \mathrm{Id}_A$.
(iv) *Il existe un morphisme* $b\colon C \longrightarrow B$ *tel que* $\beta \circ b = \mathrm{Id}_C$.

Lorsque ces conditions sont vérifiées, le morphisme $b \mapsto (a(b), \beta(b))$ *est un isomorphisme* $B \cong A \oplus C$.

Démonstration. Pour établir cette équivalence on montre successivement les implications $(i) \implies (ii) \implies (iv) \implies (iii) \implies (i)$.
On montre $(i) \implies (ii)$. Si $\alpha(A)$ est facteur direct soit F un supplémentaire à $\alpha(A)$ dans B. Par définition des suites exactes $\ker\beta = \alpha(A)$ et on a donc $\ker\beta \cap F = \{0\}$. Si $c \in C$ il existe un $b \in B$ tel que $\beta(b) = c$. Or B est somme de F et $\alpha(A)$. Il existe donc $f \in F$ et $a \in \ker(\beta)$ tel que $b = f + a$. On a donc $\beta(f) = \beta(b) = c$. La restriction de β au sous-module F est bien un isomorphisme.
On montre $(ii) \implies (iv)$. Soit F tel que $\beta\colon F \longrightarrow C$ soit un isomorphisme, soit $\gamma\colon C \longrightarrow F$ le morphisme réciproque et soit $\varepsilon\colon F \longrightarrow B$ le morphisme donné par l'inclusion. Alors $b = \varepsilon \circ \gamma$ vérifie bien $\beta \circ b = \mathrm{Id}_C$.
On montre $(iv) \implies (iii)$. Puisque α est injective il existe toujours un isomorphisme réciproque $\eta\colon \alpha(A) \longrightarrow A$. Pour $x \in b$, on pose $p(x) = x - b \circ \beta(x)$. On définit ainsi un morphisme $p\colon B \longrightarrow B$. Alors comme $\alpha(A) = \ker(\beta)$ la restriction de p à $\alpha(A)$ est

l'identité. Si $x \in B$ alors $\beta(p(x)) = \beta(x) - \beta \circ b \circ \beta(x) = 0$ car $\beta \circ b = \mathrm{Id}_C$. Donc l'image de p est contenu dans $\alpha(A)$. Le morphisme $a = \eta \circ p$ vérifie bien $a \circ \alpha = \mathrm{Id}_A$.

On montre $(iii) \implies (i)$. Pour ce, on vérifie que $\ker a$ est un supplémentaire de $\alpha(A)$ dans B. Soit $x \in \ker a \cap \alpha(A)$. Alors il existe $y \in A$ tel que $x = \alpha(y)$. Et comme $a \circ \alpha = \mathrm{Id}_A$, on a $0 = a(x) = a(\alpha(y)) = y$. Il suit $x = \alpha(y) = 0$. On a bien $\alpha(A) \cap \ker a = \{0\}$. Soit $x \in B$. Alors $a(x - \alpha(a(x))) = a(x) - a(\alpha(a(x))) = 0$ puisque $a \circ \alpha = \mathrm{Id}_A$. Donc $x - \alpha(a(x)) \in \ker a$. Donc, comme $\alpha(a(x))$ appartient à $\alpha(A)$, l'élément x appartient à $\langle \alpha(A) \cup \ker a \rangle$.

On a démontré les équivalences requises. Si ces conditions sont remplies, l'application $b \mapsto (a(b), \beta(b))$ est clairement linéaire, et son morphisme réciproque est $(x, y) \mapsto \alpha(x) + b(y)$, comme on le voit par un calcul immédiat.

Définition 1.13
Lorsque les conditions équivalentes du lemme 1.4 sont vérifiées on dit que la suite exacte $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ *est* scindée, *on dit que a est une* section *de α, et on dit que b est une* section *de β.*

Remarques

1. Lorsque A est un corps tous les sous-espaces vectoriels sont facteurs directs et toutes les suites courtes sont scindées. Il est alors préférable d'utiliser la notion de somme directe plus facile à manier et il serait ridicule de parler de suites exactes d'espaces vectoriels. Bien entendu pour les modules il existe des suites qui ne sont pas scindées, par exemple la suite exacte de $\mathbb{Z}$-modules $0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{\overline{x} \mapsto \overline{px}} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\overline{x} \mapsto \overline{x}} \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$ n'est pas scindée (voir exercice 22).

2. Soit $\ldots \longrightarrow M \xrightarrow{f} N$ une suite exacte ne terminant pas par 0. Alors la suite $\ldots \longrightarrow M \xrightarrow{f} N \xrightarrow{\pi_{f(M)}} N/f(M) \longrightarrow 0$ est une suite exacte terminant par 0.

3. Soit $N \xrightarrow{g} M \longrightarrow \ldots$ une suite exacte ne commençant pas par 0. Alors la suite $0 \longrightarrow \ker g \longrightarrow N \xrightarrow{g} M \longrightarrow \ldots$ est une suite exacte qui commence par 0.

4. Soit $\ldots \longrightarrow A \longrightarrow B \xrightarrow{f} C \longrightarrow \ldots$ une suite exacte avec plus de trois modules non nuls. Alors on peut la « couper » pour obtenir une suite exacte à trois termes non nuls (dite suite exacte courte) et les deux suites moins longues qui suivent :
$$\cdots \longrightarrow A \longrightarrow \ker f \longrightarrow 0$$
$$0 \longrightarrow \ker f \longrightarrow B \xrightarrow{f} \mathrm{Im}\, f \longrightarrow 0$$
$$0 \longrightarrow \mathrm{Im}(f) \longrightarrow C \longrightarrow \cdots$$

5. On peut conclure des remarques 2, 3 et 4 ci-dessus que l'étude des suites exactes se ramène à celle des suites exactes courtes c'est-à-dire aux modules quotients. Cependant il est plus commode et élégant lorsque c'est possible de ne considérer qu'une seule suite longue plutôt que de multiplier les suites courtes.

Définition 1.14
Soit M un A-module, soit $m \in M$ et soit S un sous-ensemble de M. On dit que m est

1. *de torsion si il existe $\lambda \in A$ non nul et ne divisant pas 0 tel que $\lambda m = 0$.*
2. *divisible si pour tout $\mu \in A$ il existe $y \in M$ tel que $m = \mu y$.*
3. *indivisible lorsque les seuls $y \in M$ et $\mu \in A$ vérifiant $m = \mu y$ sont les $\mu \in A^\times$ et $y = \mu^{-1}m$.*
4. *On note $T_A(M)$ ou $T(M)$ l'ensemble des éléments de torsion de M.*
5. *On note $\mathrm{Ann}_A(S)$ ou $\mathrm{Ann}(S)$ l'ensemble des éléments λ de A tels que $\forall s \in S \quad \lambda s = 0$.*
6. *On dit que M est de torsion si $T_A(M) = M$.*
7. *On dit que M est sans torsion si $T_A(M) = \{0\}$.*

Remarques La terminologie classique peut ici prêter à confusion. Être *indivisible* n'est pas le contraire d'être *divisible*. Par exemple dans le $\mathbb{Z}$-module libre de rang 1 seuls 1 et -1 sont indivisible (en effet on a toujours $x = x\ 1$, et x est soit inversible soit non indivisible dans $\mathbb{Z}$). Pourtant aucun élément de $\mathbb{Z}$ n'est divisible car pour tout $x \in \mathbb{Z}$ il existe $n \in \mathbb{N}$ tel que $x/2^n \notin \mathbb{Z}$.

Proposition 1.12 *Soit M un A-module et $S \subset M$. Si A est commutatif alors*

1. *$T_A(M)$ est un sous-module de M. On dit que $T_A(M)$ est le sous-module de torsion de M.*
2. *$\mathrm{Ann}_A(S)$ est un idéal de A. On dit que $\mathrm{Ann}_A(S)$ est l'annulateur du sous-module engendré par S.*

Démonstration

1. $0 \in T_A(M)$ car $1\ 0 = 0$. Soit $x, y \in T_A(M)$ et soit $\lambda, \mu \in A$ non nul et ne divisant pas 0 tels que $\lambda x = \mu y = 0$. Alors $\lambda\mu$ est non nul et ne divise pas 0. De plus pour tout $\alpha, \beta \in A$ on a $\lambda\mu(\alpha x - \beta y) = \mu\alpha\lambda x - \lambda\beta\mu y = 0$ puisque A est commutatif. On a donc bien $(\alpha x - \beta y) \in T_A(M)$.
2. voir l'exercice 15

Remarque Les modules libres sont sans torsion. Autrement dit un module dont la torsion est non triviale, comme par exemple le $\mathbb{Z}$-module de torsion $\mathbb{Z}/15\mathbb{Z}$ n'est pas libre. Le sous-module de torsion est donc une obstruction à la liberté d'un module. On verra que pour les modules de type fini sur les anneaux principaux il suffit de lever cette obstruction : un module de type fini sur un anneau principal est libre si et seulement si il est sans torsion. Dès lors que la torsion est identifiée comme une obstruction, il peut être utile de se ramener à des modules sans torsion. La méthode algébrique usuelle pour ce faire est de passer au quotient :

Proposition 1.13 *Soit M un A-module. Alors le A-module $M/T_A(M)$ est sans torsion.*

Démonstration. Soit $x \in M/T_A(M)$ de torsion, et soit $\lambda \in A$ non nul et ne divisant pas zéro tel que $\lambda x = 0$. Prenons $y \in M$ relevant x (c'est-à-dire tel que $\pi_{T_A(M)}(y) = x$). Alors $\pi_{T_A(M)}(\lambda y) = \lambda x = 0$ et donc $\lambda y \in T_A(M)$. Il existe donc un μ non nul et ne divisant pas 0 dans A tel que $\mu\lambda y = 0$. Donc y est de torsion et $x = \pi_{T_A(M)}(y) = 0$.

Chapitre 2

Classification des modules de type fini sur les anneaux principaux

Dans toute la suite A désigne un anneau commutatif unitaire intègre et principal.

2.1 Présentation matricielle des modules de type fini

Définition 2.1
Soit M un A-module. On dit que M est de type fini lorsqu'il existe une partie fini $F \subset M$ telle que $M = \langle F \rangle$.

Lemme 2.1
Soit n un entier, $L \cong A^n$ un module libre de rang n et $N \subset A^n$ un sous-module. Alors N est libre de rang inférieur ou égal à n.

Démonstration : On procède par récurrence sur n. Si $n = 1$ les sous-modules de A sont les idéaux de A qu'on a supposé principal. Un idéal de A est ou bien réduit à 0 c'est-à dire libre de rang 0 ou bien de la forme $A\alpha$ pour $\alpha \neq 0$ c'est-à-dire libre de rang 1, et le lemme est vrai pour $n = 1$. Soit k un entier quelconque et supposons le lemme pour $n = k - 1$. Soit N un sous-module de A^k. Soit $p_k \colon A^k \longrightarrow A$ la projection sur la dernière coordonnée. Alors p_k est surjective et son noyau est libre de rang $n-1$. Si $N \subset \ker p_k$ alors N est libre par récurrence. Sinon $p_k(N)$ est un sous-module non nul de A et il existe $\alpha \in A$ tel que $p_k(N) = A\alpha$. Soit $x \in N$ tel que $p_k(x) = \alpha$. Par récurrence $N \cap \ker p_k$ est libre de rang au plus $(n-1)$. Le produit direct externe $Ax \oplus (N \cap \ker p_k)$ est donc libre de rang au plus k. Pour conclure on vérifie donc que $N = (N \cap \ker p_k) \oplus Ax$. Soit $y \in N$ alors il existe $\lambda \in A$ tel que $p_k(y) = \lambda\alpha = p_k(\lambda x)$. Donc $y - \lambda x \in \ker p_k$ et on a bien $N = (\ker p_k \cap N) + Ax$. Soit $y \in N \cap \ker p_k \cap Ax = \ker p_k \cap Ax$. Alors $y \in Ax$ donc il existe $\lambda \in A$ tel que $y = \lambda x$ et $y \in \ker p_k$ on a donc $0 = p_k(y) = p_k(\lambda x) = \lambda\alpha$. Puisque $\alpha \neq 0$ et A est intègre on en déduit $\lambda = 0$ puis $y = \lambda x = 0$, ce qui termine la preuve.
Soit M un A-module de type fini et soit $F \subset M$ un système générateur fini de M. Alors $\varphi \colon (a_f)_{f\in F} \mapsto \sum_f a_f f$ est un morphisme surjectif du module libre A^F dans M, et par

factorisation M est isomorphe au quotient $A^F/\ker\varphi$. En conséquence du point de vue de la structure de module la connaissance des modules de type fini admettant n générateurs équivaut à celle des sous-modules de A^n (qui sont aussi de type fini par le lemme 2.1).

Définition 2.2
Soit f un entier et M un module de type fini admettant un système de générateurs $x_1,\dots,x_f$. Soit $(\varepsilon_i)_{i=1}^{i=f}$ la base canonique de A^f et soit $\varphi\colon A^f \longrightarrow M$ le morphisme surjectif défini par linéarité avec $\varphi(\varepsilon_i)=x_i$. On appelle sous-module des relations entre les x_i et on note R le noyau $R=\ker\varphi$. La donnée d'un système générateur fini $r_1,\dots r_s$ de R, s'appelle une présentation du module M par générateurs et relations (auquel cas on appelle parfois les r_i « relations élémentaires »).

Par définition un élément $(a_i)_{i=1}^{i=f}$ de R correspond à une relation de dépendance linéaire $\sum_i a_i x_i = 0$, d'où la terminologie. D'après le lemme 2.1 on peut présenter M à l'aide d'au plus f relations élémentaires. En complétant, si besoin est, ces relations élémentaires avec des vecteurs nuls on obtient ainsi f vecteurs $r_1,\dots,r_f$ du module libre A^f. En écrivant ces vecteurs en colonne $r_j=\sum_{i=1}^{i=f} r_{i,j}\varepsilon_i$ on obtient une matrice $\mathcal{R}=[r_{i,j}]\in M_f(A)$ qui est la matrice dans la base ε_i du morphisme $\rho\colon A^f\longrightarrow A^f$ défini par linéarité en posant $\rho(\varepsilon_i)=r_i$. Bien entendu l'image de ρ est $R=\rho(A^f)$.

Définition 2.3
La matrice $\mathcal{R}$ ainsi obtenu s'appelle la matrice des relations du module M.

Lemme 2.2
On conserve les notations f, M, ρ, R et r_i qui précédent. Soit g, h deux isomorphismes de A^f. Alors $M\cong A^f/R\cong A^f/g\circ\rho\circ h(A^f)$.

Démonstration : Comme on est parti d'une présentation du module M l'isomorphie $M\cong A^f/R$ est claire. Puisque h est un isomorphisme on a $\rho\circ h(A^f)=\rho(A^f)=R$. On vérifie l'isomorphie $A^f/R\cong A^f/g(R)$. Soit $\pi_{g(R)}$ le passage au quotient $\pi_{g(R)}\colon A^f\longrightarrow A^f/g(R)$ et soit ψ le morphisme composé surjectif $\psi=\pi_{g(R)}\circ g$. Pour $x\in A^f$ on a les équivalences $x\in\ker\psi \iff g(x)\in\ker\pi_{g(R)} \iff g(x)\in g(R) \iff x\in R$ puisque g est un isomorphisme. Autrement dit $\ker\psi=R$ et par factorisation on obtient $A^f/R\cong A^f/g(R)$.

2.2 le théorème de la base adaptée : énoncé de résultats

Soit M un A-module engendré par f générateurs $x_1,\dots,x_f$ et soit $\mathcal{R}\in M_f(A)$ la matrice des relations de M. Le lemme 2.2 montre qu'on peut sans changer la classe d'isomorphie du module M multiplier à gauche et à droite la matrice $\mathcal{R}$ par les matrices $\mathcal{G}$ et $\mathcal{H}$ de $GL_f(A)$[1] correspondant dans la base ε_i aux isomorphismes g et h. Pour en tirer des conséquences en termes de modules il suffit donc de choisir les matrices $\mathcal{G}$ et $\mathcal{H}$ de sorte que $D=\mathcal{GRH}$ soit le plus simple possible.

Définition 2.4 *Deux matrices $\mathcal{M}$ et $\mathcal{N}$ dans $M_f(A)$ sont dites équivalentes lorsqu'il existe $\mathcal{G},\mathcal{H}\in GL_f(A)$ telles que $\mathcal{M}=\mathcal{GNH}$. On note $\mathcal{M}\sim\mathcal{N}$ la relation d'équivalence ainsi définie.*

[1] $GL_f(A)$ désigne le sous-ensemble des matrices inversibles correspondant aux endomorphismes bijectifs de A^f. Le déterminant de ces matrices appartient à $A^\times$ (et M est inversible si et seulement si $\det M\in A^\times$)

Pour démontrer le théorème de la base adaptée qui est le résultat principal de ce cours, on admet provisoirement le lemme d'algèbre linéaire suivant qui donne un représentant simple des classes d'équivalences de matrices.

Lemme 2.3
Soit f un entier et soit $\mathcal{R}$ une matrice de $M_f(A)$. Il existe des matrices $\mathcal{G}$ et $\mathcal{H}$ dans $GL_f(A)$ et une suite $d_1 \mid d_2 \mid \ldots \mid d_f$ d'éléments de A ordonnée par divisibilité (les derniers d_j étant éventuellement nul) tels que $\mathcal{GRH}$ soit la matrice diagonale D dont le $i^{ème}$ coefficient diagonal est d_i. Soit D' une autre matrice diagonale de $M_f(A)$ équivalente à $\mathcal{R}$ dont les termes diagonals (d'_i) sont ordonnés par divisibilité. Alors pour tout i les idéaux principaux (d_i) et (d'_i) sont égaux. En d'autre termes les idéaux emboîtés $(d_f) \subset (d_{f-1}) \subset \ldots \subset (d_1)$ fournissent un système complet d'invariants des classes d'équivalences de matrices de $M_f(A)$.

On démontrera ce lemme dans les sections qui suivent. Pour le cas particulier des anneaux euclidien on donnera l'algorithme de Smith pour calculer D. Cela repose sur des opérations élémentaires dans le style de l'algorithme du pivot de Gauss, mais sans divisions.

Théorème 2.1 base adaptée
Soit R un sous-module de A^f. Alors il existe une suite finie $d_1 \mid d_2 \mid \ldots d_f$ d'éléments de A ordonnée par divisibilité et une base $e_1, \ldots e_f$ de A^f telle que

$$R = \bigoplus_{i=1}^{i=f} Ad_i e_i \ .$$

Démonstration : Soit $r_1, \ldots, r_f$ un système générateur (éventuellement complété par des vecteurs nuls) à f éléments de R, dont l'existence est assurée par le lemme 2.1. Soit $\varepsilon_1, \ldots \varepsilon_f$ la base canonique de A^f. On forme la matrice $\mathcal{R}$ de l'application linéaire ρ: $A^f \longrightarrow A^f$ définie par linéarité avec $\rho(\varepsilon_i) = r_i$. Bien entendu $R = \rho(A^f)$ et l'étude de R se ramène à celle de $\mathcal{R}$. Soient $d_1 \mid \ldots \mid d_f$ les éléments de A et D, $\mathcal{G}$, et $\mathcal{H}$ les matrices du lemme 2.3. Alors D est la matrice diagonale dont le $i^{ème}$ coefficient diagonal est d_i et $\mathcal{GRH} = D$. On note δ (resp. g, h) les endomorphismes de A^f représentés dans la base ε_i par les matrices D (resp. $\mathcal{G}$, $\mathcal{H}$). On a $\delta = g \circ \rho \circ h$ et donc pour tout i $d_i\varepsilon_i = g(\rho(h(\varepsilon_i)))$. Comme g est un isomorphisme la famille $e_i = g^{-1}(\varepsilon_i)$ est une base de A^f. Comme les e_i sont libre la somme $\sum Ad_ie_i$ est directe (éventuellement les derniers d_i sont nuls : on n'impose pas à R d'être de rang maximal). Il suffit donc de montrer que le système d_ie_i engendre R. Mais $R = \rho(A^f) = \rho(h(A^f)) = g^{-1}\delta(A^f)$. Donc R est engendré par les $g^{-1}(\delta(\varepsilon_i)) = d_ie_i$.

Remarque Cette démonstration fournit aussi une méthode pour calculer la base adaptée à un sous-module de A^f. On verra en effet dans la section qui suit comment calculer les matrices D et $\mathcal{G}$ qui précèdent. On obtient alors les coordonnées dans la base de départ ε_i des vecteurs e_i de la base adaptée en inversant la matrice $\mathcal{G}$, puisque $e_i = g^{-1}(\varepsilon_i)$.

Définition 2.5 *Soit $R \subsetneq A^f$. Une base $e_1, \ldots, e_f$ de A^f comme dans le théorème 2.1 s'appelle une base de A^f adaptée au sous-module R. Il existe un rang j à partir duquel les d_j du théorème 2.1 ne sont plus inversibles. On appelle diviseurs élémentaires du module quotient $M = A^f/R$ la suite $d_j \mid d_{j+1} \mid \ldots \mid d_f$.*

Corollaire 2.1.1
Soit M un A-module de type fini. Soit $q_1 \mid q_2 \mid \ldots \mid q_f$ la suite des diviseurs élémentaires (non inversibles) de M, et soit $1 \leq s \leq f+1$ tel que les q_i soient non nuls pour tout $i < s$ et $q_s = 0$ (on pose $s = f+1$ si $q_f \neq 0$).

1. *M est isomorphe à la somme directe*
$$M \cong \bigoplus_{i=1}^{i=f} A/q_iA$$
2. *Il existe un module libre $L \subset M$ de rang $f - s + 1$ tel que $M = T(M) \oplus L$.*
3. *Le sous-module de torsion de M est isomorphe à la somme directe*
$$T(M) \cong \bigoplus_{i=1}^{i=s-1} A/q_iA$$
4. *$s = 1 \iff T(M) = 0 \iff M$ est libre.*

Démonstration : puisque M est de type fini on part d'un système générateur $m_1, \ldots, m_n$ de M et on se donne un système $r_1, \ldots, r_n$ de relations élémentaires entre les m_i. On applique le théorème de la base adaptée 2.1 au sous-module $R \subset A^n$ engendré par les r_i. On obtient donc
$$M \cong \frac{A^n}{R} \cong \frac{\bigoplus_{i=1}^{i=n} Ae_i}{\bigoplus_{i=1}^{i=n} Ad_ie_i} \cong \bigoplus_{i=1}^{i=n} \frac{A}{d_iA}$$
Si d_1 est inversible le facteur $A/d_1A = 0$ est redondant et en supprimant les d_i inversibles on obtient la suite des diviseurs élémentaires $(q_i)_{i=1}^{i=f}$ de M et l'isomorphisme du 1-. Pour $j \geq s$ les q_j sont nuls et le facteur direct $\oplus_{s \leq j \leq f} A/q_jA \cong A^{f-s+1}$ est libre. Clairement $T(\oplus_{1 \leq j \leq f} A/q_jA) = \oplus_{1 \leq j < s} A/q_jA$, ce qui donne 2- et 3- et la première équivalence du 4-. L'implication L libre implique $T(M) = 0$ est évidente. L'implication réciproque provient du 2-.

Théorème 2.2
Soit M et N deux A-modules et soit $m_1, \ldots, m_s$ les diviseurs élémentaires de M et $n_1, \ldots, n_t$ les diviseurs élémentaires de N. On suppose $M \cong N$. Alors $s = t$ et pour tout i l'idéal (m_i) est égal à l'idéal (n_i).

Démonstration : Quite à échanger M et N on peut supposer $s \geq t$. On rajoute si nécessaire des 1 au début de la suite des n_i, et on peut ainsi supposer $s = t$: a posteriori on aura $(n_1) = (m_1) \neq A$ de sorte que l'égalité $s = t$ était vrai sans ajout. En partant de l'isomorphisme $M \cong N$ on obtient un isomorphisme $T(M) \cong T(N)$ et par factorisation $M/T(M) \cong N/T(N)$. Par le corollaire 2.1.1 $M/T(M)$ et $N/T(N)$ sont libres. Ils sont isomorphes donc de même rangs : il y a autant de $m_i = 0$ que de $n_i = 0$ et avec l'isomorphisme $T(M) \cong T(N)$ on est ramené au cas particulier M et N de torsion et $s = t$. Pour montrer l'égalité des idéaux $(m_i) = (n_i)$ on montre que pour tout irréductible π de A et tout entier n, on a équivalence entre $\pi^n \mid m_i$ et $\pi^n \mid n_i$. On énonce d'abord un lemme utile.

Lemme 2.4
Soit π un irréductible de A, n un entier et $d \in A$ non nul. Alors $\dfrac{\pi^n(A/dA)}{\pi^{n+1}(A/dA)}$ est un espace vectoriel sur le corps $A/\pi A$ de dimension 1 si π^{n+1} divise d et de dimension 0 sinon.

Démonstration du lemme On écrit $d = \pi^j d'$ avec d' non divisible par π. Par le lemme Chinois on a $A/dA \cong A/\pi^j A \oplus A/d'A$ et on en déduit $\dfrac{\pi^n(A/dA)}{\pi^{n+1}(A/dA)} \cong \dfrac{\pi^n(A/\pi^j A)}{\pi^{n+1}(A/\pi^j A)} \oplus \dfrac{\pi^n(A/d'A)}{\pi^{n+1}(A/d'A)}$. Puisque $\pi \nmid d'$ on sait avec une relation de Bezout inverser π modulo d' et pour tout k on a $\pi^k(A/d'A) = A/d'A$ d'où $\dfrac{\pi^n(A/d'A)}{\pi^{n+1}(A/d'A)} = 0$. On peut donc supposer $d' = 1$.
Montrons que si $j > n$ alors $\dfrac{\pi^n(A/\pi^j A)}{\pi^{n+1}(A/\pi^j A)} \cong A/\pi A$. On considère le morphisme surjectif $\theta\colon A \longrightarrow \dfrac{\pi^n(A/\pi^j A)}{\pi^{n+1}(A/\pi^j A)}$ défini par $\theta(a) = \overline{\pi^n a}$. Soit $a \in \ker\theta$. Alors $\overline{\pi^n a} \in \pi^{n+1}(A/\pi^j A)$ et donc il existe b, $c \in A$ tels que $\pi^n a = \pi^{n+1}b + \pi^j c$. Puisque $j > n$ on simplifie par π^n et il vient $a = \pi(b + \pi^{j-n-1}c) \in \pi A$. D'où l'égalité $\ker\theta = \pi A$ l'inclusion réciproque étant claire. Par factorisation on conclut $\dfrac{\pi^n(A/\pi^j A)}{\pi^{n+1}(A/\pi^j A)} \cong A/\pi A$. Si $j \leq n$ alors $\dfrac{\pi^n(A/\pi^j A)}{\pi^{n+1}(A/\pi^j A)} = 0$, puisque $\overline{\pi^n} = \overline{0}$ dans $A/\pi^j A$. Cela termine la preuve du lemme.
On reprend la démonstration du théorème. Soit $f\colon M \longrightarrow N$ l'isomorphisme dont on a supposé l'existence. Par linéarité de f on obtient pour tout $\pi \in A$ et tout $n \in \mathbb{N}$ l'égalité $f(\pi^n M) = \pi^n N$ et l'isomorphie $\pi^n M \cong \pi^n N$. En conséquence on a pour tout irréductible π et tout $n \in \mathbb{N}$ isomorphie entre $\pi^n M/\pi^{n+1}M$ et $\pi^n N/\pi^{n+1}N$. Ces deux quotients sont des espaces vectoriels sur $A/\pi A$, la dimension du premier est égale au nombre de m_i divisible par π^{n+1} la dimension du second est le nombre de n_i divisible par π^{n+1}. Comme les m_i et les n_i sont ordonnés par divisibilité on obtient bien pour tout i, $k \in \mathbb{N}$ et tout irréductible π l'équivalence $\pi^k \mid m_i \iff \pi^k \mid n_i$. Cela termine la preuve du théorème.

Proposition 2.1
Soit G un groupe abélien de type fini, alors il existe une suite d'entiers $d_1 \mid \ldots \mid d_s$ positifs ou nul et distincts de 1 tels que $G \cong \oplus_i \mathbb{Z}/d_i$. La suite des d_i s'appelle la suite des diviseurs élémentaires de G. Deux groupe abéliens sont isomorphes si et seulement si ils ont même suite de diviseurs élémentaires.

Démonstration : On considère G comme un $\mathbb{Z}$-module et on applique les théorèmes 2.2 et le corollaire 2.1.1. Puisqu'on a pris soin de prendre des diviseurs élémentaires positifs on peut remplacer l'égalité entre les idéaux engendrés par ces diviseurs par l'égalité entre ces diviseurs eux-mêmes.

Il reste à démontrer le lemme 2.3, c'est-à-dire étudier à équivalence près les matrices à coefficients dans un anneau principal. Cette démonstration fait l'objet des trois dernières sections de ce cours. La section qui suit décrit des transformations que l'ont peut faire subir à une matrice sans changer sa classe d'équivalence. Puis on donne une démonstration algorithmique du lemme 2.3 lorsque l'anneau est euclidien. En dernière section on décrit comment modifier la preuve euclidienne dans le cas plus général des anneaux principaux.

2.3 Opérations élémentaires sur les matrices

Soit M une matrice dans $M_f(A)$. On numérote $L_1, \ldots, L_f \in A^f$ les vecteurs lignes de M et $C_1, \ldots, C_f$ les vecteurs colonnes de M. On décrit une liste *d'opérations élémentaires* sur ces vecteurs lignes (respectivement colonnes) de M. Il s'agit de modifications que l'on peut apporter à ces vecteurs sans changer la classe d'équivalence de M. En un sens que l'on ne précisera pas dans ce cours, lorsque l'anneau A est euclidien, ce sont les seules opérations avec cette propriété. Effectuer une opération sur les lignes de M revient à multiplier à gauche M par une *matrice élémentaire* $E \in GL_f(A)$. Effectuer une opération sur les colonnes de M revient à multiplier à droite M par une matrice élémentaire.

Définition 2.6

1. *Soit $\lambda \in A$ et $k, l \in \{1, \ldots, f\}$ tels que $l \neq k$. On note $E_{k,l}(\lambda) = [e_{i,j}]$ la matrice dont les coefficients sont*
$$e_{i,j} = \begin{cases} 1 \text{ si } i = j \\ \lambda \text{ si } i = k \text{ et } j = l \\ 0 \text{ sinon} \end{cases}$$
2. *Soit $k, l \in \{1, \ldots, f\}$ tels que $l \neq k$. On note $S_{k,l} = [s_{i,j}]$ la matrice dont les coefficients sont*
$$s_{i,j} = \begin{cases} 1 \text{ si } i = j,\ i \neq k \text{ et } i \neq l \\ 0 \text{ si } i = j = k \text{ ou } i = j = l \\ 1 \text{ si } \{i, j\} = \{k, l\} \\ 0 \text{ sinon} \end{cases}$$

Les matrices ci-dessus s'appellent des matrices élémentaires. Examinons l'effet sur les lignes (respectivement les colonnes) de la multiplication par ces matrices :

Proposition 2.2

$$E_{k,l}(\lambda) \begin{bmatrix} L_1 \\ \vdots \\ L_k \\ \vdots \\ L_l \\ \vdots \\ L_f \end{bmatrix} = \begin{bmatrix} L_1 \\ \vdots \\ L_k + \lambda L_l \\ \vdots \\ L_l \\ \vdots \\ L_f \end{bmatrix}$$

Démonstration C'est immédiat.

Proposition 2.3

$$[C_1, \ldots, C_k, \ldots, C_l, \ldots C_f] E_{k,l}(\lambda) = [C_1, \ldots, C_k, \ldots, C_l + \lambda C_k, \ldots, C_f].$$

Démonstration C'est immédiat.

Proposition 2.4

$$S_{k,l}\begin{bmatrix} L_1 \\ \vdots \\ L_k \\ \vdots \\ L_l \\ \vdots \\ L_f \end{bmatrix} = \begin{bmatrix} L_1 \\ \vdots \\ L_l \\ \vdots \\ L_k \\ \vdots \\ L_f \end{bmatrix}.$$

Démonstration C'est immédiat.

Proposition 2.5

$$[C_1, \ldots, C_k, \ldots, C_l, \ldots, C_f]S_{k,l} = [C_1, \ldots, C_l, \ldots, C_k, \ldots, C_f]$$

Démonstration C'est immédiat.
Lorsqu'on multiplie une matrice M à gauche par la matrice $E_{k,l}(\lambda)$ on laisse toutes les lignes de de M inchangées sauf la k-ième ligne qui est remplacée par $L_k + \lambda L_l$. Lorsqu'on multiplie à droite une matrice M par la matrice $E_{k,l}(\lambda)$ on laisse toute les colonnes de M inchangées sauf la l-ième qui est remplacée par $C_l + \lambda C_k$. Multiplier une matrice M à gauche par la matrice $S_{k,l}$ échange les k-ième et l-ième lignes de M. Multiplier à droite une matrice M par la matrice $S_{k,l}$ échange les k-ième et l-ième lignes de M. Ces opérations (dites opérations élémentaires sur les lignes et colonnes de M) ne changent donc pas la classe d'équivalence de M. Dans le cas particulier des anneaux euclidiens elles suffisent pour démontrer le lemme 2.3.

Exemple Pour bien comprendre comment utiliser ces transformations élémentaire on va voir comment réduire la matrice

$$M = \left|\begin{array}{cccc} 3 & 2 & -3 & 3 \\ 2 & 2 & -2 & 2 \\ 10 & 0 & 0 & 10 \\ 8 & -2 & 2 & 8 \end{array}\right|$$

Les opérations effectuées sur les colonnes sont indiquées au fur et à mesure. La dernière colonne contenant des polynômes en X, Y, Z et T permet conserver les opérations effectuées sur les lignes. C'est une notation commode pour retrouver la la matrice $\mathcal{G}$ de la remarque qui suit le théorème de la base adaptée (théorème 2.1).

$$\left|\begin{array}{cccc|c} 3 & 2 & -3 & 3 & X \\ 2 & 2 & -2 & 2 & Y \\ 10 & 0 & 0 & 10 & Z \\ 8 & -2 & 2 & 8 & T \end{array}\right| \begin{array}{c} C_3 \leftarrow C_3 + C_1 \\ C_4 \leftarrow C_4 - C_1 \\ \sim \end{array} \left|\begin{array}{cccc|c} 3 & 2 & 0 & 0 & X \\ 2 & 2 & 0 & 0 & Y \\ 10 & 0 & 10 & 0 & Z \\ 8 & -2 & 10 & 0 & T \end{array}\right|$$

On a commencé par faire apparaître les plus de zéros possible **en utilisant des opérations sur les colonnes**. A ce stade le p.g.c.d. des coefficients de la matrice est 1. On peut le faire

apparaître en position de pivot (première ligne, première colonne) en enlevant la deuxième colonne à la première.

$$\left|\begin{array}{cccc|c} 3 & 2 & 0 & 0 & X \\ 2 & 2 & 0 & 0 & Y \\ 10 & 0 & 10 & 0 & Z \\ 8 & -2 & 10 & 0 & T \end{array}\right| \begin{array}{c} \\ C_1 \leftarrow C_1 - C_2 \\ \sim \\ \\ \end{array} \left|\begin{array}{cccc|c} 1 & 2 & 0 & 0 & X \\ 0 & 2 & 0 & 0 & Y \\ 10 & 0 & 10 & 0 & Z \\ 10 & -2 & 10 & 0 & T \end{array}\right|$$

Puisque on a un 1 en position de pivot (un diviseur commun à tous les coefficients de la matrice) on peut l'utiliser pour faire apparaître des 0 sur la première ligne et la première colonne avec les opérations élémentaires ad hoc. Ce principe théorique montre que cette méthode de calcul aboutit toujours à une matrice diagonale. En pratique si on veut obtenir ensuite une base adaptée il est préférable de toujours faire le plus possible d'opérations sur les colonnes. Ici par exemple on peut simplifier la première colonne sans opérer sur les lignes.

$$\left|\begin{array}{cccc|c} 1 & 2 & 0 & 0 & X \\ 0 & 2 & 0 & 0 & Y \\ 10 & 0 & 10 & 0 & Z \\ 10 & -2 & 10 & 0 & T \end{array}\right| \begin{array}{c} \\ C_1 \leftarrow C_1 - C_3 \\ \sim \\ \\ \end{array} \left|\begin{array}{cccc|c} 1 & 2 & 0 & 0 & X \\ 0 & 2 & 0 & 0 & Y \\ 0 & 0 & 10 & 0 & Z \\ 0 & -2 & 10 & 0 & T \end{array}\right|$$

Maintenant que la première colonne est « nettoyée » on peut annuler tous les coefficients de la première ligne.

$$\left|\begin{array}{cccc|c} 1 & 2 & 0 & 0 & X \\ 0 & 2 & 0 & 0 & Y \\ 0 & 0 & 10 & 0 & Z \\ 0 & -2 & 10 & 0 & T \end{array}\right| \begin{array}{c} \\ C_2 \leftarrow C_2 - 2C_1 \\ \sim \\ \\ \end{array} \left|\begin{array}{cccc|c} 1 & 0 & 0 & 0 & X \\ 0 & 2 & 0 & 0 & Y \\ 0 & 0 & 10 & 0 & Z \\ 0 & -2 & 10 & 0 & T \end{array}\right|$$

A ce stade on va laisser telles quelles la première ligne et la première colonne et travailler sur la sous-matrice d'ordre 3 qui reste. Grâce aux zéros sur la première ligne (resp. colonne) les opérations élémentaire sur les lignes (resp. les colonnes) de la sous-matrice n'affectent pas la première colonne (resp. ligne). Ainsi par récurrence sur la dimension on peut rendre toute matrice semblable à une matrice diagonale, pour peu que l'on puisse faire apparaître un p.g.c.d. des coefficients de la matrice à réduire. On verra que c'est toujours possible : c'est l'idée de la preuve de la section qui suit. Dans l'exemple à traiter maintenant un p.g.c.d. des coefficient de la sous-matrice est 2 et il se trouve déjà en position de pivot. On termine la réduction avec deux opérations sur les lignes.

$$\left|\begin{array}{cccc|c} 1 & 0 & 0 & 0 & X \\ 0 & 2 & 0 & 0 & Y \\ 0 & 0 & 10 & 0 & Z \\ 0 & -2 & 10 & 0 & T \end{array}\right| \sim \left|\begin{array}{cccc|c} 1 & 0 & 0 & 0 & X \\ 0 & 2 & 0 & 0 & Y \\ 0 & 0 & 10 & 0 & Z \\ 0 & 0 & 0 & 0 & Y - Z + T \end{array}\right|$$

La matrice $\mathcal{G}$ correspondant aux opérations effectuées sur les lignes et son inverse sont :

$$\mathcal{G} = \left|\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & -1 & 1 \end{array}\right| \qquad \mathcal{G}^{-1} = \left|\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 1 & 1 \end{array}\right|$$

Soit R le sous-$\mathbb{Z}$-module de $\mathbb{Z}^4$ engendré par les vecteurs colonnes de M. Une base adaptée à R est donc la base $e_1 = (1,0,0,0); e_2 = (0,1,0,-1); e_3 = (0,0,1,1); e_4 = (0,0,0,1)$. Le calcul de l'inverse de *cette* matrice $\mathcal{G}$ est très facile car j'ai pris soin de faire le plus possible d'opérations sur les colonnes (et donc moins d'opérations sur les lignes). Le module $\mathbb{Z}^4/R$ est isomorphe à $\mathbb{Z}/2\oplus\mathbb{Z}/10\oplus\mathbb{Z}$. Évidemment il existe plusieurs "bases adaptées" à R, seule la suite canonique des idéaux emboîtés $\mathbb{Z} \supset 2\mathbb{Z} \supset 10\mathbb{Z} \supset \{0\}$ est unique. Si vous réduisez la matrice suivant un autre chemin, vous devez parvenir à la même suite $\pm 1 \mid \pm 2 \mid \pm 10 \mid 0$, mais en principe à une autre base adaptée (avec plus de calculs). Après avoir trouvé une base adaptée (dans l'ordre) $e_1; \cdots; e_n$ à un sous-module R de $\mathbb{Z}^n$ il est recommandé de vérifier au moins que les $d_i e_i$ (dans le même ordre) appartiennent à R. Cette vérification est peu coûteuse en terme de calcul et permet de détecter presque toutes les erreurs. Si l'on veut être sur du résultat il faudrait en outre vérifier que le déterminant des coefficients des e_i est inversible et que les $d_i e_i$ engendrent R. On va se contenter de détailler la première vérification. Notons $r_1 = (3,2,10,8); r_2 = (2,2,0,-2); r_3 = (-3,-2,0,2)$ et $r_4 = r_1$ les générateurs initiaux de R. Ici on obtient si nécessaire après résolutions des quatres systèmes linéaires (dont les inconnus sont x, y, z et t) $d_i e_i = x r_1 + y r_2 + z r_3 + t r_4$ la vérification :

$$\begin{aligned} 1e_1 &= -r_2 - r_3 \in R \\ 2e_2 &= 3r_2 + 2r_3 \in R \\ 10e_3 &= r_1 + r_3 \in R \\ 0e_4 &= 0 \in R \end{aligned}$$

2.4 Équivalences de matrices : l'algorithme de Smith

Le but de cette section est de démontrer le lemme 2.3 et calculer en pratique les matrices $\mathcal{G}$ et D de ce lemme dans le cas particulier des anneaux euclidiens (par exemple $\mathbb{Z}$ ou $\mathbb{K}[X]$). On appelle algorithme de Smith cette méthode de calcul. On suppose donc l'anneau A euclidien et on note φ un stathme euclidien[2] sur A. Pour $A = \mathbb{Z}$ on peut prendre $\varphi(x) = |x|$ et pour $A = \mathbb{K}[X]$ on peut prendre le degré des polynômes.

Lemme 2.5
Soit $M = [m_{i,j}] \in M_f(A)$. Alors M est équivalente à une matrice $\mathcal{A} = [a_{i,j}]$ telle que :

1. $\forall i,\ a_{1,i} = a_{i,1} = 0$
2. $\forall i, \forall j,\ \ d \mid a_{i,j}$
3. *$d = a_{1,1}$ est un p.g.c.d. des coefficients de M.*

$$M \sim \begin{bmatrix} d & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & da'_{i,j} & \\ 0 & & & \end{bmatrix}$$

[2]Par définition un stathme euclidien sur un anneau A est une application $\varphi\colon A - \{0\} \longrightarrow \mathbb{N}$ telle que : (i) Pour tout $a \in A$ et tout $b \in A$, $b \neq 0$ il existe q, $r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$. (ii) Pour tout a, $b \in A - \{0\}$, $\varphi(ab) \geq \varphi(a)$. Un anneau A est euclidien si et seulement de tels stathmes sur A existent.

Démonstration Soit $\gamma\colon M_f(A) \longrightarrow \mathbb{N}$ l'application définie par

$$\gamma([\alpha_{i,j}]) = \text{Min}\{\varphi(\alpha_{i,j}),\, 1 \leq i \leq f,\, 1 \leq j \leq f\}.$$

Le principe de la démonstration est d'utiliser les opérations élémentaires pour construire une suite de matrices équivalentes $M = M_0,\, M_1,\, \ldots M_k = \mathcal{A}$. A chaque étape on diminue l'entier positif $\gamma(M_i)$ et on démontre que l'une des deux possibilités suivante a lieu : ou bien $M_i = \mathcal{A}$ est de la forme voulue, ou bien il existe une matrice M_{i+1} équivalente à M_i telle que $\gamma(M_{i+1}) < \gamma(M_i)$. La suite d'entiers positifs $\gamma(M_i)$ doit cesser de décroître, et cela se produit au rang k tel que $M_k = \mathcal{A}$. Soit $\alpha = m_{i,j}$ le coefficient tel que $\gamma(M) = \varphi(m_{i,j})$. En permutant la première et la i-ième ligne puis la première et la j-ième colonne on peut supposer $\alpha = m_{i,j} = m_{1,1}$. Supposons qu'il existe un indice l tel que $\alpha \nmid m_{1,l}$. Alors par division euclidienne il existe $q,\, r \in A$ tels que $\varphi(r) < \varphi(\alpha)$ et $r = m_{1,l} - q\alpha$. Pour obtenir une matrice M' équivalente à M et telle que $\gamma(M') < \gamma(M)$ il suffit alors de remplacer la l-ième ligne par $L_l - qL_1$ c'est-à-dire multiplier M à gauche par $E_{l,1}(-q)$.

$$M = \begin{bmatrix} \alpha & \ldots & m_{i,1} & \ldots \\ \vdots & & * & \\ m_{1,l} & \ldots & m_{i,l} & \ldots \\ \vdots & & * & \\ m_{1,f} & & \ldots & \end{bmatrix} \sim \begin{bmatrix} \alpha & \ldots & m_{i,1} & \ldots \\ \vdots & & * & \\ m_{1,l} - q\alpha = r & \ldots & m_{i,l} - qm_{i,1} & \ldots \\ \vdots & & * & \\ m_{1,f} & & \ldots & \end{bmatrix} = M'.$$

Le coefficient r apparaît alors dans la première colonne et l-ième ligne de $M' = E_{l,1}(-q)M$, et on a donc $\gamma(M') \leq \varphi(r) < \varphi(\alpha) = \gamma(M)$.
Au bout d'un nombre fini d'étape le coefficient α de stathme minimal, placé en position de pivot (première ligne, première colonne) divisera tout les $m_{1,l}$. En raisonnant de même sur les colonnes α divisera tous les $m_{k,1}$. En remplaçant la k-ième colonne par $C_k - (m_{k,1}/\alpha)C_1$ on annule le coefficient $m_{k,1}$ pour $k = 2, \ldots, f$; et en remplaçant la l-ième ligne par $L_l - (m_{1,l}/\alpha)L_l$ on annule le coefficient $m_{1,l}$ pour $l = 2, \ldots, f$. On obtient ainsi une matrice M_2 équivalente à M de la forme :

$$M_2 = \begin{pmatrix} \alpha & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & m_{i,j} & \\ 0 & & & \end{pmatrix}.$$

Avec $\varphi(\alpha) = \gamma(M_2)$. A ce stade ou bien le coefficient pivot α de stathme minimal divise tout les $m_{i,j}$ et on a bien une matrice $M_2 = \mathcal{A}$ de la forme voulue, ou bien il existe $m_{k,l}$ avec $k > 1$ et $l > 1$ et $\alpha \nmid m_{k,l}$. Mais dans le deuxième cas en remplaçant la première colonne par $C_1 + C_l$ on retrouve le même pivot α (en effet le coefficient $m_{1,l}$ est nul) et le coefficient $m_{k,l}$ sur la première colonne (en effet le coefficient $m_{k,1}$ est nul) avec $m_{1,1} \nmid m_{k,l}$. On se retrouve ainsi alors dans la situation du début de la preuve ou le coefficient de stathme minimal ne divise pas un des coefficients sur la première ligne. Par division euclidienne on peut alors trouver une matrice M_3 équivalente à M_2 telle que $\gamma(M_3) < \gamma(M_2)$. Au bout d'un nombre fini d'étape on obtient une matrice $M_k = \mathcal{A}$ de la forme voulue. Il reste encore à vérifier que le coefficient $\alpha_{1,1}$ qui divise tous les coefficient de $\mathcal{A}$ est bien un p.g.c.d. d des coefficients initiaux de M. Clairement $\alpha_{1,1}$ est un p.g.c.d. des coefficients de $\mathcal{A}$. Pour montrer que c'est aussi un p.g.c.d. des coefficient initiaux de M on montre que l'idéal engendré par les coefficient d'une matrice est un invariant des classes d'équivalence. C'est le lemme qui suit :

Lemme 2.6
Soit A un anneau principal, soient M et N deux matrices équivalentes dans $M_f(A)$. Alors le p.g.c.d des coefficient de M est égal au p.g.c.d des coefficients de N.

Démonstration Soit $G \in GL_f(A)$. Par définition du produit matriciel tous les coefficients de $B = GM$ appartiennent à l'idéal engendré par les coefficients de M. Réciproquement, tous les coefficient de $M = G^{-1}B$ appartiennent à l'idéal engendré par les coefficients de B. Cet idéal (principal) ne change pas par multiplication à gauche par un élément de $GL_f(A)$. Le même raisonnement s'applique pour les multiplications à droite par des éléments de $GL_f(A)$. Cela conclut la preuve des deux lemmes.

fin de la démonstration du lemme 2.3. Soit $\mathcal{R} \in M_f(A)$. Le lemme 2.5 et une récurrence facile sur f fournissent l'existence de la suite $d_1 \mid d_2 \mid \ldots \mid d_f$ et de matrices $\mathcal{G}$, $\mathcal{H} \in GL_f(A)$ tels que

$$\mathcal{GRH} = \begin{bmatrix} d_1 & 0 & \ldots & \ldots & 0 \\ 0 & \ddots & & & \vdots \\ \vdots & & d_i & & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & \ldots & \ldots & 0 & d_f \end{bmatrix} = D$$

Pour l'unicité, on suppose l'existence deux matrice diagonale équivalentes D et D' de la forme

$$D = \begin{bmatrix} d_1 & 0 & \ldots & \ldots & 0 \\ 0 & \ddots & & & \vdots \\ \vdots & & d_i & & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & \ldots & \ldots & 0 & d_f \end{bmatrix} \text{ et } D' = \begin{bmatrix} d'_1 & 0 & \ldots & \ldots & 0 \\ 0 & \ddots & & & \vdots \\ \vdots & & d'_i & & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & \ldots & \ldots & 0 & d'_f \end{bmatrix},$$

avec $d_1 \mid d_2 \mid \ldots \mid d_f$ et $d'_1 \mid d'_2 \mid \ldots \mid d'_f$. Alors comme D et D' sont équivalentes le lemme 2.2 donne l'isomorphie $\oplus_i A/d_iA \cong \oplus_i A/d'_iA$. Le théorème 2.2 donne l'égalité entre les idéaux $(d_i) = (d'_i)$. Le lemme 2.3 est démontré.

2.5 Démonstration du lemme 2.3 pour les anneaux principaux

Dans cette (ultime) section on indique comment modifier la preuve euclidienne qui précède dans le cas d'un anneaux principal quelconque. En fait on doit seulement modifier deux ingrédients. On va utiliser une fonction qui joue le rôle du stathme euclidien : c'est la longueur de la définition 2.7. Et on doit pouvoir faire apparaître un p.g.c.d. de deux coefficient de la matrice sans division euclidienne : pour ce on utilise une relation de Bezout et une nouvelle opération élémentaire. Dans cette section A est à nouveau un anneau principal quelconque. En particulier A est factoriel. Si p est un irréductible de A et $a \in A$ on note $v_p(a)$ l'entier tel que $p^{v_p(a)}$ divise a et pas $p^{v_p(a)+1}$. Cela définit une application

$a \mapsto v_p(a)$ de $A - \{0\}$ dans $\mathbb{N}$. On fixe un système de représentant des irréductibles de A noté $\wp$. Cela signifie que tout $p \in \wp$ est irréductible, que deux éléments de $\wp$ sont associés si et seulement si ils sont égaux et que tout irréductible de A est associé avec un élément de $\wp$. En conséquence tout $a \in A$ s'écrit de manière unique comme un produit

$$a = u \prod_{p \in \wp} p^{v_p(a)},$$

pour un unique inversible $u \in A^\times$. En outre pour a fixé les $v_p(a)$ sont tous nuls sauf un nombre fini d'entre eux. Cela permet de poser la définition suivante :

Définition 2.7
Soit $a \in A$ non nul. On appelle longueur de A le nombre naturel $\ell(a) = \sum_{p \in \wp} v_p(a)$. On définit ainsi une application $\ell \colon A - \{0\} \longrightarrow \mathbb{N}$.

Cette fonction ℓ ne permet pas de faire des divisions euclidienne, cependant ses propriétés suffisent à notre démonstration.

Proposition 2.6
Soient a, $b \in A$ non nuls.

1. *Si $a \mid b$ strictement alors $\ell(a) < \ell(b)$.*
2. *Si a et b sont associés alors $\ell(a) = \ell(b)$.*
3. *$\ell(a) = 0$ si et seulement si $a \in A^\times$.*

Démonstration C'est évident. La réciproque de 2 est fausse, par exemple les éléments de $\wp$ a priori distincts sont tous de longueur 1.

Proposition 2.7
Soient a, b deux éléments de A. On note d le p.g.c.d. de a et b. On considère une matrice M dans $M_f(A)$ de la forme

$$M_1 = \begin{bmatrix} a & b & * & \dots & * \\ * & * & * & & \\ \vdots & \vdots & & \ddots & \\ * & * & & \dots & * \end{bmatrix} \text{ ou de la forme } M_2 = \begin{bmatrix} a & * & \dots & * \\ b & * & \dots & * \\ * & * & & \\ \vdots & & \ddots & \vdots \\ * & & \dots & * \end{bmatrix}.$$

Alors M est équivalente à une matrice dont un des coefficient est d.

Démonstration. On part d'une relation de Bezout $ua + bv = d$. Alors les coefficients u et v sont premiers entre eux et il existe donc u' et v' tels que $uu' - vv' = 1$. Les matrices de la forme

$$\Delta_d = \begin{bmatrix} u & v' & \\ v & u' & 0 \\ 0 & & \mathrm{Id}_{f-2} \end{bmatrix} \text{ et } \Delta_g = \begin{bmatrix} u & v & \\ v' & u' & 0 \\ 0 & & \mathrm{Id}_{f-2} \end{bmatrix}$$

sont donc dans $GL_f(A)$. La matrice $M_1\Delta_d$ (respectivement $\Delta_g M_2$) est alors semblable à M_1 (respectivement M_2) et admet bien d comme premier coefficient.

Démonstration du lemme 2.3 pour les anneaux principaux. On reprend la preuve euclidienne du paragraphe précédent. L'hypothèse A euclidien n'est pas utilisée dans le

paragraphe intitulé **fin de la démonstration du lemme 2.3.** ni pour le lemme 2.6. Il nous suffit donc de démontrer le lemme 2.5 sans la troisième propriété (qui est une conséquence du lemme 2.6). Mais pour généraliser la démonstration du lemme 2.5 au cas A principal il suffit de remplacer partout le minimum des stathmes des coefficients (noté γ) par le minimum des longueurs des coefficients, et de remplacer les divisions euclidiennes par l'operation déduite de la proposition 2.6. En effet si le pivot a ne divise pas un coefficient b sur sa ligne ou sa colonne on peut par permutation ramener b à la place de la proposition 2.6 puis faire apparaître le p.g.c.d. de (a, b) qui divise strictement a. La longueur de d est donc strictement inférieure à celle de a. Tout le reste de la démonstration du lemme 2.3 se fait comme dans le cas euclidien.

Chapitre 3

Exercices du chapitre 0.

3.2 Exercice 1.

Soit $f\colon \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/6\mathbb{Z}$ le seul morphisme de groupes non trivial. Montrer que f vérifie les conditions 1. et 2. de la définition des morphismes d'anneaux mais pas la troisième.

3.3 Exercice 2.

Démontrer la proposition 0.2 : les noyaux et images des morphismes de groupes sont des sous-groupes.

3.4 Exercice 3.

Démontrer la proposition 0.3 : les noyaux des morphismes d'anneaux sont des idéaux bilatères, et les images des morphismes d'anneaux sont des sous-anneaux.

3.5 Exercice 4.

Démontrer que la relation associée à un sous-groupe additif $H \subset G$ définie dans la proposition 0.4 est symétrique et reflexive (ce qui complète la démonstration de cette proposition).

3.6 Exercice 5.

Soient $H \subset G$ un sous-groupe d'un groupe additif. Démontrer que la loi de composition interne sur le quotient G/H définie dans le théorème 0.1 vérifie les axiomes de la définition de groupe. Montrer que $H = \ker \pi_H$ (ce qui complète la preuve de ce théorème).

3.7 Exercice 6.

Soient A un anneau commutatif et $I \subset A$ un idéal de A. Démontrer les équivalences :

1. I est premier si et seulement si A/I est intègre.
2. I est maximal si et seulement si A/I est un corps.

3.8 Exercice 7.

Montrer les implications qui suivent.

1. Si A est un corps alors A est intègre.
2. Si A est intègre et fini alors A est un corps.

3.9 Exercice 8.

Un élément u de A est dit *nilpotent* lorsqu'il existe $n \in \mathbb{N}$ tel que $u^n = 0$. On appelle *radical nilpotent* ou encore *nilradical* de A l'ensemble $N(A) = \{u \in A, u \text{ est nilpotent}\}$.

1. Montrer que $N(A)$ est un idéal de A.
2. Soit $u \in N(A)$. Montrer que $(1+u) \in A^\times$.

3.10 Exercice 9.

Soit $\mathbb{K}$ un corps.

1. Soit I et J les sous-ensembles de $M_2(\mathbb{K})$ définis ci-dessous.

$$I := \left\{ \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} \mid \ a, b \in \mathbb{K} \right\} \text{ et } J := \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid \ a, b \in \mathbb{K} \right\}$$

   Montrer que I est un idéal à droite et J à gauche de $M_2(\mathbb{K})$.
2. Montrer que $M_2(\mathbb{K})$ n'admet que $\{0\}$ et $M_2(\mathbb{K})$ comme idéaux bilatère. (*on parle alors d'algèbre simple*).

3.11 Exercice 10.

Soit A un corps. Montrer que les seuls idéaux de A sont $\{0\}$ et A.

Chapitre 4

Exercices du chapitre 1.

4.2 Exercice 11.

Soit M un A-module et $m \in M$. Montrer que $-m = (-1) \times m$.

4.3 Exercice 12.

Soit M un groupe additif. Définir sur M la structure naturelle de $\mathbb{Z}$-module, vérifier soigneusement toutes les propriétés requises.

4.4 Exercice 13.

Soit M un $\mathbb{Z}$-module.

1. On suppose que M est muni d'une structure de A-module. Définir un morphisme d'anneau $f\colon A \longrightarrow \mathrm{End}_{\mathbb{Z}}(M)$.
2. Soit $f\colon A \longrightarrow \mathrm{End}_{\mathbb{Z}}(M)$ un morphisme d'anneau (unitaire). Définir sur M une structure de A-module (et vérifier les propriétés requises).
3. On suppose que M est un A module et soit $g\colon B \longrightarrow A$ un morphisme d'anneau. Définir sur M une structure de B-module (et vérifier les propriétés requises).

4.5 Exercice 14.

Soit $\mathbb{K}$ un corps commutatif et V un espace vectoriel sur $\mathbb{K}$. Soit $u \in \mathrm{End}_{\mathbb{K}}(V)$. Pour tout polynôme $P(X) \in \mathbb{K}[X]$ et tout $v \in V$ on pose $P(X).v = (P(u))(v)$. Démontrer qu'on munit ainsi V d'une structure de $\mathbb{K}[X]$-module (qui étend celle de $\mathbb{K}$-espace vectoriel). On notera V_u cette structure de $\mathbb{K}[X]$-module.

4.6 Exercice 15.

Soit M un A-module, N un sous-module de M, et S une partie de M. Soit $I_N^S = \{a \in A;\ \forall s \in S\ :\ a \times s \in N\}$.

1. Montrer que I_N^S et un idéal de A.
2. Soit $\langle S \rangle$ le sous-module engendré par S. Montrer que $I_N^S = I_N^{\langle S \rangle}$

Retenir que lorsque N est le sous-module nul $I^S_{\{0\}}$ se note $\mathrm{Ann}_A(S)$ et s'appelle l'annulateur (du sous-module engendré par) S.

4.7 Exercice 16.

Soit M un $\mathbb{Z}$-module non nul sans sous-module non triviaux (un tel module est dit simple). Montrer qu'il existe un nombre premier p tel que M soit isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

4.8 Exercice 17.

Soit A un anneau commutatif Soit M un A-module monogène (i.e. il existe un $m \in M$ tel que $M = Am$). Montrer que $\mathrm{End}_A(M)$ est isomorphe à $A/\mathrm{Ann}_A(M)$. L'anneau $\mathrm{End}_A(M)$ est-il commutatif ?

4.9 Exercice 18.

On suppose que A est un anneau intègre commutatif qui n'est pas un corps et soit $\mathbb{K}$ le corps des fractions de A. Montrer que le A-module $\mathbb{K}$ n'est pas libre.

4.10 Exercice 19.

Soient $M = M_1 \oplus M_2$ trois A-modules. Montrer que M_2 est isomorphe à M/M_1.

4.11 Exercice 20.

Soient $f\colon M \longrightarrow N$ et $g\colon N \longrightarrow M$ des morphismes A-linéaires. On suppose que $f \circ g = \mathrm{Id}_N$. Montrer que M est isomorphe à la somme directe $\ker f \oplus N$.

4.12 Exercice 21.

Soit M un A-module et $(M_i)_{i=1}^{i=n}$ une famille finie de sous-A-modules de M telle que :

(*i*) $M = \left\langle \bigcup_{i=1}^{i=n} M_i \right\rangle$

(*ii*) Pour tout j compris entre 1 et $n-1$ on a $\langle \bigcup_{i=1}^{i=j} M_i \rangle \cap M_{j+1} = \{0\}$

Montrer l'égalité $M = \bigoplus_{i=1}^{i=n} M_i$

4.13 Exercice 22.

Démontrer que la suite exacte de $\mathbb{Z}$-modules

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{\overline{x} \mapsto \overline{px}} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\overline{x} \mapsto \overline{x}} \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

n'est pas scindée.

4.14 Exercice 23.

Trouver le sous-module de torsion des $\mathbb{Z}$-modules suivant : $\mathbb{Z}^{(2)}$, $\mathbb{Z} \oplus (\mathbb{Z}/6\mathbb{Z})$, $\mathbb{Q}/\mathbb{Z}$ et $\mathbb{R}/\mathbb{Z}$.

4.15 Exercice 24.

Vérifier que $\{(2,0,0);\ (0,1,0)\}$ est une partie libre de $\mathbb{Z}^3$ mais qu'on ne peut pas la compléter en une base. Montrer que le système $S = \{(2,0,0);\ (3,0,0);\ (0,1,0);\ (0,0,1)\}$ engendre $\mathbb{Z}^3$ mais qu'on ne peut pas en extraire une base.

4.16 Exercice 25.

Soit N le sous-$\mathbb{Z}$-module de $M = \mathbb{Z}^3$ engendré par le système

$$S = \{(1,4,2);\ (3,2,6);\ (5,20,5);\ (3,2,1);\ (2,3,4)\}.$$

Trouver un système générateur de N contenant au plus 3 éléments.

Chapitre 5

Exercices du chapitre 2.

5.2 Exercice 26.

Calculer le $\mathbb{Z}$-rang du $\mathbb{Z}$-module $\mathbb{Z}^3/N$ lorsque N est engendré par les systèmes suivants :

1. $(1, 2, -1)$
2. $(1, -1, -1)$; $(0, 1, 2)$
3. $(1, 0, -1)$; $(0, 2, 3)$; $(2, 2, 1)$
4. $(0, 0, 1)$; $(2, 1, -1)$; $(0, 1, 2)$; $(-1, -1, 1)$
5. $(1, 2, 4)$; $(-1, 3, 2)$; $(5, 0, 8)$; $(3, -4, 0)$

5.3 Exercice 27.

Soit M le $\mathbb{Z}$-module $\mathbb{Z}^4$ et soit N le sous-module engendré par le système $S = \{(2, 0, 2, 2); (0, 6, 6, 6); (-4, 0, 2, 2)\}$. Déterminer une $\mathbb{Z}$-base de M adaptée à N et la structure de M/N.

5.4 Exercice 28.

Soient A, $B \in M_2(\mathbb{Z})$. On dit que A est équivalente à B lorsqu'il existe des matrices G, H dans $GL_2(\mathbb{Z})$ telles que $A = GBH$. On considère les matrices :

$$A = \begin{bmatrix} 4 & 0 \\ 0 & 15 \end{bmatrix} \quad \text{et} \quad B = \begin{bmatrix} 20 & 0 \\ 0 & 3 \end{bmatrix}.$$

A et B sont-elles équivalentes ? Pourquoi ?

5.5 Exercice 29.

Soit $\mathbb{K}$ un corps commutatif, V un espace vectoriel de dimension d finie sur $\mathbb{K}$ et $u \in \mathrm{End}_{\mathbb{K}}(V)$. On va donner une présentation libre du module V_u de l'exercice 14. On fixe une base $(e_i)_{i=1}^{i=d}$ de V. Soit $(a_{i,j})$ la matrice de u dans la base e_i. On note $(\varepsilon_i)_{i=1}^{i=d}$ la base canonique de $(\mathbb{K}[X])^d$.

1. Soit $\psi \in \mathrm{End}_{\mathbb{K}[X]}(K[X]^d)$ définie par $\psi(\varepsilon_i) = \sum_{j=1}^{j=d} a_{i,j}\varepsilon_j - X\varepsilon_i$.
   (a) Reconnaître (en fonction de u) le déterminant de ψ. Quel est son degré ?

(b) En utilisant la classification des $\mathbb{K}[X]$-module de type fini calculer la dimension sur $\mathbb{K}$ de $\mathbb{K}[X]^d/\operatorname{Im}(\psi)$.

2. Soit $\varphi\colon \mathbb{K}[X]^d \longrightarrow V_u$ définie par $\varphi(\varepsilon_i) = e_i$.
   (a) Montrer que $\varphi \circ \psi = 0$.
   (b) En utilisant le calcul des dimensions sur $\mathbb{K}$, en déduire un isomorphisme de $\mathbb{K}[X]$-module entre V_u et $\mathbb{K}[X]^d/\operatorname{Im}(\psi)$.
3. Soient $(P_i)_{i=1}^{i=s}$ les diviseurs élémentaires du $\mathbb{K}[X]$-module de torsion V_u. Exprimer en fonction des P_i les polynômes minimal et caractéristique de u. En déduire le théorème de Cayley-Hamilton.

5.6 Exercice 30.

Soit A un anneau principal et M un A-module de type fini. D'après le théorème de classification il existe une suite de *diviseurs élémentaires* dans A disons $(d_i)_{i=1}^{i=s}$ et des éléments $(m_i)_{i=1}^{i=s}$ dans M tels que :

$$d_i \mid d_{i+1} \qquad \operatorname{Ann}_A(m_i) = (d_i) \qquad M = \bigoplus_{i=1}^{i=s} \langle m_i \rangle \cong \bigoplus_{i=1}^{i=s} A/(d_i)$$

1. Soit $i \in \{1, ..., s\}$. Montrer qu'il existe $u_i \in \operatorname{End}_A(M)$ tel que
$$u_i(m_1) = u_i(m_2) = ... = u_i(m_{s-1}) = 0; \quad u_i(m_s) = m_i.$$
2. Soit $u \in \operatorname{End}_A(M)$ qui commute avec tous les éléments de $\operatorname{End}_A(M)$. Montrer que u est la multiplication par un scalaire $a \in A$.
3. Même question en supposant seulement que $u\colon M \longrightarrow M$ est un morphisme de groupe additif qui commute avec tous les éléments de $\operatorname{End}_A(M)$.
4. Soit $\mathbb{K}$ un corps (commutatif) V un $\mathbb{K}$-espace vectoriel de dimension finie et $u \in \operatorname{End}_K(V)$. Soit $\mathcal{C} = \{v \in \operatorname{End}_{\mathbb{K}}(V);\ u \circ v = v \circ u\}$ l'ensemble des endomorphismes de V qui commute avec u. Montrer que les seuls endomorphismes commutant avec tous les éléments de $\mathcal{C}$ sont les polynômes en u à coefficients dans $\mathbb{K}$ (on pourra utiliser la structure V_u de l'exercice 14).

5.7 Exercice 31.

Soit $\mathbb{K}$ un corps commutatif et V un espace vectoriel de dimension d finie sur $\mathbb{K}$. On dit que deux $\mathbb{K}$-endomorphismes u et v (respectivement deux matrices de A et B dans $M_d(\mathbb{K})$) sont semblables si il existe $f \in GL(V)$ (respectivement $P \in GL_d(\mathbb{K})$) telle que $u = f \circ v \circ f^{-1}$ (respectivement $A = PBP^{-1}$).

1. Montrer que u et v sont semblable si et seulement si les $\mathbb{K}[X]$-modules V_u et V_v sont isomorphes (notations de l'exercice 14).
2. Soit $P(X) = X^n + \sum_{i=n-1}^{i=0} a_i X^i \in \mathbb{K}[X]$. Soit W le $\mathbb{K}$-espace vectoriel $\mathbb{K}[X]/(P(X))$, muni de la base $(\overline{X^i})_{i=0}^{i=n-1}$. Soit u_P le $\mathbb{K}$-endomorphisme de W défini par la multiplication par X. Écrire la matrice A_P de u_P relativement à la base qui précède. Quel est le polynôme caractéristique de u_P ? son polynôme minimal ? Retenir que A_P s'appelle la *matrice compagnon* de P.

3. Soit $A \in M_d(\mathbb{K})$. Démontrer qu'il existe $s \in \mathbb{N}, s \leq d$ et des polynômes $(P_i)_{i=1}^{i=s}$ tels que A est semblable à la matrice diagonale par bloc dont le $i^{\text{ème}}$ bloc est la matrice compagnon de P_i, et $P_i \mid P_{i+1}$ pour $i \leq s-1$. On appelle ces (P_i) les invariants de similitude de A. Pourquoi deux matrice semblables ont-elles les mêmes invariants de similitude ?
4. Soit $\lambda \in \mathbb{K}$ soit $n \in \mathbb{N}$, $n \neq 0$. Soit $A_n(\lambda) = (a_{i,j})$ la matrice (dite de Jordan) de $M_n(\mathbb{K})$ dont tous les coefficients sont nuls sauf les diagonals tels que $a_{i,i} = \lambda$ pour tout i et les sous-diagonals tels que $a_{i+1,i} = 1$. Montrer que $A_n(\lambda)$ est semblable à la matrice compagnon du polynôme $P(X) = (X-\lambda)^n$.
5. Soit $A \in M_d(\mathbb{K})$, à quelle condition A est elle semblable à une matrice diagonale par bloc, chaque bloc étant une matrice de Jordan ? Que peut-on dire si $\mathbb{K}$ est algébriquement clos ?

Chapitre 6

Corrigé des exercices du chapitre 0

6.1 Exercice 1.

Commençons par préciser le morphisme f. Puisque c'est un morphisme on a $f(\overline{0}) = \overline{0}$. L'image $f(\overline{1})$ est d'ordre au plus 2 puisque f est un morphisme de groupe, et exactement 2 puisque f est non trivial. Or dans $\mathbb{Z}/6\mathbb{Z}$ le seul élément d'ordre 2 est $\overline{3}$. On a donc $f(\overline{1}) = \overline{3}$ ce qui contredit déjà la condition 3 de la définition des morphismes d'anneaux. Montrons que f vérifie la condition 2. (la condition 1. affirmant que f est un morphisme de groupe additif étant vérifiée par construction). Prenons x, $y \in \mathbb{Z}/2\mathbb{Z}$. Deux cas peuvent se produire. Ou bien l'un (au moins) des deux éléments x et y est nul et la condition 2. est vérifiée pour ce couple puisqu'alors $f(xy) = f(\overline{0}) = \overline{0} = f(x)f(y)$. Ou bien $x = y = \overline{1}$ et on a alors $f(xy) = f(\overline{1}) = \overline{3} = \overline{3}\,\overline{3} = f(\overline{1})f(\overline{1})$ et la condition 2. est aussi vérifiée.

6.2 Exercice 2.

Soit $f\colon A \longrightarrow B$ un morphisme de groupes additifs.
On montre l'égalité $f(0_A) = 0_B$. Soit $a \in A$. Alors $f(a) = f(0_A + a) = f(0_A) + f(a)$. En rajoutant à chaque membre $-f(a)$ on obtient $0 = f(0_A)$.
On montre l'égalité, pour tout a dans A, $f(-a) = -f(a)$. On a $0_B = f(0_A) = f(a+(-a)) = f(a) + f(-a)$. En rajoutant à chaque membre $-f(a)$ on obtient $-f(a) = f(-a)$.
Soient x, $y \in \ker f$. Alors $f(x-y) = f(x)+f(-y) = f(x)+(-f(y))$. Mais $f(x) = f(y) = 0_B$. On obtient donc $f(x-y) = 0_B - 0_B = 0_B$. C'est-à-dire $x - y \in \ker f$. Avec $0_A \in \ker f$ cela montre que $\ker f$ est un sous-groupe de A.
Montrons que $\operatorname{Im} f$ est un sous-groupe de B. Avant tout on a $0_B = f(0_A) \in \operatorname{Im} f$. Soient b_1, $b_2 \in \operatorname{Im} f$ et soient a_1, $a_2 \in A$ des antécédents respectifs (c'est-à-dire $f(a_1) = b_1$ et $f(a_2) = b_2$). Alors $b_1 - b_2 = f(a_1) - f(a_2) = f(a_1 - a_2) \in \operatorname{Im} f$. Cela montre que $\operatorname{Im} f$ est un sous-groupe de B.

6.3 Exercice 3.

Soit $f\colon A \longrightarrow B$ un morphisme d'anneaux. D'après la proposition 0.2 $\ker f$ est un sous-groupe additif de A et $\operatorname{Im} f$ est un sous-groupe additif de B. Soit $a \in A$ et soit $\alpha \in \ker f$. Alors $f(a\alpha) = f(a)f(\alpha) = f(a)0_B = 0_B$ et $f(\alpha a) = f(\alpha)f(a) = 0_B f(a) = 0_B$. Donc $\ker f$ est un idéal bilatère. Montrons que $\operatorname{Im} f$ est un sous-anneau de B. Comme f est un morphisme unitaire $1_B = f(1_A) \in \operatorname{Im} f$. Soient $b_1, b_2 \in \operatorname{Im} f$ et soient $a_1, a_2 \in A$ des antécédents respectifs (c'est-à-dire $f(a_1) = b_1$ et $f(a_2) = b_2$). Alors $b_1 b_2 = f(a_1)f(a_2) = f(a_1 a_2) \in \operatorname{Im} f$. Cela montre que $\operatorname{Im} f$ est un sous-anneau de B.

6.4 Exercice 4.

On montre que $\sim_H$ est symétrique. Soient $x, y \in G$ tels que $x \sim_H y$. Par définition de $\sim_H$ cela équivaut à $x - y \in H$. Mais comme H est un sous-groupe il contient l'inverse de tous ses éléments, en particulier $-(x-y) = y - x \in H$. Cela donne $y \sim_H x$.
On montre que $\sim_H$ est reflexive. Soit $x \in G$. Comme H est un sous-groupe il contient l'élément neutre, et on a donc $x - x = 0_G \in H$. D'où $x \sim_H x$.

6.5 Exercice 5.

Soient $H \subset G$ un sous-groupe additif. Au début de la preuve du théorème 0.1, on a défini sur G/H une loi de composition interne $\overline{+}$ en posant $\overline{x} \,\overline{+}\, \overline{y} = \overline{x+y}$ et on a déjà vérifiée dans cette même preuve que cette définition ne dépend pas du choix de $x \in \overline{x}$ ni de $y \in \overline{y}$. Soient $x, y, z \in G$ et soit $\overline{x}, \overline{y}, \overline{z}$ leurs classes respectives dans G/H. Comme $+$ est commutatif dans G on a $\overline{x} \,\overline{+}\, \overline{y} = \overline{x+y} = \overline{y+x} = \overline{y} \,\overline{+}\, \overline{x}$, donc $\overline{+}$ est commutatif. Comme 0_G est élément neutre pour $+$ on a $\overline{0_G} \,\overline{+}\overline{x} = \overline{x} \,\overline{+}\, \overline{0}_G = \overline{x+0_G} = \overline{x}$, donc $\overline{0_G} = 0_{G/H}$ est élément neutre pour $\overline{+}$. Comme x admet un inverse additif $-x$ pour $+$ on a $\overline{x} \,\overline{+}\, \overline{-x} = \overline{-x} \,\overline{+}\, \overline{x} = \overline{-x+x} = \overline{0_G} = 0_{G/H}$, donc tout $\overline{x}$ de G/H admet un élément neutre pour $\overline{+}$. Comme $+$ est associative on a $\overline{x} \,\overline{+}\, (\overline{y} \,\overline{+}\, \overline{z}) = \overline{x} \,\overline{+}\, \overline{y+z} = \overline{x+(y+z)} = \overline{(x+y)+z} = \overline{x+y} \,\overline{+}\, \overline{z} = (\overline{x} \,\overline{+}\, \overline{y}) \,\overline{+}\, \overline{z}$. Donc $\overline{+}$ est associative. Montrons que $\ker \pi_H = H$. On a vu que $\pi_H(0_G) = \overline{0_G} = 0_{G/H}$. Cela donne les équivalences pour tout $h \in G$:
$h \in \ker \pi_H \iff \overline{h} = \overline{0_G} \iff h \sim_H 0_G \iff h - 0_G \in H \iff h \in H$. D'où l'égalité $\ker \pi_H = H$.

6.6 Exercice 6.

1. On suppose I premier. Soient $x, y \in A/I$ tels que $xy = 0_{A/I}$, et soient $a, b \in A$, tels que $\overline{a} = x$ et $\overline{b} = y$. Alors $\overline{ab} = 0_{A/I}$ et donc $ab \in I$. Comme I est premier on a $a \in I$ ou bien $b \in I$, c'est-à-dire $x = \overline{a} = 0_{A/I}$ ou bien $y = \overline{b} = 0_{A/I}$. Cela montre que A/I est intègre. Réciproquement on suppose A/I intègre. Soient $a \in A$ et $b \in A$ tels que $ab \in I$. Alors dans le quotient A/I on obtient $0_{A/I} = \overline{ab} = \overline{a}\,\overline{b}$. Mais comme A/I est intègre on obtient $\overline{a} = 0_{A/I}$ ou bien $\overline{b} = 0_{A/I}$, c'est-à-dire $a \in I$ ou bien $b \in I$.

2. On suppose I maximal. Soit $x \in A/I$ non nul et $a \in A$ tel que $\overline{a} = x$. Alors $a \notin I$. Et comme I est maximal l'idéal $(a) + I$ qui contient strictement I est égal à A tout entier, donc contient 1_A. En particulier il existe $i \in I$ et $\alpha \in A$ tels que $1_A = \alpha a + i$. En réduisant modulo I on obtient $1_{A/I} = \overline{\alpha}\ \overline{a} = \overline{\alpha} x$ ce qui montre que $x = \overline{a}$ est inversible. L'anneau A/I est donc bien un corps. Réciproquement on suppose que A/I est un corps. Soit J un idéal de A contenant strictement I. montrons que $J = A$. Soit $j \in J$ n'appartenant pas à I. Alors dans A/I son image $\overline{j}$ est inversible. Il existe donc $i \in I$ et $\alpha \in A$ tels que $\alpha j + i = 1_A$. Mais comme $I \subset J$ il suit $1_A \in J$ c'est-à-dire $J = A$.

6.7 Exercice 7.

1. On suppose que A est un corps. Soient a, b dans A tels que $ab = 0$. Si $a \neq 0$ alors a est inversible et on obtient $b = a^{-1}ab = a^{-1}0 = 0$. Si $b \neq 0$ alors b est inversible et on obtient $a = abb^{-1} = 0b^{-1} = 0$. Cela montre que A est intègre.
2. On suppose A intègre et fini. Soit $a \in A$ tel que $a \neq 0$. Alors l'endomorphisme de groupe de A défini par $x \mapsto ax$ est injectif puisque $ax = 0 \iff x = 0$. Comme A est fini ce morphisme est donc aussi surjectif. En particulier il existe $\alpha \in A$ tel que $a\alpha = 1_A$. Cela montre que A est un corps.

6.8 Exercice 8.

1. Clairement $0 \in N(A)$. Soient $a \in N(A)$ et $\alpha \in A$. Alors il existe $n \in \mathbb{N}$ tel que $a^n = 0$. Comme A est commutatif il vient $(\alpha a)^n = \alpha^n a^n = 0$. Donc $\alpha a \in N(A)$. Montrons que $N(A)$ est un sous-groupe. Soient a, $b\ \in N(A)$. Alors il existe $n \in \mathbb{N}$ et $m \in \mathbb{N}$ tels que $a^n = b^m = 0$. Par le binôme de Newton (valable dans tout anneau commutatif) on obtient

$$(a + (-b))^{n+m} = \sum_{j=0}^{n+m} (-1)^{n+m} \left(\frac{n+m}{j}\right) a^j b^{n+m-j}$$

   Mais si $j \leq n$ alors $a^j = 0$ tandis que si $j < n$ alors $b^{n+m-j} = 0$. Chacun des sommant est nul et donc $a - b \in N(A)$.
2. Comme $N(A)$ est un sous-groupe cela revient à montrer que $1 - u \in A^\times$. Soit $n \in \mathbb{N}$ tel que $u^n = 0$. On a

$$1 = 1 - u^n = (1 - u) \sum_{j=0}^{n-1} u^j.$$

   Donc $1 - u \in A^\times$.

6.9 Exercice 9.

1. Les deux ensembles I et J sont des sous-groupes (en fait ce sont même des sous-$\mathbb{K}$-espaces vectoriels de $M_2(\mathbb{K})$). Pour montrer que I est un idéal à droite on calcule les produits (pour tout a, b, c, d, e, f de $\mathbb{K}$) :

$$\begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} \begin{pmatrix} c & d \\ e & f \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ ac+be & ad+bf \end{pmatrix} \in I$$

Pour montrer que J est un idéal à gauche on effectue le calcul ci dessous (pour tout a, b, c, d, e, f de $\mathbb{K}$) :

$$\begin{pmatrix} c & d \\ e & f \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} ca+db & 0 \\ ea+fb & 0 \end{pmatrix} \in J$$

2. On considère la matrice de permutation τ ci-dessous :

$$\tau = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

On constate que multiplier une matrice par τ à gauche (resp. à droite) échange ces deux lignes (resp. colonne) d'où la terminologie de matrice de permutation :

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix} \text{ et } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & a \\ d & c \end{pmatrix}$$

Soit $\mathcal{I}$ un idéal bilatère non-nul de $M_2(\mathbb{K})$ et soit $\alpha \in \mathcal{I}$ tel que $\alpha \neq 0$. On écrit $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. L'un au moins des coefficients a, b, c ou d est non nul. Comme pour tout $x \in I$ on a $x\tau \in I$ et $\tau x \in I$, on peut supposer (quite à changer α) que le coefficient non nul de α est $a \neq 0$. On a alors

$$\begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in \mathcal{I}.$$

Et

$$\tau \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in \mathcal{I}.$$

Et

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \tau = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{I}.$$

Et

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

Finalement, pour tout a, b, c et d de $\mathbb{K}$ on a

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$+ \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{I}$$

Cela montre que le seul idéal bilatère non nul de $M_2(\mathbb{K})$ est $M_2(\mathbb{K})$ tout entier. Ce raisonnement se généralise à $M_n(\mathbb{K})$ pour tout n (mais on doit utiliser les matrices de transpositions plus générales notées $S_{k,l}$ dans le paragraphe 2.3) .

6.10 Exercice 10.

Soit $x \neq 0$ un élément non nul d'un idéal $\mathcal{I}$ (non nul) de A. Alors x est inversible et tout $y \in A$ s'écrit $y = yx^{-1}x$ donc $y \in \mathcal{I}$. Cela montre que le seul idéal non nul de A est A tout entier.

FIN DU CORRIGÉ DES EXERCICES DU CHAPITRE 0.

Chapitre 7

Corrigé des exercices du chapitre 1

7.11 Exercice 11.

On montre d'abord pour tout $m \in M$ que $0_A \times m = 0_M$. On a $0_A \times m + m = 0_A \times m + 1_A \times m = (0_A + 1_A) \times m = 1_A \times m = m$. En rajoutant $-m$ aux deux termes extrêmes on obtient comme annoncé $0_A \times m = 0_M$. On calcule maintenant $(-1_A) \times m + m = (-1_A + 1_A) \times m = 0_A \times m = 0_M$. Par l'unicité de l'inverse additif dans M on en déduit $-m = (-1_A) \times m$.

7.12 Exercice 12.

Soit $k \in \mathbb{Z}$ et $m \in M$. On commence par définir la notation $k.m$. Pour $k \geq 0$ on procède par récurrence en posant $0.m = m$ et $k.m = (k-1).m + m$ pour $k > 0$. Pour $k < 0$ on pose $k.m = -((-k).m)$. Cela définit une opération externe de $\mathbb{Z}$ sur M. On vérifie maintenant que cette opération satisfait les axiomes (a), (b), (c), et (g) de la définition des modules. L'axiome (c) est immédiat puisque par définition pour tout $m \in M$ on a $1.m = 0.m + m = 0_M + m = m$. On va d'abord vérifier les deux propriétés ci-dessous pour tout $a \in \mathbb{Z}$ et tout $m \in M$.

(i) $(-a).m = -(a.m)$

(ii) $(a+1).m = a.m + m$

Lorsque $a \geq 0$ ces propriétés sont explicitement dans la définition de l'opération externe de $\mathbb{Z}$. Montrons (i) pour $a < 0$. Par définition $(a.m) = -((-a).m)$. Donc $(a.m) + ((-a).m) = 0_M$. Par unicité de l'inverse additif on conclut à $(-a).m = -(a.m)$. Montrons (ii) pour $a < 0$. Si $a = -1$, alors $(a+1).m = 0_M = (-1)m + m$. Par définition de l'opération externe pour tout $x \in \mathbb{Z}$, $x \geq 0$ on a $x.m = (x+1).m - m$. En particulier pour $a < -1$ on en déduit :

$$\begin{aligned}(x+1).m &= -((-x-1).m) \text{ par définition de .}\\ &= -((-x).m - m) \text{ par la remarque qui précède}\\ &= -(-x).m + (-(-m)) \text{ car dans un groupe additif l'inverse d'une somme}\\ &\quad \text{est la somme des inverses}\\ &= x.m + m \text{ par le } (i) \text{ et l'unicité de l'inverse additif}\end{aligned}$$

On commence par vérifier le (a). Soient $a \in \mathbb{Z}$ et m, $m' \in M$. Pour $a \geq 0$ on procède par récurrence. Si $a = 0$ c'est la définition de . puisque $0m = 0_M$ pour tout m. Supposons donc l'axiome (a) vérifié pour tout m, tout m' au rang $a = k \geq 0$. Alors on obtient :

$$\begin{aligned}(k+1).(m+m') &= k.(m+m') + (m+m') \text{ par définition de .} \\ &= k.m + k.m' + m + m' \text{ par récurrence} \\ &= (k+1).m + (k+1).m' \text{ par définition de .}\end{aligned}$$

Ceci démontre par le principe de récurrence l'axiome (a) pour $a \geq 0$. Si $a < 0$ alors :

$$\begin{aligned}a.(m+m') &= -((-a).(m+m')) \text{ par définition de .} \\ &= -((-a).m + (-a).m') \text{ car } -a \geq 0 \\ &= -(-(a.m) + (-(a.m'))) \text{ par } (i) \\ &= a.m + a.m' \text{ car dans un groupe additif l'inverse d'une somme} \\ &\quad \text{est la somme des inverses}\end{aligned}$$

L'axiome (a) est vérifié. On démontre maintenant l'axiome (b). Soient a, $b \in \mathbb{Z}$ et soit $m \in M$. On doit montrer que $(a+b).m = a.m+b.m$. Pour $a \geq 0$, on procède par récurrence sur a. Si $a = 0$ il n'y a rien à montrer. On suppose l'axiome (b) vérifié au rang $a = k$ et pour tout $b \in \mathbb{Z}$. Alors on obtient

$$\begin{aligned}((k+1)+b).m &= (k+(b+1)).m \\ &= k.m + (b+1).m \text{ par récurrence} \\ &= k.m + b.m + m \text{ par } (ii) \\ &= k.m + m + b.m \text{ car } M \text{ est commutatif} \\ &= (k+1).m + b.m \text{ par } (ii)\end{aligned}$$

Par le principe de récurrence ceci démontre l'axiome (b) pour tout $a \geq 0$. Si $a < 0$ alors :

$$\begin{aligned}(a+b).m &= -(-a+(-b)).m \text{ par } (i) \text{ et } -(a+b) = -a + (-b) \\ &= -((-a).m + (-b).m) \text{ par } (b) \text{ pour } -a > 0 \\ &= -(-a).m + (-(-b).m) \text{ car dans l e groupe additif } M \text{ par } (i) \\ &\quad \text{l'inverse d'une somme est la somme des inverses} \\ &= a.m + b.m\end{aligned}$$

L'axiome (b) est vérifié. Vérifions l'axiome (g) en utilisant l'axiome (b). On doit vérifier pour tout a, b dans $\mathbb{Z}$ et tout $m \in M$ l'égalité $a.(b.m) = (ab).m$. Pour $a \geq 0$ on procède par récurrence sur a. Si $a = 0$ cela équivaut à $0_M = 0_M$. Supposons l'axiome (g) vérifié pour tout b, tout m et pour $a = k \geq 0$. Alors on obtient

$$\begin{aligned}(k+1).(b.m) &= k.(b.m) + (b.m) \text{ par définition de .} \\ &= (kb).m + b.m \text{ par récurrence} \\ &= (kb+b).m \text{ par } (b) \\ &= ((k+1)b).m\end{aligned}$$

Ceci démontre par le principe de récurrence l'axiome (g) pour $a \geq 0$. Si $a < 0$ alors $(a.(b.m)) = -((-a).(b.m)) = -((-ab).m) = (ab).m$ en utilisant dans l'ordre des égalités la définition de ., l'axiome (g) pour $-a \geq 0$, et la propriété (i).

7.13 Exercice 13.

1. Soit $a \in A$, on doit définir $f(a) \in \mathrm{End}_{\mathbb{Z}}(M)$. Pour ce on pose $(f(a))(m) = a.m$. Cela définit clairement une application $f\colon A \longrightarrow M^M$, où M^M désigne l'ensemble des applications de M dans lui-même. Montrons l'image de f est contenu dans $\mathrm{End}_{\mathbb{Z}}(M)$. Soit m, $m' \in M$ et soit $a \in A$. Alors par l'axiome (a) du module M sur A, on a $f(a)(m+m') = a.(m+m') = a.m + a.m' = (f(a))(m) + (f(a))(m')$. Donc $f(a)$ est un morphisme de groupe. Par le même style de récurrence que pour l'exercice 12 et avec la propriété pour tout morphisme de groupe additif $f(-x) = -f(x)$, on démontre que tout morphisme de groupe additif est un morphisme de $\mathbb{Z}$-module pour la structure naturelle du même exercice. On a bien $\mathrm{Im}(f) \subset \mathrm{End}_{\mathbb{Z}}(M)$. Vérifions que f est un morphisme d'anneau (unitaire). Soient a, $b \in A$. Alors pour tout $m \in M$ on a $(f(a+b))(m) = (a+b).m = a.m + b.m = f(a)(m) + f(b)(m)$, par l'axiome (b) de la structure de A-module sur M. Cela montre que f est un morphisme de groupe. Pour tout m de M, par l'axiome (c) de la structure de A-module sur M on a $f(1)(m) = 1.m = m$. Donc $f(1)$ est bien le morphisme identité de M, c'est-à-dire l'élément neutre pour la composition des applications. De plus pour tout a, $b \in A$ et tout $m \in M$ on a $f(ab)(m) = (ab).m = a.(b.m) = f(a)(b.m) = f(a)(f(b)(m)) = (f(a) \circ f(b))(m)$ par l'axiome (g) de la structure de A-module de M. Cela montre que f est un morphisme d'anneau unitaire.
2. On suit la démarche réciproque à celle de la question précédente. On démontre ainsi l'équivalence entre la donnée d'une structure de A-module sur M et celle d'un morphisme d'anneau de A dans $\mathrm{End}_{\mathbb{Z}}(M)$. On commence par définir l'opération externe $a.m$ de A sur M en posant $a.m = f(a)(m)$ pour tout a et tout m de M. On vérifie ensuite les quatre propriétés requises en reprenant une à une les égalités de la question précédente. Comme pour tout a dans A l'application $f(a)$ est un morphisme de groupe on a pour tout m et tout m' de M les égalités $a.(m+m') = f(a)(m+m') = f(a)(m) + f(a)(m') = a.m + a.m'$. D'où l'axiome (a). Comme f est un morphisme de groupe on a pour tout a, $b \in A$ et tout $m \in M$ les égalités $(a+b).m = f(a+b)(m) = (f(a) + f(b))(m) = (f(a))(m) + (f(b))(m) = a.m + b.m$. D'où l'axiome (b). Comme f est un morphisme d'anneau unitaire on a pour tout $m \in M$ et tout a, $b \in A$ les égalités $1.m = f(1)(m) = m$ d'où l'axiome (c) et $(ab).m = f(ab)(m) = (f(a) \circ f(b))(m) = f(a)(f(b)(m)) = a.(f(b)(m)) = a.(b.m)$ d'où l'axiome (g).
3. En utilisant le 2., il nous suffit de définir un morphisme d'anneau unitaire $\beta\colon B \longrightarrow \mathrm{End}_{\mathbb{Z}}(M)$. Pour ce, on utilise le morphisme $f\colon A \longrightarrow \mathrm{End}_{\mathbb{Z}}(M)$ défini par le 1., et on pose $\beta = f \circ g$. Alors β est bien un morphisme d'anneau unitaire et par le 2., on sait qu'on définit une structure de B-module sur M en posant $b.m = \beta(b)(m) = f(g(b))(m) = g(b) * m$ si $*$ désigne l'opération de A.

7.14 Exercice 14.

Pour $\lambda \in \mathbb{K}$ et $x \in V$ on note $\lambda * x$ l'opération externe de $\mathbb{K}$ sur V. Étant donné un élément u de la $\mathbb{K}$-algèbre $\mathrm{End}_{\mathbb{K}}(V)$, par la propriété universelle des algèbres de polynômes il existe un unique morphisme de $\mathbb{K}$-algèbre $f_u\colon \mathbb{K}[X] \longrightarrow \mathrm{End}_{\mathbb{K}}(V)$ tel que $f_u(X) = u$. Il s'agit du morphisme d'évaluation en u défini par $f(\sum_i a_i X^i) = \sum_i a_i * u^i$ où le $*$

désigne l'opération externe de $\mathbb{K}$ sur l'algèbre $\mathrm{End}_{\mathbb{K}}(V)$ et la puissance u^i est défini par la multiplication interne dans $\mathrm{End}_{\mathbb{K}}(V)$. Avec l'inclusion $\mathrm{End}_{\mathbb{K}}(V) \subset \mathrm{End}_{\mathbb{Z}}(V)$ on obtient un morphisme d'anneau $f_u\colon \mathbb{K}[X] \longrightarrow \mathrm{End}_{\mathbb{Z}}(V)$. Par la question 2 de l'exercice 13 un tel morphisme d'anneau unitaire permet de munir V d'une structure de $\mathbb{K}[X]$-module en posant $P(X).v = f(P(X))(v) = (P(u))(v)$, ce qui redonne la formule de l'énoncé. Enfin si $\lambda \in \mathbb{K} \subset \mathbb{K}[X]$ alors $f_u(\lambda) = f_u(\lambda X^0) = \lambda * u^0 = \lambda * \mathrm{Id}$ et en particulier pour tout $v \in V$ on a bien $\lambda.v = \lambda * v$ de sorte que l'opération de $\mathbb{K}[X]$ étend bien celle de $\mathbb{K}$.

7.15 Exercice 15.

1. Pour tout $s \in S$ on a $0.s = 0 \in N$ car N est un sous-module de M. Donc $0 \in I_N^S$. Soient a, $b \in I_N^S$, alors pour tout $s \in S$ on a $(a-b).s = a.s - b.s \in N$ car N est un sous-module. Donc $(a-b) \in I_N^S$ et I_N^S est un sous-groupe additif de A. Soit $a \in A$ et $i \in I_N^S$. Alors pour tout $s \in S$ on a $(ai).s = a.(i.s) \in N$ car $i.s \in N$ et N est un sous-module. Cela montre que I_N^S est un idéal de A.
2. comme $\langle S\rangle \subset S$ on a par définition l'inclusion $I_N^S \subset I_N^{\langle S\rangle}$. Réciproquement prenons $i \in I_N^S$ et $x \in \langle S\rangle$. Par la proposition 1.10 on sait qu'il existe une famille $(\lambda_s)_{s\in S}$ d'éléments de A, tous nul sauf un nombre fini, tels que $x = \sum_{s\in S} \lambda_s s$. Il suit $ix = \sum_{s\in S} i(\lambda_s s) = \sum_{s\in S} \lambda_s (is) \in N$ car pour tout s on a $is \in N$ et N est un sous-module. Cela montre l'inclusion réciproque et l'égalité annoncée.

7.16 Exercice 16.

On doit aussi supposer $M \neq \{0\}$. Prenons $x \neq 0$ et $x \in M$. Alors le sous-module engendré par x est non nul donc égal à M tout entier. On obtient donc un morphisme surjectif $\phi_x\colon \mathbb{Z} \longrightarrow M$ en posant $\phi_x(k) = kx$. Par factorisation M est isomorphe à $\mathbb{Z}/\ker\phi_x$ et il reste à vérifier que $\ker\phi_x$ est un idéal maximal. Mais comme M est simple $\mathbb{Z}/\ker\phi_x$ n'a pas de sous-module non triviaux c'est-à-dire pas d'idéaux non triviaux. Cet anneau quotient est donc un corps, ce qui montre que $\ker\phi_x$ est un idéal maximal de $\mathbb{Z}$.

7.17 Exercice 17.

On doit supposer A commutatif. Pour toute A-algèbre B l'application $a \in A \mapsto a.1_B \in B$ est un morphisme de A-algèbre. En particulier pour tout A-module M on a un morphisme de A algèbre canonique $\varphi\colon A \longrightarrow \mathrm{End}_A(M)$ défini par $(\varphi(a))(m) = a.m$, autrement dit par l'opération externe. Montrons que $\mathrm{Ann}_A(M) = \ker\varphi$. Soit $x \in \mathrm{Ann}_A(M)$. Alors pour tout $m \in M$ on a $0 = x.m = (\varphi(x))(m)$. Donc $x \in \ker\varphi$. Réciproquement soit $x \in \ker\varphi$. Alors l'application $m \mapsto x.m$ est l'endomorphisme nul de M. Donc pour tout $m \in M$ on a $x.m = 0$. Donc $x \in \mathrm{Ann}_A(M)$. On obtient ainsi en toute généralité un morphisme injectif $f\colon A/\mathrm{Ann}_A(M) \longrightarrow \mathrm{End}_A(M)$. Montrons que si en outre M est monogène alors ce morphisme est surjectif. Soit $f \in \mathrm{End}_A(M)$ et soit $m \in M$ tel que $M = Am$. Alors $f(m) \in M$ et donc il existe $\lambda \in A$ tel que $f(m) = \lambda.m$. Mais alors pour tout $x = \mu m \in M$ on a $f(x) = f(\mu.m) = \mu.f(m) = \mu.(\lambda.m) = \lambda.(\mu.m) = \lambda.x$. Ce qui montre que $f = \varphi(\overline{\lambda}) \in \mathrm{Im}\,\varphi$. On a donc bien isomorphie entre $A/\mathrm{Ann}_A(M)$ et $\mathrm{End}_A(M)$. Cela démontre aussi que $\mathrm{End}_A(M)$ est commutatif (puisque A l'est).

7.18 Exercice 18.

On doit supposer $A \neq \mathbb{K}$ Soient $x = a/b$ et $y = c/d$ deux éléments de $\mathbb{K}$ distincts (avec a, b, c d $\in A$, $b \neq 0$ et $d \neq 0$). Alors $(bc).x = ac = (da).y$ et donc $(bc).x - (da).y = 0$. Puis que x et y sont distincts, l'un deux au moins est non nul et donc bc ou da est non nul. Donc x et y sont linéairement dépendant. Pour cette raison, si $\mathbb{K}$ est libre alors c'est un module libre de rang 1. Montrons par l'absurde que ce n'est pas le cas. Soit $x \in \mathbb{K}$ tel que $Ax = \mathbb{K}$ et soit $y \in A$ tel que $y \neq 0$ et $y \notin A^\times$. Alors Pour tout a dans A on a $ay \neq 1$ et donc $ax \neq x/y$. Donc x/y n'est pas dans le module engendré par x, ce qui contredit $Ax = \mathbb{K}$.

7.19 Exercice 19.

Par la proposition 1.9 on peut identifier les notions de sommes directes internes et externes. Pour cet exercice on considère que M_1 et M_2 sont des sous-modules de M et qu'il sont supplémentaire l'un à l'autre dans M. C'est avec ce point de vue que le quotient M/M_1 a un sens (sinon il faudrait remplacer M/M_1 par $M/\imath_1(M_1)$). Ceci dit par le premier théorème d'isomorphie de Noether on a $M/M_1 = (M_1 + M_2/M_1) \cong M_2/(M_1 \cap M_2) = M_2/\{0\} \cong M_2$.

7.20 Exercice 20.

Puisque $f \circ g = \mathrm{Id}_N$ alors g est injective. En effet si $x \in \ker g$, alors $x = f(g(x)) = f(0) = 0$. Donc on a isomorphie entre N et $g(N) \subset M$. Pour obtenir un isomorphisme entre $N \oplus \ker f$ et M on va montrer que $g(N)$ est un supplémentaire à $\ker f$ dans M. Soit $x \in (g(N) \cap \ker f)$. Alors il existe $y \in N$ tel que $x = g(y)$. Mais comme $x \in \ker f$ on obtient $y = f(g(y)) = f(x) = 0$. Et en appliquant g on trouve $x = g(y) = g(0) = 0$. Soit $m \in M$, et soit $n = f(m) \in N$. Alors $f(m - g(n)) = f(m) - f(g(n)) = n - n = 0$. Donc $m - g(n) \in \ker f$ et $m = g(n) + (m - g(n)) \in g(N) + \ker f$. Donc $M = \ker f + g(N)$ et la somme est directe.

7.21 Exercice 21.

Compte-tenu de (i) il s'agit de montrer que pour tout j le sous-module M_j est facteur direct du module $\left\langle \bigcup_{i \neq j} M_i \right\rangle$. On procède par récurrence sur n à partir de $n = 2$. Si $n = 2$ il n'y a rien à montrer. Supposons la propriété vraie pour toute famille de k sous-modules $M_1, \cdots, M_k$ dans tout module $M' = \langle M_1 \bigcup M_2 \cdots M_k \rangle$ avec $k \geq 2$. Prenons $M_1, \cdots, M_k, M_{k+1}$ des sous-modules de M vérifiant (i) et (ii). Alors la sous-famille $M_1, \cdots, M_k$ vérifie (i) et (ii) dans le sous-module $M' = \langle M_1 \bigcup M_2 \bigcup \cdots M_k \rangle$. Par récurrence M' est somme directe interne $M' = \bigoplus_{i=1}^{i=k} M_i$. De plus la propriété (ii) pour $j = n = (k+1)-1$ montre que les sous-modules M_{k+1} et M' sont facteurs directs. Par (i) ils sont supplémentaires l'un à l'autre et on a donc $M = M' \bigoplus M_{k+1} = (\bigoplus_{i=1}^{i=k} M_i) \bigoplus M_{k+1}$.

7.22 Exercice 22.

Par le lemme 1.4 si cette suite exacte est scindée on a un isomorphisme (de groupe ou de $\mathbb{Z}$-module) entre $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/p^2\mathbb{Z}$. Cela est absurde puisque tous les éléments du

premier groupe sont d'ordre divisant p tandis que dans le second $\overline{1}$ est d'ordre p^2.

7.23 Exercice 23.

$$T_{\mathbb{Z}}(\mathbb{Z}^{(2)}) = \{(x,y) \in \mathbb{Z}^2;\ \exists \lambda \in \mathbb{Z}\ \lambda x = \lambda y = 0\} = \{(0,0)\}$$

Et en général tout module libre sur un anneau intègre est sans torsion.
Le module $\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ contient le sous-module $\{(0,y);\ y \in \mathbb{Z}/6\mathbb{Z}\}$ ce dernier étant de torsion puisqu'annulé par 6. Réciproquement si $(x,y) \in T_{\mathbb{Z}}(\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z})$ alors il existe λ non nul dans $\mathbb{Z}$ tel que $\lambda(x,y) = (\lambda x, \lambda y) = (0,0)$. Cela entraîne $x = 0$ d'où $(x,y) \in \{(0,y);\ y \in \mathbb{Z}/6\mathbb{Z}\}$. On a donc $T_{\mathbb{Z}}(\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}) = \{(0,y);\ y \in \mathbb{Z}/6\mathbb{Z}\}$.
Le module $\mathbb{Q}/\mathbb{Z}$ est de torsion. Montrons le. Soit $x \in \mathbb{Q}/\mathbb{Z}$. Alors il existe $a,\ b\ \in \mathbb{Z}$ tels que $b \neq 0$ et $x = \pi_{\mathbb{Z}}(a/b)$. Il suit $bx = b\pi_{\mathbb{Z}}(x) = \pi_{\mathbb{Z}}(bx) = \pi_{\mathbb{Z}}(a) = 0$ car $a \in \mathbb{Z}$. En particulier $T_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$. Le même raisonnement (et sa conclusion) demeurent valable si on remplace $\mathbb{Z}$ par tout anneau commutatif intègre et $\mathbb{Q}$ par le corps des fractions de cet anneau.
Pour $x \in \mathbb{R}$ on a équivalence entre l'existence d'un λ dans $\mathbb{Z}$ non nul tel que $\lambda x \in \mathbb{Z}$ et l'appartenance de x à $\mathbb{Q}$. En passant au quotient modulo $\mathbb{Z}$ on en déduit $T_{\mathbb{Z}}(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$.

7.24 Exercice 24.

Les vecteurs $e_1 = (2,0,0)$ et $e_2 = (0,1,0)$ sont clairement linéairement indépendants. Montrons par l'absurde qu'on ne peut pas les compléter en une base. Soit $e_3 = (x,y,z)$ dans $\mathbb{Z}^3$ tels que e_1, e_2, e_3 soit une base de $\mathbb{Z}^3$. Alors il existe λ, μ, ν dans $\mathbb{Z}$ tels que $\lambda e_1 + \mu e_2 + \nu e_3 = (1,0,0)$. Cela conduit au système d'équations linéaires :

$$\begin{cases} 2\lambda + \nu x = 1 \\ \mu + \nu y = 0 \\ \nu z = 0 \end{cases}$$

En regardant la troisième équation on obtient $\nu = 0$ ou $z = 0$. Si $\nu = 0$ alors on trouve sur la première équation $2\lambda = 1$ ce qui est absurde. Si $z = 0$ alors tous les e_i sont dans le sous-module (strict) engendré par $(1,0,0)$ et $(0,1,0)$. Dans tous les cas $\{e_1, e_2, e_3\}$ n'est pas une base.
On remarque que $(2,0,0) = 2(1,0,0)$ *c'est-à-dire que le vecteur* $(2,0,0)$ *n'est pas indivisible. Dans les modules libres de rang finis sur les anneaux principaux les vecteurs d'une base sont indivisible, et réciproquement.*
On note $\varepsilon_1 = (2,0,0)$, $\varepsilon_2 = (3,0,0)$, $\varepsilon_3 = (0,1,0)$ et $\varepsilon_4 = (0,0,1)$ de sorte que $S = \{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4\}$. Pour tout $(x,y,z) \in \mathbb{Z}^3$ on a $(x,y,z) = x(\varepsilon_2 - \varepsilon_1) + y\varepsilon_3 + z\varepsilon_4$ donc S engendre $\mathbb{Z}^3$. Par l'unicité du rang des modules libres si il est possible d'extraire une base de S ce sera en enlevant un seul vecteur. En outre ε_1 et ε_2 sont linéairement dépendant car ils vérifient $3\varepsilon_1 - 2\varepsilon_2 = 0$. Donc si il est possible d'extraire une base de S ou bien $S\backslash\{\varepsilon_1\}$ est une base ou bien $S\backslash\{\varepsilon_2\}$ est une base. Mais $S\backslash\{\varepsilon_2\}$ contient les vecteurs e_1 et e_2 du début de l'exercice donc n'est pas une base. En reprenant exactement le même raisonnement on peut voir qu'il n'est pas possible de compléter $\{\varepsilon_2, \varepsilon_3\}$ en une base. On a donc épuisé toutes les possibilités : S ne contient pas de base.

7.25 Exercice 25.

On obtient un tel système en prenant $S_2 = \{(1,4,2);(5,20,5);(2,3,4)\}$. En effet $S_2 \subset S$ donc $\langle S_2 \rangle \subset \langle S \rangle = N$. Réciproquement on doit montrer l'inclusion $S \backslash S_2 \subset \langle S_2 \rangle$. Cette dernière inclusion est une conséquence des égalités : $(3,2,6) = 2(2,3,4) - (1,4,2)$ et $(3,2,1) = (5,20,5) + 2(2,3,4) - 6(1,4,2)$.

Fin du corrigé des exercices du chapitre 1.

Chapitre 8

Corrigé des exercices du chapitre 2

8.26 Exercice 26.

1. Le vecteur $(1, 2, -1)$ est non nul il engendre donc un sous-module de rang 1.
2. Les deux vecteurs $(1, -1, -1)$ et $(0, 1, 2)$ sont linéairement indépendants, ils engendrent donc un sous-module de rang 2.
3. les vecteurs $(1, 0, -1)$ et $(0, 2, 3)$ sont linéairement indépendants. Par contre on a $(2, 2, 1) = 2(1, 0, -1) + (0, 2, 3)$. Donc N est de rang 2.
4. D'après le lemme 2.1 le module N est libre de rang au plus 3. Réciproquement les vecteurs $(-1, -1, 1)$; $(0, 1, 2)$ et $(0, 0, 1)$ et sont linéairement indépendants (en effet la matrice de leur coefficients est triangulaire avec des coefficients ± 1 sur la diagonale). Donc N est de rang 3.
5. Les deux vecteurs $(1, 2, 4)$ et $(-1, 3, 2)$ sont linéairement indépendants. Le rang de N est donc au moins 2. De plus on constate que $(5, 0, 8) = 3(1, 2, 4) - 2(-1, 3, 2)$ et $(3, -4, 0) = (1, 2, 4) - 2(-1, 3, 2)$. Le sous-module N est donc librement engendré par les deux vecteurs $(1, 2, 4)$ et $(-1, 3, 2)$: son rang est 2.

8.27 Exercice 27.

On doit réduire, en suivant la méthode de l'exemple détaillé en cours la matrice des coordonnées des vecteurs de S, que l'on complète par $(0, 0, 0, 0)$ pour obtenir une matrice carrée.

$$\left|\begin{array}{cccc|c} 2 & 0 & -4 & 0 & X \\ 0 & 6 & 0 & 0 & Y \\ 2 & 6 & 2 & 0 & Z \\ 2 & 6 & 2 & 0 & T \end{array}\right| \quad C_1 \leftarrow C_1 - C_3 \sim \left|\begin{array}{cccc|c} 6 & 0 & -4 & 0 & X \\ 0 & 6 & 0 & 0 & Y \\ 0 & 6 & 2 & 0 & Z \\ 0 & 6 & 2 & 0 & T \end{array}\right| \sim$$

$$\left|\begin{array}{cccc|c} 0 & 6 & 2 & 0 & Z \\ 0 & 6 & 0 & 0 & Y \\ 6 & 0 & -4 & 0 & X \\ 0 & 6 & 2 & 0 & T \end{array}\right| \quad \begin{array}{c} C_1 \leftarrow C_3 \\ C_3 \leftarrow C_1 \end{array} \sim \left|\begin{array}{cccc|c} 2 & 6 & 0 & 0 & Z \\ 0 & 6 & 0 & 0 & Y \\ -4 & 0 & 6 & 0 & X \\ 2 & 6 & 0 & 0 & T \end{array}\right| \sim$$

$$\left|\begin{array}{cccc|c} 2 & 6 & 0 & 0 & Z \\ 0 & 6 & 0 & 0 & Y \\ 0 & 12 & 6 & 0 & X+2Z \\ 0 & 0 & 0 & 0 & T-Z \end{array}\right| \begin{array}{c} C_1 \leftarrow C_3 \\ C_2 \leftarrow C_2 - 3C_1 \\ \sim \end{array} \left|\begin{array}{cccc|c} 2 & 0 & 0 & 0 & Z \\ 0 & 6 & 0 & 0 & Y \\ 0 & 12 & 6 & 0 & X+2Z \\ 0 & 0 & 0 & 0 & T-Z \end{array}\right| \sim$$

$$\left|\begin{array}{cccc|c} 2 & 0 & 0 & 0 & Z \\ 0 & 6 & 0 & 0 & Y \\ 0 & 0 & 6 & 0 & X+2Z-2Y \\ 0 & 0 & 0 & 0 & T-Z \end{array}\right|$$

Cette matrice donne la structure de M/N avec

$$\frac{M}{N} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{6\mathbb{Z}} \oplus \frac{\mathbb{Z}}{6\mathbb{Z}} \oplus \frac{\mathbb{Z}}{0} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{6\mathbb{Z}} \oplus \frac{\mathbb{Z}}{6\mathbb{Z}} \oplus \mathbb{Z}$$

Pour connaître une base de $\mathbb{Z}^4$ adaptée à N on doit calculer l'inverse de la matrice $\mathcal{G}$ qui correspond aux opérations effectuées sur les lignes. Ces opérations ont été « stockées » sur les polynômes de la dernière colonnes, la matrice $\mathcal{G}$ est donc

$$\mathcal{G} = \begin{array}{c} \begin{array}{cccc} X & Y & Z & T \end{array} \\ \left|\begin{array}{cccc} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & -2 & 2 & 0 \\ 0 & 0 & -1 & 1 \end{array}\right| \end{array}.$$

On doit ensuite calculer la matrice inverse de $\mathcal{G}$. Vous pouvez utiliser la méthode que vous préférez pour ce calcul. Dans ce qui suit je détaille le calcul de l'inversion de $\mathcal{G}$ en la réduisant à la matrice identité par des *opérations sur les lignes*. Si on fait subir simultanément à la matrice identité les mêmes opérations sur les lignes on obtient la matrice inverse de $\mathcal{G}$ en fin d'algorithme. (exercice supplémentaire : pourquoi ?).

$$\left|\begin{array}{cccc||cccc} 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & -2 & 2 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 1 \end{array}\right| \sim \left|\begin{array}{cccc||cccc} 1 & -2 & 2 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 1 \end{array}\right| \sim$$

$$\left|\begin{array}{cccc||cccc} 1 & 0 & 2 & 0 & 0 & 2 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 1 \end{array}\right| \sim \left|\begin{array}{cccc||cccc} 1 & 0 & 0 & 0 & -2 & 2 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right|.$$

La matrice inverse de $\mathcal{G}$ est donc

$$\mathcal{G}^{-1} = \left|\begin{array}{cccc} -2 & 2 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right|$$

Une base adaptée à N s'obtient donc avec le système de vecteurs

$$B = \{(-2,0,1,1);(2,1,0,0);(1,0,0,0);(0,0,0,1)\}.$$

La terminologie "base adaptée" signifie

- B est une base de $\mathbb{Z}^4$
- le système $\tilde{B} = \{2(-2,0,1,1); 6(2,1,0,0); 6(1,0,0,0); 0(0,0,0,1)\}$ obtenu en multipliant **dans l'ordre** les vecteurs de B par les diviseurs élémentaires de N est une base de N (après que l'on ait supprimé les vecteurs nuls).

Après le calcul d'une base adaptée je recommande vivement de s'assurer par un calcul direct que le système $d_i b_i$ où d_i est le i$^{\text{ème}}$ diviseur élémentaire et b_i le i$^{\text{ème}}$ vecteur de la base adaptée est bien contenu dans le module de départ. Cela fournit un test assez rapide pour la justesse des autres calculs. Par exemple ici on a :

$$2(-2,0,1,1) = (-4,0,2,2) \in N$$

$$6(2,1,0,0) = (12,6,0,0) = -3(-4,0,2,2) + (0,6,6,6) \in N$$

$$6(1,0,0,0) = (6,0,0,0) = (2,0,2,2) - (-4,0,2,2) \in N$$

8.28 Exercice 28.

Il est important de retenir que classifier les modules à isomorphisme près c'est la même chose que classifier les matrices de relations à équivalence près. Dans le cours on a fait la classification des modules en se servant de la classification des matrices. Ici on utilise la démarche réciproque. En effet par le lemme Chinois, on a des isomorphismes :$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/60\mathbb{Z} \cong \mathbb{Z}/20\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$. En particulier lorsqu'on réduit chaque matrice à son représentant canonique, à savoir diagonal et avec des coefficients diagonals ordonnés par divisibilité on obtient dans les deux cas la matrice

$$\begin{bmatrix} 1 & 0 \\ 0 & 60 \end{bmatrix}.$$

Les deux matrices du départ sont donc équivalentes. On pouvait aussi de façon plus calculatoire réduire chaque matrice par l'algorithme de Smith.

8.29 Exercice 29.

On note $A = (a_{i,j})$ la matrice de u de l'énoncé.

1. (a) Si on écrit la matrice de ψ dans la base canonique de $\mathbb{K}[X]^d$ on retrouve la *matrice caractéristique* de u c'est-à-dire la matrice $A - X\,\mathrm{Id}$. Le déterminant de ψ est donc le polynôme caractéristique de u, de degré d. Pour la suite de l'exercice on notera $\chi(X)$ ce polynôme.

   (b) D'après le théorème de classification on sait qu'il existe $P_1(X), \cdots, P_s(X)$ dans $\mathbb{K}[X]$ tels que $\mathbb{K}[X]^d/\operatorname{Im}\psi$ soit isomorphe à la somme directe

   $$\bigoplus_{i=1}^{s} \mathbb{K}[X]/(P_i(X)) \ .$$

   Pour calculer ces P_i on sait qu'on réduit la matrice de ψ avec des opérations élémentaires qui laissent le déterminant inchangé. En particulier $\chi(X) = \det\psi = \prod_i P_i$. Aucun P_i n'est nul et la dimension sur $\mathbb{K}$ de chaque facteur $\mathbb{K}[X]/(P_i(X))$ est égal au degré de $P_i(X)$. Il suit $\dim_{\mathbb{K}}(\mathbb{K}[X]^d/\operatorname{Im}\psi) = \sum_i \deg(P_i(X)) = \deg(\chi(X)) = d$.

2. (a) Soit i fixé $1 \leq i \leq d$. On calcule $\varphi(\psi(\varepsilon_i)) = \varphi(\sum_j a_{i,j}\varepsilon_j - X\varepsilon_i) = \sum_j a_{i,j}\varepsilon_j - X.\varepsilon_i = u(\varepsilon_i) - u(\varepsilon_i) = 0$. Donc le morphisme $\mathbb{K}[X]$-linéaire $\varphi \circ \psi$ est nul sur un système générateur de $\mathbb{K}[X]^d$.

   (b) L'égalité $\varphi \circ \psi = 0$ donne l'inclusion $\operatorname{Im}\psi \subset \ker\varphi$. Par factorisation on en déduit l'existence d'un morphisme surjectif $\overline{\varphi}\colon \mathbb{K}[X]/\operatorname{Im}\psi \longrightarrow \operatorname{Im}\varphi = V_u$. Enfin puisque ces deux $\mathbb{K}$-espaces vectoriels ont même dimension ce morphisme est aussi injectif. Cela démontre aussi que l'inclusion $\operatorname{Im}\psi \subset \ker\varphi$ est en fait une égalité. En d'autre terme nous avons montré l'exactitude de la suite

$$0 \longrightarrow \mathbb{K}[X]^d \xrightarrow{\psi} \mathbb{K}[X]^d \xrightarrow{\varphi} V_u \longrightarrow 0$$

3. Avant tout il faut remarquer que les $(P_i)_{i=1}^{i=s}$ sont bien les mêmes que ceux de la question 1 : cela vient de l'isomorphie établie en question 2. Ensuite après quelques minutes de reflection le lecteur se convaincra que le polynôme minimal de u est aussi un générateur de l'idéal annulateur du $\mathbb{K}[X]$-module de torsion V_u. Cet annulateur est très facile à calculer pour un module de la forme $\bigoplus_{i=1}^{s}\mathbb{K}[X]/(P_i(X))$: comme les P_i sont ordonnés par divisibilité il s'agit de (P_s). Le polynôme minimal de u est donc égal à P_s (à multiplication par une constante inversible près). De même on a vu en question 1 que $\chi(X)$ est égal au produit des $P_i(X)$ (à multiplication par une constante inversible près). En particulier le polynôme minimal divise le polynôme caractéristique : c'est le théorème de Cayley-Hamilton.

8.30 Exercice 30.

1. Soit A^s le module libre de rang s muni de sa base canonique $\{\varepsilon_i, i = 1, \cdots, s\}$. Le morphisme $\psi\colon \varepsilon_i \mapsto m_i$ est bien défini surjectif et son noyau est $\ker\psi = \oplus_i(d_i)\varepsilon_i$. Soit δ_{js} le symbole de Kronecker (c'est-à-dire $\delta_{js} = 1$ si $j = s$ et $\delta_{js} = 0$ sinon). Le morphisme $\tilde{u}_i\colon \varepsilon_j \mapsto \delta_{js}m_i$ est bien défini. Le noyau de ce morphisme est $\ker\tilde{u}_i = \oplus_{i\neq s}A\varepsilon_i \oplus (d_i)\varepsilon_s$, et comme $(d_s) \subset (d_i)$ on a $\ker\psi \subset \ker\tilde{u}_i$. Par factorisation on obtient un morphisme $u_i\colon M \cong A^s/\ker\psi \longrightarrow M$ tel que $u_i(m_j) = \delta_{js}m_i$.
2. Soient $a_{i,j}$ des éléments de A tels que $u(m_i) = \sum_{j=1}^{s} a_{i,j}m_j$. Alors on a $u(m_i) = u(u_i(m_s)) = u_i(u(m_s))$ puisque u commute avec u_i. On en déduit $u(m_i) = u_i(\sum_{j=1}^{s} a_{s,j}m_j) = u_i(a_{s,s}m_s) = a_{s,s}m_i$. Si on pose $a = a_{s,s}$ on a montré que u coïncide avec la multiplication par a sur le système générateur $\{m_i, i = 1, \cdots, s\}$.
3. Si u est un morphisme de groupe qui commute avec tous les endomorphisme A linéaire, alors u commute aussi avec la multiplication par λ pour tout λ de A. Autrement dit pour tout m de M et tout λ de A on a $u(\lambda m) = \lambda u(m)$ et u est A-linéaire. Par la question qui précède u est la multiplication par un scalaire $a \in A$.
4. On munit V de la structure de $\mathbb{K}[X]$-module V_u. Montrons l'égalité $\mathcal{C} = \operatorname{End}_{\mathbb{K}[X]}(V_u)$. Soit $v \in \mathcal{C}$. Alors v est $\mathbb{K}$-linéaire donc est un morphisme de groupe. Soit $P(X) = \sum p_iX^i \in \mathbb{K}[X]$ et $m \in V_u$. On a $v(P(X).m) = v(P(u)(m)) = P(u)(v(m)) = P(X).v(m)$. En effet comme v commute avec u il commute aussi avec tous les polynômes en u. On a démontré l'inclusion $\mathcal{C} \subset \operatorname{End}_{\mathbb{K}[X]}(V_u)$. Réciproquement si $v \in \operatorname{End}_{\mathbb{K}[X]}(V_u)$, alors $v \in \operatorname{End}_{\mathbb{K}}(V)$ et pour tout $m \in V$ on a $v(u(m)) = v(X.m) = X.v(m) = u(v(m))$. On a démontré l'égalité $\mathcal{C} = \operatorname{End}_{\mathbb{K}[X]}(V_u)$. Maintenant si f est un endomorphisme de groupe de V qui commute avec tous les éléments de $\mathcal{C}$ alors par la question précédente f est la multiplication par un scalaire de $\mathbb{K}[X]$ c'est-à-dire un

polynôme en u.

8.31 Exercice 31.

1. Supposons u et v semblables. Alors il existe un K-endomorphisme f de V tel que $u = f \circ v \circ f^{-1}$ ou encore tel que $u \circ f = f \circ v$. On note $*_u$ et $*_v$ les opérations externes de $\mathbb{K}[X]$ sur respectivement V_u et V_v. En terme de $\mathbb{K}[X]$ modules on obtient pour tout $m \in V$ l'égalité $X *_u f(m) = f(X *_v m)$, puis par une récurrence immédiate $X^n *_u f(m) = f(X^n *_v m)$ pour tout $n \in \mathbb{N}$. Comme f est $\mathbb{K}$-linéaire cela suffit à montrer que f est $\mathbb{K}[X]$-linéaire : f est un $\mathbb{K}[X]$-isomorphisme entre V_u et V_v. Réciproquement supposons que V_u et V_v soient isomorphes, et soit f un $\mathbb{K}[X]$ isomorphisme $f\colon V_u \longrightarrow V_v$. Pour tout $m \in V$ on a $f(X *_u m) = X *_v f(m)$ c'est-à-dire $f(u(m)) = v(f(m))$. Donc v et u sont semblables.
2. Pour $0 \leq i \leq n-2$ on a $X\ \overline{X^i} = \overline{X^{i+1}}$ et $X\ \overline{X^{n-1}} = \overline{X^n} = \sum_{i=0}^{i=n-1} -a_i\overline{X^i}$. On en déduit que la la matrice A_P est de la forme :

$$A_P = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & -a_2 \\ \vdots & & \ddots & 0 & \vdots \\ 0 & 0 & & 1 & -a_{n-1} \end{pmatrix}$$

   D'après l'exercice 29 le polynôme caractéristique de u_P est égal à son polynôme minimal et ils sont tous deux égaux à P (à une constante inversible près).
3. D'après la question 1 classer les endomorphismes de $\mathbb{K}^d$ à similitude près est équivalent à classer les $\mathbb{K}[X]$-modules de torsion de $\mathbb{K}$-dimension d à isomorphisme près. Comme ces $\mathbb{K}[X]$-modules sont classifiés par leurs diviseurs élémentaires les endomorphismes à similitude près sont classifiés par la suite des diviseurs élémentaires du module associé. Cela donne l'existence des (P_i) et le fait qu'ils caractérisent la classe de similitude d'un endomorphisme.
4. Soit $\chi(X)$ le polynôme caractéristique de $A_n(\lambda)$ et $\mu(X)$ son polynôme minimal. Par une récurrence immédiate on constate que $\chi(X) = (X-\lambda)^n$. Donc $\mu(X) \mid (X-\lambda)^n$. Notons $\varepsilon_1, \cdots, \varepsilon_n$ la base canonique de $\mathbb{K}^n$. Sur la matrice de $A_n(\lambda)$ on constate que $(A_n(\lambda) - \lambda id)(\varepsilon_i) = \varepsilon_{i+1}$ si $i < n$ (et aussi $(A_n(\lambda) - \lambda id)(\varepsilon_n) = 0$). Il suit que si $k < n$ $(A_n(\lambda) - \lambda \operatorname{Id})^k \neq 0$ et donc $\mu(X) = \chi(X) = (X-\lambda)^n$. D'après l'exercice 29 les invariants de similitude $P_1, \cdots, P_s$ de $A_n(\lambda)$ vérifient $P_s = \mu$ et $\prod P_i = \chi$. En conséquence on a $s = 1$ et $P_1 = \chi = \mu = (X-\lambda)^n$. Donc $A_n(\lambda)$ est semblable à la matrice compagnon de $(X-\lambda)^n$.
5. Soit $P(X)$ un polynôme de $\mathbb{K}[X]$ dont toutes les racines sont dans $\mathbb{K}$. Alors $P(X)$ se factorise en $P(X) = \prod_{i=1}^{i=t}(X-\lambda_i)^{n_i}$, et par le lemme Chinois on a un isomorphisme :

$$\frac{\mathbb{K}[X]}{(P(X))} \cong \bigoplus_{i=1}^{i=t} \frac{\mathbb{K}[X]}{((X-\lambda_i)^{n_i})}\ .$$

   En terme de similitude on obtient que la matrice compagnon de P est semblable à la matrice diagonale par bloc dont les blocs sont les $A_{n_i}(\lambda_i)$. En général on a vu que

toute matrice est semblable à une matrice diagonale par bloc, chaque bloc étant la matrice compagnon de certains polynôme (les P_i de la question 3). En raisonnant bloc diagonal par bloc diagonal on constate que si chaque P_i à toutes ses racines dans $\mathbb{K}$ on peut réduire le bloc compagnon de P_i en une matrice elle-même diagonale par bloc, chacun de blocs étant de Jordan. Comme le produit des P_i est le polynôme caractéristique de A, une condition suffisante pour qu'une matrice A soit semblable a une matrice diagonale par bloc chaque bloc étant de Jordan est que les valeurs propres de A soient toutes dans $\mathbb{K}$. Si $\mathbb{K}$ est algébriquement clos cette condition est remplie par toute matrice.

Fin du corrigé des exercices du chapitre 2.

Chapitre 9

Annales.

9.1 premier devoir 04/05.

Master de mathématiques Année 1 semestre 2

UV Module

à renvoyer le lundi 28 février 2005

Exercice 1 Existe-t'il des sous-$\mathbb{Z}$-modules non nuls M et N de $\mathbb{Z}$ tels que $\mathbb{Z} = M \oplus N$?

Exercice 2 On suppose A commutatif, soit M un A-module. Soit $m \in M$ tel que pour tout $\alpha \neq 0$ dans A on ait $\alpha m \neq 0$.

1. Montrer que $\langle m \rangle$ est isomorphe à A.
2. Montrer l'équivalence entre les assertions suivantes :
   (a) $\langle m \rangle$ admet un supplémentaire dans M (c'est-à-dire il existe un sous-module $N \subset M$ tel que $M = N \oplus \langle m \rangle$).
   (b) Il existe une forme linéaire $f \in \mathrm{Hom}(M, A)$ telle que $f(m) = 1$.

Exercice 3 Soit A un anneau commutatif. On note $T(M)$ le sous-module de torsion du A-module M.

1. Soit $f\colon M \longrightarrow N$ est un morphisme de A-modules. Montrer l'inclusion $f(T(M)) \subset T(N)$.
2. On suppose donnée une suite exacte de modules
   $$0 \longrightarrow M \xrightarrow{\mu} N \xrightarrow{\nu} P.$$
   Définir les morphismes de A modules et vérifier l'exactitude de la suite
   $$0 \longrightarrow T(M) \xrightarrow{\mu} T(N) \xrightarrow{\nu} T(P).$$
3. La suite de $\mathbb{Z}$-modules ci dessous est exacte (le vérifier) :
   $$0 \longrightarrow \mathbb{Z} \xrightarrow{x \mapsto 2x} \mathbb{Z} \xrightarrow{x \mapsto \overline{x}} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$
   Existe-t'il une suite de $\mathbb{Z}$-modules
   $$0 \longrightarrow T(\mathbb{Z}) \longrightarrow T(\mathbb{Z}) \longrightarrow T(\mathbb{Z}/2\mathbb{Z}) \longrightarrow 0 \text{ ? pourquoi ?}$$

9.2 solution du premier devoir 04/05.

Master de mathématiques Année 1 semestre 2

UV Module : solution du premier devoir.

Exercice 1 Soit M et N deux sous-modules non nuls de $\mathbb{Z}$, et soit $m \in M$ et $n \in N$ non nuls. Alors $0 \neq mn \in M \cap N$. Donc $\mathbb{Z}$ n'admet pas de facteurs directs non triviaux.

Exercice 2

1. Par définition du sous-module engendré le morphisme $a \mapsto a.m$ est une surjection de A sur $\langle m \rangle$. Puisque l'annulateur de m est trivial cette surjection est un isomorphisme.
2. Supposons (a), c'est-à-dire que $M = N \oplus \langle m \rangle$. Soit $\varphi\colon \langle m \rangle \longrightarrow A$ l'isomorphisme de la question précédente (défini par $\varphi(a.m) = a$), et $\psi\colon N \longrightarrow A$ le morphisme nul. Alors le morphisme $f = \psi \oplus \varphi\colon N \oplus \langle m \rangle \longrightarrow A$ est une forme linéaire vérifiant $f(m) = 1$.
   Réciproquement supposons (b) et soit $g\colon A \longrightarrow \langle m \rangle$ l'isomorphisme $g(a) = a.m$. Alors on a $f \circ g = \mathrm{Id}_A$. Et de même que dans l'exercice 20 on en déduit l'égalité $M = \ker f \oplus \langle m \rangle$.

Exercice 3

1. Soit $m \in T(M)$. Alors il existe $\lambda \in A$ tel que $\lambda \neq 0$ et $\lambda m = 0$. Il suit $\lambda f(m) = f(\lambda m) = 0$, avec $\lambda \neq 0$. Donc $f(m) \in T(N)$ et $f(M) \subset T(N)$.
2. Par le 1 les restrictions de μ et ν définissent des morphismes $\mu'\colon T(M) \longrightarrow T(N)$ et $\nu'\colon T(N) \longrightarrow T(P)$. Naturellement μ' reste injectif et on a $\nu' \circ \mu' = 0$ c'est-à-dire $\operatorname{Im}\mu' \subset \ker\nu'$. Réciproquement soit $n \in \ker\nu'$. Alors $n \in \ker\nu \cap T(N)$, et il existe donc $m \in M$ tel que $\mu(m) = n$ et aussi $\lambda \neq 0$ tel que $\lambda n = 0$. Il suit $0 = \lambda\mu(m) = \mu(\lambda m)$ et comme μ est injectif on a $\lambda m = 0$. On a donc $m \in T(M)$ et $\mu'(m) = n$. Donc $n \in \operatorname{Im}\mu'$. Cela démontre que la suite $0 \longrightarrow T(M) \xrightarrow{\mu'} T(N) \xrightarrow{\nu'} T(P)$ est exacte.
3. Comme $\mathbb{Z}$ est intègre l'application $x \mapsto 2x$ est injective, et son image est bien entendu égale à $2\mathbb{Z}$ qui est le noyau de la surjection $\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$. ce qui montre que la suite requise est exacte.
   On a $T(\mathbb{Z}) = 0$ et $T(\mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z} \neq 0$. Si il existait une suite
   $$0 \longrightarrow T(\mathbb{Z}) \longrightarrow T(\mathbb{Z}) \longrightarrow T(\mathbb{Z}/2\mathbb{Z}) \longrightarrow 0\,,$$
   on aurait $\mathbb{Z}/2\mathbb{Z} = 0$ ce qui est absurde.

9.3 deuxième devoir 04/05.

Master de mathématiques Année 1 semestre 2

UV Module : deuxième devoir.

à renvoyer le lundi 18 avril 2005

Exercice 1 Soit A un anneau principal. Pour tout A-module M et tout irréductible p de A, on appelle sous-module p-primaire de M et note $T_p(M)$ l'ensemble $T_p(M) = \{m \in M; \exists n \in \mathbb{N}\ p^n m = 0\}$. On fixe un système de représentant $\mathcal{P}$ des irréductibles dans A. On veut démontrer l'égalité

$$T(M) = \bigoplus_{p\in\mathcal{P}} T_p(M).$$

1. Montrer que pour tout p et tout M l'ensemble $T_p(M)$ est un sous-module de M.
2. Soit
$$a = u\prod_{p\in\mathcal{P}} p^{e_p} \in A \text{ avec } u \in A^\times\ .$$
Montrer que
$$\left(\frac{A}{(a)}\right) \cong \bigoplus_{p\in\mathcal{P}} \frac{A}{(p^{e_p})} \text{et en déduire } \frac{A}{(a)} = \bigoplus_{p\in\mathcal{P}} T_p\left(\frac{A}{(a)}\right)\ .$$
3. conclure.

Exercice 2 En utilisant la classification des $\mathbb{Z}$-modules et la décomposition p-primaire de l'exercice 1, donner la liste complète à isomorphisme près des groupes d'ordre 400.

Exercice 3 Soit N le sous-$\mathbb{Z}$-module de $\mathbb{Z}^4$ engendré par les quatres vecteurs $(1,1,-1,1)$, $(1,3,-3,1)$, $(1,1,5,1)$ et $(1,1,-7,7)$. Donner la structure de $\mathbb{Z}^4/N$ et une base de $\mathbb{Z}^4$ adaptée à N.

9.4 solution du deuxième devoir 04/05.

Master de mathématiques Année 1 semestre 2

UV Module : solution du deuxième devoir.

Exercice 1

1. Soient λ, $\mu \in A$ et x, $y \in T_p(M)$. Alors il existe $n \in \mathbb{N}$ tel que $p^n x = p^n y = 0$. Il suit $p^n(\lambda x + \mu y) = \lambda p^n x + \mu p^n y = 0$. Donc $\lambda x + \mu y \in T_p(M)$ et cet ensemble est bien un sous-module de M.
2. Le premier isomorphisme n'est rien d'autre que le lemme Chinois. En utilisant cet isomorphisme il reste à démontrer que

$$\bigoplus_{p\in\mathcal{P}} \frac{A}{(p^{e_p})} = \bigoplus_{q\in\mathcal{P}} T_q\left(\bigoplus_{p\in\mathcal{P}} \frac{A}{(p^{e_p})}\right).$$

   Pour pouvoir conclure il suffit de montrer l'égalité (après identification de $\frac{A}{(q^{e_q})}$ avec son image dans la somme directe) :

$$T_q\left(\bigoplus_{p\in\mathcal{P}} \frac{A}{(p^{e_p})}\right) = \frac{A}{(q^{e_q})}.$$

   Trivialement $q^{e_q}\frac{A}{(q^{e_q})} = 0$ d'où l'inclusion $\frac{A}{(q^{e_q})} \subset T_q\left(\bigoplus_{p\in\mathcal{P}} \frac{A}{(p^{e_p})}\right)$. Réciproquement soit $x = (x_p)_{p\in\mathcal{P}} \in T_q\left(\bigoplus_{p\in\mathcal{P}} \frac{A}{(p^{e_p})}\right)$. Alors il existe $n \in \mathbb{N}$ tel que $q^n x = 0$. Pour montrer que $x \in \frac{A}{(q^{e_q})}$ on doit voir que $x_p = 0$ pour tout $p \neq q$. Mais si $p \neq q$ alors grâce à une relation de Bezout on sait que q^n est inversible modulo p^{e_p} et donc $q^n x_p = 0$ entraîne $x_p = 0$. D'où l'égalité attendue.
3. Par le théorème de classification $T(M)$ est somme directe interne de modules de la forme $A/(a)$. Par la question qui précède ces facteurs sont sommes directes internes de leurs sous-modules p-primaires. En regroupant les parties p-primaires (par commutativité de la somme directe) on obtient bien

$$T(M) = \bigoplus_{p\in\mathcal{P}} T_p(M).$$

Exercice 2 On factorise $400 = 2^4 \times 5^2$. Soit G un groupe abélien d'ordre 400. Alors par l'exercice 1 $G = T_2(G) \oplus T_5(G)$ et on a $\#T_2(G) = 2^4$ et $\#T_5(G) = 5^2$. En utilisant le théorème de classification, on dresse la liste complète des groupes abéliens d'ordre 2^4 et des groupes abéliens d'ordre 5^2. En combinant ces deux listes on obtient alors la liste complète sans répétition des groupes abéliens d'ordre 400.

- liste des groupes abélien d'ordre 25 : Soit H abélien un groupe d'ordre 25 et soit $d_1 \mid d_2 \cdots \mid d_r$ les diviseurs élémentaires de H. Alors comme $\prod_i d_i = 25$ on a seulement deux possibilités, $r = 2$ et $d_1 = d_2 = 5$ ou $r = 1$ et $d_1 = 25$. A isomorphismes près les deux seuls groupes abéliens d'ordre 25 sont donc $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/25\mathbb{Z}$.
- liste des groupes abélien d'ordre 16 : Soit H un groupe abélien d'ordre 16 et $d_1 \mid d_2 \mid \cdots \mid d_r$ les diviseurs élémentaires de H. Alors comme $\prod_i d_i = 2^4$ le nombre r est compris entre 1 et 4. Pour $r = 1$ la seule possibilité est $d_1 = 16$. Pour $r = 2$ les deux seules possibilités sont $d_1 = 2$ et $d_2 = 8$ ou bien $d_1 = d_2 = 4$. Pour $r = 3$ la seule possibilité est $d_3 = 4$ et $d_1 = d_2 = 2$. Pour $r = 4$ la seule possibilité est $d_1 = d_2 = d_3 = d_4 = 2$. A isomorphismes près il existe exactement 5 groupes d'ordre 16 à savoir : $(\mathbb{Z}/2\mathbb{Z})^4$; $(\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/4\mathbb{Z}$; $(\mathbb{Z}/4\mathbb{Z})^2$; $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$; et $\mathbb{Z}/16\mathbb{Z}$.
- liste des groupes abélien d'ordre 400 : A isomorphismes près il existe exactement 10 groupes d'ordre 400 dont la liste (sous la forme canonique du théorème des diviseurs élémentaires) suit : $\mathbb{Z}/400\mathbb{Z}$; $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/200\mathbb{Z}$; $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/100\mathbb{Z}$; $(\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/100\mathbb{Z}$; $(\mathbb{Z}/2\mathbb{Z})^3 \oplus \mathbb{Z}/50\mathbb{Z}$; $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/80\mathbb{Z}$; $\mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/40\mathbb{Z}$; $\mathbb{Z}/20\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$; $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$; et $(\mathbb{Z}/2\mathbb{Z})^2 \oplus (\mathbb{Z}/10\mathbb{Z})^2$.

Exercice 3 On applique l'algorithme de Smith à la matrice déduite des générateurs de N. On obtient :

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 1 & 1 \\ -1 & -3 & 5 & -7 \\ 1 & 1 & 1 & 7 \end{pmatrix} \begin{matrix} X \\ Y \\ Z \\ T \end{matrix} \quad \begin{matrix} C_2 \leftarrow C_2 - C_1 \\ C_3 \leftarrow C_3 - C_1 \\ C_4 \leftarrow C_4 - C_1 \\ \sim \end{matrix} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ -1 & -2 & 6 & -6 \\ 1 & 0 & 0 & 6 \end{pmatrix} \begin{matrix} X \\ Y \\ Z \\ T \end{matrix}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & -2 & 6 & -6 \\ 0 & 0 & 0 & 6 \end{pmatrix} \begin{matrix} X \\ -X+Y \\ X+Z \\ -X+T \end{matrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 6 & -6 \\ 0 & 0 & 0 & 6 \end{pmatrix} \begin{matrix} X \\ -X+Y \\ Y+Z \\ -X+T \end{matrix}$$

$$\begin{matrix} C_4 \leftarrow C_4 + C_3 \\ \sim \end{matrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 6 \end{pmatrix} \begin{matrix} X \\ -X+Y \\ Y+Z \\ -X+T \end{matrix}$$

On en déduit $\mathbb{Z}^4/N \simeq \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ et la matrice $\mathcal{G}$ provenant des opérations sur les lignes effectuées se déduit des polynômes de la dernière colonne.

On a

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix} \text{ et } \mathcal{G}^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ -1 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

D'après le cours la $\mathbb{Z}$-base de $\mathbb{Z}^4$ formée des vecteurs ε_1, ε_2, ε_3, ε_4 qui suivent est une base adaptée à N.

$$\varepsilon_1 = \begin{pmatrix} 1 \\ 1 \\ -1 \\ 1 \end{pmatrix}; \varepsilon_2 = \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}; \varepsilon_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}; \varepsilon_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Comme conseillé dans le cours on vérifie que les $d_i\varepsilon_i$ sont bien des éléments de N :

$$\varepsilon_1 = (1, 1, -1, 1) \in N$$

$$2\varepsilon_2 = (1, 3, -3, 1) - (1, 1, -1, 1) \in N$$

$$6\varepsilon_3 = (1, 1, 5, 1) - (1, 1, -1, 1) \in N$$

$$6\varepsilon_4 = (1, 1, -7, 7) + (1, 1, 5, 1) - 2(1, 1, -1, 1) \in N$$

9.5 Épreuve principale première session 2005.

Master de mathématiques Année 1 semestre 2

session de juin 2005

UV Module

Épreuve principale

Les documents, calculatrices et téléphones portables sont interdits.

Exercice 1 Dresser la liste à isomorphisme près et sans répétition des groupes abéliens d'ordre 72.

Exercice 2 Soit A un anneau unitaire. Soient M et N deux A-modules. Montrer qu'il existe deux suites exactes $0 \longrightarrow M \longrightarrow M \oplus N \longrightarrow N \longrightarrow 0$ et $0 \longrightarrow N \longrightarrow M \oplus N \longrightarrow M \longrightarrow 0$.

Exercice 3 Soit R le sous-$\mathbb{Z}$-module de $\mathbb{Z}^4$ engendré par les vecteurs colonnes de la matrice

$$\mathcal{R} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 2 & 2 & 4 & 12 \\ 1 & 1 & 1 & 11 \end{pmatrix}.$$

Donner la structure de $\mathbb{Z}^4/R$ et une base adaptée à R.

9.6 Solution de l'épreuve principale première session 2005.

Master de mathématiques Année 1 semestre 2

session de juin 2005

UV Module

Solution de l'épreuve principale

Exercice 1 Soit G un tel groupe. Partant de $72 = 2^3\ 3^2$, on sait que $G = T_2(G) \oplus T_3(G)$, avec $o(T_2(G)) = 2^3$ et $o(T_3(G)) = 3^2$. En utilisant la classification on sait qu'il y a (à isomorphisme près) 3 groupes abéliens d'ordre 8 (à savoir $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$, et $(\mathbb{Z}/2\mathbb{Z})^3$) ; et 2 groupes abéliens d'ordre 9 (à savoir $\mathbb{Z}/9\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$). En combinant ces deux listes on conclut à la liste de 6 groupes abéliens d'ordre 72 ci-dessous :

$$G_1 = \mathbb{Z}/72\mathbb{Z} \qquad G_2 = \mathbb{Z}/3 \oplus \mathbb{Z}/24\mathbb{Z}$$

$$G_2 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/36\mathbb{Z} \qquad G_4 = \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$$

$$G_5 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z} \qquad G_6 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$$

Exercice 2 Dans cette solution la notation $M \oplus N$ désigne le somme directe externe, on pouvait aussi considérer les sommes directes internes, d'après le cours ces deux notions coïncident. En utilisant l'isomorphie naturelle $M \oplus N \cong N \oplus M$ obtenue avec $(m, n) \mapsto (n, m)$ il suffit par symétrie de montrer l'existence de la première suite exacte. On définit $\imath\colon M \longrightarrow M \oplus N$ avec $\imath(m) = (m, 0)$ et $\rho\colon M \oplus N \longrightarrow N$ par $\rho(m, n) = n$. Manifestement $\imath$ est injective, ρ est surjective et $\ker\rho = \{(m, n) \in M \oplus N | n = 0\} = \operatorname{Im}\imath$. Cela établit l'exactitude de la suite :

$$0 \longrightarrow M \xrightarrow{\imath} M \oplus N \xrightarrow{\rho} N \longrightarrow 0$$

Exercice 3 On applique à la matrice $\mathcal{R}$ l'algorithme de Smith tel que décrit dans le cours.

$$\mathcal{R} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 2 & 0 & 2 & 10 \\ 1 & 0 & 0 & 10 \end{pmatrix} \begin{matrix} X \\ Y \\ Z \\ T \end{matrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 10 \\ 0 & 0 & 0 & 10 \end{pmatrix} \begin{matrix} X \\ -X+Y \\ -2X+Z \\ -X+T \end{matrix}$$

$$\mathcal{R} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 10 \end{pmatrix} \begin{matrix} X \\ -X+Y \\ -2X+Z \\ -X+T \end{matrix}.$$

On a donc

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -2 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix} \text{ et } \mathcal{G}^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

D'après le cours le système $e_1 = (1, 1, 2, 1)$; $e_2 = (0, 1, 0, 0)$; $e_3 = (0, 0, 1, 0)$; et $e_4 = (0, 0, 0, 1)$ forme une base adaptée à R et on a $\mathbb{Z}^4/R \simeq Z/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

9.7 Épreuve complémentaire première session 2005.

Master de mathématiques Année 1 semestre 2

session de juin 2005

UV Module

Épreuve complémentaire

Les documents, calculatrices et téléphones portables sont interdits.

Exercice 1 Dans $M_2(\mathbb{Z})$ les matrices $A = \begin{pmatrix} 15 & 0 \\ 0 & 42 \end{pmatrix}$ et $B = \begin{pmatrix} 30 & 0 \\ 0 & 21 \end{pmatrix}$ sont elles semblables ?

Exercice 2 Soit $a \in \mathbb{Z}$ un entier et soit d le pgcd de a et 12 et soit a' tel que $a = da'$. Soit $\mathcal{R}$ la matrice de $M_3(\mathbb{Z})$ suivante

$$\mathcal{R} = \begin{pmatrix} 2 & 6 & 0 \\ 0 & a & 0 \\ 4 & 0 & a \end{pmatrix}.$$

1. Calculer le déterminant de $\mathcal{R}$.
2. Montrer que $\begin{pmatrix} a & 0 \\ -12 & a \end{pmatrix}$ et $\begin{pmatrix} d & 0 \\ 0 & aa' \end{pmatrix}$ sont semblables.
3. Soit R le sous-$\mathbb{Z}$-module de $\mathbb{Z}^3$ engendré par les vecteurs colonnes de la matrice $\mathcal{R}$. Montrer que $\mathbb{Z}^3/R$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/aa'\mathbb{Z}$.
4. Donner (suivant la parité de a) les diviseurs élémentaires de $\mathbb{Z}^3/R$.

9.8 Solution de l'épreuve complémentaire première session 2005.

Master de mathématiques Année 1 semestre 2

session de juin 2005

UV Module

Solution de l'épreuve complémentaire

Exercice 1 Par le théorème chinois on a des isomorphismes :

$$\mathbb{Z}/15\mathbb{Z} \oplus \mathbb{Z}/42\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z} \cong \mathbb{Z}/30\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z}.$$

Les deux matrices présentent donc des modules isomorphes : elles sont semblables.

Exercice 2

1. $\det \mathcal{R} = 2a^2$.
2. Par le théorème de classification on sait a priori que la matrice $A = \begin{pmatrix} a & 0 \\ -12 & a \end{pmatrix}$ est semblable à une matrice diagonale $D = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ telle que (i) le pivot α soit le p.g.c.d. positif des coefficients de A et (ii) $\det(A) = \det(B)$. Il suit $\alpha = d$ et $\beta = a^2/d = aa'$.
3. En effectuant sur $\mathcal{R}$ l'opération élémentaire $C_2 \leftarrow C_2 - 3C_1$ on obtient la matrice

   $$\mathcal{R} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & a & 0 \\ 0 & -12 & a \end{pmatrix}. \text{ Avec 2 on en déduit : } \mathcal{R} \sim \begin{pmatrix} 2 & 0 & 0 \\ 0 & d & 0 \\ 0 & 0 & aa' \end{pmatrix}.$$

   Cela donne l'isomorphie annoncée.
4. D'après 3, on sait que $\mathbb{Z}^3/R \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/aa'\mathbb{Z}$. Si 2 divise a alors 2 divise d qui divise aa' et donc la suite des invariants de similitude de $\mathbb{Z}^3/R$ est $(2, d, aa')$. Si 2 ne divise pas a, alors par le lemme Chinois et commutativité de $\oplus$ on obtient $\mathbb{Z}^3/R \cong \mathbb{Z}/d \oplus \mathbb{Z}/2aa'$ et comme d divise $2aa'$ la suite des invariants de similitude de $\mathbb{Z}^3/R$ est $(d, 2aa')$.

9.9 Épreuve principale deuxième session 2005.

Master de mathématiques Année 1 semestre 2

session d'août 2005

UV Module

Épreuve principale

Exercice 1 Dresser la liste à isomorphisme près et sans répétition des groupes abéliens d'ordre $500 = 2^2 \times 5^3$.

Exercice 2 Soit V un espace vectoriel sur un corps commutatif $\mathbb{K}$.

1. Soit $f \in \mathrm{End}_{\mathbb{K}}(V)$. Justifier que l'application ci-dessous définie munit V d'une structure de $\mathbb{K}[X]$-module. Dans la suite on notera V_f ce module.

$$\mathbb{K}[X] \times V \longrightarrow V$$

$$(\textstyle\sum_{i=0}^{i=n} a_i X^i, v) \longmapsto \sum_{i=0}^{i=n} a_i f^i(v)$$

2. Soient f et g deux endomorphismes $\mathbb{K}$-linéaires de V. On dit que f est semblable à g et on note $f \sim g$ lorsqu'il existe un automorphisme $\mathbb{K}$-linéaire α de V tel que $f = \alpha^{-1} \circ g \circ \alpha$. Montrer que f est semblable à g si et seulement si les modules V_f et V_g sont isomorphes.

Exercice 3 Soit R le sous-$\mathbb{Z}$-module de $\mathbb{Z}^4$ engendré par les vecteurs colonnes de la matrice

$$\mathcal{R} = \begin{pmatrix} 8 & 12 & 6 & 4 \\ 7 & 12 & 6 & 5 \\ 5 & 10 & 12 & 7 \\ 2 & 10 & 6 & 10 \end{pmatrix}.$$

Donner la structure de $\mathbb{Z}^4/R$ et une base adaptée à R.

9.10 Solution de l'épreuve principale deuxième session 2005.

Master de mathématiques Année 1 semestre 2

session d'août 2005

UV Module

Solution de l'épreuve principale

Exercice 1 Voir l'exercice 1 de l'épreuve principale de la première session 2005 (en remplaçant le couple ordonné de nombre premier (2,3) par (5,2)).

Exercice 2

1. Voir l'exercice 14 du cours.
2. Voir la première question de l'exercice 31 du cours.

Exercice 3 Voir l'exemple détaillé du cours et tous les exercices similaires, par exemple le troisième exercice de l'épreuve principale de la première session.

9.11 Épreuve complémentaire deuxième session 2005.

Master de mathématiques Année 1 semestre 2

session de juin 2005

UV Module

Épreuve complémentaire

Les documents, calculatrices et téléphones portables sont interdits.

Exercice 1 Soit $A = \{a + b\sqrt{7};\ a,\ b \in \mathbb{Z}\}$, on note $A^\times$ le groupe (multiplicatif) formé des éléments inversibles dans A de A.

1. Montrer que A est un sous-anneau de $\mathbb{R}$.
2. Soit $x = a + b\sqrt{7} \in A$. Montrer l'équivalence $x \in A^\times \iff a^2 - 7b^2 = \pm 1$.
3. Montrer que $A^\times$ est infini (on pourra vérifier puis utiliser $8 + 3\sqrt{7} \in A^\times$).

Exercice 2 Soit R le sous-$\mathbb{Q}[X]$-module de $\mathbb{Q}[X]^3$ engendré par les vecteurs colonnes de la matrice

$$\mathcal{R} = \begin{pmatrix} 3X-1 & -2X & 3X-1 \\ X^2-1 & 0 & 2X^2-2 \\ X^2-11X+3 & 7X & 2X^2-11X+2 \end{pmatrix}.$$

Donner la structure de $\mathbb{Q}[X]^3/R$. On ne précisera pas de base adapté et il n'est pas forcément utile de finir l'algorithme de Smith.

9.12 Solution de l'épreuve complémentaire deuxième session 2005.

Master de mathématiques Année 1 semestre 2

session de juin 2005

UV Module

Solution de l'épreuve complémentaire.

Exercice 1

1. Clairement $A \subset \mathbb{R}$ et $1 \in A$. On vérifie immédiatement que A est stable par l'addition et le passage à l'inverse additif. Si $x = a + b\sqrt{7} \in A$ et $x' = a' + b'\sqrt{7} \in A$, alors $xx' = ((aa' + tbb') + (ab' + a'b)\sqrt{7})$ appartient encore à A. Donc A est un sous-anneau de $\mathbb{R}$.
2. On définit $N\colon A \longrightarrow \mathbb{Z}$ par la formule $N(a+b\sqrt{7}) = (a+b\sqrt{7})(a-b\sqrt{7}) = a^2 - 7b^2$. On vérifie facilement que N est multiplicative. Il suit que si $x = a+b\sqrt{7}$ est inversible dans A alors $N(x)$ est inversible dans $\mathbb{Z}$ c'est-à-dire égal à plus ou moins 1, et réciproquement que si $N(x) = \pm 1$, alors $\pm(a - b\sqrt{7})$ est un inverse à x dans A.
3. Le nombre $x = 8 + 3\sqrt{7}$ vérifie $N(x) = 1$ donc est inversible dans A. D'autre part on a $x > 1$ et donc pour tout n entier $x^n > 1$. En particulier l'ordre multiplicatif de x est infini et donc $A^\times$ contient le sous-groupe isomorphe à $\mathbb{Z}$ engendré par x qui est infini.

Exercice 2 On réduit la matrice $\mathcal{R}$. On obtient

$$\mathcal{R} \sim \begin{pmatrix} 3X-1 & -2X & 0 \\ X^2-1 & 0 & X^2-1 \\ X^2-11X+3 & 7X & X^2-1 \end{pmatrix} \sim \begin{pmatrix} 3X-1 & -2X & 0 \\ 0 & 0 & X^2-1 \\ -11X+4 & 7X & X^2-1 \end{pmatrix}$$

$$\sim \begin{pmatrix} 3X-1 & -2X & 0 \\ 0 & 0 & X^2-1 \\ -11X+4 & 7X & 0 \end{pmatrix} \sim \begin{pmatrix} X^2-1 & 0 & 0 \\ 0 & 3X-1 & -2X \\ 0 & -11X+4 & 7X \end{pmatrix}.$$

A ce stade on voit que $\mathbb{Q}[X]^3/R$ est isomorphe à la somme directe de $\mathbb{Q}[X]/(X^2-1)$ avec le module correspondant à la sous-matrice carré

$$\mathcal{R}' = \begin{pmatrix} 3X-1 & -2X \\ -11X+4 & 7X \end{pmatrix}.$$

Les invariants de similitude de cette matrice se calculent facilement : le pgcd des coefficient est 1 et le second invariant est donc égal au déterminant qui vaut $X(1-X)$. On obtient ainsi l'isomorphie :

$$\mathbb{Q}[X]^3/R \cong \mathbb{Q}[X]/(X^2-1) \bigoplus \mathbb{Q}[X]/(X(1-X)).$$