Algèbre Commutative

Johan Huisman

Année 1997–1998

Table des matières

Chapitre 1

Anneaux

1.1 Anneaux et morphismes

Rappelons la définition d'un anneau. Soit A un ensemble. Soient $+$ et $\cdot$ deux lois internes sur A, c-à-d, $+$ et $\cdot$ sont des applications de $A \times A$ dans A. On notera $a + b$ au lieu de $+(a, b)$ et $a \cdot b$, voir ab, au lieu de $\cdot(a, b)$. On va considérer les conditions suivantes :

A1 $\forall a, b, c \in A : (a + b) + c = a + (b + c)$ (l'associativité de $+$)

A2 $\exists z \in A : \forall a \in A : a + z = z + a = a$ (l'existence élément neutre additif)

Lorsque **A2** est satisfaite, l'élément neutre additif z de A est unique. En effet, si $z' \in A$ satisfait aussi $a + z' = z' + a = a$ quel que soit $a \in A$, on aura en particulier $z' = z' + z = z$. Cela montre l'unicité de l'élément neutre additif. Désormais, on lui réserve la notation 0.

Sous l'hypothèse de **A2** :

A3 $\forall a \in A : \exists b \in A : a + b = b + a = 0$ (l'existence d'opposé)

Lorsque **A1**–**A3** sont satisfaites, l'opposé d'un élément $a \in A$ est uniquement déterminé. En effet, si b' est aussi un opposé de a, on aura $b' = b' + 0 = b' + (a + b) = (b' + a) + b = 0 + b = b$. Cela montre l'unicité de l'opposé d'un élément $a \in A$. On le notera $-a$.

A4 $\forall a, b \in A : a + b = b + a$ (la commutativité de $+$)

A5 $\forall a, b, c \in A : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ et $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (la distributivité)

A6 $\forall a, b, c \in A : (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (l'associativité de $\cdot$)

A7 $\exists u \in A \forall a \in A : a \cdot u = u \cdot a = a$ (l'existence élément neutre multiplicatif)

On peut montrer l'unicité de u comme l'on a fait pour l'élément neutre additif. On le désignera par 1.

A8 $\forall a, b \in A : a \cdot b = b \cdot a$ (la commutativité de $\cdot$)

Définition 1.1.1. Soit A un ensemble muni de deux lois internes $+$ et $\cdot$. Le triplet $(A, +, \cdot)$ est un *anneau* si les conditions **A1**–**A6** sont satisfaites. Le triplet $(A, +, \cdot)$ est un *anneau unitair* si de plus **A7** est satisfaite. Le triplet $(A, +, \cdot)$ est un *anneau unitair commutatif* si toutes les conditions **A1**–**A8** sont satisfaites. Par abus de langage, on dira aussi que A au lieu du triplet $(A, +, \cdot)$ est un anneau, anneau unitair ou un anneau unitair commutatif.

Comme on ne considérera essentiellement que des anneaux unitairs commutatifs, on dira «anneau» au lieu «d'anneau unitair commutatif» pour simplifier. Lorsqu'on considère des anneaux non commutatifs ou non unitairs, on l'explicitera.

Observons que l'ensemble A muni de sa loi additive $+$ est un groupe abélien lorsque $(A, +, \cdot)$ est un anneau.

Exemple 1.1.2.

1. L'ensemble $\{0\}$ n'admet qu'une structure d'anneau. C'est l'anneau nul, noté 0.

2. Tous les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ munis de leurs lois internes habituelles sont des anneaux.

3. Pour un entier n positif, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des entiers modulo n muni de ses lois internes habituelles est un anneau.

4. Lorsque A est un anneau, $A[X]$ désigne l'ensemble des polynômes à coefficients dans A. Un tel polynôme est une somme formelle $\sum_{i=0}^{n} a_i X^i$ où $a_i \in A$, $i = 0, \ldots, n$ et $n \in \mathbb{N}$. Deux de tels polynômes $\sum_{i=0}^{n} a_i X^i$ et $\sum_{i=0}^{m} b_i X^i$ sont égaux si et seulement si $a_i = b_i$ pour tout i. Là et ailleurs, il est sous-entendu que $a_i = 0$ pour $i > n$ et $b_i = 0$ pour $i > m$. On définit deux lois internes sur $A[X]$ par

$$\sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{m} b_i X^i = \sum_{i=0}^{\max\{n,m\}} (a_i + b_i) X^i$$

et

$$(\sum_{i=0}^{n} a_i X^i) \cdot (\sum_{i=0}^{m} b_i X^i) = \sum_{k=0}^{n+m} (\sum_{\substack{i \geq 0, j \geq 0 \\ i+j=k}} a_i b_j) X^k.$$

On peut vérifier que $A[X]$ est alors un anneau, c'est l'anneau des polynômes en X à coefficients dans A.

5. On définit alors par récurrence l'anneau des polynômes en $X_1, \ldots, X_n$ à coefficients dans A : $A[X_1, \ldots, X_n] = (A[X_1, \ldots, X_{n-1}])[X_n]$.

6. Soit G un groupe abélien. Soit $\mathrm{End}(G)$ l'ensemble des endomorphismes de G, i.e., l'ensemble des homomorphismes de G dans lui-même. On définit deux lois internes $+$ et $\cdot$ sur $\mathrm{End}(G)$ par

$$f \cdot g = f \circ g \text{ et } (f + g)(x) = f(x) + g(x)$$

quel que soit $x \in G$. On vérifie facilement que $\mathrm{End}(G)$ est un anneau unitair qui n'est pas forcément commutatif.

Les conditions **A1**, **A2** et **A4** permettent de définir, dans un anneau quelconque A, les sommes indexées par un ensemble fini. En effet, soit I un ensemble fini et soit $a_i \in A$ pour tout $i \in I$. On définit $\sum_{i\in I} a_i \in A$ par récurrence sur le cardinal de I. Si I est vide, $\sum_{i\in I} a_i = 0$ par définition. Lorsque I est non vide, soit $i_0 \in I$. On définit alors

$$\sum_{i\in I} a_i = a_{i_0} + \sum_{i\in I\setminus\{i_0\}} a_i,$$

la dernière somme étant définie par récurrence. On notera $\sum_{i\in\{m,\dots,n\}} a_i$ par $\sum_{i=m}^{n} a_i$ ou encore par $a_m + a_{m+1} + \cdots + a_n$.

De même, les conditions **A6**, **A7** et **A8** permettent de définir, dans un anneau quelconque, les produits $\prod_{i\in I} a_i$ indexés par un ensemble fini I. Cette fois-ci ce produit est égal à 1 lorsque I est vide. On notera $\prod_{i=m}^{n} a_i$ ou encore $a_m \cdot a_{m+1} \cdots a_n$ au lieu de $\prod_{i\in\{m,\dots,n\}} a_i$.

Définition 1.1.3. Soit A un anneau. Un élément $a \in A$ est *régulier* lorsque $ab = 0$ implique que $b = 0$. Un élément $a \in A$ est un *diviseur de zéro* si a n'est pas régulier, i.e., s'il existe $b \in A$, $b \neq 0$ et $ab = 0$. L'anneau A est *intègre* lorsque A est non nul et chaque élément non nul de A est régulier, autrement dit, A est non nul et n'a pas de diviseurs de zéro non nuls.

Exemple 1.1.4.

1. L'anneau des entiers $\mathbb{Z}$ est intègre.
2. L'anneau des polynômes $A[X]$ est intègre lorsque A l'est.
3. $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est nul ou premier.

Définition 1.1.5. Soit A un anneau. Un élément $a \in A$ est *inversible* s'il existe $b \in A$ tel que $ab = ba = 1$. L'anneau A est un *corps* lorsque A est non nul et chaque élément non nul de A est inversible.

On voit qu'un élément inversible est nécessairement régulier. En particulier, un corps est intègre.

Exemple 1.1.6.

1. Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.
2. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.
3. Les anneaux $A[X]$ et $\mathbb{Z}$ ne sont pas de corps.

Si $a \in A$ est inversible, l'élément $b \in A$ tel que $ab = ba = 1$ est uniquement déterminé par a (démonstration comme dans le cas additif). On notera b alors par a^{-1} et on l'appelle *l'inverse* de a. L'ensemble des éléments inversibles d'un anneau A est noté par $A^\star$.

Proposition 1.1.7. *Soit A un anneau. L'ensemble des éléments inversibles $A^\star$ de A est fermé sous multiplication et la paire $(A^\star, \cdot)$ est un groupe abélien.*

Démonstration. D'abord, on montre que $A^\star$ est stable pour la multiplication. Lorsque $a, b \in A^\star$, on a leurs inverses a^{-1} et b^{-1} dans A, et on a $(ab)(b^{-1}a^{-1}) = 1$. Il s'ensuit que ab est inversible. Par conséquent, $A^\star$ est stable pour la multiplication et $\cdot$ est alors bien une loi interne sur $A^\star$.

Comme $\cdot$ est déjà associative et commutative sur A, elle l'est forcément sur le sous-ensemble $A^\star$ de A. Evidemment, l'élément neutre multiplicatif 1 de A

est inversible, donc appartient à $A^\star$. L'élément neutre 1 de A est alors aussi l'élément neutre de $A^\star$. Quant à l'inverse de $a \in A^\star$: on a $a^{-1} \in A$ tel que $aa^{-1} = a^{-1}a = 1$, ce qui montre que a^{-1} appartient lui aussi à $A^\star$ et que a^{-1} est l'inverse de a dans $A^\star$. □

Définition 1.1.8. Soit A un anneau. Le groupe des éléments inversibles de A est le *groupe multiplicatif* de A, noté par $A^\star$.

Définition 1.1.9. Soient A et B des anneaux et $f : A \to B$ une application. L'application f est un *morphisme d'anneaux*, ou par abus de langage un *morphisme*, lorsque

M1 $f(a+b) = f(a) + f(b)$;

M2 $f(ab) = f(a)f(b)$;

M3 $f(1) = 1$;

quels que soient $a, b \in A$.

Exemple 1.1.10.

1. L'identité $\mathrm{id}_A : A \to A$ est un morphisme d'anneaux pour tout anneau A.
2. Quel que soit l'anneau A, l'unique application de A dans l'anneau nul est un morphisme d'anneaux.
3. Les inclusions $\mathbb{Z} \to \mathbb{Q}$, $\mathbb{Z} \to \mathbb{R}$, $\mathbb{Z} \to \mathbb{C}$, $\mathbb{Q} \to \mathbb{R}$, $\mathbb{Q} \to \mathbb{C}$ et $\mathbb{R} \to \mathbb{C}$ sont toutes des morphismes d'anneaux.
4. Soit $n \in \mathbb{Z}$ un entier non nul. L'application $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ de réduction modulo n est un morphisme d'anneaux.

Proposition 1.1.11. *Soient A, B et C des anneaux. Soient $f : A \to B$ et $g : B \to C$ des morphismes d'anneaux. Alors, $g \circ f : A \to C$ est un morphisme d'anneaux.*

Démonstration. Exercice. □

Proposition 1.1.12. *Soit A un anneau. Il existe un et un seul morphisme d'anneaux de $\mathbb{Z}$ dans A.*

Démonstration. Exercice. (Voir aussi Exercice 37.) □

Soit A un anneau. D'après Proposition 1.1.12 il existe un et un seul morphisme d'anneaux de $\mathbb{Z}$ dans A. On notera l'image d'un entier n par ce morphisme encore par n. On fera attention à ce que deux entiers différents ne sont pas forcément différents en tant qu'éléments de A. (Exemple : $1 = 3$ dans $\mathbb{Z}/2\mathbb{Z}$.)

Définition 1.1.13. Soient A et B des anneaux. Un *endomorphisme* de A est un morphisme d'anneaux de A dans lui-même. Un *isomorphisme* de A dans B est un morphisme $f : A \to B$ tel qu'il existe un morphisme $g : B \to A$ avec $g \circ f = \mathrm{id}_A$ et $f \circ g = \mathrm{id}_B$. On dit que A et B sont *isomorphes* s'il existe un isomorphisme de A dans B, noté par $A \cong B$. Un *automorphisme* de A est un isomorphisme de A dans lui-même.

Exemple 1.1.14. 1. L'identité id_A est évidemment un automorphisme d'un anneau A.

2. Un automorphisme non trivial est la conjugaison complexe $\mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$.

3. Les anneaux $A[X]$ et $A[Y]$ sont isomorphes, quel que soit l'anneau A.

1.2 Sous-anneaux

Parmi les sous-ensembles d'un anneau A, ceux qui héritent de A la structure d'un anneau nous intéressent particulièrement.

Définition 1.2.1. Soit $(A, +, \cdot)$ un anneau. Un sous-ensemble B de A est un *sous-anneau* de A lorsque

SA1 $b + b'$, bb' et $-b$ appartiennent à B pour tous les $b, b' \in B$;

SA2 1 appartient à B.

Exemple 1.2.2. 1. $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, de $\mathbb{R}$ et de $\mathbb{C}$. $\mathbb{Q}$ est un sous-anneau de $\mathbb{R}$ et de $\mathbb{C}$. $\mathbb{R}$ est un sous-anneau de $\mathbb{C}$.

2. Soit $\mathbb{D} \subseteq \mathbb{Q}$ le sous-ensemble des nombre décimaux, i.e.,

$$\mathbb{D} = \{\frac{a}{10^n} \mid a \in \mathbb{Z} \text{ et } n \in \mathbb{N}\}.$$

Alors, $\mathbb{D}$ est un sous-anneaux de $\mathbb{Q}$.

3. A est un sous-anneaux de l'anneau de polynômes $A[X]$.

4. Lorsque $f : A \to B$ est un morphisme d'anneaux, $f(A)$ est un sous-anneau de B.

Observons qu'un sous-anneau B de A contient nécessairement l'élément neutre additif 0 de A.

La terminologie de sous-anneau est justifiée par la proposition suivante :

Proposition 1.2.3. *Soit A un anneau et $B \subseteq A$ un sous-anneau de A. Les lois internes $+$ et $\cdot$ sur A induisent des lois internes sur B. L'ensemble B muni de ces lois internes est un anneau.*

Démonstration. Exercice. □

Soit $\mathcal{C}$ une collection de sous-ensembles d'un ensemble E, c-à-d, $\mathcal{C} \subseteq \mathcal{P}(E)$. Rappelons que l'intersection $\bigcap \mathcal{C}$ de $\mathcal{C}$ est par définition

$$\bigcap \mathcal{C} = \{x \in E \mid x \in X \text{ pour tout } X \in \mathcal{C}\}.$$

Lemme 1.2.4. *Soit A un anneau. Soit $\mathcal{C}$ une collection de sous-anneaux de A. Alors l'intersection $\bigcap \mathcal{C}$ est un sous-anneau de A.*

Démonstration. Exercice. □

Proposition 1.2.5. *Soit A un anneau et S un sous-ensemble de A. Alors, le plus petit sous-anneau de A contenant S existe.*

Démonstration. Soit $\mathcal{C}$ la collection des sous-anneaux de A contenant S. D'après Lemme 1.2.4, $\bigcap \mathcal{C}$ est un sous-anneau de A. Evidemment, $\bigcap \mathcal{C}$ contient S. Il reste à montrer que $\bigcap \mathcal{C}$ est le plus petit sous-anneau de A contenant S. Soit alors B un sous-anneau de A contenant S. Comme $B \in \mathcal{C}$, on a $\bigcap \mathcal{C} \subseteq B$. □

Soit A un anneau. Soit B un sous-anneau de A et s un élément de A. Le plus petit sous-anneau de A contenant $B \cup \{s\}$ est noté par $B[s]$. C'est le sous-anneau de A obtenu de B en adjoignant s. On vérifie que

$$B[s] = \{a \in A \mid \exists n \in \mathbb{N} \exists b_i \in B : a = \sum_{i=0}^{n} b_i s^i\}.$$

Exemple 1.2.6.

1. L'anneau de Gauss $\mathbb{Z}[i]$ est le sous-anneau de $\mathbb{C}$ obtenu de $\mathbb{Z}$ en adjoignant i. On a $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.
2. L'anneau des décimaux $\mathbb{D}$ est égal au sous-anneau de $\mathbb{Q}$ obtenu de $\mathbb{Z}$ en adjoignant $\frac{1}{10}$, i.e., $\mathbb{D} = \mathbb{Z}[\frac{1}{10}]$.

1.3 Idéaux

Soit $f : A \to B$ un morphisme d'anneaux. On a vu que l'image $f(A)$ de f est un sous-anneaux de B. On aimerait construire l'anneau $f(A)$, à isomorphisme près, à partir des données intrinsèques à l'anneau A, i.e., sans avoir recours à B ou f. Observons que $f(a) = f(a')$ si et seulement si $a - a' \in \ker(f)$ quels que soient $a, a' \in A$. De ce fait il suffit de connaître le noyau $I = \ker(f)$ de f pour pouvoir construire l'ensemble $f(A)$. En effet, $f(A)$, en tant qu'ensemble, est le quotient de l'ensemble A par la relation d'équivalence $\sim$ définie par

$$a \sim a' \iff a - a' \in I.$$

Le fait que f soit un morphisme d'anneaux impose sur l'ensemble I entre autres les conditions suivantes :

I1 $0 \in I$;

I2 $x, y \in I \Longrightarrow x + y \in I$;

I3 $a \in A$ et $x \in I \Longrightarrow ax \in I$.

Réciproquement, soit $I \subseteq A$ un sous-ensemble vérifiant **I1**, **I2** et **I3**. On verra dans le paragraphe suivant que la relation $\sim$ définie sur A par $a \sim a' \Leftrightarrow a - a' \in I$ est alors une relation d'équivalence et que le quotient de l'ensemble A par $\sim$ admet une structure d'anneau induite par celle de A.

Définition 1.3.1. Soit A un anneau. Un sous-ensemble I de A est un *idéal* de A lorsque les conditions **I1**, **I2** et **I3** sont satisfaites.

La proposition suivante servira à construire des idéaux.

Proposition 1.3.2. *Soient A un anneau et S un sous-ensemble de A. Soit*

$$(S) = \{\sum_{i=1}^{n} a_i s_i \mid a_i \in A, s_i \in S \text{ et } n \in \mathbb{N}\}.$$

Alors, (S) est un idéal de A. C'est le plus petit idéal de A contenant S.

Démonstration. On voit bien que (S) est un idéal de A. De plus, si I est un idéal de A contenant S, $\sum_{i=1}^{n} a_i s_i \in I$ pour tout $a_i \in A$, $s_i \in S$ et $n \in \mathbb{N}$. D'où $(S) \subseteq I$. □

Définition 1.3.3. Soit A un anneau et S un sous-ensemble de A. Alors, l'idéal (S) de A est *l'idéal engendré par* S.

Soit S un sous-ensemble de A. On rencontrera une multitude de notations pour l'idéal engendré par S : (S), AS ou aussi SA ; $(s_1, \ldots, s_n)$ lorsque $S = \{s_1, \ldots, s_n\}$; sA ou aussi As lorsque $S = \{s\}$.

Exemple 1.3.4.

1. L'idéal $n\mathbb{Z}$ dans $\mathbb{Z}$, n un entier.
2. L'idéal (X, Y) dans $A[X, Y]$. C'est l'idéal des polynômes en X et Y sans terme constant.
3. Soit A un sous-anneau de B et I un idéal de A. Alors BI est un idéal de B.

Définition 1.3.5. Soit A un anneau, I un idéal de A et S un sous-ensemble de A. L'idéal I est *engendré* par le sous-ensemble S lorsque $I = (S)$. L'idéal I de A est *de type fini* s'il existe un sous-ensemble fini de A engendrant I, i.e., s'il existe un entier n et $s_1, \ldots, s_n \in A$ tels que $I = (s_1, \ldots, s_n)$. L'idéal I est *principal* lorsque I est engendré par un singleton, i.e., lorsque $I = As$, pour certain $s \in A$.

Malheureusement, un idéal n'est pas forcément de type fini, comme le montre l'exemple suivant :

Exemple 1.3.6. Soit A un anneau non nul et $B = K[X_1, X_2, X_3, \ldots]$ l'anneau de polynômes en les indéterminées $X_1, X_2, X_3, \ldots$ à coefficients dans A. L'idéal $I = (X_1, X_2, X_3, \ldots)$ de B n'est pas de type fini. Pour le montrer on aura besoin du fait suivant.

Soit $n \in \mathbb{N}$. Soit B_n le sous-anneau $K[X_1, \ldots, X_n]$ de B et $I_n \subseteq B_n$ l'idéal de B_n engendré par $X_1, \ldots, X_n$. Alors, on a que l'intersection $I \cap B_n$ est égale à l'idéal I_n de B_n. Effectivement, L'inclusion $I_n \subseteq I \cap B_n$ est évidente car $I_n \subseteq I$ et $I_n \subseteq B_n$. Pour montrer l'inclusion $I_n \supseteq I \cap B_n$, soit $P \in I \cap B_n$. Comme P appartient à I, il existe $m \in \mathbb{N}$ et $P_1, \ldots, P_m \in B$ tels que

$$P = \sum_{i=1}^{m} P_i X_i.$$

Quitte à augmenter m, on peut supposer que chaque P_i est un polynôme en $X_1, \ldots, X_i$ à coefficients dans A. Pour que P appartienne à B_n, il faut alors que P_i soit nul pour tout $i > n$. Comme $P_i \in B_n$ quel que soit $i \leq n$, on a $P \in I_n$. Cela montre que $I \cap B_n = I_n$.

Maintenant on montre que l'idéal I de B n'est pas de type fini. Supposons qu'il existe $P_1, \ldots, P_n \in B$ tels que

$$I = (P_1, \ldots, P_n).$$

Comme B est la réunion de ses sous-anneaux B_k, $k \in \mathbb{N}$. Il existe $k \in \mathbb{N}$ tel que $P_i \in B_k$ quel que soit $i = 1, \ldots, n$. Soit $f : B \to A$ un morphisme d'anneaux tel

que $f(X_{k+1}) = 1$ et $f(X_i) = 0$ quel que soit $i \neq k$. D'après ce qui précède, chaque P_i appartient à l'idéal I_k de B_k engendré par $X_1, \ldots, X_k$. D'où, $P_i \in \ker(f)$ quel que soit i. Comme $\ker(f)$ est un idéal, l'idéal de B engendré par les P_i est contenu dans $\ker(f)$. D'où $I \subseteq \ker(f)$. Mais $X_{k+1} \in I$ et $f(X_{k+1}) = 1 \neq 0$. Contradiction.

Définition 1.3.7. Un anneau A est *noetherien* lorsque tout idéal de A est de type fini. Un anneau A est *principal* lorsque A est intègre et tout idéal de A est principal.

Exemple 1.3.8.

1. Les corps, l'anneau des entiers $\mathbb{Z}$, les anneaux $K[X]$, pour K un corps, sont tous des anneaux principaux.
2. Tout anneau principal est noetherien.
3. Tout anneau fini est noetherien.

On voit souvent la condition équivalente suivante comme définition d'un anneau noetherien :

Proposition 1.3.9. *Soit A un anneau. Alors, A est noetherien si et seulement si chaque chaîne croissante d'idéaux de A*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

est stationnaire, c-à-d, il existe $N \in \mathbb{N}$ tel que $I_{N+k} = I_N$ quel que soit $k \in \mathbb{N}$.

Démonstration. Supposons que A est noetherien. Soit $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ une chaîne croissante d'idéaux de A. L'union $I = \bigcup I_i$ est un idéal de A. Comme A est noetherien, il existe $a_1, \ldots, a_n \in I$ tels que $I = (a_1, \ldots, a_n)$. Puisque I est la réunion des idéaux I_i, $a_j \in I_{i_j}$ pour certain $i_j \in \mathbb{N}$, $j = 1, \ldots, n$. Soit $N = \max\{i_1, \ldots, i_n\}$. Comme $I_{i_j} \subseteq I_N$, on a $a_j \in I_N$ pour $j = 1, \ldots, n$. D'où $I_N \supseteq (a_1, \ldots, a_n) = I$ ce qui implique que la chaîne d'idéaux I_i est stationnaire à partir du rang N.

Réciproquement, supposons que chaque chaîne croissante d'idéaux de A est stationnaire à partir d'un certain rang. Soit $I \subseteq A$ un idéal. On va montrer que I est de type fini. Par l'absurde : si I n'est pas de type fini, on peut choisir $a_1, a_2, a_3, \ldots \in I$ tels que $a_{n+1} \notin (a_1, \ldots, a_n)$. D'après l'hypothèse, la chaîne croissante d'idéaux

$$(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \cdots$$

est stationnaire à partir d'un certain rang $N \in \mathbb{N}$. En particulier, $a_{N+1} \in (a_1, \ldots, a_N)$. Contradiction. □

Rappelons que pour un polynôme non nul $P = a_d X^d + \cdots + a_1 X + a_0$ dans $A[X]$, où $a_d \neq 0$, le degré $\deg(P)$ de P est égal à d. Le degré du polynôme nul est par définition $-\infty$. Observons que l'on a les propriétés suivantes :

D1 $\deg(P) = 0$ lorsque $P \in A \backslash \{0\}$;

D2 $\deg(P + Q) \leq \max\{\deg(P), \deg(Q)\}$ quels que soient $P, Q \in A[X]$;

D3 $\deg(P + Q) = \max\{\deg P, \deg(Q)\}$ lorsque $\deg(P) \neq \deg(Q)$;

D4 $\deg(PQ) \leq \deg(P) + \deg(Q)$ quels que soient $P, Q \in A[X]$;

D5 $\deg(PQ) = \deg(P) + \deg(Q)$ quel que soit $Q \in A[X]$, lorsque le coefficient dominant de P est un élément régulier de A.

Théorème de la base de Hilbert. *Soit A un anneau noetherien. Alors, l'anneau de polynômes $A[X]$ est noetherien.*

Démonstration. Par l'absurde : supposons I est un idéal de $A[X]$ qui n'est pas de type fini. Evidemment, $I \neq \{0\}$. On va construire, par récurrence, des éléments $P_1, P_2, P_3, \ldots$ de I. Soit $P_1 \in I\backslash\{0\}$ un polynôme de plus bas degré. Comme I n'est pas de type fini, $(P_1) \subsetneq I$. Soit $P_2 \in I\backslash(P_1)$ un polynôme de plus bas degré. Alors, $(P_1, P_2) \subsetneq I$. On continue ainsi et on trouve finalement une suite des polynômes $P_1, P_2, P_3, \ldots$ dans I telle que P_{n+1} soit un polynôme dans $I\backslash(P_1, \ldots, P_n)$ de plus bas degré.

Soit d_i le degré du polynôme P_i et $a_i \in A$ le coefficient dominant du polynôme P_i, $i = 1, 2, 3, \ldots$. Par construction, $d_{i+1} \geq d_i$ quel que soit $i \in \mathbb{N}$. Comme A est noetherien, la chaîne croissante d'idéaux de A

$$(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \cdots$$

est stationnaire à partir d'un certain rang n. En particulier, $a_{n+1} \in (a_1, \ldots, a_n)$, c-à-d, il existe $b_i \in A$ tels que $a_{n+1} = \sum_{i=1}^{n} b_i a_i$. On a alors

$$P_{n+1} - \sum_{i=1}^{n} b_i X^{d_{n+1}-d_i} P_i \ \in \ I\backslash(P_1, \ldots, P_n)$$

dont le degré est strictement inférieur à celui de P_{n+1}. Contradiction. □

Corollaire 1.3.10. *Soit A un anneau noetherien. Alors, l'anneau de polynômes $A[X_1, \ldots, X_n]$ est noetherien.*

1.4 Anneaux quotients

Soient A un anneau et I un idéal de A. On va construire *l'anneau quotient* A/I de A par I : Soit $\sim$ la relation sur A définie par

$$a \sim b \Longleftrightarrow a - b \in I.$$

Cette relation est une relation d'équivalence. Soit A/I le quotient de l'ensemble A par $\sim$, c-à-d, A/I est l'ensemble des classes d'équivalences de $\sim$. Pour $a \in A$ on notera sa classe d'équivalence par $\overline{a}$.

Ensuite on définit deux lois internes binaires $+$ et $\cdot$ sur A/I induites par celles de A. D'abord, soient

$$\alpha, \mu \colon A \times A \longrightarrow A/I$$

les applications définies par $\alpha(a, b) = \overline{a + b}$ et $\mu(a, b) = \overline{ab}$. On vérifie que $\alpha(a, b)$ et $\mu(a, b)$ ne dépendent que des classes d'équivalence de a et b. En effet, si $a \sim c$ et $b \sim d$, $(a+b)-(c+d) = (a-c)+(b-d) \in I$ et $ab-cd = b(a-c)+c(b-d) \in I$. D'où, $a + b \sim c + d$ et $ab \sim cd$, c-à-d, $\alpha(a, b) = \alpha(c, d)$ et $\mu(a, b) = \mu(c, d)$. Par

conséquent, α et μ induisent deux lois internes binaires $+$ et $\cdot$ sur A/I définies par

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{et} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Il est facile de vérifier que A/I muni de ces lois internes est un anneau. On a $0 = \overline{0}$, $1 = \overline{1}$ et $-\overline{a} = \overline{-a}$ dans A/I. De plus, l'application

$$\pi : A \longrightarrow A/I$$

qui envoie $a \in A$ sur sa classe d'équivalence $\overline{a}$ est un morphisme d'anneaux.

Définition 1.4.1. Soient A un anneau et I un idéal de A. Le *quotient* de A par I est la paire $(A/I, \pi)$ consistant de *l'anneau quotient* A/I et du *morphisme de passage au quotient* $\pi : A \to A/I$. Parfois on dira par abus de langage que A/I est le quotient.

Soit A un anneau et $I \subseteq A$ un idéal. En général, il n'est pas facile de expliciter un système de représentants pour les classes d'équivalence modulo I. Cependant, pour l'anneau de polynômes $A[X]$ et pour I un idéal de $A[X]$ engendré par un polynôme unitair, il en existe un moyen grâce à la division euclidienne.

Théorème de la division euclidienne. *Soit A un anneau non nul. Soit $F \in A[X]$ unitair. Pour tout polynôme $P \in A[X]$, il existe uniques $Q, R \in A[X]$ tels que $P = FQ + R$ et $\deg(R) < \deg(F)$.*

Démonstration. Tout d'abord, l'assertion est bien vraie lorsque $\deg(F) = 0$, i.e., lorsque $F = 1$. Supposons dans la suite que $F \in A[X]$ est unitair de degré strictement positif.

Puis on montre l'unicité. Supposons que l'on a $P = FQ + R = FQ' + R'$ où $\deg(R) < \deg(F)$ et $\deg(R') < \deg(F)$. Alors, $F \cdot (Q - Q') = R' - R$. On a que $Q - Q' = 0$. En effet, si $Q - Q'$ était non nul, $\deg(Q - Q')$ serait non négatif et $\deg(R - R') = \deg(F \cdot (Q - Q')) = \deg(F) + \deg(Q - Q') \geq \deg(F)$. Tandis que $\deg(R - R') < \deg(F)$. Cela montre bien que $Q - Q' = 0$, i.e., $Q = Q'$ et $R = R'$. D'où l'unicité.

Ensuite, on montre par récurrence l'existence de l'écriture $P = FQ + R$ avec $\deg(R) < \deg(F)$ pour tout $P \in A[X]$. Lorsque $\deg(P) < \deg(F)$, on prend tout simplement $Q = 0$ et $R = P$.

Supposons que l'on a montre l'existence pour tous les polynômes P de degré strictement inférieur à n, où $n \geq \deg(F)$. Soit P un polynôme de degré n. Soit a_n son coefficient dominant. Comme le degré $d = \deg(F)$ de F est inférieur ou égal à n, $P' = P - a_n X^{n-d} F$ est un polynôme. Evidemment, $\deg(P') < \deg(P) = n$. D'après l'hypothèse de récurrence, il existe $Q', R \in A[X]$ tels que $P' = FQ' + R$ et $\deg(R) < \deg(F)$. On a alors $P = F \cdot (Q + a_n X^{n-d}) + R$. D'où l'existence de $Q, R \in A[X]$ tels que $P = FQ + R$ et $\deg(R) < \deg(F)$. □

Corollaire 1.4.2. *Soit A un anneau non nul et $F \in A[X]$ unitair. Soit d le degré de F et $I \subseteq A$ l'idéal engendré par F. Alors, pour tout $P \in A[X]$ il existe un et un seul polynôme $Q \in A[X]$ de degré strictement inférieur à d tel que P soit équivalent à Q modulo I. Autrement dit, le sous-ensemble de $A[X]$ des polynômes de degré strictement inférieur à d est un système de représentants pour les classes d'équivalence modulo I.*

La définition du quotient comme l'anneau quotient muni du morphisme de passage au quotient est d'une subtilité que l'on va expliquer : Le morphisme de passage au quotient établit le lien entre l'anneau et son anneau quotient. Sans ce morphisme il n'y aurait eu aucun rapport entre A et A/I. Ils auraient été tout simplement deux anneau flottant dans l'univers. Par contre, c'est le morphisme, lui, qui les met en rapport. La propriété suivante en est une illustration.

Propriété universelle du quotient. *Soient A un anneau et I un idéal de A. Soit $\pi\colon A \to A/I$ le passage au quotient. Alors, on a $\pi(I) = \{0\}$ et π est le morphisme universel ayant cette propriété, c-à-d, pour tout anneau B et tout morphisme $f\colon A \to B$ avec $f(I) = \{0\}$ il existe un et un seul morphisme $\overline{f}\colon A/I \to B$ tel que le diagramme commute :*

$$\begin{array}{ccc} A & \xrightarrow{\pi} & A/I \\ & \searrow^{f} & \downarrow{\scriptstyle \overline{f}} \\ & & B \end{array} \tag{1.1}$$

Démonstration. Soient $a, b \in A$ tels que $a - b \in I$. Comme $f(I) = 0$, on a $f(a) = f(b)$. Cela montre que l'application $\overline{f}\colon A/I \to B$ définie par $\overline{f}(\overline{a}) = f(a)$ est bien définie. Comme $\overline{f} \circ \pi = f$ est un morphisme d'anneaux et π est un morphisme d'anneaux surjectif, $\overline{f}$ est un morphisme d'anneaux (Exercice 23). L'unicité de $\overline{f}$ s'ensuit de la surjectivité de π. □

On ne veut pas favoriser la construction ci-dessus du quotient d'un anneau et on appelle un quotient de A par I tout morphisme $\rho\colon A \to Q$ étant universel parmi les morphismes d'anneaux $f\colon A \to B$ tels que $f(I) = \{0\}$. Plus précisément :

Définition 1.4.3. Soit A un anneau et $I \subseteq A$ un idéal. Un morphisme d'anneaux $\rho\colon A \to Q$ est *un quotient de A par I* si $\rho(I) = \{0\}$ et pour tout anneau B et tout morphisme d'anneaux $f\colon A \to B$ avec $f(I) = \{0\}$, il existe un et un seul morphisme d'anneaux $\overline{f}\colon Q \to B$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} A & \xrightarrow{\rho} & Q \\ & \searrow^{f} & \downarrow{\scriptstyle \overline{f}} \\ & & B \end{array}$$

Proposition 1.4.4. *Soit A un anneau et $I \subseteq A$ un idéal. Soit $\pi\colon A \to A/I$ le passage au quotient. Lorsque $\rho\colon A \to Q$ est un quotient de A par I, il existe un isomorphisme $f\colon A/I \to Q$ tel que $f \circ \pi = \rho$. En particulier, A/I et Q sont isomorphes.*

Démonstration. Il existe un morphisme d'anneaux $f\colon A/I \to Q$ tel que $f \circ \pi = \rho$, d'après la propriété universelle de π. De même, il existe un morphisme d'anneaux $g\colon Q \to A/I$ tel que $g \circ \rho = \pi$, d'après la propriété universelle de ρ. On a alors le morphisme $g \circ f$ de A/I dans lui-même satisfaisant $(g \circ f) \circ \pi = \pi$. Or, l'identité $\mathrm{id}_{A/I}$ sur A/I satisfait lui aussi $\mathrm{id}_{A/I} \circ \pi = \pi$. D'après l'unicité, $g \circ f = \mathrm{id}_{A/I}$. De même, en utilisant la propriété universelle de ρ cette fois-ci, on montre $f \circ g = \mathrm{id}_Q$, c-à-d, $f\colon A/I \to Q$ est un isomorphisme. □

Proposition 1.4.5. *Soit A un anneau, $I \subseteq A$ un idéal et $\rho\colon A \to Q$ un morphisme d'anneaux. Le morphisme ρ est un quotient de A par I si et seulement si ρ est surjectif et* $\ker(\rho) = I$.

Démonstration. Supposons que ρ est un quotient de A par I. Soit $\pi\colon A \to A/I$ le quotient de A par I. D'après Proposition 1.4.4, il existe un isomorphisme $f\colon A/I \to Q$ tel que $f \circ \pi = \rho$. On a alors $\ker(\rho) = \ker(\pi)$. Or $\ker(\pi) = I$, donc $\ker(\rho) = I$. De plus, comme f et π sont surjectifs, ρ est surjectif.

Pour montrer l'autre implication, supposons que $\ker(\rho) = I$ et que ρ est surjectif. Il faut montrer que ρ est universel. Soit $f\colon A \to B$ un morphisme d'anneaux tel que $f(I) = \{0\}$. En utilisant la surjectivité de ρ, définissons une application $\overline{f}\colon Q \to B$ par $\overline{f}(q) = f(a)$ où $a \in A$ est tel que $\rho(a) = q$. Observez que $\overline{f}(q)$ ne dépend pas du choix de $a \in A$ tel que $\rho(a) = q$. En effet, si $a' \in A$ satisfait $\rho(a') = q$ lui aussi, alors $a - a' \in \ker(\rho) = I$. D'où $f(a) - f(a') = f(a - a') = 0$. Par conséquent, on a $\overline{f} \circ \rho = f$. Comme f est un morphisme et ρ est un morphisme surjectif, $\overline{f}$ est un morphisme. Il est clair que la surjectivité de ρ implique l'unicité de $\overline{f}$. On conclut que ρ est universel. □

Exemple 1.4.6. Soit A un anneau et $a \in A$. Soit $f\colon A[X] \to A$ le morphisme d'évaluation en a, c-à-d, $f(P) = P(a)$, où

$$P(a) = a_n a^n + \cdots + a_1 a + a_0$$

lorsque $P = a_n X^n + \cdots + a_1 X + a_0$. Alors, f est un quotient de $A[X]$ par l'idéal $(X - a)$. Effectivement, f est surjectif et on a $(X - a) \subseteq \ker(f)$. Pour montrer l'inclusion $\ker(f) \subseteq (X - a)$ on utilise la division euclidienne dans $A[X]$ par un polynôme unitaire : Soit $P \in \ker(f)$. Alors, il existe $Q, R \in A[X]$ tels que $P = (X - a)Q + R$ où $\deg(R) < \deg(X - a) = 1$. D'où $R \in A$ et l'évaluation en a donne $0 = P(a) = 0 \cdot Q(a) + R(a) = R$, i.e., $R = 0$ et donc $P \in (X - a)$.

1.5 Localisation

La localisation d'un anneau A va permettre de considérer un anneau de fractions $\frac{a}{s}$ où a est un élément de A et s est un élément d'un sous-ensemble de dénominateurs S de A. Pour que l'ensemble de tels fractions soit un anneau il va falloir que S soit une partie multiplicative de A :

Définition 1.5.1. Soit A un anneau. Un sous-ensemble S de A est une *partie multiplicative* lorsque S est stable pour produits finis. Autrement dit, $1 \in S$ et $st \in S$ pour tout $s, t \in S$.

Exemple 1.5.2.

1. $\{1, 10, 10^2, \dots\} \subseteq \mathbb{Z}$ est une partie multiplicative.
2. Soit A un anneau et $R \subseteq A$ l'ensemble des éléments réguliers. Alors, R est une partie multiplicative de A.

Soit A un anneau et $S \subseteq A$ une partie multiplicative. On définira l'anneau de la localisation de A par S, noté par $S^{-1}A$.

Tout d'abord, on définit sur $A \times S$ une relation $\sim$ par

$$(a, s) \sim (b, t) \iff \exists r \in S : rat = rbs.$$

Lemme 1.5.3. *La relation $\sim$ sur l'ensemble $A \times S$ est une relation d'équivalence.*

Démonstration. La reflexivité et le symétrie de $\sim$ sont évidents. Pour la transitivité supposons que $(a,s) \sim (b,t)$ et $(b,t) \sim (c,r)$. Alors il existe $u, v \in S$ tels que $uat = ubs$ et $vbr = vct$. Multiplier la première équation par vr et la deuxième par us et on obtient :

$$uvtra = uvrbs = uvtcs.$$

Comme $uvt \in S$ on a $(a,s) \sim (c,r)$. □

Soit $S^{-1}A$ alors le quotient de $A \times S$ par la relation d'équivalence $\sim$. La classe d'équivalence d'un élément (a,s) de $A \times S$ sera notée par $\frac{a}{s}$. Observons que l'on a $\frac{at}{st} = \frac{a}{s}$ dans $S^{-1}A$ pour $t \in S$.

Ensuite on définira deux lois internes binaires $+$ et $\cdot$ sur $S^{-1}A$. On se laisse guider par la somme et le produit de deux fractions rationelles. Soient

$$\alpha, \mu \colon (A \times S) \times (A \times S) \to S^{-1}A$$

les applications définies par

$$\alpha((a,s),(b,t)) = \frac{at+bs}{st} \quad \text{et} \quad \mu((a,s),(b,t)) = \frac{ab}{st}.$$

C'est un exercice de montrer que $\alpha((a,s),(b,t))$ et $\mu((a,s),(b,t))$ ne dépendent que des classes d'équivalence de (a,s) et (b,t). Les applications α et μ induisent alors les lois internes attendues sur $S^{-1}A$:

$$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st} \quad \text{et} \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

On vérifie sans peine que $S^{-1}A$ est un anneau. On a dans $S^{-1}A$

$$0 = \frac{0}{1}, \quad 1 = \frac{1}{1}, \quad \text{et} \quad -\frac{a}{s} = \frac{-a}{s}.$$

De plus, on a une application

$$\iota \colon A \to S^{-1}A$$

définie par $\iota(a) = \frac{a}{1}$. Il est clair que ι est un morphisme d'anneaux.

Définition 1.5.4. Soient A un ensemble et $S \subseteq A$ une partie multiplicative. La *localisation* de A par S est l'anneau $S^{-1}A$ muni du morphisme $\iota \colon A \to S^{-1}A$. Parfois on appelle $S^{-1}A$ lui-même la localisation de A par S.

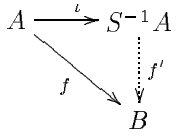
Exemple 1.5.5.

1. Soit S le sous-ensemble de $\mathbb{Z}$ des entiers non nuls. Alors, $\frac{n}{s} = \frac{m}{t}$ dans $S^{-1}\mathbb{Z}$ si et seulement si $nt = ms$. Par conséquent, $S^{-1}\mathbb{Z}$ *est* l'anneau $\mathbb{Q}$, et le morphisme $\iota \colon \mathbb{Z} \to S^{-1}\mathbb{Z}$ est l'inclusion de $\mathbb{Z}$ dans $\mathbb{Q}$.
2. Soit $S = \{1, 10, 10^2, 10^3, \dots\} \subseteq \mathbb{Z}$. Alors, la localisation $S^{-1}\mathbb{Z}$ de $\mathbb{Z}$ par S est isomorphe à l'anneau de décimaux $\mathbb{D}$.

Soit $S \subseteq A$ une partie multiplicative et $\iota \colon A \to S^{-1}A$ le morphisme de localisation. Evidemment, les images d'éléments de S dans $S^{-1}A$ sont inversibles. En fait, l'anneau $S^{-1}A$, ou plus précisément, le morphisme de localisation $\iota \colon A \to S^{-1}A$, est universel :

Propriété universelle de la localisation. *Soit A un anneau et $S \subseteq A$ une partie multiplicative. Soit $\iota \colon A \to S^{-1}A$ le morphisme de localisation. Alors,*

$\iota(s)$ est inversible dans $S^{-1}A$ quel que soit $s \in S$ et ι est universel ayant cette propriété, c-à-d, pour tout anneau B et pour tout morphisme d'anneaux $f : A \to B$ avec $f(s)$ inversible quel que soit $s \in S$, il existe un et un seul morphisme d'anneaux $f' : S^{-1}A \to B$ rendant commutatif le diagramme suivant :

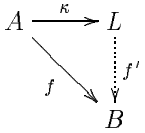


Démonstration. Soit $g : A \times S \to B$ définie par $g(a,s) = f(s)^{-1}f(a)$. Lorsque $(a,s) \sim (b,t)$ dans $A \times S$, il existe $u \in S$ tel que $uat = ubs$. On a alors $f(u)f(a)f(t) = f(u)f(b)f(s)$ dans B. Comme $f(u)$, $f(t)$ et $f(s)$ sont inversibles dans B, on a $g(a,s) = f(s)^{-1}f(a) = f(t)^{-1}f(b) = g(b,t)$. Cela montre que g induit une application f' de $S^{-1}A$ dans B. On a alors $f'(\frac{a}{s}) = f(s)^{-1}f(a)$. Il s'ensuit que f' est un morphisme d'anneaux. De plus, on a $f' \circ \iota = f$. Cela montre l'existence de f'.

Pour montrer l'unicité de f', supposons que f'' est aussi un morphisme de $S^{-1}A$ dans B tel que $f'' \circ \iota = f$. En particulier, on a $f''(\frac{s}{1}) = f(s) = f'(\frac{s}{1})$ pour tout $s \in S$. Comme $\frac{s}{1}$ est inversible dans $S^{-1}A$ et son inverse est $\frac{1}{s}$, $f''(\frac{1}{s}) = f'(\frac{1}{s})$. D'où $f''(\frac{a}{s}) = f''(\frac{a}{1})f''(\frac{1}{s}) = f'(\frac{a}{1})f'(\frac{1}{s}) = f'(\frac{a}{s})$ pour tout $\frac{a}{s} \in S^{-1}A$. □

Comme pour les anneaux quotients, on ne veut pas favoriser la construction de la localisation $S^{-1}A$ de A :

Définition 1.5.6. Soit A un anneau et $S \subseteq A$ une partie multipicative. Soit $\kappa : A \to L$ un morphisme d'anneaux tel que $\kappa(s)$ soit inversible quel que soit $s \in S$. On appelle κ une *localisation de A par S* lorsque pour tout anneau B et pour tout morphisme $f : A \to B$ avec $f(s)$ inversible quel que soit $s \in S$, il existe un et un seul morphisme d'anneaux $f' : L \to B$ tel que le diagramme suivant commute :



Comme pour les quotients, lorsque L est une localisation de A par S, L est isomorphe à $S^{-1}A$.

Grace à la localisation, on peut généraliser la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$:

Définition 1.5.7. Soit A un anneau. Soit R la partie multiplicative des éléments réguliers A (Exercice 7). *L'anneau total de fractions* de A est l'anneau $R^{-1}A$, noté par $\mathrm{Frac}(A)$. Si A est intègre, $\mathrm{Frac}(A)$ est un corps, appelé le *corps de fractions* de A.

Exemple 1.5.8.
1. $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$.
2. Soit K un corps. Le corps de fractions de $K[X]$ est le corps des polynômes rationnels, noté par $K(X)$, i.e.,

$$K(X) = \{\frac{P}{Q} \mid P, Q \in K[X], Q \neq 0\}.$$

Au lieu de localiser par la partie multiplicative de tous les éléments réguliers on peut également localiser par une partie multiplicative engendré par un seul élément, qu'il soit régulier ou non :

Définition 1.5.9. Soient A un anneau et s un élément de A. Soit S la plus petite partie multiplicative de A contenant s, i.e., $S = \{1, s, s^2, s^3, \dots\}$. On notera A_s au lieu de $S^{-1}A$. La *localisation* de A par s est l'anneau A_s, ou plus précisément, l'anneau A_s muni du morphisme $\iota\colon A \to A_s$, défini par $\iota(a) = \frac{a}{1}$.

Exemple 1.5.10. Voir Exemple 1.5.5.2

Soit $S \subseteq A$ une partie multiplicative et $I \subseteq A$ un idéal de A. L'idéal de $S^{-1}A$ engendré par l'image de I dans $S^{-1}A$ est noté par $S^{-1}I$. On a

$$S^{-1}I = \{\frac{x}{s} \mid x \in I, s \in S\}.$$

Bien que I ne soit pas un sous-ensemble de $S^{-1}A$, on note l'idéal $S^{-1}I$ de $S^{-1}A$ engendré par $\iota(I)$ aussi par $(S^{-1}A)I$ ou bien par $I(S^{-1}A)$.

Proposition 1.5.11. *Soit $S \subseteq A$ une partie multiplicative et $I \subseteq A$ un idéal de A. Soit $\overline{S}$ l'image de S dans le quotient A/I. Alors, $\overline{S}$ est une partie multiplicative et on a un isomorphisme*

$$\overline{S}^{-1}(A/I) \cong (S^{-1}A)/(S^{-1}I).$$

Démonstration. Il est clair que l'image $\overline{S}$ de S par le morphisme de passage au quotient $\pi\colon A \to A/I$ est une partie multiplicative de A/I (voir Exercice 106). Pour montrer l'isomorphisme en question on va utiliser la propriété universelle du quotient : on construit un morphisme

$$\rho\colon S^{-1}A \longrightarrow \overline{S}^{-1}(A/I)$$

et on montre qu'il est surjectif et que son noyau est égal à $S^{-1}I$. D'après Proposition 1.4.5, ρ est un quotient de $S^{-1}A$ par $S^{-1}I$. On en déduit l'isomorphisme en question.

Soit ι le morphisme de localisation de A par S et $\overline{\iota}$ celui de A/I par $\overline{S}$. Le morphisme de passage au quotient $\pi\colon A \to A/I$ envoie S dans $\overline{S}$. Le morphisme composé $\overline{\iota} \circ \pi$ a donc la propriété que $\overline{\iota} \circ \pi(s)$ est inversible quel que soit $s \in S$. D'après la propriété universelle de ι, il existe un morphisme ρ de $S^{-1}A$ dans $\overline{S}^{-1}(A/I)$ tel que le diagramme

$$\begin{array}{ccc} A & \xrightarrow{\pi} & A/I \\ {\scriptstyle\iota}\downarrow & & \downarrow{\scriptstyle\overline{\iota}} \\ S^{-1}A & \overset{\rho}{\dashrightarrow} & \overline{S}^{-1}(A/I) \end{array}$$

commute. En fait, on a $\rho(\frac{a}{s}) = \frac{\pi(a)}{\pi(s)}$ pour tout $\frac{a}{s} \in S^{-1}A$. De ce fait, ρ est surjectif. Effectivement, chaque élément de $\overline{S}^{-1}(A/I)$ est de la forme $\frac{\pi(a)}{\pi(s)}$, et est donc dans l'image de ρ.

De plus, le noyau de ρ est égal à $S^{-1}I$. En effet, il est clair de la description de $S^{-1}I$ comme $\{\frac{x}{s} \mid x \in I, s \in S\}$ que $S^{-1}I$ est contenu dans $\ker(\rho)$. Pour montrer

l'autre inclusion, soit $\frac{a}{s} \in \ker(\rho)$. Alors, $\frac{\pi(a)}{\pi(s)} = 0$ dans $\overline{S}^{-1}(A/I)$. Comme $\overline{S}$ est l'image de S, il existe $t \in S$ tel que $\pi(t)\pi(a) = 0$ dans A/I. Donc $ta \in I$, et alors $\frac{ta}{s} \in S^{-1}I$. Comme $t \in S$, $\frac{a}{s} = \frac{1}{t} \cdot \frac{ta}{s} \in S^{-1}I$. □

1.6 Idéaux premiers et maximaux

Définition 1.6.1. Soit I un idéal de l'anneau A. L'idéal I est *premier* lorsque l'anneau quotient A/I est intègre. L'ensemble des idéaux premiers de A est le *spectre* de A, noté par $\mathrm{Spec}(A)$.

Exemple 1.6.2.

1. Les idéaux $n\mathbb{Z}$ de $\mathbb{Z}$ sont premiers lorsque n est nul ou premiers.
2. Les idéaux $(P) \subseteq K[X]$, K un corps, sont premiers lorsque P est nul ou irréductible.
3. Soient $k, n \in \mathbb{N}$, $k \leq n$, et soit K un corps. L'idéal $(X_1, \ldots, X_k)$ dans $K[X_1, \ldots, X_n]$ est premier, car le quotient $K[X_1, \ldots, X_n]/(X_1, \ldots, X_k)$ est isomorphe à l'anneau intègre $K[X_{k+1}, \ldots, X_n]$.

Voici une caractérisation d'idéaux premiers :

Proposition 1.6.3. *Soit I un idéal de l'anneau A. Les conditions suivantes sont équivalentes :*

1. *I est premier ;*
2. *$I \neq A$ et $ab \in I$ implique que $a \in I$ ou $b \in I$, quels que soient $a, b \in A$;*
3. *$A \backslash I$ est une partie multiplicative de A.*

Démonstration. $1 \Rightarrow 2$: Soit I premier et soient $a, b \in A$ tels que $ab \in I$. Alors, leurs classes $\overline{a}$ et $\overline{b}$ modulo I satisfont $\overline{a} \cdot \overline{b} = \overline{ab} = 0$ dans A/I. Comme I est premier, A/I est intègre. En particulier, $\overline{a} = 0$ ou $\overline{b} = 0$ dans A/I, c-à-d, $a \in I$ ou $b \in I$.

$2 \Rightarrow 3$: Supposons $I \neq A$ et $a \in I$ ou $b \in I$ lorsque $ab \in I$. Comme $I \neq A$, $1 \notin I$. De plus, si $s, t \notin I$, alors $st \notin I$ car sinon, on aura $s \in I$ ou $t \in I$.

$3 \Rightarrow 1$: Supposons $A \backslash I$ est une partie multiplicative. Comme $1 \notin I$, $I \neq A$ et alors l'anneau A/I est non nul. Soient $x, y \in A/I$ tels que $xy = 0$. Il existe $a, b \in A$ tels que $\overline{a} = x$ et $\overline{b} = y$. Alors, $\overline{ab} = \overline{a} \cdot \overline{b} = 0$. D'où, $ab \in I$. Or $A \backslash I$ est multiplicative, donc on ne peut avoir $a \notin I$ et $b \notin I$. Par conséquent, $a \in I$ ou $b \in I$, c-à-d, $x = 0$ ou $y = 0$. □

Définition 1.6.4. L'idéal I est *maximal* lorsque l'anneau quotient est un corps. L'ensemble des idéaux maximaux de A est le *spectre maximal* de A, noté par $\mathrm{Max}(A)$.

Exemple 1.6.5.

1. Les idéaux $n\mathbb{Z}$ de $\mathbb{Z}$ sont maximaux lorsque n est premier.
2. Les idéaux $(P) \subseteq K[X]$, K un corps, sont maximaux lorsque P est irréductible.

3. Soient $k, n \in \mathbb{N}$, $k \leq n$, et soit K un corps. L'idéal $(X_1, \ldots, X_k)$ dans $K[X_1, \ldots, X_n]$ est maximal si et seulement si $k = n$.

Evidemment, un idéal maximal est premier. La terminologie «idéal maximal» est justifiée car un idéal est maximal si et seulement s'il est maximal parmi les idéaux différents de A :

Proposition 1.6.6. *Soit A un anneau et $I \subseteq A$ un idéal. Les conditions suivantes sont équivalentes :*

1. *I est maximal ;*
2. *$I \neq A$ et pour tout $a \notin I$ il existe $b \in A$ tel que $ab - 1 \in I$;*
3. *$I \neq A$ et pour tout idéal J de A avec $I \subseteq J \neq A$ on a $J = I$.*

Démonstration. $1 \Rightarrow 2$: Soit I maximal. Comme A/I est un corps, $A/I \neq 0$, i.e., $I \neq A$. De plus, lorsque $a \notin I$, on a $\overline{a} \neq 0$ dans le corps A/I. D'où l'existence de $y \in A/I$ tel que $\overline{a} \cdot y = 1$. Il existe $b \in A$ tel que $\overline{b} = y$. Alors, $\overline{ab} = \overline{a} \cdot \overline{b} = 1$, c-à-d, $ab - 1 \in I$.

$2 \Rightarrow 3$: Supposons que $I \neq A$ et que pour $a \notin I$ il existe $b \in A$ tel que $ab - 1 \in I$. Soit $J \subseteq A$ un idéal contenant I et différent de A. S'il existe $a \in J \backslash I$, il existe en particulier $b \in A$ tel que $ab - 1 \in I$ car $a \notin I$. Comme $a \in J$, on aurait $ab \in J$ et $ab - 1 \in J$. D'où $1 = ab - (ab - 1) \in J$ et alors $J = A$. Contradiction, c-à-d, $I = J$.

$3 \Rightarrow 1$: Supposons que $I \neq A$ et que I est maximal parmi les idéaux différent de A. Cela veut dire qu'il n'y a que deux idéaux de A contenant I, à savoir I et A. D'après Exercice 68, l'ensemble des idéaux de A/I correspond bijectivement à l'ensemble des idéaux de A contenant I. Par conséquent, l'anneau A/I a exactement deux idéaux, il est donc un corps. □

Pour montrer l'existence d'idéaux maximaux, et donc aussi d'idéaux premiers, dans un anneau quelconque on va utiliser le Lemme de Zorn, que l'on rappelle : Soit $(E, \leq)$ un ensemble partiellement ordonné. Un élément x de E est *maximal* si $y \in E$ evec $x \leq y$ implique $x = y$. Un *majorant* d'un sous-ensemble F de E est un élément $x \in E$ tel que $y \leq x$ pour tout $y \in F$. Une *chaîne* dans E est un sous-ensemble totalement ordonné de E.

Lemme de Zorn. *Soit $(E, \leq)$ un ensemble partiellement ordonné. Si chaque chaîne de E a un majorant, alors E a un élément maximal.* □

Proposition 1.6.7. *Soit A un anneau et $I \subseteq A$ un idéal différent de A. Alors il existe un idéal maximal m de A contenant I.*

Démonstration. Soit $\mathcal{I}$ l'ensemble des idéaux de A contenant I et différent de A. Alors, $\mathcal{I}$ est partiellement ordonné par l'inclusion. Montrons que chaque chaîne de $\mathcal{I}$ admet un majorant.

Soit $\mathcal{C} \subseteq \mathcal{I}$ une chaîne de $\mathcal{I}$. Si $\mathcal{C}$ est vide, I est un majorant de $\mathcal{C}$. On peut donc supposer $\mathcal{C}$ non vide. La réunion

$$\bigcup \mathcal{C} = \{x \in A \mid \exists J \in \mathcal{C} : x \in J\}$$

est alors un idéal de A différent de A, donc appartenant à $\mathcal{I}$. Visiblement, $\bigcup \mathcal{C}$ est un majorant de $\mathcal{C}$.

D'après le Lemme de Zorn, il existe un élément maximal m dans $\mathcal{I}$. D'après Proposition 1.6.6, m est un idéal maximal de A. De plus m contient I car $m \in \mathcal{I}$. □

Corollaire 1.6.8. *Soit $a \in A$. Si $a \notin m$ pour tout idéal maximal m de A, alors a est inversible dans A.*

Démonstration. Soit $I = Aa$ l'idéal de A engendré par a. Comme a n'appartient à aucun idéal maximal de A, $I = A$ d'après Proposition 1.6.7. Cela implique que $1 \in I = Aa$, i.e., il existe $b \in A$ tel que $ab = 1$. □

Corollaire 1.6.9. *Chaque anneau A est la réunion disjointe de son groupe multiplicatif $A^\star$, d'une part, et l'union de tous ses idéaux maximaux, d'autre part, i.e.,*

$$A = A^\star \cup \bigcup_{m \in \mathrm{Max}(A)} m \quad et \quad A^\star \cap (\bigcup_{m \in \mathrm{Max}(A)} m) = \emptyset. \quad \square$$

Corollaire 1.6.10. *Soit A un anneau non nul. Alors il existe un idéal maximal m de A.*

Démonstration. Appliquer Proposition 1.6.7 à l'anneau A et à l'idéal $I = \{0\}$. □

Définition 1.6.11. Un anneau A est un *anneau local* si A n'a qu'un idéal maximal m. Le corps A/m est le *corps résiduel* de A, noté par $k(A)$.

Proposition 1.6.12. *Un anneau A est local si et seulement si A a un idéal I tel que $A\backslash I = A^\star$. Dans ce cas, I est l'unique idéal maximal de A.*

Démonstration. Lorsque A est local, soit I son unique idéal maximal. Evidemment, $A\backslash I \supseteq A^\star$. Pour montrer l'autre inclusion, soit $a \in A\backslash I$. Comme I est l'unique idéal maximal, a n'appartient à aucun idéal maximal. D'après Corollaire 1.6.8, a est inversible, ce qui montre l'inclusion $A\backslash I \subseteq A^\star$. D'où $A\backslash I = A^\star$.

Supposons que $I \subseteq A$ est un idéal de A tel que $A\backslash I = A^\star$. Montrons d'abord que I est maximal. Comme $1 \in A^\star$, $1 \notin I$ et donc $I \neq A$. De plus, lorsque $a \notin I$, a est inversible dans A, c-à-d, il existe $b \in A$ tel que $ab = 1$. En particulier, $ab - 1 \in I$. D'après Proposition 1.6.6, I est maximal. Montrons que I est l'unique idéal maximal. Soit $m \subseteq A$ un idéal maximal de A. On a alors $m \subseteq I$ car sinon, il existe $a \in m\backslash I$. Comme $a \notin I$, a serait inversible et donc m serait égal à A. D'où $m \subseteq I$. Mais m est maximal et $I \neq A$, donc $m = I$. □

L'exemple typique d'un anneau local est le suivant : Soit A un anneau et $p \subseteq A$ un idéal premier. D'après Proposition 1.6.3, le sous-ensemble $A\backslash p$ de A est une partie multiplicative de A.

Définition 1.6.13. La localisation de A par $A\backslash p$ est la *localisation de A en p*, notée par A_p.

Proposition 1.6.14. *Soit p un idéal premier de A. Alors, la localisation A_p de A en p est un anneau local. Son idéal maximal est l'idéal pA_p engendré par p. Le corps résiduel $k(A_p)$ de A_p est isomorphe au corps de fractions du quotient A/p.*

Démonstration. D'abord, l'idéal pA_p n'est pas égal à A. En effet, si 1 appartenait à pA_p, il existerait $x \in p$ et $s, t \notin p$ tel que $ts = tx$. Or $tx \in p$, d'où $ts \in p$. Comme p est premier, on a $s \in p$ ou bien $t \in p$. Contradiction. D'où $I \neq A$, et donc $A_p \backslash pA_p \supseteq A_p^\star$.

Ensuite, on montre que chaque élément de $A_p \backslash pA_p$ est inversible dans A_p. Soit $\frac{a}{s} \in A_p \backslash pA_p$. Comme $\frac{a}{s} \notin pA_p$, on a nécessairement $a \notin p$. D'où $\frac{s}{a} \in A_p$, et bien-sûr $\frac{a}{s}\frac{s}{a} = 1$. Par conséquent $\frac{a}{s}$ est inversible. Cela montre que $A_p \backslash pA_p \subseteq A_p^\star$.

D'après Proposition 1.6.12, A_p est un anneau local et son idéal maximal est pA_p.

Pour montrer l'assertion sur le corps résiduel de A_p, soit S la partie multiplicative $A \backslash p$ de A. Soit $\overline{S}$ l'image de S dans le quotient A/p. En fait, $\overline{S} = (A/p) \backslash \{0\}$. D'après Proposition 1.5.11, on a que

$$k(A_p) = A_p/pA_p = (S^{-1}A)/(S^{-1}p) \cong \overline{S}^{-1}(A/p) = \mathrm{Frac}(A/p),$$

ce qui montre la proposition. □

1.7 Idéaux radicaux

Définition 1.7.1. Soit A un anneau. Un élément a de A est *nilpotent* s'il existe un entier positif n tel que $a^n = 0$. L'anneau A est *réduit* si 0 est le seul nilpotent dans A.

Exemple 1.7.2.

1. Tout anneau intègre est réduit.
2. $\mathbb{Z}/n\mathbb{Z}$ et réduit lorsque n est un produit de premiers différents.
3. Soit K un corps et n un entier, $n > 1$. Soit A le quotient $K[X]/(X^n)$. On a $X \neq 0$ dans A tandis que $X^n = 0$ dans A. Alors, l'anneau A n'est par réduit.

On vérifie facilement que l'ensemble des nilpotents dans un anneau A est un idéal. En effet, 0 est nilpotent. Lorsque x et y sont nilpotents, disons $x^n = y^m = 0$, alors

$$(x+y)^{n+m} = \sum_{\substack{i+j=n+m \\ i\geq 0, j\geq 0}} \frac{(n+m)!}{i! \cdot j!}\, x^i y^j = 0$$

car soit $i \geq n$, soit $j \geq m$ pour chaque terme de cette somme. Finalement, si x est nilpotent, disons $x^n = 0$, alors $(ax)^n = a^n x^n = 0$ pour $a \in A$. Par conséquent, l'ensemble des éléments nilpotents est bien un idéal.

Définition 1.7.3. Soit A un anneau. L'idéal des nilpotents de A est le *nilradical* de A, noté par $\mathrm{Nil}(A)$.

Exemple 1.7.4.

1. Soit $n \in \mathbb{N}$ non nul. Soit $n = \prod p_i^{e_i}$ sa décomposition en facteurs premiers, i.e., $e_i > 0$ et $p_i \neq p_j$ lorsque $i \neq j$. Le nilradical $\mathrm{Nil}(\mathbb{Z}/n\mathbb{Z})$ de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est l'idéal engendré par $m = \prod p_i$.
2. Soit A l'anneau $K[X]/(X^n)$. Le nilradical de A est l'idéal de A engendré par X, i.e., $\mathrm{Nil}(A) = AX$. Effectivement, X est nilpotent dans A, d'où l'inclusion $\mathrm{Nil}(A) \supseteq AX$. Pour montrer l'autre inclusion, soit $P \in A$

nilpotent. Considérer son image par le passage au quotient $A \to A/AX$. Evidemment, l'image de P est nilpotent dans A/AX. Comme A/AX est isomorphe à K, A/AX est un corps. Le seul élément nilpotent d'un corps étant 0, l'image de P dans A/AX est nul, i.e., $P \in AX$.

Proposition 1.7.5. *Soit A un anneau. Alors,* $\mathrm{Nil}(A/\mathrm{Nil}(A)) = 0$, *c-à-d, le seul élément nilpotent du quotient* $A/\mathrm{Nil}(A)$ *est* 0.

Démonstration. Soit $a \in A$ tel que a soit nilpotent dans $A/\mathrm{Nil}(A)$. Alors il existe un entier positif n tel que $a^n \in \mathrm{Nil}(A)$. Or, $a^n \in \mathrm{Nil}(A)$ veut dire qu'il existe un entier positif m tel que $0 = (a^n)^m = a^{nm}$. D'où $a \in \mathrm{Nil}(A)$, c-à-d, $a = 0$ dans le quotient $A/\mathrm{Nil}(A)$. □

D'après la proposition précédente, le quotient $A/\mathrm{Nil}(A)$ est un anneau réduit.

Définition 1.7.6. Soit A un anneau. Le quotient $A/\mathrm{Nil}(A)$ est *l'anneau réduit associé à* A, noté par A_{red}.

Exemple 1.7.7. (notation comme dans Exemple 1.7.4)

1. L'anneau réduit associé à $\mathbb{Z}/n\mathbb{Z}$ est l'anneau $\mathbb{Z}/m\mathbb{Z}$.

2. L'anneau réduit associé à $K[X]/(X^n)$ est le corps K.

Rappelons que le nilradical $\mathrm{Nil}(A)$ est l'ensemble de $a \in A$ tel qu'il existe $n \in \mathbb{N}$ avec $a^n = 0$. Plus généralement définit-on pour un idéal I de A le radical de I par

$$\mathrm{Rad}(I) = \{a \in A \mid \exists n \in \mathbb{N} : a^n \in I\}.$$

Evidemment, on a $\mathrm{Rad}((0)) = \mathrm{Nil}(A)$.

Il s'ensuit de la définition du radical d'un idéal que ce radical est un idéal. En effet, $\mathrm{Rad}(I)$ est égal à l'image réciproque du nilradical du quotient A/I par le morphisme de passage au quotient. Par conséquent, $\mathrm{Rad}(I)$ est un idéal de A.

Définition 1.7.8. Soit I un idéal de A. Le *radical* de I est l'idéal $\mathrm{Rad}(I)$. L'idéal I est un *idéal radical* si $I = \mathrm{Rad}(I)$.

Exemple 1.7.9. (notation comme dans Exemple 1.7.4)

1. Le radical de l'idéal $n\mathbb{Z}$ de $\mathbb{Z}$ est l'idéal $m\mathbb{Z}$.

2. Le radical de l'idéal (X^n) de $K[X]$ est l'idéal (X).

3. Tout idéal premier est un idéal radical. Plus généralement, l'intersection d'un ensemble d'idéaux premiers est un idéal radical.

Proposition 1.7.10. *Soit I un idéal de A. Alors, le radical* $\mathrm{Rad}(I)$ *de I est égal à l'intersection de tous les idéaux premiers de A contenant I, i.e.,*

$$\mathrm{Rad}(I) = \bigcap_{\substack{P \supseteq I \\ P \in \mathrm{Spec}(A)}} P.$$

Démonstration. L'inclusion $\subseteq$ est évidente : Si x appartient à $\mathrm{Rad}(I)$ et P est un idéal premier de A contenant I, $x^n \in I \subseteq P$ implique $x \in P$ car P est premier.

Pour montrer l'inclusion $\supseteq$ on montre que $x \notin \mathrm{Rad}(I)$ implique qu'il existe un idéal premier P de A contenant I tel que $x \notin P$. En effet, soit $S = \{1, x, x^2, \dots\}$ la partie multiplicative engendrée par x. Comme $x \notin \mathrm{Rad}(I)$, $S \cap \mathrm{Rad}(I) = \emptyset$. D'après Exercice 124, il existe un idéal premier P de A contenant I tel que $S \cap P = \emptyset$. En particulier, $x \notin P$. □

Corollaire 1.7.11. *Soit A un anneau et $a \in A$. Alors, l'ensemble des nilpotents de A est égal à l'intersection de tous les idéaux premiers de A, i.e.,*

$$\mathrm{Nil}(A) = \bigcap_{P \in \mathrm{Spec}(A)} P. \quad \square$$

Définition 1.7.12. Soit I un idéal de A. Un idéal J de A est un *diviseur* de I lorsque J contient I, i.e., lorsque $I \subseteq J$. L'idéal J de A est un *diviseur premier* de I lorsque J est premier et J est un diviseur de I. L'idéal J de A est un *diviseur premier minimal* de I lorsque J est un diviseur premier de I et J est minimal parmi les diviseurs premiers de I, i.e., pour tout idéal premier P de A avec $I \subseteq P \subseteq J$, on a $P = J$. Un diviseur premier minimal de l'idéal (0) de A est un *idéal premier minimal* de A.

Exemple 1.7.13. Soient $m, n \in \mathbb{Z}$. L'idéal $m\mathbb{Z}$ de $\mathbb{Z}$ est un diviseur de l'idéal $n\mathbb{Z}$ si et seulement si m est un diviseur de n. Lorsque n est non nul, l'idéal $m\mathbb{Z}$ est un diviseur premier de $n\mathbb{Z}$ si et seulement si m est un premier divisant n. Les diviseurs premiers de $n\mathbb{Z}$ sont tous minimaux.

Lemme 1.7.14. *Soit I un idéal de A. Si P est un diviseur premier de I, il existe un diviseur premier minimal P' de I contenu dans P.*

Démonstration. Soit $\mathcal{P}$ l'ensemble des idéaux premiers contenant I et contenus dans P. Alors, $\mathcal{P}$ est partiellement ordonné par la relation $\supseteq$. De plus, chaque chaîne $\mathcal{C}$ dans $\mathcal{P}$ admet un majorant. En effet, si $\mathcal{C}$ est vide, P est un majorant de $\mathcal{C}$. Si $\mathcal{C}$ est non vide, soit $Q = \bigcap \mathcal{P}$. Evidemment, Q est un idéal de A. Montrons que Q est un idéal premier de A. Soit $a, b \in A$ tels que $ab \in Q$. Supposons $a \notin Q$ et $b \notin Q$. Alors il existe $P' \in \mathcal{P}$ tel que $a \notin P'$ et $b \notin P'$. Or P' est premier, donc $ab \notin P'$. Comme $Q \subseteq P'$, on a $ab \notin Q$. Contradiction. Par conséquent, Q est premier. Visiblement Q contient I et est contenu dans P si bien que $Q \in \mathcal{P}$. De plus, Q est un majorant de $\mathcal{C}$ car on a $P' \supseteq Q$ pour tout $P' \in \mathcal{C}$. D'après le Lemme de Zorn, $\mathcal{P}$ a un élément maximal P' pour l'ordre $\supseteq$, c-à-d, P' est un diviseur premier minimal de I. □

Corollaire 1.7.15. *Soit I un idéal de A. Alors*

$$\mathrm{Rad}(I) = \bigcap_{\substack{P \text{ div. premier} \\ \text{min. de } I}} P.$$

En particulier, un idéal radical est égal à l'intersection de ses diviseurs premiers minimaux. □

Proposition 1.7.16. *Soient I_1 et I_2 deux idéaux de A. Un idéal premier P de A est un diviseur du produit I_1I_2 si et seulement s'il en est un de I_1 ou de I_2. En particulier, un idéal premier P de A est un diviseur premier minimal du produit I_1I_2 si et seulement s'il en est un de I_1 ou de I_2.*

Démonstration. Evidemment, $P \supseteq I_1I_2$ lorsque $P \supseteq I_1$ ou $P \supseteq I_2$. Réciproquement, soit $P \supseteq I_1I_2$. Supposons $P \not\supseteq I_1$. Montrons que $P \supseteq I_2$. Soit $x_2 \in I_2$. Comme $P \not\supseteq I_1$, il existe $x_1 \in I_1 \backslash P$. On a alors $x_1x_2 \in I_1I_2 \subseteq P$. comme P est premier, $x_1 \in P$ ou $x_2 \in P$. Mais $x_1 \notin P$, d'où $x_2 \in P$. Par conséquent, $P \supseteq I_2$. □

Corollaire 1.7.17. *Soient I_1 et I_2 deux idéaux de A. Alors, le produit I_1I_2 et l'intersection $I_1 \cap I_2$ ont les mêmes diviseurs premiers. En particulier, les idéaux I_1I_2 et $I_1 \cap I_2$ ont les mêmes diviseurs premiers minimaux.*

Démonstration. Comme $I_1I_2 \subseteq I_1 \cap I_2$, un diviseur premier de $I_1 \cap I_2$ est forcément un diviseur premier de I_1I_2. Réciproquement, soit P un diviseur premier de I_1I_2. D'après Proposition 1.7.16, soit P est un diviseur premier de I_1, soit il est un diviseur premier de I_2. Dans les deux cas, P est un diviseur de $I_1 \cap I_2$. □

Proposition 1.7.18. *Soit A un anneau noetherien. Soit I un idéal de A. Alors, il n'y a qu'un nombre fini de diviseurs premiers minimaux de I.*

Démonstration. Soit $\mathcal{I}$ l'ensemble des idéaux de A ne satisfaisant pas cette condition de finitude. En raisonnant par l'absurde on suppose que $\mathcal{I} \neq \emptyset$. On considère l'ordre de l'inclusion $\subseteq$ sur $\mathcal{I}$. Comme A est noetherien, chaque chaîne dans $\mathcal{I}$ est stationnaire, donc admet en particulier un majorant. D'après le Lemme de Zorn, $\mathcal{I}$ a un élément maximal I. Comme I n'est pas premier, il existe $a_1, a_2 \in A$ tels que $a_1a_2 \in I$, $a_1 \notin I$ et $a_2 \notin I$. Soit $I_1 = I + Aa_1$ et $I_2 = I + Aa_2$. Alors I_1 et I_2 sont tous les deux strictement plus grand que I. Par conséquent, I_1 et I_2 ont tous les deux un nombre fini de diviseurs premiers minimaux. On va montrer que I lui aussi a alors un nombre fini de diviseurs premiers minimaux en montrant que tout diviseur premier minimal de I est soit un diviseur premier minimal de I_1, soit un diviseur premier minimal de I_2, ce qui contredira le fait que $I \in \mathcal{I}$.

Soit alors P un diviseur premier minimal de I. Comme $I_1I_2 \subseteq I$, P est un diviseur premier du produit I_1I_2. D'après Corollaire 1.7.17, P est alors un diviseur premier de $I_1 \cap I_2$. Comme $I \subseteq I_1 \cap I_2$ et P est un diviseur premier minimal de I, il en est forcément un de $I_1 \cap I_2$. D'après Corollaire 1.7.17, P est alors un diviseur minimal de I_1I_2. D'après Proposition 1.7.16, P est soit un diviseur premier minimal de I_1, soit un diviseur premier minimal de I_2. □

Corollaire 1.7.19. *Un anneau noetherien n'a qu'un nombre fini d'idéaux premiers minimaux.* □

1.8 Anneaux factoriels

Définition 1.8.1. Soit A un anneau intègre et $a, b \in A$. On dit que a *divise* b, ou a est un *diviseur* de b s'il existe $c \in A$ tel que $ac = b$. On le note par $a|b$. Deux éléments $a, b \in A$ sont *associés* s'il existe $u \in A^\star$ tel que $a = ub$. Un élément $p \in A$, $p \neq 0$ et $p \notin A^\star$, est *premier* si $p|ab$ implique que $p|a$ ou $p|b$,

quels que soient $a, b \in A$. L'élément $p \in A$, $p \neq 0$ et $p \notin A^\star$, est *irréductible* lorsque tout diviseur de p est soit inversible, soit associé à p.

Evidemment, $p \in A$, $p \neq 0$ est premier si et seulement si l'idéal (p) engendré par p est premier.

Soit A un sous-anneau de B et soient $a, b \in A$. Evidemment, si a divise b en tant qu'éléments de A, alors a divise b en tant qu'éléments de B. Par contre, la réciproque n'est pas valable en général : 2 divise 3 dans $\mathbb{Q}$, mais 2 ne divise pas 3 dans $\mathbb{Z}$. De même, si a et b sont associés dans A, ils le sont aussi dans B. Mais la réciproque n'est pas vraie : 2 et 3 sont associés dans $\mathbb{Q}$, mais ils ne le sont pas dans $\mathbb{Z}$.

Pour les éléments premiers ou irréductibles on n'a pas d'implications dans aucun sens : $X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$, mais il ne l'est pas dans son corps de fractions $\mathbb{Q}(X)$, et, le polynôme $2X^2 - 4$ est irréductible dans $\mathbb{Q}[X]$, mais il ne l'est pas dans le sous-anneau $\mathbb{Z}[X]$ de $\mathbb{Q}[X]$.

Proposition 1.8.2. *Soit A un anneau intègre. Soient $a, b \in A$. Alors, a et b sont associés si et seulement si a et b se divisent.*

Démonstration. Lorsque a et b sont associés, il existe $u \in A^\star$ tel que $a = ub$. En particulier a divise b. Et comme $b = u^{-1}a$, b divise a.

Pour montrer l'autre implication, on peut supposer que a est non nul. Lorsque a et b se divisent, il existe $c, d \in A$ tels que $ac = b$ et $bd = a$. Alors, $acd = bd = a$. D'où $a(cd - 1) = 0$. Comme $a \neq 0$, $cd = 1$, i.e., c et inversible et a et b sont alors associés. □

Proposition 1.8.3. *Soit A un anneau intègre. Alors, tout élément premier est irréductible.*

Démonstration. Soit $p \in A$ premier. Soit a un diviseur de p. Alors, il existe $b \in A$ tel que $ab = p$. En particulier, $p|ab$. Or p est premier, donc $p|a$ ou $p|b$. Si $p|a$, p et a sont associés. Sinon, il existe $c \in A$ tel que $cp = b$. D'où $acp = ab = p$ et $ac = 1$, c-à-d, a est inversible. □

La réciproque à la proposition précédente n'est pas vraie en général :

Exemple 1.8.4. Soit A le sous-anneau $\mathbb{Z}[i\sqrt{5}]$ de $\mathbb{C}$. L'élément $2 \in A$ est irréductible. En effet, si $a + ib\sqrt{5}$, $a, b \in \mathbb{Z}$, divise 2 dans A, sa norme $a^2 + 5b^2$ divise 4 dans $\mathbb{Z}$. D'où $b = 0$ et $a = \pm 1, \pm 2$. Par conséquent, $2 \in A$ est irréductible. Cependant, 2 divise $6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ dans A, mais ne divise aucun des deux facteurs, c-à-d, $2 \in \mathbb{Z}[i\sqrt{5}]$ n'est pas premier.

Définition 1.8.5. Soit A un anneau intègre. Un *système de représentants des irréductibles* de A est un sous-ensemble $\mathcal{P}$ d'irréductibles de A tel que pour tout $p \in A$ irréductible il existe un et un seul $q \in P$ qui soit associé à p.

Exemple 1.8.6.

1. Le sous-ensemble de $\mathbb{Z}$ des premiers positifs est un système de représentants des premiers de $\mathbb{Z}$.
2. Le sous-ensemble de $K[X]$ des polynômes irréductibles unitairs en est un de $K[X]$, où K est un corps.
3. L'ensemble vide est un systéme de représentants des irréductibles d'un corps.

Définition 1.8.7. Soit A un anneau intègre. Soit $\mathcal{P}$ un systéme de représentants des irréductibles de A. On appelle A *factoriel* lorsque tout élément $a \in A$, $a \neq 0$, s'écrive de façon unique comme

$$a = u \cdot \prod_{p \in \mathcal{P}} p^{v_p},$$

où $u = u(a) \in A^\star$ et les $v_p = v_p(a) \in \mathbb{N}$ sont presque tous nuls. Lorsque A est factoriel, on appelle $v_p(a)$ la *valuation p-adique* de a, et $u(a)$ *l'inversible* de a.

Exemple 1.8.8.

1. L'anneau $\mathbb{Z}$ est factoriel (voir Corollaire 1.8.13).
2. L'anneau $K[X]$, K un corps, est factoriel (voir Corollaire 1.8.14).
3. Un corps est factoriel.

Soit A un anneau factoriel. On fixe un système $\mathcal{P}$ de représentants des irréductibles de A. Soient $a, b \in A$ non nuls. D'après la définition d'un anneau factoriel,

$$a = u(a) \cdot \prod_{p \in \mathcal{P}} p^{v_p(a)} \quad \text{et} \quad b = u(b) \cdot \prod_{p \in \mathcal{P}} p^{v_p(b)}.$$

On a que a divise b dans A si et seulement si $v_p(a) \leq v_p(b)$ quel que soit $p \in \mathcal{P}$.

Il en résulte que l'on peut définir le pgcd et le ppcm dans un anneau factoriel. Soient $a_1, \ldots, a_n \in A$ non nuls. Définissons

$$\operatorname{pgcd}(a_1, \ldots, a_n) = \prod_{p \in P} p^{\inf\{v_p(a_i) \mid i=1,\ldots,n\}}$$

et

$$\operatorname{ppcm}(a_1, \ldots, a_n) = \prod_{p \in P} p^{\max\{v_p(a_i) \mid i=1,\ldots,n\}}.$$

Observez que le pgcd et le ppcm dépendent du choix du système de représentants des irréductibles $\mathcal{P}$.

Proposition 1.8.9. *Soit A un anneau factoriel et $p \in A$. Alors, p est premier si et seulement si p est irréductible.*

Démonstration. D'après Proposition 1.8.3, p est irréductible lorsque p est premier. Supposons donc p irréductible. Soient $a, b \in A$ tels que $p|ab$. On a alors $v_p(ab) \geq 1$. Comme $v_p(ab) = v_p(a) + v_p(b)$, on a $v_p(a) \geq 1$ ou bien $v_p(b) \geq 1$, i.e., p divise a ou b. □

Proposition 1.8.10. *Soit A un anneau intègre. Alors A est factoriel si*

1. *tout élément irréductible est premier, et*
2. *toute chaîne croissante d'idéaux principaux est stationnaire.*

Démonstration. Soit $\mathcal{P}$ un système de représentants des irréductibles de A. Montrons que tout élément $a \in A$, $a \neq 0$, s'écrit comme $u \prod p^{e_p}$. Soit $S \subseteq A$ l'ensemble des élément de A ne s'écrivant pas sous cette forme-là. Supposons que S soit non vide. Considérer l'ensemble $\mathcal{I} = \{As \mid s \in S\}$ d'idéaux de A. L'ensemble $\mathcal{I}$ est ordonné par l'inclusion. D'après 2, toute chaine dans $\mathcal{I}$ a une borne supérieure. D'après le Lemme de Zorn, $\mathcal{I}$ a un élément maximal, c-à-d, il existe

$s \in S$ tel que As soit maximal dans $\mathcal{I}$. Comme s appartient à S, s n'est pas irréductible, i.e., s s'écrit comme $s_1 s_2$ où ni s_1 ni s_2 n'est inversible. On a alors $As \subsetneq As_1$ et $As \subsetneq As_2$. Par conséquent, $s_1, s_2 \notin S$, i.e.,

$$s_1 = u_1 \prod p^{e_p} \text{ et } s_2 = u_2 \prod p^{f_p},$$

et donc $s = u_1 u_2 \prod p^{e_p + f_p}$. Contradiction. Cela montre l'existence de l'écriture $a = u \prod p^{e_p}$. Pour en montrer l'unicité on utilise le fait que tout élément $p \in \mathcal{P}$ soit premier. □

Corollaire 1.8.11. *Un anneau noetherien A est factoriel lorsque tout élément irréductible de A est premier.* □

Corollaire 1.8.12. *Un anneau principal est factoriel.*

Démonstration. Soit A un anneau principal. Il suffit de montrer que tout élément irréductible de A est premier. Soit $p \in A$ alors irréductible, et soient $a, b \in A$ tels que p divise ab. Supposons que p ne divise pas a. Considérer l'idéal (a, p) de A. Comme A est principal, il existe $c \in A$ engendrant (a, p). En particulier, c divise p. Or, p est irréductible. D'où, c est soit associé à p, soit c est inversible. Dans le premier cas, p divise a ce qui contredirait le fait que p ne divise pas a. Par conséquent, c est inversible. Du coup, $(a, p) = A$, i.e., il existe $x, y \in A$ tels que $xa + yp = 1$. On a alors, $xab + ypb = b$. Comme p divise ab, p divise xab et ypb, et donc aussi leur somme qui est égale à b. □

Corollaire 1.8.13. *L'anneau des entiers $\mathbb{Z}$ est factoriel.* □

Corollaire 1.8.14. *L'anneau $K[X]$ des polynômes à coefficients dans un corps K est factoriel.* □

Le résultat principal de ce paragraphe c'est que l'anneau de polynômes $A[X]$ sur A est factoriel lorsque A l'est. Avant de montrer ce résultat, il nous faut quelques définitions.

Définition 1.8.15. Soit A un anneau factoriel. Soit $P \in A[X]$. Alors, le *contenu* de P, noté par $\mathrm{cont}(P)$, est le pgcd de tous ses coefficients.

Lemme 1.8.16. *Soit A un anneau factoriel, $a \in A$ et $P \in A[X]$. Alors, $u(a) \cdot \mathrm{cont}(aP) = a \cdot \mathrm{cont}(P)$.*

Démonstration. Soient a_i, $i = 0, \ldots, n$, les coefficients de P. Alors, $u(a) \cdot \mathrm{cont}(aP) = u(a) \cdot \mathrm{pgcd}(aa_1, \ldots, aa_n) = a \cdot \mathrm{pgcd}(a_1, \ldots, a_n) = a \cdot \mathrm{cont}(P)$. □

Lemme 1.8.16 nous permet d'étendre la définition du contenu aux polynômes à coefficients dans le corps de fractions K d'un anneau factoriel A: Soit $P \in K[X]$. Soit $a \in A$, $a \neq 0$ tel que $aP \in A[X]$. Définissons le contenue $\mathrm{cont}(P) \in K$ de P par

$$\mathrm{cont}(P) = \frac{u(a) \cdot \mathrm{cont}(aP)}{a}.$$

On vérifie facilement que cette définition ne dépend pas de a en utilisant Lemme 1.8.16.

Lemme 1.8.17. *Soit A un anneau factoriel, K son corps de fractions et $P \in K[X]$. Alors, $P \in A[X]$ si et seulement si $\mathrm{cont}(P) \in A$.*

Démonstration. Evidemment, $P \in A[X]$ implique que $\mathrm{cont}(P) \in A$. Réciproquement, supposons que $\mathrm{cont}(P) \in A$. Montrons que $P \in A[X]$. Soit $P = a_n X^n + \cdots + a_1 X + a_0$, $a_i \in K$. Soit $a \in A$ non nul tel que $aP \in A[X]$. Soit $b_i = aa_i$, $i = 0, \ldots, n$. Alors, le contenu de P est par définition $u(a)\mathrm{pgcd}(b_0, \ldots, b_n)/a$. Lorsque ce contenu appartient à A, on a que a divise $\mathrm{pgcd}(b_0, \ldots, b_n)$, donc a divise b_i, quel que soit i. Par conséquent, $a_i = b_i/a$ appartient à A, c-à-d, P est dans $A[X]$. □

Lemme de Gauss. *Soit A un anneau factoriel et K son corps de fractions. Soient $P, Q \in K[X]$. Alors,*

$$\mathrm{cont}(PQ) = \mathrm{cont}(P) \cdot \mathrm{cont}(Q).$$

Démonstration. Il suffit de montrer l'assertion pour $P, Q \in A[X]$. De plus, on peut supposer P et Q non nuls. Comme $\mathrm{cont}(P)$ divise tous les coefficients de P, il existe $P' \in A[X]$ tel que $\mathrm{cont}(P) \cdot P' = P$. De même, il existe $Q' \in A[X]$ tel que $\mathrm{cont}(Q) \cdot Q' = Q$. Evidemment, $\mathrm{cont}(P') = \mathrm{cont}(Q') = 1$. On va montrer que $\mathrm{cont}(P'Q') = 1$ également. Soit $P' = a_n X^n + \cdots + a_0$ et $Q' = b_m X^m + \cdots + b_0$. Alors $P'Q' = c_{n+m} X^{n+m} + \cdots + c_0$, où

$$c_k = \sum_{i+j=k} a_i b_j.$$

Supposons qu'il existe p premier divisant tous les coefficients c_k de $P'Q'$. Comme P' et Q' ont contenu égal à 1, il existe i_0 et j_0 tels que $p \not| a_{i_0}$ et $p \not| b_{j_0}$. De plus, on peut prendre i_0 et j_0 minimaux sous cette condition. Soit $k = i_0 + j_0$. Comme p divise a_i pour $i < i_0$ et p divise b_j pour $j < j_0$, p divise $a_i b_j$ pour $i + j = k$, $(i, j) \neq (i_0, j_0)$. Mais p divise aussi c_k, donc p divise $a_{i_0} b_{j_0}$. Or p est premier, donc p divise a_{i_0} ou p divise b_{j_0}. Contradiction. On a alors $\mathrm{cont}(P'Q') = 1$ et

$$\begin{aligned} \mathrm{cont}(PQ) &= \mathrm{cont}(\mathrm{cont}(P) \cdot P' \cdot \mathrm{cont}(Q) \cdot Q') = \\ &= \mathrm{cont}(P) \cdot \mathrm{cont}(Q) \cdot \mathrm{cont}(P'Q') = \\ &= \mathrm{cont}(P) \cdot \mathrm{cont}(Q) \end{aligned}$$

d'après Lemme 1.8.16. □

Corollaire 1.8.18. *Soit A un anneau factoriel et K son corps de fractions. Soient $P, Q \in A[X]$. Alors Q divise P dans $A[X]$ lorsque Q divise P dans $K[X]$ et $\mathrm{cont}(Q)$ divise $\mathrm{cont}(P)$ dans A.* □

Proposition 1.8.19. *Soit A un anneau factoriel et K son corps de fractions. Soit $P \in A[X]$ de degré strictement positif. Si P est irréductible dans $A[X]$ alors P est irréductible dans $K[X]$.*

Démonstration. Comme P est de degré strictment positif, P n'est ni nul ni inversible dans $K[X]$. Soit $Q \in K[X]$ un diviseur de P dans $K[X]$. On veut montrer que Q est soit inversible dans $K[X]$, soit associé à P dans $K[X]$. On peut alors supposer Q de contenu 1. En particulier, $Q \in A[X]$, d'après Lemme 1.8.17. D'après Corollaire 1.8.18, Q divise P dans $A[X]$. Or P est irréductible dans $A[X]$, donc Q est soit inversible dans $A[X]$, soit associé à P dans $A[X]$. Dans le premier cas, Q est nécessairement inversible dans $K[X]$. Dans le deuxième cas, Q est forcément associé à P dans $K[X]$. □

Théorème 1.8.20. *Soit A un anneau factoriel. Alors, l'anneau des polynômes $A[X]$ est factoriel.*

Démonstration. Soit $P \in A[X]$ irréductible. Montrons qu'il est premier. Soient $F, G \in A[X]$ tels que P divise FG. Distinguer deux cas : le cas $\deg(P) = 0$ et le cas $\deg(P) \neq 0$.

Lorsque $\deg(P) = 0$, $P \in A$, P est irréductible dans A, et P divise $\mathrm{cont}(FG) = \mathrm{cont}(F)\mathrm{cont}(G)$. Or A est factoriel, donc P est même premier dans A. Alors, P divise $\mathrm{cont}(F)$ ou bien P divise $\mathrm{cont}(G)$. En particulier, P divise F ou P divise G.

Lorsque $\deg(P) \neq 0$, P est irréductible dans $K[X]$, d'après Proposition 1.8.19. Comme $K[X]$ est factoriel, P est premier dans $K[X]$. Par conséquent, P divise F ou P divise G dans $K[X]$. Or P est irréductible dans A et $\deg(P) \neq 0$, donc le contenu de P est égal à 1. D'après Corollaire 1.8.18, P divise alors F ou P divise G dans $A[X]$.

Cela montre qu'un élément irréductible de $A[X]$ est forcément premier. Ensuite, montrons que toute chaîne croissante d'idéaux principaux de $A[X]$ est stationnaire.

Soient $P_i \in A[X]$ tels que $A[X]P_i \subseteq A[X]P_{i+1}$. On en déduit deux chaînes d'idéaux principaux croissantes : la chaîne

$$K[X]P_0 \subseteq K[X]P_1 \subseteq K[X]P_2 \subseteq \cdots$$

dans $K[X]$, et la chaîne

$$A\mathrm{cont}(P_0) \subseteq A\mathrm{cont}(P_1) \subseteq A\mathrm{cont}(P_2) \subseteq \cdots$$

dans A. Or, les anneaux A et $K[X]$ sont factoriels donc ces deux suites sont stationnaires. Par conséquent, il existe un entier $n \in \mathbb{N}$ tel que

$$K[X]P_{n+k} = K[X]P_n \quad \text{et} \quad A\mathrm{cont}(P_{n+k}) = A\mathrm{cont}(P_n)$$

quel que soit $k \in \mathbb{N}$. Montrons alors que $A[X]P_{n+k} = A[X]P_n$ quel que soit $k \in \mathbb{N}$.

Soit $Q \in A[X]$ dans $A[X]P_{n+k}$. En particulier, $Q \in K[X]P_{n+k}$ et $\mathrm{cont}(Q) \in A\mathrm{cont}(P_{n+k})$. Comme $K[X]P_{n+k} = K[X]P_n$ et $A\mathrm{cont}(P_{n+k}) = A\mathrm{cont}(P_n)$, $Q \in K[X]P_n$ et $\mathrm{cont}(Q) \in A\mathrm{cont}(P_n)$. Autrement dit, P_n divise Q dans $K[X]$ et $\mathrm{cont}(P_n)$ divise $\mathrm{cont}(Q)$ dans A. D'après Corollaire 1.8.18, P_n divise Q dans $A[X]$, i.e, $Q \in A[X]P_n$. □

Corollaire 1.8.21. *Soit A un anneau factoriel. Alors l'anneau de polynômes $A[X_1, \ldots, X_n]$ est factoriel. En particulier, $\mathbb{Z}[X_1, \ldots, X_n]$ et $K[X_1, \ldots, X_n]$, K un corps, sont factoriels.* □

1.9 Exercices

§1

1. Soit A un anneau. Montrer que

a. $0 \cdot a = a \cdot 0 = 0$ pour tout $a \in A$;

b. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ quels que soient $a, b \in A$;

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

2. Soit E un ensemble. Montrer que

a. E n'admet qu'une seule structure d'anneau lorsque E est un singleton. On a alors $E = \{0\}$. On l'appelle l'anneau nul, noté par 0 ;

b. E admet exactement 2 structures d'anneau lorsque E est un ensemble à deux éléments (prenons $E = \{e, \pi\}$ par exemple).

3. L'ensemble des entiers naturels $\mathbb{N}$, muni de l'addition $+$ et de la multiplication $\cdot$, est-il un anneau ?

4. a. Définissons sur $\mathbb{Z}$ les lois internes $\oplus, \odot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ par $m \oplus n = m + n$ et $m \odot n = -mn$. L'ensemble $\mathbb{Z}$ avec les lois internes $\oplus$ et $\odot$ est-il un anneau ?

b. Même question pour les lois $\oplus$ et $\odot$ sur $\mathbb{Z}$ définies par $m \oplus n = m + n + 1$ et $m \odot n = mn + m + n$.

c. Les lois des a et b ainsi que les lois habituelles sur $\mathbb{Z}$ nous donnent trois structures d'anneau différentes. Donner encore une autre structure d'anneau sur $\mathbb{Z}$.

5. Soient A un anneau et I et J des ensembles finis et disjoints. Soit $a : I \cup J \to A$ une application. On notera a_i au lieu de $a(i)$. Montrer que

$$\sum_{i \in I \cup J} a_i = \sum_{i \in I} a_i + \sum_{j \in J} a_j \quad \text{et que} \quad \prod_{i \in I \cup J} a_i = \prod_{i \in I} a_i \cdot \prod_{j \in J} a_j .$$

6.* Déterminer $\sum_{a \in A} a$ et $\prod_{a \in A \setminus \{0\}} a$, pour les anneaux finis $A = \mathbb{Z}/n\mathbb{Z}$, n étant un entier non nul.

7. Soit A un anneau. Montrer que l'ensemble R des éléments réguliers de A est une partie multiplicative, c-à-d, $1 \in R$, et $r, s \in R$ implique $rs \in R$.

8. a. Montrer que dans un anneau fini tous les éléments réguliers sont inversibles.

b. Montrer qu'un anneau fini intègre est un corps.

9. Montrer que $\mathbb{Z}^\star = \{-1, 1\}$.

10.* Déterminer le groupe multiplicatif de l'anneau $\mathbb{Z}/p^n\mathbb{Z}$, où p est premier et $n \in \mathbb{N}$, $n \neq 0$.

11. Soit A un anneau et $a \in A$ inversible. Montrer que $-a$ est alors inversible et $(-a)^{-1} = -a^{-1}$.

12. Soit $f\colon A \to B$ un morphisme d'anneaux. Montrer que

a. $f(0) = 0$;

b. $f(-a) = -f(a)$ quel que soit $a \in A$;

c. $f(a)$ est inversible si $a \in A$ l'est, et $f(a)^{-1} = f(a^{-1})$.

13. Soient A et B deux anneaux et $f\colon A \to B$ une application satisfaisant les conditions **M1** et **M2**.

a. Est-ce que f est nécessairement un morphisme d'anneaux?

b. Montrer que f est un morphisme d'anneaux si l'image $f(A)$ de f contient un élément régulier.

14. Montrer qu'il n'y a pas de morphismes d'anneaux

a. de $\mathbb{C}$ dans $\mathbb{R}$;

b. de $\mathbb{R}$ dans $\mathbb{Q}$;

c. de $\mathbb{Q}$ dans $\mathbb{Z}$;

d. de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}$ quel que soit $n > 0$.

15. Montrer qu'il existe un morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ si et seulement si m divise n. Montrer que s'il existe, il est unique.

16. Soit $f\colon A \to B$ un morphisme d'anneaux. Soient I un ensemble fini et $a\colon I \to A$ une application. Montrer que

$$f(\sum_{i\in I} a_i) = \sum_{i\in I} f(a_i) \quad \text{et que} \quad f(\prod_{i\in I} a_i) = \prod_{i\in I} f(a_i).$$

17. Soit $f\colon A \to B$ un morphisme d'anneaux.

a. Montrer que $f(A^\star) \subseteq B^\star$ et que la restriction $f_{|A^\star}$ de f à $A^\star$ est un morphisme de groupes de $A^\star$ dans $B^\star$. Cette restriction est notée par $f^\star$.

b. A-t-on $f^\star(A^\star) = B^\star$? Même question lorsque f est surjectif.

18. Soit A un corps et B un anneau non nul. Montrer qu'un morphisme d'anneaux $f\colon A \to B$ est nécessairement injectif.

19. Soit A un anneau. Rappelons qu'il existe un unique morphisme d'anneaux f_A de $\mathbb{Z}$ dans A d'après Proposition 1.1.12. Dans cet exercice on notera l'image $f_A(n)$ d'un entier n par n_A.

Soient A et B des anneaux. Soit $f\colon A \to B$ un morphisme d'anneaux. Montrer que $f(n_A) = n_B$ quel que soit $n \in \mathbb{Z}$.

20. (Propriété universelle de l'anneau de polynômes) Soit $f\colon A \to B$ un morphisme d'anneaux.

a. Soit b un élément de B. Montrer qu'il existe un unique morphisme d'anneaux $F\colon A[X] \to B$ tel que $F_{|A} = f$ et $F(X) = b$.

b. Soit $n \in \mathbb{N}$. Soient $b_1, \ldots, b_n \in B$. Montrer qu'il existe un unique morphisme d'anneaux $F\colon A[X_1, \ldots, X_n] \to B$ tel que $F_{|A} = f$ et $F(X_i) = b_i$ pour $i = 1, \ldots, n$.

21. a. Soit A un anneau. Montrer qu'il y a une bijection entre A et l'ensemble des morphismes d'anneaux de $\mathbb{Z}[X]$ dans A.

b. Soit A l'anneau $\mathbb{Z}[X]$. Pour un polynôme $P \in \mathbb{Z}[X]$, soit $f_P\colon \mathbb{Z}[X] \to \mathbb{Z}[X]$ le morphisme d'anneaux correspondant selon le a.

Soient $P, Q \in \mathbb{Z}[X]$. Trouver $R \in \mathbb{Z}[X]$ tel que $f_R = f_Q \circ f_P$.

22. Soit A un anneau. Lorsque $P = \sum_{i=0}^{d} c_i X^i$ est un polynôme en X à coefficients dans A, et a est un élément de A, on défini $P(a) \in A$ par

$$P(a) = \sum_{i=0}^{d} c_i a^i.$$

Ensuite, on définit par récurrence $P(a) \in A$ pour $P \in A[X_1, \ldots, X_n]$ et $a = (a_1, \ldots, a_n) \in A^n$: $P(a) = (P(a_n))(a_1, \ldots, a_{n-1})$.

a. Soit $a \in A$ Montrer que l'application d'évaluation en a

$$\mathrm{ev}_a\colon A[X] \longrightarrow A$$

définie par $\mathrm{ev}_a(P) = P(a)$ est un morphisme d'anneaux. On dit que $a \in A$ est une *racine* du polynôme P lorsque $\mathrm{ev}_a(P) = P(a) = 0$.

b. Soit $a = (a_1, \ldots, a_n) \in A^n$. Montrer que l'application d'évaluation

$$\mathrm{ev}_a\colon A[X_1, \ldots, X_n] \longrightarrow A$$

définie par $\mathrm{ev}_a(P) = P(a)$ est un morphisme d'anneaux.

23. Soient A, B et C des anneaux. Soient $f\colon A \to B$ et $g\colon B \to C$ des applications.

a. Supposons que g est un morphisme d'anneaux injectif. Montrer que f est un morphisme si et seulement si $g \circ f$ en est un.

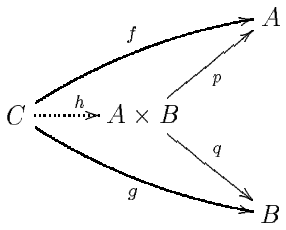
b. Supposons que f est un morphisme d'anneaux surjectif. Montrer que g est un morphisme d'anneaux si et seulement si $g \circ f$ en est un.

24. Soit $f\colon A \to B$ un morphisme d'anneaux. Montrer que f est un isomorphisme si et seulement si f est bijectif.

25. a. Soient A et B des anneaux. Définissons sur le produit $A \times B$ une addition $+$ et une multiplication $\cdot$ par $(a, b) + (a', b') = (a + a', b + b')$ et $(a, b) \cdot (a', b') = (aa', bb')$. Montrer que $A \times B$ est un anneau.

b. Montrer que les deux projections $p\colon A \times B \to A$ et $q\colon A \times B \to B$ définies par $p(a, b) = a$ et $q(a, b) = b$ sont des morphismes d'anneaux.

c. Montrer que $A \times B$ muni de ses deux projections p et q satisfait la propriété universelle suivante : pour tout anneau C et pour tous les morphismes $f : C \to A$ et $g : C \to B$, il existe un et un seul morphisme $h : C \to A \times B$ faisant commutatif le diagramme suivant :



Comme h est uniquement déterminé par f et g, on le notera par (f, g).

d. Montrer que $(A \times B)^\star = A^\star \times B^\star$.

e. Est-ce que le produit $A \times B$ est intègre lorsque A et B sont intègres?

f. Est-ce que le produit $A \times B$ est un corps lorsque A et B sont des corps?

26. Soient X un ensemble et $(A, +, \cdot)$ un anneau. L'ensemble des applications de X dans A sera noté par A^X.

a. Définissons pour deux applications f et g de X dans A leur somme $f + g : X \to A$ par $(f + g)(x) = f(x) + g(x)$ pour tout $x \in X$. Définissons également leur produit $f \cdot g : X \to A$ par $(f \cdot g)(x) = f(x) \cdot g(x)$ pour tout $x \in X$. Montrer que A^X est un anneau.

b. Soit $x \in X$. Soit $\mathrm{ev}_x : A^X \to A$ l'application d'évaluation en x, i.e., $\mathrm{ev}_x(f) = f(x)$. Montrer que ev_x est un morphisme d'anneaux.

c. Montrer que $(A^X)^\star = (A^\star)^X$.

27. Soit A_i, $i \in I$, une famille d'anneaux. Définissons sur le produit $A = \prod_{i \in I} A_i$ deux lois internes $+$ et $\cdot$ par

$$(a_i)_{i \in I} + (b_i)_{i \in I} = (a_i + b_i)_{i \in I} \quad \text{et} \quad (a_i)_{i \in I} \cdot (b_i)_{i \in I} = (a_i b_i)_{i \in I}.$$

Soit $p_i : A \to A_i$ la projection sur le i-ième facteur, $i \in I$. Montrer que

a. A est un anneau ;

b. p_i est un morphisme d'anneaux ;

c. l'anneau A muni des morphismes p_i, $i \in I$, est universel, i.e., montrer que pour tout anneau B et pour tous les morphismes $q_i : B \to A_i$, $i \in I$, il existe un et un seul morphisme $f : B \to A$ tel que $p_i \circ f = q_i$, $i \in I$;

d. $A^\star = \prod A_i^\star$.

28.* Soit A un anneau. Montrer qu'il existe un et un seul morphisme d'anneaux de $\mathbb{Z}$ dans A.

29. Montrer que la relation d'isomorphie est une relation d'équivalence.

30. Soient A et B deux anneaux isomorphes. Montrer que

a. B est intègre lorsque A l'est ;

b. B est un corps lorsque A l'est ;

c. les groupes multiplicatifs $A^\star$ et $B^\star$ sont isomorphes.

31. Soit A un anneau. Montrer que A est isomorphe à l'anneau nul si et seulement si $0 = 1$ dans A.

32. Soit A un anneau. Montrer que

a. A est isomorphe à l'anneau nul lorsque A n'a qu'un seul élément ;

b. A est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ lorsque A a exactement 2 éléments ;

c. A est isomorphe à $\mathbb{Z}/3\mathbb{Z}$ lorsque A a exactement 3 éléments.

Analyser les cas de 4, 5, 6 et 7 éléments.

33. Soient A un anneau, E un ensemble et $\varphi : E \to A$ une bijection.

a. Montrer que l'ensemble E admet une et une seule structure d'anneau telle que φ soit un morphisme d'anneaux. C'est la structure d'anneau sur E obtenue par *transport de structure*.

b. Montrer que chaque ensemble fini non vide admet une structure d'anneau.

c. Expliquer comment trouver des structures d'anneau exotiques sur $\mathbb{Z}$ telles que celles d'Exercice 4.

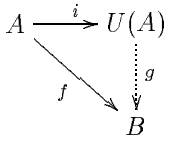
34. Soit E un ensemble à n éléments, n étant un entier positif. Montrer que l'ensemble E admet exactement $n!$ structures d'anneaux différentes isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

35.* a. Combien y a-t-il de lois multiplicatives faisant du groupe abélien $(\mathbb{Z}, +)$ un anneaux ?

b. Même question pour les groupes abéliens $\mathbb{Z}/n\mathbb{Z}$, n un entier non nul.

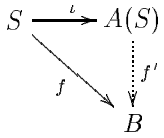
c. Même question pour le groupe abélien $\mathbb{Q}/\mathbb{Z}$.

36.* Dans cet exercice on considère des anneaux non nécessairement unitaires. Un morphisme de tels anneaux est une application satisfaisant les conditions **M1** et **M2**. Soit A un anneau (pas forcément unitaire). Montrer qu'il existe un anneau unitaire $U(A)$ et un morphisme d'anneaux non unitaires $i : A \to U(A)$ étant universel, c-à-d, pour tout anneau unitair B et tout morphisme d'anneaux non unitaires $f : A \to B$, il existe un et un seul morphisme d'anneaux $g : U(A) \to B$ tel que le diagramme suivant commute :



37.* Soit S un ensemble muni de deux lois internes $+$ et $\cdot$. On appelle S un *semi-anneau* si $(S, +, \cdot)$ satisfait toutes les conditions d'anneau sauf l'existence d'un opposé (**A3**). Un *morphisme de semi-anneau* est une application f satisfaisant hormi les conditions **M1**, **M2**, **M3**, la condition $f(0) = 0$.

a. Soit S un semi-anneau. Montrer qu'il existe un anneau $A(S)$ et un morphisme de semi-anneaux $\iota : S \to A(S)$ qui satisfont la propriété universelle suivante : pour tout anneau B et pour tout morphisme de semi-anneaux $f : S \to B$ il existe un et un seul morphisme d'anneaux $f' : A(S) \to B$ rendant le diagramme suivant commutatif :



Comme application on va montrer que pour tout anneau A, il existe un et un seul morphisme d'anneaux de $\mathbb{Z}$ dans A.

b. Montrer que $\mathbb{N}$ est un semi-anneau.

c. Soit S un semi-anneau. Montrer qu'il existe un et un seul morphisme de semi-anneaux de $\mathbb{N}$ dans S.

d. Montrer que l'anneau $A(\mathbb{N})$ est isomorphe à $\mathbb{Z}$.

e. Conclure.

§2

38. Le sous-ensemble $\{-1, 0, 1\}$ de $\mathbb{Z}$ est-il un sous-anneau ?

39. Soit A un anneau. Montrer que A est un sous-anneau de l'anneau $A[X]$.

40. Est-ce que $A \times \{0\}$ est un sous-anneau de $A^2 = A \times A$? Même question pour la diagonale $\Delta = \{(a, a) \mid a \in A\}$.

41. Soit A un anneau. Supposons que $B \subseteq A$ est un sous-ensemble tel que les lois internes de A induisent des lois internes sur B de façon à ce que B soit un anneau. Est-ce que B est nécessairement un sous-anneau de A ?

42. Si A est un sous-anneau de l'anneau B, l'inclusion $i : A \to B$ est un morphisme d'anneaux.

43. Soit $f : A \to B$ un morphisme d'anneaux. Montrer que

a. $f(C)$ est un sous-anneau de B lorsque C est un sous-anneau de A ;

b. l'image $f(A)$ de f est un sous-anneau de B.

44. La réunion de deux sous-anneaux est-elle un sous-anneau ?

45. Soit X un espace topologique. Montrer que l'ensemble $C(X, \mathbb{R})$ des fonctions réelles continues sur X est un sous-anneau de l'anneau de toutes les fonctions réelles $\mathbb{R}^X$ sur X.

46. a. Soit A un anneau et $f\colon \mathbb{Z} \to A$ l'unique morphisme d'anneaux de $\mathbb{Z}$ dans A. Montrer que l'image $f(\mathbb{Z})$ de f est le plus petit sous-anneau de A.

b. Déterminer le plus petit sous-anneau des anneaux $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

47. Soit A un sous-anneau de l'anneau B. Soit $s \in B$. Le plus petit sous-anneau $A[s]$ de B contenant $A \cup \{s\}$ est-il isomorphe à l'anneau de polynômes $A[X]$?

48. Soit d un entier positif. Montrer qu'il n'y a pas de morphismes d'anneaux du sous-anneaux $\mathbb{Z}[i\sqrt{d}]$ de $\mathbb{C}$ dans $\mathbb{Z}$.

49. Soit d un entier positif qui n'est pas un carré. Montrer qu'il n'y a pas de morphismes d'anneaux du sous-anneaux $\mathbb{Z}[\sqrt{d}]$ de $\mathbb{R}$ dans $\mathbb{Z}$.

50. Soit d un entier positif. Montrer que le sous-anneau $\mathbb{Q}[i\sqrt{d}]$ de $\mathbb{C}$ est un corps. Même question pour le sous-anneau $\mathbb{Q}[\sqrt{d}]$ de $\mathbb{C}$.

51.* Soit A un anneau et $K \subseteq A$ un sous-anneau. Supposons que K est en plus un corps. Montrer que

a. la restriction à $K \times A$ de la loi interne multiplicative $\cdot\colon A \times A \to A$ est une structure de K-espace vectoriel sur A ;

b. tout élément régulier de A est inversible lorsque A est de dimension finie en tant que K-espace vectoriel ;

c. A est un corps lorsque A est intègre et de dimension finie en tant que K-espace vectoriel ;

52. Soient B un anneaux et A un sous-anneau de B. Soit $S \subseteq B$ un sous-ensemble. Montrer que le plus petit sous-anneau $A[S]$ de B contenant $A \cup S$ est égal au sous-ensemble

$$\Big\{ \sum_{i \in I} a_i \cdot \prod_{j \in J_i} s_{ij} \,|\, a_i \in A, s_{ij} \in S, \text{ et } I, J_i \text{ finis} \Big\}.$$

53. Existe-t-il $s \in \mathbb{C}$ tel que $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[s]$?

54. Soient A, B et C des anneaux. Soient $f\colon B \to A$ et $g\colon C \to A$ des morphismes d'anneaux. On définit le *produit fibré* de B et C sur A par

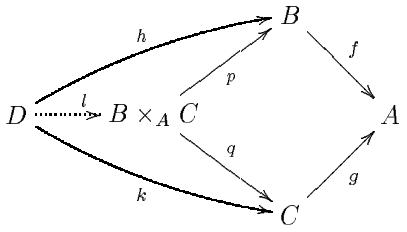
$$B \times_A C = \{(b, c) \in B \times C \,|\, f(b) = g(c)\}.$$

a. Montrer que $B \times_A C$ est un sous-anneau du produit $B \times C$.

b. Soient $p\colon B \times_A C \to B$ et $q\colon B \times_A C \to C$ les applications définies par $p(b, c) = b$ et $q(b, c) = c$. Montrer que p et q sont des morphismes d'anneaux.

c. Montrer que $B \times_A C$ muni de ses projections p et q est universel d'ayant la propriété que $f \circ p = g \circ q$, c-à-d, pour tout anneau D et pour tous les morphismes d'anneaux $h\colon D \to B$ et $k\colon D \to C$ tels que $f \circ h = g \circ k$,

il existe un et un seul morphisme d'anneaux $l\colon D \to B \times_A C$ tel que le diagramme suivant commute :



55. Soit A un anneau unitair, non forcément commutatif.

a. Montrer que le centre $Z(A) = \{a \in A \,|\, \forall b \in A\colon ab = ba\}$ est un sous-anneau unitair commutatif de A.

b. Montrer qu'il existe un unique morphisme d'anneau de $\mathbb{Z}$ dans A.

§3

56. Soit I un idéal de l'anneau A. Montrer l'équivalence des conditions suivantes :

a. $I = A$;

b. $1 \in I$;

c. $I \cap A^\star \neq \emptyset$.

57. Soit $f\colon A \to B$ un morphisme d'anneaux. Montrer que le noyau $\ker(f)$ est un idéal de A.

58. Soit $\mathcal{I}$ une famille d'idéaux de A. Montrer que l'intersection $\bigcap \mathcal{I}$ est un idéal de A. En déduire, étant donné un sous ensemble $S \subseteq A$, l'existence du plus petit idéal de A contenant S.

59. Soit A un anneau tel que $A[X]$ soit noetherien. Montrer que A est noetherien.

60. Un sous-anneau d'un anneau noetherien, est-il forcément noetherien?

61. Soient A et B deux anneaux. Montrer que

a. $I \times J$ est un idéal de $A \times B$ lorsque I est un idéal de A et J en est un de B ;

b. pour tout idéal K de $A \times B$ il existe des idéaux I de A et J de B tels que $K = I \times J$;

c. tout idéal de $A \times B$ est principal lorsque tous les idéaux de A et B le sont ;

d. $A \times B$ est noetherien si et seulement si A et B le sont.

62. Soit A un anneau intègre et soient a et b deux éléments de A. Rappelons que a et b sont *associés* s'il existe $u \in A^\star$ tel que $a = ub$. Montrer que les idéaux Aa et Ab de A sont égaux si et seulement si a et b sont associés.

63. L'idéal $(n_1, \ldots, n_k)$ engendré par $n_1, \ldots, n_k \in \mathbb{Z}$ est égal à l'idéal de $\mathbb{Z}$ engendré par le pgcd de $n_1, \ldots, n_k$.

64. Soient I et J des idéaux de A. Soient $a_1, \ldots, a_n$ et $b_1, \ldots, b_m$ des éléments de A. Montrer que

a. la somme
$$I + J = \{x + y \mid x \in I, y \in J\}$$
est un idéal de A ;

b. $I + I = I$, plus généralement, $I + J = J$ lorsque $I \subseteq J$;

c. $(a_1, \ldots, a_n) + (b_1, \ldots, b_m) = (a_1, \ldots, a_n, b_1, \ldots, b_m)$;

d. le produit
$$I \cdot J = \{\sum_{i=1}^{n} x_i y_i \mid x_i \in I, y_i \in J, n \in \mathbb{N}\}$$
est un idéal de A ;

e. $(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_m) = (a_i b_j \mid i = 1, \ldots, n \text{ et } j = 1, \ldots, m)$;

65. Soient I et J des idéaux de A.

a. Montrer que $I \cap J \supseteq I \cdot J$.

b. Montrer par un exemple que $I \cap J$ n'est pas forcément égal à $I \cdot J$.

c. Montrer que $I \cap J = I \cdot J$ lorsque I est J sont étrangers. (Rappelons que deux idéaux I et J de A sont *étrangers* si $I + J = A$.)

d. Généraliser à un nombre fini d'idéaux de A deux à deux étrangers.

66. Soit A un anneau. Soient I, J, K des idéaux de A. Montrer que

a. I et $J \cdot K$ sont étrangers lorsque $I + J = A$ et $I + K = A$;

b. I et $J \cap K$ sont étrangers lorsque $I + J = A$ et $I + K = A$;

c. I^m et J^n sont étrangers lorsque $I + J = A$, où $m, n \in \mathbb{N}$.

67. Soit A un anneau non nul.

a. Montrer que 0 et A sont les seuls idéaux de A lorsque A est un corps ;

b. Remontrer exercice 18.

c. Montrer qu'un corps est noetherien.

d. Montrer que A est un corps lorsque 0 et A sont les seuls idéaux de A.

68. Désignons par $\mathrm{Id}(A)$ l'ensemble des idéaux de l'anneau A. Soit $f : A \to B$ un morphisme d'anneaux.

a. Soit $I \subseteq A$ un idéal. L'image directe $f(I)$ est-elle un idéal de B?

b. Soit $J \subseteq B$ un idéal. Montrer que l'image réciproque $f^{-1}(J)$ est un idéal de A. On a alors une application induite, notée par $\mathrm{Id}(f)$, de l'ensemble $\mathrm{Id}(B)$ des idéaux de B dans l'ensemble $\mathrm{Id}(A)$ des idéaux de A.

c. Soient J et J' des idéaux de B. Montrer que $f^{-1}(J \cdot J') = (f^{-1}(J)) \cdot (f^{-1}(J'))$.

d. Soient J et J' des idéaux de B. Montrer que $f^{-1}(J + J') = (f^{-1}(J)) + (f^{-1}(J'))$.

e. Soit $I \subseteq A$ un idéal. Montrer que $f(I)$ est un idéal de B lorsque f est surjectif.

f. Supposeons encore que f est surjectif. Soit $S \subseteq A$ un sous-ensemble. Montrer que $f((S)) = (f(S))$.

g. Soit $I \subseteq A$ un idéal. Montrer que $f^{-1}(f(I)) = I + \ker(f)$.

h. Montrer que l'application $\mathrm{Id}(f)$ est injective et que son image est l'ensemble des idéaux de A contenant $\ker(f)$, lorsque f est surjectif.

i. Déterminer tous les idéaux de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

69. Soit K un corps. Soit $S \subseteq K[X_1, \ldots, X_n]$ un ensemble de polynômes en $X_1, \ldots, X_n$ à coefficients dans K. Soit

$$Z(S) = \{(a_1, \ldots, a_n) \in K^n \mid \forall P \in S : P(a_1, \ldots, a_n) = 0\}.$$

On appelle $Z(S)$ *l'ensemble de zéros* de S. Un sous-ensemble X de K^n est un *ensemble algébrique* s'il existe un sous-ensemble S de $K[X_1, \ldots, X_n]$ tel que $X = Z(S)$. Montrer que

a. l'ensemble des zéros de S est égal à l'ensemble des zéros de l'idéal engendré par S, i.e., $Z(S) = Z((S))$;

b. pour tout ensemble algébrique X de K^n il existe un nombre fini de polynômes $P_1, \ldots, P_m \in K[X_1, \ldots, X_n]$ tels que

$$X = Z(P_1, \ldots, P_m) \ ;$$

c. lorsque $I \subseteq J$ sont des idéaux de $K[X_1, \ldots, X_n]$, on a $Z(I) \supseteq Z(J)$;

d. pour tout $(a_1, \ldots, a_n) \in K^n$ et tout idéal I de $K[X_1, \ldots, X_n]$, on $(a_1, \ldots, a_n) \in Z(I)$ si et seulement si $I \subseteq (X_1 - a_1, \ldots, X_n - a_n)$.

§4

70. Soit A un anneau. Déterminer le plus petit et le plus grand idéal de A, I et $\boldsymbol{I}$, respectivement. Déterminer les quotients correspondants.

71. Soit $f\colon A \to B$ un morphisme d'anneaux. Montrer que

a. le morphisme induit $\overline{f}\colon A/\ker(f) \to B$ est injectif ;

b. $\overline{f}$ est un isomorphisme lorsque f est surjectif ;

c. il existe un morphisme d'anneaux surjectif g et un morphisme d'anneaux injectif h tels que $f = h \circ g$.

72. Montrer que chaque idéal est le noyau d'un morphisme d'anneaux.

73. a. Soit A un anneau et $I \subseteq A$ un idéal. Montrer que A/I est noetherien si A l'est.

b. Soit A un anneau et $I \subseteq A[X_1, \ldots, X_n]$ un idéal. Montrer que le quotient $A[X_1, \ldots, X_n]/I$ est noetherien si A l'est.

74. a. Soit A un anneau dont chaque idéal est principal. Montrer que chaque idéal du quotient A/I est principal, quel que soit l'idéal $I \subseteq A$.

b. Est-ce que l'anneau A/I est principal si A l'est?

75. Soit A un anneau et $a \in A$. Montrer que le morphisme $\mathrm{ev}_a \colon A[X] \to A$ d'évaluation en a est un quotient de $A[X]$ par l'idéal $(X - a)$.

76. Soit A et B des anneaux. Soit $p \colon A \times B \to A$ la projection $p(a, b) = a$. Montrer que $\{0\} \times B$ est un idéal de $A \times B$ et que p est un quotient de $A \times B$ par $\{0\} \times B$.

77. Montrer qu'il n'y a pas d'anneaux A ayant un élément $a \neq 1$ tel que $a^3 = 1$ et $a^5 = 1$.

78. Soit A un anneau et $P \in A[X]$ un polynôme. Soit B le quotient $A[T]/(P(T))$ et $f \colon A \to B$ le morphisme canonique.

a. Montrer par un exemple que f n'est pas nécessairement injectif.

b. Montrer que f est injectif si P est unitaire et de degré positif.

c. Soit $F \colon A[X] \to B[X]$ l'unique morphisme tel que $F_{|A} = f$ et $F(X) = X$. Montrer que l'image $F(P)$ de P a une racine dans B.

d. Lorsque f est injectif on peut considérer A comme sous-anneau de B. Montrer que P considéré comme polynôme à coefficients dans B, a une racine dans B.

e. Montrer que f est injectif lorsque P est unitaire de degré strictement positif.

f. Montrer que A est un sous-anneau d'un anneau B dans lequel ont une racine tous les polynômes unitaires à coefficients dans A et de degré strictement positif.

g. Soit P un polynôme unitaire de degré supérieur à 1. Soit n un entier non négatif. Montrer qu'il existe un anneau C contenant A comme sous-anneau dans lequel P a au moins n racines différentes.

79. Soit A un anneau. Déterminer un système de représentants pour les quotients suivants :

a. $A[X, Y]/(Y - P)$, où $P \in A[X]$;

b. $A[X, Y]/(X^2 + Y^2 - 1)$;

c. $A[X, Y]/(XY - 1)$;

80. Soit d un entier positif.

a. Montrer que le sous-anneau $\mathbb{Q}[i\sqrt{d}]$ de $\mathbb{C}$ est isomorphe au quotient $\mathbb{Q}[X]/(X^2+d)$. Est-ce que l'isomorphisme est unique ?

b. Montrer que le sous-anneau $\mathbb{Z}[i\sqrt{d}]$ de $\mathbb{C}$ est isomorphe au quotient $\mathbb{Z}[X]/(X^2+d)$. Est-ce que l'isomorphisme est unique ?

81. Soit d un entier positif et un non carré.

a. Montrer que le sous-anneau $\mathbb{Q}[\sqrt{d}]$ de $\mathbb{R}$ est isomorphe au quotient $\mathbb{Q}[X]/(X^2-d)$. Est-ce que l'isomorphisme est unique ?

b. Montrer que le sous-anneau $\mathbb{Z}[\sqrt{d}]$ de $\mathbb{R}$ est isomorphe au quotient $\mathbb{Z}[X]/(X^2-d)$. Est-ce que l'isomorphisme est unique ?

82. Soit A le quotient $\mathbb{Z}[X]$ par l'idéal engendré par X^n-1. Soit $k \in \mathbb{N}$. Soit $f_k : \mathbb{Z}[X] \to \mathbb{Z}[X]$ le morphisme défini par $f_k(P) = P(X^k)$.

a. Montrer que f_k induit un endomorphisme φ_k de A.

b. Montrer que φ_k est un automorphisme lorsque k et n sont premiers entre eux.

83. Soit $\pi : A \to A/I$ le quotient de l'anneau A par l'idéal I. Montrer que π est surjectif en n'utilisant que la propriété universelle du quotient.

84. Soit $f : A \to B$ un morphisme d'anneaux. Soit I un idéal de A, et J un idéal de B.

a. Montrer que $f(I) \subseteq J$ si et seulement s'il existe un morphisme d'anneaux $\bar{f} : A/I \to B/J$ faisant commuter le diagramme suivant :

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle \pi_I}\downarrow & & \downarrow{\scriptstyle \pi_J} \\ A/I & \xrightarrow{\bar{f}} & B/J \end{array}$$

b. Montrer que le noyau de $\bar{f}$ est alors égal à l'image de l'idéal $I + \ker(f)$ dans A/I.

85.* (Théorème Chinois) Soient I et J des idéaux de A. Soient π et ρ les morphismes de passage au quotient correspondant.

a. Montrer que le morphisme $(\pi, \rho) : A \to A/I \times A/J$ induit un isomorphisme $\gamma : A/(I \cap J) \to A/I \times A/J$ lorsque I et J sont étrangers.

b. Montrer que (π, ρ) induit un isomorphisme $\delta : A/IJ \to A/I \times A/J$ lorsque I et J sont étrangers.

c. Montrer les réciproques à a. et b.

d. Généraliser à un nombre fini d'idéaux de A qui sont deux à deux étrangers.

86.* Montrer que $\mathbb{Q}[X]/(X^2-1)$ est isomorphe à $\mathbb{Q}^2$. Est-ce que le quotient $\mathbb{Z}[X]/(X^2-1)$ est isomorphe à $\mathbb{Z}^2$?

87. Soit A un anneau et soient I et J des idéaux de A tels que $I \subseteq J$. Montrer que

a. l'image directe de J dans A/I est un idéal de A/I (on notera par la suite cet idéal par J/I) ;

b. le quotient $(A/I)/(J/I)$ de A/I par J/I est isomorphe à A/J.

88. Soit I un idéal de A. Considérons A comme sous-anneau de l'anneau $A[X]$ des polynômes en X à coefficients dans A. Soit $I[X]$ l'idéal de $A[X]$ engendré par I dans $A[X]$. Montrer que

a. $I[X] = \{\sum_{i=0}^{n} a_i X^i \mid a_i \in I, n \in \mathbb{N}\}$;

b. $A[X]/I[X] \cong (A/I)[X]$.

89. Déterminer le quotient $\mathbb{Z}[X]/(X^2 - 5, p)$ pour $p = 2, 3$ et 5.

90. Déterminer le quotient $\mathbb{R}[X, Y]/(Y^2 - X, X - x)$ pour $x = -1, 0$ et 1.

91. Soit A un anneau et $f\colon \mathbb{Z} \to A$ l'unique morphisme d'anneaux de $\mathbb{Z}$ dans A. Comme $\mathbb{Z}$ est principal, le noyau de f est engendré par un entier non négatif uniquement déterminé. On appelle cet unique entier la *caractéristique* de l'anneau A, notée par $\mathrm{car}(A)$. Montrer que

a. on a $na = 0$ quel que soit $a \in A$, où $n = \mathrm{car}(A)$;

b. si n est un entier non négatif, alors il existe un anneau de caractéristique n ;

c. le plus petit sous-anneau de A est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, où $n = \mathrm{car}(A)$;

d. $\mathrm{car}(B)$ divise $\mathrm{car}(A)$ s'il existe un morphisme d'anneaux de A dans B ;

e. $\mathrm{car}(A) = \mathrm{car}(B)$ si A et B sont isomorphes ;

f. $\mathrm{car}(A)$ est soit zéro, soit premier lorsque A est intègre ;

g. $\mathrm{car}(A \times B) = \mathrm{ppcm}(\mathrm{car}(A), \mathrm{car}(B))$;

h. Si $n \in \mathbb{N}$ divise $\mathrm{car}(A)$, alors $\mathrm{car}(A/nA) = n$.

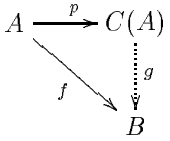
92.* a. Soit A un anneau de caractéristique $n \neq 0$. Soit $n = \prod_{i=1}^{g} p_i^{e_i}$ sa décomposition en facteurs premiers. En particulier, $e_i > 0$ et $p_i \neq p_j$ si $i \neq j$. Montrer qu'il existe des anneaux A_i, $i = 1, \ldots, g$, tels que A soit isomorphe au produit $\prod A_i$ et que A_i soit de caractéristique $p_i^{e_i}$.

b. Soit n un entier dont la décomposition en facteurs premiers est $\prod_{i=1}^{g} p_i$. Montrer que chaque anneau à n éléments est isomorphe à

$$\mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_g\mathbb{Z}.$$

c. Est-ce qu'un anneau à p^2 éléments, p premier, est forcément isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$?

93.* Soit A un anneau (pas forcément commutatif). Montrer qu'il existe un anneau commutatif $C(A)$ et un morphisme d'anneau $p\colon A \to C(A)$ étant universel, i.e., pour tout anneau commutatif B et pour tout morphisme d'anneaux $f\colon A \to B$ il existe un et un seul morphisme d'anneaux $g\colon C(A) \to B$ tel que le diagramme suivant commute :



94. Soit X_e, $e \in E$ une famille d'indeterminés. Soit $\mathbb{Z}[X_e \,|\, e \in E]$ l'anneau de polynômes en les déterminés X_e à coefficients entiers. Soit A un anneau quelconque. Montrer qu'il existe un ensemble E et un idéal I de l'anneau de polynômes $\mathbb{Z}[X_e \,|\, e \in E]$ tels que A soit isomorphe au quotient $\mathbb{Z}[X_e \,|\, e \in E]/I$.

§5

95. Soit d un entier postif. Montrer que $\mathbb{Q}[i\sqrt{d}]$ est le corps de fractions de $\mathbb{Z}[i\sqrt{d}]$ et que $\mathbb{Q}[\sqrt{d}]$ est le corps de fractions de $\mathbb{Z}[\sqrt{d}]$.

96. Soient A un anneau et $S \subseteq A$ une partie multiplicative. Donner une condition nécessaire et suffisante sur S pour que la localisation $\iota\colon A \to S^{-1}A$ soit injective.

97. Soient A un anneau et $S \subseteq A$ une partie multiplicative. Déterminer $S^{-1}A$ si $0 \in S$. Déterminer $S^{-1}A$ lorsque $S = \{1\}$. Plus généralement, déterminer $S^{-1}A$ lorsque $S \subseteq A^\star$.

98. Soit A un anneau et $S \subseteq A$ une partie multiplicative telle que $0 \notin S$. Montrer que

a. la localisation $S^{-1}A$ est intègre si A l'est ;

b. l'idéal $S^{-1}I$ est principal lorsque I l'est ;

c. l'anneau $S^{-1}A$ est principal lorsque A l'est.

99. Soit A un anneau et $S \subseteq A$ une partie multiplicative contenue dans l'ensemble des réguliers de A. Montrer que le morphisme induit $S^{-1}A \to \mathrm{Frac}(A)$ est injectif. De ce fait, on peut considérer $S^{-1}A$ comme sous-anneau du corps de fractions $\mathrm{Frac}(A)$ lorsque S est contenue dans l'ensemble des réguliers de A.

100. Soient A un anneau et $S \subseteq A$ une partie multiplicative. Montrer que $S^{-1}A$ est noetherien si A l'est.

101. Soient A et B des anneaux. Soit $p\colon A \times B \to A$ la projection. Montrer que p est un morphisme de localisation de $A \times B$ par la partie multiplicative $S = \{(1,0),(1,1)\}$.

102. Soit A un anneau et $s \in A$. Soit $\mathrm{Ann}(s)$ l'annulateur de s, i.e.,

$$\mathrm{Ann}(s) = \{a \in A \,|\, as = 0\}.$$

Montrer que

a. $\mathrm{Ann}(s)$ est un idéal de A ;

b. le noyau du morphisme de localisation $\iota : A \to A_s$ contient $\mathrm{Ann}(s)$;

c. si l'image de s dans le quotient $A/\mathrm{Ann}(s)$ est régulier, alors $\ker(\iota) = \mathrm{Ann}(s)$;

d. si l'image de s dans le quotient $A/\mathrm{Ann}(s)$ est inversible, alors $A_s \cong A/\mathrm{Ann}(s)$.

103. Soit n un entier non nul. Déterminer $(\mathbb{Z}_n)^\star$.

104. Soit n un entier non nul. Soit I un idéal non nul de la localisation $\mathbb{Z}_n$ de $\mathbb{Z}$ par n. Montrer que

a. il existe un entier m tel que $I = m\mathbb{Z}_n$;

b. cet entier m peut etre pris premier avec n.

Conclure que l'ensemble des idéaux non nuls de $\mathbb{Z}_n$ est en correspondance bijective avec l'ensemble des entiers positifs et premiers avec n.

105. Soit K un corps. Soit p la caractéristique de K. Rappelons que p est soit zéro, soit premier. Montrer que

a. K contient un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$ si p est premier ;

b. K contient un sous-corps isomorphe à $\mathbb{Q}$ si $p = 0$.

Dans les deux cas, ce sous-corps de K est le plus petit sous-corps de K. On l'appelle le *sous-corps premier* de K. Le corps K est un *corps premier* si K est égal à son propre sous-corps premier.

106. Soit $f : A \to B$ un morphisme d'anneaux.

a. Soit $S \subseteq A$ une partie multiplicative. Montrer que l'image directe de S, $f(S)$, est une partie multiplicative de B.

b. Soit $T \subseteq B$ une partie multiplicative. Montrer que l'image réciproque de T, $f^{-1}(T)$, est une partie multiplicative de A.

107. Soient A et B des anneaux et $S \subseteq A$ et $T \subseteq B$ des parties multiplicatives. Si f est un morphisme de A dans B avec $f(S) \subseteq T$, alors f induit un morphisme f' de $S^{-1}A$ dans $T^{-1}B$ rendant le diagramme suivant commutatif.

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & B \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} \\ S^{-1}A & \xrightarrow{\ f'\ } & T^{-1}B \end{array}$$

108. Soit K un corps. Montrer que $(K[X,Y]/(XY))_X$ est isomorphe à $K[X]_X$.

109.* Soient A un anneau et $S \subseteq A$ une partie multiplicative. Soit $\iota_S : A \to S^{-1}A$ le morphisme de localisation. Soit

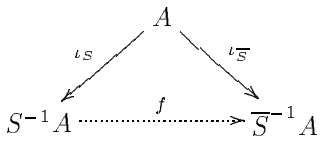
$$\overline{S} = \{t \in A \mid \exists a \in A : at \in S\},$$

i.e., $\overline{S}$ est l'ensemble de tous les diviseurs d'éléments de S. On appelle une partie multiplicative S *saturée* lorsque $\overline{S} = S$.

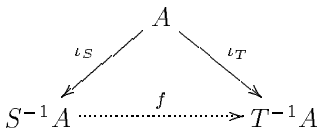
a. Montrer que $\overline{S} = \iota_S^{-1}((S^{-1}A)^\star)$.

b. Montrer que $\overline{S}$ est une partie multiplicative de A.

c. Montrer qu'il existe un isomorphisme $f : S^{-1}A \to \overline{S}^{-1}A$ rendant commutatif le diagramme suivant :



d. Soient S et T deux parties multiplicatives de A. Montrer que $\overline{S} = \overline{T}$ si et seulement s'il existe un isomorphisme $f : S^{-1}A \to T^{-1}A$ rendant commutatif le diagramme



Dans ce cas, on dira que les localisations ι_S et ι_T sont *isomorphes*.

e. Montrer qu'il y a une correspondance entre les localisations de A à isomorphisme près, et les parties multiplicatives saturées de A.

f. Déterminer toutes les localisations de $\mathbb{Z}$ à isomorphisme près, ainsi que celles de $K[X]$, K étant un corps.

g. Déterminer tous les sous-anneaux de $\mathbb{Q}$.

h. Déterminer tous les sous-anneaux de $K(X)$ contenant $K[X]$, K étant un corps.

i. Un sous-anneau de $K(X,Y)$ contenant $K[X,Y]$ est-il forcément une localisation de $K[X,Y]$?

110. Soit A un anneau. Montrer que

a. tout élément régulier de l'anneau de fractions $\mathrm{Frac}(A)$ de A est inversible.

b. l'anneau de fractions de A est son propre anneau de fractions, i.e., le morphisme $\iota : \mathrm{Frac}(A) \to \mathrm{Frac}(\mathrm{Frac}(A))$ est un isomorphisme.

c. tout anneau est isomorphe à un sous-anneau d'un anneau dans lequel chaque élément est soit inversible, soit un diviseur de zéro.

111. a. Soit A un anneau et $s \in A$. Montrer que l'anneau A_s obtenu de A en localisant par s est isomorphe à l'anneau $A[X]/(sX-1)$.

b. Soit A un anneau et $s,t \in A$ Soit S a plus petite partie multiplicative de A contenant s et t. A-t-on $S^{-1}A \cong A[X,Y]/(sX-1, tY-1)$?

§6

112. a. Soit $P \in \mathbb{Z}[X]$ un polynôme et soit $p \in \mathbb{Z}$ premier. Soit $A = \mathbb{Z}[X]/(P)$. Montrer que l'idéal pA est premier si et seulement si P est zéro ou bien irréductible modulo p.

b. Soit $P = X^2 - d$, d un entier quelconque. Soit $A = \mathbb{Z}[X]/(P)$ et $p \in \mathbb{Z}$ premier. Montrer que l'idéal pA est premier si et seulement si d n'est pas un carré modulo p.

113.* Soit X un espace topologique. Soit $A = C(X, \mathbb{R})$ l'anneau des fonctions réelles continues sur X. Lorsque $x \in X$ soit $m_x = \{f \in A \mid f(x) = 0\}$. Montrer que

a. m_x est un idéal maximal de A quel que soit $x \in X$;

b. pour tout idéal maximal m de A il existe $x \in X$ tel que $m_x = m$ lorsque X est compact ;

c. il existe un idéal maximal m de A tel que $m \neq m_x$ pour tout $x \in X$ lorsque X n'est pas compact et X a suffisamment de fonctions continues à support compact, i.e., quel que soit $x \in X$, il existe $f \in C(X, \mathbb{R})$ à support compact avec $f(x) \neq 0$.

114. Montrer que $A^\star = A \setminus \bigcup_{m \in \mathrm{Max}(A)} m$.

115. Soit A un anneau. On appelle l'intersection

$$\bigcap_{m \in \mathrm{Max}(A)} m$$

de tous les idéaux maximaux de A le *radical de Jacobson* de A. Le radical de Jacobson de A est un idéal de A, noté par $\mathrm{JRad}(A)$. Soit I un idéal de A. Montrer que

a. $I \subseteq \mathrm{JRad}(A)$ si et seulement si $1 + I \subseteq A^\star$;

b. le morphisme de groupes $\pi^\star \colon A^\star \to (A/I)^\star$ induit par le morphisme de passage au quotient π est surjectif lorsque $I \subseteq \mathrm{JRad}(A)$.

116.* Soit A un anneau n'ayant qu'un nombre fini d'idéaux maximaux et qu'un nombre fini d'éléments inversibles. Montrer que A est fini.

117. Soit $f \colon A \to B$ un morphisme d'anneaux.

a. Montrer que $f^{-1}(p)$ est un idéal premier de A lorsque p en est un de B. On a alors une application $\mathrm{Spec}(f)$ de $\mathrm{Spec}(B)$ dans $\mathrm{Spec}(A)$ qui associe à $p \in \mathrm{Spec}(B)$ l'idéal premier $f^{-1}(p)$ de A.

b. Est-ce que $f^{-1}(m)$ est un idéal maximal de A lorsque m en est un de B ?

c. Montrer que $\mathrm{Spec}(f)$ est injective et son image est l'ensemble d'idéaux premiers de A contenant $\ker(f)$ lorsque f est surjectif.

d. Montrer que $f^{-1}(m)$ est un idéal maximal de A si m en est un de B lorsque f est surjectif. On a alors une application $\mathrm{Max}(f)$ de $\mathrm{Max}(B)$ dans $\mathrm{Max}(A)$.

e. Montrer que $\mathrm{Max}(f)$ est injective et son image est l'ensemble d'idéaux maximaux de A contenant $\ker(f)$ lorsque f est surjectif.

f. Déterminer les idéaux premiers et les idéaux maximaux de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

118. a. Montrer que l'application induite $\mathrm{Spec}(\mathrm{id}_A)$ par le morphisme d'identité id_A sur A est égale à l'identité $\mathrm{id}_{\mathrm{Spec}(A)}$ sur $\mathrm{Spec}(A)$.

b. Soient $f\colon A \to B$ et $g\colon B \to C$ des morphismes d'anneaux. Montrer que $\mathrm{Spec}(g \circ f) = \mathrm{Spec}(f) \circ \mathrm{Spec}(g)$.

c. Soit $f\colon A \to B$ un isomorphisme. Montrer que $\mathrm{Spec}(f)$ est une bijection.

119. Trouver un idéal maximal de $\mathbb{Z}[X]$ contenant l'idéal $(X^3 - 2, 9)$.

120. Soit K un corps. Soit $A = K[X_1, \ldots, X_n]$ et soit $x = (x_1, \ldots, x_n) \in K^n$. Soit m l'idéal $(X_1 - x_1, \ldots, X_n - x_n)$ de A.

a. Montrer que le quotient de A par l'idéal m est isomorphe au morphisme d'évaluation au point x

$$\mathrm{ev}_x\colon A = K[X_1, \ldots, X_n] \longrightarrow K$$

défini par $\mathrm{ev}_x(P) = P(x)$.

b. Montrer que m est un idéal maximal de A.

c. Soit $I \subseteq A$ un idéal. Montrer que l'image de m dans le quotient A/I est un idéal maximal si x appartient à l'ensemble de zéros $Z(I) \subseteq K^n$ de I. Montrer que l'image de m dans A/I est égale à A/I si $x \notin Z(I)$.

121. Soit I l'idéal $(X^2 + Y^2 - 1)$ de $\mathbb{R}[X, Y]$. Trouver un idéal maximal m de $\mathbb{R}[X, Y]$ contenant I. Même question pour l'idéal $J = (X^2 + Y^2 + 1)$.

122. Soient A et B deux anneaux. Montrer qu'il y a une correspondance entre

a. $\mathrm{Spec}(A \times B)$ et $\mathrm{Spec}(A) \cup \mathrm{Spec}(B)$;

b. $\mathrm{Max}(A \times B)$ et $\mathrm{Max}(A) \cup \mathrm{Max}(B)$.

123. Soit A un anneau et $S \subseteq A$ une partie multiplicative. Soit $\iota\colon A \to S^{-1}A$ le morphisme de localisation.

a. Montrer que l'application $\mathrm{Spec}(\iota)\colon \mathrm{Spec}(S^{-1}A) \to \mathrm{Spec}(A)$ est injective et son image est l'ensemble d'idéaux premiers p de A tels que $p \cap S = \emptyset$.

b. Soit n un entier non nul. Déterminer les idéaux premiers et les idéaux maximaux de la localisation $\mathbb{Z}_n$ de $\mathbb{Z}$ par n.

c. Soit $p \in \mathbb{Z}$ premier. Déterminer les idéaux premiers et les idéaux maximaux de la localisation $\mathbb{Z}_{(p)}$ de $\mathbb{Z}$ en (p).

124.* Soient A un anneau, $I \subseteq A$ un idéal et $S \subseteq A$ une partie multiplicative telle que $S \cap I = \emptyset$. Montrer qu'il existe un idéal premier p de A tel que $I \subseteq p$ et $p \cap S = \emptyset$.

125. Soit A un anneau et $S \subseteq A$ multiplicative. Montrer que S est saturée si et seulement si $A \backslash S$ est la réunion d'idéaux premiers de A.

126. Montrer que chaque corps a une clôture algébrique.

§7

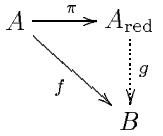
127. Soit n un entier. Déterminer le radical de l'idéal $n\mathbb{Z}$ de $\mathbb{Z}$. Déterminer $(\mathbb{Z}/n\mathbb{Z})_{\mathrm{red}}$.

128. Soit $P \in K[X]$ un polynôme, K un corps. Déterminer le radical de l'idéal (P) de $K[X]$. Déterminer $(K[X]/(P))_{\mathrm{red}}$.

129. Soit K un corps. Soit I l'idéal de $K[X,Y]$ engendré par $Y^2 - X$ et X^2. Déterminer le radical $\mathrm{Rad}(I)$ de I.

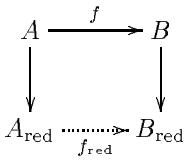
130. Soit A un anneau et soit $\pi : A \to A_{\mathrm{red}}$ le morphisme de passage au quotient. Montrer que l'application $\mathrm{Spec}(\pi) : \mathrm{Spec}(A_{\mathrm{red}}) \to \mathrm{Spec}(A)$ est bijective. Montrer l'énoncé analogue pour l'application $\mathrm{Max}(\pi)$.

131. Soit A un anneau. Soit $\pi : A \to A_{\mathrm{red}}$ le passage au quotient. Montrer que π satisfait la propriété universelle suivante : pour tout anneau réduit B et pour tout morphisme $f : A \to B$ il existe un et un seul morphisme $g : A_{\mathrm{red}} \to B$ tel que le diagramme suivant commute :



132. Soit $f : A \to B$ un morphisme d'anneaux. Montrer que

a. f induit un unique morphisme d'anneaux $f_{\mathrm{red}} : A_{\mathrm{red}} \to B_{\mathrm{red}}$ tel que le diagramme suivant commute :



b. f_{red} est surjectif lorsque f l'est ;

c. f_{red} est injectif lorsque f l'est ;

d. $A_{\mathrm{red}} \cong B_{\mathrm{red}}$ si $A \cong B$;

e. A_{red} est un sous-anneau de B_{red} si A en est un de B.

133. Soit A un anneau et $S \subseteq A$ multiplicative. Soit S_{red} l'image de S dans l'anneau réduit A_{red} associé à A. Montrer que

a. $\mathrm{Nil}(S^{-1}A) = S^{-1}\mathrm{Nil}(A)$;

b. $S_{\mathrm{red}} \subseteq A_{\mathrm{red}}$ est multiplicative ;

c. $S_{\mathrm{red}}^{-1}A_{\mathrm{red}}$ est isomorphe à $(S^{-1}A)_{\mathrm{red}}$.

134. Soient I et J des idéaux de A. Montrer que $\mathrm{Rad}(I \cap J) = \mathrm{Rad}(IJ) = \mathrm{Rad}(I) \cap \mathrm{Rad}(J)$.

135.* Soit A un anneau réduit. Montrer que

a. A est isomorphe à un sous-anneau d'un produit de corps ;

b. A est isomorphe à un sous-anneau d'un produit fini de corps lorsque A est noetherien ;

c. A est isomorphe à un produit fini de corps lorsque A est fini.

136. Soient I et J des idéaux de A. Montrer qu'un idéal K de A est un diviseur de I et J si et seulement si K est un diviseur de $I + J$.

137. Soit $I \subseteq A$ un idéal et $n \in \mathbb{N}$ un entier. Montrer que l'idéal I^n a les même diviseurs premier que l'idéal I lui-même.

138. Soient I et J des idéaux de A. Montrer que $\mathrm{Rad}(IJ) = \mathrm{Rad}(I \cap J)$.

139. Soit A un anneau. Soient $P_i \in \mathrm{Spec}(A)$, $i = 1, \ldots n$, des idéaux premiers tels que $P_i \not\subseteq P_j$ lorsque $i \neq j$. Soit $I = \bigcap_{i=1}^{n} P_i$. Montrer que $\{P_1, \ldots, P_n\}$ est l'ensemble des diviseurs premiers minimaux de I. Est-ce encore vrai pour une infinité d'idéaux premiers?

140. Soit A noetherien. Soient I et J des idéaux de A tels que $I \subseteq J \subseteq \mathrm{Rad}(I)$. Montrer que

a. il existe un entier $n \in \mathbb{N}$ tel que $J^n \subseteq I$;

b. il existe un entier $n \in \mathbb{N}$ tel que $\mathrm{Rad}(I)^n \subseteq I$.

141. Soit A noetherien et soit I un idéal de A contenu dans le nilradical $\mathrm{Nil}(A)$ de A. Montrer qu'il existe un entier $n \in \mathbb{N}$ tel que $I^n = (0)$.

142. Soient A et B des anneaux. Déterminer les idéaux premiers minimaux de $A \times B$.

143. Soit A un anneau noetherien. Soit I un idéal de A et soient $P_1, \ldots, P_n$ les diviseurs premiers minimaux de I. Montrer qu'il existe des entiers $e_i \in \mathbb{N}$ tels que

$$\bigcap_{i=1}^{n} P_i^{e_i} \subseteq I.$$

§8

144. Soit $f : A \to B$ un morphisme d'anneaux intègres. Soient $a, b \in A$. Vrai ou faux :

a. a divise b implique que $f(a)$ divise $f(b)$;

b. $f(a)$ divise $f(b)$ implique que a divise b ;

c. a et b associés implique que $f(a)$ et $f(b)$ sont associés ;

d. $f(a)$ et $f(b)$ associés implique que a et b le sont ;

e. a irréductible implique $f(a)$ irréductible ;

f. $f(a)$ irréductible implique a irréductible ;

g. a premier implique $f(a)$ premier ;

h. $f(a)$ premier implique a premier ;

145. Soit A un anneau intègre et K son corps de fractions. Considérer A comme sous-anneau de K. Soient $a, b \in A$. Alors, b divise a dans A si et seulement si $\frac{a}{b} \in A$.

146. Soit A un anneau factoriel. Soient $a, b \in A$ tels que $\operatorname{pgcd}(a, b) = 1$. Y-a-t-il des $x, y \in A$ tels que $xa + yb = 1$?

147. Soit A un anneau factoriel et $S \subseteq A$ une partie multiplicative ne contenant pas 0. Soit $\mathcal{P}$ un système de représentants des irréductibles de A.

a. Montrer que $\mathcal{P}' = \{p \in \mathcal{P} \mid p \text{ ne divise aucun élément de } S\}$ est un système de représentants des irréductibles de $S^{-1}A$.

b. Montrer que $S^{-1}A$ est factoriel.

148. Soit A un anneau factoriel et K son corps de fractions.

a. Montrer qu'un élément irréductible P de A est irréductible dans $A[X]$.

b. Soit $P \in A[X]$ de contenu 1. Montrer que P est irréductible dans $A[X]$ lorsque P est irréductible dans $K[X]$.

c. Soit $\mathcal{P}_A$ un système de représentants des irréductibles de A. Soit $\mathcal{P}_{K[X]}$ un système de représentants des irréductibles de $K[X]$ tel que $\operatorname{cont}(P) = 1$ quel que soit $P \in \mathcal{P}_{K[X]}$. Montrer que $\mathcal{P} = \mathcal{P}_A \cup \mathcal{P}_{K[X]}$ est un système de représentants des irréductibles de $A[X]$.

149. (Critère d'Eisenstein) Soit A un anneau factoriel et $F \in A[X]$ de degré strictement positif et de contenu 1. Soit $a_i \in A$ tels que $F = a_n X^n + \cdots + a_1 X + a_0$. Supposons qu'il existe $p \in A$ irréductible tel que p ne divise pas a_n, p divise $a_{n-1}, \ldots, a_0$, et p^2 ne divise pas a_0. Montrer que F est irréductible dans $A[X]$.

150. Déterminer les décompositions en facteurs irréductibles de

a. 120 dans la localisation $\mathbb{Z}_{(2)}$ de $\mathbb{Z}$ en l'idéal premier (2) ;

b. 120 dans la localisation $\mathbb{Z}_2$ de $\mathbb{Z}$ par 2 ;

c. $X^2Y^2 - X^3 - Y^3 + XY$ dans $\mathbb{C}[X, Y]$;

d. $-X^2Y + X^2Z + XY^2 - XZ^2 - Y^2Z + YZ^2$ dans $\mathbb{Q}[X, Y, Z]$;

e. $Y^n - X$ dans $K[X, Y]$, K un corps ;

f. $X^n + Y^n - 1$ dans $K[X, Y]$, K un corps ;

g. $a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ dans l'anneau de polynômes $\mathbb{Z}[a_0, \ldots, a_n, X]$ en les indéterminées $a_0, \ldots, a_n, X$.

151. Soit A un anneau factoriel et a un élément de A. Déterminer l'anneau réduit associé au quotient A/Aa.

152.* Soit A l'anneau $\mathbb{R}[X, Y]/(X^2+Y^2-1)$. Montrer que A n'est pas factoriel.

153. Est-ce que le quotient d'un anneau factoriel est nécessairement factoriel ?

154. Soit A un anneau factoriel, K son corps de fractions et $\mathcal{P}$ un système de représentants de ses irréductibles. Montrer que le groupe quotient $K^\star/A^\star$ est un groupe abélien libre sur $\mathcal{P}$.

Chapitre 2

Modules

2.1 Modules et morphismes

Définition 2.1.1. Soit A un anneau. Un *A-module* est un groupe abélien $(M, +)$ muni d'une loi externe $\cdot$ de $A \times M$ dans M tel que

M1 $(a + b) \cdot m = a \cdot m + b \cdot m$;

M2 $a \cdot (m + n) = a \cdot m + a \cdot n$;

M3 $(a \cdot b) \cdot m = a \cdot (b \cdot m)$;

M4 $1 \cdot m = 1$;

quels que soient $a, b \in A$ et $m, n \in M$.

Exemple 2.1.2.
1. Lorsque A est un corps un A-module n'est rien d'autre qu'un A-espace vectoriel.
2. A^n est un A-module pour tout anneau A et pour tout entier non négatif n. Le A-module $A^0 = \{0\}$ est le *A-module nul*, noté par 0.

Comme dans le cas d'un anneau, on a, dans un module, des sommes indexées par des ensembles finis.

Rappelons que, pour un groupe abélien M, $\mathrm{End}(M)$ est l'anneau (non commutatif em général) des endomorphismes de M. Lorsque M est un A-module, on peut définir une application

$$\Phi \colon A \to \mathrm{End}(M)$$

par $\Phi(a)(m) = am$ pour $a \in A$ et $m \in M$. Effectivement, $\Phi(a)$ ainsi défini est bien un endomorphisme du groupe abélien M d'après **M2**. En outre, les conditions **M1**, **M3** et **M4** assurent que Φ est un morphisme d'anneaux.

Réciproquement, soit M un groupe abélien et $\Phi \colon A \to \mathrm{End}(M)$ un morphisme d'anneaux. On peut alors définir une loi externe sur M par

$$a \cdot m = \Phi(a)(m)$$

pour $a \in A$ et $m \in M$. Cette loi externe satisfait conditions **M1**, **M3** et **M4** car Φ est un morphisme d'anneaux. Elle satisfait **M2** puisque $\Phi(a)$ est un endomorphisme du groupe abélien M.

On a alors :

Proposition 2.1.3. *Soient A un anneau et M un groupe abélien. Une structure de A-module sur M équivaut à un morphisme d'anneau de A dans l'anneau des endomorphismes de M.* □

Exemple 2.1.4.
1. Soit M un groupe abélien. Il existe un unique morphisme Φ d'anneaux de $\mathbb{Z}$ dans $\mathrm{End}(M)$. Le groupe abélien M admet donc une unique structure de $\mathbb{Z}$-module. On a alors $0 \cdot m = 0$, $1 \cdot m = m$, $(n+1) \cdot m = n \cdot m + m$ et $(-n) \cdot m = -(n \cdot m)$ quel que soit $m \in M$ et $n \in \mathbb{N}$.

2. Soit $p \in \mathbb{Z}$ premier. Le groupe abélien $\mathbb{Z}/p\mathbb{Z}$ admet une structure de $\mathbb{Z}[i]$-module si et seulement si $p \equiv 1 \mod 4$.

Soit $f\colon A \to B$ un morphisme d'anneaux. Soit M un B-module. On vérifie facilement que l'on définit une structure de A-module sur M par

$$a \cdot m = f(a) \cdot m$$

quels que soient $m \in M$, $a \in A$. On désigne M muni de cette structure de A-module par ${}_AM$.

Définition 2.1.5. Soit $f\colon A \to B$ un morphisme d'anneaux. Soit M un B-module. Le A-module ${}_AM$ est le module *obtenu par restriction de scalaires.*

Exemple 2.1.6. ${}_{\mathbb{R}}\mathbb{C} = \mathbb{R}^2$.

Définition 2.1.7. Soient M et N des A-modules. Une application $f\colon M \to N$ est un *morphisme de A-modules* lorsque f est *A-linéaire*, c-à-d,

MM1 $f(m+n) = f(m) + f(n)$;

MM2 $f(a \cdot m) = a \cdot f(m)$; quels que soient $a \in A$ et $m, n \in M$.

Exemple 2.1.8.
1. Lorsque A est un corps, un morphisme de A-modules $f\colon M \to N$ n'est rien d'autre qu'une application A-linéaire de A-espaces vectoriels.

2. L'identité $\mathrm{id}_M\colon M \to M$ est un morphisme de A-modules pour tout A-module M.

3. Une matrice $m \times n$ à coefficients dans A détermine par la multiplication matricielle un morphisme de A-modules de A^n dans A^m.

4. Chaque morphisme de groupes abéliens est automatiquement un morphisme de $\mathbb{Z}$-modules.

Proposition 2.1.9. *Soient M, N et L des A-modules. Soient $f\colon M \to N$ et $g\colon N \to L$ des morphismes des A-modules. Alors, l'application composée $g \circ f$ est un morphisme de A-modules.*

Démonstration. Exercice. □

Définition 2.1.10. Un morphisme de A-modules $f\colon M \to N$ est un *isomorphisme* lorsqu'il existe un morphisme de A-modules $g\colon N \to M$ tel que $g \circ f = \mathrm{id}_M$ et $f \circ g = \mathrm{id}_N$. Les A-modules M et N sont alors *isomorphes*, noté par $M \cong N$, ou $M \cong_A N$ si on veut préciser qu'il s'agit d'un isomorphisme de A-modules. Un morphisme d'un A-module M dans lui-même est un *endomorphisme*. Un isomorphisme de M dans lui-même est un *automorphisme*.

Soient M et N des A-modules. On notera l'ensemble des morphismes de M dans un N par $\mathrm{Hom}_A(M,N)$. On définit une structure de A-module sur $\mathrm{Hom}_A(M,N)$ par

$$(f+g)(m) = f(m) + g(m) \quad \text{et} \quad (a \cdot f)(m) = a \cdot f(m)$$

pour $a \in A$, $m \in M$ et $f, g \in \mathrm{Hom}_A(M,N)$. Ce A-module est noté par $\mathrm{End}_A(M)$ lorsque $M = N$, c'est l'anneau des endomorphismes de M. En fait, $\mathrm{End}_A(M)$ est un sous-anneau de l'anneau $\mathrm{End}(M)$. Finalement, l'ensemble des automorphismes de M est noté par $\mathrm{Aut}_A(M)$, c'est le groupe multiplicatif de l'anneau $\mathrm{End}_A(M)$.

Définition 2.1.11. Soit M un A-module. Le *module dual* à M est le A-module $\mathrm{Hom}_A(M,A)$, noté par $M^\vee$.

2.2 Sous-modules

Définition 2.2.1. Soit M un A-module. Un *sous-A-module* de M est un sous-ensemble N de M tel que

SM1 $0 \in N$;

SM2 $x, y \in N$ implique $x + y \in N$;

SM3 $a \in A$ et $x \in N$ implique $a \cdot x \in N$.

Observons qu'un idéal d'un anneau A est exactement la même chose qu'un sous-A-module de A.

Lorsque A est un corps, un sous-A-module d'un A-module M est exactement la même chose qu'un sous-A-espace vectoriel de M.

La terminologie sous-module est justifiée car un sous-A-module est lui-même un A-module.

Proposition 2.2.2. *Soit $f\colon M \to N$ un morphisme de A-modules. Alors, $\ker(f)$ est un sous-A-module de M et $\mathrm{im}(f)$ est un sous-A-module de N.* □

Proposition 2.2.3. *Soient M un A-module et $S \subseteq M$ un sous-ensemble. Soit*

$$(S) = \{\sum_{i=1}^{n} a_i s_i \mid a_i \in A, s_i \in S \text{ et } n \in \mathbb{N}\}.$$

Alors, (S) est le plus petit sous-A-module de M contenant S. □

Définition 2.2.4. Soient M un A-module et $S \subseteq M$ un sous-ensemble. Le sous-A-module (S) de M est le sous-module *engendré* par S. Lorsque S est fini, disons $S = \{m_1, \ldots, m_n\}$, on notera (S) par $(m_1, \ldots, m_n)$. Si $S = \{m\}$, on notera (S) aussi par Am.

Définition 2.2.5. Soient M un A-module et $S \subseteq M$ un sous-ensemble. On dit que S est un *système générateur* ou une *famille génératrice* de M lorsque $M = (S)$, i.e., lorsque pour tout $m \in M$ il existe $a_i \in A$, $s_i \in S$, i parcourant un ensemble fini I, tels que

$$m = \sum_{i \in I} a_i s_i.$$

On dit que S est un *système libre* ou une *famille libre* lorsque, pour $a_i \in A$ et $s_i \in S$, i parcourant un ensemble fini I,

$$\sum_{i \in I} a_i s_i = 0$$

implique que $a_i = 0$ pour tout $i \in I$. Le sous-ensemble $S \subseteq M$ est un *système lié* ou une *famille liée* lorsque S n'est pas libre. On dit que S est une *base* de M si S est à la fois libre et générateur. Un A-module M est *libre* si M admet une base. Un A-module M est *libre de rang fini* si M admet une base fini.

Exemple 2.2.6.

1. Le A-module A^n est libre de base $\{e_1, \ldots, e_n\}$, quel que soit $n \in \mathbb{N}$, où $e_i = (e_{ij}) \in A^n$ est défini par $e_{ij} = \delta_{ij}$. En particulier, le A-module 0 est libre : l'ensemble vide $\emptyset$ en est une base.
2. Bien que $\mathbb{Z}$ soit libre en tant que $\mathbb{Z}$-module, le système $\{2, 3\}$ est générateur de $\mathbb{Z}$ sans que l'on puisse en extraire une base de $\mathbb{Z}$.
3. Le système $\{2\}$ dans $\mathbb{Z}$ est libre sans que l'on puisse le compléter en une base de $\mathbb{Z}$.
4. Il y a des modules qui n'ont pas de systèmes libres non vides : quel que soit s dans le $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, le système $\{s\}$ est lié. Effectivement, $6 \cdot s = 0$ quel que soit $s \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
5. Le A-module A/I n'est pas libre si $I \neq 0, A$.

Soient A un anneau et S un ensemble. On va construire un A-module libre dont S est une base. Soit $A^{(S)}$ l'ensemble des sommes formelles

$$\sum_{s \in S} a_s \cdot s$$

où les a_s appartiennent à A et sont nuls sauf un nombre fini des a_s. Deux de telles sommes $\sum a_s \cdot s$ et $\sum b_s \cdot s$ sont égales si et seulement si $a_s = b_s$ pour tout $s \in S$. On définit une structure de groupe abélien sur $A^{(S)}$ par

$$\sum_{s \in S} a_s \cdot s + \sum_{s \in S} b_s \cdot s = \sum_{s \in S} (a_s + b_s) \cdot s.$$

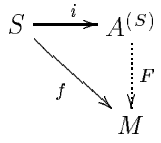
Ensuite définit-on une structure de A-module sur $A^{(S)}$ par

$$a \cdot \sum_{s \in S} a_s \cdot s = \sum_{s \in S} (a a_s) \cdot s.$$

Il est évident que S est alors une base $A^{(S)}$ ce qui montre que $A^{(S)}$ est un A-module libre.

Définition 2.2.7. Soient A un anneau et S un ensemble. Le *A-module* libre sur S est le A-module $A^{(S)}$. Ce module contient l'ensemble S comme base.

Propriété Universelle. *Soient A un anneau et S un ensemble. L'inclusion $i\colon S \to A^{(S)}$ est universelle parmi toutes les applications de S dans un A-module : pour tout A-module M et toute application $f\colon S \to M$ il existe un et un seul morphisme de A-module $F\colon A^{(S)} \to M$ tel que le diagramme suivant commute.*



Evidemment, chaque A-module M admet un système générateur S. Il suffit de prendre $S = M$. Les A-modules admettant un système générateur fini sont particulièrement intéressants.

Définition 2.2.8. Soit A un anneau. Un A-module M est de *type fini* si M admet un système générateur fini.

Exemple 2.2.9.

1. Le A-module A^n est de type fini, pour $n \in \mathbb{N}$.

2. Soit A un corps. Un A-module M est de type fini si et seulement si M est un A-espace vectoriel de dimension finie.

3. Le $\mathbb{Z}$-module $\mathbb{Q}$ n'est pas de type fini.

4. Un sous-A-module de type fini n'est pas forcément de type fini.

Proposition 2.2.10. *Soient A un anneau noetherien et M un A-module de type fini. Alors, chaque sous-A-module de M est de type fini.*

Démonstration. D'abord on réduit au cas $M = A^n$. Comme M est de type fini, il existe un morphisme surjectif $f\colon A^n \to M$. Soit $N \subseteq M$ un sous-A-module. Son image réciproque $f^{-1}(N)$ est un sous-A-module de A^n, et N est de type fini si $f^{-1}(N)$ l'est. Donc, il suffit de montrer que chaque sous-A-module de A^n est de type fini. Cela, on le montre pa récurrence.

Pour $n = 0$, l'assertion est triviale. Pour $n = 1$ c'est exactement la définition de noetheriennité. Supposons alors que tout sous-A-module de A^n est de type fini et montrons que tout sous-A-module de A^{n+1} l'est aussi. Soit $N \subseteq A^{n+1}$ un sous-A-module. Soit $p\colon A^{n+1} \to A^n$ la projection définie par $p(a_1, \ldots, a_{n+1}) = (a_1, \ldots, a_n)$. Comme $p(N)$ est un sous-module de A^n, il est de type fini, d'après l'hypothèse de récurrence. Il existe alors un système générateur fini $\{s_1, \ldots, s_k\}$ de $p(N)$. Soit $t_i \in N$ tel que $p(t_i) = s_i$, pour $i = 1, \ldots, k$. Le noyau de p est le sous-A-module $\{0\} \times A$ de A^{n+1}. Comme A est noetherien, le sous-A-module $N \cap (\{0\} \times A)$ est de type fini. Il existe alors $t_{k+1}, \ldots, t_l \in N \cap (\{0\} \times A)$ qui engendrent $N \cap (\{0\} \times A)$. J'affirme que $t_1, \ldots, t_l \in N$ engendrent N.

En effet, soit $x \in N$. Alors $p(x) \in p(N)$. Comme $s_1, \ldots, s_k$ engendrent $p(N)$ il existe $a_1, \ldots, a_k \in A$ tels que $p(x) = \sum_{i=1}^{k} a_i s_i$. Alors a-t-on

$$p(x - \sum_{i=1}^{k} a_i t_i) = p(x) - \sum_{i=1}^{k} a_i p(t_i) = p(x) - \sum_{i=1}^{k} a_i s_i = 0.$$

D'où $x - \sum_{i=1}^{k} a_i t_i \in \ker(p) \cap N = N \cap (\{0\} \times A)$. Comme $t_{k+1}, \ldots, t_l$ engendrent $N \cap (\{0\} \times A)$, il existe alors $a_{k+1}, \ldots, a_l \in A$ tels que

$$x - \sum_{i=1}^{k} a_i t_i = \sum_{i=k+1}^{l} a_i t_i,$$

c-à-d, $x = \sum_{i=1}^{l} a_i t_i$. □

2.3 Modules quotients

Soient M un A-module et N un sous-A-module de M. Comme la construction du quotient de M par N est analogue à celle du quotient d'un anneau par un idéal, on se contentera d'esquisser cette construction. Soit $\sim$ la relation sur M définie par

$$m \sim n \Leftrightarrow m - n \in N.$$

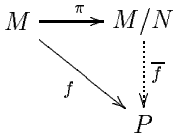
On vérifie facilement que $\sim$ est une relation d'équivalence. On notera l'ensemble des classes d'équivalence par M/N. Ensuite, on vérifie que la loi interne $+$ sur M en induit une sur M/N de façon à ce que M/N soit un groupe abélien, et que la loi externe $\cdot$ sur M en induit une sur M/N de façon à ce que M/N soit un A-module. De plus, l'application

$$\pi : M \longrightarrow N$$

définie par $\pi_N(m) = \overline{m}$ est un morphisme de A-modules.

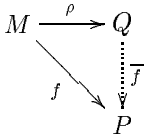
Définition 2.3.1. Soient M un A-module et N un sous-A-module de M. Le *quotient* de M par N est le couple $(M/N, \pi)$ consistant du *A-module quotient* M/N et du *morphisme de passage au quotient* π. Parfois on dira, par abus de langage, que M/N est le quotient.

Propriété Universelle. *Soient M un A-module et $N \subseteq M$ un sous-A-module. Le morphisme de passage au quotient $\pi : M \to M/N$ est universel d'ayant la propriété $\pi(N) = \{0\}$, c-à-d, pour tout A-module P et pour tout morphisme de A-modules $f : M \to P$ tel que $f(N) = \{0\}$, il existe un et un seul morphisme de A-modules $\overline{f} : M/N \to P$ faisant commuter le diagramme suivant.*



Démonstration. Exercice. □

Définition 2.3.2. Soit M un A-module et $N \subseteq M$ un sous-A-module. Un morphisme de A-modules $\rho : M \to Q$ est un *quotient de M par N* lorsque $\rho(N) = \{0\}$ et ρ est universel : pour tout A-module P et pour tout morphisme $f : M \to P$ tel que $f(N) = \{0\}$, il existe un unique morphisme de A-modules $\overline{f} : Q \to P$ faisant commuter le diagramme suivant :



Comme toujours, lorsque $\rho\colon M \to Q$ est un quotient de M par N, Q est isomorphe au quotient M/N.

Proposition 2.3.3. *Soit M un A-module et $N \subseteq M$ un sous-A-module. Un morphisme de A-modules $\rho\colon M \to Q$ est un quotient de M par N si et seulement si ρ est surjectif et* $\ker(\rho) = N$.

Un exemple important d'un quotient est le suivant. Soient A un anneau et $I \subseteq A$ un idéal. Lorsque M est un A-module, le sous-ensemble

$$IM = \{\sum_{i=1}^{n} x_i m_i \mid x_i \in I, m_i \in M \text{ et } n \in \mathbb{N}\}$$

est un sous-A-module de M. Le quotient M/IM est un A-module avec la propriété que $x \cdot \overline{m} = 0$ pour tout $x \in I$ et $\overline{m} \in M/IM$. Cela implique que M/IM admet une structure de A/I-module définie par

$$\overline{a} \cdot \overline{m} = \overline{am}$$

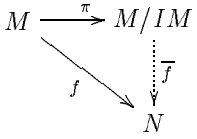
pour tout $a \in A$ et $m \in M$.

Exemple 2.3.4. Montrons que l'idéal $(2, X) \subseteq \mathbb{Z}[X]$ n'est pas principal. Soit $A = \mathbb{Z}[X]$, $I = (2, X)$ et $M = I$. On a $A/I \cong \mathbb{Z}/2\mathbb{Z}$. On va d'abord déterminer M/IM en tant que $\mathbb{Z}/2\mathbb{Z}$-module.

Observons que M en tant que $\mathbb{Z}$-module est libre de base $\{2, X, X^2, \dots\}$. Le sous-A-module IM est engendré par $(4, 2X, X^2)$. De ce fait, IM en tant que $\mathbb{Z}$-module est libre de base $\{4, 2X, X^2, X^3, \dots\}$. De ce fait, le quotient M/IM est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. En particulier, M/IM est de dimension 2 en tant que $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel.

Montrons ensuite que I n'est pas principal. Si I était principal, il devrait y avoir $m \in M$ engendrant M comme A-module. En particulier, m engendrait le quotient M/IM en tant que A-module. Par définition de la structure de A/I-module sur M/IM, m engendrait M/IM en tant que A/I-module. Mais A/I est un corps, donc cela impliquerait que la dimension de M/IM serait inférieure ou égale à 1. Contradiction avec ce qui précède.

Propriété Universelle. *Soient A un anneau et $I \subseteq A$ un idéal. Soit M un A-module. Le morphisme de passage au quotient $\pi\colon M \to M/IM$ est universel parmi tous les morphismes de A-modules f de M dans un A/I-module, c-à-d, pour tout A/I-module N et pour tout morphisem de A-modules $f\colon M \to N$ il existe un et un seul morphisme de A/I-modules $\overline{f}\colon M/IM \to N$ tel que le diagramme suivant soit commutatif.*



Démonstration. Exercice. □

Proposition 2.3.5. *Soit A un anneau et $I \subseteq A$ un idéal. Soit $f\colon M \to N$ un morphisme de A-modules. Alors, il existe un unique morphisme de A/I-modules*

$\overline{f}$: $M/IM \to N/IN$ *tel que le diagramme*

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\rho} \\ M/IM & \xrightarrow[\overline{f}]{} & N/IN \end{array}$$

commute, où les morphismes verticaux sont les passages au quotient.

Démonstration. Le morphisme composé $\rho \circ f$ de M dans N/IN est un morphisme de A-modules de M dans un A/I-module. D'après la propriété universelle, il existe un unique morphisme de A/I-modules $\overline{f}$: $M/IM \to N/IN$ tel que $\overline{f} \circ \pi = \rho \circ f$. □

Proposition 2.3.6. *Soit A un anneau et $I \subseteq A$ un idéal.*

1. *Soient f: $M \to N$ et g: $N \to P$ des morphismes de A-modules. Alors, $\overline{g \circ f} = \overline{g} \circ \overline{f}$.*
2. *Soit M un A-module. Alors, $\overline{\mathrm{id}_M} = \mathrm{id}_{M/IM}$.* □

Le passage du A-module M vers le A/I-module M/IM est le premier exemple de ce qu'on appelle *extension de scalaires*.

Exemple 2.3.7. Soit A un anneau non nul. Soient $r, s \in \mathbb{N}$. Montrons que $A^r \cong A^s$ si et seulement si $r = s$.

Evidemment, $A^r \cong A^s$ lorsque $r = s$. Supposons donc qu'il existe un isomorphisme f: $A^r \to A^s$. Comme A est non nul, il existe un idéal maximal m de A. D'après la proposition précédente, f induit un morphisme $\overline{f}$: $A^r/mA^r \to A^s/mA^s$. Or f est un isomorphisme, il existe donc un morphisme g: $A^s \to A^r$ tel que $f \circ g = \mathrm{id}$ et $g \circ f = \mathrm{id}$. Par conséquent, $\overline{f} \circ \overline{g} = \overline{f \circ g} = \overline{\mathrm{id}} = \mathrm{id}$ et $\overline{g} \circ \overline{f} = \mathrm{id}$. D'où $\overline{f}$ est un isomorphisme. On a $A^r/mA^r \cong (A/m)^r$ et $A^s/mA^s \cong (A/m)^s$. Donc, $(A/m)^r$ et $(A/m)^s$ sont isomorphes. Comme A/m est un corps, on a que $r = s$.

Définition 2.3.8. Soit A un anneau non nul. Soit M un A-module libre de rang fini. Le *rang* de M, ou plus précisément, le *A-rang* de M, est l'unique entier $r \in \mathbb{N}$, noté par $\mathrm{rang}(M) = \mathrm{rang}_A(M)$, tel que M soit isomorphe à A^r.

2.4 Localisation

On a vu que lorsque S est une partie multiplicative d'un anneau A on peut construire un anneau $S^{-1}A$ dans lequel les éléments de S sont inversibles. Dans ce paragraphe on va étendre cette construction aux A-modules.

Soient alors A un anneau et $S \subseteq A$ une partie multiplicative. Soit M un A-module. On définit une relation $\sim$ sur l'ensemble $M \times S$ par

$$(m, s) \sim (n, t) \Leftrightarrow \exists r \in S : rtm = rsn.$$

On vérifie que $\sim$ est une relation d'équivalence. On pose $S^{-1}M$ l'ensemble des classes d'équivalence de $\sim$. On note la classe d'un élément (m, s) par $\frac{m}{s}$. Puis, on définit une loi interne $+$ sur $S^{-1}M$ par

$$\frac{m}{s} + \frac{n}{t} = \frac{tm + sn}{st},$$

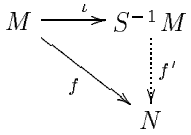
où $m, n \in M$, et $s, t \in S$. On vérifie que $S^{-1}M$ est alors un groupe abélien. Ensuite, on définit une loi externe $\cdot$ de $S^{-1}A \times S^{-1}M$ dans $S^{-1}M$ par

$$\frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st},$$

où $m \in M$, $a \in A$ et $s, t \in S$. On vérifie que $S^{-1}M$ est alors un $S^{-1}A$-module. De plus, on dispose d'une application ι de M dans $S^{-1}M$ définie par $\iota(m) = \frac{m}{1}$. Observons que ι est A-linéaire.

Définition 2.4.1. Soient A un anneau et $S \subseteq A$ une partie multiplicative. Soit M un A-module. Alors le A-module $S^{-1}M$ muni du morphisme ι est la *localisation* de M par S.

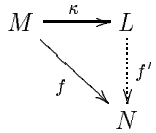
Propriété Universelle. *Soient S une partie multiplicative d'un anneau A et M un A-module. Le morphisme $\iota : M \to S^{-1}M$ est universel parmi tous les morphismes A-linéaires de M dans un $S^{-1}A$-module, c-à-d, pour tout $S^{-1}A$-module N et pour tout morphisme de A-modules $f : M \to N$ il exiset un et un seul morphisme de $S^{-1}A$-modules $f' : S^{-1}M \to N$ faisant commuter le diagramme suivant.*



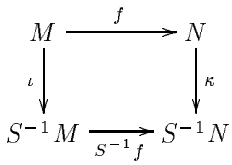
Démonstration. Exercice. □

Comme avant, on ne veut pas favoriser la construction de la localisation d'un module :

Définition 2.4.2. Soit A un anneau et $S \subseteq A$ multiplicative. Soit M un A-module et L un $S^{-1}A$-module. Soit $\kappa : M \to L$ un morphisme de A-modules. Le morphisme κ est une *localisation* de M par S lorsque pour tout $S^{-1}A$-module N et pour tout morphisme de A-modules $f : M \to N$ il existe un unique morphisme de $S^{-1}A$-modules $f' : L \to N$ tel que le diagramme suivant commute :



Proposition 2.4.3. *Soit A un anneau et $S \subseteq A$ multiplicative. Soit $f : M \to N$ un morphisme de A-modules. Alors, il existe un unique morphisme de $S^{-1}A$-modules $S^{-1}f : S^{-1}M \to S^{-1}N$ tel que le diagramme*



commute, où ι et κ sont les morphismes de localisation.

Proposition 2.4.4. *Soit A un anneau et $S \subseteq A$ multiplicative.*

1. *Soient $f\colon M \to N$ et $g\colon N \to P$ des morphismes de A-modules. Alors, $S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f$.*
2. *Soit M un A-module. Alors, $S^{-1}\mathrm{id}_M = \mathrm{id}_{S^{-1}M}$.* □

Passer d'un A-module à un $S^{-1}A$-module est le deuxième exemple de ce que l'on appelle extension de scalaires.

Proposition 2.4.5. *Soit A un anneau et $S \subseteq A$ multiplicative. Soit M un A-module et $N \subseteq M$ un sous-A-module. Soit $i\colon N \to M$ l'inclusion. Alors, $S^{-1}i\colon S^{-1}N \to S^{-1}M$ est injectif, et, en identifiant $S^{-1}N$ et son image dans $S^{-1}M$,*

$$(S^{-1}M)/(S^{-1}N) \cong_{S^{-1}A} S^{-1}(M/N).$$

Soit A un anneau intègre et $R = A\backslash\{0\}$ le sous-ensemble des éléments non nuls. Notons le corps de fractions $\mathrm{Frac}(A) = R^{-1}A$ de A par K. Soit M un A-module. Alors, $R^{-1}M$ est un K-module, i.e., un K-espace vectoriel, noté par M_K.

Exemple 2.4.6. Soit A un anneau intègre et K son corps de fractions. Alors, $(A^r)_K \cong K^r$. Effectivement, soit $i\colon A^n \to K^n$ l'inclusion. On montre que i est une localisation de A^n par R, où R est la partie multiplicative des réguliers de A. Soit M un K-module et $f\colon A^r \to M$ un morphisme de A-modules. Il faut montrer qu'il existe un unique morphisme de K-modules $g\colon K^r \to M$ tel que $g \circ i = f$.

Quant à l'unicité, supposons que $g\colon K^r \to M$ est un morphisme tel que $g \circ i = f$. Soit $(x_1, \ldots, x_r) \in K^r$. Il existe $s \in R$ tel que $sx_i \in A$ quel que soit i. Soit $a_i = sx_i \in A$. On a alors

$$g(x_1, \ldots, x_r) = \frac{1}{s} \cdot g(a_1, \ldots, a_r) = \frac{1}{s} \cdot f(a_1, \ldots, a_r).$$

D'où l'unicité de g.

Pour l'existence on utilise ce qui précède et définit une application $g\colon K^r \to M$ par $g(x_1, \ldots, x_n) = \frac{1}{s} \cdot f(a_1, \ldots, a_n)$, où $s \in R$ est tel que $a_i = sx_i \in A$. On vérifie que cette définition ne dépend pas de s et que g est un morphisme de K-modules tel que $g \circ i = f$.

Soit A un anneau intègre, K son corps de fractions et soit M un A-module libre de rang r. D'après l'exemple précédent, le K-espace vectoriel M_K est de dimension r. Cela nous permet d'étendre la notion du rang a tous les modules sur un anneau intègre :

Définition 2.4.7. Soient A un anneau intègre, K son corps de fraction et M un A-module. Le *rang* de M, ou pus précisément le *A-rang* de M, est la dimension du K-espace vectoriel M_K.

Exemple 2.4.8. Considérons le $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}^r$, où $n \in \mathbb{Z}$ est non nul. Alors, $\mathrm{rang}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}^r) = r$. Effectivement, on a

$$(\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}^r)_{\mathbb{Q}} \cong (\mathbb{Z}/n\mathbb{Z})_{\mathbb{Q}} \oplus (\mathbb{Z}^r)_{\mathbb{Q}}.$$

Mais $(\mathbb{Z}/n\mathbb{Z})_{\mathbb{Q}} \cong (\mathbb{Z}_{\mathbb{Q}})/((n\mathbb{Z})_{\mathbb{Q}}) = \mathbb{Q}/\mathbb{Q} = 0$ et $(\mathbb{Z}^r)_{\mathbb{Q}} \cong \mathbb{Q}^r$, d'où le résultat.

Proposition 2.4.9. *Soit A un anneau intègre et K son corps de fractions. Soit M un A-module de type fini. Alors, le rang de M est fini.*

Démonstration. Soit $S \subseteq M$ un système générateur de M. Soit $\iota : M \to M_K$ le morphisme de localisation, i.e., $\iota(m) = \frac{m}{1}$. Montrons que $\iota(S)$ est générateur du K-module M_K. Soit $\frac{m}{a} \in M_K$, i.e., $m \in M$ et $a \in A$, $a \neq 0$. Comme S engendre M, il existe $s_1, \ldots, s_n \in S$ et $a_1, \ldots, a_n \in A$ tels que $m = \sum a_i s_i$. Par conséquent,

$$\frac{m}{a} = \frac{1}{a} \cdot \iota(m) = \frac{1}{a} \cdot \iota(\sum a_i s_i) = \sum \frac{a_i}{a} \cdot \frac{s_i}{1}.$$

Ce qui montre que $\iota(S)$ engendre M_K. Or K est un corps et M_K est donc un K-espace vectoriel admettant un système générateur fini. D'où M_K est de dimension finie, i.e., $\mathrm{rang}(M) = \dim(M_K) < \infty$. □

Soit A un anneau et $s \in A$. Soit $S \subseteq A$ la partie multiplicative engendrée par s. Rappelons que A_s est la localisation $S^{-1}A$ de A par s. Soit M un A-module. On note la localisation $S^{-1}M$ de M par S par M_s.

Exemple 2.4.10. Soit $A = \mathbb{Z}$, $s \in \mathbb{Z}$ et $M = \mathbb{Z}/s\mathbb{Z}$. Alors, $M_s = \{0\}$. Effectivement, $sm = 0$ dans M, quel que soit $m \in M$. D'où $\frac{m}{s^n} = 0$ dans M_s quels que soient $m \in M$, $n \in \mathbb{N}$.

Soit A un anneau et $P \subseteq A$ un idéal premier. Soit S la partie multiplicative $A \backslash P$. Rappelons que la localisation A_P de A en P est l'anneau $S^{-1}A$. Soit M un A-module. Alors, $S^{-1}M$ est un A_P-module. On note ce module par M_P.

Définition 2.4.11. Soit A un anneau et M un A-module. Rappelons que $\mathrm{Spec}(A)$ est l'ensemble des idéaux premiers de A. On définit le *support de* M, noté par $\mathrm{supp}(M)$ ou $\mathrm{supp}_A(M)$, par

$$\mathrm{supp}(M) = \{P \in \mathrm{Spec}(A) \mid M_P \neq \{0\}\}.$$

Proposition 2.4.12. *Soit A un anneau et M un A-module. Alors,* $\mathrm{supp}(M) = \emptyset$ *si et seulement si* $M = \{0\}$.

Démonstration. Evidemment, le support de M est vide lorsque $M = 0$. Réciproquement, supposons que M est un A-module de support vide. Montrons que $M = \{0\}$. Soit $m \in M$. On a l'annulateur

$$\mathrm{Ann}(m) = \{a \in A \mid am = 0\}$$

de m qui est un idéal de A. Si $m \neq 0$, alors $\mathrm{Ann}(m) \neq A$. En particulier, il existe un idéal premier P contenant $\mathrm{Ann}(m)$. Or $M_P = \{0\}$ implique qu'il existe $s \in A \backslash P$ tel que $sm = 0$. On a alors $s \in \mathrm{Ann}(m)$ et $s \notin P$. Contradiction. □

2.5 Suites exactes

Définition 2.5.1. Soit A un anneau. Une suite de morphismes de A-modules

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \longrightarrow \cdots$$

est *exacte* lorsque $\ker(f_i) = \mathrm{im}(f_{i-1})$ pour tout i.

Exemple 2.5.2. 1. La suite $0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$ est exacte.

2. La suite $0 \longrightarrow M \xrightarrow{f} N$ est exacte si et seulement si f est injectif.

3. La suite $M \xrightarrow{f} N \longrightarrow 0$ est exacte si et seulement si f est surjectif.

4. La suite $0 \longrightarrow M \xrightarrow{f} N \longrightarrow 0$ est exacte si et seulement si f est un isomorphisme.

5. Soient M et N des A-modules. Soient $i\colon M \to M \oplus N$ et $p\colon M \oplus N \to N$ définis par $i(m) = m \oplus 0$ et $p(m \oplus n) = n$. Alors la suite

$$0 \longrightarrow M \xrightarrow{i} M \oplus N \xrightarrow{p} N \longrightarrow 0$$

est exacte.

6. Soit M un A-module. M est de type fini si et seulement s'il existe une suite exacte $A^n \longrightarrow M \longrightarrow 0$.

Définition 2.5.3. Soit A un anneau. Une *suite exacte courte* est une suite exacte de morphismes de A-modules du type

$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0 .$$

Proposition 2.5.4. *Soit A un anneau et*

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

une suite exacte courte de A-modules. Les conditions suivantes sont équivalentes :

1. *Il existe un morphisme $s\colon P \to N$ tel que $g \circ s = \mathrm{id}_P$.*
2. *Il existe des morphismes $s\colon P \to N$ et $r\colon N \to M$ tels que $s \circ g + f \circ r = \mathrm{id}_N$.*
3. *Il existe un morphisme $r\colon N \to M$ tel que $r \circ f = \mathrm{id}_M$.*
4. *Le sous-A-module $f(M)$ de N admet un supplémentaire.*

Démonstration. $1 \Rightarrow 2$: Soit $s\colon P \to N$ tel que $g \circ s = \mathrm{id}_P$. Considérer $id_N - s \circ g\colon N \to N$. Comme $g \circ (id_N - s \circ g) = g - g = 0$, le morphisme $\mathrm{id}_N - s \circ g$ envoie N dans l'image de f. Or f est injectif, donc il existe un morphisme $r\colon N \to M$ tel que $f \circ r = \mathrm{id}_N - s \circ g$.

$2 \Rightarrow 3$: Soit $s\colon P \to N$ et $r\colon N \to M$ des morphismes tels que $s \circ g + f \circ r = \mathrm{id}_N$. On a $f \circ (r \circ f) = (f \circ r) \circ f = (\mathrm{id}_N - s \circ g) \circ f) = f$. Or f est injectif, donc $r \circ f = \mathrm{id}_M$.

$3 \Rightarrow 4$: Soit $Q = \ker(r)$. Alors, $Q \cap f(M) = \{0\}$. En effet, si $n \in Q \cap f(M)$, il existe $m \in M$ tel que $f(m) = n$. D'où $0 = r(n) = (r \circ f)(m) = m$, donc $n = 0$. De plus, $Q + f(M) = N$. En effet, soit $n \in N$. Soit $q = n - (f \circ r)(n)$. On a $r(q) = r(n) - r \circ (f \circ r)(n) = r(n) - r(n) = 0$, i.e., $q \in Q$. Comme $(f \circ r)(n) \in f(M)$, on a que $n \in Q + f(M)$.

$4 \Rightarrow 1$: Soit $Q \subseteq N$ un sous-A-module tel que $N = Q \oplus f(M)$. Montrons que la restriction g' de g à Q est un isomorphisme. En effet, g' est surjectif car $g'(Q) = g(Q) = g(Q + \ker(g)) = g(Q + f(M)) = g(N) = P$. De plus, g' est injectif, car $\ker(g') = Q \cap \ker(g) = Q \cap f(M) = \{0\}$. Par conséquent, g' est un isomorphisme. Soit $s\colon P \to Q$ l'application réciproque. Considérer s comme morphisme dans N. On a alors $g \circ s = \mathrm{id}_P$. □

Définition 2.5.5. On appelle une telle suite *scindée*.

Exemple 2.5.6. Le 5 de l'exemple ci-dessus est une suite scindée.

Proposition 2.5.7. *Soit A un anneau et*

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

une suite exacte courte de A-modules, où P est libre. Alors, la suite est scindée. En particulier, $N \cong M \oplus P$.

Démonstration. Soit $S \subseteq P$ une base de P. Définir un morphisme de A-modules $s\colon P \to N$ par $s(x) \in N$ tel que $g(s(x)) = x$. Alors, $g \circ s = \mathrm{id}_P$, i.e., la suite est scindée. □

Proposition 2.5.8. *Soit A un anneau et $S \subseteq A$ multiplicative. Soit $f\colon M \to N$ un morphisme de A-modules. Alors,*

$$\ker(S^{-1}f) = S^{-1}\ker(f) \text{ et } \mathrm{im}(S^{-1}f) = S^{-1}\mathrm{im}(f).$$

Démonstration. Pour $\frac{m}{s} \in S^{-1}M$, son image par $S^{-1}f$ est l'élément $\frac{f(m)}{s}$ de $S^{-1}N$. D'où l'égalité $\mathrm{im}(S^{-1}f) = S^{-1}\mathrm{im}(f)$ et l'inclusion $\ker(S^{-1}f) \supseteq S^{-1}\ker(f)$. Pour montrer que $\ker(S^{-1}f) \subseteq S^{-1}\ker(f)$ soit $\frac{m}{s} \in \ker(S^{-1}f)$. Comme $\frac{f(m)}{s} = 0$, il existe $t \in S$ tel que $tf(m) = 0$ dans N. Alors, $tm \in \ker(f)$ et $\frac{m}{s} = \frac{tm}{ts} \in S^{-1}\ker(f)$. □

Corollaire 2.5.9. *Soient A un anneau et $S \subseteq A$ une partie multiplicative. Soit*

$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0$$

une suite exacte courte de A-modules. Alors, la suite courte induite par localisation

$$0 \longrightarrow S^{-1}M_1 \xrightarrow{S^{-1}f_1} S^{-1}M_2 \xrightarrow{S^{-1}f_2} S^{-1}M_3 \longrightarrow 0$$

est exacte. □

Corollaire 2.5.10. *Soit A un anneau intègre. Soit*

$$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0$$

une suite exacte courte. Alors, $\mathrm{rang}(M_2) = \mathrm{rang}(M_1) + \mathrm{rang}(M_3)$.

2.6 Modules de torsion

Opposé aux modules libres sont les modules de torsion. On s'interessera dans ce paragraphe à la notion de torsion.

Définition 2.6.1. Soient A un anneau et M un A-module. Un élément m de M est dit *de A-torsion*, ou *de torsion* tout court, s'il existe un élément régulier $a \in A$ tel que $am = 0$.

Exemple 2.6.2.
1. Tous les élément du $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$, n un entier non nul, sont de $\mathbb{Z}$-torsion. Mais aucun entre eux, sauf 0, n'est de $\mathbb{Z}/n\mathbb{Z}$-torsion.
2. Dans un A-module libre 0 est le seul élément de A-torsion.

Proposition 2.6.3. *Soient A un anneau et M un A-module. Le sous-ensemble de M des éléments de A-torsion est un sous-A-module.*

Démonstration. Soit $R \subseteq A$ l'ensemble des éléments réguliers de A. Alors, le sous-ensemble des éléments de A-torsion est le noyau du morphisme $M \to R^{-1}M$, donc est un sous-A-module de M. □

Définition 2.6.4. Soient A un anneau et M un A-module. Le sous-A-module de M des éléments de A-torsion est appelé le *sous-module de torsion* de M, noté par M_{tors}. Lorsque $M_{\text{tors}} = M$ on dit que M est un *module de torsion*. On dit que M est *sans torsion* si $M_{\text{tors}} = 0$.

Exemple 2.6.5.
1. Le sous-module de torsion du $\mathbb{Z}$-module $M = \mathbb{Z}^r \oplus \mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n^{e_n}\mathbb{Z}$ est $M_{\text{tors}} = \mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n^{e_n}\mathbb{Z}$.
2. Les modules libres sont sans torsion.

Proposition 2.6.6. *Soit M un A-module. On a*

1. *$(M_{\text{tors}})_{\text{tors}} = M_{\text{tors}}$, i.e., M_{tors} est un module de torsion ;*
2. *$(M/M_{\text{tors}})_{\text{tors}} = 0$, i.e., M/M_{tors} est sans torsion.*

Démonstration. 1. L'inclusion $\subseteq$ est évidente. Pour montrer l'autre inclusion, soit $m \in M_{\text{tors}}$. Il existe $s \in A$ régulier tel que $sm = 0$ dans M. Mais M_{tors} est un module lui-même et $m \in M_{\text{tors}}$ avec $sm = 0$ dans M_{tors}, c-à-d, $m \in (M_{\text{tors}})_{\text{tors}}$.

2. Soit $x \in M/M_{\text{tors}}$ de A-torsion. Il existe donc $s \in A$ régulier tel que $sx = 0$ dans M/M_{tors}. Soit $m \in M$ tel que sa classe modulo M_{tors} $\overline{m}$ soit égale à x. Alors, $\overline{sm} = s \cdot \overline{m} = sx = 0$. D'où, $sm \in M_{\text{tors}}$. Cela veut dire qu'il existe $s' \in A$ régulier tel que $s'(sm) = 0$ dans M. Mais $ss' \in A$ est régulier et $(ss')m = s(s'm) = 0$, donc $m \in M_{\text{tors}}$. Par conséquent, $x = \overline{m} = 0$ dans M/M_{tors}. □

L'interêt de la proposition précédente est que l'on a pour tout A-module M une suite exacte

$$0 \longrightarrow T \longrightarrow M \longrightarrow L \longrightarrow 0 \ ,$$

où $T = M_{\text{tors}}$ et L est le quotient de M par M_{tors}. D'après la proposition précédente, tout A-module M est une extension d'un module sans torsion L par un module de torsion T.

Proposition 2.6.7. *Soit A un anneau principal. Soit L un A-module de type fini sans torsion. Alors, L est libre.*

Démonstration. Soit K le corps de factions de A. Comme L est de type fini, le K-espace vectoriel L_K est de dimension finie. Soit $\{v_1, \ldots, v_n\}$ une base de L_K. Considérer L comme sous-A-module de L_K. Soit $S \subseteq L$ un système générateur fini. Tout élément $s \in S$ s'écrit comme $s = \sum_{i=1}^{n} \lambda_i v_i$, où $\lambda_i \in K$. Il existe $a_s \in A$, $a_s \neq 0$ tel que $a_s \lambda_i \in A$ quel que soit i. Soit $a = \prod_{s \in S} a_s$. Alors, $a \neq 0$ et $aL \subseteq (v_1, \ldots, v_n)$. Autrement dit, L est contenu dans le sous-A-module de L_K engendré par $\{\frac{v_1}{a}, \ldots, \frac{v_n}{a}\}$. Ce dernier sous-module est libre de rang n car $\{v_1, \ldots, v_n\}$ est une base de L_K. D'après Exercice 180, L peut être engendré par n éléments $w_1, \ldots, w_n$. Regardons le morphisme de A-modules

$$f \colon A^n \longrightarrow L$$

défini par $f(e_i) = w_i$ quel que soit i. Comme $\{w_1, \ldots, w_n\}$ est générateur, f est surjectif. Montrons que f est aussi injectif. Le morphisme K-linéaire induit f_K est un morphisme de K^n dans L_K. De plus, f_K est surjectif et K^n et L_K ont la même dimension. Par conséquent, f_K est injectif. Il s'ensuit que f est injectif et donc que f est un isomorphisme. □

Théorème 2.6.8. *Soit A un anneau principal. Soit M un A-module de type fini. Soit r le rang de M. Alors, il existe un A-module de torsion T tel que M soit isomorphe à la somme directe $T \oplus A^r$. De plus, T est un A-module de type fini.*

Démonstration. Soit T le module de torsion M_{tors} de M. Soit L le quotient de M par T. Alors, L est de type fini et sans torsion. D'après la proposition précédente, L est un A-module libre. Comme $M_K \cong L_K$, où K désigne le corps de fractions de A, L est libre de rang r. On a alors une suite exacte courte

$$0 \longrightarrow T \longrightarrow M \longrightarrow A^r \longrightarrow 0 \,.$$

Une telle suite est toujours scindée, en particulier, M est isomorphe à $T \oplus A^r$. On en déduit également que T est un quotient de M par A^r et donc que T est de type fini. □

Dans la suite de cette Section on étudiera les modules de torsion de type fini sur un anneau principal. Soit désormais A un anneau principal. Soit T un A-module de torsion et de type fini. Il existe alors un entier $n \in \mathbb{N}$ et un morphisme surjectif $f \colon L \to T$, où L est libre de rang n. Autrement dit, T est isomorphe au quotient d'un module libre L de rang n par un sous-A-module, à savoir $M = \ker(f)$. Le module M est tel que le quotient L/M est de torsion.

Théorème 2.6.9. *Soit A un anneau principal. Soit L un A-module libre de rang n. Soit M un sous-A-module de L tel que le quotient L/M soit de torsion. Alors, il existe une base $\{e_1, \ldots, e_n\}$ de L et il existe $d_1, \ldots, d_n \in A$ tels que*

1. *M soit engendré par $\{d_1 e_1, \ldots, d_n e_n\}$, et*
2. *d_i divise d_{i+1} pour $i = 1, \ldots, n-1$.*

De plus, si une base $\{e'_1, \ldots, e'_n\}$ de L et $d'_1, \ldots, d'_n \in A$ satisfont également conditions 1 et 2, alors d'_i et d_i sont associés, quel que soit i.

Démonstration. Par récurrence sur n. Si $n = 0$, l'énoncé est trivial. Supposons l'assertion est vraie au rang $n-1$, où $n \in \mathbb{N}$, $n > 1$. Soit L un A-module libre de rang n et $M \subseteq L$ un sous-A-module tel que L/M soit de torsion.

Soit $f\colon L \to A$ un morphisme de A-module. L'image directe $f(M)$ est alors un idéal de A. Comme A est noetherien, il existe, d'après Zorn, un morphisme $f\colon L \to A$ tel que $f(M)$ soit maximal. Comme A est principal, il existe $d_1 \in A$ tel que $f(M) = Ad_1$. Soit $m_1 \in M$ tel que $f(m_1) = d_1$.

On montre qu'il existe $e_1 \in L$ tel que $m_1 = d_1e_1$. On montre cela en montrant que $g(m_1)$ est divisible par d_1 pour tout morphisme $g\colon L \to A$. Soit $g\colon L \to A$ donc un morphisme. Montrons que $g(m_1)$ est contenue dans $f(M)$. Soit $c = g(m_1)$, et soit b un générateur de l'idéal $Ad_1 + Ac$. Il existe alors $x, y \in A$ tels que $b = xd_1 + yc$. Considérons le morphisme $h = xf + yg\colon L \to A$. Comme $h(m_1) = b$, l'imegae directe $h(M)$ contient Ab qui contient Ad_1. Par construction de f, $h(M) = f(M)$. En particulier, $b \in f(M)$, d'où $Ad_1 + Ac = Ab \subseteq f(M) = Ad_1$ et donc $c \in Ad_1$.

Par ce qui précède, il existe $e_1 \in L$ tel que $m_1 = d_1e_1$. Comme $f(m_1) = d_1$, on a que $d_1f(e_1) = f(d_1e_1) = f(m_1) = d_1$, i.e., $f(e_1) = 1$.

Montrons que L est somme directe de Ae_1 et $\ker(f)$. Soit $v \in Ae_1 \cap \ker(f)$. Alors, $v = ae_1$ pour certain $a \in A$. Mais aussi $0 = f(v) = f(ae_1) = a$. D'où $v = 0$, ce qui montre que $Ae_1 \cap \ker(f) = \{0\}$. Puis on montre que $Ae_1 + \ker(f) = L$. Soit $v \in L$. On écrit $v = f(v)e_1 + (v - f(v)e_1)$, et on a bien-sûr $f(v)e_1 \in Ae_1$ et $v - f(v)e_1 \in \ker(f)$. Par conséquent, $L = Ae_1 \oplus \ker(f)$.

De même, M est somme directe de Am_1 et $M \cap \ker(f)$. En effet, on a $Am_1 \cap (M \cap \ker(f)) \subseteq Ae_1 \cap \ker(f) = \{0\}$. De plus, lorsque $v \in M$, on a $f(v) \in f(M) = Ad_1$. D'où $v \in Am_1 + (M \cap \ker(f))$.

Comme $\ker(f)$ est libre de rang $n-1$ et $M \cap \ker(f)$ est un sous-module tel que $\ker(f)/(M \cap \ker(f))$ soit de torsion, on a, par récurrence, une base $e_2, \ldots, e_n \in \ker(f)$ et $d_2, \ldots, d_n \in A$ tels que

1. $M \cap \ker(f)$ est engendré par $\{d_2e_2, \ldots, d_ne_n\}$, et
2. d_i divise d_{i+1} pour $i = 2, \ldots, n-1$.

Il suit de la somme directe $L = Ae_1 \oplus \ker(f)$ que $\{e_1, \ldots, e_n\}$ est une base de L. Comme $M = Am_1 + (M \cap \ker(f))$, il suit que M est engendré par $\{d_1e_1, \ldots, d_ne_n\}$. On montre encore que d_1 divise d_2. Soit $g\colon L \to A$ le morphisme défini par $g(e_i) = 0$ pour $i > 2$ et $g(e_1) = g(e_2) = 1$. On a alors, $d_1, d_2 \in g(M)$. En particulier, $f(M) \subseteq g(M)$. par maximalité de f, $f(M) = g(M)$, i.e., $d_2 \in f(M) = Ad_1$ d'où d_1 divise d_2. Ceci montre que les conditions 1 et 2 sont satisfaites.

On montre facilement la dernière assertion. □

2.7 Produits tensoriels

Définition 2.7.1. Soit A un anneau et soient M, N et P des A-modules. Une application $f\colon M \times N \to P$ est *A-bilinéaire*, où *bilinéaire*, lorsque $f(am + a'm', n) = af(m,n) + a'f(m',n)$ et $f(m, an + a'n') = af(m,n) + a'f(m,n')$ quels que soient $m, m' \in M$, $n, n' \in N$ et $a, a' \in A$.

Soit $f\colon M \times N \to P$ une application A-bilinéaire. Soit $n \in N$ fixé. L'application de M dans P qui envoie m sur $f(m,n)$ est un morphisme de A-modules.

En particulier, $f(0,n)=0$ quel que soit $n\in N$. De même, $f(m,0)=0$ quel que soit $m\in M$.

Exemple 2.7.2. 1. La loi multiplicative $\cdot\colon A\times A\to A$ est A-bilinéaire.

2. L'application nulle de $M\times N$ dans P est A-bilinéaire.

3. Soient $a,b\in\mathbb{Z}$ premiers entre eux. L'application nulle de $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$ dans un $\mathbb{Z}$-module P est la seule application bilinéaire de $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$ dans P. En effet, soit $(m,n)\in\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$. Soit $c\in\mathbb{Z}$ tel que $ac=1$ dans $\mathbb{Z}/b\mathbb{Z}$. Alors, $f(m,n)=f(m,acn)=af(m,cn)=f(am,cn)=f(0,cn)=0$.

Soient M et N des A-modules. On va montrer qu'il existe une application bilinéaire universelle de $M\times N$ dans un A-module P :

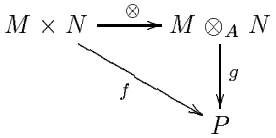
Soit L le A-module libre $A^{(M\times N)}$. Soit $b\colon M\times N\to L$ l'application définie par $b(m,n)=(m,n)$. On va rendre b A-bilinéaire en quotientant par un sous-A-module de L : Soit $B\subseteq L$ le sous-A-module engendré par les éléments

$$(am+a'm',n)-a(m,n)-a'(m',n),\ \ (m,an+a'n')-a(m,n)-a'(m,n'),$$

où $m,m'\in M$, $n,n'\in N$ et $a,a'\in A$. Soit $\pi\colon L\to L/B$ le morphisme de passage au quotient. Alors, $\pi\circ b\colon M\times N\to L/B$ est A-bilinéaire. On note le quotient L/B par $M\otimes_A N$ et l'image d'un couple (m,n) dans $M\otimes_A N$ par $m\otimes n$.

Définition 2.7.3. Soient M et N des A-modules. Le A-module $M\otimes_A N$ est le *produit tensoriel* de M et N. Un élément de $M\otimes_A N$ s'appelle un *tenseur*. Un élément du type $m\otimes n$ est un *tenseur simple*.

Propriété Universelle. *Soient M et N des A-modules. L'application $\otimes$ A-bilinéaire de $M\times N$ dans $M\otimes_A N$ qui envoie (m,n) sur $m\otimes n$ est universelle, c-à-d, pour tout A-module P et pour toute application A-bilinéaire $f\colon M\times N\to P$ il existe un unique morphisme de A-modules $g\colon M\otimes_A N\to P$ tel que le diagramme suivant commute :*



Démonstration. Soit $f\colon M\times N\to P$ une application A-bilinéaire. D'après la propriété universelle du A-module libre, il existe un morphisme de A-modules $F\colon L\to P$ tel que $F(m,n)=f(m,n)$ quel que soit $(m,n)\in M\times N$. Comme f est A-bilinéaire,

$$\begin{aligned}F((am+a'm',n)-a(m,n)-a'(m',n))&=\\&=F(am+a'm',n)-aF(m,n)-a'F(m',n)=\\&=f(am+a'm',n)-af(m,n)-a'f(m',n)=0\end{aligned}$$

et de même $F((m,an+a'n')-a(m,n)-a'(m,n'))=0$ quels que soient $m,m'\in M$, $n,n'\in N$ et $a,a'\in A$. Par conséquent, $F(B)=\{0\}$. D'après la propriété universelle su quotient, il existe un morphisme de A-modules $g\colon M\otimes_A N\to P$ tel que $g(m\otimes n)=f(m,n)$ quel que soit $(m,n)\in M\times N$. Cela montre l'existence de g.

Montrons ensuite l'unicité de g. Soit $g' : M \otimes_A N \to P$ aussi un morphisme de A-modules tel que $g'(m \otimes n) = f(m,n)$. On a alors un morphisme de A-modules $g' \circ \pi : L \to P$ tel que $(g' \circ \pi)(m,n) = f(m,n)$ quel que soit $(m,n) \in M \times N$. Or, $F : L \to P$ satisfait aussi $F(m,n) = f(m,n)$ quel que soit $(m,n) \in M \times N$. D'après l'unicité dans la propriété universelle du A-module libre L, $g' \circ \pi = F$. Or, $g : M \otimes_A N \to P$ satisfait aussi $g \circ \pi = F$. D'après l'unicité dans la propriété universelle du quotient, $g' = g$, ce qui montre l'unicité de g. □

Exemple 2.7.4. Soient $a, b \in \mathbb{Z}$ premiers entre eux. Alors, $\mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} = 0$. En effet, on a vu que toute application $\mathbb{Z}$-bilinéaire de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ dans n'importe quel $\mathbb{Z}$-module P est l'application nulle. Par conséquent, l'application nulle $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \to 0$ est universelle, i.e., $\mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} = 0$.

Proposition 2.7.5. *Soit M un A-module. Alors, $A \otimes_A M \cong M$.*

Démonstration. Soit $\beta : A \times M \to M$ l'application définie par $\beta(a,m) = am$. Evidemment, β est A-bilinéaire. On montre que β est universel pour pouvoir conclure que $A \otimes_A M \cong M$. Soit $f : A \times M \to P$ une application A-bilinéaire. Lorsque $g : M \to P$ est un morphisme de A-modules tel que $(g \circ \beta)(a,m) = f(a,m)$ quel que soit $(a,m) \in A \times M$, alors on a forcément $g(m) = (g \circ \beta)(1,m) = f(1,m)$. Ce qui montre l'unicité de g. Pour en montrer l'existence, on définit $g : M \to P$ par $g(m) = f(1,m)$. Alors, g est un morphisme de A-modules et $(g \circ \beta)(a,m) = g(am) = ag(m) = af(1,m) = f(a,m)$ quel que soit $(a,m) \in A \times M$. Cela montre l'existence. □

Proposition 2.7.6. *Soient M et N des A-modules. Alors, $M \otimes_A N \cong N \otimes_A M$.*

Démonstration. Exercice. □

Proposition 2.7.7. *Soient M, N et P des A-modules. Alors,*

$$M \otimes_A (N \oplus P) \cong_A (M \otimes_A N) \oplus (M \otimes_A P).$$

Démonstration. Montrons que $(M \otimes_A N) \oplus (M \otimes_A P)$ satisfait la propriété universelle du produit tensoriel de M et $N \oplus P$. Soit

$$\beta : M \times (N \oplus P) \to (M \otimes_A N) \oplus (M \otimes_A P)$$

définie par $\beta(m, n \oplus p) = (m \otimes n) \oplus (m \otimes p)$. On vérifie facilement que β est A-bilinéaire. Pour montrer que β est universelle, soit $\gamma : M \times (N \oplus P) \to Q$ une application A-bilinéaire. Considérons N et P comme sous-A-modules de la somme directe $N \oplus P$. On a alors deux applications A-bilinéaires $\gamma_1 = \gamma_{|M \times N}$ et $\gamma_2 = \gamma_{|M \times P}$. D'après la propriété universelle du produit tensoriel, il existe des morphismes de A-modules $g_1 : M \otimes_A N \to Q$ et $g_2 : M \otimes_A P \to Q$ tels que $g_1(m,n) = \gamma(m \otimes n)$ et $g_2(m,p) = \gamma(m \otimes p)$ quels que soient $m \in M$, $n \in N$ et $p \in P$. Le morphisme de A-modules $g : (M \otimes_A N) \oplus (M \otimes_A P) \to Q$ défini par $g((m \otimes n) \oplus (m' \otimes p)) = g_1(m \otimes n) + g_2(m' \otimes p)$ satisfait alors $g \circ \beta = \gamma$. L'unicité de g se montre facilement. Par conséquent, β est universelle et donc en particulier $(M \otimes_A N) \oplus (M \otimes_A P)$ est isomorphe à $M \otimes_A (N \oplus P)$. □

Proposition 2.7.8. *Soit A un anneau et $I \subseteq A$ un idéal. Soient M et N des A-modules. Alors,*

$$(M \otimes_A N)/I(M \otimes_A N) \cong_{A/I} (M/IM) \otimes_{A/I} (N/IN).$$

Démonstration. Soit $\beta\colon M \times N \to (M \otimes_A N)/I(M \otimes_A N)$ l'application A-bilinéaire définie par $\beta(m,n) = \pi(m \otimes n)$ où π est le morphisme de passage au quotient de $M \otimes_A N$ par $I(M \otimes_A N)$. Comme $\beta(m,n) = 0$ lorsque $m \in IM$ ou $n \in IN$, on a une application

$$\overline{\beta}\colon (M/IM) \times (N/IN) \longrightarrow (M \otimes_A N)/I(M \otimes_A N)$$

définie par $\overline{\beta}(\overline{m},\overline{n}) = \beta(m,n)$. Evidemment, $\overline{\beta}$ est A-bilinéaire. On montre facilement que $\overline{\beta}$ est universelle et donc que $(M \otimes_A N)/I(M \otimes_A N)$ est isomorphe à $(M/IM) \otimes_{A/I} (N/IN)$. □

Proposition 2.7.9. *Soit A un anneau et $S \subseteq A$ multiplicative. Soient M et N des A-modules. Alors,*

$$S^{-1}(M \otimes_A N) \cong_{S^{-1}A} (S^{-1}M) \otimes_{S^{-1}A} (S^{-1}N).$$

Démonstration. Exercice. □

Proposition 2.7.10. *Soient M et N des A-modules. Alors, $M \otimes_A N$ est engendré par les tenseurs $m \otimes n$, où $m \in M$ et $n \in N$.*

Démonstration. Soit $P \subseteq M \otimes_A N$ le sous-A-module engendré par les tenseurs simples $m \otimes n$. Soit $f\colon M \times N \to P$ l'application A-bilinéaire définie par $f(m,n) = m \otimes n$. D'après la propriété universelle, il existe un morphisme de A-modules $g\colon M \otimes_A N \to P$ tel que $g(m \otimes n) = m \otimes n$. Soit $i\colon P \to M \otimes_A N$ l'inclusion. On a alors un morphisme de A-modules $i \circ g$ de $M \otimes_A N$ dans lui-même satisfaisant $(i \circ g)(m \otimes n) = m \otimes n$. Or, l'identité id sur $M \otimes_A N$ satisfait aussi $\mathrm{id}(m \otimes n) = m \otimes n$. D'après l'unicité, $i \circ g = \mathrm{id}$. Par conséquent, l'inclusion i est surjective, c-à-d, $P = M \otimes_A N$. □

Proposition 2.7.11. *Soient M et N des A-modules libres de bases S et T respectivement. Alors, le produit tensoriel $M \otimes_A N$ est libre de base*

$$\{s \otimes t \mid s \in S, t \in T\}.$$

Démonstration. On montre d'abord que $\{s \otimes t \mid s \in S, t \in T\}$ engendre $M \otimes_A N$. D'après la proposition précédente il suffit de montrer que tout tenseur simple $m \otimes n$ est une combinaison linéaire de $s \otimes t$, $s \in S$ et $t \in T$. Mais S engendre M et T engendre N donc il existe $a_s \in A$ et $b_t \in A$, presque tous nuls, tels que $m = \sum a_s s$ et $n = \sum b_t t$. Alors,

$$m \otimes n = (\sum_{s \in S} a_s s) \otimes (\sum_{t \in T} b_t t) = \sum_{s \in S, t \in T} a_s b_s \cdot s \otimes t.$$

Cela montre que $\{s \otimes t \mid s \in S, t \in T\}$ est générateur.

Ensuite on montre que $\{s \otimes t \mid s \in S, t \in T\}$ est libre. Soit $a_{s,t} \in A$ presque tous nuls tels que $\sum a_{s,t} \cdot s \otimes t = 0$. On va montrer que tous les $a_{s,t}$ sont nuls. Soient $s \in S$ et $t \in T$. Soit $\varphi_s\colon M \to A$ le morphisme de A-modules défini par $\varphi_s(s') = \delta_{s,s'}$ quel que soit $s' \in S$. De même, soit $\psi_t\colon N \to A$ le morphisme de A-modules défini par $\psi_t(t') = \delta_{t,t'}$ quel que soit $t' \in T$. Soit $f\colon M \times N \to A$ l'application définie par $f(m,n) = \varphi_s(m) \cdot \psi_t(n)$. Alors, f est A-bilinéaire. Par

conséquent, il existe un morphisme $g\colon M \otimes_A N \to A$ tel que $g(m \otimes n) = f(m,n)$. On a alors

$$\begin{aligned} 0 = g(\sum_{s' \in S, t' \in T} a_{s',t'} \cdot s' \otimes t') = \\ = \sum_{s' \in S, t' \in T} a_{s',t'} \cdot g(s' \otimes t') = \\ = \sum_{s' \in S, t' \in T} a_{s',t'} \cdot f(s',t') = a_{s,t}. \end{aligned}$$

Cela montre que $\{s \otimes t \mid s \in S, t \in T\}$ est libre. □

Corollaire 2.7.12. *Soient M et N des A-modules libre de rang fini. Alors, $M \otimes_A N$ est libre de rang fini et on a*

$$\operatorname{rang}(M \otimes_A N) = \operatorname{rang}(M) \cdot \operatorname{rang}(N).$$

En particulier, lorsque A est un corps,

$$\dim(M \otimes_A N) = \dim(M) \cdot \dim(N). \quad \square$$

Corollaire 2.7.13. *Soit A un anneau intègre. Soient M et N des A-modules de type fini. Alors,*

$$\operatorname{rang}(M \otimes_A N) = \operatorname{rang}(M) \cdot \operatorname{rang}(N).$$

Démonstration. Soit K le corps de fractions de A. On a

$$\begin{aligned} \operatorname{rang}_A(M \otimes_A N) &= \dim_K((M \otimes_A N)_K) = \\ &= \dim_K(M_K \otimes_K N_K) = \\ &= \dim_K(M_K) \cdot \dim_K(N_K) = \\ &= \operatorname{rang}_A(M) \cdot \operatorname{rang}_A(N). \end{aligned}$$

□

Soient $f\colon M \to M'$ et $g\colon N \to N'$ des morphismes de A-modules. On définit un morphisme de A-modules induit

$$f \otimes g\colon M \otimes_A N \longrightarrow M' \otimes_A N'.$$

En effet, soit $h\colon M \times N \to M' \otimes_A N'$ l'application définie par $h(m,n) = f(m) \otimes g(n)$. Alors, h est A-bilinéaire, donc il existe un unique morphisme $f \otimes g$ de $M \otimes_A N$ dans $M' \otimes_A N'$ tel que $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$ quel que soit $m \in M$ et $n \in N$. On a les propriétés habituelles :

Proposition 2.7.14. *Soient A un anneau.*

1. *Soient $f\colon M \to M'$, $g\colon N \to N'$, $f'\colon M' \to M''$ et $g'\colon N' \to N''$ des morphismes de A-modules. Alors, $(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g)$.*
2. $\mathrm{id}_M \otimes \mathrm{id}_N = \mathrm{id}_{M \otimes_A N}$. □

Théorème 2.7.15. *Soit* $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ *une suite exacte de A-modules. Soit Q un A-module. Alors, la suite induite*

$$Q \otimes_A M \xrightarrow{\mathrm{id}_Q \otimes f} Q \otimes_A N \xrightarrow{\mathrm{id}_Q \otimes g} Q \otimes P \longrightarrow 0$$

est exacte. De plus, lorsque la suite $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ *est scindée, le morphisme* $\mathrm{id}_Q \otimes f$ *est injectif.*

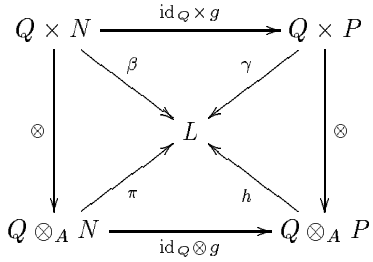
Démonstration. Montrons que $\mathrm{id}_Q \otimes g$ est surjectif. Comme $Q \otimes_A P$ est engendré par les tenseurs simples, il suffit de montrer que tout élément de la forme $q \otimes p$ est dans l'image de $\mathrm{id}_Q \otimes g$. Soient donc $q \in Q$ et $p \in P$. Or, g est surjectif, il existe donc $n \in N$ tel que $g(n) = p$. Alors, $(\mathrm{id}_Q \otimes g)(q \otimes n) = \mathrm{id}_Q(q) \otimes g(n) = q \otimes p$. Cela montre que $\mathrm{id}_Q \otimes g$ est surjectif.

Comme $g \circ f = 0$, on a $(\mathrm{id}_Q \otimes g) \circ (\mathrm{id}_Q \otimes f) = \mathrm{id}_Q \otimes (g \circ f) = \mathrm{id}_Q \otimes 0 = 0$, i.e., $\mathrm{im}(\mathrm{id}_Q \otimes f) \subseteq \ker(\mathrm{id}_Q \otimes g)$.

Pour montrer l'inclusion $\mathrm{im}(\mathrm{id}_Q \otimes f) \supseteq \ker(\mathrm{id}_Q \otimes g)$ on montre que le morphisme de passage au quotient

$$\pi \colon Q \otimes_A N \longrightarrow L = (Q \otimes_A N)/\mathrm{im}(\mathrm{id}_Q \otimes f)$$

envoie $\ker(\mathrm{id}_Q \otimes g)$ sur 0. En effet, soit $\beta \colon Q \times N \to L$ l'application bilinéaire qui envoie (q, n) sur $\pi(q \otimes n)$. Comme $\beta(q, n) = 0$ pour tout $n \in \mathrm{im}(f)$ quel que soit $q \in Q$, β induit une application $\gamma \colon Q \times P \to L$ telle que $\gamma(q, g(n)) = \beta(q, n)$ quel que soit $(q, n) \in N$. Evidemment, γ est A-bilinéaire. Il existe alors $h \colon Q \otimes_A P \to L$ tel que $\gamma(q, p) = h(q \otimes p)$. On a le diagramme



dans lequel tous les triangles commutent sauf éventuellement celui d'en-dessous. On va montrer justement que celui-ci commute également. Comme les autres triangles commutent et comme le carré commute, on a que $h \circ (\mathrm{id}_Q \otimes g) = \pi$ sur l'image de $Q \times N$ dans $Q \otimes_A N$. Or, cette image est l'ensemble des tenseurs simples dans $Q \otimes_A N$ qui engendrent ce module, on a donc $h \circ (\mathrm{id}_Q \otimes g) = \pi$ sur $Q \otimes_A N$ tout entier. Par conséquent, $\pi(\ker(\mathrm{id}_Q \otimes g)) = \{0\}$, i.e., $\ker(\mathrm{id}_Q \otimes g) \subseteq \mathrm{im}(\mathrm{id}_Q \otimes f)$.

Finalement, supposons que la suite $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ est scindée. Il existe alors une retraction $r \colon N \to M$ à f, i.e., $r \circ f = \mathrm{id}_M$. Par conséquent, $(\mathrm{id}_Q \otimes r) \circ (\mathrm{id}_Q \otimes f) = \mathrm{id}_Q \otimes (r \circ f) = \mathrm{id}_Q \otimes \mathrm{id}_M = \mathrm{id}_{Q \otimes M}$. En particulier, $\mathrm{id}_Q \otimes f$ est injectif. □

2.8 Lemme de Nakayama

Avant d'attaquer le Lemme de Nakayama on généralise la notion du déterminant d'une matrice $n \times n$.

Rappelons que S_n est le groupe symétrique agissant sur l'ensemble $\{1, \ldots, n\}$. On a un morphisme de groupes

$$\text{sign}\colon S_n \longrightarrow \{-1, +1\}$$

qui est tel que $\text{sign}(\sigma) = -1$ pour une transposition $\sigma \in S_n$. En général, $\text{sign}(\sigma) = (-1)^k$ lorsque σ s'écrit comme composition de k transpositions. Ou encore, $\text{sign}(\sigma) = (-1)^m$, où m est le nombre d'inversions de σ, i.e.,

$$m = \text{Card}\{(i,j) \mid i < j \text{ et } \sigma(i) > \sigma(j)\}.$$

L'équivalence de ces deux définitions de $\text{sign}(\sigma)$ se montre par récurrence sur k.

Soit A un anneau et $L = (a_{ij})_{i,j=1,\ldots,n}$ une matrice $n \times n$ à coefficients dans A. Le déterminant de L est alors défini comme dans le cas où A est un corps :

$$\det(L) = \sum_{\sigma \in S_n} \text{sign}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$

On a les propriétés usuelles :

Lemme 2.8.1. *Soit $L = (a_{ij})_{i,j=1,\ldots,n}$ une matrice $n \times n$ à coefficients dans A. Alors,*

1. $\det(L) = 0$ *lorsque L a deux colonnes identiques ;*

2. $\det(L) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} L_{ij}$ *quel que soit j, où L_{ij} est le cofacteur de L défini par*

$$L_{ij} = \det\left((a_{kl})_{\substack{k,l=1,\ldots,n \\ k \neq i, l \neq j}} \right).$$

Démonstration. 1. Supposons que la j-ième colonne et la k-ième colonne de L sont identiques. Soit τ la transposition qui échange j et k. Soit $E \subseteq S_n$ un sous-ensemble tel que S_n soit la réunion disjointe de E et $\tau \cdot E$. (On peut prendre par exemple le sous-groupe alterné A_n de S_n). Alors,

$$\begin{aligned}
\det(L) &= \sum_{\sigma \in S_n} \text{sign}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} = \\
&= \sum_{\sigma \in E} \text{sign}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} + \sum_{\sigma \in E} \text{sign}(\tau\sigma) a_{1\tau\sigma(1)} \cdots a_{n\tau\sigma(n)} = \\
&= \sum_{\sigma \in E} \text{sign}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} + \sum_{\sigma \in E} \text{sign}(\tau)\text{sign}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} = \\
&= 0,
\end{aligned}$$

car $\tau\sigma(i) = \sigma(i)$ lorsque $\sigma(i) \neq j, k$ et $a_{i\tau\sigma(i)} = a_{i\sigma(i)}$ lorsque $\sigma(i)$ est égal à j ou k.

2. On se fixe une colonne $j \in \{1, \dots, n\}$. On a

$$\begin{aligned}
\det(L) &= \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} = \\
&= \sum_{i=1}^{n} \sum_{\substack{\sigma \in S_n \\ \sigma(i)=j}} \operatorname{sign}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} = \\
&= \sum_{i=1}^{n} a_{ij} \cdot \sum_{\substack{\sigma \in S_n \\ \sigma(i)=j}} \operatorname{sign}(\sigma) a_{1\sigma(1)} \cdots \widehat{a_{i\sigma(i)}} \cdots a_{n\sigma(n)} = \\
&= \sum_{i=1}^{n} (-1)^{i+j} a_{ij} L_{ij},
\end{aligned}$$

où $\widehat{a_{i\sigma(i)}}$ signifie «ômettre le facteur $a_{i\sigma(i)}$». On explique encore la dernière égalité : Soient $i, j \in \{1, \dots, n\}$ et soit $\sigma \in S_n$ tel que $\sigma(i) = j$. Soit

$$\tau \colon \{1, \dots, n\} \backslash \{i\} \to \{1, \dots, n\} \backslash \{j\}$$

la restriction de σ. Il faut montrer que le nombre d'inversions de σ est congru modulo 2 à la somme du nombre d'inversions de τ et $i + j$. Considérons les inversions de σ :

$$\begin{aligned}
&\operatorname{Card}\{(k,l) \mid k < l, \sigma(k) > \sigma(l)\} = \\
&\qquad = \operatorname{Card}\{(k,l) \mid k \neq i, l \neq i, k < l, \sigma(k) > \sigma(l)\} + \\
&\qquad\quad + \operatorname{Card}\{(i,l) \mid i < l, j > \sigma(l)\} + \\
&\qquad\quad + \operatorname{Card}\{(k,i) \mid k < i, \sigma(k) > j\} = \\
&\qquad = \operatorname{Card}\{(k,l) \mid k \neq i, l \neq i, k < l, \sigma(k) > \sigma(l)\} + \\
&\qquad\quad + ((j-1) - \operatorname{Card}\{(i,l) \mid i > l, j > \sigma(l)\}) + \\
&\qquad\quad + ((i-1) - \operatorname{Card}\{(k,i) \mid k < i, \sigma(k) < j\}) = \\
&\qquad = \operatorname{Card}\{(k,l) \mid k \neq i, l \neq i, k < l, \sigma(k) > \sigma(l)\} + i + j + \\
&\qquad\quad - 2 - 2 \cdot \operatorname{Card}\{(k,i) \mid k < i, \sigma(k) < j\}
\end{aligned}$$

Mais $\operatorname{Card}\{(k,l) \mid k \neq i, l \neq i, k < l, \sigma(k) > \sigma(l)\}$ est exactement le nombre d'inversion de τ, d'où le résultat. □

Soit C la matrice des cofacteurs de L, i.e., $C = (c_{ij})_{i,j=1,\dots,n}$ où

$$c_{ij} = (-1)^{i+j} L_{ji}.$$

Alors, on a $C \cdot L = \det(L) I_n$, où I_n est la matrice $n \times n$ d'identité. En effet, l'élément (j, j) de $C \cdot L$ est égal à

$$\sum_{i=1}^{n} c_{ji} a_{ij} = \sum_{i=1}^{n} (-1)^{i+j} L_{ij} a_{ij} = \det(L)$$

quel que soit j. De plus, lorsque $k \neq j$, l'élément (k, j) de $C \cdot L$ est égal à

$$\sum_{i=1}^{n} c_{ki} a_{ij} = \sum_{i=1}^{n} (-1)^{i+k} L_{ik} a_{ij} = \det(L')$$

où L' est la matrice que l'on obtient à partir de L en remplaçant la k-ième colonne par la colonne $(a_{ij})_{i=1,\dots,n}$. En particulier, la k-ième et la j-ième colonne de L' sont les mêmes. Comme $k \neq j$, on a $\det(L') = 0$. Cela montre que $C \cdot L = \det(L) I_n$.

Maintenant on est prêt pour le résultat principal de ce paragraphe :

Lemme de Nakayama (première version). *Soit A un anneau et $I \subseteq A$ un idéal. Soit M un A-module de type fini. Supposons que $IM = M$. Alors, il existe $x \in I$ tel que $(1+x)M = 0$.*

Démonstration. Soit $\{m_1, \dots, m_n\}$ un système générateur de M. Or, $M = IM$, d'où $x_{ij} \in I$ tels que

$$m_i = \sum_{j=1}^{n} x_{ij} m_j$$

quel que soit i. On écrit cela sous la forme

$$\sum_{j=1}^{n} (\delta_{ij} - x_{ij}) m_j = 0$$

quel que soit i. Ou encore, avec notation matricielle

$$(I_n - X)m = 0,$$

où I_n est la matrice $n \times n$ d'identité, X est la matrice $(x_{ij})_{i,j=1,\dots,n}$ et m est le vecteur $(m_i)_{i=1,\dots,n}$. On multiplie l'équation $(I_n - X)m = 0$ par la matrice C des cofacteurs de $I_n - X$, et on obtient alors

$$(\det(I_n - X) \cdot I_n) \cdot m = C \cdot (I_n - X) \cdot m = 0.$$

Par conséquent, $\det(I_n - X) \cdot m_i = 0$ quel que soit i. D'après la définition du déterminant, il existe $x \in I$ tel que $\det(I_n - X) = 1 + x$. D'où $x \in I$ tel que $(1+x)M = 0$. □

On rencontre le Lemme de Nakayama plus souvent dans la forme suivante :

Lemme de Nakayama (deuxième version). *Soit A un anneau local et $m \subseteq A$ son idéal maximal. Soit M un A-module de type fini et $N \subseteq M$ un sous-A-module. Supposons que $M = mM + N$. Alors, $M = N$.*

Démonstration. Considérer le quotient M/N. Evidemment, M/N est un A-module de type fini. On a $m(M/N) = M/N$. En effet, lorsque $u \in M$, il existe, d'après l'hypothèse, $v \in mM$ et $n \in N$ tels que $u = v + n$. Dans le quotient M/N on a alors $u = v \in m(M/N)$. Cela montre que $m(M/N) = M/N$. D'après la première version du Lemme de Nakayama, il existe $x \in m$ tel que $(1+x)(M/N) = 0$. Or A est un anneau local et $1 + x \notin m$, d'où $1 + x$ est inversible dans A. Il s'ensuit que $M/N = 0$, i.e., $M = N$. □

Corollaire 2.8.2. *Soit A un anneau local, $m \subseteq A$ son idéal maximal, et $k = A/m$ le corps résiduel. Soit M un A-module de type fini. Soient $m_1, \dots, m_n \in M$ tels que leurs images dans M/mM engendrent le k-vectoriel M/mM. Alors, $m_1, \dots, m_n$ engendrent le A-module M.*

Démonstration. Soit $N \subseteq M$ le sous-A-module engendré par $\{m_1, \ldots, m_n\}$. Or, $\{m_1, \ldots, m_n\}$ engendre M/mM comme A-module, c-à-d, $M = N + mM$. D'après la deuxième version du Lemme de Nakayama, $M = N$, i.e., le système $\{m_1, \ldots, m_n\}$ engendre M. □

Corollaire 2.8.3. *Soit A un anneau local intègre, soit $m \subseteq M$ son idéal maximal, et k son corps résiduel. Soit M un A-module de type fini. Alors,* $\mathrm{rang}_A(M) \leq \dim_k(M/mM)$. *Le A-module M est libre de rang* $\dim_k(M/mM)$ *lorsque l'on a l'égalité* $\mathrm{rang}_A(M) = \dim_k(M/mM)$.

Démonstration. Soient $m_1, \ldots, m_n \in M$ tels que leurs images dans M/mM constituent une base de M/mM. D'après le corollaire précédent, le système $\{m_1, \ldots, m_n\}$ dans M est générateur. Il existe alors une surjection $f\colon A^n \to M$. Le morphisme induit $f_K\colon K^n \to M_K$, où K est le corps de fractions de A, est donc aussi surjectif. Par conséquent, $\mathrm{rang}_A(M) = \dim_K(M_K) \leq n = \dim_k(M/mM)$.

Supposons que l'on a égalité, i.e., $\mathrm{rang}_A(M) = n$. Le morphisme f_K est alors aussi injectif. Par conséquent $\ker(f) \subseteq \ker(f_K) \cap A^n = 0$, i.e., f est injectif et donc un isomorphisme. □

2.9 Exercices

§1

155. Soit M un A-module. Montrer que

a. $0 \cdot m = 0$ quel que soit $m \in M$;

b. $(-1) \cdot m = -m$ quel que soit $m \in M$;

c. $a \cdot 0 = 0$ quel que soit $a \in A$;

156. Il n'y a qu'un seul module sur l'anneau nul, le 0-module 0.

157. Soit M un groupe abélien. Montrer que M est un $\mathrm{End}(M)$-module lorsqu'on définit $\varphi \cdot m = \varphi(m)$ pour $\varphi \in \mathrm{End}(M)$ et $m \in M$.

158. Soit $f\colon A \to B$ un morphisme d'anneaux.

a. Soit M un B-module. Montrer que l'on définit une structure de A-module sur M par
$$a \cdot m = f(a) \cdot m,$$
où $a \in A$ et $m \in M$. Cette structure de A-module sur le B-module M est dite *obtenue par réduction de scalaires de B à A*, parfois notée par ${}_AM$.

b. Soit $\varphi\colon M \to N$ un morphisme de B-modules. Montrer que φ est A-linéaire pour les structures de A-modules sur M et N obtenues par réduction de scalaires, i.e., $\varphi\colon {}_AM \to {}_AN$ est A-linéaire.

c. Supposons que A et B sont des corps et que B, ou plus précisément ${}_AB$, est de A-dimension finie. Montrer que $\dim({}_AM) = \dim({}_AB) \cdot \dim(M)$ pour tout B-espace vectoriel M de dimension finie.

159. Montrer que tout morphisme de groupes abéliens est automatiquement $\mathbb{Z}$-linéair en n'utilisant que la propriété universelle du groupe abélien $\mathbb{Z}$.

160. Soit M un A-module. *L'annulateur* de M est par définition

$$\mathrm{Ann}(M) = \{a \in A \,|\, \forall m \in M : a \cdot m = 0\}.$$

Montrer que $\mathrm{Ann}(M)$ est un idéal de A.

161. Soit M un A-module. Soit $I \subseteq A$ un idéal contenu dans l'annulateur de M.

a. Montrer que l'on peut définir une structure de A/I-module sur M par $\overline{a} \cdot m = a \cdot m$.

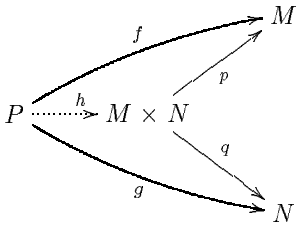
b. Soient de plus N un A-module avec $I \subseteq \mathrm{Ann}(N)$ et $f\colon M \to N$ un morphisme de A-modules. Montrer que f est un morphisme de A/I-modules.

162. Soient M et N des A-modules.

a. Montrer que la loi externe sur $M \times N$ défini par $a \cdot (m, n) = (am, an)$ fait du produit $M \times N$ un A-module.

b. Soient $p\colon M \times N \to M$ et $q\colon M \times N \to N$ les projections. Montrer que p et q sont des morphismes de A-modules.

c. Montrer que $M \times N$ muni de ses projections satisfait la propriété universelle suivante. Pour tout A-module P et pour tous les morphismes $f\colon P \to M$ et $g\colon P \to N$ il existe un et un seul morphisme $h\colon P \to M \times N$ faisant commuter le diagramme suivant.



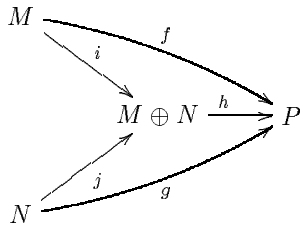
On appelle $M \times N$ le *produit* des modules M et N.

163. Soient M et N des A-modules. Dans cet exercice on montrera que le produit $M \times N$ de M et N satisfait encore une autre propriété universelle. Lorsqu'on veut insister sur cette propriété-ci on note $M \oplus N$ au lieu de $M \times N$ et $m \oplus n$ au lieu de (m, n), pour $m \in M$ et $n \in N$.

a. Soient $i\colon M \to M \oplus N$ et $j\colon M \to M \oplus N$ les injections définies par $i(m) = m \oplus 0$ et $j(n) = 0 \oplus n$. Montrer que i et j sont des morphismes de A-modules.

b. Montrer que $M \oplus N$ muni de ses injections i et j satisfait la propriété universelle suivante. Pour tout A-module P et pour tous les morphismes

$f\colon M \to P$ et $g\colon N \to P$ il existe un et un seul morphisme $h\colon M \oplus N \to P$ faisant commuter le diagramme suivant.



On appelle $M \oplus N$ la *somme directe (externe)* des modules M et N.

164. Soit $\{M_i \mid i \in I\}$ une famille de A-modules. Montrer l'existence d'un A-module

$$\prod_{i \in I} M_i$$

muni de morphismes $f_i\colon \prod M_i \to M_i$, $i \in I$, satisfaisant la propriété universelle suivante. Pour tout A-module N muni de morphismes $g_i\colon N \to M_i$, $i \in I$, il existe un et un seul morphisme $h\colon N \to \prod M_i$ tel que $f_i \circ h = g_i$ pour tout $i \in I$. On appelle $\prod M_i$ le *produit* des A-modules M_i.

165. Soit $\{M_i \mid i \in I\}$ une famille de A-modules. Montrer l'existence d'un A-module

$$\bigoplus_{i \in I} M_i$$

muni de morphismes $f_i\colon M_i \to \bigoplus M_i$, $i \in I$, satisfaisant la propriété universelle suivante. Pour tout A-module N et pour tous les morphismes $g_i\colon M_i \to N$, $i \in I$, il existe un et un seul morphisme $h\colon \bigoplus M_i \to N$ tel que $h \circ f_i = g_i$ pour tout $i \in I$. On appelle $\bigoplus M_i$ la *somme directe* des A-modules M_i.

166. Montrer par un exemple que $\prod_{i \in I} M_i \ncong \bigoplus_{i \in I} M_i$.

167. Déterminer les $\mathbb{Z}$-modules $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z})$, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$, $(\mathbb{Z}/n\mathbb{Z})^{\vee}$, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$, où m et n sont des entiers non nuls.

168. Soit $f\colon M \to N$ un morphisme de A-modules. Soit L un A-module.

a. Montrer que $f_\star(\varphi) = f \circ \varphi$ définit une application $f_\star\colon \mathrm{Hom}_A(L, M) \longrightarrow \mathrm{Hom}_A(L, N)$.

b. Montrer que $f_\star$ est A-linéaire.

c. Soit de plus $g\colon N \to P$ un morphisme de A-modules. Montrer que $(g \circ f)_\star = g_\star \circ f_\star$.

d. Montrer que $(\mathrm{id}_M)_\star = \mathrm{id}_{\mathrm{Hom}_A(L,M)}$.

169. Soit $f\colon M \to N$ un morphisme de A-modules. Soit L un A-module.

a. Montrer que $f^\star(\varphi) = \varphi \circ f$ définit une application $f^\star\colon \mathrm{Hom}_A(N, L) \longrightarrow \mathrm{Hom}_A(M, L)$.

b. Montrer que $f^\star$ est A-linéaire.

c. Soit de plus $g\colon N \to P$ un morphisme de A-modules. Montrer que $(g \circ f)^\star = f^\star \circ g^\star$.

d. Montrer que $(\mathrm{id}_M)^\star = \mathrm{id}_{\mathrm{Hom}_A(M,L)}$.

170. Soient M, N et L des A-modules. Montrer que

a. $\mathrm{Hom}_A(M \oplus N, L)$ est isomorphe à $\mathrm{Hom}_A(M, L) \times \mathrm{Hom}_A(N, L)$;

b. $\mathrm{Hom}_A(L, M \times N)$ est isomorphe à $\mathrm{Hom}_A(L, M) \times \mathrm{Hom}_A(L, N)$;

c. Généraliser à $\bigoplus M_i$ et $\prod M_i$.

171. Soient m et n des entiers non négatifs. Soit $\mathbf{M}_{n\times m}(A)$ l'ensemble des matrices $n \times m$ à coefficients dans A. Définir

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}) \text{ et } a \cdot (a_{ij}) = (a \cdot a_{ij}),$$

quel que soient $(a_{ij}), (b_{ij}) \in \mathbf{M}_{n\times m}(A)$ et quel que soit $a \in A$.

a. Montrer que $\mathbf{M}_{n\times m}(A)$ est un A-module.

b. Montrer que $\mathbf{M}_{n\times m}(A)$ est isomorphe à A^{nm}.

§2

172. Soit M un A-module. Soit $\mathcal{C}$ une collection de sous-A-modules de M. Montrer que l'intersection $\bigcap \mathcal{C}$ est un sous-A-module de M.

173. Soit M un A-module. Soient $N_1, N_2 \subseteq M$ des sous-A-modules. Soit

$$N_1 + N_2 = \{n_1 + n_2 \,|\, n_1 \in N_1 \text{ et } n_2 \in N_2\}.$$

Montrer que $N_1 + N_2$ est un sous-A-module de M.

174. Soit M un A-module. Soit $N \subseteq M$ un sous-A-modules. Un sous-A-module P de M est *supplémentaire* à N lorsque $N + P = M$ et $N \cap P = (0)$. Dans ce cas on dit que M est *somme directe (interne)* de N et P, noté par $M = N \oplus P$. Est-ce qu'un sous-A-module N de M admet forcément un supplémentaire ?

175. Soit M un A-module. Soient $N_1, N_2, P \subseteq M$ des sous-A-modules. A-t-on $(N_1 + N_2) \cap P = (N_1 \cap P) + (N_2 \cap P)$?

176. Soit $f\colon M \to N$ un morphisme de A-modules. Montrer que

a. $f(P)$ est un sous-A-module de N lorsque P est un sous-A-module de M ;

b. $f^{-1}(Q)$ est un sous-A-module de M lorsque Q est un sous-A-module de N ;

c. $f^{-1}(f(P)) = P + \ker(f)$ lorsque P est un sous-A-module de M.

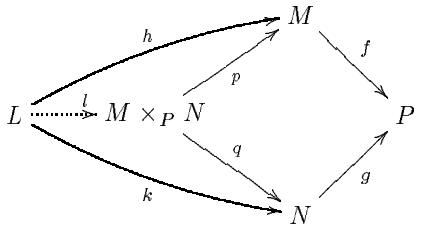
177. Soit A un anneau. Soient M, N et P des A-modules. Soient $f\colon M \to P$ et $g\colon N \to P$ des morphismes de A-modules. On définit le *produit fibré* de M et N sur P par

$$M \times_P N = \{(m,n) \in M \times N \mid f(m) = g(n)\}.$$

a. Montrer que $M \times_P N$ est un sous-A-module du module produit $M \times N$.

b. Soient $p\colon M \times_P N \to M$ et $q\colon M \times_P N \to N$ les applications définies par $p(m,n) = m$ et $q(m,n) = n$. Montrer que p et q sont des morphismes de A-modules.

c. Montrer que $M \times_P N$ muni de ses projections p et q est universel d'ayant la propriété que $f \circ p = g \circ q$, c-à-d, pour tout A-module L et pour tous les morphismes de A-modules $h\colon L \to M$ et $k\colon L \to N$ tels que $f \circ h = g \circ k$, il existe un et un seul morphisme de A-modules $l\colon L \to M \times_P N$ tel que le diagramme suivant commute :



d. Soient $P' = \mathrm{im}(f) \cap \mathrm{im}(g)$, $M' = f^{-1}(P')$, $N' = g^{-1}(P')$, et soient f' et g' les restrictions de f et g à M' et N', respectivement. Considérer f' et g' comme morphismes de A-modules dans P'. Montrer que $M \times_P N = M' \times_{P'} N'$. (De ce fait, en ce qui concerne les produit fibrés, on peut toujours supposer f et g surjectifs.)

e. Soit A un corps. Soient M, N, P des A-espaces vectoriels de dimension finie. Soient $f\colon M \to P$ et $g\colon N \to P$ des morphismes A-linéaires surjectifs. Exprimer la dimension du produit fibré $M \times_P N$ en fonction des dimensions de M, N et P.

178. Soit $f\colon M \to N$ un morphisme de A-modules. Montrer qu'il y a une correspondance entre les sous-A-modules de $\mathrm{im}(f)$ et les sous-A-modules de M contenant $\ker(f)$.

179. Soit $f\colon M \to N$ un morphisme de A-modules.

a. Soit $S \subseteq M$ un sous-ensemble. Montrer que $f((S)) = (f(S))$.

b. Montrer que $f(P)$ est de type fini lorsque P est un sous-A-module de M de type fini.

180. Soit A un anneau, I un idéal de A et M un A-module. Soit

$$IM = \{\sum_{i=1}^{n} x_i m_i \mid x_i \in I, m_i \in M \text{ et } n \in \mathbb{N}\}.$$

a. Montrer que IM est un sous-A-module de M.

b. Soit de plus $J \subseteq A$ un idéal. Montrer que $(I+J)M = IM + JM$.

c. Montrer que $I(JM) = (IJ)M$.

d. Montrer que

$$I(\bigoplus_{j\in J} M_j) = \bigoplus_{j\in J}(IM_j),$$

où les M_j sont des A-modules, $j \in J$.

e. Montrer que $I(A^n) = I^n$.

181. Soit M un A-module et $I \subseteq A$ un idéal tel que $I + \mathrm{Ann}(M) = A$. Montrer que $IM = M$.

182. Soit M un A-module libre de base $\mathcal{E} = \{e_1, \ldots, e_m\}$ et N un A-module libre de base $\mathcal{F} = \{f_1, \ldots, f_n\}$. Pour un morphisme A-linéaire $\varphi\colon M \to N$, définissons la *matrice* $M_{\mathcal{F},\mathcal{E}}(\varphi)$ *de* φ *dans les bases* $\mathcal{E}$ *et* $\mathcal{F}$ par $M_{\mathcal{F},\mathcal{E}}(\varphi) = (a_{ij})$, où les $a_{ij} \in A$ sont déterminés par

$$\varphi(e_j) = \sum_{i=1}^{n} a_{ij} f_i.$$

Montrer que l'application

$$M_{\mathcal{F},\mathcal{E}}\colon \mathrm{Hom}_A(M,N) \to \mathbf{M}_{n\times m}(A)$$

est un isomorphisme de A-modules.

183. Soit A un anneau et n un entier non négatif. Soit $\mathbf{M}_n(A)$ l'ensemble des matrices $n \times n$ à coefficients dans A. Le but de cet exercice est de montrer que les lois d'addition et multiplication matricielles sur $\mathbf{M}_n(A)$ en font un anneau.

Soit $\mathcal{E} = \{e_1, \ldots, e_n\}$ la base standarde du A-module A^n. Soit M l'application de $\mathrm{End}_A(A^n)$ dans $\mathbf{M}_n(A)$ qui associe à $f \in \mathrm{End}_A(A^n)$ sa matrice $M_{\mathcal{E},\mathcal{E}}(f)$ dans la base $\mathcal{E}$.

a. Montrer que $M(f+g) = M(f) + M(g)$ et $M(f \circ g) = M(f) \cdot M(g)$.

b. Montrer que $\mathbf{M}_n(A)$ est un anneau.

184. Soit A un anneau. Soit n un entier non négatif. Soit $\mathcal{E} = \{e_1, \ldots, e_n\}$ la base standarde de A^n. Définir $\varphi_i \in (A^n)^\vee$ par $\varphi_i(e_j) = \delta_{ij}$. Montrer que $\mathcal{E}^\vee = \{\varphi_1, \ldots, \varphi_n\}$ est une base de $(A^n)^\vee$.

185. Soit $f\colon M \to N$ un morphisme de A-modules. Définir $f^\vee : N^\vee \to M^\vee$ par $f^\vee(\varphi) = \varphi \circ f$.

a. Montrer que $f^\vee$ est un morphisme de A-modules de $N^\vee$ dans $M^\vee$.

b. Soit $M = A^m$ et $N = A^n$. Soient $\mathcal{E}$ et $\mathcal{F}$ les bases standardes de A^m et A^n respectivement. Montrer que la matrice de $f^\vee$ dans les bases $\mathcal{F}^\vee$ et $\mathcal{E}^\vee$ est la transposée de la matrice de f dans les bases $\mathcal{E}$ et $\mathcal{F}$, i.e.,

$$M_{\mathcal{E}^\vee,\mathcal{F}^\vee}(f^\vee) = M_{\mathcal{F},\mathcal{E}}(f)^t.$$

186. Soit M un A-module. Soient $S, T \subseteq M$ des sous-ensembles tels que $S \subseteq T$. Montrer que

a. S est un système libre de M lorsque T l'est ;

b. T est un système générateur de M lorsque S l'est.

187. Soit M un A-module.

a. Montrer qu'il existe un système libre $S \subseteq M$.

b. Montrer qu'il existe un système générateur $S \subseteq M$.

c. Montrer qu'il existe un système libre maximal $\mathcal{B} \subseteq M$.

d. Est-ce que $\mathcal{B}$ est nécessairement une base de M ?

e. Est-ce que M a nécessairement un système générateur minimal?

f. Montrer que M a un système générateur minimal $\mathcal{S} \subseteq M$ lorsque M est de type fini.

g. Est-ce que $\mathcal{S}$ est nécessairement une base de M ?

188. Soit $f\colon M \to N$ un morphisme de A-modules. Soit $S \subseteq M$ un sous-ensemble.

a. Est-ce que $f(S)$ est générateur de $\mathrm{im}(f)$ lorsque S est générateur de M?

b. Est-ce que S est libre si $f(S)$ est libre?

189. Soit A un anneau. Soient M un A-module et $S \subseteq M$ un sous-ensemble. Soit $A^{(S)}$ le A-module libre sur l'ensemble S. Soit $f\colon A^{(S)} \to M$ le morphisme défini par $f(s) = s$. Montrer que

a. S est générateur de M si et seulement si f est surjectif ;

b. S est libre si et seulement si f est injectif ;

c. S est une base de M si et seulement si f est un isomorphisme.

190. Soit A un anneau. Soient M un A-module et $S \subseteq M$ un sous-ensemble. Montrer que

a. S est un système générateur de M si et seulement si pour tout A-module N et pour tous morphismes $F, G\colon M \to N$, $F|_S = G|_S$ implique $F = G$.

b. S est un système libre de M si et seulement si pour tout A-module N et pour toute application $f\colon S \to N$ il existe un morphisme $F\colon (S) \to N$ tel que $F|_S = f$.

c. S est une base de M si et seulement si pour tout A-module N et pour toute application $f\colon S \to N$ il existe un et un seul morphisme $F\colon M \to N$ ayant $F|_S = f$.

191. Soit A un anneau et M un A-module. Soient $S, T \subseteq M$ des sous-ensembles. Supposons que S est fini et que $(S) \subseteq (T)$.

a. Montrer qu'il existe un sous-ensemble fini $T' \subseteq T$ tel que $(S) \subseteq (T')$.

b. Montrer que M est libre de rang fini si et seulement si M est libre et de type fini.

192.* Soient A un anneau fini et S un ensemble. Montrer que le A-module A^S est libre.

193. Trouver un système générateur fini pour le sous-module engendré par S dans les cas suivants :

a. S est l'ensemble des nombres premiers dans $\mathbb{Z}$;

b. $S = \{(a, b) \in \mathbb{Z}^2 \mid a^2 + b^2 > 100\}$;

c. $S = \{(a, a^2) \in \mathbb{Z}^2 \mid a \in \mathbb{Z}\}$.

194.* Soit A un anneau dans lequel chaque idéal est engendré par au plus d éléments. Montrer que chaque sous-A-module de A^n admet un système générateur à au plus dn éléments.

195. Soit $f\colon A \to B$ un morphisme d'anneaux. Supposons que B, pour la structure de A-module obtenue par réduction de scalaires, est de type fini.

a. Montrer que ${}_A M$ est de type fini lorsque M est un B-module de type fini.

b. Montrer que M est de type fini lorsque ${}_A M$ est de type fini.

c. Montrer que B est noetherien lorsque A l'est.

196. Soit $f\colon A \to B$ un morphisme d'anneaux. Supposons que B, pour la structure de A-module obtenue par réduction de scalaires, est libre.

a. Montrer que ${}_A M$ est libre lorsque M est un B-module libre.

b. Supposons que A est non nul et que ${}_A B$ est libre de rang n. Montrer que ${}_A M$ est libre de rang nr lorsque M est un B-module libre de rang r.

197. Soit A un anneau et $s \in A$ régulier. Montrer que la localisation A_s de A par s est de type fini en tant que A-module, si et seulement si s est inversible dans A.

198.* Déterminer tous les sous-$\mathbb{Z}$-modules de type fini de $\mathbb{Q}$. Même question pour $\mathbb{Q}/\mathbb{Z}$.

§3

199. Soient M et N des A-modules. Montrer que $(M \oplus N)/M$ est isomorphe à N. Expliquer pourquoi on n'a pas besoin de la notion de quotients pour les espaces vectoriels.

200. Soient M_i des A-modules, $i \in I$. Soient $N_i \subseteq M_i$ des sous-A-modules, $i \in I$. Montrer que

a. $\bigoplus (M_i/N_i) \cong (\bigoplus M_i)/(\bigoplus N_i)$;

b. $\prod (M_i/N_i) \cong (\prod M_i)/(\prod N_i)$.

201. Soit M un A-module. Soient $N_1, N_2 \subseteq M$ des sous-A-modules tels que $N_1 \subseteq N_2$. Soit $\pi : M \to M/N_1$ le passage au quotient.

a. Montrer que la restriction de π à N_2 considérée comme morphisme dans $\pi(N_2)$ est un quotient de N_2 par N_1. Ainsi, on identifie $\pi(N_2)$ et N_2/N_1.

b. Montrer que π induit un isomorphisme de M/N_2 sur $(M/N_1)/(N_2/N_1)$.

202. Soit $f : M \to N$ un morphisme de A-modules.

a. Soient $P \subseteq M$ et $Q \subseteq N$ des sous-A-modules tels que $f(P) \subseteq Q$. Montrer que f induit un morphisme $\overline{f} : M/P \to N/Q$ tel que le diagramme

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow & & \downarrow \\ M/P & \xrightarrow{\overline{f}} & N/Q \end{array}$$

commute, où les morphismes verticaux sont les passages au quotient.

b. Montrer que $\ker(\overline{f}) = f^{-1}(Q)/P$.

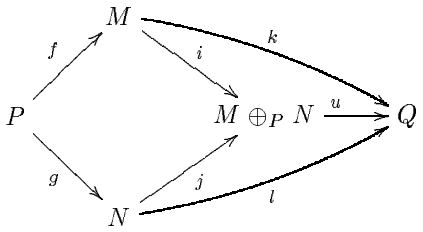
c. Montrer que $\mathrm{im}(\overline{f}) = (\mathrm{im}(f) + Q)/Q$.

203. Soit M un A-module. Soient $N, P \subseteq M$ des sous-A-modules. Montrer que $(N + P)/P \cong N/(N \cap P)$.

204. Soient M, N et P des A-modules. Soient $f : P \to M$ et $g : P \to N$ des morphismes de A-modules. Soit $h : P \to M \oplus N$ le morphisme défini par $h(p) = f(p) \oplus -g(p)$. Soit $M \oplus_P N$ le quotient de $M \oplus N$ par $\mathrm{im}(h)$. On appelle $M \oplus_P N$ la *somme amalgamée* de M et N sur P. On note l'image de l'élément $m \oplus n$ dans $M \oplus_P N$ par $m \oplus_P n$. Soient de plus $i : M \to M \oplus_P N$ et $j : N \to M \oplus_P N$ les morphismes définis par $i(m) = m \oplus_P 0$ et $j(n) = 0 \oplus_P n$.

a. Montrer que $i \circ f = j \circ g$.

b. Montrer que $M \oplus_P N$ muni de ses morphismes i et j satisfait la propriété universelle suivante. Pour tout A-module Q et pour tous les morphismes $k : M \to Q$ et $l : N \to Q$ tels que $k \circ f = l \circ g$, il existe un et un seul morphisme $u : M \oplus_P N \to Q$ faisant commuter le diagramme suivant.



c. Supposons que M, N et P sont des sous-A-modules d'un A-module K, que $P = M \cap N$, et que f et g sont les inclusions. Montrer que $M \oplus_P N \cong M + N$.

d. Soit $P' = P/(\ker(f) \cap \ker(g))$. Soient $f' : P' \to M$ et $g' : P' \to N$ les morphisme induits. Montrer que $M \oplus_P N \cong M \oplus_{P'} N$. (De ce fait, en ce qui concerne les sommes amalgamées, on peut toujours supposer $\ker(f) \cap \ker(g) = \{0\}$.)

e. Soit A un corps et soient M, N et P des A-espaces vectoriels de dimension finies. Soient $f : P \to M$ et $g : P \to N$ des morphismes A-linéaires tels que $\ker(f) \cap \ker(g) = \{0\}$. Exprimer la dimension de $M \oplus_P N$ en fonction des dimensions de M, N et P.

205.* (Théorème Chinois pour modules) Soit M un A-module.

a. Soient N_1 et N_2 des sous-A-modules de M tels que $N_1 + N_2 = M$. Soit $f : M \to M/N_1 \oplus M/N_2$ le morphisme canonique. Montrer que f induit un isomorphisme de $M/(N_1 \cap N_2)$ dans $M/N_1 \oplus M/N_2$.

b. Soient I_1 et I_2 des idéaux étrangers de A. Montrer que $M/(I_1 \cap I_2)M$ est isomorphe à $M/I_1M \oplus M/I_2M$.

c. Soit N_i, $i = 1, \ldots, n$, une famille de sous-A-modules de M telle que

$$N_i + \bigcap_{j \neq i} N_j = M$$

quel que soit i. Soit f le morphisme canonique de M dans $\bigoplus_i M/N_i$. Montrer que f induit un isomorphisme de $M/(\bigcap_i N_i)$ dans $\bigoplus_i M/N_i$.

d. Soit I_i, $i = 1, \ldots, n$, une famille d'idéaux de A telle que $I_i + I_j = A$ lorsque $i \neq j$. Montrer que $M/(\bigcap I_i)M$ est isomorphe à $\bigoplus(M/I_iM)$.

206. Soient A et B des anneaux. Soit M un A-module et N un B-module.

a. Montrer que l'on définit une structure de $A \times B$-module sur $M \times N$ par $(a, b) \cdot (m, n) = (am, bn)$.

b. Soient M, M' des A-modules et N, N' des B-modules. Montrer que $M \times N \cong_{A\times B} M' \times N'$ si et seulement si $M \cong_A M'$ et $N \cong_B N'$.

c. Soit P un $A \times B$-module. Montrer qu'il existe un A-module M et un B-module N tels que $P \cong_{A\times B} M \times N$. Montrer que M et N sont uniquement déterminés par P à isomorphisme près.

d. Généraliser à un nombre fini d'anneaux.

207. Soient K et L des corps. Classifier tous les $K \times L$-modules de type fini à isomorphisme près. Généraliser à un nombre fini de corps.

208. Soient A un anneau et $I \subseteq A$ un idéal. Montrer que $A^{(S)}/IA^{(S)}$ est isomorphe à $(A/I)^{(S)}$.

209. Montrer que l'anneau $A[X_1, \ldots, X_n]$ n'est pas principal lorsque $n \geq 2$.

210. Soit M un A-module de type fini. Soit

$$\mu(M) = \mu_A(M) = \inf\{\mathrm{Card}(S) \mid S \subseteq M \text{ est générateur et fini}\}.$$

a. Supposons que A est un corps. Montrer que $\mu_A(M) = \dim_A M$.

b. Supposons que A est un anneau non nul. Montrer que $\mu_A(A^r) = r$ quel que soit $r \in \mathbb{N}$.

c. Soit $N \subseteq M$ un sous-A-module de type fini. Y a-t-il une relation entre $\mu(M)$ et $\mu(N)$?

d. Soit $N \subseteq M$ un sous-A-module. Montrer que $\mu(M/N) \leq \mu(M)$.

e. Montrer que $\mu(M \oplus N) \leq \mu(M) + \mu(N)$, où M et N sont des A-modules de type fini.

f. Montrer par un exemple que $\mu(M \oplus N)$ n'est pas forcément égal à $\mu(M) + \mu(N)$.

g. Soit $I \subseteq A$ un idéal, $I \subseteq \mathrm{Ann}(M)$. Montrer que $\mu_{A/I}(M) = \mu_A(M)$.

h. Soit $I \subseteq A$ un idéal. Montrer que $\mu_{A/I}(M/IM) \leq \mu_A(M)$.

i. Montrer par un exemple que $\mu_{A/I}(M/IM)$ n'est pas forcément égal à $\mu_A(M)$.

§4

211. Soit A un anneau et $S \subseteq A$ multiplicative.

a. Soient M et N des A-modules. Montrer que $S^{-1}(M \oplus N) \cong (S^{-1}M) \oplus (S^{-1}N)$.

b. Soit M_i un A-module, quel que soit $i \in I$, Montrer que $S^{-1}(\bigoplus_{i\in I} M_i) \cong \bigoplus_{i\in I}(S^{-1}M_i)$.

c. A-t-on un isomorphisme $S^{-1}(\prod_{i\in I} M_i) \cong \prod_{i\in I}(S^{-1}M_i)$?

212. Soit A un anneau et $S \subseteq A$ multiplicative. Soit M un A-module et $N \subseteq M$ un sous-A-module. Soit $i\colon N \to M$ l'inclusion.

a. Montrer que le morphisme $S^{-1}i\colon S^{-1}N \to S^{-1}M$ est injectif. On identifiera $S^{-1}N$ avec son image dans $S^{-1}M$.

b. Montrer que $(S^{-1}M)/(S^{-1}N) \cong S^{-1}(M/N)$.

213. Soit A un anneau, $S \subseteq A$ multiplicative et M un A-module. Montrer que $S^{-1}M$ est de type fini en tant que $S^{-1}A$-module lorsque M est un A-module de type fini.

214. Soit A un anneau intègre et M un A-module. Est-ce que M est de type fini lorsque M est de rang fini?

215. Soit A un anneau intègre. Soit M un A-module et $N \subseteq M$ un sous-A-module. Montrer que $\mathrm{rang}(N) \leq \mathrm{rang}(M)$.

216. Soit A un anneau intègre et K son corps de fractions.

a. Lorsque M est un A-module, le morphisme induit $(\mathrm{id}_M)_K$ par id_M est égal à l'identité id_{M_K}.

b. Soient $f\colon M \to N$ et $g\colon N \to P$ des morphismes de A-modules. Montrer que $(g \circ f)_K = g_K \circ f_K$.

c. Montrer que f_K est un isomorphisme lorsque $f\colon M \to N$ est un isomorphisme. Est-ce que le réciproque est vrai?

217. Soit A un anneau.

a. Soient M et N des A-modules. Montrer que $\mathrm{supp}(M \oplus N) = \mathrm{supp}(M) \cup \mathrm{supp}(N)$.

b. Soit $f\colon M \to N$ un morphisme de A-modules. Montrer que $\mathrm{supp}(M) = \mathrm{supp}(\ker(f)) \cup \mathrm{supp}(\mathrm{im}(f))$.

c. Soit $f\colon M \to N$ un morphisme de A-modules. Montrer que $f = 0$ lorsque $\mathrm{supp}(M) \cap \mathrm{supp}(N) = \emptyset$.

d. Soit $N \subseteq M$ un sous-A-module. Montrer que $\mathrm{supp}(N) \subseteq \mathrm{supp}(M)$.

e. Soit $N \subseteq M$ un sous-A-module. Montrer que $\mathrm{supp}(M/N) \subseteq \mathrm{supp}(M)$.

f. Soit $I \subseteq A$ un idéal et soit M un A-module. Montrer que

$$\mathrm{supp}_{A/I}(M/IM) = \mathrm{supp}_A(M) \cap \mathrm{Spec}(A/I).$$

g. Soit $S \subseteq A$ multiplicative et soit M un A-module. Montrer que

$$\mathrm{supp}_{S^{-1}A}(S^{-1}M) = \mathrm{supp}_A(M) \cap \mathrm{Spec}(S^{-1}A).$$

218. Soit A un anneau.

a. Soit M un A-module. Montrer que $\mathrm{supp}(M) \subseteq \mathrm{Spec}(A/\mathrm{Ann}(M))$.

b. Montrer que $\mathrm{supp}(M) = \mathrm{Spec}(A/\mathrm{Ann}(M))$ lorsque M est de type fini.

§5

219. a. Soient K un corps et

$$0 \longrightarrow V_0 \xrightarrow{f_0} V_1 \xrightarrow{f_1} \cdots \xrightarrow{f_{n-1}} V_n \longrightarrow 0$$

une suite exacte de K-espaces vectoriels de dimension finie. Montrer que

$$\sum_{i=0}^{n} (-1)^i \dim(V_i) = 0.$$

b. Soient A un anneau et

$$0 \longrightarrow M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} \cdots \xrightarrow{f_{n-1}} M_n \longrightarrow 0$$

une suite exacte de A-modules de type fini. Montrer que

$$\sum_{i=0}^{n} (-1)^i \mathrm{rang}(M_i) = 0.$$

220. Soit A un anneau intègre. Soit $f\colon M \to N$ un morphisme de A-modules, M étant de type fini. Montrer que $\mathrm{rang}(\ker(f)) + \mathrm{rang}(\mathrm{im}(f)) = \mathrm{rang}(M)$.

§6

221. Soit $f\colon M \to N$ un morphisme de A-modules. Montrer que $f(M_{\mathrm{tors}}) \subseteq N_{\mathrm{tors}}$.

222. Montrer que l'on ne peut définir le sous-module de «sans torsion» M_{st} d'un A-module M tel qu'on ait $f(M_{\mathrm{st}}) \subseteq N_{\mathrm{st}}$ pour chaque morphisme de A-modules $f\colon M \to N$.

223. Soit A un anneau intègre et K son corps de fractions. Soit M un A-module et

$$0 \longrightarrow A^n \xrightarrow{f} A^n \xrightarrow{g} M \longrightarrow 0$$

une suite exacte courte.

a. Montrer que M est un A-module de torsion.

b. Soit L la matrice de f dans la base standard. Montrer que $\det(L) \in \mathrm{Ann}(M)$.

c. Montrer par un exemple que $\det(L)$ n'est pas forcément un générateur de l'idéal $\mathrm{Ann}(M)$.

d. Montrer que f est surjectif si et seulement si $\det(L) \in A^\star$.

224.* Soit A un anneau principal.

a. Soit M un A-module de type fini sans torsion. Montrer que M est libre.

b. Soit M un A-module de type fini. Montrer que M est isomorphe à une somme directe $T \oplus L$ de A-modules où T est de torsion et L est libre.

225. a. Soit A un anneau dans lequel chaque élément régulier est inversible. Montrer que tout A-module est sans torsion.

b. Soit A un anneau fini. Montrer que tout A-module est sans torsion.

c. Montrer qu'un module de type fini sans torsion n'est pas forcément libre.

§7

226. Soient M et N des A-modules libres de rang fini. Montrer que les A-modules $\mathrm{Hom}_A(M, N)$ et $M^\Upsilon \otimes_A N$ sont isomorphes.

227. Soient M, N et P des A-modules. Soit $\beta\colon M \times N \to P$ une application A-bilinéaire. Soient $f\colon M' \to M$, $g\colon N' \to N$ et $h\colon P \to P'$ des morphismes de A-modules. Montrer que $\beta'\colon M' \times N' \to P'$ définie par $\beta'(m, n) = h(\beta(f(m), g(n)))$ est une application A-bilinéaire.

228. Soit $\beta\colon M \times N \to P$ une application A-bilinéaire. Soit $M' \subseteq M$ un sous-A-module tel que $\beta(m, n) = 0$ quel que soit $(m, n) \in M' \times N$. Montrer qu'il existe une unique application A-bilinéaire $\overline{\beta}\colon (M/M') \times N \to P$ telle que $\overline{\beta}(\overline{m}, n) = \beta(m, n)$ quel que soit $(m, n) \in M \times N$.

229. Soit $I \subseteq A$ un idéal. Soient M et N des A-modules. Montrer l'isomorphisme $(M \otimes_A N)/I(M \otimes_A N) \cong_{A/I} (M/IM) \otimes_{A/I} (N/IN)$ en montrant que le produit tensoriel $(M/IM) \otimes_{A/I} (N/IN)$ satisfait la propriété universelle du quotient $(M \otimes_A N)/I(M \otimes_A N)$.

230. Soit A un anneau et $S \subseteq A$ multiplicative. Soient M et N des A-modules. Montrer l'isomorphisme $S^{-1}(M \otimes_A N) \cong_{S^{-1}A} (S^{-1}M) \otimes_{S^{-1}A} (S^{-1}N)$ de deux façons :

a. en montrant que $S^{-1}(M \otimes_A N)$ satisfait la propriété universelle du produit tensoriel ;

b. en montrant que $(S^{-1}M) \otimes_{S^{-1}A} (S^{-1}N)$ satisfait la propriété universelle de la localisation $S^{-1}(M \otimes_A N)$.

231. Soit K un corps et V un K-espace vectoriel de dimension 2. Déterminer le sous-ensemble des tenseurs simples dans $V \otimes_K V$.

232. Soient M et N des A-modules. Soient $S \subseteq M$ et $T \subseteq N$ des systèmes générateurs. Montrer que $\{s \otimes t \mid s \in S,\ t \in T\}$ est un système générateur de $M \otimes_A N$.

233. Soient $a, b \in \mathbb{Z}$. Déterminer $d \in \mathbb{Z}$ tel que $\mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z}$ soit isomorphe à $\mathbb{Z}/d\mathbb{Z}$.

234. Soit $I \subseteq A$ un idéal et M un A-module.

a. Montrer qu'il y a un morphisme de A-modules f de $I \otimes_A M$ dans M qui envoie $x \otimes m$ sur xm.

b. Montrer que $\mathrm{im}(f) = IM$.

235. Soient $M_1, \ldots, M_n$ des A-modules. Une application f de $\prod_{i=1}^n M_i$ dans un A-module N est *multilinéaire* lorsque

$$f(m_1, \ldots, am_i + a'm_i', \ldots, m_n) = \\ = af(m_1, \ldots, m_i, \ldots, m_n) + a'f(m_1, \ldots, m_i', \ldots, m_n)$$

quels que soient $m_1, \ldots, m_n, m_i' \in M_i$, $a, a' \in A$ et $1 \leq i \leq n$.

a. Montrer qu'il existe un A-module $\bigotimes_{i=1}^n M_i$ et une application multilinéaire $\otimes$ de $\prod M_i$ dans $\bigotimes M_i$ qui est universelle.

b. Soient M, N et P des A-modules. Montrer que $M \otimes_A N \otimes_A P \cong_A M \otimes_A (N \otimes_A P)$.

c. Soient M, N et P des A-modules. Montrer que $(M \otimes_A N) \otimes_A P \cong_A M \otimes_A (N \otimes_A P)$.

236. Soit M un A-module. Soit n un entier non négatif. Soit $T_A^n(M) = \bigotimes_{i=1}^n M$. Soit $R_A^n(M)$ le sous-A-module de $T_A^n(M)$ engendré par les éléments

$$m_1 \otimes m_2 \otimes \cdots \otimes m_p \otimes \cdots \otimes m_q \otimes \cdots \otimes m_n + \\ - m_1 \otimes m_2 \otimes \cdots \otimes m_q \otimes \cdots \otimes m_p \otimes \cdots \otimes m_n$$

quels que soient $m_1, \dots m_n \in M$ et $1 \leq p < q \leq n$. On pose $\mathrm{Sym}^n_A(M)$ le quotient de $T^n_A(M)$ par $R^n_A(M)$. On appelle $\mathrm{Sym}^n_A(M)$ la *puissance symétrique n-ième* de M. On note la classe dans $\mathrm{Sym}^n_A(M)$ d'un élément $m_1 \otimes \cdots \otimes m_n$ de $T^n_A(M)$ encore par $m_1 \otimes \cdots \otimes m_n$. Le but de cet exercice est de montrer qu'elle satisfait une propriété universelle.

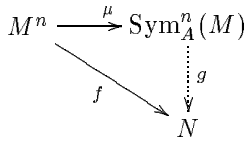
On appelle une application multilinéaire $f\colon M^n \to N$ dans un A-module N *symétrique* lorsque

$$f(m_1, \dots, m_p, \dots, m_q, \dots, m_n) = f(m_1, \dots, m_q, \dots, m_p, \dots, m_n)$$

quels que soient $m_1, \dots, m_n \in M$ et $1 \leq p < q \leq n$.

a. L'application μ de M^n dans $\mathrm{Sym}^n_A(M)$ qui envoie $(m_1, \dots, m_n)$ sur $m_1 \otimes \cdots \otimes m_n$ est multilinéaire symétrique.

b. Soit N un A-module et $f\colon M^n \to N$ multilinéaire symétrique. Montrer qu'il existe un unique morphisme de A-modules $g\colon \mathrm{Sym}^n_A(M) \to N$ tel que le diagramme suivant commute :



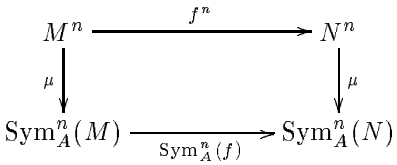
c. Montrer que $\mathrm{Sym}^n_A(M)$ est libre lorsque M l'est.

d. Montrer que $\mathrm{Sym}^n_A(M)$ est libre de rang $\frac{(n+r-1)!}{n!\cdot(r-1)!}$ lorsque M est libre de rang r.

e. Soit $I \subseteq A$ un idéal. Montrer que $\mathrm{Sym}^n_A(M)/I\mathrm{Sym}^n_A(M)$ est isomorphe à $\mathrm{Sym}^n_{A/I}(M/IM)$.

f. Soit $T \subseteq A$ multiplicative. Montrer que $T^{-1}\mathrm{Sym}^n_A(M)$ est isomorphe à $\mathrm{Sym}^n_{T^{-1}A}(T^{-1}M)$.

g. Soit $f\colon M \to N$ un morphisme de A-modules. Montrer qu'il existe un unique morphisme de A-modules $\mathrm{Sym}^n_A(f)\colon \mathrm{Sym}^n_A(M) \to \mathrm{Sym}^n_A(N)$ tel que le diagramme suivant commute :



237. Soit M un A-module. Soit $T^n_A(M) = \bigotimes_{i=1}^n M$. Soit $P^n_A(M)$ le sous-A-module de $T^n_A(M)$ engendré par les éléments de la forme

$$m_1 \otimes m_2 \otimes \cdots \otimes m_p \otimes \cdots \otimes m_q \otimes \cdots \otimes m_n$$

où $m_i \in M$ avec $m_p = m_q$, et $1 \leq p < q \leq n$. On pose $\bigwedge^n_A M$ le quotient de $T^n_A(M)$ par $P^n_A(M)$. On appelle $\bigwedge^n_A(M)$ la *puissance extérieure n-ième* de

M. On note la classe dans $\bigwedge_A^n M$ d'un élément $m_1 \otimes \cdots \otimes m_n$ de $T_A^n(M)$ par $m_1 \wedge \cdots \wedge m_n$. Le but de cet exercice est de montrer qu'elle satisfait une propriété universelle.

On appelle une application multilinéaire $f\colon M^n \to N$ dans un A-module N *alternée* lorsque

$$f(m_1, \ldots, m_p, \ldots, m_q, \ldots, m_n) = 0$$

quels que soient $m_1, \ldots, m_n \in M$ avec $m_p = m_q$, et $1 \leq p < q \leq n$.

a. Soit $f\colon M^n \to N$ multilinéaire alternée. Montrer que

$$f(m_1, \ldots, m_p, \ldots, m_q, \ldots, m_n) = -f(m_1, \ldots, m_q, \ldots, m_p, \ldots, m_n)$$

quels que soient $m_1, \ldots, m_n \in M$ et $1 \leq p < q \leq n$.

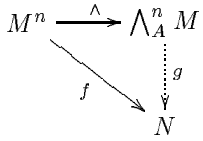
b. Soit $f\colon M^n \to N$ multilinéaire alternée. Montrer que

$$f(m_{\sigma(1)}, \ldots, m_{\sigma(n)}) = \operatorname{sign}(\sigma) \cdot f(m_1, \ldots, m_n)$$

quels que soient $m_1, \ldots, m_n \in M$ et $\sigma \in S_n$. Montrer par un exemple que la réciproque n'est pas vraie.

c. L'application $\wedge$ de M^n dans $\bigwedge_A^n M$ qui envoie $(m_1, \ldots, m_n)$ sur $m_1 \wedge \cdots \wedge m_n$ est multilinéaire alternée.

d. Soit N un A-module et $f\colon M^n \to N$ multilinéaire alternée. Montrer qu'il existe un unique morphisme de A-modules $g\colon \bigwedge_A^n M \to N$ tel que le diagramme suivant commute :



e. Montrer que $\bigwedge_A^n M$ est libre lorsque M l'est.

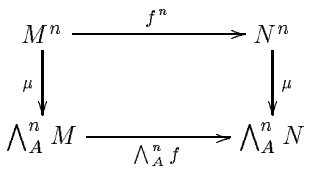
f. Montrer que $\bigwedge_A^n M$ est libre de rang $\frac{r!}{n! \cdot (r-n)!}$ lorsque M est libre de rang r et $0 \leq n \leq r$.

g. Montrer que $\bigwedge_A^n M = \{0\}$ lorsque M est libre de rang r et $n > r$.

h. Soit $I \subseteq A$ un idéal. Montrer que $\bigwedge_A^n M/I \bigwedge_A^n M$ est isomorphe à $\bigwedge_{A/I}^n (M/IM)$.

i. Soit $T \subseteq A$ multiplicative. Montrer que $T^{-1} \bigwedge_A^n M$ est isomorphe à $\bigwedge_{T^{-1}A}^n T^{-1}M$.

j. Soit $f\colon M \to N$ un morphisme de A-modules. Montrer qu'il existe un unique morphisme de A-modules $\bigwedge_A^n f\colon \bigwedge_A^n M \to \bigwedge_A^n N$ tel que le diagramme suivant commute :



k. Soit f un endomorphisme d'un A-module libre M de rang r. Soit $\mathcal{B}$ une base de M et soit L la matrice de f dans la base $\mathcal{B}$. Montrer que $\bigwedge_A^r f$ est la multiplication par $\det(L)$.

l. Soit L une matrice $n \times n$ à coefficients dans A. Montrer que $\det(L) = 0$ lorsque L a deux colonnes identiques.

m. Soit $L = (a_{ij})$ une matrice $n \times n$ à coefficients dans A. Montrer que $\det(L) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} L_{ij}$ quel que soit j, où L_{ij} est le cofacteur de L défini par

$$L_{ij} = \det\left((a_{kl})_{\substack{k,l=1,\dots,n \\ k \neq i, l \neq j}} \right).$$

n. Soient L et L' des matrices $r \times r$ à coefficients dans A. Montrer que $\det(LL') = \det(L)\det(L')$.

Chapitre 3

Algèbres

3.1 Algèbres et morphismes

Définition 3.1.1. Soit A un anneau (unitair et commutatif). Un A-module B muni d'une loi interne, notée par $\cdot$, est une *A-algèbre* lorsque $(B, +, \cdot)$ est un anneau unitair, pas nécessairement commutatif, et

ALG1 $a(b \cdot b') = (ab) \cdot b' = b \cdot (ab')$;

quels que soient $a \in A$ et $b, b' \in B$. B est une *A-algèbre commutative* lorsque l'anneau B est commutatif.

Exemple 3.1.2.

1. Chaque anneau B est automatiquement une $\mathbb{Z}$-algèbre.
2. Soit A un anneau et $A[X]$ l'anneau des polynômes en X à coefficients dans A. Alors $A[X]$ est une A-algèbre.
3. L'anneau des matrices $n \times n$ à coefficients dans un anneau A est une A-algèbre.
4. Lorsque A est un sous-anneau d'un anneau B, B est une A-algèbre.

Soit B un anneau pas forcément commutatif. On définit le *centre* de B par

$$\mathrm{Cent}(B) = \{b \in B \mid \forall b' \in B \colon bb' = b'b\}.$$

Lorsque B est une A-algèbre, l'application $\varphi \colon A \to B$ définie par $\varphi(a) = a \cdot 1$ est un morphisme d'anneaux. En effet, $\varphi(1) = 1 \cdot 1 = 1$ et $\varphi(a+a') = (a+a') \cdot 1 = a \cdot 1 + a' \cdot 1 = \varphi(a) + \varphi(a')$ pour tout $a, a' \in A$, puisque B est un A-module. De plus, $\varphi(a \cdot a') = (a \cdot a') \cdot 1 = a \cdot (a' \cdot 1) = a \cdot \varphi(a') = a \cdot (1 \cdot \varphi(a')) = (a \cdot 1) \cdot \varphi(a') = \varphi(a) \cdot \varphi(a')$ pour tout $a, a' \in A$. Par conséquent, φ est un morphisme d'anneaux. De plus, l'image de φ est contenu dans le centre de B. En effet, $b \cdot \varphi(a) = b \cdot (a \cdot 1) = a(b \cdot 1) = a(1 \cdot b) = (a \cdot 1) \cdot b = \varphi(a) \cdot b$ quel que soit $b \in B$. D'où $\varphi(a) \in \mathrm{Cent}(B)$ quel que soit $a \in A$. Résumant, lorsque B est une A-algèbre, l'application $\varphi \colon A \to B$ définie par $\varphi(a) = a \cdot 1$ est un morphisme s'anneaux tel que $\varphi(A) \subseteq \mathrm{Cent}(B)$.

Réciproquement, lorsque A et B sont des anneaux, B pas forcément commutatif, et $\varphi \colon A \to B$ est un morphisme d'anneaux tel que $\varphi(A) \subseteq \mathrm{Cent}(B)$, on peut définir une structure de A-algèbre sur B : Soit $a \cdot b = \varphi(a) \cdot b$ pour $a \in A$

et $b \in B$. Alors, B est un A-module et satisfait de plus condition **ALG1**. Donc, B est une A-algèbre.

On a alors :

Proposition 3.1.3. *Soit A un anneau. Se donner une A-algèbre B équivaut à se donner un morphisme d'anneaux $\varphi : A \to B$ dont l'image est contenue dans le centre de B.* □

Dans la suite, on entend par «A-algèbre» «A-algèbre commutative» pour simplifier.

Définition 3.1.4. Soient B et C des A-algèbres. Une application $f : B \to C$ est un *morphisme de A-algèbres* lorsque f est un morphisme d'anneaux et un morphisme de A-modules.

Exemple 3.1.5.

1. Chaque morphisme d'anneaux $f : B \to C$ est automatiquement un morphisme de $\mathbb{Z}$-algèbres.
2. L'identité id_B est un morphisme de A-algèbres lorque B est une A-algèbre.

Proposition 3.1.6. *Soient B et C des A-algèbres. Soient $\varphi : A \to B$ et $\psi : A \to C$ les morphismes d'anneaux correspondants. Une application f de B dans C est un morphisme de A-algèbres si et seulement si $f \circ \varphi = \psi$.*

Démonstration. Exercice. □

Proposition 3.1.7. *Soient B, C et D des A-algèbres. Soient $f : B \to C$ et $g : C \to D$ des morphismes de A-algèbres. Alors, $g \circ f$ est un morphisme de A-algèbres.*

Démonstration. Exercice. □

Définition 3.1.8. Un morphisme de A-algèbres $f : B \to C$ est un *isomorphisme* lorsqu'il existe un morphisme de A-algèbres $g : C \to B$ tel que $g \circ f = \mathrm{id}_B$ et $f \circ g = \mathrm{id}_C$. Les A-algèbres B et C sont alors dites *isomorphes*, noté par $B \cong_A C$, ou simplement par $B \cong C$. Un morphisme de A-algèbres d'une A-algèbre dans elle-même est un *endomorphisme*. Un endomorphisme qui est un isomorphisme est un *automorphisme*.

L'ensemble des automorphismes d'une A-algèbre B est noté par $\mathrm{Aut}_{A-\mathrm{Alg}}(B)$. Il est clair que $\mathrm{Aut}_{A-\mathrm{Alg}}(B)$ est un groupe.

Exemple 3.1.9. Les seuls automorphismes de $\mathbb{C}$ en tant que $\mathbb{R}$-algèbre sont l'identité $\mathrm{id}_{\mathbb{C}}$ et la conjugaison complexe. Le groupe $\mathrm{Aut}_{\mathbb{R}-\mathrm{Alg}}(\mathbb{C})$ est donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

3.2 Algèbres de polynômes

Soit A un anneau. L'anneau $A[X]$ de polynômes en X à coefficients dans A est naturellement une A-algèbre. Elle satisafait la propriété universelle suivante :

Propriété Universelle. *Soit A un anneau. Pour toute A-algèbre B et pour tout $b \in B$ il existe un unique morphisme de A-algèbres $f : A[X] \to B$ tel que $f(X) = b$.*

Démonstration. Exercice. □

Soit n un entier non négatif. L'algèbre $A[X_1, \ldots, X_n]$ des polynômes en $X_1, \ldots, X_n$ à coefficients dans A est universelle dans le sens suivant :

Propriété Universelle. *Soit A un anneau et n un entier non négatif. Pour toute A-algèbre B et pour tout $b_1, \ldots, b_n \in B$ il existe un et un seul morphisme de A-algèbres $f\colon A[X_1, \ldots, X_n] \to B$ tel que $f(X_i) = b_i$ pour tout $i = 1, \ldots, n$.*

Démonstration. Démonstration par récurrence. □

3.3 Extension de scalaires

Soit B une A-algèbre. Soit M un A-module. On va définir une structure de B-module sur le produit tensoriel $B \otimes_A M$. Soit $b \in B$ Soit $\mu_b\colon B \to B$ la multiplication par b, i.e., $\mu_b(b') = bb'$ quel que soit $b' \in B$. L'application μ_b étant A-linéaire, elle induit un morphisme de A-modules

$$\Phi(b) = \mu_b \otimes \mathrm{id}_M : B \otimes_A M \longrightarrow B \otimes_A M.$$

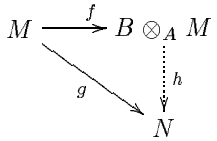
On a $\Phi(b + b') = \Phi(b) + \Phi(b')$, $\Phi(bb') = \Phi(b) \circ \Phi(b')$ et $\Phi(1) = \mathrm{id}$, i.e., $\Phi\colon B \to \mathrm{End}(M)$ est un morphisme d'anneaux. Par conséquent, Φ définit une structure de B-module sur $B \otimes_A M$. On a sur les tenseurs simples

$$b \cdot (b' \otimes m) = (bb') \otimes m.$$

Définition 3.3.1. Soit B une A-algèbre et M un A-module. Le B-module $B \otimes_A M$ est dit *obtenu par extension des scalaires de A à B.*

Exemple 3.3.2. Soient K et L des corps, K un sous-anneau de L. Soit V un K-espace vectoriel. Alors, $L \otimes_K V$ est un L-espace vectoriel. Dans le cas où $V = K^n$, $L \otimes_K V = L \otimes_K K^n \cong_L L^n$.

Propriété Universelle. *Soit B une A-algèbre et M un A-module. Soit $f\colon M \to B \otimes_A M$ le morphisme de A-modules défini par $f(m) = 1 \otimes m$. Alors, f est le morphisme universel de M dans un B-module, i.e., pour tout B-module N et pour tout morphisme de A-modules $g\colon M \to N$, il existe un unique morphisme de B-modules $h\colon B \otimes_A M \to N$ tel que le diagramme suivant commute*



Démonstration. Montrons d'abord que l'application $f\colon M \to B \otimes_A M$ est A-linéaire. Evidemment, f est additive. Soit $m \in M$ et $a \in A$. Alors, $f(am) = 1 \otimes (am) = a \cdot (1 \otimes m) = a \cdot f(m)$. Cela montre que f est A-linéaire.

Ensuite, montrons que le morphisme f est universel. Soit $g\colon M \to N$ un morphisme de A-modules où N est de plus un B-module. Définir $\beta\colon B \times M \to N$ par $\beta(b, m) = b \cdot g(m)$. On vérifie facilement que β est A-bilinéaire et induit alors un morphisme de A-modules $h\colon B \otimes_A M \to N$ tel que $h(b \otimes m) = b \cdot g(m)$. Vérifions que h est bien B-linéaire. Comme h est déjà A-linéaire, il suffit de

vérifier que $h(bx) = bh(x)$ pour tout $b \in B$ et $x \in B \otimes_A M$. Mais $B \otimes_A M$ est engendré comme A-module par les tenseurs simples, d'où il suffit de vérifier cette égalité pour ceux-là. Soient donc $b, b' \in B$ et soit $m \in M$. Alors, $h(b \cdot (b' \otimes m)) = h((bb') \otimes m) = bb'g(m) = b \cdot h(b' \otimes m)$. Cela montre bien que h est B-linéaire et donc l'existence de h.

Pour montrer l'unicité de h, soit $h' : B \otimes_A M \to N$ aussi un morphisme de B-modules satisfaisant $h' \circ f = g$. Montrons que h et h' coïncident sur les tenseurs simples de $B \otimes_A M$. Cela suffira pour montrer que $h = h'$. Soit donc $b \in B$ et $m \in M$. Alors, $h'(b \otimes m) = h'(b \cdot (1 \otimes m)) = b \cdot h'(1 \otimes m) = b \cdot (h' \circ f)(m) = b \cdot g(m) = h(b \otimes m)$. □

Corollaire 3.3.3. *Soit B une A-algèbre. Soient M et N des A-modules. Alors,*

$$B \otimes_A (M \oplus N) \cong_B (B \otimes_A M) \oplus (B \otimes_A N)$$
$$B \otimes_A (M \otimes_A N) \cong_B (B \otimes_A M) \otimes_B (B \otimes_A N)$$

Corollaire 3.3.4. *Soit B une A-algèbre. Soit S un ensemble. Alors,*

$$B \otimes_A A^{(S)} \cong_B B^{(S)}.$$

En particulier, $B \otimes_A A^n \cong_B B^n$.

Corollaire 3.3.5. *Soit $I \subseteq A$ un idéal. Considérer A/I comme A-algèbre par le morphisme de passage au quotient. Soit M un A-module. Alors,*

$$A/I \otimes_A M \cong_{A/I} M/IM.$$

Corollaire 3.3.6. *Soit $S \subseteq A$ multiplicative. Considérer $S^{-1}A$ comme A-algèbre par le morphisme de localisation. Soit M un A-module. Alors,*

$$S^{-1}A \otimes_A M \cong_{S^{-1}A} S^{-1}M.$$

Corollaire 3.3.7. *Soit A un anneau intègre. Soit K son corps de fractions. Considérer K comme A-algèbre par le morphisme de localisation. Soit M un A-module. Alors,*

$$K \otimes_A M \cong_K M_K.$$

3.4 Exercices

§1

238. Soit B une A-algèbre, pas forcément commutative. Une *sous-A-algèbre* de B est un sous-ensemble B' de B qui est à la fois un sous-A-module et un sous-anneau de B. Montrer que le centre $\mathrm{Cent}(B)$ est une sous-A-algèbre de B.

239.* Soit A un anneau principal. Soit $X \subseteq A$ un systéme de représentants pour les classes d'éléments associés. Lorsque B est une A-algèbre, soit $x \in X$ l'unique élément engendrant le noyau du morphisme $A \to B$. On appelle x la A-caractéristique de la A-algèbre B. Généraliser Exercice 91.

§2

240.* Soit A un anneau. Déterminer le groupe $\mathrm{Aut}_{A-\mathrm{Alg}}(A[X_1, \ldots, X_n])$.

241. Soit A un anneau.

a. Soit $I \subseteq A$ un idéal. Montrer que $A[X]/IA[X] \cong (A/I)[X]$.

b. Soit $S \subseteq A$ multiplicative. Montrer que $S^{-1}(A[X]) \cong S^{-1}A[X]$.

§3

242. Soit A un anneau.

a. Montrer que $A[X, Y] \cong_A A[T] \otimes_A A[T]$.

b. Montrer que $\otimes_A^n A[T]$ est isomorphe à l'algèbre des polynômes sur A en n indéterminées.

243. Soit B une A-algèbre. Soit M un A-module et N un B-module. Montrer que l'on a un isomorphisme

$$\mathrm{Hom}_A(M, N) \cong_B \mathrm{Hom}_B(B \otimes_A M, N).$$

244. Soit M un A-module. Soit $T^i(M) = \bigotimes_{i=1}^n M$.

245. Soit M un A-module. $S(M)$