II. Algèbre de base

Sommaire

1	Groupes	**35**
2	Anneaux et corps	**41**
3	Les nombres réels	**48**
4	Modules	**52**
5	Anneaux de polynômes	**59**
6	Matrices et espaces vectoriels	**64**
7	Déterminants	**68**
8	Polynômes symétriques	**72**
9	Notes	**75**

1 Groupes

Un **monoïde** est un ensemble G avec une application (ou loi de composition) φ de $G \times G$ vers G, habituellement écrite sous la forme $\varphi(a, b) = ab$, et un élément spécifié de G, habituellement noté 1, tel que pour tous a, b, $c \in G$

(i) $(ab)c = a(bc)$ (associativité),

(ii) $1a = a1 = a$ (élément neutre).

L'application φ est appelée la **multiplication** et l'élément 1 le **neutre**. L'associativité de la multiplication nous permet d'ignorer les parenthèses dans les produits $a_1 a_2 \cdots a_n$. Le monoïde est dit **abélien**, ou **commutatif**, lorsque $ab = ba$ pour tous éléments a et b. Dans un monoïde abélien, la loi φ est souvent appelée **addition** et écrite sous la forme $\varphi(a, b) = a + b$; l'élément neutre est alors noté 0. Dans ce cas nous parlons d'un monoïde **additif**, en opposition à un monoïde **multiplicatif**. Dans un monoïde multiplicatif, nous écrivons le produit itéré n fois $aa \cdots a$ sous la forme a^n pour chaque entier strictement positif n, et nous posons $a^0 = 1$; dans un monoïde additif, nous écrivons la somme itérée n fois $a + a + \cdots + a$ sous la forme na et nous écrivons $0a = 0$.

Si X est un ensemble, l'ensemble des fonctions de X vers X forme un monoïde : la multiplication est la composition des fonctions, et l'élément neutre est la fonction identique. L'ensemble des entiers naturels $\mathbb{N}$ est un monoïde commutatif pour l'addition, avec 0 pour élément neutre.

Un **homomorphisme de monoïdes** est une fonction f d'un monoïde G vers un monoïde H telle que $f(1) = 1$ et $f(ab) = f(a)f(b)$ pour tous a et $b \in G$. Si G est un monoïde multiplicatif, et $a \in G$, alors l'application de $\mathbb{N}$ vers G qui envoie n sur a^n est un homomorphisme. Un homomorphisme f est **non trivial** si $\{1\}$ est un sous-ensemble propre de im f. Un sous-ensemble H d'un monoïde G est un **sous-monoïde** si $1 \in H$ et si H est stable pour la multiplication. Si S est un sous-ensemble du monoïde G, alors l'ensemble formé par 1 et tous les produits finis d'éléments de S est un sous-monoïde de G appelé le **sous-monoïde engendré par** S. Le sous-monoïde de $\mathbb{N}$ engendré par $\{3, 4\}$ est $\mathbb{N} \setminus \{1, 2, 5\}$.

Soit X un ensemble. Définissons X^* comme l'ensemble des suites finies d'éléments de X, y compris la suite vide. Les éléments de X^* sont appelés des **mots**. Deux mots $u \equiv x_1 x_2 \cdots x_m$ et $v \equiv y_1 y_2 \cdots y_n$ sont **égaux** si $m = n$ et $x_i = y_i$ pour $i = 1, 2, \cdots, m$. Si u et v sont égaux dans X^* nous écrirons $u \equiv v$. On définit une **multiplication** (appelée aussi **concaténation**) sur X^* en posant $uv \equiv x_1 \cdots x_m y_1 \cdots y_n$. Cette multiplication est associative et le mot vide est l'élément neutre, de sorte que X^* est un monoïde, appelé le **monoïde libre sur l'ensemble** X. Si X est un ensemble à un élément, X^* est isomorphe au monoïde additif des entiers naturels.

Si a et b sont des éléments d'un monoïde et si $ab = 1$, alors disons que a est un **inverse à gauche** de b et que b est un **inverse à droite** de a. Si b a un inverse à gauche a et un inverse à droite c, alors $a = a(bc) = (ab)c = c$; dans ce cas nous disons que a est l'**inverse** de b et nous écrivons $a = b^{-1}$. Si b a un inverse nous disons que b est une **unité**, ou que b est **inversible**.

Un **groupe** est un monoïde G dans lequel tout élément est inversible. Dans un groupe additif, l'inverse de a est noté $-a$ plutôt que a^{-1}. Pour un entier strictement positif n nous définissons a^{-n} comme $(a^{-1})^n$; les lois usuelles pour les exposants sont valables. Dans un groupe additif, cette définition prend la forme $(-n)a = n(-a)$, et les lois de distributivité et d'associativité s'appliquent (voir la définition d'un R-module dans la section 3). Le prototype d'un groupe abélien est le groupe des entiers $\mathbb{Z}$ pour l'addition.

L'**ordre** d'un élément a d'un groupe est la cardinalité de l'ensemble $\{\, a^n : n \in \mathbb{N} \,\}$. L'ordre de a est $n \in \mathbb{N}$ si, et seulement si, $a^n = 1$ et $a^m \neq 1$ pour $m = 1, \ldots, n-1$. Dans le groupe $\mathbb{Z}$ l'élément 0 est d'ordre 1, comme l'élément neutre dans n'importe quel groupe, et tout élément non nul est d'ordre infini. Dans un groupe discret l'ordre d'un élément a est la cardinalité de l'ensemble $\{\, n \in \mathbb{N} : a^m \neq 1$ pour tous les m tels que $0 < m \leqslant n \,\}$ (cet ensemble contient 0), et par suite c'est un ordinal $\beta \leqslant \omega$.

Si G et H sont des groupes et si f est un homomorphisme de monoïdes de G

vers H, alors $f(a^{-1}) = f(a)^{-1}$ et $f(a^{-1})f(a) = f(a^{-1}a) = f(1) = 1$. Par suite un homomorphisme de monoïdes entre deux groupes préserve toute la structure de groupe : multiplication, élément neutre et inverse. Si G est un groupe et si $a \in G$, alors l'application qui envoie $x \in G$ sur axa^{-1} est un automorphisme de G, comme on le voit facilement ; un tel automorphisme est appelé **intérieur**.

Si G et H sont des groupes abéliens, alors l'ensemble $\mathrm{Hom}(G, H)$ des homomorphismes de G vers H a une structure naturelle de groupe abélien obtenue en posant $(f_1 + f_2)(x) = f_1(x) + f_2(x)$. Les groupes $\mathrm{Hom}(\mathbb{Z}, H)$ et H sont naturellement isomorphes en considérant l'application qui envoie $f \in \mathrm{Hom}(\mathbb{Z}, H)$ sur $f(1) \in H$. Si h est un homomorphisme de H vers H', alors h induit un homomorphisme de $\mathrm{Hom}(G, H)$ vers $\mathrm{Hom}(G, H')$ qui envoie f sur hf ; c'est-à-dire que l'on a $h(f_1 + f_2) = hf_1 + hf_2$. De la même manière un homomorphisme $g\colon G' \to G$ induit un homomorphisme de $\mathrm{Hom}(G, H)$ vers $\mathrm{Hom}(G', H)$ qui envoie f sur fg.

Une catégorie $\mathcal{C}$ comme la catégorie des groupes abéliens, telle que $\mathcal{C}(G, H)$ est un groupe abélien pour chaque couple d'objets G et H de $\mathcal{C}$, et telle que les fonctions induites de $\mathcal{C}(G, H)$ vers $\mathcal{C}(G, H')$ par une flèche $H \to H'$, et de $\mathcal{C}(G, H)$ vers $\mathcal{C}(G', H)$ par une flèche $G' \to G$, sont des homomorphismes de groupes, est appelée une **catégorie pré-additive**.

Une **permutation** d'un ensemble X est une bijection de X sur lui-même. L'ensemble des permutations de X est un groupe appelé le **groupe symétrique** sur X. Si $x_1, \ldots, x_n$ sont des éléments distincts dans un ensemble discret X, alors nous notons $(x_1, \ldots, x_n)$ la permutation π de X telle que

$$\pi x_i = x_{i+1} \text{ pour } i = 1, \ldots, n-1, \quad \pi x_n = x_1, \quad \pi x = x \text{ sinon.}$$

Une telle permutation est appelée un n-**cycle** de **support** $\{x_1, \ldots, x_n\}$, et deux cycles sont appelés **disjoints** si leurs supports sont disjoints. Si X est un ensemble fini, alors toute permutation est un produit de cycles disjoints. Comme $(x_1, \ldots, x_n) = (x_1, x_n) \cdots (x_1, x_3)(x_1, x_2)$, toute permutation d'un ensemble fini est un produit de 2-cycles (non nécessairement disjoints). Une permutation qui peut être écrite comme un produit d'un nombre pair de 2-cycles est appelée une permutation **paire**, et sinon **impaire**. Si π est une permutation d'un ensemble fini nous définissons

$$\operatorname{sgn} \pi = \begin{cases} 1 & \text{si } \pi \text{ est paire} \\ -1 & \text{si } \pi \text{ est impaire.} \end{cases}$$

Le produit d'un nombre pair de 2-cycles ne peut pas être égal au produit d'un nombre impair de 2-cycles (exercice 7). Par suite la signature est bien définie et $\operatorname{sgn} \pi_1\pi_2 = (\operatorname{sgn} \pi_1)(\operatorname{sgn} \pi_2)$ (exercice 8).

Un **sous-groupe** d'un groupe est un sous-monoïde stable pour le passage à l'inverse. Si G est un groupe, G et $\{1\}$ sont des sous-groupes de G ; nous notons

souvent le sous-groupe $\{1\}$ par 1. Si S est un sous-ensemble d'un groupe G, alors l'ensemble

$$\langle S\rangle = \{1\} \cup \{\, s_1 s_2 \cdots s_k : s_i \in S \cup S^{-1},\, k \geqslant 1 \,\}$$

de tous les produits finis d'éléments de S, ou d'inverses d'éléments de S, est un sous-groupe de G appelé le **sous-groupe engendré par** S. Si $\langle S\rangle = G$, alors S est appelé un **ensemble de générateurs**, ou un **système générateur** pour G. Un groupe est **de type fini** s'il possède un système générateur finiment énumérable, **cyclique** s'il possède un système générateur à un élément. Le groupe additif $\mathbb{Q}$ des nombres rationnels n'est pas de type fini ; en fait, tout sous-groupe de type fini de $\mathbb{Q}$ est cyclique (on voit facilement que tout sous-groupe de type fini de $\mathbb{Q}$ est *contenu dans* un sous-groupe cyclique).

Un sous-groupe H d'un groupe G est **normal** si $ghg^{-1} \in H$ pour tous $g \in G$ et $h \in H$. Tout sous-groupe d'un groupe abélien est normal. Si f est un homomorphisme de G vers H, alors on voit facilement que le **noyau** de f,

$$\ker f = \{\, x \in G : f(x) = 1 \,\} = f^{-1}(1)$$

est un sous-groupe normal de G. La taille du noyau de f nous dit dans quelle mesure f échoue à être injectif, comme le montre l'équivalence des propriétés suivantes :

— $f(a) = f(b)$,
— $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = 1$,
— $ab^{-1} \in \ker f$,

de sorte que f est un monomorphisme si, et seulement si, $\ker f = 1$. Nous étudierons les structures algébriques qui sont des groupes abéliens avec une structure additionnelle. Dans ces cas le noyau d'un homomorphisme f signifie le noyau de f en tant qu'homomorphisme de groupes ; si le groupe est écrit additivement, comme c'est normalement le cas pour ces structures plus complexes, on a $\ker f = f^{-1}(0)$.

Tout sous-groupe normal H d'un groupe G est le noyau d'un homomorphisme construit comme suit. L'ensemble G/H a les mêmes éléments que G, mais l'égalité est définie en posant $a = b$ si $ab^{-1} \in H$. Quand il est nécessaire de distinguer entre les deux égalités sur G et sur G/H nous écrivons $a = b \bmod H$ pour noter l'égalité dans G/H. La multiplication et le passage à l'inverse restent des fonctions par rapport à l'égalité de G/H, et donc G/H est un groupe, appelé le **groupe quotient** de G par H. Le prototype d'un groupe quotient est obtenu en prenant pour G le groupe $\mathbb{Z}$ des entiers et en prenant pour H le sous-groupe de $\mathbb{Z}$ formé par les multiples d'un entier donné n ; le groupe quotient G/H est alors le groupe $\mathbb{Z}_n$ des entiers modulo n.

Les faits essentiels qui relient les sous-groupes normaux et les groupes quotients sont réunis dans le théorème suivant.

Théorème 1.1. *Soient N un sous-groupe normal d'un groupe G et f un homomorphisme de G vers un groupe L avec $f(N) = 1$. Alors f est un homomorphisme de G/N vers L. Si f est surjectif et si le noyau de f est N, alors f est un isomorphisme de G/N sur L.*

Démonstration. Si $a = b \pmod N$, alors $ab^{-1} \in N$, d'où $f(a) = f(b)$; par suite f est une fonction sur G/N, qui est clairement un homomorphisme. Réciproquement si $f(a) = f(b)$, alors $f(ab^{-1}) = 1$, de sorte que $ab^{-1} \in N$ et $a = b \pmod N$. Par suite, si $\ker f = N$, alors f est une fonction injective de G/N vers L ; et donc, si $f\colon G \to L$ est surjective, la fonction $f\colon G/N \to L$ possède un inverse g. Clairement g est aussi un homomorphisme. □

Soit N un sous-groupe normal du groupe G. Un sous-groupe (normal) de G/N est un sous-groupe (normal) H de G qui est un sous-ensemble de G/N, c'est-à-dire, si $a \in H$ et $a = b \pmod N$, alors $b \in H$. On voit facilement qu'un sous-groupe H de G est un sous-ensemble de G/N exactement dans le cas où $N \subseteq H$. La différence entre un sous-groupe H de G contenant N et un sous-groupe H de G/N est la relation d'égalité sur H. Nous faisons la distinction entre H comme un sous-groupe de G et H comme un sous-groupe de G/N en écrivant H/N pour ce dernier. Si H est un sous-groupe normal de G qui contient N, alors $(G/N)/(H/N)$ est isomorphe à G/H ; en fait, les éléments des deux groupes sont simplement les éléments de G, et les égalités sont les mêmes.

Théorème 1.2. *Soient H et K des sous-groupes du groupe G. Si K est normal, alors*

(i) *l'ensemble $HK = \{\, hk : h \in H \text{ et } k \in K \,\}$ est un sous-groupe,*

(ii) *le sous-groupe $H \cap K$ est normal dans H, et*

(iii) *les groupes quotients HK/K et $H/(H \cap K)$ sont isomorphes.*

Démonstration. Exercice. □

Dans un groupe additif, le sous-groupe HK est écrit sous la forme $H + K$.

Si $a \in G$ et si H est un sous-groupe de G, alors $Ha = \{\, ha : h \in H \,\}$ est appelé une **classe à droite** de H, tandis que $aH = \{\, ah : h \in H \,\}$ est appelée une **classe à gauche** de H. Le passage à l'inverse induit une bijection entre classes à gauche et à droite de H qui envoie aH sur Ha^{-1}, et nous pouvons donc parler sans ambigüité de la cardinalité de l'ensemble des classes de H dans G. Cette cardinalité est appelée l'**indice** de H dans G et nous le notons $[G : H]$. Si H est normal, alors $Ha = aH$ pour chaque élément a de G.

Exercices

1. Montrer que dans un monoïde fini, si a possède un inverse à droite ou à gauche, alors $a^n = 1$ pour un entier strictement positif n, de sorte que

l'élément peut avoir au plus un inverse à droite ou à gauche. Donner un exemple d'un élément dans un monoïde qui admet deux inverses à gauche distincts ; deux inverses à droite distincts.

2. Montrer qu'un monoïde peut être identifié avec une catégorie à un seul objet, et que les homomorphismes de monoïdes sont des foncteurs entre les catégories correspondantes. Parmi ces catégories, lesquelles correspondent à des groupes ?

3. Montrer que l'ensemble des unités d'un monoïde est un groupe.

4. Montrer que l'ensemble S des suites binaires forme un groupe abélien G pour l'addition des coordonnées modulo 2. Soit $a \in S$ et définissons $b, c \in S$ par $b_n = 1$ si, et seulement si, $a_n = 1$ et $a_m = 0$ pour tous les $m < n$, et $c_n = 1$ si, et seulement si, $b_{n-1} = 1$. Montrer que si le sous-groupe de G engendré par b et c est engendré par un sous-ensemble fini de G, alors, ou bien $a = 0$, ou bien $a \neq 0$.

5. Soit G un groupe multiplicatif avec une inégalité. L'inégalité est dite **invariante par translation** si $x \neq y$ implique $zx \neq zy$ et $xz \neq yz$. Étant donnée une inégalité invariante par translation, montrer que

   (i) le passage à l'inverse qui envoie x sur x^{-1} est fortement extensionnel si, et seulement si, l'inégalité est symétrique.

   (ii) l'inégalité est cotransitive si, et seulement si, la multiplication est fortement extensionnelle (l'inégalité sur $G \times G$ est donnée par $(x_1, x_2) \neq (y_1, y_2)$ si $x_1 \neq y_1$ ou $x_2 \neq y_2$).

   Enfin, démontrer que si l'inégalité est consistante et si la multiplication est fortement extensionnelle, alors l'inégalité est invariante par translation.

6. En regardant une inégalité sur G comme un sous-ensemble de $G \times G$, montrer que la réunion d'une famille d'inégalités sur un groupe G pour lesquelles la loi de groupe est fortement extensionnelle est elle-même une inégalité de cette sorte. Montrer qu'il existe une unique inégalité sur G/N qui rend le théorème 1.1 vrai dans la catégorie des groupes avec inégalité, avec pour flèches les homomorphismes fortement extensionnels. Montrer que si G est l'ensemble des suites binaires avec pour addition l'addition des coordonnées modulo 2 et si $N = \{\, x \in G : \text{il y a un } m \text{ tel que } x_n = 0 \text{ pour tous } n \geqslant m \,\}$, alors $x \neq 0$ dans G/N si, et seulement si, $x_n = 1$ une infinité de fois et LPO est valide.

7. Soient $x_1, \ldots, x_m, y_1, \ldots, y_n$ des éléments distincts d'un ensemble fini X, soit G le groupe symétrique sur X, et soit $1 \leqslant i < j \leqslant m$. Vérifiez les deux égalités suivantes sur G.

   (i) $(x_i, x_j)(x_1, \ldots, x_m) = (x_1, \ldots, x_{i-1}, x_j, \ldots, x_m)(x_i, \ldots, x_{j-1})$

   (ii) $(x_1, y_1)(x_1, \ldots, x_m)(y_1, \ldots, y_n) = (y_1, \ldots, y_n, x_1, \ldots, x_m)$.

Pour $\pi \in G$, nous pouvons écrire π d'une manière essentiellement unique comme un produit de cycles disjoints dont les supports recouvrent X [1]. Soit N_π le nombre de cycles dans un tel produit. En utilisant (i) et (ii), montrer que si τ est un 2-cycle, alors $N_{\tau\pi} = N_\pi \pm 1$. En conclure qu'une permutation paire ne peut pas être écrite comme produit d'un nombre impair de 2-cycles.

8. Montrer que la fonction sgn est un homomorphisme du groupe symétrique d'un ensemble fini vers le groupe multiplicatif $\{-1, 1\}$.
9. Donner un exemple brouwerien d'un sous-groupe d'un groupe abélien fini qui est engendré par un sous-ensemble dénombrable mais qui n'est pas de type fini.
10. Montrer que l'ensemble des sous-groupes normaux d'un groupe est un treillis modulaire.

2 Anneaux et corps

Un **anneau** est un groupe abélien additif R qui est aussi un monoïde multiplicatif, les deux structures étant reliées par les **lois de distributivité** :

$$\begin{aligned} a(b+c) &= ab+ac, \\ (a+b)c &= ac+bc. \end{aligned}$$

Un anneau est **trivial** si $0 = 1$. Si la structure de monoïde multiplicatif est commutative, alors R est un **anneau commutatif**. Une **unité** de R est une unité du monoïde multiplicatif de R. On dit qu'un anneau a des **unités détachables** lorsque ses unités forment d'un sous-ensemble détachable.

Si A est un groupe abélien, alors l'ensemble des endomorphismes $\mathrm{E}(A) = \mathrm{Hom}(A, A)$ est un anneau (en prenant pour multiplication la composition) appelé l'**anneau des endomorphismes** de A. Plus généralement, si $\mathcal{C}$ est une catégorie pré-additive, $\mathcal{C}(A, A)$ est un anneau pour chaque objet A de $\mathcal{C}$.

Un anneau non trivial k est un **anneau à division** [2] (ou un **corps gauche**) si, pour chaque a et $b \in k$,

$$a \neq b \text{ si, et seulement si, } a - b \text{ est une unité.}$$

Nous rappelons à la lectrice que l'interprétation du symbole $a \neq b$ dépend du contexte : si k possède une inégalité, alors $a \neq b$ fait référence à cette inégalité, et sinon $a \neq b$ fait référence à la non-égalité. Une conséquence immédiate de la définition est que si k est un anneau à division, alors l'inégalité sur k est

1. **NdT.** Ici, pour recouvrir X, nous acceptons les cycles (a), de support $\{a\}$, tous égaux à la permutation identité.
2. **NdT.** Division ring.

symétrique et **invariante par translation** : si $a \neq b$, alors $a + c \neq b + c$. Notez que la non-égalité est automatiquement invariante par translation parce que l'addition est une fonction.

Naturellement, nous pourrions définir l'inégalité $a \neq b$ sur un anneau arbitraire comme signifiant que $a - b$ est une unité et, techniquement, nous aurions alors un anneau à division ; de sorte que la théorie générale des anneaux à division contient la théorie des anneaux. Cependant, l'idée est d'utiliser le symbole $a \neq b$ pour représenter des relations qui peuvent être raisonnablement appelées des inégalités : si vous prenez une inégalité stupide et que vous obtenez un anneau à division stupide, ne nous blâmez pas. Comme règle de conduite, vous pouvez choisir une inégalité standard. Pour l'essentiel, nous serons intéressés par des anneaux à division qui sont discrets, et, dans une moindre mesure, par des anneaux à division avec une relation de séparation étroite.

Les éléments non nuls d'un anneau à division sont exactement les unités ; dans le cas discret c'est une propriété caractéristique des anneaux à division (exercice 3). Un **corps** est un anneau à division commutatif. Un **corps de Heyting** est un corps avec une relation de séparation étroite. Dans un corps de Heyting ou plus généralement dans un corps avec une inégalité cotransitive, les opérations arithmétiques sont fortement extensionnelles (exercice 5). Les nombres rationnels $\mathbb{Q}$ forment un corps discret ; les nombres réels (section suivante) forment un corps de Heyting. Les quaternions rationnels (exercice 4) forment un anneau à division discret et non commutatif.

Un sous-ensemble d'un anneau est un **sous-anneau** si c'est un sous-groupe additif et un sous-monoïde multiplicatif. Soit S un sous-anneau d'un anneau commutatif R, et soient $a_1, \ldots, a_n$ des éléments de R. Alors l'ensemble des sommes d'éléments de R de la forme

$$s a_1^{m_1} a_2^{m_2} \cdots a_n^{m_n},$$

avec $s \in S$ et $m_i \in \mathbb{N}$, est un sous-anneau de R que l'on note $S[a_1, \ldots, a_n]$; il est contenu dans tout sous-anneau de R qui contient $S \cup \{a_1, \ldots, a_n\}$. Si S et R sont des corps, alors $S(a_1, \ldots, a_n)$ désigne l'ensemble des quotients f/g avec $f, g \in S[a_1, \ldots, a_n]$ et $g \neq 0$. On voit facilement que $S(a_1, \ldots, a_n)$ est un corps contenu dans chaque sous-corps de R qui contient $S \cup \{a_1, \ldots, a_n\}$.

Un **anneau intègre**, ou encore un **domaine d'intégrité** est un anneau avec inégalité qui est isomorphe à un sous-anneau d'un corps ; de manière plus informelle, un anneau intègre est simplement un sous-anneau d'un corps. Si R est un sous-anneau d'un corps, alors l'ensemble $\{\, ab^{-1} : a, b \in R \text{ et } b \neq 0 \,\}$ est un corps qui contient R, appelé le **corps de fractions** de R. Le corps de fractions d'un anneau intègre est essentiellement unique (exercice 6).

Si R est un anneau intègre discret, alors, pour chaque a et $b \in R$,

$$\text{si } a \neq 0 \text{ et } b \neq 0, \text{ alors } ab \neq 0. \qquad (*)$$

Inversement, si R est un anneau commutatif intègre discret qui satisfait la condition $(*)$, alors nous pouvons **immerger** [1] R dans un corps discret k en imitant la construction du corps des nombres rationnels $\mathbb{Q}$ à partir de l'anneau des nombres entiers $\mathbb{Z}$. Soit $k = \{\,(a,b) \in R \times R : b \neq 0\,\}$ avec $(a,b) = (c,d)$ si $ad = bc$. Nous définissons la multiplication sur k par $(a,b)\cdot(c,d) = (ac,bd)$ et l'addition par $(a,b)+(c,d) = (ad+bc,bd)$. On vérifie sans peine que cela fait de k un anneau avec l'élément neutre additif $(0,1)$ et l'élément neutre multiplicatif $(1,1)$. Si $(a,b) \neq (0,1)$, alors $a \neq 0$ et donc l'élément (b,a) est dans k et $(a,b)(b,a) = (1,1)$; inversement, si $(a,b)(c,d) = (1,1)$, alors $ac = bd \neq 0$, d'où $a \neq 0$ et $(b,a) \in k$, et par suite k est un corps. Nous immergeons R dans k en envoyant a sur $(a,1)$.

Une caractérisation intrinsèque d'un anneau intègre arbitraire est donnée dans l'exercice 7. Pour démontrer que cette caractérisation est correcte, construisez le corps de fractions comme dans le cas discret.

Si k est un corps, alors le sous-corps de k formé par tous les éléments de la forme $(n\cdot 1)/(m\cdot 1)$ où m et n sont des entiers et $m\cdot 1 \neq 0$, est le plus petit sous-corps de k, et il est appelé le **sous-corps premier** [2] de k. Ce corps est le corps de fractions du sous-anneau $\{\,n\cdot 1 : n \in \mathbb{Z}\,\}$ de k. Si $a_1,\ldots,a_n \in k$ et si k_0 est le sous-corps premier de k, nous disons que k est **engendré par** $a_1,\ldots,a_n$ si $k_0(a_1,\ldots,a_n) = k$. Un **corps premier** est un corps égal à son sous-corps premier.

Une fonction f d'un anneau R vers un anneau S est un **homomorphisme d'anneaux** si c'est un homomorphisme des groupes additifs et un homomorphisme des monoïdes multiplicatifs. La fonction de l'anneau des entiers $\mathbb{Z}$ vers S qui envoie n sur $n\cdot 1$ est un homomorphisme d'anneaux. Un sous-groupe additif I d'un anneau R est un **idéal** si pour tous $x \in I$ et $r \in R$ les éléments rx et xr sont dans I. On voit facilement que si f est un homomorphisme d'anneaux, alors $\ker f = f^{-1}(0)$ est un idéal. Un idéal I est **propre** si $1 \notin I$. Un **idéal à gauche** (resp. **idéal à droite**) I d'un anneau R est un sous-groupe additif de R tel que pour tous $r \in R$ et $x \in I$ l'élément rx (resp. xr) appartient à I. Un idéal à gauche I d'un anneau est **non nul** si I contient un élément non nul. Pour éviter la confusion entre idéaux à gauche, idéaux à droite et idéaux, un idéal est souvent appelé un **idéal bilatère**. Si I est un idéal bilatère de l'anneau R, alors la multiplication est une loi de composition sur le groupe quotient R/I, de sorte que R/I est un anneau.

Soient X et Y des sous-ensembles de l'anneau R. On définit XY comme le sous-groupe additif de R engendré par $\{\,xy : x \in X \text{ et } y \in Y\,\}$. Si X, Y et Z sont des sous-ensembles de R, alors $(XY)Z = X(YZ)$. Un sous-ensemble non

1. **NdT.** To embed. Nous utilisons dans la traduction de cet ouvrage la terminologie peu habituelle « immerger A dans B » pour dire qu'on donne un isomorphisme de l'objet A sur un sous-objet de B. Nous disons aussi parfois « plonger A dans B », et nous utilisons les termes de « plongement » ou « immersion ».

2. **NdT.** Prime field of k.

vide I est un idéal si, et seulement si, $RIR = I$, tandis que I est un idéal à gauche (resp. à droite) si $RI = I$ (resp. $IR = I$).

Si S est un sous-ensemble d'un anneau R, alors $(S) := RSR$ est le plus petit idéal de R contenant S, et on l'appelle l'**idéal engendré par** S. Si S est la famille finie $\{s_1, \ldots, s_n\}$, alors l'idéal engendré par S est noté $(s_1, \ldots, s_n)$. L'**idéal à gauche engendré par** S est RS, tandis que l'**idéal à droite engendré par** S est SR ; si S est un ensemble à un élément $\{s\}$, alors l'idéal à gauche ou à droite correspondant est appelé **principal**, et on le note Rs ou sR.

Si I et J sont des idéaux, alors IJ et $I \cap J$ sont des idéaux. L'ensemble $I \cup J$ n'est pas nécessairement un idéal ; l'idéal engendré par $I \cup J$ est l'ensemble $\{\, i + j : i \in I \text{ et } j \in J \,\}$ et on le note $I + J$. Plus généralement, si $\{I_i\}$ est une famille d'idéaux, alors l'idéal engendré par $\bigcup_i I_i$ est noté $\sum_i I_i$.

Le **transporteur**[1] **d'un ensemble** S **dans un idéal à gauche** I est l'idéal à gauche

$$I : S = \{\, x \in R : xS \subseteq I \,\}.$$

Le **radical** d'un idéal I dans un anneau commutatif est l'idéal $\sqrt{I} = \{\, x \in R : x^n \in I \text{ pour un } n \,\}$.

Le théorème fondamental des homomorphismes d'anneaux résulte immédiatement du théorème correspondant pour les groupes.

Théorème 2.1. *Soit I un idéal de l'anneau R. Si f est un homomorphisme de R vers un anneau S avec $f(I) = 0$, alors f est un homomorphisme de R/I vers S. Si f est surjectif et si le noyau de f est l'idéal I, alors f est un isomorphisme de R/I sur S.*

Soit I un idéal de l'anneau R. Un idéal (à gauche) de R/I est un idéal (à gauche) J de R contenant I. Si J est un idéal de R contenant I, alors $R/J \simeq (R/I)/(J/I)$.

Théorème 2.2. *Soient R un anneau, S un sous-anneau et I un idéal de R. Alors $S + I$ est un sous-anneau de R contenant I en tant qu'idéal, $S \cap I$ est un idéal de S, et $(S + I)/I \simeq S/(S \cap I)$.*

Démonstration. Clairement $S + I$ est un sous-anneau et I est un idéal de $S + I$. Définissons une fonction f de $S/(S \cap I)$ vers $(S + I)/I$ en posant $f(s) = s$. Notez que f est bien une fonction parce que si $s_1 = s_2$ dans $S/(S \cap I)$, alors $s_1 - s_2 \in I$ et donc $s_1 = s_2$ dans $(S+I)/I$. Clairement f est un homomorphisme. Maintenant définissons une fonction g de $(S + I)/I$ vers $S/(S \cap I)$ en posant $g(s + i) = s$. Pour voir que g est une fonction nous remarquons que si $s_1 + i_1 = s_2 + i_2$ dans $(S + I)/I$, alors $s_1 - s_2 \in I$, et donc $s_1 = s_2$ dans $S/(S \cap I)$. Il s'ensuit que f est un isomorphisme. □

1. **NdT.** Quotient of a left ideal I by a set S

Si P est un idéal d'un anneau commutatif R, alors nous disons que P est un **idéal premier** [1] si chaque fois que $xy \in P$, alors $x \in P$ ou $y \in P$. Si P est un idéal détachable propre de R, alors on voit facilement que P est premier si, et seulement si, R/P est un anneau intègre. Si p est un nombre premier, alors l'idéal (p) de $\mathbb{Z}$ est un idéal premier détachable propre, et il en va de même pour l'idéal 0.

Théorème 2.3. [2] *Soient $P_1, \ldots, P_n$ des idéaux détachables d'un anneau commutatif R tels que P_i est premier pour $i \leqslant n-2$. Si I est un idéal de type fini de R, alors, ou bien $I \subseteq P_i$ pour un i, ou bien il existe un $z \in I \setminus \bigcup_i P_i$.*

Démonstration. Soit $\{x_1, \ldots, x_m\}$ un système générateur de I et soit F l'ensemble des sous-ensembles finis S de $\{1, 2, \ldots, n\}$ tels que $\{x_1, \ldots, x_m\} \subseteq \bigcup_{j\in S} P_j$. Nous raisonnons par récurrence [3] sur $\#F$, le nombre des éléments de F. Si $\#F = 0$, alors $x_j \in I \setminus \bigcup_i P_i$ pour un j. Sinon prenons un $S \in F$ qui minimise $\#S$. Si $\#S \leqslant 1$, alors $I \subseteq P_i$ pour un i. Sinon $\#S \geqslant 2$ et pour chaque $i \in S$, il existe $a_i \in \{x_1, \ldots, x_m\}$ tel que $a_i \in P_i \setminus \bigcup_{S\setminus\{i\}} P_j$. Si $\#S = 2$, alors posons $x_{m+1} = \sum_{i\in S} a_i \in I \setminus \bigcup_{i\in S} P_i$. Si $\#S > 2$, alors P_i est premier pour un $i \in S$, de sorte que $x_{m+1} = a_i + \prod_{j\in S\setminus\{i\}} a_j \in I \setminus \bigcup_{i\in S} P_i$. Dans chaque cas nous pouvons agrandir $\{x_1, \ldots, x_m\}$, sans agrandir I, d'où $S \notin F$, et nous terminons par récurrence sur $\#F$. □

Théorème 2.4. *Soient $I_1, \ldots, I_n$ des idéaux de type fini dans un anneau commutatif R et soit P un idéal premier de R tel que le produit $I_1 \cdots I_n$ est contenu dans P. Alors $I_i \subseteq P$ pour un i.*

Démonstration. Par récurrence sur n il suffit de considérer le cas où $n = 2$. Soient $I_1 = (a_1, \ldots, a_s)$ et $I_2 = (b_1, \ldots, b_t)$. Puisque $a_i b_j \in P$, on a pour chaque i ou bien $a_i \in P$, ou bien $b_j \in P$ pour tous les j. □

Un **corps par négation** est un anneau commutatif qui est un corps pour la non-égalité et tel que 0 est un idéal premier. Un corps discret est un corps par négation. Un **idéal maximal** dans un anneau commutatif R est un idéal M tel que R/M est un corps par négation ; ainsi, un idéal M de R est maximal si, et seulement si, d'une part M est un idéal premier, et d'autre part « $x \in R \setminus M$ » équivaut à « $\exists r \in R,\ rx - 1 \in M$ ». Un idéal maximal détachable M est un idéal tel que R/M est un corps discret.

1. **NdT.** En mathématiques classiques, les idéaux premiers sont définis comme des idéaux propres, i.e. avec $1 \notin P$. Certaines démonstrations en mathématiques constructives préfèrent ne pas utiliser cette propriété, notamment lorsque l'idéal n'est pas à priori détachable.

2. **NdT.** Cette forme constructive du lemme d'évitement des idéaux premiers sera très utile dans les chapitres VIII et X.

3. **NdT.** Plutôt qu'une démonstration par récurrence coutumière, les auteurs donnent ici une démonstration de terminaison d'un algorithme.

La **caractéristique** d'un anneau k est l'ordre de l'élément 1 dans le groupe additif de k. Une convention standard est de dire que k est de **caractéristique 0** si l'ordre de 1 est infini. Ainsi la caractéristique d'un anneau discret k est le plus petit entier strictement positif n tel que $n \cdot 1 = 0$, si un tel entier existe, et est égale à 0 sinon. Le corps des nombres rationnels est de caractéristique 0, et le corps $\mathbb{F}_p = \mathbb{Z}/(p)$ est de caractéristique p. La caractéristique d'un corps discret n'est pas nécessairement un élément de $\mathbb{N}$ comme le montre l'exemple brouwerien suivant.

Une suite binaire qui contient au plus un élément 1 est appelée une **suite binaire fugitive**.

Exemple 2.5. Soit a une suite binaire fugitive. Définissons p_n par

$$p_n = \begin{cases} 0 & \text{si } a_n = 0 \\ \text{le } n\text{-ième nombre premier} & \text{si } a_n = 1. \end{cases}$$

Soit P l'idéal de $\mathbb{Z}$ engendré par les nombres p_n, et soit $R = \mathbb{Z}/P$. Alors R est un anneau intègre discret ; soit k son corps de fractions. La caractéristique de k n'est pas un élément de $\mathbb{N}$. □

Exercices

1. Montrer les identités suivantes dans un anneau arbitraire.
   (i) $a0 = 0a = 0$,
   (ii) $a(-b) = (-a)(b) = -ab$.
2. Utiliser les anneaux $\mathbb{Z}$ et $\mathbb{Q}$ pour construire un exemple brouwerien d'un anneau intègre discret dont les unités ne sont pas détachables.
3. Montrer qu'un anneau discret est un anneau à division si, et seulement si, les éléments non nuls forment un groupe multiplicatif.
4. *Les quaternions rationnels.* On écrit les éléments (a, b, c, d) de $R = \mathbb{Q}^4$ comme des sommes formelles $a + bi + cj + dk$, où les éléments de $\mathbb{Q}$ commutent avec i, j, et k, et où on pose $i^2 = j^2 = -1$ et $k = ij = -ji$. Notez que
$$(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$$
et montrez que R est un anneau à division non commutatif discret.
5. Montrer que dans un corps avec une inégalité cotransitive les opérations d'addition, de soustraction, de multiplication et de division (restreinte aux unités) sont fortement extensionnelles (voir l'exercice 1.5).
6. Soit R un sous-anneau d'un corps K. Montrer que
$$k = \{\, ab^{-1} : a, b \in R \text{ et } b \neq 0 \,\}$$

est un corps qui contient R. Montrer que si R est un sous-anneau d'un autre corps K', et si les inégalités sur K et K' coïncident sur R, alors k est isomorphe à k'. Montrer que l'inégalité sur R est consistante, cotransitive, étroite ou discrète si, et seulement si, l'inégalité sur k possède la même propriété.

7. Montrer qu'un anneau commutatif est un anneau intègre si, et seulement si, les conditions suivantes sont satisfaites :
   (i) $1 \neq 0$,
   (ii) $a \neq b$ si, et seulement si, $a - b \neq 0$,
   (iii) si $a \neq 0$ et $ab = 0$, alors $b = 0$,
   (iv) $a \neq 0$ et $b \neq 0$ si, et seulement si, $ab \neq 0$,

   Montrer qu'une condition nécessaire et suffisante pour qu'un anneau commutatif avec la non-égalité soit un anneau intègre est que l'on a $a \neq 0$ si, et seulement si, a est **simplifiable** [1] ($ab = 0$ implique $b = 0$).
8. Montrer les propriétés suivantes pour les idéaux dans un anneau commutatif.
   (i) $IJ \subseteq I \cap J$
   (ii) $IJ \subseteq K$ si, et seulement si, $I \subseteq K : J$
   (iii) Si $I \subseteq J$ alors $K : J \subseteq K : I$
   (iv) $(\bigcap_i I_i) : J = \bigcap_i (I_i : J)$
   (v) $I : \sum_i J_i = \bigcap_i (I : J_i)$
   (vi) $I : JK = (I : J) : K$
9. Montrer les propriétés suivantes pour les idéaux dans un anneau commutatif.
   (i) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
   (ii) Si $I^n \subseteq J$ pour un n, alors $\sqrt{I} \subseteq \sqrt{J}$.
   (iii) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.
   (iv) $\sqrt{\sqrt{I}} = \sqrt{I}$.
10. Soit $\varphi\colon R \to R'$ un homomorphisme d'anneaux commutatifs, et soient I et J des idéaux de R'. Montrer que $\varphi^{-1}(I) \cap \varphi^{-1}(J) = \varphi^{-1}(I \cap J)$, que $\varphi^{-1}(I)\varphi^{-1}(J) \subseteq \varphi^{-1}(IJ)$, et que $\sqrt{\varphi^{-1}(I)} = \varphi^{-1}(\sqrt{I})$. Montrer que si φ est surjective, alors $\varphi^{-1}(I : J) = \varphi^{-1}I : \varphi^{-1}J$.
11. Montrer que $(12) \cup (45)$ n'est pas un idéal de l'anneau des entiers $\mathbb{Z}$. Montrer que $(12) + (45)$ et $(12) : (45)$ sont des idéaux principaux.

1. **NdT.** On dit aussi **régulier**.

12. Dans le théorème 2.3 il n'est pas nécessaire de savoir *lesquels* des $n-2$ idéaux sont premiers. Démontrer le théorème 2.3 sous l'hypothèse plus faible selon laquelle si $a_i b_i \in P_i$ pour $i = 1, \ldots, n$, alors pour au moins $n-2$ indices i, ou bien $a_i \in P_i$ ou bien $b_i \in P_i$.
13. Modifier le théorème 2.3 de manière qu'aucun des idéaux P_i ne soit supposé être premier, et la conclusion est alors que $I \subseteq P_i$ pour un certain i, ou alors il existe trois indices j distincts tels que P_j n'est pas premier (en un sens fort, convenable). Pouvez-vous démontrer que les trois idéaux P_j sont distincts (et pas seulement leurs indices) ?
14. Soient B et C deux sous-groupes détachables d'un groupe G. Montrer que si A est un sous-groupe de type fini de G, ou bien $A \subseteq B$, ou bien $A \subseteq C$, ou bien il existe un x dans $A \setminus (B \cup C)$. Donner un contre-exemple (non brouwerien) pour montrer que le résultat est faux pour trois sous-groupes.
15. Montrer qu'un anneau discret non trivial R est un anneau à division si, et seulement si, tout idéal de type fini est égal à R ou à 0. Donner un exemple brouwerien pour un idéal de $\mathbb{Q}$ qui n'est égal ni à $\mathbb{Q}$ ni à 0.
16. Montrer qu'un idéal d'un anneau commutatif R est un idéal premier propre si, et seulement si, c'est le noyau d'un homomorphisme de R dans un corps par négation.
17. Montrer qu'un anneau intègre fini est un corps. Montrer qu'un idéal détachable I de $\mathbb{Z}$ est maximal si, et seulement si, $I = (p)$ pour un nombre premier p.

3 Les nombres réels

Le prototype d'un corps de Heyting est le corps des nombres réels $\mathbb{R}$. L'ensemble $\mathbb{Q}^{\mathbb{N}}$ des suites de nombres rationnels forme un anneau commutatif pour l'addition et la multiplication coordonnée par coordonnée. Une suite de nombres rationnels $\{q_n\}$ est une **suite de Cauchy** si pour tout $\varepsilon \in \mathbb{Q}^{*+}$ il existe un $N \in \mathbb{N}$ tel que

$$|q_n - q_m| \leqslant \varepsilon \text{ pour tous } m, n \geqslant N.$$

On voit immédiatement que l'ensemble C des suites de Cauchy de nombres rationnels forme un sous-anneau de $\mathbb{Q}^{\mathbb{N}}$.

Une suite de nombres rationnels $\{q_n\}$ **converge vers 0** si pour tout $\varepsilon \in \mathbb{Q}^{*+}$, il existe un $N \in \mathbb{N}$ tel que $|q_n| \leqslant \varepsilon$ pour tout $n \geqslant N$. On vérifie facilement que l'ensemble I des suites de nombres rationnels qui convergent vers zéro forme un idéal de l'anneau C des suites de Cauchy. L'ensemble $\mathbb{R}$ des **nombres réels** est l'anneau quotient C/I. À chaque élément $q \in \mathbb{Q}$ nous pouvons faire correspondre la suite dont tous les éléments sont égaux à q, et nous immergeons ainsi de manière naturelle $\mathbb{Q}$ dans $\mathbb{R}$.

L'ensemble des nombres réels $\mathbb{R}$ possède un ordre naturel. On définit le fait que $a \in \mathbb{R}$ est **strictement positif** en demandant qu'il existe un $\varepsilon \in \mathbb{Q}^{*+}$ et un $N \in \mathbb{N}$ tels que $a_n \geqslant \varepsilon$ pour tout $n \geqslant N$. On vérifie facilement que cette définition respecte l'égalité de $\mathbb{R} = C/I$, et que l'ensemble des nombres réels strictement positifs est stable pour l'addition et la multiplication. Nous écrivons $a < b$, ou $b > a$, si $b - a$ est strictement positif ; en particulier, $a > 0$ signifie que a est strictement positif.

Théorème 3.1. *Les conditions suivantes pour un nombre réel a sont équivalentes.*

(i) *Il existe un $\varepsilon \in \mathbb{Q}^{*+}$ et un $N \in \mathbb{N}$ tels que $|a_n| \geqslant \varepsilon$ pour tout $n \geqslant N$.*

(ii) *$a < 0$ ou $a > 0$.*

(iii) *a est inversible.*

Démonstration. Supposons (i). Nous pouvons supposer que $|a_N - a_n| < \varepsilon/2$ pour tout $n \geqslant N$. Si $a_N \geqslant \varepsilon$, alors $a_n > \varepsilon/2$ pour tout $n \geqslant N$, donc $a > 0$. De même, si $a_N \leqslant -\varepsilon$, $a < 0$.

Supposons (ii), par exemple $a > 0$. Il existe un $\varepsilon \in \mathbb{Q}^{*+}$ et un $N \in \mathbb{N}$ tels que $a_n > \varepsilon$ pour tout $n \geqslant N$. Nous pouvons supposer que $a_n > \varepsilon$ pour *tout* $n \in \mathbb{N}$. Alors la suite $\{1/a_n\}$ est une suite de Cauchy et elle est l'inverse de a dans $\mathbb{R}$.

Finalement supposons (iii). Il existe une suite de Cauchy $\{b_n\}$ telle que $a_n b_n - 1$ converge vers 0. Considérons un $\varepsilon \in \mathbb{Q}^{*+}$ tel que $|b_n| < 1/\varepsilon$ pour tout n. Alors $|a_n|$ est plus grand que ε pour n assez grand. □

Nous définissons une inégalité sur $\mathbb{R}$ en disant que $a \neq b$ signifie que $b - a$ est inversible, de sorte que le théorème 3.1 nous dit que $a \neq b$ si, et seulement si, $a < b$ ou $b < a$. La cotransitivité de $a < b$ est le substitut constructif de la loi de trichotomie classique.

Théorème 3.2 (cotransitivité)**.** *Soient a, b et c des nombres réels. Si $a < c$, alors $a < b$ ou $b < c$.*

Démonstration. Considérons $m \in \mathbb{N}$ et $\varepsilon > 0$ tels que $a_m < c_m - 6\varepsilon$ et, pour tout $n \geqslant m$,

$$|a_n - a_m| < \varepsilon,$$
$$|c_n - c_m| < \varepsilon \text{ et}$$
$$|b_n - b_m| < \varepsilon.$$

Ou bien $b_m < c_m - 3\varepsilon$, auquel cas $b_n < c_n - \varepsilon$ pour tout $n \geqslant m$, et donc $b < c$, ou bien $b_m > a_m + 3\varepsilon$, auquel cas $b_n > a_n + \varepsilon$ pour tout $n \geqslant m$, et donc $b > a$. □

Nous écrivons $a \leqslant b$ lorsque $a < b + \varepsilon$ pour tout $\varepsilon > 0$. Cette relation est clairement transitive et réflexive. Pour démontrer que c'est une relation d'ordre, nous avons besoin du résultat suivant.

Théorème 3.3. *Si $a \leqslant b$ et $b \leqslant a$, alors $a = b$.*

Démonstration. Soit un $\varepsilon \in \mathbb{Q}^{*+}$. Comme $a \leqslant b$, nous avons un $N \in \mathbb{N}$ tel que $a_n - b_n < \varepsilon$ pour tout $n \geqslant N$. Comme $b \leqslant a$, nous avons un tel N qui vérifie en outre que $b_n - a_n < \varepsilon$ pour tout $n \geqslant N$. Cela dit que $|a_n - b_n| < \varepsilon$ pour tout $n \geqslant N$, et nous avons donc montré que $a_n - b_n$ converge vers 0, ce qui signifie que $a = b$. □

Corolaire 3.4. $\mathbb{R}$ *est un corps de Heyting.*

Démonstration. Si $a + b \neq 0$, ou bien $a + b > 0$, ou bien $a + b < 0$, et nous pouvons supposer que $a + b > 0$. Alors ou bien $a > 0$, ou bien $a < a + b$, en vertu du théorème 3.2 ; dans le premier cas on a $a \neq 0$, dans le second on a $0 < b$ et donc $b \neq 0$. Ainsi l'inégalité sur $\mathbb{R}$ est cotransitive.

Pour montrer que l'inégalité est étroite, supposons que $a \neq 0$ soit impossible. Pour chaque $\varepsilon > 0$, ou bien $a > 0$, ou bien $a < \varepsilon$ en vertu du théorème 3.2 ; le premier cas est impossible, donc $a < \varepsilon$. Par suite $a \leqslant 0$. De manière analogue $a \geqslant 0$, de sorte que $a = 0$ par le théorème 3.3. □

L'ensemble $\mathbb{R}$ n'est pas seulement un ensemble ordonné, c'est un treillis. Si a et b sont des nombres réels, alors la suite $c_n = \max(a_n, b_n)$ définit un nombre réel c qui est le supremum de a et b, ce que l'on écrit $c = \sup(a, b)$. L'infimum de a et b est $\inf(a, b) = -\sup(-a, -b)$. On peut définir la valeur absolue du nombre réel a comme $|a| = \sup(a, -a)$.

Le corps $\mathbb{C}$ des **nombres complexes** est obtenu à partir de l'espace vectoriel $\mathbb{R}^2$ en définissant la multiplication $(a, b)(c, d) = (ac - bd,\ ad + bd)$. On vérifie facilement que $\mathbb{C}$ est un corps de Heyting avec le neutre multiplicatif $(1, 0)$. Nous posons $i = (0, 1)$ et nous voyons que $i^2 = -1$ et que $\mathbb{C} = \mathbb{R} + \mathbb{R}i$.

Un **espace métrique** est un ensemble S donné avec une fonction d, appelée la **métrique**, ou encore la **distance**, de $S \times S$ vers $\mathbb{R}$ telle que

(i) $d(x, y) = d(y, x) \geqslant 0$,

(ii) $d(x, y) = 0$ si, et seulement si, $x = y$,

(iii) $d(x, z) \leqslant d(x, y) + d(y, z)$.

Les nombres réels forment un espace métrique pour la distance $d(x, y) = |x - y|$. Une **suite de Cauchy** dans un espace métrique S est une suite $\{x_n\}$ dans S telle que pour tout $\varepsilon \in \mathbb{Q}^{*+}$ il existe un $N \in \mathbb{N}$ tel que

$$d(x_n, x_m) \leqslant \varepsilon \text{ pour tous } m, n \geqslant N.$$

Une suite $\{x_n\}$ dans S **converge** vers $y \in S$ si pour tout $\varepsilon \in \mathbb{Q}^{*+}$ il existe un $N \in \mathbb{N}$ tel que $d(x_n, y) \leqslant \varepsilon$ pour tout $n \geqslant N$. Si $\{x_n\}$ converge vers y, nous disons que y est la **limite** de la suite $\{x_n\}$. On vérifie facilement que toute suite convergente est une suite de Cauchy. Si, inversement, toute suite de Cauchy converge vers un élément de S, nous disons que l'espace métrique S est **complet**. L'espace $\mathbb{R}$ est complet.

En imitant la construction de $\mathbb{R}$ à partir de $\mathbb{Q}$, nous pouvons immerger n'importe quel espace métrique S dans sa **complétion** $\hat{S}$, dont les éléments sont les suites de Cauchy dans S, avec $d(a, b)$ égal à la limite de $d(a_n, b_n)$, et en définissant $a = b$ par $d(a, b) = 0$. L'espace S est **dense** dans $\hat{S}$, i.e. pour tout ε strictement positif et tout $s \in \hat{S}$, on a un $a \in S$ tel que $d(a, s) < \varepsilon$. L'espace $\hat{S}$ est complet.

Exercices

1. Montrer que $a > b$ est impossible si, et seulement si, $a \leqslant b$.
2. Montrer que les propriétés suivantes sont équivalentes.
   (i) Pour tout $a \in \mathbb{R}$, ou bien $a > 0$ ou bien $a \leqslant 0$.
   (ii) LPO.
3. Montrer que $\mathbb{R}$ est un treillis distributif pour la relation d'ordre $\leqslant$.
4. Montrer que $|a| \geqslant 0$, et que $|a|$ est > 0 si, et seulement si, $a \neq 0$. Montrer que $|a + b| \leqslant |a| + |b|$.
5. Montrer que les propriétés suivantes sont équivalentes.
   (i) LLPO.
   (ii) Pour tout $a \in \mathbb{R}$, ou bien $a \leqslant 0$ ou bien $a \geqslant 0$.
   (iii) Pour tous $a, b \in \mathbb{R}$, si $ab = 0$, alors $a = 0$ ou $b = 0$.
   (iv) Si $a, b \in \mathbb{R}$, alors on a un $c \in \mathbb{R}$ tel que $a = cb$ ou $b = ca$.
   (v) Pour tous $a, b \in \mathbb{R}$, si $\sup(a, b) = 1$, alors $a = 1$ ou $b = 1$.
6. Montrer que le principe de Markov équivaut à ce que $\mathbb{R}$ soit un corps par négation.
7. *Le corps des nombres p-adiques.* Si p est un nombre premier, la **métrique p-adique sur** $\mathbb{Q}$ est définie pour $x_1 \neq x_2$ en posant $d(x_1, x_2) = p^n$ lorsque $p^n(x_1 - x_2)$ peut être écrit avec un numérateur et un dénominateur non divisibles par p. Montrer que d est une métrique, et que la complétion de $\mathbb{Q}$ pour cette métrique est un corps de Heyting.
8. Montrer que tout espace métrique est dense dans sa complétion, et que sa complétion est un espace métrique complet.

4 Modules

Si R est un anneau, un **R-module à gauche** est un groupe abélien additif M donné avec une fonction μ de $R \times M$ vers M, écrite $\mu(r,a) = ra$, appelée **multiplication scalaire**, telle que

(i) $r(a+b) = ra + rb$

(ii) $(r+s)a = ra + sa$

(iii) $(rs)a = r(sa)$

(iv) $1 \cdot a = a$

pour tous r, $s \in R$ et a, $b \in M$. Les **R-modules à droite** sont définis de la même manière, à ceci près que la multiplication scalaire est à droite : la seule réelle différence se trouve dans (iii) que l'on doit lire $a(rs) = (ar)s$, de sorte que pour les modules à droite, multiplier par rs est la même chose que d'abord multiplier par r et ensuite multiplier par s, tandis que pour les modules à gauche, multiplier par rs est la même chose que multiplier d'abord par s puis par r.

Tout groupe abélien est un $\mathbb{Z}$-module. L'ensemble R^n des n-uplets d'éléments de R est un R-module pour l'addition et la multiplication scalaire coordonnée par coordonnée. Si R est un anneau à division, un R-module est appelé un **espace vectoriel** sur R.

Soient M et N des R-modules à gauche. Un homomorphisme de groupes f de M vers N est un **homomorphisme de R-modules**, ou **une application R-linéaire**, si $f(ra) = rf(a)$ pour tous $r \in R$ et $a \in M$. Le **noyau** de f est $\ker f = \{\, a \in M : f(a) = 0 \,\}$, et l'**image** de f est $\operatorname{im} f = \{\, f(a) : a \in M \,\}$. On vérifie facilement que la catégorie des R-modules est une catégorie pré-additive.

L'ensemble $\mathrm{E}(M)$ des endomorphismes d'un groupe abélien M forme un anneau, où la multiplication est la composition des fonctions. Si R est un anneau et f est un homomorphisme d'anneaux de R vers $\mathrm{E}(M)$, alors M peut être muni d'une structure de R-module en posant $rm = f(r)m$ pour $r \in R$ et $m \in M$. Inversement, si M est un R-module, alors on peut définir un homomorphisme d'anneaux φ de R vers $\mathrm{E}(M)$ en posant $\varphi(r)(m) = rm$. L'homomorphisme φ est appelé une **représentation** de R comme anneau d'endomorphismes de M. Les représentations et les modules sont deux manières de regarder la même chose. Si le noyau de la représentation est nul, la représentation est dite **fidèle**. Un R-module M est **fidèle** si $r = 0$ chaque fois que $rm = 0$ pour tout $m \in M$.

Un sous-groupe N d'un R-module M est un **R-sous-module** si $ra \in N$ pour tous $a \in N$ et $r \in R$. Le sous-module de M engendré par un sous-ensemble X est le sous-groupe additif engendré par l'ensemble $\{\, rx : r \in R \text{ et } x \in X \,\}$. Le groupe quotient M/N est un R-module parce que la multiplication scalaire opère sur lui. Les théorèmes 1.1 et 1.2 s'appliquent pour les R-modules si nous remplaçons partout « groupe » par « module », et si nous considérons que tous les sous-modules sont normaux (ce qu'ils sont en tant que sous-groupes).

Si R et S sont des sous-anneaux d'un anneau A, alors A est, entre autres choses, un R-module à gauche et un S-module à droite. Ce genre de situation se produit suffisamment souvent pour mériter un nom. Soient R et S des anneaux et soit M un R-module à gauche qui est aussi un S-module à droite. Alors on dit que M est un **R-S-bimodule** si $(ra)s = r(as)$ pour tous $r \in R$, $a \in M$ et $s \in S$. Ainsi l'anneau R est un R-R-bimodule, et tout R-module est un R-$\mathbb{Z}$-bimodule. Si R est un anneau commutatif, il n'y a aucune différence entre R-modules à droite et à gauche, et chacun est un R-R-bimodule.

Les idéaux de R peuvent être décrits en termes des structures de modules sur R : un idéal à gauche est un sous-module du module à gauche R, un idéal à droite est un sous-module du module à droite R, et un idéal bilatère est un sous-module du R-R-bimodule R.

Soient M un R-module et $\{A_i\}_{i\in I}$ une famille de sous-modules de M. Le sous-module de M engendré par $\bigcup_{i\in I} A_i$ est noté $\sum_{i\in I} A_i$. Les A_i sont dits **indépendants** si lorsque $i_1, \ldots, i_n, j \in I$ et $x \in A_j \cap (A_{i_1} + \cdots + A_{i_n})$, alors ou bien $x = 0$ ou bien $i_m = j$ pour un m. Nous disons que M est la **somme directe** (**interne**) des sous-modules A_i, et nous écrivons $M = \bigoplus_{i\in I} A_i$, si $M = \sum_{i\in I} A_i$ avec les A_i indépendants. Si $I = \{1, \ldots, n\}$, nous écrivons $M = A_1 \oplus \cdots \oplus A_n$. Lorsque $I = \{1, 2\}$, on a $M = A_1 \oplus A_2$ si, et seulement si, $M = A_1 + A_2$ et $A_1 \cap A_2 = 0$. Par exemple, $M = \mathbb{Z}/(6)$, $A_1 = \{0, 2, 4\}$, et $A_2 = \{0, 3\}$.

Le produit d'une famille de R-modules $\{A_i\}_{i\in I}$ possède une structure naturelle de R-module pour laquelle il est le produit catégorique, ou **produit direct**, des modules A_i. Si f et g sont des fonctions dans ce produit, on définit $f + g$ par $(f + g)(i) = f(i) + g(i)$, et rf par $(rf)(i) = rf(i)$. Le produit direct est noté $\prod_{i\in I} A_i$.

Soient I un ensemble discret et $\{A_i\}_{i\in I}$ une famille de R-modules. Nous pouvons construire le coproduit catégorique (somme directe externe) de la manière suivante. Un élément $f \in \prod_{i\in I} A_i$ a un **support fini** s'il existe un sous-ensemble fini J de I tel que $f(i) = 0$ pour $i \in I \setminus J$. Pour un ensemble discret I, la somme directe externe de la famille $\{A_i\}_{i\in I}$ est l'ensemble des éléments du produit direct qui ont un support fini. On voit facilement que si f et g ont des supports finis, alors il en va de même pour $f + g$ et rf, de sorte que la somme directe externe est un sous-module du produit direct. Notez que si I est fini, alors le produit direct et la somme directe externe sont le même module. Si nous identifions le module A_i avec le sous-module $\{ f : f(j) = 0 \text{ pour } j \neq i \}$, nous voyons que la somme directe externe est une somme directe.

La construction précédente pose un problème si l'ensemble d'indices I n'est pas discret, parce que si A_i est discret et si $\{ f : f(j) = 0 \text{ pour } j \neq i \}$ contient un élément non nul, alors $\{i\}$ est une partie détachable de I. Pour construire une **somme directe externe** lorsque l'ensemble d'indices I n'est pas nécessairement discret, on considère l'ensemble F des suites finies d'éléments de la réunion disjointe des A_i. Soit alors l'égalité sur F engendrée par

(i) $(a_1, \ldots, a_n) = (a_{\sigma(1)}, \ldots, a_{\sigma(n)})$ si σ est une permutation de $\{1, \ldots, n\}$.

(ii) $(a_1, \ldots, a_{n-1}, a_n) = (a_1, \ldots, a_{n-1})$ si $a_n = 0$.

(iii) $(a_1, \ldots, a_{n-1}, a_n) = (a_1, \ldots, a_{n-1} + a_n)$ si a_{n-1} et a_n sont des éléments d'un même A_i.

Plus précisément, disons que deux suites de F sont **adjacentes** lorsqu'une permutation de l'une est obtenue en appliquant (ii) ou (iii) à une permutation de l'autre. Alors σ et τ sont **égales** dans F si l'on a une chaine de suites de F

$$\sigma = s_1, s_2, \ldots, s_m = \tau$$

telle que s_i est adjacente à s_{i+1} pour $i = 1, \ldots, m-1$.

Nous désirons identifier $\{\, (a) \in F : a \in A_i \,\}$ avec A_i. Pour ce faire nous devons montrer que si $(a) = (b)$, alors $a = b$. Cela est une conséquence de la propriété de Church-Rosser pour F.

Lemme 4.1 (propriété de Church-Rosser)**.** *Supposons que les suites σ et τ sont égales dans F, et notons $\ell(s)$ la longueur de la suite s. Alors il existe une chaine $\sigma = s_1, s_2, \ldots, s_m = \tau$ de suites de F telle que s_i est adjacente à s_{i+1} pour $i = 1, \ldots, m-1$, et pour $i = 2, \ldots, m-1$, si $\ell(s_{i-1}) < \ell(s_i)$, alors $\ell(s_i) < \ell(s_{i+1})$.*

Démonstration. Soit $\sigma = s_1, s_2, \ldots, s_m = \tau$ une chaine de suites de F telle que s_i est adjacente à s_{i+1} pour $i = 1, \ldots, m-1$. Nous procédons par récurrence sur $N = \sum_i \ell(s_i)$, en montrant que si $\ell(s_{i-1}) < \ell(s_i)$ et $\ell(s_i) > \ell(s_{i+1})$ pour un i, alors nous pouvons diminuer N.

Supposons que nous allions de s_i à s_{i+1} en supprimant un zéro z. Si z apparait dans s_{i-1}, nous pouvons remplacer s_i par s_{i-1} dans laquelle nous supprimons z. Sinon s_{i-1} provient de s_i en supprimant z, auquel cas nous pouvons omettre s_i. Le même argument s'applique si nous allons de s_i à s_{i-1} en supprimant un zéro.

Supposons que nous allions de s_i à s_{i+1}, et de s_i à s_{i-1}, en appliquant (iii). Dépendant du nombre de positions distinctes de s_i qui sont concernées, nous pouvons décrire les différents cas comme suit

s_{i-1}	s_i	s_{i+1}
$(a+b)$	(a,b)	$(a+b)$
$(a+b,c)$	(a,b,c)	$(a,b+c)$
$(a+b,c,d)$	(a,b,c,d)	$(a,b,c+d)$

Dans le premier cas nous pouvons omettre s_i et s_{i+1}. Dans le second cas, nous pouvons remplacer s_i par $(a+b+c)$, et dans le troisième nous pouvons remplacer s_i par $(a+b, c+d)$. □

Deux suites de F sont additionnées en les concaténant, la multiplication scalaire est faite coordonnée par coordonnée, et la suite vide sert d'élément neutre.

Vu la relation d'égalité nous pouvons de manière sûre et sans ambigüité écrire un élément $(a_1, a_2, \ldots, a_n)$ de F comme une somme formelle $a_1 + a_2 + \cdots + a_n$.

En identifiant le module A_i avec $\{(a) : a \in A_i\}$, nous voyons que F est somme directe interne des A_i ; la vérification de cette affirmation téméraire est laissée en exercice 5.

Si I est discret et si $(a_1, \ldots, a_n) \in F$, nous pouvons supposer que $a_m \in A_{i_m}$ avec $i_m \neq i_{m'}$ si $m \neq m'$, et nous pouvons identifier F avec l'ensemble des éléments de $\prod_{i\in I} A_i$ qui ont un support fini, comme précédemment.

Si chaque A_i est un même module M et si I est un ensemble d'indices arbitraire, nous notons la somme directe externe par $M^{(I)}$.

Le théorème suivant dit qu'une somme directe interne (et donc aussi la somme directe externe que nous avons identifiée à une somme directe interne) est un coproduit catégorique.

Théorème 4.2. *Si $M = \bigoplus_{i\in I} A_i$ et si $f_i \colon A_i \to N$ est une famille d'applications R-linéaires, alors il y a une unique application R-linéaire f de M vers N telle que $f = f_i$ sur A_i pour tout $i \in I$.*

Démonstration. Si $x \in M = \sum_{i\in I} A_i$, alors $x = \sum_{m=1}^{n} a_{i_m}$, avec $a_{i_m} \in A_{i_m}$. Par suite $f(x)$ doit être égal à $\sum_{m=1}^{n} f_{i_m}(a_{i_m})$, et donc f est unique. Si nous définissons $f(x)$ comme égal à $\sum_{m=1}^{n} f_{i_m}(a_{i_m})$, nous devons montrer que $f(x)$ est bien défini ; il suffit de montrer que si $x = 0$, alors $f(x) = 0$. Supposons que $x = \sum_{m=1}^{n} a_{i_m} = 0$. Comme les A_i sont indépendants, ou bien $a_{i_m} = 0$ pour chaque m, ou bien il y a un $m \neq m'$ tel que $i_m = i_{m'}$. Dans le dernier cas, nous pouvons additionner a_{i_m} et $a_{i_{m'}}$ dans A_{i_m}, et par suite $f(x) = 0$ pas récurrence sur n. On vérifie facilement que f est une application R-linéaire. □

Un R-module F est **libre** sur une famille d'éléments $\{x_i\}_{i\in I}$ de F si pour chaque fonction f qui envoie I dans le R-module M, il y a une unique application R-linéaire f^* de F vers M telle que $f^*(x_i) = f(i)$. Nous disons que $\{x_i\}_{i\in I}$ est une **base** pour F. L'unicité de f^* implique que des modules libres sur $\{x_i\}_{i\in I}$ et sur $\{y_i\}_{i\in I}$ sont isomorphes pour un isomorphisme qui envoie x_i sur y_i, de sorte que des modules libres dont les bases ont le même ensemble d'indices sont essentiellement les mêmes. Si $F = \bigoplus_{i\in I} Rx_i$ et si la fonction de R vers Rx_i qui envoie r sur rx_i est un isomorphisme pour chaque $i \in I$, le théorème 4.2 montre que F est libre sur $\{x_i\}_{i\in I}$. Si R est un anneau non trivial, alors $x_i \neq 0$ pour chaque $i \in I$, de sorte que si $x_i = x_j$, alors $i = j$; ainsi les éléments x_i de la base sont en correspondance bijective avec les éléments i de I. Ainsi lorsque nous nous restreignons aux anneaux non triviaux, nous pourrons définir une base comme un *ensemble* plutôt que comme une famille. Si R est un anneau trivial, alors toute famille d'éléments de n'importe quel R-module M est une base pour M.

Soit I un ensemble discret, et pour chaque $i \in I$ soit $\delta_i \in R^{(I)}$ tel que $\delta_i(i) = 1$ et $\delta_i(j) = 0$ pour $j \neq i$. Alors $R^{(I)}$ est libre sur $\{\delta_i\}_{i\in I}$. Pareillement, supposons

que I est un ensemble d'indices arbitraire, et que $\{R_i\}_{i\in I}$ est une famille telle que chaque R_i est une copie de R. Si pour chaque $i \in I$ nous définissons x_i comme la suite de longueur 1 dont l'élément est le neutre multiplicatif de R_i, alors $R^{(I)}$ est libre sur $\{x_i\}_{i\in I}$. Par abus de langage nous dirons que $R^{(I)}$ est **le module libre sur** I.

Si $I = \{1, \ldots, n\}$, alors nous écrivons R^n au lieu de $R^{(I)}$. Un module M possède une base de n éléments si, et seulement si, il est isomorphe à R^n, auquel cas nous disons que M est un **module libre de rang** n. Dans la section 6 nous verrons que pour un anneau commutatif non trivial R, le rang de M est un invariant. L'exercice 3 donne un exemple d'un anneau non commutatif non trivial R tel que les R-modules à gauche R et R^2 sont isomorphes.

Un R-module M est **de type fini** s'il existe une application R-linéaire surjective de R^n sur M pour un n strictement positif ; c'est-à-dire s'il existe des éléments $x_1, \ldots, x_n$ de M tels que tout élément de M peut s'écrire sous la forme $\sum_{i=1}^n r_i x_i$. Un R-module M est **cyclique** s'il existe une application R-linéaire surjective de R sur M ; c'est-à-dire s'il existe un $x \in M$ tel que tout élément de M est un multiple scalaire de x.

Théorème 4.3. *Soit R un sous-anneau d'un anneau E. Si M est un E-module de type fini (libre de rang n) et si E est un R-module de type fini (libre de rang m), alors M est un R-module de type fini (libre de rang mn).*

Démonstration. Soient $\varphi\colon R^m \to E$ un épimorphisme (isomorphisme) de R-modules et $\psi\colon E^n \to M$ un épimorphisme (isomorphisme) de E-modules. Alors $\varphi^n\colon R^{mn} \to E^n$ est un épimorphisme (isomorphisme) de R-modules, et $\psi\varphi^n\colon R^{mn} \to M$ est un épimorphisme (isomorphisme) de R-modules. □

Un R-module P est dit **projectif** si pour toute application R-linéaire g d'un R-module A sur un R-module B, et toute application R-linéaire f de P vers B, il existe une application R-linéaire $h\colon P \to A$ telle que $gh = f$. Les modules libres de rang fini sont projectifs : si $x_1, \ldots, x_n$ est une base de P, alors il existe $a_1, \ldots, a_n \in A$ tels que $g(a_i) = f(x_i)$ pour chaque i, et on a une application R-linéaire h telle que $h(x_i) = a_i$ pour chaque i ; les applications R-linéaires gh et f sont égales parce qu'elles coïncident sur la base.

Soit M un R-module de type fini. Si π est un épimorphisme d'un R-module libre de rang fini F sur M, de noyau K, alors M est isomorphe à F/K. Le théorème suivant montre ce qu'il advient lorsque nous obtenons la même chose pour d'autres couples (F, π) ; le résultat ressemble à la règle pour déterminer quand deux fractions sont égales.

Théorème 4.4 (l'astuce de Schanuel)**.** *Soient M un R-module, P_1 et P_2 des R-modules projectifs, et π_i une application R-linéaire de P_i sur M ($i = 1, 2$). Si K_i est le noyau de π_i, alors $K_1 \oplus P_2$ est isomorphe à $K_2 \oplus P_1$.*

Démonstration. Comme les modules P_i sont projectifs, nous avons des applications R-linéaires $\varphi_1 \colon P_2 \to P_1$ et $\varphi_2 \colon P_1 \to P_2$ qui vérifient $\pi_1\varphi_1 = \pi_2$ et $\pi_2\varphi_2 = \pi_1$. Considérons l'application R-linéaire de $K_1 \oplus P_2$ vers $K_2 \oplus P_1$ qui envoie (k_1, p_2) sur (k_2, p_1) où

$$k_2 = p_2 - \varphi_2(k_1 + \varphi_1 p_2), \quad p_1 = k_1 + \varphi_1 p_2$$

et l'application R-linéaire de $K_2 \oplus P_1$ vers $K_1 \oplus P_2$ qui envoie (k_2, p_1) sur (k_1, p_2) où

$$k_1 = p_1 - \varphi_1(k_2 + \varphi_2 p_1), \quad p_2 = k_1 + \varphi_2 p_1$$

On vérifie facilement que ces applications R-linéaires sont inverses l'un de l'autre. □

Un élément e d'un anneau est **idempotent** si $e^2 = e$. Un sous-module A de M est un **facteur direct** de M s'il existe un sous-module B de M, appelé un **supplémentaire** de A dans M, tel que $M = A \oplus B$. Les sous-modules 0 et M de M sont toujours facteurs directs supplémentaires l'un de l'autre.

Théorème 4.5. *Soit A un sous-module d'un R-module M. Alors A est un facteur direct de M si, et seulement si, il y a un endomorphisme idempotent e de M tel que $A = eM$. Dans ce cas le sous-module $(1-e)M$ et un supplémentaire de A.*

Démonstration. Supposons que $M = A \oplus B$. Si $x \in M$, nous pouvons écrire x de manière unique sous la forme $a + b$ pour un $a \in A$ et un $b \in B$. On définit un endomorphisme e de M en posant $e(x) = a$. On voit facilement que e est idempotent et que $eM = A$.

Inversement, supposons que e est un endomorphisme idempotent de M et que $A = eM$. Posons $B = (1-e)M$. Comme $x = ex + (1-e)x$, nous avons $A + B = M$. Si $x \in A \cap B$, alors $x = (1-e)y$ et $x = ez$. Donc $ex = e(1-e)y = (e - e^2)y = 0$ et $ex = e^2 z = ez = x$, de sorte que $x = 0$. Ainsi $A \cap B = 0$. □

L'idempotent e dans le théorème 4.5 est appelé la **projection** de M sur A (parallèlement à B).

Exercices

1. L'**anneau opposé** R^{op} d'un anneau R est formé avec le groupe additif R et la multiplication $ab \in R^{op}$ définie comme le produit ba de R. Montrer que tout R-module à gauche est un R^{op}-module à droite de manière naturelle. Si R est un anneau commutatif, l'anneau opposé est isomorphe à R, donc tout R-module à gauche est aussi un R-module à droite, et il n'est pas nécessaire de distinguer entre R-modules à gauche et à droite.

2. Soit R un anneau et soit M un R-module. Montrer qu'il existe un homomorphisme surjectif d'un R-module libre sur M.

3. Soient A et B des espaces vectoriels sur un corps discret k, chacun avec une base dénombrable infinie. Soit $V = A \oplus B$ et soit R l'anneau des endomorphismes de V. Construire un $x \in R$ tel que $xA = 0$ et $x\colon B \to V$ est un isomorphisme, et un $y \in R$ tel que $yB = 0$ et $y\colon A \to V$ est un isomorphisme. Montrer que $Rx \simeq Ry \simeq R$ comme R-modules, et que $R = Rx \oplus Ry$. Que nous dit cet exercice ?

4. Soient M un R-module et $\{A_i\}_{i\in I}$ une famille de R-modules. Soit $\{f_i\}_{i\in I}$ une famille d'homomorphismes de R-modules telle que f_i envoie M dans A_i. Soit π_i la projection de $\prod_{i\in I} A_i$ vers A_i. Montrer qu'il existe une unique application R-linéaire f de M vers $\prod_{i\in I} A_i$ telle que $\pi_i f = f_i$ pour chaque $i \in I$.

5. Soit F la somme directe externe de la famille $\{A_i\}_{i\in I}$, pour un ensemble d'indices arbitraire I. Montrer que l'homomorphisme de A_i vers F défini en envoyant $a \in A_i$ sur la suite (a) définie avant le lemme 4.1 est un monomorphisme. Montrer que si nous identifions A_i avec son image par ce monomorphisme, alors $F = \bigoplus_{i\in I} A_i$.

6. *Un facteur n'est pas nécessairement facteur direct.* Soit a une suite binaire fugitive, et soit $S = \{0, s, 2s, t, 2t\}$ avec
   — $s = t$ et $2s = 2t$ si $a_n = 1$ pour un entier pair n,
   — $s = 2t$ et $2s = t$ si $a_n = 1$ pour un entier impair n.
   Soit $I = \{x, y\}$ avec $x = y$ si $a_n = 1$ pour un n. Enfin soient $A_x = \{0, s, 2s\}$ et $A_y = \{0, t, 2t\}$ avec leurs structures évidentes de groupes à trois éléments. Montrer que l'on obtient ainsi un exemple brouwerien (LLPO) avec A_x qui n'est pas facteur direct dans $\bigoplus_{i\in I} A_i$.

7. Soient $\{A_i\}_{i\in I}$ une famille de modules et $f_i\colon A_i \to A$ une famille d'isomorphismes. Montrer que le noyau de l'homomorphisme $f\colon \bigoplus_{i\in I} A_i \to A$ induit par les isomorphismes f_i est un supplémentaire de chaque sous-module A_i.

8. Montrer que $A \oplus B$ est projectif si, et seulement si, A et B sont projectifs. Construire un module projectif à deux éléments sur l'anneau $\mathbb{Z}/(6)$.

9. Montrer qu'un module libre sur un ensemble projectif (voir l'exercice I.3.4) est projectif. Quel est le module libre sur un ensemble vide ?

10. *Les modules libres ne sont pas nécessairement projectifs.* Construire un exemple brouwerien pour une application R-linéaire α depuis un module F_1 libre de rang 2 sur un module libre F_2 tel qu'il n'y a pas d'application R-linéaire φ de F_2 vers F_1 avec $\alpha\varphi$ égal à l'application identique sur F_1. Suggestion : soient F_2 et F_1 des k-modules libres sur les ensembles A et B de l'exemple 3.1, où k est l'anneau des entiers modulo 2.

11. Montrer que si les modules libres sur des bases discrètes sont projectifs, alors l'axiome du choix le plus simple du monde est valide.
12. Soient I un ensemble discret et φ un homomorphisme non trivial de $\mathbb{Z}$-modules, de $\mathbb{Z}^{(I)}$ vers $\mathbb{Z}$. Montrer que $\ker\varphi$ est un facteur direct de $\mathbb{Z}^{(I)}$ si, et seulement si, $\operatorname{im}\varphi$ est cyclique. Construire un exemple brouwerien d'un homomorphisme φ (pas nécessairement non trivial) tel que $\ker\varphi$ est facteur direct mais $\operatorname{im}\varphi$ n'est pas cyclique.

5 Anneaux de polynômes

Si M est un monoïde et R un anneau, notons $R^{(M)}$ le R-module libre sur l'ensemble M. Nous pouvons voir les éléments de $R^{(M)}$ comme des sommes formelles finies $r_1m_1 + \cdots + r_nm_n$ avec les $m_i \in M$ et les $r_i \in R$. Définissons le produit de deux éléments de $R^{(M)}$ par

$$\Big(\sum\nolimits_{i=1}^{n} r_i m_i\Big)\Big(\sum\nolimits_{j=1}^{n'} r'_j m'_j\Big) = \sum\nolimits_{i=1}^{n}\sum\nolimits_{j=1}^{n'}(r_ir'_j)(m_im'_j).$$

Le produit $m_im'_j$ est le produit dans le monoïde M, tandis que $r_ir'_j$ est le produit dans l'anneau R. Cela fait de $R^{(M)}$ un anneau, que l'on appelle **la R-algèbre du monoïde** M [1], avec pour élément neutre multiplicatif $1 = 1_R1_M$. Si M est un groupe, alors $R^{(M)}$ est **la R-algèbre du groupe** M [2]. La fonction qui envoie r sur $r1$ est un isomorphisme de R sur un sous-anneau de $R^{(M)}$, et nous pouvons voir R comme un sous-ensemble de $R^{(M)}$ défini par cette immersion, autrement dit, l'élément $r1$ sera noté r et 1 sera identifié à 1_R.

Soit M le monoïde libre sur l'ensemble à un élément $\{X\}$. Alors

$$R^{(M)} = \{\, r_0 + r_1X + \cdots + r_nX^n : r_i \in R \text{ et } n \in \omega \,\}.$$

L'élément X est appelé une **indéterminée** et les éléments de $R^{(M)}$ sont appelés des **polynômes**. L'algèbre $R^{(M)}$ est notée $R[X]$ et on l'appelle l'**anneau de polynômes** [3] en (l'indéterminée) X (sur R).

L'anneau des polynômes en n indéterminées, $R[X_1, \ldots, X_n]$ est défini de manière inductive comme $R[X_1, \ldots, X_{n-1}][X_n]$. Un élément de $R[X_1, \ldots, X_n]$ écrit sous la forme $X_1^{e_1} \cdots X_n^{e_n}$ est appelé un **monôme** de **degré** $\sum_{i=1}^{n} e_i$. Si l'anneau R est discret, alors le **degré (total)** d'un polynôme non nul $f \in R[X_1, \ldots, X_n]$ est le maximum des degrés des monômes qui apparaissent dans f avec un coefficient non nul. L'anneau $R[X_1, \ldots, X_n]$ est le R-module libre sur l'ensemble des monômes ; en fait, les monômes forment un monoïde commutatif, et $R[X_1, \ldots, X_n]$ est la R-algèbre de ce monoïde.

1. **NdT.** Monoid ring.
2. **NdT.** Group ring.
3. **NdT.** Polynomial ring.

Si R est un sous-anneau d'un anneau commutatif S, un polynôme $f \in R[X_1, \dots, X_n]$ définit une fonction de S^n vers S : si $a_1, \dots, a_n$ sont des éléments de S, nous définissons $f(a_1, \dots, a_n)$ comme le résultat de la substitution des a_i aux X_i dans l'expression formelle de f, et en interprétant les opérations formelles dans $R[X_1, \dots, X_n]$ comme des opérations dans S. Nous demandons la commutativité parce que les indéterminées commutent les unes avec les autres ainsi qu'avec les éléments de R. Comme les a_i commutent entre eux, ainsi qu'avec les éléments de R, la fonction qui envoie f sur $f(a_1, \dots, a_n)$ est un homomorphisme d'anneaux.

Pour $n \in \mathbb{N}$, un polynôme $f \in R[X]$ qui peut être écrit sous la forme $\sum_{i=0}^{n-1} r_i X^i$ est dit être de **degré au plus** $n-1$, ce que l'on écrit $\deg f \leqslant n-1$, ou $\deg f < n$. Un polynôme est nul si, et seulement si, il a un degré au plus -1. Si $\deg f \leqslant d$ et si $r_d = 1$, nous disons que f est **unitaire**. Notez que ces définitions ne font pas référence à une inégalité sur R. Si $r_i \neq 0$ pour un $i \geqslant d$, nous disons que f est de **degré au moins** d, ce que l'on écrit $\deg f \geqslant d$. Si $\deg f \leqslant d$ et $\deg f \geqslant d$, nous disons que f est de **degré** d, et l'on écrit $\deg f = d$; dans ce cas nous disons que r_d est le **coefficient dominant** de f. Si R n'est pas discret, alors f n'a pas nécessairement un degré, même s'il a un coefficient non nul.

Si f et g sont des polynômes, nous écrivons $\deg f \leqslant \deg g$ si $\deg g < n$ implique $\deg f < n$ pour tout $n \in \mathbb{N}$; et nous écrivons $\deg f < \deg g$ si $\deg g < n+1$ implique $\deg f < n$ pour tout $n \in \mathbb{N}$. Notez que si $g = X^n + r_{n-1}X^{n-1} + \cdots + r_0$, alors $\deg f \leqslant \deg g$ si, et seulement si, $\deg f \leqslant n$, y compris si l'anneau est trivial.

Théorème 5.1. *Soient k un corps et $f, g \in k[X]$. Si $\deg f = m$ et $\deg g = n$, alors $\deg fg = m+n$.*

Démonstration. Soient a le coefficient dominant de f et b le coefficient dominant de g. Alors ab est le coefficient dominant de fg, et $\deg fg = \deg f + \deg g$. □

Théorème 5.2 (algorithme de division)**.** *Soit R un anneau commutatif et soient $f, g \in R[X]$ des polynômes tels que $\deg f \leqslant m$ et $\deg g \leqslant n \leqslant m+1$. Soit a le coefficient de X^n dans g. Il existe des polynômes $q, r \in R[X]$ tels que $a^{m-n+1} f = qg + r$ et $\deg r \leqslant n-1$.*

Démonstration. Nous procédons par récurrence sur $m-n$. Si $m-n = -1$, on prend $q = 0$ et $r = f$. Si $m-n \geqslant 0$ et $f = b_0 + b_1 X + \cdots + b_m X^m$, posons $f_1 = af - b_m X^{m-n} g$. Alors $\deg f_1 \leqslant m-1$, donc par récurrence $a^{m-n} f_1 = q_1 g + r$ pour un couple (q_1, r) de $R[X]$ avec $\deg r \leqslant n-1$. Ainsi $a^{m-n+1} f = (q_1 + a^{m-n} b_m X^{m-n})g + r$. □

Si le diviseur g est unitaire, ce que l'on peut supposer lorsque R est un corps discret, l'algorithme de division a une forme beaucoup plus agréable.

Corolaire 5.3. *Soient $f, g \in R[X]$ des polynômes sur un anneau commutatif R avec g unitaire. Alors il y a un unique couple (q, r) de $R[X]$ tel que $f = qg + r$ et $\deg r < \deg g$.*

Démonstration. Par le théorème 5.2 on a q et $r \in R[X]$, avec $\deg r < \deg g$, tel que $f = qg + r$. Pour démontrer l'unicité, on suppose que $f = q_1 g + r_1$ avec $\deg r_1 < \deg g$. Alors $(q - q_1)g = r_1 - r$ et $\deg(r_1 - r) < \deg g$, donc $q - q_1 = 0$ parce que g est unitaire (par récurrence sur l'entier n tel que $\deg(q - q_1) \leqslant n$), et ainsi $r_1 - r = 0$. □

Corolaire 5.4 (théorème du reste[1])**.** *Soient $f \in R[X]$ un polynôme sur un anneau commutatif R, et a un élément de R. Alors il existe un unique $q \in R[X]$ tel que $f(X) = q(X)(X - a) + f(a)$.*

Démonstration. Par le théorème 5.2 il existe $q \in R[X]$ et $r \in R$ uniques tels que $f(X) = q(X)(X - a) + r$. Mais alors $f(a) = q(a)(a - a) + r = r$. □

Sur un corps donné, nous pouvons construire un polynôme de degré au plus n qui prend des valeurs prescrites en $n + 1$ points distincts. Le théorème du reste montre que ce polynôme est unique, de sorte qu'un polynôme de degré au plus n ne peut pas avoir $n + 1$ racines distinctes. Ceci est l'un des quelques résultats dans la théorie générale des corps (comme opposés aux corps discrets ou aux corps de Heyting).

Théorème 5.5 (interpolation unique)**.** *Soient $a_0, \ldots, a_n$ des éléments deux à deux distincts dans un corps k, et soient $n + 1$ éléments $v_0, \ldots, v_n$ de k. Alors il existe un unique polynôme $f \in k[X]$ de degré au plus n tel que $f(a_i) = v_i$ pour chaque i.*

Démonstration. Nous démontrons l'existence par récurrence sur n. Si $n = 0$, prenons $f = v_0$. Si $n > 0$, alors par hypothèse de récurrence, on a un polynôme g de degré au plus $n - 1$ tel que $g(a_i) = (v_i - v_0)/(a_i - a_0)$ pour $1 \leqslant i \leqslant n$. Prenons $f(X) = (X - a_0)g(X) + v_0$.

Pour démontrer l'unicité, il suffit de montrer que si f est un polynôme de degré au plus n et si $f(a_i) = 0$ pour chaque i, alors $f = 0$. Nous procédons par récurrence sur n. Si $n = 0$, alors f est une constante, donc $f = 0$ parce que $f(a_0) = 0$. Supposons $n > 1$. Par le théorème du reste, nous pouvons écrire $f(X) = (X - a_n)g(X)$, où $\deg g \leqslant n - 1$. Comme $a_j \neq a_n$ pour $j < n$ et comme k est un corps, nous obtenons que $g(a_j) = 0$ pour $j < n$, donc $g = 0$ par récurrence. Par suite $f = 0$. □

1. **NdT.** Remainder theorem.

La démonstration du théorème 5.5 donne une construction par récurrence des coefficients λ_i de la **formule d'interpolation de Newton**

$$f = \lambda_0 + \lambda_1(X - a_0) + \lambda_2(X - a_0)(X - a_1) + \\ \cdots + \lambda_n(X - a_0)(X - a_1)\cdots(X - a_{n-1}).$$

Pour la **formule d'interpolation de Lagrange**, voir l'exercice 5.

Nous établissons l'algorithme d'Euclide pour les anneaux commutatifs discrets avec unités détachables, plutôt que seulement pour les corps discrets. L'algorithme construit le facteur commun recherché ou une non-unité non nulle. Une application typique est avec l'anneau $k[X]/(f)$, où k est un corps discret : la construction d'une non-unité non nulle donne une factorisation de f.

Théorème 5.6 (algorithme d'Euclide [1])**.** *Soient R un anneau commutatif discret avec unités détachables et I un idéal de type fini de $R[X]$. Ou bien l'idéal I est principal, ou bien il existe un élément de R non inversible et non nul.*

Démonstration. Ou bien $I = 0$, et alors I est principal, ou bien il y a un $n \in \mathbb{N}$ et un polynôme non nul $f \in I$ de degré $\deg f = n$. Nous pouvons supposer que f est unitaire (sinon nous avons une non-unité non nulle) et nous procédons par récurrence sur n. Si $n = 0$, alors $f = 1$, et donc $I = k[X] = (f)$. Si $n > 0$, alors chaque générateur g de I peut s'écrire comme $g = qf + r$ avec $\deg r < n$. Notons que $r \in I$. Ou bien chaque r est nul, ou bien l'un des r est $\neq 0$. Si chaque r est nul, alors $I = (f)$. Si un r est $\neq 0$, alors nous avons un polynôme non nul dans I de degré $< n$, et nous terminons par récurrence. □

Si $c = ab$ dans un anneau commutatif, alors nous disons que a **divise** c ; si a divise c nous disons que a est un **diviseur**, ou un **facteur**, de c.

Corolaire 5.7. *Soient k un corps discret et $a, b \in k[X]$. Alors il existe $s, t \in k[X]$ tels que $sa + tb$ divise a et b. Par suite $sa + tb$ est le plus grand commun diviseur de a et b au sens où tout diviseur commun de a et b divise $sa + tb$.*

Démonstration. Soit I l'idéal de $k[X]$ engendré par a et b. Comme k est un corps discret, le théorème 5.6 dit que I est principal ; autrement dit il existe s et t tels que $sa + tb$ divise a et b. □

Nous disons que deux éléments a et b dans un anneau commutatif sont **étrangers** [2] ou **fortement premiers entre eux** s'il existe des éléments s et t tels que $sa + tb = 1$. Ainsi le corolaire 5.7 implique que si deux polynômes sur un corps discret n'ont pas de facteur commun de degré strictement positif, ils sont étrangers. On voit facilement que si a et b sont étrangers et si a et c sont étrangers, alors a et bc sont étrangers (multiplier les deux équations).

1. **NdT.** L'algorithme d'Euclide est presque toujours utilisé sous la forme du corollaire 5.7, pour le cas où R est un corps discret. Voir cependant la démonstration du lemme IX.3.5.
2. **NdT.** Strongly relatively prime.

Exercices

1. Soient R et S des anneaux commutatifs, φ un homomorphisme d'anneaux de R vers S, et $s_1, \ldots, s_n$ des éléments de S. Montrer que φ admet une unique extension en un homomorphisme de $R[X_1, \ldots, X_n]$ vers S qui envoie X_i sur s_i.
2. Un **anneau intègre avec relation de séparation (étroite)** est un anneau intègre dont l'inégalité est une relation de séparation (étroite). Montrer que le corps de fractions d'un anneau intègre avec relation de séparation étroite est un corps de Heyting. Soient f et g des polynômes sur un anneau intègre avec relation de séparation R. Montrer que si $\deg f \geqslant i$ et $\deg g \geqslant j$, alors $\deg fg \geqslant i + j$. Utiliser ce résultat pour montrer que si R est un anneau intègre avec relation de séparation (étroite), alors il en va de même pour $R[X]$.
3. Soit R un anneau. L'**anneau des séries formelles** [1] $R[[X]]$ est défini comme l'ensemble des suites $\{a_n\}$ dans R, écrites sous la forme
$$a_0 + a_1 X + a_2 X^2 + \cdots ,$$
avec l'addition et la multiplication suggérées par la notation. Montrer que si R est un anneau intègre avec relation de séparation, il en va de même pour $R[[X]]$.
Idée. Supposez que R est un anneau intègre avec relation de séparation et que $fg = h \in R[[X]]$ avec
$$\begin{aligned} f &= f_0 + f_1 X + \cdots , \\ g &= g_0 + g_1 X + \cdots , \\ h &= h_0 + h_1 X + \cdots . \end{aligned}$$
Supposez que $f_i \neq 0$ et $g_j \neq 0$ pour un i, j ; montrez que $h_k \neq 0$ pour un $k \leqslant i + j$.
4. *Interpolation de Lagrange.* Montrer que le polynôme suivant satisfait le théorème 5.5.
$$f(X) = \sum\nolimits_{i=0}^{n} v_i \prod\nolimits_{j \neq i} \frac{X - \alpha_j}{\alpha_i - \alpha_j}.$$
5. Soit k un corps de Heyting et soit $f \in k[X]$ un polynôme non nul de degré au plus m. Montrer que si $a_0, a_1, \ldots, a_m$ sont des éléments distincts de k, alors il existe un i tel que $f(a_i) \neq 0$.
6. Soit k un corps de Heyting et soit $f \in k[X_1, \ldots, X_n]$ un polynôme non nul de degré au plus m en chaque variable séparément. Montrer que si k contient $m + 1$ éléments distincts, alors $f(a_1, \ldots, a_n) \neq 0$ pour des $a_i \in R$.

1. **NdT.** Formal power series ring.

7. Soit k un corps discret. Montrer que tout idéal premier propre non nul de $k[X]$ est maximal.
8. Soit f un polynôme non nul sur un corps discret k et soit $a \in k$. Montrer qu'il existe un unique entier naturel n et un unique polynôme $u \in k[X]$ tels que $f(X) = (X-a)^n u(X)$ et $u(a) \neq 0$. Si $n = 1$, a est appelé une **racine simple** de f ; si $n > 1$, a est appelé une **racine de multiplicité** n.
9. Donner un polynôme de degré 2 sur l'anneau des entiers modulo 6 avec 3 racines distinctes. Faire la même chose pour les quaternions rationnels.
10. Donner un contre-exemple brouwerien pour l'affirmation selon laquelle $\deg f \leqslant \deg g$ ou $\deg g \leqslant \deg f$ pour tous les polynômes f et g sur un anneau commutatif.

6 Matrices et espaces vectoriels

Soit α une application R-linéaire depuis un R-module à droite libre N vers un R-module à droite libre M. Si $e_1, \ldots, e_n$ est une base pour N et $f_1, \ldots, f_m$ est une base pour M, alors α détermine, et est déterminé par, la matrice $A = \{a_{ij}\}$ de format $m \times n$ telle que

$$\alpha(e_j) = \sum\nolimits_{i=1}^{m} f_i a_{ij}.$$

Si β est un homomorphisme d'un R-module libre L de base $d_1, \ldots, d_\ell$ vers N, alors nous obtenons une matrice $B = \{b_{jk}\}$ de format $n \times \ell$ telle que

$$\beta(d_k) = \sum\nolimits_{j=1}^{n} e_j b_{jk}.$$

Ainsi

$$\alpha\beta(d_k) = \alpha \sum\nolimits_{j=1}^{n} e_j b_{jk} = \sum\nolimits_{j=1}^{n} \alpha(e_j) b_{jk} = \sum\nolimits_{j=1}^{n} \sum\nolimits_{i=1}^{m} f_i a_{ij} b_{jk},$$

de sorte que la matrice qui correspond à $\alpha\beta$ est la **matrice produit** AB, qui est une matrice de format $m \times \ell$ dont l'entrée ik est $\sum_{j=1}^{n} a_{ij} b_{jk}$. Si nous considérons les applications R-linéaires de N vers N, nous obtenons un isomorphisme entre l'anneau $E_R(N)$ des endomorphismes du R-module à droite libre N et l'anneau $\mathrm{Mat}_n(R)$ des matrices de format $n \times n$ sur l'anneau R. La matrice qui correspond à l'endomorphisme identité est appelée une **matrice identité** et on la note I.

Si $e'_1, \ldots, e'_n$ est une autre base pour N, et $f'_1, \ldots, f'_m$ est une autre base pour M, notons σ et τ les automorphismes de N et M définis par $\sigma(e_j) = e'_j$, et $\tau(f_i) = f'_i$, et soient S et T les matrices de σ et τ par rapport aux anciennes bases. Alors la matrice de α par rapport aux nouvelles bases est donnée par

$$\alpha(e'_j) = \alpha(\sigma e_j) = \alpha\Big(\sum\nolimits_i e_i s_{ij}\Big) = \sum\nolimits_{i,k} f_k a_{ki} s_{ij} = \sum\nolimits_{i,k} \tau^{-1}(f'_k) a_{ki} s_{ij}$$

Ainsi $\tau\alpha(e'_j) = \sum_{ik} f'_k a_{ki} s_{ij}$, et donc la nouvelle matrice de $\tau\alpha$ est AS, et la nouvelle matrice de α est $T^{-1}AS$, où T^{-1} est la matrice de τ^{-1}.

La i-ième **ligne** $(a_{i1}, \ldots, a_{in})$ de A peut être considérée comme un élément du R-module à gauche R^n. L'**espace des lignes** de A est le sous-module de R^n engendré par les lignes de A. Une **manipulation élémentaire de lignes** [1] sur A consiste à

(i) échanger deux lignes, ou

(ii) multiplier une ligne par une unité de R, ou

(iii) ajouter un multiple d'une ligne à une autre ligne.

La matrice qui est obtenue à partir d'une manipulation élémentaire de lignes de A est la matrice de α par rapport à une autre base de M. Celle obtenue en échangeant les lignes s et t de A est la matrice de α si nous échangeons les éléments de base f_s et f_t. Celle obtenue en multipliant la ligne s de A par l'unité u est la matrice de α si nous remplaçons l'élément de base f_s par $f_s u^{-1}$. Celle obtenue en ajoutant r fois la ligne s à la ligne t est la matrice de α si nous remplaçons l'élément de base f_s par $f_s - f_t r$. L'espace des lignes de A est inchangé par les manipulations élémentaires de lignes.

La j-ième colonne $(a_{1j}, \ldots, a_{mj})$ de A peut être considérée comme un élément du R-module à droite R^m. Une **manipulation élémentaire de colonnes** [2] sur A consiste à

(i) échanger deux colonnes, ou

(ii) multiplier une colonne par une unité de R, ou

(iii) ajouter un multiple d'une colonne à une autre colonne.

La matrice qui est obtenue à partir d'une manipulation élémentaire de colonnes de A est la matrice de α par rapport à une autre base de M. Celle obtenue en échangeant les colonnes s et t de A est la matrice de α si nous échangeons les éléments de base e_s et e_t. La matrice obtenue en multipliant (à droite) la colonne s de A par l'unité u est la matrice de α si nous remplaçons l'élément de base e_s par $e_s u$. Celle obtenue en ajoutant r fois la colonne s à la colonne t est la matrice de α si nous remplaçons l'élément de base e_t par $e_t + e_s r$.

Une **matrice élémentaire** est une matrice obtenue en appliquant une manipulation élémentaire de lignes à une matrice identité. Si E est la matrice obtenue en appliquant la manipulation élémentaire de lignes ρ à la matrice identité, alors E peut être obtenue en appliquant une manipulation élémentaire de colonnes ρ' à la matrice identité. De plus, si A et B sont des matrices de formats convenables, alors EA est obtenue en appliquant la manipulation ρ à A, et BE est obtenue en appliquant la manipulation ρ' à B.

1. **NdT.** Elementary row operation.
2. **NdT.** Elementary column operation.

Une matrice avec exactement un 1 dans chaque ligne et chaque colonne et tous les autres coefficients nuls est appelée une **matrice de permutation**, et c'est un produit de matrices élémentaires.

On voit facilement qu'une matrice élémentaire a une inverse (à droite et à gauche) qui est aussi élémentaire.

Si k est un anneau à division, alors un k-module est appelé un **espace vectoriel** sur k. En mathématiques classiques tout espace vectoriel sur un anneau à division est libre. Ce n'est plus le cas constructivement, même pour les espaces vectoriels de type fini sur les corps discrets, comme le montre l'exemple brouwerien suivant.

Exemple 6.1. Soit a une suite binaire, soit $i^2 = -1$ et considérons la suite des sous-corps

$$k_n = \{\, s + ta_n i : s, t \in \mathbb{Q} \,\}.$$

du corps des nombres de Gauss $\mathbb{Q}(i)$. Posons $k = \bigcup k_n$. Alors k est un corps discret, et $\mathbb{Q}(i)$ est un k-module discret engendré par les deux éléments 1 et i. Mais nous ne pouvons pas construire une base de $\mathbb{Q}(i)$ sur k. □

Si l'espace vectoriel V est un k-module libre de rang n, alors n est appelé la **dimension** de V et on écrit $n = \dim_k V$, ou simplement $\dim V$; l'espace V est alors appelé un **espace vectoriel de dimension finie** sur k. Le théorème suivant montre, entre autres choses, que $\dim V$ est bien définie si k est discret.

Théorème 6.2. *Soient V et W des espaces vectoriels sur un anneau à division discret k, de dimensions respectives n et m, et soit T une application linéaire de V vers W. Alors il existe des bases $e_1, \ldots, e_n$ de V et $f_1, \ldots, f_m$ de W, et un indice $\ell \leqslant n$, tels que $T(e_i) = f_i$ pour $i \leqslant \ell$, et $T(e_i) = 0$ pour $i > \ell$.*

Démonstration. Soit $A = \{a_{ij}\}$ la matrice de T par rapport aux bases données pour V et W. Par des manipulations élémentaires de lignes et de colonnes nous pouvons faire que $a_{ij} = 0$ pour $i \neq j$, que $a_{ii} \in \{0, 1\}$, et que $a_{ii} \geqslant a_{jj}$ si $i \leqslant j$. Et ceci revient à construire les nouvelles bases voulues pour V et W. □

En prenant pour f l'application identique dans le théorème 6.2, nous voyons que la dimension d'un espace vectoriel de dimension finie est bien définie. Le théorème 6.2 implique de manière immédiate que $\ker T$ et $\operatorname{im} T$ sont des facteurs directs de dimension finie, et que $\dim \ker T + \dim \operatorname{im} T = \dim V$.

La difficulté dans l'exemple 6.1 est que le k-sous-espace engendré par 1 n'est pas détachable : nous ne pouvons pas dire si i est ou n'est pas dans ce sous-espace. Un *facteur direct* A d'un espace vectoriel discret est détachable parce que $x \in A$ si, et seulement si, la projection de x dans A est égale à x. Par suite le corolaire suivant implique que les sous-espaces vectoriels de type fini d'un espace vectoriel de dimension finie sont détachables.

Corolaire 6.3. *Soit V un espace vectoriel de dimension finie sur un anneau à division discret k. Soit W un sous-espace de type fini de V. Alors W est un facteur direct de dimension finie de V.*

Démonstration. Puisque W est de type fini, il existe un espace vectoriel de dimension finie F sur k et une application linéaire T de F sur W. Le théorème 6.2 montre que W est un facteur direct de dimension finie. □

Corolaire 6.4. *Soit V un espace vectoriel de dimension finie sur un anneau à division discret k. Alors l'intersection de deux sous-espaces de type fini de V est un facteur direct de dimension finie.*

Démonstration. Soient A et B des sous-espaces de type fini de V. Par le corolaire 6.3 nous pouvons trouver un sous-espace C supplémentaire de B dans V. La projection sur C, restreinte à A, est une application linéaire de A vers C dont le noyau est $A \cap B$. Par suite $A \cap B$ est un facteur direct de dimension finie de V. □

Soit V un espace vectoriel sur un anneau à division k. Nous disons que $v_1, \ldots, v_n \in V$ sont **(linéairement) dépendants** si l'on a des $a_i \in k$ tels que $\sum_i a_i v_i = 0$ avec $a_i \neq 0$ pour un i. Lorsque k et V sont discrets, nous disons que $v_1, \ldots, v_n$ sont **(linéairement) indépendants** s'ils ne sont pas dépendants ; on voit alors facilement que $v_1, \ldots, v_n$ forment une base de V si, et seulement si, ils sont indépendants et engendrent V (k et V supposés discrets).

Corolaire 6.5. *Soit V un espace vectoriel de dimension finie sur un anneau à division discret k. Si $v_1, \ldots, v_n$ sont des éléments de V, alors ou bien $v_1, \ldots, v_n$ sont dépendants, ou bien ils sont indépendants.*

Démonstration. Considérons l'application linéaire T de k^n vers V qui envoie la base naturelle sur $v_1, \ldots, v_n$. Le noyau de T est de dimension finie d'après le théorème 6.2, et $v_1, \ldots, v_n$ sont dépendants si, et seulement si, le noyau de T est non nul. □

Théorème 6.6. *Soient $k \subseteq K$ des anneaux à division discrets tels que K soit un espace vectoriel de dimension finie sur k, et soit V un espace vectoriel sur K. Alors V est de dimension finie sur K si, et seulement si, V est de dimension finie sur k, et dans ce cas on a $\dim_k V = \dim_k K \dim_K E$.*

Démonstration. Si V est de dimension finie sur K, alors, d'après le théorème 4.3, V est de dimension finie sur k, et la formule du produit pour les dimensions s'applique. Inversement, supposons que V soit de dimension finie sur k et que nous ayons construit un système $x_1, \ldots, x_m \in V$ qui est K-indépendant. Alors $Kx_1 + \cdots + Kx_m$ est un facteur direct de V en tant qu'espace vectoriel sur k, ceci d'après le corolaire 6.3. Si $Kx_1 + \cdots + Kx_m = V$, nous avons terminé ;

sinon un élément de V qui n'appartient pas à $Kx_1 + \cdots + Kx_m$ étend le système K-indépendant $x_1, \ldots, x_m$ et nous terminons par récurrence sur la dimension (sur k) d'un supplémentaire de $Kx_1 + \cdots + Kx_m$. □

Dans le théorème 6.6 il est également vrai que si V est de dimension finie sur k et sur K, et non nul, alors K est de dimension finie sur k. Nous n'aurons pas besoin de ce résultat qui est une conséquence immédiate du théorème d'Azumaya du chapitre suivant.

Exercices

1. Donner un exemple brouwerien pour un espace vectoriel V sur $\mathbb{Q}$ qui contient deux sous-espaces de dimension finie dont l'intersection n'est pas de dimension finie. (Suggestion : considérer l'espace vectoriel $V = \mathbb{Q}^2/S$ avec un sous-espace convenable S de $\mathbb{Q}^2$). Vous pouvez arranger les choses pour que votre exemple soit discret.
2. Généraliser les corolaires 6.3 et 6.4 au cas où V est un module libre sur un anneau à division discret k.
3. Montrer qu'une manipulation élémentaire de lignes de type (i) peut être réalisée au moyen de manipulations élémentaires de lignes de types (ii) et (iii).
4. Un anneau R est **von-Neumann-régulier** si pour chaque $a \in R$ on a un $x \in R$ tel que $axa = a$. Montrer que l'anneau des matrices $n \times n$ sur un anneau à division discret est von-Neumann-régulier. Montrer qu'un anneau est von-Neumann-régulier si, et seulement si, tout idéal principal à gauche est engendré par un idempotent.

7 Déterminants

Soit un anneau commutatif R et soit $A = \{a_{ij}\}$ un élément de $\mathrm{Mat}_n(R)$. Le **déterminant** de A est défini comme

$$\det A = \sum\nolimits_{\sigma} \mathrm{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)},$$

où σ parcourt le groupe S_n des permutations de $\{1, 2, \ldots, n\}$.

Théorème 7.1. *Soient A et B des matrices $n \times n$ sur un anneau commutatif.*

(i) $\det A = \det A^t$.

(ii) $\det A$ *est une fonction linéaire de chaque ligne de* A.

(iii) *Si deux lignes sont égales,* $\det A = 0$.

(iv) $\det AB = \det A \det B$.

Démonstration. Pour vérifier le point (i) notez que si $\tau = \sigma^{-1}$, alors

$$\text{dét } A = \sum\nolimits_{\sigma} \text{sgn}(\sigma) a_{\tau(1)1} \cdots a_{\tau(n)n} = \text{dét } A^t$$

car $\text{sgn}(\sigma) = \text{sgn}(\tau)$. Le point (ii) est clair d'après la définition de dét A car chaque terme dans la somme qui définit le déterminant contient exactement un élément de la ligne i. Concernant le point (iii), si les lignes i et j de A sont égales et si $i \neq j$, alors les permutations peuvent être rangées par paires $\{\sigma, \sigma \cdot (i,j)\}$. Les termes correspondant aux éléments de chaque paire dans la définition du déterminant sont égaux au signe près, de sorte que leur somme est nulle, ce qui établit le point (iii). Enfin considérons dét A dét $B =$

$$\Big(\sum\nolimits_{\sigma} \text{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}\Big) \cdot \Big(\sum\nolimits_{\tau} \text{sgn}(\tau) b_{1\tau(1)} \cdots b_{n\tau(n)}\Big) =$$

$$\sum\nolimits_{\sigma,\tau} \text{sgn}(\sigma\tau) a_{1\sigma(1)} \cdots a_{n\sigma(n)} b_{1\tau(1)} \cdots b_{n\tau(n)} =$$

$$\sum\nolimits_{\sigma,\tau} \text{sgn}(\sigma\tau) a_{1\sigma(1)} b_{\sigma(1)\tau\sigma(1)} \cdots a_{n\sigma(n)} b_{\sigma(n)\tau\sigma(n)} =$$

$$\sum\nolimits_{\sigma} \sum\nolimits_{\pi} \text{sgn}(\pi) a_{1\sigma(1)} b_{\sigma(1)\pi(1)} \cdots a_{n\sigma(n)} b_{\sigma(n)\pi(n)}. \tag{7.2}$$

Si σ est une fonction de $\{1, 2, \ldots, n\}$ vers $\{1, 2, \ldots, n\}$ plutôt qu'une permutation, et si $\sigma(i) = \sigma(j)$ pour $i \neq j$, alors

$$\sum\nolimits_{\pi} \text{sgn}(\pi) a_{1\sigma(1)} b_{\sigma(1)\pi(1)} \cdots a_{n\sigma(n)} b_{\sigma(n)\pi(n)} = 0$$

parce que pour chaque permutation π les termes dans la somme indexés par π et par $\pi \cdot (i,j)$ ont pour somme 0. Par suite nous pouvons considérer que σ parcourt toutes les fonctions de $\{1, 2, \ldots, n\}$ vers $\{1, 2, \ldots, n\}$ dans (7.2), et ainsi

$$\text{dét } A \ \text{ dét } B = \sum\nolimits_{\pi} \text{sgn}(\pi) \prod\nolimits_{i} \sum\nolimits_{j} a_{ij} b_{j\pi(i)} = \text{dét } AB. \qquad \square$$

Le **cofacteur** A_{ij} de l'élément a_{ij} dans la matrice A est $(-1)^{i+j}$ fois le déterminant de la matrice de $\text{Mat}_{n-1}(R)$ obtenue en supprimant la ligne i et la colonne j de A. On voit facilement d'après la définition de dét A que, pour chaque i,

$$a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in} = \text{dét } A,$$

ce qui explique le nom de *cofacteur*. D'après le théorème 7.1(iii), nous avons aussi l'égalité

$$a_{i1}A_{j1} + a_{i2}A_{j2} + \cdots + a_{in}A_{jn} = 0$$

lorsque $i \neq j$. Si nous définissons la **matrice adjointe** de A comme la matrice B dont l'entrée ij est A_{ji}, alors

$$AB = (\text{dét } A)\text{I} = (\text{dét } A^t)\text{I} = (A^t B^t)^t = BA. \tag{7.3}$$

Ainsi nous pouvons construire une inverse de la matrice A si nous pouvons construire un inverse du déterminant dét A.

Théorème 7.4. *Soient R un anneau commutatif et $A \in \mathrm{Mat}_n(R)$. Alors A est une unité de $\mathrm{Mat}_n(R)$ si, et seulement si,* dét A *est une unité de R* [1].

Démonstration. Si $AB = \mathrm{I}$, alors $(\text{dét}\, A)(\text{dét}\, B) = \text{dét}\, \mathrm{I} = 1$, et dét A est une unité de R. Inversement, si dét A est une unité de R, alors (7.3) montre que A est une unité de $\mathrm{Mat}_n(R)$. □

Nous pouvons maintenant montrer que le rang d'un module libre de rang fini sur un anneau commutatif non trivial est un invariant. En fait, nous démontrons un peu mieux.

Théorème 7.5. *Soit R un anneau commutatif. Soient $m < n$ des entiers strictement positifs et $\varphi\colon R^m \to R^n$ un épimorphisme de R-modules. Alors $R = 0$.*

Démonstration. On a une application R-linéaire $\psi\colon R^n \to R^m$ telle que $\varphi\psi = 1$. On étend φ en une application linéaire depuis $R^n = R^m \oplus R^{n-m}$ en posant $\varphi(R^{n-m}) = 0$ et l'on regarde ψ comme une application linéaire vers R^n. Comme $(\text{dét}\, \varphi)(\text{dét}\, \psi) = 1$ et dét $\varphi = 0$, on a $1 = 0$ dans R. □

Lemme 7.6. *Soient R un anneau commutatif, M un R-module, et une matrice $A \in \mathrm{Mat}_n(R)$. Si U est une matrice de format $n \times 1$ à coefficients dans M et si $AU = 0$, alors* $(\text{dét}\, A)U = 0$.

Démonstration. Soit B la matrice adjointe de A. Alors $BAU = 0$, et donc $(\text{dét}\, A)U = 0$. □

Si $A \in \mathrm{Mat}_n(R)$ avec R un anneau commutatif, $X\mathrm{I} - A$ est une matrice à coefficients dans $R[X]$. Le déterminant de $X\mathrm{I} - A$ est appelé le **polynôme caractéristique** de A. Le **polynôme caractéristique** d'un endomorphisme α d'un R-module libre F de rang n est le polynôme caractéristique de la matrice de α par rapport à une base de F. Le polynôme caractéristique de α est unitaire de degré n. Si B est la matrice de α par rapport à une autre base de F, alors $B = S^{-1}AS$ pour une matrice inversible $S \in \mathrm{Mat}_n(R)$. Par suite, le polynôme caractéristique de B est le déterminant de $X\mathrm{I} - S^{-1}AS = S^{-1}(X\mathrm{I} - A)S$, qui est égal au déterminant de $X\mathrm{I} - A$, de sorte que le polynôme caractéristique de α ne dépend pas de la base choisie de F. Le théorème de Cayley-Hamilton dit que α annule son polynôme caractéristique.

1. **NdT.** En fait, la démonstration dit aussi que si la matrice est inversible à gauche, ou à droite, elle est inversible.

Théorème 7.7 (Cayley-Hamilton)**.** *Soient R un anneau commutatif et $f(X)$ le polynôme caractéristique d'un endomorphisme α d'un R-module F libre de rang fini. Alors $f(\alpha) = 0$.*

Démonstration. Soit S le sous-anneau (commutatif) de l'anneau des endomorphismes de F engendré par α et R. Alors F est un S-module *via* la multiplication dans F. Soit $A = \{a_{ij}\}$ la matrice de α par rapport à une base $u_1, \ldots, u_n$ de F, de sorte que

$$\alpha u_j = \sum\nolimits_i a_{ij} u_i.$$

Soit $U = (u_1, \ldots, u_n)^t$ et soit $C = \alpha \mathrm{I} - A$, qui est une matrice $\in \mathrm{Mat}_n(S)$. Alors $C^t U = 0$ et donc $(\det C^t)U = 0$ par le lemme 7.6. Par suite $\det C^t = 0$. Or $\det C^t = \det C = f(\alpha)$. □

Exercices

1. Soit R un anneau commutatif et soit une application $f\colon \mathrm{Mat}_n(R) \to R$ telle que

   (i) $f(A)$ est une fonction linéaire de chaque ligne de A ;

   (ii) $f(A) = 0$ si deux lignes de A sont égales.

   Montrer qu'il existe un $r \in R$ tel que $f(A) = r \det A$. Utiliser ce résultat pour montrer que $\det AB = \det A \det B$.

2. Soit M un module libre de rang n sur un anneau commutatif R et soit α un endomorphisme de M. Si A et $B \in \mathrm{Mat}_n(R)$ sont des matrices de α par rapport à des bases de M, montrer que $\det A = \det B$.

3. Une autre démonstration du théorème de Cayley-Hamilton.

   (i) Montrer que $\mathrm{Mat}_n(R[X])$ est isomorphe à $\mathrm{Mat}_n(R)[X]$ pour tout anneau R.

   (ii) Soient S un anneau non nécessairement commutatif, $a \in S$, et $f, g \in S[X]$. Montrer que si $f(X) = g(X)(X - a)$, alors $f(a) = 0$. (Attention, il n'est pas vrai que si $f(X) = (X - a)g(X)$, alors $f(a) = 0$.)

   (iii) Démontrer le théorème 7.7 en posant $S = \mathrm{Mat}_n(R)$ et en utilisant (7.3) pour factoriser le polynôme caractéristique $f(X)$ sous la forme $g(X)(X - a)$, vu comme un élément de $S[X]$. Enfin appliquer (ii).

4. On considère le déterminant $\det M$ de la **matrice de Vandermonde**

$$M = \begin{bmatrix} 1 & X_1 & X_1^2 & \cdots & X_1^{m-1} \\ 1 & X_2 & X_2^2 & \cdots & X_2^{m-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & X_m & X_m^2 & \cdots & X_m^{m-1} \end{bmatrix}$$

à coefficients dans l'anneau commutatif $k[X_1, \ldots, X_m]$. Montrer que

$$\text{dét } M = \prod_{i<j}(X_j - X_i).$$

Utiliser cette formule pour démontrer que si $f = f_0 + f_1X + \cdots + f_{m-1}X^{m-1} \neq 0$ est un polynôme sur un corps de Heyting k, et si $a_1, \ldots, a_m$ sont des éléments deux à deux distincts de k, alors $f(a_i) \neq 0$ pour un i.

8 Polynômes symétriques

Soient R un anneau commutatif et $f \in R[X_1, \ldots, X_n]$ un polynôme à coefficients dans R. Nous disons que f est **invariant** par une permutation π de l'ensemble des indéterminées $\{X_1, \ldots, X_n\}$ si

$$f(X_1, \ldots, X_n) = f(\pi(X_1), \ldots, \pi(X_n)).$$

Si f est invariant par toute permutation de ses indéterminées, nous disons que f est un **polynôme symétrique**. Si nous considérons

$$f = (Y + X_1)(Y + X_2) \cdots (Y + X_n)$$

comme un polynôme en les indéterminées $Y, X_1, \ldots, X_n$ à coefficients dans R, il est clair que f est invariant par toute permutation des indéterminées $X_1, \ldots, X_n$. Donc si nous écrivons f comme un polynôme

$$Y^n + \sigma_1 Y^{n-1} + \cdots + \sigma_n$$

en Y à coefficients dans $R[X_1, \ldots, X_n]$, les coefficients σ_i sont des polynômes symétriques de $R[X_1, \ldots, X_n]$. En développant f comme une somme de monômes, nous trouvons

$$\sigma_1 = \sum_i X_i,\ \sigma_2 = \sum_{i<j} X_iX_j,\ \sigma_3 = \sum_{i<j<k} X_iX_jX_k,\ \ldots,\ \sigma_n = X_1X_2 \cdots X_n.$$

Les polynômes $\sigma_1, \ldots, \sigma_n$ sont appelés les **polynômes symétriques élémentaires** en n indéterminées.

Clairement tout polynôme dans le sous-anneau $R[\sigma_1, \ldots, \sigma_n]$ de $R[X_1, \ldots, X_n]$ est symétrique ; le fait que chaque polynôme symétrique a une représentation unique en tant qu'élément de $R[\sigma_1, \ldots, \sigma_n]$ est le théorème fondamental des polynômes symétriques.

Théorème 8.1. *Soit f un polynôme symétrique de $R[X_1, \ldots, X_n]$. Alors il existe un unique polynôme $h \in R[Y_1, \ldots, Y_n]$ tel que $f = h(\sigma_1, \ldots, \sigma_n)$.*

Démonstration. Nous construisons h par récurrence sur n. En remplaçant R par $\mathbb{Z}[r_1, \ldots, r_m]$, où les r_i sont les indéterminées qui correspondent aux coefficients des monômes dans l'expression de f, nous pouvons supposer, afin de construire h, que R est discret ; cette convention technique nous permet de parler de degrés. Si $n = 1$, alors $\sigma_1 = X_1$ et tout polynôme est symétrique, de sorte que nous pouvons choisir $h = f(Y_1)$. Si $n > 1$, considérons les polynômes symétriques élémentaires $\tau_1, \ldots, \tau_{n-1}$ en les indéterminées $X_1, \ldots, X_{n-1}$. Notons que $\tau_i = \sigma_i(X_1, \ldots, X_{n-1}, 0)$. Par récurrence nous pouvons construire $g \in R[Y_1, \ldots, Y_{n-1}]$ tel que

$$f(X_1, \ldots, X_{n-1}, 0) = g(\tau_1, \ldots, \tau_{n-1}).$$

Nous pouvons supposer que g ne contient aucun monôme $Y_1^{e_1} \cdots Y_{n-1}^{e_{n-1}}$ tel que $\sum_{i=1}^{n-1} ie_i$ soit supérieur au degré total de $f(X_1, \ldots, X_{n-1}, 0)$. Alors le polynôme

$$f_1 = f - g(\sigma_1, \ldots, \sigma_{n-1})$$

est symétrique et $f_1(X_1, \ldots, X_{n-1}, 0) = 0$. Donc f_1 est divisible par X_n, et par symétrie il est divisible par X_i pour chaque i. Ceci implique que f_1 est divisible par $\sigma_n = X_1 X_2 \cdots X_n$, et nous pouvons écrire $f_1 = \sigma_n f_2$ où f_2 est symétrique et de plus petit degré que f_1 et f. Par récurrence sur le degré de f nous savons construire $p \in R[Y_1, \ldots, Y_n]$ tel que $f_2 = p(\sigma_1, \ldots, \sigma_n)$, et nous posons $h = Y_n p + g$.

Pour montrer que h est unique, il suffit de montrer que si $g(\sigma_1, \ldots, \sigma_n) = 0$ pour un $g \in R[Y_1, \ldots, Y_n]$, alors $g = 0$. Nous procédons par récurrence sur n. Le cas $n = 1$ est trivial, aussi nous pouvons supposer que $n > 1$ et écrire $g = g_m Y_n^m + g_{m-1} Y_n^{m-1} + \cdots + g_0$ comme un polynôme en Y_n ayant ses coefficients g_i dans $R[Y_1, \ldots, Y_{n-1}]$. En substituant σ_i à Y_i et en posant ensuite $X_n = 0$ nous obtenons $g_0(\tau_1, \ldots, \tau_{n-1}) = 0$, où les τ_i sont des polynômes symétriques élémentaires en $X_1, \ldots, X_{n-1}$. Par récurrence sur n nous concluons que $g_0 = 0$. Alors $g = Y_n p$ pour un $p \in R[Y_1, \ldots, Y_n]$. Puis, comme $0 = g(\sigma_1, \ldots, \sigma_n) = \sigma_n p(\sigma_1, \ldots, \sigma_n)$, nous en déduisons que $p(\sigma_1, \ldots, \sigma_n) = 0$, et par récurrence sur m que $p = 0$, et donc que $g = 0$. □

Corolaire 8.2. *Les polynômes symétriques élémentaires $\sigma_1, \ldots, \sigma_n$ sont algébriquement indépendants sur R ; c'est-à-dire, si $g(\sigma_1, \ldots, \sigma_n) = 0$, alors $g = 0$.* □

L'anneau de polynômes $R[X_1, \ldots, X_n]$ est un module sur le sous-anneau $R[\sigma_1, \ldots, \sigma_n]$ des polynômes symétriques. Nous montrons que c'est un module libre de rang fini.

Lemme 8.3. *Le sous-anneau $R[\sigma_1, \ldots, \sigma_n, X_j, \ldots, X_n]$ de $R[X_1, \ldots, X_n]$ est formé des polynômes qui sont invariants par toute permutation de $X_1, \ldots, X_{j-1}$.*

Démonstration. Soit $S = R[X_j, \dots, X_n]$, et soient $\tau_1, \dots, \tau_{j-1}$ les polynômes symétriques élémentaires en $X_1, \dots, X_{j-1}$. Les polynômes de $R[X_1, \dots, X_n] = S[X_1, \dots, X_{j-1}]$ qui sont invariants par toute permutation de $X_1, \dots, X_{j-1}$ constituent le sous-anneau $S[\tau_1, \dots, \tau_{j-1}]$ d'après le théorème 8.1. On doit donc montrer que $S[\sigma_1, \dots, \sigma_n] = S[\tau_1, \dots, \tau_{j-1}]$. Comme chaque σ_i est invariant par les permutations de $X_1, \dots, X_{j-1}$, on a $S[\sigma_1, \dots, \sigma_n] \subset S[\tau_1, \dots, \tau_{j-1}]$. Posons

$$f(Y) = (Y + X_1)(Y + X_2) \cdots (Y + X_n) \text{ et}$$
$$g(Y) = (Y + X_j)(Y + X_{j+1}) \cdots (Y + X_n).$$

Les polynômes unitaires f et g sont des éléments de $S[\sigma_1, \dots, \sigma_n][Y]$ et l'on a

$$f = gq \text{ où } q = (Y + X_1) \cdots (Y + X_{j-1}) = Y^{j-1} + \tau_1 Y^{j-2} + \cdots + \tau_{j-1}.$$

Par ailleurs, la division de f par g dans $S[\sigma_1, \dots, \sigma_n][Y]$ donne $f = gq_1 + r_1$ avec $\deg(r_1) < \deg(g)$.
Donc on a $\deg_Y(g(q_1 - q)) < \deg_Y(g)$ dans $R[X_1, \dots, X_n][Y]$, ce qui implique $q_1 = q$.
Ainsi $q \in S[\sigma_1, \dots, \sigma_n][Y]$ et donc $S[\tau_1, \dots, \tau_{j-1}] \subset S[\sigma_1, \dots, \sigma_n]$. □

Théorème 8.4. *Les monômes $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ avec $i_k \leqslant k - 1$ forment un système libre de $n!$ générateurs de $R[X_1, \dots, X_n]$ lorsque l'on voit cet anneau comme un module sur $R[\sigma_1, \dots, \sigma_n]$.*

Démonstration. Soit $R_j = R[\sigma_1, \dots, \sigma_n, X_j, \dots, X_n]$. Nous allons montrer que les éléments $1, X_j, X_j^2 \dots, X_j^{j-1}$ forment une famille libre de générateurs de R_j sur R_{j+1}. D'après le lemme 8.3, le polynôme $f_j(Y) = (Y - X_1)(Y - X_2) \cdots (Y - X_j)$ a ses coefficients dans R_{j+1}. Le polynôme f_j est unitaire de degré j, et $f_j(X_j) = 0$. Donc $1, X_j, X_j^2 \dots, X_j^{j-1}$ engendrent $R_j = R_{j+1}[X_j]$ sur R_{j+1}. Il reste à voir que $1, X_j, X_j^2 \dots, X_j^{j-1}$ sont indépendants sur R_{j+1}. Supposons que $g(X_j) = 0$ pour un $g \in R_{j+1}[Y]$ tel que $\deg g < j - 1$. Comme g est invariant par les permutations de $X_1, \dots X_j$, nous avons $g(X_i) = 0$ si $1 \leqslant i \leqslant j$, de sorte que g a j racines distinctes ; donc $g = 0$ car $X_i - X_j$ est simplifiable d'après l'unicité dans le théorème du reste. □

Exercices

1. Soit K un corps discret et soient $\sigma_1, \dots, \sigma_n$ les polynômes symétriques élémentaires de $K[X_1, \dots, X_n]$. Montrer que l'ensemble des $n!$ monômes $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ avec $i_k \leqslant k - 1$ forment une base du corps de fractions de $K[X_1, \dots, X_n]$ en tant qu'espace vectoriel sur le corps de fractions de $K[\sigma_1, \dots, \sigma_n]$.

2. Montrer que l'algorithme suivant réécrit un polynôme symétrique donné f comme un polynôme en les polynômes symétriques élémentaires. On ordonne les monômes $X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ lexicographiquement en posant

$$X_1^{i_1}X_2^{i_1}\cdots X_n^{i_n} \leqslant X_1^{j_1}X_2^{j_2}\cdots X_n^{j_n}$$

si pour chaque k ou bien $i_k \leqslant j_k$ ou bien il y a un $m < k$ tel que $i_m < j_m$. Soit $aX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ le terme dominant de f par rapport à cet ordre lexicographique. Montrer que $i_k \geqslant i_{k+1}$ pour $k = 1, \ldots, n-1$. Retrancher

$$a\sigma_1^{i_1-i_2}\sigma_2^{i_2-i_3}\cdots\sigma_n^{i_n}$$

de f. Montrer que la différence a un degré plus petit pour cet ordre lexicographique. Remplacer f par la différence et recommencer.

3. Exprimer $\sum_{i=1}^n X_i^3$ en termes des polynômes symétriques élémentaires $\sigma_1, \ldots, \sigma_n$.
4. Soient R un anneau commutatif et $E = \prod_{i<j}(X_i - X_j) \in R[X_1, \ldots, X_n]$.
   (a) Montrer que le polynôme E est **alternant**, c'est-à-dire

$$E(\pi X_1, \ldots, \pi X_n) = \operatorname{sgn}(\pi)E(X_1, \ldots, X_n)$$

   pour chaque permutation π, et que E^2 est symétrique. Montrer que si 2 est une unité de R, alors tout polynôme alternant est de la forme fE où f est un polynôme symétrique.

   (b) Montrer qu'il existe un polynôme $d \in \mathbb{Z}[Y_1, \ldots, Y_n]$ tel que si $\prod_{i=1}^n (X - r_i) = X^n + a_1X^{n-1} + \cdots + a_n$, où les r_i et a_j sont dans un corps K, alors les r_i sont distincts si, et seulement si, $d(a_1, \ldots, a_n) \neq 0$ dans K.

   (c) Montrer que E est invariant par les permutations paires des X_i. Montrer que si 2 est une unité de R, alors $R[E, \sigma_1, \ldots, \sigma_n]$ est l'anneau de tous les polynômes invariants par les permutations paires des X_i.

9 Notes

Nous laissons ouverte la question de savoir ce que devrait être une inégalité raisonnable sur un anneau à division. Pour qu'un anneau à division soit un anneau à division au sens classique, l'inégalité doit être standard ; mais cette requête est trop faible pour fournir des conséquences utiles. Beaucoup de corps non discrets, comme les nombres réels ou les nombres complexes, sont des corps de Heyting. Quoique les corps discrets soient aussi des corps de Heyting, la tentation d'identifier la notion de corps avec celle de corps de Heyting est amoindrie par l'existence de corps par négation naturels (les corps résiduels de

valeurs absolues non archimédiennes) qui ont une inégalité ni cotransitive ni étroite.

Lorsqu'un idéal P dans un anneau commutatif n'est pas détachable ce n'est pas clair de déterminer ce que ce devrait être pour cet idéal d'être premier. Dans l'anneau des nombres réels, l'idéal 0 n'est pas premier selon notre définition, parce qu'il est possible de construire deux nombres réels dont le produit est nul et pour lesquels nous ne pouvons pas dire lequel est nul. En effet, LLPO est équivalent à l'affirmation à propos de nombres réels que si $ab = 0$, alors $a = 0$ ou $b = 0$ (exercice 3.5). Dans les anneaux avec une notion d'inégalité positive, comme les nombres réels, il est naturel de définir un idéal premier comme un idéal tel que chaque fois que $a, b \notin P$, alors $ab \notin P$. Notre définition d'un idéal premier a le mérite de ne pas se référer à l'inégalité.

Comme P est un idéal premier si, et seulement si, P est le noyau d'un homomorphisme dans un corps par négation, il est naturel de définir un idéal maximal comme le noyau d'un homomorphisme *sur* un corps par négation. Il peut y avoir une meilleure définition mais nous ne le saurons pas tant que nous n'aurons pas trouvé une théorie intéressante concernant les idéaux maximaux non détachables.

Les modules libres sur des ensembles non discrets ne sont pas juste des curiosités. Ils sont utilisés par exemple pour construire les groupes d'homologie singulière et pour construire les produits tensoriels de modules arbitraires.