Compléments d'algèbre et de géométrie pour l'agrégation

Bernard Le Stum[1]
Université de Rennes 1

Version du 7 février 2003

[1]bernard.le-stum@univ-rennes1.fr

Table des matières

Table of contents ii

Introduction iii

1 Algèbre générale 1
- 1.1 Ensembles . . . 2
- 1.2 Fonctions . . . 3
- 1.3 Relation dans un ensemble . . . 5
- 1.4 Monoïdes . . . 8
- 1.5 Groupes . . . 9
- 1.6 Action de groupe . . . 11
- 1.7 Commutativité . . . 14

2 Algèbre commutative 17
- 2.1 Anneaux et modules . . . 17
- 2.2 Sous-modules et quotients . . . 19
- 2.3 Produits et sommes . . . 22
- 2.4 Algèbres . . . 25
- 2.5 Polynômes, localisation . . . 27
- 2.6 Structure des anneaux commutatifs . . . 30
- 2.7 Anneaux noethériens et factoriels . . . 33
- 2.8 Anneaux principaux . . . 35
- 2.9 Extensions algébriques . . . 37
- 2.10 Corps de rupture et de décomposition . . . 38
- 2.11 Extensions galoisiennes . . . 39
- 2.12 Théorie de Galois . . . 41
- 2.13 Produit tensoriel . . . 42
- 2.14 Produits tensoriels. Le cas commutatif . . . 45
- 2.15 Algèbres tensorielles et symétriques . . . 48
- 2.16 Déterminants . . . 50

3 Géométrie 53
- 3.1 Espaces affines et applications affines . . . 54
- 3.2 Sous-espaces affines . . . 56
- 3.3 Théorèmes de Thales, Desargues et Pappus . . . 58
- 3.4 L'enveloppe vectorielle . . . 60

3.5 Repères affines 62
3.6 Caractérisation des applications affines 63
3.7 Géométrie affine sur un corps ordonné 65
3.8 Espaces projectifs et sous-espaces 66
3.9 Applications projectives 68
3.10 Repères projectifs 70
3.11 Espaces affines et projectifs 71
3.12 Théorèmes de Desargues et Pappus 73
3.13 Caractérisation des applications projectives 75

4 Le langage des catégories **77**
4.1 Définition et exemples 77
4.2 Structure interne 80
4.3 Propriétés universelles 81
4.4 Foncteurs 86
4.5 Transformations naturelles 90
4.6 Foncteurs représentables 92
4.7 Diagrammes et limites 94
4.8 Foncteurs Exacts 98
4.9 Foncteurs adjoints 100
4.10 Catégories additives 103
4.11 Catégories abéliennes 105

Bibliography **109**

Index **109**

Introduction

Le but avoué de ce cours est de vous rendre plus performant en algèbre et en géométrie dans les épreuves écrites et orales de l'agrégation. Il ne s'agit pas cependant d'établir une liste de recettes plus ou moins inspirées des concours des années précédentes. Il ne s'agit pas non plus de refaire des cours que vous avez plus ou moins déjà suivi.
Ce cours se situe donc en complément à la préparation classique à l'agrégation. Nous allons nous attacher à dégager les principes qui gèrent les notions fondamentales en algèbre (commutative) et en géométrie (linéaire). Notre but est de mieux comprendre les structures fondamentales, sans chercher à développer des applications pointues. Bien sûr, cette approche s'applique aussi à d'autres domaines des mathématiques, ce que nous illustrerons dans la dernière partie avec des applications à la topologie par exemple.

Comme nous n'aurons pas le temps de voir cette dernière partie, le reste de cette introduction lui sera consacrée. On étudie en mathématiques des *objets*, qui sont principalement des ensembles munis d'une structure supplémentaire, et des *morphismes* qui sont en général, des applications qui préservent ces structures. Par exemple, on peut regarder les ensembles, les groupes, les espaces topologiques, les espaces de Banach, etc. On dégage ainsi la notion de *catégorie*.
Dans chaque catégorie, on retrouve des notions analogues comme celle d'isomorphisme, de produit, etc. On peut donc fédérer toutes ces notions grâce à notre nouveau formalisme. Dans toute catégorie, on a une notion de dualité. Par exemple, la surjectivité est la notion duale de l'injectivité. Moins évident, le produit tensoriel d'anneaux commutatifs est la notion duale du produit d'anneaux. Moralement, cela permet de diviser par deux la quantité de notions à étudier.
Une fois que l'on maîtrise la notion de catégorie, on peut s'intéresser aux constructions qui permettent d'associer à un objet (ou un morphisme) d'une catégorie, un objet (ou un morphisme) d'une autre catégorie. A un anneau, on associe le groupe des inversibles, à un groupe, on associe son abélianisé, à un espace métrique, on associe son complété, etc. On dégage ainsi la notion de *foncteur*.
Connaître quelques propriétés d'un foncteur permet d'obtenir de nombreux résultats. Je ne donnerai pas d'exemples ici car cela nous emmènerait trop loin. Ce formalisme nous permet aussi de donner un sens précis à des notions parfois floues comme celle de propriété universelle, de construction naturelle ou même de diagramme commutatif.
A ce point de l'introduction, le lecteur peut être amené à penser qu'avec ce cours, il va à acquérir de nouvelles connaissances dont il ne voit pas l'usage à court terme, ni même peut être à long terme. Il faut vraiment avoir à l'esprit qu'un formalisme élaboré permet rarement d'obtenir des résultats pointus. Mais il permet de faire la

part des choses entre ce qui est formel et ce qui demande un réel travail. Et donc de se consacrer à l'essentiel.
Ce cours ne contient que les définitions et les résultats (plus quelques remarques, exemples et exercices). Je n'ai pas encore rédigé les démonstrations.

Chapitre 1

Algèbre générale

1.1 Ensembles

1.1.1 Définition

On admet les notions d'*ensemble* E et d'*élément* x de cet ensemble comme intuitives.
On écrit $x \in E$ et on dit que x *appartient*à E.
Deux ensembles sont *égaux* s'ils ont les mêmes éléments.
On note $\{a, b, \ldots\}$ l'ensemble dont les éléments sont a, b, ...(ensemble défini en *extension*) et $\{x/P(x)\}$ l'ensemble des x qui possèdent la propriété P (ensemble défini en *compréhension*).
On utilisera aussi librement les *quantificateurs existentiel*$\exists$ et *universel*$\forall$ ainsi que les connecteurs logiques de *conjonction* "et", de *disjonction*"ou", d'*implication* $\Rightarrow$ et d'*équivalence* $\Leftrightarrow$.

1.1.2 Définition

On note $\emptyset$ l'*ensemble vide* qui ne contient aucun élément.
Un ensemble à un élément est un *singleton*.
Un ensemble à deux éléments (distincts) est une *paire*.

1.1.3 Définition

On dit que E est *contenu*, est une *partie*, est un *sous ensemble* ou est *inclus* dans F et on écrit $E \subset F$ si tout élément de E est élément de F.
Si x n'appartient pas à E, on écrit $x \notin E$.

1.1.4 Définition

L'*intersection*d'une "famille" (non vide) $\{E_i\}_{i \in I}$ d'ensembles est l'ensemble

$$\cap E_i := \{x/\forall i \in I, x \in E_i\}.$$

L'*union* de ces ensembles est

$$\cup E_i := \{x/\exists i \in I, x \in E_i\}.$$

On dit que deux ensembles E et F sont *disjoints* si $E \cap F = \emptyset$.

1.1.5 Définition

Une *partition* de E est un ensemble de parties non vides de E, disjointes deux à deux et dont l'union est E.

1.1.6 Définition

On admettra l'existence du *produit* $\prod E_i$ d'une "famille" $\{E_i\}_{i\in I}$ d'ensembles : se donner un élément x de $\prod E_i$ revient à se donner, pour chaque $i \in I$, un élément x_i de de E_i. On écrira $x = (x_i)_{i\in I}$.
On dit *couple* , *triplet*, etc. pour un élément d'un produit double, triple, etc. Par convention, le produit vide est le singleton $\{\emptyset\}$.
On admettra aussi l'existence de l' *union disjointe* $\coprod E_i$ de la "famille" $\{E_i\}_{i\in I}$: se donner un élément de $\coprod E_i$ revient à se donner un $i \in I$ et un élément de E_i.

1.2 Fonctions

1.2.1 Définition

Une *relation* ou *correspondance* $\mathcal{R} : E \to F$ est la donnée de deux ensembles E, F et d'un sous ensemble Γ de $E \times F$.
On dit que E est la *source*, F le *but* et Γ le *graphe*.
Si $(x, y) \in \Gamma$, on écrit $y\mathcal{R}x$. On dit que y est une *image*de x et que x est un *antécédent*de y.
Si $F = E$, on dit que $\mathcal{R}$ est une relation dans E.
Le *domaine de définition* est l'ensemble $\mathcal{D}_\mathcal{R}$ de tous les antécédents.
L'*image* de $\mathcal{R}$ est l'ensemble $\operatorname{Im}\mathcal{R}$ de toutes les images.

1.2.2 Définition

L'*identité*dans E est la relation $y\ Id_E\ x$ si et seulement si $x = y$.
On peut aussi considérer la *relation vide* $\emptyset : E \to F$ dont le graphe est vide.

1.2.3 Définition

Soient $\mathcal{R} : E \to F$ une relation de graphe Γ, $E' \subset E, F' \subset F$, et $\mathcal{R}' : E' \to F'$ une relation de graphe Γ'.
On dit que $\mathcal{R}$ est un *prolongement*de $\mathcal{R}'$ si $\Gamma' \subset \Gamma$.
On dit aussi que $\mathcal{R}'$ est une *restriction*de $\mathcal{R}$.
Lorsque $\Gamma' = \Gamma \cap (E' \times F')$ on dit que $\mathcal{R}'$ est la *relation induite* par $\mathcal{R}$, ou la *restriction* de $\mathcal{R}$.

1.2.4 Définition

La relation *réciproque* de $\mathcal{R}$ est la relation $\mathcal{R}^{-1}$ de F vers E définie par $x\mathcal{R}^{-1}y$ si et seulement si $y\mathcal{R}x$.
Si $\mathcal{R}$ est une relation de E vers F et $\mathcal{S}$ une relation de F vers G, la relation *composée* $\mathcal{S} \circ \mathcal{R}$ est définie par

$$z(\mathcal{S} \circ \mathcal{R})x \Leftrightarrow \exists y \in F, y\mathcal{R}x \text{ et } z\mathcal{S}y.$$

1.2.5 Proposition

i) On a toujours $(\mathcal{R}^{-1})^{-1} = \mathcal{R}$. De plus, $\operatorname{Im} \mathcal{R}^{-1} = \mathcal{D}_{\mathcal{R}}$ et réciproquement.

ii) On a toujours $(\mathcal{T} \circ \mathcal{S}) \circ \mathcal{R} = \mathcal{T} \circ (\mathcal{S} \circ \mathcal{R})$.

1.2.6 Définition

L'*image* par une relation $\mathcal{R} : E \to F$ d'une partie A de E est

$$\mathcal{R}(A) := \{y \in F / \exists x \in A, y\mathcal{R}x\}.$$

L'*image réciproque*d'une partie B de F est $\mathcal{R}^{-1}(B)$.

1.2.7 Définition

Une *fonction* $f : E \to F$ est une relation telle que tout $x \in E$ ait au plus une image y dans F. On écrit alors $y = f(x)$.
La fonction f est une *application*si $\mathcal{D}_f = E$ (si tout élément de E à une image dans F).
Une application $f : E \to F$ est *injective*si deux éléments distincts de E n'ont jamais la même image dans F.
Elle est *surjective* si tout élément de F à un antécédent dans E (si $\operatorname{Im} f = F$).
Elle est *bijective* si elle est à la fois injective et surjective.
Attention : certains auteurs considèrent fonction et application comme synonymes.

1.2.8 Proposition

i) Si f et g sont deux fonctions, deux applications, deux applications injectives, deux applications surjectives ou deux applications bijectives, alors $g \circ f$ aussi.

ii) Si f et g sont deux applications et $g \circ f$ injective (resp. surjective) alors f est injective (resp. g est surjective).

iii) Une application $f : E \to F$ est bijective si et seulement s'il existe une application $g : F \to E$ telle que $g \circ f = Id_E$ et $f \circ g = Id_F$. On a alors $g = f^{-1}$.

1.2.9 Proposition

i) Si on note F^E l'ensemble des applications de E dans F, on a une bijection

$$G^{E\times F}\xrightarrow{\sim}(G^F)^E$$

$$f\mapsto(x\mapsto(y\mapsto f(x,y)),$$

la réciproque étant donnée par

$$g\to((x,y)\mapsto g(x)(y)).$$

ii) On a une bijection canonique

$$(\prod E_i)^F\simeq\prod E_i^F.$$

iii) On a une bijection canonique

$$F^{\coprod E_i}\simeq\prod F^{E_i},$$

et en particulier,

$$F^E\simeq\prod_{e\in E}F.$$

1.2.10 Proposition et définition

La définition du *cardinal*d'un ensemble est délicate. En fait, on dit que $|E|=|F|$ s'il existe une bijection entre E et F.
On écrit $0:=|\emptyset|$ et $1:=|\{0\}|$.
On vérifie que les définitions

$$\prod|E_i|=|\prod E_i|$$

et

$$\sum|E_i|=|\coprod E_i|$$

ou encore

$$|F|^{|E|}=|F^E|$$

ont bien un sens.
On écrit aussi $|E|\leq|F|$ s'il existe une injection $E\hookrightarrow F$ (ou, ce qui est équivalent si $E\neq\emptyset$, une surjection $F\twoheadrightarrow E$).
On peut considérer l'ensemble $\mathbf{N}$ des cardinaux finis appelés aussi *entiers naturels*.
On retrouve alors les notions et résultats bien connus.

1.2.11 Proposition (Schroeder-Bernstein)

On a $|E|=|F|$ si et seulement si $|E|\leq|F|$ et $|F|\leq|E|$.

1.3 Relation dans un ensemble

1.3.1 Définition

Une relation dans un ensemble E est *réflexive*si $\forall x \in E, x\mathcal{R}x$.
Elle est *symétrique*si $\forall x, y \in E, x\mathcal{R}y \Rightarrow y\mathcal{R}x$.
Elle est *antisymétrique*si

$$\forall x, y \in E, (y\mathcal{R}x \text{ et } x\mathcal{R}y) \Rightarrow y = x.$$

Elle est *transitive* si

$$\forall x, y, z \in E, (z\mathcal{R}y \text{ et } y\mathcal{R}x) \Rightarrow z\mathcal{R}x.$$

1.3.2 Définition

Une relation d'*équivalence* dans un ensemble est une relation réflexive, symétrique et transitive.
Une relation d'*ordre* est une relation réflexive, antisymétrique et transitive.
Une relation de *préordre* est une relation réflexive et transitive.
On note en général $\sim$ une relation d'équivalence, $\leq$ une relation d'ordre et $\geq$ son inverse.

1.3.3 Proposition

i) Toutes ces propriétés (réflexivité, symétrie, antisymétrie, transitivité, équivalence, ordre, préordre) sont respectées par restriction à une partie F de E.

ii) Si $\mathcal{R}$ satisfait une ce ces propriétés, il en va de même de $\mathcal{R}^{-1}$. En fait, une relation symétrique est égale à son inverse.

1.3.4 Définition

Une application $f : (E, \mathcal{R}) \to (F, \mathcal{S})$ entre ensembles munis de relations est *compatible*aux relations si $x\mathcal{R}y \Rightarrow f(x)\mathcal{S}f(y)$.
Dans le cas ou $\mathcal{R}$ et $\mathcal{S}$ sont des relations d'ordre, on dit que f est *croissante*.
Dans le cas ou $\mathcal{S}$ n'est pas précisée, il s'agit de la relation d'égalité.

1.3.5 Définition

Si $\sim$ est une relation d'équivalence dans E, la *classe*de $x \in E$ est l'ensemble

$$\bar{x} = \{y \in E, y \sim x\}.$$

On note $E/\sim$, et on appelle *ensemble quotient*de E par $\sim$, l'ensemble des classes d'équivalence de $\sim$.

On dit que l'application

$$p : E \twoheadrightarrow E/\sim, x \mapsto \bar{x}$$

est la *projection*.

1.3.6 Proposition

i) Si $\sim$ est une relation d'équivalence dans E, l'ensemble quotient $E/\sim$ est une partition de E. Et toute partition correspond ainsi à une unique relation d'équivalence.

ii) Si une application $f : E \to F$ est compatible à une relation d'équivalence $\sim$ sur E, il existe une unique application $\bar{f} : E/\sim \to F$ telle que $f = \bar{f} \circ p$.

1.3.7 Définition

Soit $\leq$ une relation d'ordre sur un ensemble I.
Un *majorant* pour une partie $J \subset I$ est un $x \in I$ tel que $\forall y \in J, y \leq x$.
Un *plus grand élément* dans I est un majorant pour I.
Un élément *maximal* dans I est un $x \in I$ tel que $\forall y \in I, x \leq y \Rightarrow x = y$.
On définit un *minorant*, un *plus petit élément*et un *élément minimal*en considérant la relation inverse $\geq$.
Une *borne supérieure* (resp. *inférieure*) pour une partie $J \subset I$ est un plus petit majorant (resp. grand minorant).

1.3.8 Remarque

La relation d'inclusion sur un ensemble de parties d'un ensemble est une relation d'ordre. On a donc en particulier, une relation d'ordre sur les relations dans un ensemble E qui est donnée par le prolongement.

1.3.9 Proposition

Si $\mathcal{R}$ est une relation de préordre sur E, la relation

$$x \sim y \Leftrightarrow x\mathcal{R}y \text{ et } y\mathcal{R}x$$

est une relation d'équivalence. De plus, la relation

$$\bar{x} \leq \bar{y} \Leftrightarrow x\mathcal{R}y$$

sur $E/\sim$ est bien définie et c'est une relation d'ordre sur $E/\sim$.

1.3.10 Définition

Une relation d'ordre $\leq$ sur un ensemble I est *totale*si on a toujours $x \leq y$ ou $y \leq x$. Sinon, on parle parfois d'*ordre partiel*.
Un ensemble ordonné est *inductif*si toute partie non-vide totalement ordonnée a un majorant.

1.3.11 Théorème (Lemme de Zorn)

Tout ensemble ordonné inductif non vide possède un élément maximal.

1.3.12 Remarque

La démonstration (difficile) du lemme de Zorn nécessite l'axiome du choix. En fait, cet axiome est équivalent au lemme de Zorn. Il dit que si un produit est vide, l'un des facteurs est vide, ou encore qu'un produit d'ensembles non-vide est non-vide. Cet axiome est aussi équivalent au théorème de Tychonoff qui dit qu'un produit de compacts est compact.
Le prochain résultat nécessite aussi l'axiome du choix.

1.3.13 Proposition

Soit $(I, \leq)$ un ensemble ordonné. Alors, les conditions suivantes sont équivalentes :

a) Toute suite croissante dans I est stationnaire

b) Toute partie non-vide de I possède un élément maximal.

1.4 Monoïdes

1.4.1 Définition

Une *loi de composition* est une application $E \times F \to G, (x, y) \longmapsto xy$ (ou plus généralement, $x * y$).
Si $E = F = G$, on dit que c'est une *loi de composition interne* dans, ou sur E.
La loi $F \times E \to G, (y, x) \longmapsto xy$ est la loi *opposée*.

1.4.2 Définition

Une loi de composition interne sur un ensemble G est *associative* si pour tout $x, y, z \in G$, on a $(xy)z = x(yz) =: xyz$.
On dit que $1 \in G$ est une *unité*(ou plus généralement un *élément neutre*) si pour tout $x \in G$, on a $1x = x1 = x$.
On parle d' *élément nul* noté 0, au lieu l'unité lorsque la loi est notée additivement.

1.4.3 Définition

Un *monoïde* est un ensemble muni d'une loi de composition interne associative et unitaire.
Un *homomorphisme* $f : G \to H$, entre deux monoïdes, est une application telle que

$$f(1) = 1 \text{ et } \forall x, y \in G, f(xy) = f(x)f(y).$$

C'est un *isomorphisme*s'il existe un autre homomorphisme $g : H \to G$ tel que $g \circ f = \mathrm{Id}_G$ et $f \circ g = \mathrm{Id}_H$.

On dit *endomorphisme*et *automorphisme*lorsque $G = H$.

1.4.4 Proposition

i) Si $f : G \to H$ et $g : H \to K$ sont deux homomorphismes, il en va de même de $g \circ f$.

ii) Un homomorphisme $f : G \to H$ est un isomorphisme si et seulement il est bijectif et f^{-1} est alors aussi un homomorphisme.

1.4.5 Définition

Un monoïde H est un *sous-monoïde*d'un monoïde G si $H \subset G$ et si l'inclusion $H \hookrightarrow G$ est un morphisme de monoïdes.
Le *noyau*d'un homomorphisme de monoïdes $f : G \to H$ est $\ker f := f^{-1}(1)$.
Le *centre* d'un monoïde G est $Z(G) := \{g \in G, \forall h \in G, gh = hg\}$.

1.4.6 Proposition

L'image et l'image inverse d'un sous-monoïde par un homomorphisme de monoïdes sont des sous-monoïdes. En particulier, le noyau et l'image sont des sous-monoïdes. Le centre est aussi un sous-monoïde.

1.4.7 Proposition

i) Toute intersection de sous monoïdes est un sous monoïde.

ii) Il existe un plus petit sous monoïde H contenant une partie donnée S d'un monoïde G : c'est l'intersection de tous les sous-monoïdes de G contenant S. C'est aussi l'ensemble des produits d'éléments de S.

1.4.8 Définition

On dit alors que H est le *sous-monoïde engendré* par S ou que S est un *ensemble de générateurs*de H.

1.4.9 Proposition

i) Si G est un monoïde, la loi opposée fait de l'ensemble G un nouveau monoïde noté G^{op}.

ii) Si les $G_i, i \in I$ sont des monoïdes, $\prod_{i\in I} G_i$ est un monoïde pour $(g_i)(h_i) = (g_i h_i)$.

iii) Si G est un monoïde et E un ensemble, l'ensemble G^E est un monoïde pour $(fg)(x) = f(x)g(x)$.

iv) Si E est un ensemble, alors E^E est un monoïde pour $\circ$.

v) Si G est un monoïde, alors l'ensemble $\mathrm{End}(G)$ des endomorphismes de G est un sous-monoïde de G^G pour $\circ$.

vi) L'ensemble $\mathbf{N}$ est un monoïde pour l'addition et si G est un monoïde et $g \in G$, il existe un unique morphisme $\mathbf{N} \to G$ tel que $1 \mapsto g$. On note g^n l'image de n (ou ng si la loi de G est notée additivement).

1.5 Groupes

1.5.1 Définition

Soit G un monoïde.
On dit que $x' \in G$ est un *inverse à droite (resp. à gauche)*pour $x \in G$ si $xx' = 1$ (resp. $x'x = 1$).
On dit *inverse* si c'est un inverse à droite et à gauche.

1.5.2 Remarque

Si x possède un inverse à droite et un inverse à gauche, il possède un inverse et celui-ci est unique. On le note x^{-1}.
Lorsque la loi est notée additivement on parle d'*opposé* $-x$ de x.

1.5.3 Proposition

i) Si x est inversible, alors x^{-1} aussi et $(x^{-1})^{-1} = x$.
ii) Si $x, y \in G$ possèdent des inverses, alors xy aussi et $(xy)^{-1} = y^{-1}x^{-1}$.

1.5.4 Définition

Un *groupe* est un monoïde G dans lequel tout élément possède un inverse.
Un *homomorphisme de groupes* $f : G \to H$ est un morphisme de monoïdes entre deux groupes.
Enfin, un *sous-groupe*est un sous-monoïde d'un groupe qui est un groupe.

1.5.5 Proposition

i) L'image et l'image inverse d'un sous-groupe par un morphisme de groupes sont des sous-groupes. En particulier, le noyau et l'image sont des sous-groupes. Le centre d'un groupe est est aussi un groupe.
ii) Un homomorphisme de groupes est injectif si et seulement si son noyau est réduit à 1.

1.5.6 Proposition

i) Toute intersection de sous-groupes est un sous-groupe.
ii) Il existe un plus petit sous groupe H contenant une partie donnée S d'un groupe G : c'est l'intersection de tous les sous-groupes de G contenant S. C'est aussi l'ensemble des produits d'éléments de S et d'inverses d'éléments de S.

1.5.7 Définition

On dit alors que H est le *sous-groupe engendré*par S ou que S est un *ensemble de générateurs* de H.

1.5.8 Proposition

i) Si G est un groupe, il en va de même de G^{op}.

ii) Si les $G_i, i \in I$ sont des groupes, $\prod_{i\in I} G_i$ aussi.

iii) Si G est un groupe et E un ensemble, alors G^E est un groupe.

iv) Si G est un monoïde, alors l'ensemble G^* des inversibles de G est un sous-monoïde qui est un groupe.

v) Si E est un ensemble, l'ensemble $\mathcal{S}(E)$ des bijections de E sur E est un groupe.

vi) Si G est un monoïde, l'ensemble $\mathrm{Aut}(G)$ des automorphismes de G est un groupe.

vii) Si G est un groupe, tout morphisme de monoïdes $G \to H$ est à valeurs dans H^*.

1.5.9 Définition

Le groupe $S_n := S(\{1, \ldots, n\})$ est le *groupe symétrique*.

1.5.10 Proposition

Si $n > 1$, il existe un unique homomorphisme de groupes non trivial $\epsilon : S_n \to \{\pm 1\}$.

1.5.11 Définition

Si $\sigma \in S_n$, on dit que $\epsilon(\sigma)$ est la *signature*de σ.
On dit aussi que $\mathcal{A}_n := \ker \epsilon$ est le *groupe alterné*.

1.6 Action de groupe

1.6.1 Définition

Si G est un monoïde, un *G-ensemble(à gauche)* est un ensemble E muni d'un morphisme de monoïdes $G \to E^E, g \mapsto (x \mapsto gx)$.
Un *G-ensemble à droite*est un G^{op}-ensemble à gauche.

1.6.2 Remarque

Avec un vocabulaire plus classique, se donner une structure de G-ensemble sur un ensemble E revient à se donner une *action (à gauche)* de G, c'est à dire, une loi de composition externe $G \times E \to E, (g, x) \longmapsto gx$ telle que

a) pour tout $x \in E, 1x = x$

b) pour tous $g, h \in G$ et $x \in E, (gh)x = g(hx)$.

1.6.3 Proposition

Si G est un groupe et E un G-ensemble, alors la relation $x \sim y$ si et seulement si $\exists g \in G, y = gx$ est une relation d'équivalence sur E.

1.6.4 Définition

Soit G un groupe et E un G-ensemble.
L'ensemble quotient se note $G\backslash E$ (ou E/G pour une action à droite) et la classe de x est l'*orbite* de x.
On dit que l'action de G sur E est *transitive* s'il y a au plus une orbite.
On dit que l'action est *fidèle* si l'application $G \to \mathcal{S}(E)$ est injective.
Si $x \in E$ on dit que $G_x := \{g \in G, gx = x\}$ est le *stabilisateur* de x.
On dit que l'action de G sur E est *simple* ou *libre* si tous les stabilisateurs sont triviaux.

1.6.5 Proposition (Théorème de Lagrange)

Si le groupe G agit librement sur E, alors $E \simeq G \times G\backslash E$.

1.6.6 Proposition

Soit H un sous-monoïde d'un monoïde G. Alors,

i) H agit sur G par translation à gauche $(h, g) \mapsto hg$ et à droite $(h, g) \mapsto gh$. Si H est un groupe, on note $H\backslash G$ et G/H les ensembles quotients.

ii) Si G aussi est un groupe, alors les actions sont libres. En particulier,

$$|G| = |H||H\backslash G| = |H||G/H|.$$

1.6.7 Définition

On dit qu'un sous-monoïde H d'un monoïde G est *distingué*dans G si H est un groupe et $H\backslash G = G/H$.

1.6.8 Proposition

Un sous-monoïde H est distingué dans G si et seulement si c'est un groupe et s'il existe une structure de monoïde sur G/H qui fasse de la projection $G \twoheadrightarrow G/H$ un homomorphisme de monoïdes. Celle-ci est alors unique. De plus, si G est un groupe, G/H aussi.

1.6.9 Proposition

Si un groupe G agit sur un ensemble E, alors le stabilisateur G_x de $x \in E$ st un sous-groupe de G et l'application $G \to E, g \to gx$ induit une bijection $G/G_x \simeq Gx$.

1.6.10 Définition

Une suite d'homomorphismes de monoïdes

$$\cdots \longrightarrow G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \longrightarrow \cdots$$

est *exacte* si $\operatorname{Im} f_{i-1} = \ker f_i$.
Une suite exacte de la forme

$$1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$$

est une *suite exacte courte* . On dit aussi que G est une *extension extension de monoïdes* de H par N. On dit que cette extension est *scindée* si $\pi : G \to H$ possède un inverse à gauche, encore appelé section, c'est à dire un homomorphisme $\sigma : H \to G$ tel que $\pi \circ \sigma = Id_H$.

1.6.11 Proposition

i) La suite $G \xrightarrow{\pi} H \longrightarrow 1$ est exacte si et seulement si π est surjectif. Lorsque G est un groupe, alors H est aussi un groupe, $\ker \pi$ est un sous-groupe distingué de G, et la suite

$$1 \longrightarrow \ker \pi \longrightarrow G \longrightarrow H \longrightarrow 1$$

est exacte.

ii) Lorsque N est un groupe, la suite $1 \longrightarrow N \longrightarrow G$ est exacte si et seulement si le morphisme est injectif. Lorsque N est un sous-monoïde distingué de G, la suite

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1$$

est une suite exacte courte.

iii) Si N et H sont deux monoïdes, la suite évidente

$$1 \longrightarrow N \longrightarrow N \times H \longrightarrow H \longrightarrow 1$$

est exacte (produit direct).

1.6.12 Définition

Un monoïde H *agit par endomorphismes à gauche* sur un autre monoïde N si l'action est donnée par un morphisme

$$H \to \operatorname{End}(N), h \mapsto (n \mapsto {}^h n).$$

En d'autres termes, on doit toujours avoir

$$^1n = n, ^{(gh)}n = {}^g({}^hn), {}^h1 = 1, {}^h(mn) = {}^hm{}^hn$$

On dit alors que l'ensemble $N \times H$ muni de la loi

$$(n, h)(n', h') = (n{}^hn', hh')$$

est un *produit semi-direct* de N par H (via cette action) et on le note $N \rtimes H$.

1.6.13 Proposition

Si un monoïde H agit par endomorphismes à gauche sur un monoïde N, alors $N \rtimes H$ est un monoïde et la suite

$$1 \longrightarrow N \longrightarrow N \rtimes H \longrightarrow H \longrightarrow 1$$

est exacte et scindée. Si N et H sont des groupes, il en va de même de $N \rtimes H$.
Réciproquement, soit

$$1 \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} H \longrightarrow 1$$

une suite exacte de groupes et σ une section de π. Alors, pour tout $h \in H$ et $n \in N$, il existe un unique ${}^hn \in N$ tel que

$$\iota({}^hn) = \sigma(h)\iota(n)\sigma(h)^{-1}.$$

On obtient ainsi une action par endomorphismes de H sur N et on a un isomorphisme

$$\varphi : N \rtimes H \simeq G, (n, h) \to i(n)\sigma(h).$$

1.6.14 Remarque

On dit parfois que G est "produit semi-direct"' de N et H.

1.7 Commutativité

1.7.1 Définition

Une loi de composition interne sur un ensemble E est *commutative* si pour $x, y \in E$, on a $xy = yx$.
Un groupe dont la loi est commutative est un *groupe abélien*. La loi est généralement notée additivement.

1.7.2 Définition

Soit M un monoïde commutatif.
Si y est inversible on définit le *quotient* $x/y := xy^{-1}$.
Lorsque la loi est notée additivement, on parle de la *différence* $x - y$.

1.7.3 Proposition

i) Tout sous-groupe d'un groupe abélien est abélien et distingué.

ii) Si les $M_i, i \in I$ sont des groupes abéliens, alors $\prod_{i\in I} M_i$ aussi. En particulier, si M est un groupe abélien et E un ensemble, alors M^E est abélien.

iii) Si M et N sont deux groupes abéliens, l'ensemble

$$\mathrm{Hom}(M, N)$$

des homomorphismes de groupes de M dans N est un sous-groupe commutatif de N^M.

1.7.4 Proposition

Si E est un ensemble, alors,

i) Les familles nulles presque partout de $\mathbf{N}^E$ forment un sous monoïde noté $\mathbf{N}^{(E)}$. On identifie $e \in E$ avec la famille nulle sauf en e ou elle vaut 1.

ii) Tout élément de $N^{(E)}$ s'écrit de manière unique comme somme finie $\sum_{e\in E} n_e e$ avec $n_e \in \mathbf{N}$.

iii) Si M est un monoïde commutatif, toute application $E \to M$ se prolonge de manière unique en un homomorphisme $\mathbf{N}^{(E)} \to M$.

1.7.5 Définition

On dit que $\mathbf{N}^{(E)}$ est le *monoïde commutatif libre* sur E.
Un *monoïde commutatif libre* est un monoïde isomorphe à un monoïde de la forme $\mathbf{N}^{(E)}$.

1.7.6 Définition

Un monoïde commutatif (multiplicatif) est *intègre* si $ab = ac \Rightarrow b = c$.

1.7.7 Proposition

Soit G un monoïde commutatif (multiplicatif), alors

i) la relation de divisibilité : $a|b \Leftrightarrow \exists c \in G, b = ac$ est une relation de préordre.

ii) Tout homomorphisme de monoïdes est compatible avec les relations de divisibilité.

iii) Si G est intègre, la relation de divisibilité sur G/G^* est une relation d'ordre.

1.7.8 Exemple

Sur $\mathbf{N}$ muni de l'addition, on retrouve la relation d'ordre habituelle $\leq$ et sur $\mathbf{N}$ muni de la multiplication, on trouve la relation de divisibilité.

1.7.9 Proposition

i) Si M est un monoïde commutatif, l'ensemble $M^{gr} := (M \times M)/\sim$ ou $(a,b) \sim (a',b')$ si et seulement si $\exists c \in M, cab' = ca'b$ est un groupe pour la multiplication (qui est bien définie). On écrit $\mathbf{Z} := \mathbf{N}^{gr}$.

L'application $M \to M^{gr}, a \to (a,1)$ est un homomorphisme de monoïdes. Elle est injective lorsque M est intègre.

ii) Si G est un groupe et si $g \in G$, il existe un unique homomorphisme de groupes $\mathbf{Z} \to G$ tel que $1 \mapsto g$. On note g^n l'image de n.

Chapitre 2

Algèbre commutative

2.1 Anneaux et modules

2.1.1 Définition

Un *anneau (unitaire)* est un ensemble muni d'une loi de groupe abélien (notée additivement) et d'une loi de monoïde notée multiplicativement qui est *distributive* sur la première, c'est à dire telle que la multiplication à gauche comme à droite soit une action par endomorphisme du monoïde multiplicatif sur le groupe additif.
Un *homomorphisme (unitaire)* d'anneaux

$$f : A \to B$$

est un homomorphisme pour les deux lois. C'est un *isomorphisme* s'il existe un autre homomorphisme d'anneaux $g : B \to A$ tel que $g \circ f = \mathrm{Id}_A$ et $f \circ g = \mathrm{Id}_B$.
Enfin, on dit que A est *commutatif* si la multiplication est commutative.

2.1.2 Remarque

Bien sur, la distributivité signifie que :

$$\forall a, b, c \in A, \begin{cases} a(b+c) = ab + ac \\ (a+b)c = ac + bc \end{cases} .$$

2.1.3 Exemples

L'anneau des entiers $\mathbf{Z}$ et l'anneau nul. Si A est un anneau, il existe un unique homomorphisme d'anneaux $\mathbf{Z} \to A$ (resp. $A \to 0$).
Si M est un groupe abélien, la composition fait de

$$\mathrm{End}(M) := \mathrm{Hom}(M, M)$$

un anneau (non-commutatif en général).

2.1.4 Proposition

Le composé de deux homomorphismes d'anneaux est encore un homomorphisme.
Un homomorphisme d'anneaux est bijectif si et seulement si c'est un isomorphisme.

2.1.5 Définition

Un anneau B est un *sous-anneau* d'un anneau A si c'est un sous-groupe pour l'addition et un sous-monoïde pour la multiplication. Autrement dit, c'est un anneau contenu dans A et l'inclusion est un homomorphisme d'anneaux.

2.1.6 Définition

Un *module (à gauche)* M sur un anneau A, ou *A-module (à gauche)* est un groupe abélien muni d'un homomorphisme d'anneaux $A \to \mathrm{End}(M)$ que l'on note $a \mapsto (m \mapsto am)$.
Un *A-module à droite* est un module (à gauche) sur A^{op}.
Un homomorphisme de groupes $f : M \to N$ entre deux A-modules, est un *homomorphisme de A-modules* si le diagramme

$$\begin{array}{ccc} A & \to & \mathrm{End}(M) \\ \downarrow & & \downarrow \\ \mathrm{End}(N) & \to & Hom(M,N) \end{array},$$

ou les secondes flèches sont les homomorphismes obtenus par composition à droite et à gauche par f, est commutatif.
C'est un *isomorphisme* s'il existe un autre homomorphisme de A-modules $g : N \to M$ tel que $g \circ f = \mathrm{Id}_M$ et $f \circ g = \mathrm{Id}_N$.

2.1.7 Remarque

Avec un vocabulaire plus classique, se donner une structure de A-module (à gauche) sur un groupe abélien M revient à se donner une loi de composition externe

$$A \times M \to M, (a,m) \longmapsto am$$

telle que

a) $\forall a \in A, m, n \in E, a(m+n) = am + an.$

b) $\forall a, b \in A, m \in E, (a+b)m = am + bm.$

c) $\forall m \in M, 1m = m$

d) $\forall a, b \in A, m \in E, (ab)m = a(bm).$

De même, un homomorphisme de groupes $f : M \to N$ est un homomorphisme de A-modules (à gauche) si

$$\forall a \in A, m \in M, f(am) = af(m).$$

2.1.8 Exemples

Un anneau A est de manière évidente un module (à gauche et à droite) sur lui même. De même, 0 est toujours un A-module (à gauche et à droite).

2.1.9 Remarque

Si M est un groupe abélien, il existe un unique homomorphisme d'anneaux $\mathbf{Z} \to \mathrm{End}(M)$. On peut donc identifier groupes abéliens et $\mathbf{Z}$-modules.

2.1.10 Proposition

Le composé de deux homomorphismes de A-modules (à gauche) est encore un homomorphisme.
Un homomorphisme de A-modules est bijectif si et seulement si c'est un isomorphisme.

2.1.11 Remarque

Si $f : A \to B$ est un homomorphisme d'anneaux et M un B-module (à gauche), alors l'application composée

$$A \to B \to \mathrm{End}(M)$$

fait de M un A-module (à gauche). On dit que c'est la structure de A-module obtenue par *restriction des scalaires* .
Bien sûr, tout homomorphisme de B-modules est aussi un homomorphisme de A-modules.
En particulier, B peut être vu comme un A-module à gauche ou à droite et $A \to B$ est un homomorphisme de A-modules.

2.2 Sous-modules et quotients

Dans cette section, tous les modules considérés sont des modules à gauche. Tous les résultats ont bien sûr un analogue pour les modules à droite.

2.2.1 Définition

Un A-module N est un *sous-A-module* d'un A-module M s'il est contenu dans M et si l'application d'inclusion $N \hookrightarrow M$ est un homomorphisme de A-modules.
Un sous-module (à gauche) de A s'appelle un *idéal (à gauche)* de A. Si c'est aussi un idéal à droite, on dit *idéal bilatère* .

2.2.2 Exemple

L'ensemble des matrices de la forme

$$\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$$

est un idéal à gauche qui n'est pas bilatère.

2.2.3 Proposition

Soit $(M_i)_{i\in I}$ une famille de sous-modules de M. Alors, $\cap_{i\in I} M_i$ est un sous-module de M. De plus, le sous groupe $\sum_{i\in I} M_i$ de M engendré par $\cup_{i\in I} M_i$ est un sous-module. En fait,

$$\sum_{i\in I} M_i = \{\sum_{i\in I} m_i, m_i \in M_i \text{ presque tous nuls}\}.$$

2.2.4 Définition

Le plus petit sous-module de M contenant une partie S donnée est le *module engendré* par cette partie.
Si M est engendré par une partie finie, il est dit *de type fini* .
Si M est engendré par un unique élément, il est dit *monogène* .
Pour un idéal, on dit *principal* . On note parfois (S) l'idéal engendré par une partie S.

2.2.5 Proposition

Si N est un sous-module de M, il existe une unique structure de A-module sur M/N qui fasse de la projection $\pi : M \twoheadrightarrow M/N$ un homomorphisme de A-modules.
De plus si $f : M \to M'$ est un homomorphisme dont la restriction à N est nulle, il existe une unique application $\bar{f} : M/N \to M'$ tel que $\bar{f} \circ \pi = f$ et c'est un homomorphisme.

2.2.6 Proposition

Soit $f : M \to N$ un homomorphisme de A-modules. Alors,

i) Si M' est un sous-module de M, alors $f(M')$ est un sous-module de N.

ii) Si N' est un sous-module de N, alors $f^{-1}(N')$ est un sous-module de M.

iii) $\ker f$ est un sous-module de M, $\operatorname{Im} f$ est un sous-module de N et f induit un isomorphisme
$$M/\ker f \tilde{\to} \operatorname{Im} f.$$

iv) On a toujours $f^{-1}(f(M')) = M' + \ker f$ et $f(f^{-1}(N')) = N' \cap \operatorname{Im} f$.

v) f et f^{-1} induisent une bijection entre les sous modules de M contenant $\ker f$ et les sous-modules de $\operatorname{Im} f$.

2.2.7 Proposition

Si A est un anneau et si $\mathfrak{a}$ est un idéal bilatère de A, il existe une unique structure d'anneau sur $A/\mathfrak{a}$ qui fasse de la projection $A \twoheadrightarrow A/\mathfrak{a}$ un homomorphisme d'anneaux.
De plus si $f : A \to B$ est un homomorphisme d'anneaux dont la restriction à $\mathfrak{a}$ est nulle, alors $\bar{f} : A/\mathfrak{a} \to B$ est l'unique homomorphisme d'anneaux tel que $\bar{f} \circ \pi = f$.

2.2.8 Proposition

Si $f : A \to B$ est un homomorphisme d'anneaux, alors $\ker f$ est un idéal bilatère de A, $\operatorname{Im} f$ est un sous-anneau de B et f induit un isomorphisme d'anneaux $A/\ker f \tilde{\to} \operatorname{Im} f$. De plus, f et f^{-1} induisent une bijection entre les idéaux de A contenant $\ker f$ et les idéaux de $\operatorname{Im} f$.

2.2.9 Proposition

Si N est un sous-module de M et N' un sous-module de N, l'application d'inclusion $N \hookrightarrow M$ induit un homomorphisme injectif $N/N' \hookrightarrow M/N'$ qui permet d'identifier N/N' avec un sous-module de M/N'. L'application canonique $M \twoheadrightarrow M/N'$ induit alors un isomorphisme

$$M/N \tilde{\to} (M/N')/(N/N').$$

Si N et N' sont deux sous-modules de M, l'application d'inclusion $N \hookrightarrow N + N'$ induit un isomorphisme

$$N/(N \cap N') \tilde{\to} (N + N')/N'.$$

2.2.10 Proposition

Si $\mathfrak{b} \subset \mathfrak{a}$ sont des idéaux bilatères d'un anneau A, alors $\mathfrak{a}/\mathfrak{b}$ est un idéal bilatère de $A/\mathfrak{b}$ et l'isomorphisme

$$A/\mathfrak{a} \tilde{\to} (A/\mathfrak{b})/(\mathfrak{a}/\mathfrak{b})$$

est un isomorphisme d'anneaux.
Si $\mathfrak{a}$ est un idéal bilatère de A et B un sous-anneau de A, alors $B+\mathfrak{a}$ est un sous-anneau de A, $\mathfrak{a}$ est un idéal bilatère de $B + \mathfrak{a}$ et l'isomorphisme

$$B/(B \cap \mathfrak{a}) \simeq (B + \mathfrak{a})/\mathfrak{a}$$

est un isomorphisme d'anneaux.

2.2.11 Remarque

Si M et N sont deux A-modules à gauche, on note $\operatorname{Hom}_A(M, N)$ l'ensemble des homomorphismes de A-modules de M dans N.
On voit aisément que $\operatorname{Hom}_A(M, N)$ est un sous-groupe de $\operatorname{Hom}(M, N)$.
De plus, si M est un A-module, alors

$$\operatorname{End}_A(M) := \operatorname{Hom}_A(M, M)$$

est un sous-anneau de $\operatorname{End}(M)$.
Remarquons aussi que l'on a toujours

$$\operatorname{Hom}_A(A, M) \simeq M, f \mapsto f(1).$$

Enfin, étant donné $f : M \to M'$, on obtient un homomorphisme

$$f^* : \mathrm{Hom}_A(M', N) \to \mathrm{Hom}_A(M, N), g \mapsto g \circ f.$$

De même, étant donné $g : N \to N'$, on obtient un homomorphisme

$$g_* : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, N'), f \mapsto g \circ f.$$

2.2.12 Proposition

Une suite $0 \to N' \to N \to N''$ est exacte si et seulement si, pour tout M, la suite

$$0 \to \mathrm{Hom}_A(M, N')$$

$$\to \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, N'')$$

est exacte.
Une suite $M' \to M \to M'' \to 0$ est exacte si et seulement si, pour tout N, la suite

$$0 \to \mathrm{Hom}_A(M'', N)$$

$$\to \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M', N)$$

est aussi exacte.

2.2.13 Corollaire

Un homomorphisme $M \to N$ est un isomorphisme si et seulement si, pour tout P, l'homomorphisme

$$\mathrm{Hom}_A(P, M) \to \mathrm{Hom}_A(P, N)$$

$$(\text{resp. } \mathrm{Hom}_A(N, P) \to \mathrm{Hom}_A(M, P))$$

est un isomorphisme.

2.3 Produits et sommes

2.3.1 Proposition

Soit $(A_i)_{i \in I}$ une famille d'anneaux. Alors, il existe sur $\prod A_i$ une unique structure d'anneau telle que les projections soient des homomorphismes.
Soit $(M_i)_{i \in I}$ une famille de A-modules. Alors, il existe sur $\prod M_i$ une unique structure de A-module telle que les projections soient des homomorphismes.
La partie $M := \bigoplus M_i$ des familles presque toutes nulles est un sous-module de $\prod M_i$ et les applications $M_i \to M, x \mapsto (\ldots, 0, x, 0, \ldots)$ sont des homomorphismes.

2.3.2 Définition

On dit que $\prod A_i$ est le *produit* des A_i, que $\prod M_i$ est le *produit* des M_i et que $\bigoplus M_i$ est la *somme* des M_i.

2.3.3 Remarque

On a toujours des isomorphismes

$$\prod_{i\in I}\prod_{j\in J_i} M_j \simeq \prod_{j\in\coprod_{i\in I} J_i} M_j$$

et

$$\bigoplus_{i\in I}\bigoplus_{j\in J_i} M_j \simeq \bigoplus_{j\in\coprod_{i\in I} J_i} M_j.$$

2.3.4 Remarque

On a aussi des isomorphismes canoniques

$$\mathrm{Hom}_A(M, \prod N_i) \simeq \prod \mathrm{Hom}_A(M, N_i)$$

et

$$\mathrm{Hom}_A(\bigoplus M_i, N) \simeq \prod \mathrm{Hom}_A(M_i, N).$$

2.3.5 Remarque

Si E est un ensemble, on voit que $A^E = \prod_{e\in E} A$ est muni d'une structure de A-module et on peut considérer aussi son sous-module $A^{(E)}$ des familles presque toutes nulles.

2.3.6 Proposition

On a des isomorphismes

$$A^E \bigoplus A^F = A^{E\coprod F}$$

et

$$A^{(E)} \bigoplus A^{(F)} = A^{(E\coprod F)}.$$

On a aussi

$$A^{E\times F} \simeq (A^F)^E \simeq \mathrm{Hom}_A(A^{(E)}, A^F)$$

et

$$(A^{(F)})^{(E)} \simeq A^{(E\times F)}.$$

Enfin, si M est un A-module, toute application $E \to M$ se prolonge de manière unique en un homomorphisme de A-modules $A^{(E)} \to M$.

2.3.7 Définition

On dit que $A^{(E)}$ est le *module libre* sur E. On dit aussi que $A^{E\times F}$ est le *module des matrices* $E \times F$ sur A et on le note $\mathcal{M}_{E\times F}(A)$.
Soit $E \to M$ une famille d'éléments de M. On dit que celle ci est *libre* (resp. *génératrice* , resp. une *base*) si l'homomorphisme $A^{(E)} \to M$ est injectif (resp. surjectif, resp. bijectif).
Si le cardinal $|E|$ d'une base de M est indépendant de la base, on dit que $|E|$ est le *rang* de M.

2.3.8 Remarques

Si $A \neq 0$, $E \to M$ est une base infinie et $F \to M$ une famille génératrice, alors $|E| \leq |F|$. En particulier, si M possède une base infinie, son rang est bien défini. Par contre, on peut avoir un isomorphisme de A-modules $A^2 \simeq A$, par exemple avec $A := \mathrm{End}_{\mathbf{Q}}(\mathbf{Q}^{\mathbf{N}})$.
Il est clair qu'un A-module M est engendré par S si et seulement si la famille $S \hookrightarrow M$ est génératrice. En particulier, M est de type fini (resp. monogène) si et seulement s'il existe un homomorphisme surjectif $A^n \to M$ (resp. $A \to M$).

2.3.9 Proposition

Soit $0 \to M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \to 0$ une suite exacte courte. Alors, les conditions suivantes sont équivalentes

i) Il existe $\sigma : M'' \to M$ tel que $\pi \circ \sigma = \mathrm{Id}$ (la suite est scindée).

ii) Il existe $\rho : M \to M'$ tel que $\rho \circ \iota = \mathrm{Id}$.

iii) Il existe $\sigma : M'' \to M$ et $\rho : M \to M'$ tel que $\iota \circ \rho + \sigma \circ \pi = \mathrm{Id}$.

iv) Il existe un isomorphisme $\varphi : M' \oplus M'' \xrightarrow{\sim} M$ tel que $\varphi(m', 0) = \iota(m')$ et $\pi(\varphi(m', m'')) = m''$.

2.3.10 Corollaire

Si M'' est libre, la suite est scindée. En particulier, si M' et M'' sont tous les deux libres, alors M aussi et le rang de M est la somme des rangs de M' et de M'' (si ceux-ci sont bien définis).

2.3.11 Remarque

Si M est un A-module à gauche et $\mathfrak{a}$ un idéal bilatère, alors

$$\mathfrak{a}M := \{\sum a_i m_i, a_i \in \mathfrak{a}, m_i \in M\}$$

est un sous-A-module à gauche.
De plus, $M/\mathfrak{a}M$ est implicitement muni d'une structure de $A/\mathfrak{a}$-module à gauche et pour tout $A/\mathfrak{a}$-module N, on a un isomorphisme

$$\mathrm{Hom}_{A/\mathfrak{a}}(M/\mathfrak{a}M, N) \simeq \mathrm{Hom}_A(M, N).$$

2.3.12 Proposition

On a toujours

$$(\oplus M_i)/\mathfrak{a}(\oplus M_i) \simeq \oplus(M_i/\mathfrak{a}M_i).$$

et en particulier,

$$A^{(E)}/\mathfrak{a}A^{(E)} \simeq \oplus(A/\mathfrak{a})^{(E)}.$$

D'autre part, si une suite

$$M' \to M \to M'' \to 0$$

est exacte à droite, alors la suite

$$M'/\mathfrak{a}M' \to M/\mathfrak{a}M \to M''/\mathfrak{a}M'' \to 0$$

est aussi exacte à droite.

2.4 Algèbres

2.4.1 Définitions

Soit A un anneau commutatif. Une *A-algèbre (associative et unitaire)* est un anneau B muni d'un homomorphisme d'anneaux $f : A \to B$.
On dit que B est une A-algèbre centrale si $f(A) \subset Z(B)$.
Si C est une autre A algèbre, avec morphisme structural $g : A \to C$, un *A-morphisme* $h : B \to C$, est un homomorphisme d'anneaux tel que $h \circ f = g$. On définit de manière évidente une *sous-algèbre* .

2.4.2 Exemples

L'anneau non-commutatif des opérateurs différentiels $\mathbf{C}[t, \partial]$ est une $\mathbf{C}[t]$-algèbre non-centrale. Mais $M_n(\mathbf{C})$ est une $\mathbf{C}$-algèbre centrale.

Nous ne considérerons dans la suite que des algèbres centrales.

2.4.3 Remarque

Il revient au même de se donner une structure de A-algèbre (centrale) sur un anneau B ou une structure de A module telle que

$$\forall a \in A, b, b' \in B, a(bb') = b(ab') = (ab)b'.$$

L'équivalence est donnée par $ab = f(a)b$ et $f(a) = a1_B$.
Un homomorphisme de A-algèbres est un homomorphisme d'anneaux qui est en même temps un homomorphisme de A-modules. Une sous-algèbre est un sous-anneau qui est aussi un sous-module.

2.4.4 Remarque

Si A est un anneau quelconque, il existe un unique homomorphisme d'anneaux $\mathbf{Z} \to A$ et son image est contenue dans le centre de A. On peut ainsi identifier anneaux et $\mathbf{Z}$-algèbres (centrales).

2.4.5 Exemples

Soit A un anneau commutatif. Si M est un A-module, alors $\mathrm{End}_A(M)$ est une A-algèbre.
Il en résulte que si E est un ensemble fini, alors

$$\mathcal{M}_{E\times E}(A) \simeq \mathrm{End}_A(A^E)$$

est muni d'une structure de A-algèbre par transport de structure.
Aussi, si E est un ensemble, alors A^E est une A-algèbre (commutative).

2.4.6 Remarque

Si B est une A-algèbre, se donner un B-module revient à se donner un A-module M et un homomorphisme de A-algèbres $B \to \mathrm{End}_A(M)$.

2.4.7 Proposition

Si B est une A-algèbre, toute intersection de sous-algèbre de B est une sous-algèbre. En particulier, si $S \subset B$, il existe une plus petite sous-algèbre $A[S]$ de B contenant S.

2.4.8 Définition

On dit que $A[S]$ est la *sous-algèbre engendrée par* S .

2.4.9 Proposition

Soit A un anneau commutatif et G un monoïde (multiplicatif). Il existe sur le A-module $A^{(G)}$ une unique structure de A-algèbre telle que la multiplication prolonge celle de G (i.e. $(ag)(bh) = (ab)(gh)$).
Si B est une A-algèbre, tout homomorphisme de monoïdes $G \to B$ se prolonge de manière unique en un homomorphisme de A-algèbres $A^{(G)} \to B$.

2.4.10 Définition

Soit A un anneau commutatif et E un ensemble. Si G le monoïde commutatif libre sur E, on dit que $A[E] := A^{(G)}$ est *l'algèbre des polynômes sur* E (pour retrouver la définition habituelle, il faut noter multiplicativement le monoïde).

2.4.11 Proposition

Si B est une A-algèbre commutative, toute application $E \to B$ se prolonge de manière unique en un homomorphisme de A-algèbres $A[E] \to B$.

2.4.12 Remarques

On a donc une application

$$A[E] \times B^E \to B, (P, (b_e)_{e\in E}) \mapsto P((b_e)_{e\in E}).$$

De plus, si $(b_e)_{e\in E} \in B^E$ et $S := \{b_e\}_{e\in E} \subset B$, alors l'image de l'homomorphisme

$$A[E] \to B, P \mapsto P((b_e)_{e\in E})$$

est $A[S]$, ce qui justifie nos notations.
Il résulte aussi de la proposition que l'on a un homomorphisme de A-algèbres $A[E] \to B^{B^E}$: un polynôme P est envoyé sur l'application

$$P : B^E \to B, \{b_e\}_{e\in E} \mapsto P(\{b_e\})$$

qui sera dite *polynomiale* .

2.4.13 Remarque

Si E et F sont deux ensembles, on a un isomorphisme $A[E][F] \simeq A[E \coprod F]$.

2.5 Polynômes, localisation

2.5.1 Remarques

Si A est un anneau commutatif et

$$E := \{T_1, \ldots, T_n\},$$

alors, $A[E]$ est l'anneau de polynômes habituel

$$A[T_1, \ldots, T_n].$$

De même, si B est une A-algèbre commutative, l'application polynomiale $B^n \to B$ associée à

$$P = \sum a_{i_1,\ldots,i_n} T_1^{i_1} \ldots T_n^{i_n}$$

n'est autre que l'application

$$P : (b_1, \ldots, b_n) \mapsto \sum a_{i_1,\ldots,i_n} b_1^{i_1} \ldots b_n^{i_n}.$$

C'est un résultat classique que l'application canonique

$$A[T_1, \ldots, T_n] \to A^{A^n}$$

est injective si A est intègre (voir plus bas) et infini.
Enfin, on a l'isomorphisme $A[T][S] \simeq A[T, S]$.

2.5.2 Remarque

Si B est une A-algèbre pas nécessairement commutative et $b \in B$, il existe un unique homomorphisme de A-algèbres $A[T] \to B$ tel que $T \mapsto b$.
On sait que se donner un $A[T]$-module revient à se donner un A-module M et un homomorphisme de A-algèbres $A[T] \to \mathrm{End}_A(M)$. Cette dernière donnée correspond à un élément $u \in \mathrm{End}_A(M)$.
Si de même, N est un A module muni d'un endomorphisme v, dire qu'une application $f : M \to N$ est un homomorphisme de $A[T]$-modules signifie que c'est un homomorphisme de A-modules et que $v \circ f = f \circ u$. En particulier, un sous-$A[T]$-module de M est un sous-A-module stable par u.

2.5.3 Définition

Par définition, tout $P \in A[T]$ s'écrit de manière unique $P = \sum_n a_n T^n$. Si $P \neq 0$, le *degré* d de P est le plus grand entier tel que $a_n \neq 0$. On dit que a_d est le *coefficient dominant* et que P est *unitaire* si $a_d = 1$. On pose aussi $\deg(0) = -\infty$.

2.5.4 Remarques

Ces considérations s'appliquent aussi à

$$A[T_1, \cdots, T_n] = A[T_1, \cdots, T_{n-1}][T_n].$$

On parle alors de degré en T_n ou de polynôme unitaire en T_n.
Enfin, on vérifie aisément que

$$\deg(P + Q) \leq \max(\deg P, \deg Q)$$

avec égalité si $\deg P \neq \deg Q$ et que

$$\deg(PQ) \leq \deg P + \deg Q$$

avec égalité si P ou Q est unitaire (ou si A est intègre).

2.5.5 Proposition (Division euclidienne)

Les polynômes de degré strictement inférieur à d forment un sous-module libre $A[T]_{<d}$ de rang d de $A[T]$.
Si $P \in A[T]$ est unitaire de degré d, l'application canonique

$$A[T]_{<d} \to A[T]/P$$

est un isomorphisme de A-modules.

2.5.6 Remarque

Si A est un anneau commutatif et $S \subset A$, on pose $A[S^{-1}] := A[\{X_s\}_{s \in S}]/(\{1 - sX_s\}_{s \in S})$ et on note $\frac{a}{s}$ l'image de aX_s dans $A[S^{-1}]$.

2.5.7 Proposition

Tout $s \in S$ devient inversible dans $A[S^{-1}]$.
De plus, si B est une A-algèbre commutative telle que tout $s \in S$ devienne inversible dans B, il existe un unique homomorphisme de A-algèbres $A[S^{-1}] \to B$.

2.5.8 Définition

Une *partie multiplicative d'un anneau* A est un sous-monoïde pour la multiplication.

2.5.9 Proposition

L'algèbre $A[S^{-1}]$ ne dépend que de la partie multiplicative engendrée par S.
De plus, si S est une partie multiplicative de A, alors tout élément de $A[S^{-1}]$ s'écrit sous la forme $\frac{a}{s}$ et le noyau de l'application canonique $A \to A[S^{-1}]$ est l'ensemble des $a \in A$ tels qu'il existe $s \in S$ avec $sa = 0$.

2.5.10 Proposition

Soit M un A-module et $S \subset A$ une partie multiplicative. Alors,

i) La relation
$$(s, m) \sim (s', m') \Leftrightarrow \exists t \in S, t(sm' - s'm) = 0$$
sur $S \times M$ est une relation d'équivalence.
On note $S^{-1}M$ l'ensemble quotient.

ii) La loi
$$(s, m) + (s', m') = (ss', s'm + sm')$$
induit une loi de groupe abélien sur $S^{-1}M$.

iii) La loi
$$(s, a)(s', a') = (ss', aa')$$
induit sur $S^{-1}A$ une loi d'anneau.

iv) la loi
$$(s, a)(s', m') = (ss', am')$$
induit sur $S^{-1}M$ d'une loi de $S^{-1}A$ module.

v) L'application
$$A \to S^{-1}A, a \mapsto \overline{(1, a)}$$
est un homomorphisme d'anneaux.

vi) Tout homomorphisme de A-module $M \to N$ se prolonge de manière unique en un homomorphisme de $S^{-1}A$-modules $S^{-1}M \to S^{-1}N$.

2.5.11 Définition

Si M est un A-module, on dit que $S^{-1}M$ est le *localisé* en S de M.

2.5.12 Proposition

On a un isomorphisme canonique d'anneaux

$$S^{-1}A \simeq A[S^{-1}].$$

2.5.13 Lemme

Une suite

$$\cdots \to M_i \xrightarrow{d_i} M_{i+1} \to \cdots$$

est exacte si et seulement si pour tout i, on a

$$d_{i+1} \circ d_i = 0$$

et les suites

$$0 \to \operatorname{Im} d_{i-1} \to M_i \to \ker d_{i+1} \to 0$$

sont exactes.

2.5.14 Proposition

On a toujours

$$S^{-1}(\oplus M_i) \simeq \oplus S^{-1}M_i.$$

et en particulier,

$$S^{-1}(A^{(E)}) \simeq (S^{-1}A)^{(E)}.$$

D'autre part, si une suite

$$\cdots \to M_i \to M_{i+1} \to \cdots$$

est exacte, alors la suite

$$\to \cdots S^{-1}M_i \to S^{-1}M_{i+1} \to \cdots$$

est aussi exacte.

2.6 Structure des anneaux commutatifs

2.6.1 Définitions

Soit A un anneau commutatif.
On dit que $a \in A$ est *nilpotent* si

$$\exists n \in \mathbf{N}, a^n = 0.$$

On dit que c'est un *diviseur de zéro* si

$$\exists b \in A \backslash 0, ab = 0.$$

Sinon, on dit que x est *régulier* .
On dit que A est *réduit* si 0 est le seul élément nilpotent.
On dit que A est *intègre* si 0 est le seul diviseur de 0.
On dit que A est un *corps* si 0 est le seul élément non-inversible.
Le *radical d'un idéal* $\mathfrak{a}$ est

$$\sqrt{\mathfrak{a}} := \{a \in A, \exists n \in \mathbf{N}, a^n \in \mathfrak{a}\}.$$

On dit que $\mathfrak{a}$ est *radical* si $\sqrt{\mathfrak{a}} = \mathfrak{a}$.
On dit qu'un idéal $\mathfrak{p} \subset A$ de A est *premier* si $S := A \backslash \mathfrak{p}$ est une partie multiplicative.
On dit qu'un idéal $\mathfrak{m}$ est *maximal* s'il est maximal parmi les idéaux $\neq A$.

2.6.2 Lemme

Soit A un anneau commutatif. Alors,

i) si $\mathfrak{a}$ est un idéal de A, on a $\mathfrak{a} = A \Leftrightarrow 1 \in \mathfrak{a}$

ii) Si $a \in A$, on a $a \in A^* \Leftrightarrow (a) = A$.

iii) L'anneau A est un corps si et seulement si A a exactement 2 idéaux (0 et A).

2.6.3 Proposition

Soit $\mathfrak{a}$ un idéal d'un anneau commutatif A. Alors, $\mathfrak{a}$ est radical (resp. premier, resp. maximal) si et seulement si $A/\mathfrak{a}$ est réduit (resp. intègre, resp. un corps).
En particulier, A est réduit (resp. intègre, resp. un corps) si et seulement si l'idéal 0 est radical (resp. premier, resp. maximal).
Enfin, tout idéal maximal est premier et tout idéal premier est radical.

2.6.4 Corollaire

Soit $f : A \to B$ est un homomorphisme d'anneaux commutatifs et $\mathfrak{q}$ un idéal premier de B. Alors $\mathfrak{p} := f^{-1}(\mathfrak{q})$ est un idéal premier de A.
Soit $\pi : A \to B$ est un homomorphisme surjectif d'anneaux commutatifs, $\mathfrak{b}$ un idéal de B et $\mathfrak{a} := \pi^{-1}(\mathfrak{b})$. Alors $\mathfrak{a}$ est un idéal radical (resp. premier, resp. maximal) de A si et seulement si $\mathfrak{b}$ est un idéal radical (resp. premier, resp. maximal) de B.

2.6.5 Théorème

Soit A un anneau commutatif. Alors,

a) Tout idéal de A distinct de A est contenu dans un idéal maximal.

b) L'intersection des idéaux premiers de A contenant $\mathfrak{a}$ est $\sqrt{\mathfrak{a}}$.

2.6.6 Définition

Si K est un corps, un K-module s'appelle un *espace vectoriel* et le rang s'appelle la *dimension*.

2.6.7 Théorème

Tout espace vectoriel est libre : plus précisément, si E est une famille libre qui se prolonge en une famille génératrice F, il existe une base entre E et F.

2.6.8 Corollaire

Si A est un anneau commutatif non-nul, M un A-module, $E \to M$ une base et $F \to M$ une famille génératrice, alors $|E| \leq |F|$. En particulier, $|E|$ ne dépend que de M.

2.6.9 Remarque

Si S est le sous-monoïde engendré par $a \in A$, on note $M_a := S^{-1}M$. En particulier, on a

$$A_a \simeq A[a^{-1}].$$

Si $\mathfrak{p}$ est un idéal premier, et $S_\mathfrak{p} := A \backslash \mathfrak{p}$, on note $M_\mathfrak{p} := S_\mathfrak{p}^{-1}M$.
Enfin, si S est l'ensemble des éléments réguliers de A, $S^{-1}A$ est l'*anneau de fractions* de A. C'est un corps si A est intègre.

2.6.10 Définition

Un *anneau local* est un anneau commutatif A dans lequel il y a un plus grand idéal $\mathfrak{m} \neq A$.
On dit alors que $A/\mathfrak{m}$ est son *corps résiduel* .

2.6.11 Proposition

Un anneau commutatif A est local si et seulement si $\mathfrak{m} := A \backslash A^*$ est un idéal. C'est alors l'idéal maximal de A.
Si $\mathfrak{p}$ est un idéal premier d'un anneau commutatif A, alors $A_\mathfrak{p}$ est un anneau local d'idéal maximal $\mathfrak{p}_\mathfrak{p}$.

2.6.12 Proposition

Une suite de A modules

$$\cdots \to M_i \to M_{i+1} \to \cdots$$

est exacte si et seulement si pour tout idéal maximal $\mathfrak{m}$, la suite

$$\cdots \to (M_i)_\mathfrak{m} \to (M_{i+1})_\mathfrak{m} \to \cdots$$

l'est.
En particulier, on a $M = 0$ si et seulement si pour tout idéal maximal $\mathfrak{m}$, on a $M_\mathfrak{m} = 0$.

2.6.13 Définition

Une *valuation discrète* sur un corps K est un homomorphisme surjectif de groupes $v : K^* \to \mathbf{Z}$ tel que

$$\forall a, b \in K, v(a+b) \geq \min(v(a), v(b)).$$

Pour donner un sens à cette formule, on prolonge v à K en posant $v(0) := \infty$.

2.6.14 Proposition

Si v est une valuation discrète sur K, alors

$$\mathcal{O} := v^{-1}(\mathbf{N} \cup \{\infty\})$$

est un anneau local (principal) d'idéal maximal

$$\mathfrak{m} := v^{-1}(\mathbf{N}\backslash 0 \cup \{\infty\}).$$

2.7 Anneaux noethériens et factoriels

2.7.1 Définition

Soit A un anneau commutatif. Un A-module M est *noethérien* si toute suite croissante de sous-modules est stationnaire. On dit que A est *noethérien* s'il l'est en tant que A-module.

2.7.2 Remarque

Bien sûr, c'est équivalent à dire que toute famille non-vide de sous-modules possède un élément maximal.

2.7.3 Proposition

Étant donné une suite exacte de A-modules,

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0,$$

on a M noethérien si et seulement si M' et M'' sont noethériens.
En particulier, $M' \oplus M''$ est noethérien si et seulement si M' et M'' le sont.

2.7.4 Proposition

Un A-module M est noethérien si et seulement si tout sous-module est de type fini.
Si A est noethérien, alors M est noethérien si et seulement s'il est de type fini.

2.7.5 Proposition

Soit A est un anneau noethérien. Alors,
Si $\mathfrak{a}$ est un idéal de A, $A/\mathfrak{a}$ est un anneau noethérien.
Si $S \subset A$, alors $A[S^{-1}]$ est un anneau noethérien.

2.7.6 Définition

Une A-algèbre (commutative) B est *de type fini* s'il existe un homomorphisme surjectif

$$A[T_1, \cdots, T_n] \to B.$$

2.7.7 Théorème (de Hilbert)

Si A est un anneau noethérien, toute A-algèbre de type fini est un anneau noethérien.

2.7.8 Définition

Un anneau intègre A est *factoriel* si et seulement si le monoïde $\mathcal{I}$ des idéaux principaux non-nuls de A est libre.

2.7.9 Remarques

On a toujours un isomorphisme de monoïdes

$$(A\backslash 0)/A^* \simeq \mathcal{I}.$$

On voit donc que A est factoriel si et seulement s'il existe un ensemble $\mathcal{P}$ d'éléments non-nuls de A tel que tout élément non-nul de A s'écrive de manière unique sous la forme $u \prod_p p^{n_p}$ avec $u \in A^*$ et $n_p \in \mathbf{N}$. On pose alors $v_p(a) := n_p$.
De plus, comme on a alors un isomorphisme de monoïdes $(A\backslash 0)/A^* \simeq \mathbf{N}^{(\mathcal{P})}$, on voit que

$$a|b \Leftrightarrow \forall p \in \mathcal{P}, v_p(a) \leq v_p(b).$$

En particulier, si $p \in \mathcal{P}$, on a

$$p^n|a \Leftrightarrow v_p(a) \geq n.$$

2.7.10 Proposition

Si K est le corps de fractions de A, v_p se prolonge de manière unique en un homomorphisme de groupes $v_p : K^* \to \mathbf{Z}$ et c'est une valuation discrète.

2.7.11 Définition

Soit A un anneau intègre et $0 \neq p \in A$. On dit que p est *premier* si l'idéal principal (p) est premier et que p est *irréductible* si (p) est maximal parmi les idéaux principaux distincts de A.

2.7.12 Proposition

i) Un élément premier est toujours irréductible.

ii) Si A est factoriel, tout élément irréductible est premier.

iii) Si A est factoriel, l'application $p \mapsto (p)$ est alors une bijection entre $\mathcal{P}$ et l'ensemble des idéaux premiers principaux non nuls.

2.7.13 Proposition

Un anneau intègre A est factoriel si et seulement si tout élément irréductible est premier et toute suite croissante d'idéaux principaux est stationnaire.

2.7.14 Théorème

Si A est factoriel, il en va de même de $A[T_1, \ldots, T_n]$.

2.8 Anneaux principaux

2.8.1 Définition

Un anneau intègre est *principal* si tout idéal est principal. Si $(a_1, \ldots, a_n) = (d)$, on dit que d est un *plus grand diviseur commun* des a_i. On dit que les a_i sont *premiers entre eux* si $d = 1$.

2.8.2 Définition

Un anneau intègre A est *euclidien* s'il existe une application $d : A\backslash 0 \to \mathbf{N}$ compatible avec les relations $|$ et $\leq$, que l'on prolonge par $d(0) = -\infty$, telle que si $a \neq 0$ et $d(a) = d$, l'application

$$A_{<d} \to A/a$$

soit surjective (on pose

$$A_{<d} = \{b \in A, d(b) < d\}).$$

2.8.3 Remarques

L'anneau $\mathbf{Z}$ est euclidien. De même, si K est un corps, $K[T]$ est euclidien. Un anneau euclidien est principal. Un anneau principal est noethérien et factoriel.

2.8.4 Proposition (Théorème chinois)

Si A est un anneau principal et $a, b \in A$ premiers entre eux, alors l'application canonique

$$A \to A/a \times A/b$$

induit un isomorphisme d'anneaux

$$A/ab \simeq A/a \times A/b.$$

En particulier, si $a \in A$, alors

$$A/a \simeq \prod_p A/p^{v_p(a)}.$$

2.8.5 Proposition

Soit $\varphi : M \to N$ un homomorphisme entre deux modules libres de rang finis sur un anneau principal A. Alors, φ est "diagonalisable" : il existe des bases $\{e_i\}_{i=1}^m$ et $\{f_i\}_{i=1}^n$ de M et N respectivement et $a_1, \ldots, a_r \in A$ avec $r \leq m, n$, tels que

$$\varphi(e_i) = a_i f_i$$

pour $i \leq r$ et 0 sinon.

2.8.6 Proposition

Soit M un module de type fini sur un anneau principal A et N un sous-module de M. Si M est engendré par (au plus) n éléments, alors N aussi. Si M est libre, alors N aussi.

2.8.7 Proposition

Si A est un anneau principal, tout A-module de type fini est somme directe de A-modules monogènes.

2.8.8 Théorème (de Jordan)

Soit M un module de type fini sur un anneau principal A. Alors, M est somme directe d'un module libre et de modules de la forme A/p^n avec p irréductible.

2.8.9 Corollaire

Soit K un corps algébriquement clos et u un endomorphisme d'un K-espace vectoriel E de dimension finie. Alors, il existe des $\lambda_i \in K$ et une base $\{e_{i,j}\}_{j=1,\ldots,n_i}$ de E tels que

$$u(e_{i,j}) = \lambda_i e_{i,j} + e_{i,j+1}$$

pour $j < n_i$ et

$$u(e_{i,n_i}) = \lambda_i e_{i,n_i}.$$

2.9 Extensions algébriques

2.9.1 Définition

Une *extension* L d'un corps K est une K-algèbre qui est un corps.
Un *morphisme d'extensions* est un homomorphisme de K-algèbre.
On définit une *sous-extension* ou *extension intermédiaire* de manière évidente.
On dispose aussi de la notion de *composée* M/K d'extensions L/K et M/L.
Enfin, on dit que $[L : K] := \dim_K L$ est le *degré de l'extension* et que L est *finie* sur K si et seulement si $[L : K] < \infty$.

2.9.2 Proposition

Si L/K est une extension de corps et E un espace vectoriel sur L, on a

$$\dim_K E = [L : K] \dim_L E.$$

En particulier, on a toujours

$$[M : L][L : K] = [M : K].$$

Il suit que la composée de deux extensions finies est finie.

2.9.3 Remarque

Toute intersection de sous-extensions de K dans L est une extension de K. Si $E \subset L$, on note $K(E)$ la plus petite sous-extension de L contenant E. On a bien sûr toujours $K(E)(F) = K(E \cup F)$. Enfin, on note $\deg_K(E) := [K(E) : K]$.

2.9.4 Proposition

Soient $\alpha \in L$ et

$$\Phi_\alpha : K[T] \to L, T \mapsto \alpha.$$

On pose $d := \deg_K(\alpha)$. Alors,
Si $d = \infty$, Φ_α est injective et se prolonge de manière unique en un isomorphisme $K(T)\tilde{\to}K(\alpha)$.
Si $d < \infty$, Φ_α induit un isomorphisme

$$K[T]/P_\alpha \tilde{\to} K(\alpha)$$

où P_α est l'unique polynôme unitaire (irréductible) de degré d tel que $P_\alpha(\alpha) = 0$.

2.9.5 Définition

Dans le premier cas, on dit que α est *transcendant* .
Dans le second, on dit qu'il est *algébrique* et que P_α est son *polynôme minimal* . On écrira $P_{\alpha/K}$ si nécessaire.
On dit que $\alpha, \beta \in L$ algébriques sont *conjugués* si $P_\beta = P_\alpha$.
On dit que L est *algébrique* sur K si tous les éléments de L sont algébriques sur K.

2.9.6 Remarque

Soit $\sigma : L \to M$ un homomorphisme de K-extensions, $\alpha \in L$ et $\beta = \sigma(\alpha)$. Alors σ induit un isomorphisme $K(\alpha) \simeq K(\beta)$. En particulier, α est algébrique si et seulement si β est algébrique et on a alors $P_\beta = P_\alpha$.

2.9.7 Proposition

i) Toute extension finie est algébrique.

ii) Une extension L/K est finie si et seulement s'il existe $\alpha_1, \ldots, \alpha_n$ algébriques sur K tels que $L = K(\alpha_1, \ldots, \alpha_n)$.

iii) La composée de deux extensions algébriques est algébrique.

iv) Si L/K est une extension algébrique, tout K-morphisme $\sigma : L \to L$ est bijectif.

2.9.8 Remarque

Si L est finie sur K et si $\alpha \in L$, alors, P_α n'est autre que le polynôme minimal de la multiplication par α sur le K-espace vectoriel L. De plus, le polynôme caractéristique de la multiplication par α sur L est $P_\alpha^{[L:K(\alpha)]}$.
On définit aussi la *trace* $Tr_{L/K}(\alpha)$ et la *norme* $N_{L/K}(\alpha)$ comme étant respectivement la trace et le déterminant de la multiplication par α sur L. Bien sûr la trace est K-linéaire et on a toujours $N(\alpha\beta) = N(\alpha)N(\beta)$. Enfin, si $a \in K$, $Tr(a) = [L : K]a$ et $N(a) = a^{[L:K]}$.

2.10 Corps de rupture et de décomposition

2.10.1 Définition

Un *corps de rupture* pour $P \in K[T]$ est une extension L de K muni d'un $\alpha \in L$ avec $P(\alpha) = 0$ et $L = K(\alpha)$.

2.10.2 Proposition

Si $P \notin K$, il existe un corps de rupture L pour P sur K.
Supposons P irréductible. Soit L'/K une extension et $\alpha' \in L'$ tels que $P(\alpha') = 0$. Alors, il existe un unique K-morphisme

$$\sigma : L \to L'$$

tel que $\sigma(\alpha) = \alpha'$. Si L' est aussi un corps de rupture de P sur K, σ est un isomorphisme.

2.10.3 Remarque

Soit L/K une extension et $\alpha \in L$. Alors, $K(\alpha)$ est un corps de rupture pour P_α sur K.

2.10.4 Définition

Un *corps de décomposition* pour $P \in K[T]$ est une extension L de K telle qu'il existe $c \in K$ et $\alpha_1, \ldots, \alpha_d \in L$ avec

$$P = c(T - \alpha_1) \cdots (T - \alpha_d)$$

et $L = K(\alpha_1, \ldots, \alpha_d)$.

2.10.5 Proposition

Tout $P \in K[T]$ admet un corps de décomposition L.
Soient L'/K une extension et $\alpha'_1, \ldots, \alpha'_d \in L$ avec

$$P = c(T - \alpha'_1) \cdots (T - \alpha'_d).$$

Alors, il existe un K-morphisme $\sigma : L \to L'$. Si L' est aussi un corps de décomposition de P sur K, σ est un isomorphisme.

2.10.6 Définition

Un corps K est *algébriquement clos* s'il n'existe pas d'extension algébrique non-triviale de K. Une *clôture algébrique* d'un corps K est une extension algébrique $\bar{K}$ de K qui est un corps algébriquement clos.

2.10.7 Théorème

Tout corps K possède une clôture algébrique $\bar{K}$. Si L/K est une extension algébrique, il existe un K-morphisme $\sigma : L \to \bar{K}$. Si L est algébriquement clos, σ est un isomorphisme.

2.11 Extensions galoisiennes

2.11.1 Définition

Une extension algébrique L/K est *normale* si pour toute extension M de L et tout K-morphisme $\sigma : L \to M$, on a $\sigma(L) \subset L$.

2.11.2 Remarques

Il suffit de considérer le cas ou M est une clôture algébrique de L.

2.11.3 Proposition

Une extension algébrique L/K est normale si et seulement si tout $P \in K[T]$ irréductible avec une racine dans L se décompose en produit de facteurs linéaires sur L.
Une extension finie est normale si et seulement si c'est le corps de décomposition d'un polynôme.

2.11.4 Définition

On dit que $\alpha \in L$ est *séparable* sur K si

$$P'_\alpha(\alpha) \neq 0.$$

Une extension algébrique L/K *séparable* si tout $\alpha \in L$ est séparable sur K.

2.11.5 Remarque

On dit qu'un polynôme non-constant $P \in K[T]$ est *séparable* s'il se décompose sur un corps de décomposition en produit de facteurs linéaires distincts. On voit alors que $\alpha \in L$ est séparable sur K si et seulement si P_α est séparable.

2.11.6 Définition

Soit L/K une extension finie. Le nombre $[L : K]_s$ de K-morphismes distincts de L dans une clôture algébrique $\bar{K}$ de K est le *degré de séparabilité* de L/K.

2.11.7 Proposition

On a toujours $[L : K]_s \leq [L : K]$ avec égalité si et seulement si L/K est séparable.

2.11.8 Lemme

Si K est un corps fini, alors K^* est un groupe cyclique (i.e. monogène fini).

2.11.9 Théorème

Si L/K est une extension finie, il existe $\alpha \in L$ tel que $[L : K]_s = [K(\alpha) : K]_s$.

2.11.10 Corollaire (théorème de l'élément primitif)

Si L/K est une extension séparable finie, il existe $\alpha \in L$ tel que $L = K(\alpha)$.

2.11.11 Définition

Une extension algébrique L/K est *galoisienne* si et seulement si elle est normale et séparable.

2.11.12 Remarque

Une extension algébrique L/K est galoisienne si et seulement si pour tout $\alpha \in L$, P_α se décompose sur L en produit de facteurs linéaires distincts.

2.12 Théorie de Galois

2.12.1 Définition

Si L/K une extension algébrique, le groupe

$$G := Gal(L/K)$$

des K-automorphismes de L est le *groupe de Galois* de L/K.
Attention, certains auteurs donnent une définition différente du groupe de Galois dans le cas d'une extension non-galoisienne.

2.12.2 Proposition

Une extension finie L/K est galoisienne si et seulement si

$$|Gal(L/K)| = [L : K].$$

2.12.3 Proposition

Soit L/K une extension algébrique et G son groupe de Galois. Si M est une extension intermédiaire, alors

$$H := Gal(L/M)$$

est le sous-groupe de G composé des σ tels que $\sigma_{|M} = \mathrm{Id}_M$.
Réciproquement, si $H \subset G$, alors

$$M := L^H := \{\alpha \in L, \forall \sigma \in H, \sigma(\alpha) = \alpha\}$$

est une extension de corps intermédiaire.

2.12.4 Théorème

Soit L/K une extension algébrique de groupe de Galois G. Alors, L/K est galoisienne (resp. finie) si et seulement s'il existe un sous-groupe (resp. fini) $H \subset G$ tel que $L^H = K$ (resp. et on a alors $H = G$).

2.12.5 Corollaire (théorème de Galois)

Soit L/K une extension galoisienne finie et

$$G := Gal(L/K).$$

Alors, les applications

$$M \mapsto H := Gal(L/M)$$

et

$$H \mapsto M := L^H$$

établissent une bijection décroissante entre les extensions intermédiaires M et les sous-groupes H de G.
De plus, M/K est galoisienne si et seulement si H est distingué dans G et on a alors un isomorphisme canonique

$$Gal(M/K) \cong G/H.$$

2.13 Produit tensoriel

2.13.1 Définition

Soient A un anneau, M un A-module à droite, M' un A-module à gauche et N un groupe abélien. Une application $f : M \times M' \to N$ est *bilinéaire* si on a toujours

$$f(m+n, m') = f(m, m') + f(n, m'),$$

$$f(m, m'+n') = f(m, m') + f(m, n')$$

et

$$f(m, an) = f(ma, n).$$

2.13.2 Remarques

L'ensemble $\mathrm{Bil}(M \times M', N)$ des applications bilinéaires $M \times M' \to M$ est un sous-groupe de $N^{M\times M'}$.
Si M est un A-module à gauche et N un groupe abélien, on munit $\mathrm{Hom}(M, N)$ d'une structure de A-module à droite en posant $(fa)(m) = f(am)$.

2.13.3 Proposition

La bijection $N^{M\times M'} \simeq (N^{M'})^M$ induit un isomorphisme de groupes abéliens

$$\mathrm{Bil}(M \times M', N) \tilde{\to} \mathrm{Hom}_A(M, \mathrm{Hom}(M', N)).$$

2.13.4 Définition

Soient A un anneau, M un A-module à droite et M' un A-module à gauche. Le *produit tensoriel* de M par M' est le quotient $M \otimes_A M'$ du groupe abélien libre sur l'ensemble $M \times M'$ par le sous-groupe engendré par tous les

$$(m, m' + n') - (m, m') - (m, n'),$$

$$(m + n, m') - (m, m') - (m', n)$$

et

$$(am, n) - (m, an).$$

On note $m \otimes n$ l'image de $(m, n) \in M \times M'$ dans $M \otimes_A M'$.

2.13.5 Proposition

L'application canonique

$$M \times M' \to M \otimes_A M'$$

est bilinéaire et toute application bilinéaire

$$M \times M' \to N$$

se factorise de manière unique par $M \otimes_A M'$. On obtient ainsi un isomorphisme de groupes abéliens

$$\mathrm{Bil}(M \times M', N) \tilde{\to} \mathrm{Hom}(M \otimes_A M', N)).$$

2.13.6 Corollaire

Soient $f : M \to N$ et $g : M' \to N'$ deux homomorphismes de A-modules à droite et à gauche, respectivement. Alors, il existe un unique homomorphisme de groupes

$$f \otimes g : M \otimes_A M' \to N \otimes_A N'$$

tel que pour tout $m \in M, m' \in M'$, on ait

$$(f \otimes g)(m \otimes m') = f(m) \otimes g(m').$$

2.13.7 Proposition

i) On a toujours

$$A \otimes_A M' \simeq M'$$

(et symétriquement).

ii) On a toujours

$$\bigoplus (M_i \otimes_A M') \simeq (\bigoplus M_i) \otimes_A M'$$

(et symétriquement).

iii) Si la suite

$$N \to M \to P \to 0$$

est exacte, la suite

$$N \otimes_A M' \to M \otimes_A M' \to P \otimes_A M' \to 0$$

est aussi exacte (et symétriquement).

2.13.8 Remarque

En général,

$$\ker(f \otimes_A \mathrm{Id}'_M) \neq (\ker f) \otimes_A \mathrm{Id}'_M$$

(prendre pour f la multiplication par 2 dans $\mathbf{Z}$ et $M' = \mathbf{Z}/2$).

2.13.9 Exercice

Montrer que

$$\mathbf{Z}/m \otimes_{\mathbf{Z}} \mathbf{Z}/n \simeq \mathbf{Z}/d$$

avec $d = (m, n)$.

2.13.10 Proposition

Soient $A \to B$ un homomorphisme d'anneaux et M un A-module à gauche. Alors, il existe une unique structure de B-module à gauche sur sur $B \otimes_A M$ telle que l'on ait toujours

$$b'(b \otimes m) = b'b \otimes m.$$

2.13.11 Définition

On dit que $B \otimes_A M$ est le B-module déduit de M par extension des scalaires.

2.13.12 Proposition

Si $f : M \to N$ est un homomorphisme de A-modules, alors $\mathrm{Id}_B \otimes f$ est un homomorphisme de B-modules.
Si M est un A-module à gauche et N est un B-module à gauche, on a un isomorphisme

$$\mathrm{Hom}_B(B \otimes_A M, N) \simeq \mathrm{Hom}_A(M, N).$$

2.13.13 Remarque

Si M est un A-module à gauche et $\mathfrak{a}$ un idéal à droite, l'application

$$\mathfrak{a} \times M \to M, (a, m) \mapsto am$$

est bilinéaire et l'image de l'homomorphisme correspondant

$$\mathfrak{a} \otimes_A M \to M$$

est $\mathfrak{a}M$.
Si $\mathfrak{a}$ est un idéal bilatère, on a un isomorphisme canonique

$$A/\mathfrak{a} \otimes_A M \tilde{\to} M/\mathfrak{a}M$$

de $A/\mathfrak{a}$-modules à gauche.

2.14 Produits tensoriels. Le cas commutatif

Soit A un anneau commutatif.

2.14.1 Proposition

Si M et M' sont deux A-modules, il existe sur $M \otimes_A M'$ une unique structure de A-module telle que

$$a(m \otimes n) = am \otimes n.$$

On a alors un isomorphisme (d'adjonction)

$$\mathrm{Hom}_A(M, \mathrm{Hom}_A(M', N)) \tilde{\to} \mathrm{Hom}_A(M \otimes_A M', N)).$$

De plus, on a des isomorphismes naturels de A-modules

$$A \otimes_A M \simeq M,$$

$$M \otimes_A M' \simeq M' \otimes_A M$$

et

$$(M \otimes_A M') \otimes_A M'' \simeq M \otimes_A (M' \otimes_A M'').$$

2.14.2 Proposition

Si E est une base (resp. une famille génératrice) de M et E' une base (resp. une famille génératrice) de M', alors

$$\{e \otimes e', e \in E, e' \in E'\}$$

est une base (resp. une famille génératrice) de $M \otimes_A M'$.

2.14.3 Remarque

Soient M, N, N' trois A-modules. On a un homomorphisme évident

$$\mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M \otimes_A N', N \otimes_A N'),$$
$$u \mapsto u \otimes \mathrm{Id}_{N'}$$

qui en utilisant l'identification

$$\mathrm{Hom}_A(M \otimes_A N', N \otimes_A N') \simeq \mathrm{Hom}_A(N', \mathrm{Hom}_A(M, N \otimes_A N')$$

fournit par adjonction, un homomorphisme

$$\mathrm{Hom}_A(M,N) \otimes_A N' \to \mathrm{Hom}_A(M, N \otimes_A N').$$

Si N' est libre de rang fini, c'est un isomorphisme.

2.14.4 Remarque

Ci-dessus, on fait $N = A$ et $N' = M$ et on note

$$\check{M} := \mathrm{Hom}_A(M, A).$$

On obtient un homomorphisme

$$\check{M} \otimes_A M \to \mathrm{End}_A(M)$$

qui est bijectif si M est libre de rang fini.
D'autre part, l'identité sur $\check{M}$ correspond à un homomorphisme

$$\check{M} \otimes M \to A$$

ou encore a un homomorphisme

$$M \to \check{\check{M}}$$

qui est bijectif si M est libre de rang fini.
Enfin, on a toujours un isomorphisme canonique

$$(\oplus M_i)\check{} \simeq \prod \check{M}_i$$

et comme $\check{A} \simeq A$, on voit que $(A^{(E)})\check{} \simeq A^E$.

2.14.5 Définition

Si M est un A-module, on dit que $\check{M}$ est le *dual* de M.
Si $f : M \to N$ est un homomorphisme, on note

$$\check{f} : \check{N} \to \check{M}, \varphi \to \varphi \circ f.$$

C'est le *transposé* de f.
Si M est libre de rang fini, l'homomorphisme composé

$$tr_M : \mathrm{End}_A(M) \simeq \check{M} \otimes_A M \to A$$

est l'application *trace* .
Si $E \to M$ est une base finie pour M, l'isomorphisme $A^E \simeq M$ fournit par dualité un isomorphisme $A^E \simeq \check{M}$ et donc une base $E \to \check{M}$, appelée *base duale* .

2.14.6 Proposition

Si B et C sont deux A-algèbres, il existe une unique structure de A-algèbre sur $B \otimes_A C$ telle que l'on ait toujours

$$(bb' \otimes cc') = (b \otimes c)(b' \otimes c')$$

2.14.7 Proposition

Si B est une A-algèbre commutative et G un monoïde, on a un isomorphisme canonique de B-algèbres

$$B \otimes_A A^{(G)} \simeq B^{(G)}.$$

En particulier, si G et H sont deux monoïdes commutatifs, on a

$$A^{(G)} \otimes_A A^{(H)} \simeq A^{(G \times H)}.$$

2.14.8 Proposition

Soit A un anneau commutatif.
Si B est une A-algèbre commutative et E un ensemble, on a

$$B \otimes_A A[E] \simeq B[E].$$

En particulier, si E et F sont deux ensembles, on a

$$A[E] \otimes_A A[F] \simeq A[E \coprod F].$$

En particulier, on a les isomorphismes

$$B \otimes_A A[T] \simeq B[T]$$

ou encore

$$A[T, S] \simeq A[T] \otimes_A A[S].$$

2.14.9 Proposition

Remarquons que, si M est un A-module muni d'un endomorphisme u, on a une suite exacte à droite de $A[T]$-modules

$$A[T] \otimes_A M \to A[T] \otimes_A M \to M \to 0$$

ou la première flèche est $T \otimes_A \mathrm{Id}_M - \mathrm{Id}_{A[T]} \otimes_A u$ et la seconde est la flèche évidente.
En particulier, si K est un corps et E un K-espace vectoriel de dimension finie muni d'un endomorphisme u, on obtient une présentation de E comme quotient d'un morphisme de $K[T]$-modules libres de rang finis.

2.14.10 Proposition

Si S est une partie multiplicative d'un anneau commutatif A, on a un isomorphisme de $A[S^{-1}]$-modules

$$S^{-1}M \simeq A[S^{-1}] \otimes_A M.$$

2.15 Algèbres tensorielles et symétriques

2.15.1 Définition

Soient $(M_i)_{i\in I}$ et M des A-modules. Une application A-*multilinéaire*

$$f : (M_i)_{i\in I} \to M$$

est une application

$$f : \prod M_i \to M$$

telle que pour tout $i_0 \in I$, et $(m_i)_{i\in I\setminus\{i_0\}} \in \prod_{i\neq i_0} M_i$ l'application

$$M_{i_0} \to M, m_{i_0} \to f((m_i)_{i\in I})$$

est un homomorphisme de A-modules.

2.15.2 Remarque

L'ensemble $\mathrm{Hom}_A((M_i)_{i\in I}, N)$ des applications A-multilinéaires

$$(M_i)_{i\in I} \to M$$

est un sous-A-module de $N^{\prod M_i}$.
De plus, si $J \subset I$, on a un isomorphisme

$$\mathrm{Hom}_A((M_i)_{i\in I}, N) \simeq \mathrm{Hom}_A((M_i)_{i\in J}, \mathrm{Hom}_A((M_i)_{i\notin J}, N))$$

2.15.3 Remarque

Soient $(M_i)_{i=1,\dots,n}$ et M des A-modules. On définit alors par récurrence

$$\otimes_{i=1}^{n} M_i = \otimes_{i=1}^{n-1} M_i \otimes M_n.$$

On vérifie alors aisément que

$$\mathrm{Hom}_A((M_i)_{i=1,\dots n}, N) \simeq \mathrm{Hom}_A(\otimes_{i=1}^{n} M_i, M).$$

2.15.4 Définition

Soit A un anneau commutatif, B une A-algèbre et G un monoïde commutatif. Une *graduation de type* G sur B est la donnée d'une famille $\{B_g\}_{g\in G}$ de sous-A-modules de B telle que l'application canonique $\oplus_{g\in G} B_g \to B$ soit bijective et que pour tout $g, h \in G, B_g B_h \subset B_{gh}$.

2.15.5 Exemple

Soit A un anneau commutatif et M un A-module. On note $T^r(M)$ le produit tensoriel r fois itéré de M par lui même et $T(M) = \oplus T^r(M)$. Les isomorphismes

$$T^r(M) \otimes_A T^s(M) \simeq T^{r+s}(M)$$

fournissent des applications bilinéaires

$$T^r(M) \times T^s(M) \to T^{r+s}(M)$$

qui munissent $T(M)$ d'une structure de A-algèbre graduée (de type $\mathbf{N}$).

2.15.6 Définition

On dit que $T(M)$ est l'*algèbre tensorielle* sur M. On dit que le quotient $S(M)$ de $T(M)$ par l'idéal bilatère engendré par les $m \otimes n - n \otimes m$ est l'*algèbre symétrique* sur M.

2.15.7 Proposition

Si M est un A-module, B une A-algèbre (resp. commutative) et $f : M \to B$ un homomorphisme de A-modules, alors f se prolonge de manière unique en un homomorphisme d'algèbres $T(M) \to B$ (resp. $S(M) \to B$.).

2.15.8 Proposition

On a toujours

$$T(M \oplus N) \simeq T(M) \otimes_A T(N).$$

Aussi, si B est une A-algèbre commutative, alors

$$T(B \otimes_A M) \simeq B \otimes_A T(M).$$

On a la même chose avec l'algèbre symétrique :

$$S(M \oplus N) \simeq S(M) \otimes_A S(N)$$

et

$$S(B \otimes_A M) \simeq B \otimes_A S(M).$$

2.15.9 Remarque

On voit facilement que $S(M)$ est gradué de type $\mathbf{N}$. De plus, si M est libre de base E, alors $S(M) \simeq A[E]$.

2.15.10 Définition

Une applications r-linéaire

$$(M, \ldots, M) \to N$$

est *symétrique* si elle est invariante sous l'action évidente de S_r sur $(M, \ldots, M)$. Leur ensemble se note $Sym^r(M, N)$.

2.15.11 Proposition

L'ensemble $Sym^r(M, N)$ est un sous-A-module de $\mathrm{Hom}_A((M, \ldots, M), N)$ et on a un isomorphisme

$$\mathrm{Hom}_A(S^r(M), N) \simeq Sym^r(M, N).$$

2.16 Déterminants

2.16.1 Définition

Soit A un anneau commutatif et M un A-module. On dit que le quotient $\Lambda(M)$ de $T(M)$ par l'idéal bilatère engendré par les $m \otimes m$ est l'*algèbre extérieure* sur M.

2.16.2 Proposition

Si M est un A-module, B une A-algèbre et $f : M \to B$ un homomorphisme de A-modules tel que $\forall m \in M, f(m)^2 = 0$, alors f se prolonge de manière unique en un homomorphisme d'algèbres $\Lambda(M) \to B$. En particulier, tout homomorphisme $f : M \to N$ fournit un homomorphisme $\Lambda(f) : \Lambda(M) \to \Lambda(N)$.

2.16.3 Remarque

En général, $\Lambda(M)$ est gradué de type $\mathbf{N}$ et $\Lambda(f)$ préserve la graduation. On note $\Lambda^r(M)$ (resp. $\Lambda^r(f)$) la composante de degré r et $m_1 \wedge \cdots \wedge m_r$ l'image de $m_1 \otimes \cdots \otimes m_r$.

2.16.4 Définition

Une application A-multilinéaire

$$f : (M, \ldots, M) \to N$$

est dite *alternée* si $f(m_1, \ldots, m_r) = 0$ chaque fois qu'il existe $i \neq j$ avec $m_i = m_j$.

2.16.5 Proposition

L'ensemble $Alt^r(M, N)$ des applications r-linéaires alternées $(M, \ldots, M) \to N$ est un sous-A-module de $\mathrm{Hom}_A((M, \ldots, M), N)$ et on a un isomorphisme

$$\mathrm{Hom}_A(\Lambda^r(M), N) \simeq Alt^r(M, N).$$

2.16.6 Proposition

Si M est libre de base $(e_1, \ldots, e_t)$, alors $\Lambda^r(M)$ est libre de base les $e_{i_1} \wedge \cdots \wedge e_{i_r}$ avec $i_1 < \cdots < i_r$. En particulier, c'est un A-module libre de rang $\binom{t}{r}$.

2.16.7 Définition

Soit M un A-module libre de rang t. On dit alors que $\Lambda^t(M)$ est le *déterminant* de M. Si $u \in \mathrm{End}(M)$, alors, le *déterminant* de u est l'unique entier $a \in A$ tel que $\Lambda^t(u)$ soit la multiplication par a.
Si $\mathcal{B} := (e_1, \ldots, e_t)$ est une base de M et si $m_1, \ldots, m_t \in M$, le *déterminant* de $(m_1, \ldots, m_t)$ dans la base $\mathcal{B}$ est le déterminant de l'unique endomorphisme de M qui envoie e_i sur m_i.

2.16.8 Remarque

On voit ainsi que $det_{\mathcal{B}}(m_1, \ldots, m_t) \neq 0$ si et seulement si $(m_1, \ldots, m_t)$ est une base de M.

2.16.9 Proposition

On a toujours $\det(v \circ u) = \det(v)\det(u)$. De plus, u est injectif si et seulement si $\det(u)$ n'est pas diviseur de zéro, et surjectif si et seulement si $\det(u) \in A^*$. Dans ce dernier cas, u est donc bijectif.

2.16.10 Définition

Si u est un endomorphisme d'un module libre M de rang fini t sur A, le *polynôme caractéristique* de u est

$$P_u := \det(T \otimes_A \mathrm{Id}_M - \mathrm{Id}_{A[T]} \otimes_A u) \in A[T].$$

2.16.11 Lemme

Il existe v tel que $u \circ v = \det u \, \mathrm{Id}_M$.

2.16.12 Corollaire (Cayley-Hamilton)

On a toujours $P_u(u) = 0$.

2.16.13 Remarque

Si u est un endomorphisme d'un espace vectoriel E sur un corps K, alors le noyau de l'homomorphisme $K[T] \to \mathrm{End}(E), T \mapsto u$ est principal et donc engendré par un unique polynôme M_u appelé *polynôme minimal* de u. Et on a $M_u | P_u$.

Chapitre 3

Géométrie

On fixe un corps de base K.

3.1 Espaces affines et applications affines

3.1.1 Définition

Un *espace affine*sur K est un ensemble non-vide E muni d'une action simplement transitive du groupe additif d'un espace vectoriel $\vec{E}$ appelé *espace directeur*de E.
La *dimension*de E est celle de $\vec{E}$. En particulier, on parle de *droite affine*ou de *plan affine*.
Enfin, un élément de E s'appelle un *point*.

3.1.2 Remarque

On voit donc qu'un espace affine E de direction $\vec{E}$ est décrit par une application

$$\vec{E} \times E \to E, (u, P) \longmapsto P + u$$

satisfaisant

a) si $P \in E$, alors $P + 0 = P$.

b) si $P \in E$ et $u, v \in \vec{E}$, alors

$$P + (u + v) = (P + u) + v.$$

c) si $P, Q \in E$, il existe u unique tel que

$$Q = P + u.$$

On écrit alors $\overrightarrow{PQ} := u$ et on dispose donc de la *relation de Chasles* :

$$\overrightarrow{PQ} + \overrightarrow{QR} = \overrightarrow{PR}.$$

3.1.3 Remarques

Tout espace vectoriel E a une structure naturelle d'espace affine : On a $\vec{E} = E$ et l'action est tout simplement donnée par l'addition dans E (identification des vecteurs et de leur extrémité).
De même, si E est un espace affine et $\Omega \in E$, l'application $E \to \vec{E}, P \mapsto \overrightarrow{\Omega P}$ est bijective. Par transport de structure, on munit ainsi E d'une structure d'espace vectoriel que l'on note E_Ω (choix d'une origine).

3.1.4 Définition

Si $\Omega \in E$ et $\mathcal{B}$ est une base de $\vec{E}$ on dit que $(\Omega, \mathcal{B})$ est un *repère cartésien*de E.
Si $P \in E$, on dit que les composantes de $\overrightarrow{\Omega P}$ sont les *coordonnées* de P.

3.1.5 Définition

Soient E et F deux espaces affines. On dit que $f : E \to F$ est *affines*'il existe une application linéaire $\vec{f} : \vec{E} \to \vec{F}$ telle que pour tout $P, Q \in E$, on ait

$$f(Q) = f(P) + \vec{f}(\overrightarrow{PQ}).$$

Celle-ci est alors unique. On note $\mathcal{A}(E, F)$ l'ensemble des applications affines de E dans F. Si $F = E$, on écrit $\mathcal{A}(E)$.
On dit *endomorphisme*si $E = F$, *isomorphisme*si f est bijective et *automorphisme*si les deux conditions sont vérifiées.
On dit aussi *forme affine*si $F = K$.

3.1.6 Remarque

Soient E et F deux espaces affines, $f : E \to F$ et $\Omega \in E$. Alors, f est affine si et seulement si

$$f_\Omega : E_\Omega \to F_{f(\Omega)}$$

est linéaire. On a alors un diagramme commutatif

$$\begin{array}{ccc} E_\Omega & \xrightarrow{f_\Omega} & F_{f(\Omega)} \\ \downarrow & & \downarrow \\ \vec{E} & \xrightarrow{\vec{f}} & \vec{F} \end{array}$$

3.1.7 Proposition

i) Soient $f : E \to F$ et $g : F \to G$ deux applications affines. Alors $g \circ f$ est affine et $\overrightarrow{g \circ f} = \vec{g} \circ \vec{f}$.

ii) Soit $f : E \to F$ une application affine. Alors, f est injective (resp. surjective, resp. bijective) si et seulement si $\vec{f}$ l'est.

iii) Si f est un isomorphisme, alors f^{-1} est affine et $\overrightarrow{f^{-1}} = \vec{f}^{-1}$.

3.1.8 Proposition

Soient E et F deux espaces affines. Alors, $\mathcal{A}(E, \vec{F})$ est un sous-espace vectoriel de $\vec{F}^E$ et $\mathcal{A}(E, F)$ est un espace affine d'espace directeur $\mathcal{A}(E, \vec{F})$. De plus, l'application

$$\mathcal{A}(E, F) \to L(E, F), f \mapsto \vec{f}$$

est affine.

3.1.9 Définition

On dit qu'une application affine f est une *dilatation*de *rapport*$k \neq 0$ si $\vec{f} = k\,\mathrm{Id}_{\vec{E}}$.
On dit *translation*si $k = 1$ et *homothétie* si $k \neq 1$.

3.1.10 Proposition

Soit E un espace affine et $GA(E)$ (resp. $Dil(E)$, resp. $Tr(E)$) l'ensemble des automorphismes (resp. dilatations, resp. translations) de E. Alors, on a la suite d'inclusion de sous groupes

$$Tr(E) \subset Dil(E) \subset GA(E) \subset S(E).$$

De plus, l'application canonique $\vec{E} \to S(E)$ induit un isomorphisme de groupes de $\vec{E} \simeq Tr(E)$.
Enfin, on a des suites exactes

$$0 \longrightarrow \vec{E} \longrightarrow GA(E) \longrightarrow GL(\vec{E}) \longrightarrow 1$$

et

$$0 \longrightarrow \vec{E} \longrightarrow Dil(E) \longrightarrow K^* \longrightarrow 1,$$

la seconde flèche étant soit $f \mapsto \vec{f}$, soit l'application qui a une dilatation associe son rapport.

3.1.11 Remarque

Le groupe $GA(E)$ est produit semi-direct de $\vec{E}$ et $GL(\vec{E})$.

3.2 Sous-espaces affines

3.2.1 Définition

On dit qu'un espace affine F est un *sous-espace affine*d'un espace affine E si F est contenu dans E, l'inclusion $i : F \hookrightarrow E$ est une application affine et $\vec{i}$ est l'inclusion de $\vec{F}$ dans $\vec{E}$. Cette structure est unique si elle existe.
Si $\vec{F}$ est un hyperplan (noyau d'une forme linéaire), on parle d'*hyperplan affine* de E.

3.2.2 Remarque

Soient E un espace affine, $F \subset E$ et $\Omega \in F$. Alors, F est un sous-espace affine de E si et seulement si F_Ω est un sous-espace vectoriel de E_Ω.

3.2.3 Proposition

Soit $f : E \to F$ une application affine. Alors,

i) Si G est un sous-espace affine de E, $f(G)$ est un sous-espace affine de F de direction $\vec{f}(\vec{G})$.

ii) Si G est un sous-espace affine de F, $f^{-1}(G)$ est est soit vide, soit un sous-espace affine de F de direction $f^{-1}(\vec{G})$.

3.2.4 Proposition

Toute intersection non-vide de sous-espaces affines d'un espace affine E est un sous-espace affine de E. Et l'espace directeur de l'intersection est l'intersection des espaces directeurs. En particulier, il existe toujours un plus petit sous-espace affine F contenant une partie non-vide A donnée.

3.2.5 Définition

On dit alors que F est le sous-espace affine *engendré* par A. On le note parfois (A). Si $A = \{P_1, \ldots, P_n\}$, on écrit $(P_1 \cdots P_n)$.

3.2.6 Définition

On dit que des points sont *alignés* s'ils sont tous sur une même droite.
On dit que des droites sont *concourantes*si leur intersection est non-vide.
Un *triangle* est un triplet $\{P, Q, R\}$ de points non-alignés. On dit que P est un *sommet* et que la droite (QR) est le *côté opposé*à P.

3.2.7 Lemme

Soient F et G deux sous-espaces affines d'un espace affine E. Soient $P \in F$ et $Q \in G$. Alors

$$F \cap G \neq \emptyset \text{ si et seulement si } \overrightarrow{PQ} \in \vec{F} + \vec{G}.$$

3.2.8 Théorème (d'incidence)

Soient F et G deux sous-espaces d'un espace affine E. Alors

i) Si $F \cap G \neq \emptyset$, on a

$$\begin{aligned} \dim(F \cup G) &= \dim(\vec{F} + \vec{G}) \\ &= \dim F + \dim G - \dim(F \cap G). \end{aligned}$$

ii) Si $F \cap G = \emptyset$, on a

$$\dim(F \cup G) = \dim(\vec{F} + \vec{G}) + 1$$

$$= \dim F + \dim G + 1 - \dim(\vec{F} \cap \vec{G}).$$

3.2.9 Définition

Soient F et G deux sous-espaces affines d'un espace affine E. On dit que F et G sont *parallèles*, et on écrit $F \parallel G$, si $\vec{F} = \vec{G}$.
On dit que F et G sont *supplémentaires*dans E, et on écrit $E = F \oplus G$, si les espaces directeurs associés le sont.
Enfin, on dit aussi que F et G sont *faiblement parallèles* si $\vec{F} \subset \vec{G}$ ou $\vec{G} \subset \vec{F}$.

3.2.10 Proposition

Dans un espace affine E,

i) Si $F \parallel G$, alors $F = G$ ou $F \cap G = \emptyset$.

ii) Si F est un sous-espace affine de E et P un point de E, il existe un unique sous-espace affine G passant par P et parallèle à F.

iii) Soient F, G deux sous-espace affine de E tels que $\vec{E} = \vec{F} + \vec{G}$, alors $F \cap G \neq \emptyset$.

iv) Si F et G sont supplémentaires dans E, alors $F \cap G = \Omega$.

v) Si $\dim E < \infty$, on a $E = F \oplus G$ si et seulement si $\dim E = \dim F + \dim G$ et $F \cap G = \Omega$.

vi) Si H est un hyperplan de E et D une droite, on a on a $E = H \oplus D$ si et seulement si $H \cap D = \Omega$.

3.2.11 Définition

On dit qu'un quadruplet (P, Q, R, S) est un *parallélogramme* si $\overrightarrow{PQ} + \overrightarrow{RS} = 0$. Si les points ne sont pas alignés et sont tous distincts, c'est équivalent à $(PQ) \parallel (RS)$ et $(PS) \parallel (QR)$.

3.3 Théorèmes de Thales, Desargues et Pappus

3.3.1 Définition

Une application affine $p : E \to E$ est une *projection*(resp. *symétrie*) si $p \circ p = p$ (resp. $s \circ s = \mathrm{Id}_E$).

3.3.2 Remarques

Si un endomorphisme f de E possède des points fixes, ceux-ci forment un sous-espace affine de direction $\ker(\mathrm{Id}_{\vec{E}} - \vec{f})$.
Une application $p : E \to E$ est une projection si et seulement s'il existe un sous-espace affine F de E et un supplémentaire G à $\vec{F}$ dans $\vec{E}$ tels que $p(P)$ soit l'intersection de F et de l'unique sous-espace affine de E de direction G passant par P. On a alors $G = \ker p$ et F est l'ensemble des points fixes.
Une dilatation n'a aucun point fixe si c'est une translation non-triviale et un seul point fixe (son *centre*)si c'est une homothétie (non triviale).

3.3.3 Définition

Soit D une droite affine munie d'un repère cartésien $\{\Omega, e\}$. La *mesure algébrique* $\overline{PQ}$ de $\overrightarrow{PQ}$ est définie par la formule $\overrightarrow{PQ} = \overline{PQ}e$.

3.3.4 Proposition

Soient P, Q et R trois points d'une droite D avec $P \neq Q$. Alors,

i) Le rapport $\frac{\overline{PR}}{\overline{PQ}}$ ne dépend pas du choix du repère.

ii) Soient P', Q' et R' trois points d'une droite D' avec $P' \neq Q'$. Pour qu'il existe une application affine $f : D \to D'$ avec

$$f(P) = P', f(Q) = Q', f(R) = R',$$

il faut et suffit que

$$\frac{\overline{P'R'}}{\overline{P'Q'}} = \frac{\overline{PR}}{\overline{PQ}}.$$

3.3.5 Corollaire (Théorème de Thales)

Soient D et D' deux droites distinctes d'un plan munies de points P, Q, R et P', Q', R' respectivement avec $P \neq Q$, $P' \neq Q'$ et $P \neq P'$. Supposons que $Q = Q'$ ou que $(PP') \parallel (QQ')$. Alors

$$\frac{\overline{P'R'}}{\overline{P'Q'}} = \frac{\overline{PR}}{\overline{PQ}}$$

si et seulement si $R = R'$ ou $(PP') \parallel (RR')$.

3.3.6 Proposition

Un endomorphisme f de E est une dilatation si et seulement si pour toute droite $D \subset E$, $f(D)$ est une droite parallèle à D. De plus, on a $f(D) = D$ si et seulement si f est une translation de vecteur $u \in \vec{D}$ ou une homothétie dont le centre est sur D.

3.3.7 Proposition

Soient P, Q, P' et Q' quatre points de E avec $P \neq Q$. Alors, il existe une dilatation f telle que

$$f(P) = P', f(Q) = Q'$$

si et seulement si

$$P' \neq Q' \text{ et } (PQ) \parallel (P'Q').$$

Celle ci est alors unique. De plus, f est

i) une translation si $(PP') \parallel (QQ')$ ou alors $P = P'$ et $Q = Q'$.

ii) une homothétie de centre Ω si

$$(PP') \cap (QQ') = \{\Omega\},$$

ou $P = P' = \Omega$ et $Q \neq Q'$, ou encore $Q = Q' = \Omega$ et $P \neq P'$.

3.3.8 **Corollaire** (Petit théorème de Desargues)

Soient $\{P, Q, R\}$ et $\{P', Q', R'\}$ deux triangles avec $P' \neq P, Q' \neq Q$ et $R' \neq R$, dont les côtés sont parallèles deux à deux :

$$(PQ) \parallel (P'Q'), (QR) \parallel (Q'R'), (RP) \parallel (R'P').$$

Alors, les droites $(PP'), (QQ')$ et (RR') sont, soit concourantes, soit parallèles.

3.3.9 Proposition

Deux dilatations commutent si et seulement si, l'une est l'identité, ce sont deux translations ou ce sont deux homothéties de même centre.

3.3.10 **Corollaire** (Théorème de Pappus)

Soient D et D' deux droites munies de points tous distincts P, Q, R et P', Q', R', respectivement. Supposons que $(PQ') \parallel (QP')$ et $(QR') \parallel (RQ')$. Alors $(PR') \parallel (RP')$.

3.4 L'enveloppe vectorielle

3.4.1 Définition

Soit E un espace affine. On dit que le quotient $\hat{E}$ de $K^{(E)}$ par le sous-espace vectoriel engendré par les

$$\lambda P - \lambda Q + \mu R - \mu S$$

avec $\lambda\overrightarrow{PQ} + \mu\overrightarrow{RS} = 0$, est l'*enveloppe vectorielle* de E.

3.4.2 Proposition

L'application composée

$$i : E \to K^{(E)} \to \hat{E}$$

est affine et toute application affine $E \to F$ ou F est un espace vectoriel se factorise de manière unique par i pour donner une application linéaire $\hat{E} \to F$.

3.4.3 Corollaire

Toute application affine $f : E \to F$ se prolonge de manière unique en une application linéaire

$$\hat{f} : \hat{E} \to \hat{F}$$

et on a toujours

$$\hat{g} \circ \hat{f} = \widehat{g \circ f}.$$

3.4.4 Proposition

L'application linéaire

$$K^{(E)} \to K, P \mapsto 1$$

se factorise par $\hat{E}$ pour donner une forme linéaire $h : \hat{E} \to K$ et l'application $i : E \to \hat{E}$ induit un isomorphisme $E \simeq h^{-1}(1)$.

3.4.5 Remarque

On identifie alors E avec l'hyperplan d'équation $h = 1$ dans $\hat{E}$.
Il y a d'autres constructions de $\hat{E}$, par exemple on peut mettre une structure d'espace vectoriel sur

$$(E \times K^*) \cup \vec{E}.$$

Les vérifications sont alors assez laborieuses. On peut aussi considérer l'application

$$E \times E \to \vec{E}, (P, Q) \mapsto \overrightarrow{PQ}.$$

Celle-ci fournit une application affine $E \hookrightarrow \vec{E}^E$ affine et on prend pour $\hat{E}$ le sous-espace vectoriel engendré par l'image de E. C'est assez naturel comme construction mais celle-ci ne fonctionne que si $\dim E > 0$.

3.4.6 Proposition

Soit $f : E \to F$ une application entre deux espaces affines. Alors, f est affine si et seulement si f se prolonge en une application linéaire $f' : \hat{E} \to \hat{F}$ et on a alors $f' = \hat{f}$.

3.4.7 Proposition

Soit F une partie non-vide d'un espace affine E.
Alors, F est un sous-espace affine de E si et seulement s'il existe un sous-espace vectoriel F' de $\hat{E}$ tel que $F = F' \cap E$.
L'application canonique $\hat{F} \to F'$ est alors un isomorphisme et on identifie ces deux espaces.
Si F est le sous-espace affine de E engendré par une partie non vide A de E, alors $\hat{F}$ est le sous-espace vectoriel engendré par A.

3.4.8 Remarque

Tout élément de $\hat{E} \backslash \vec{E}$ s'écrit de manière unique sous la forme λP avec $\lambda \in K^*$ et $P \in E$. On parle parfois de *point massique*. Il est bon de rappeler qu'une somme finie $\sum \lambda_P P$ est dans E (resp. $\hat{E}$) si et seulement si $\sum \lambda_P = 1$ (resp. 0).

3.4.9 Définition

Si $\sum \lambda_P = 1$, on dit que $\sum \lambda_P P$ est un *barycentre* et que les λ_P sont les *coefficients*. Le *centre de gravité* de $P_1, \ldots, P_n$ est $\sum \frac{1}{n} P_i$ (si $n \neq 0$ dans K). Si $n = 2$, on dit *milieu*.
Enfin, dans un triangle, les droites joignant un sommet au milieu du côté opposé sont les *médianes* (si $2 \neq 0$ dans K).

3.4.10 Remarque

Dans E, on a $Q = \sum \lambda_P P$ si et seulement si $\sum \lambda_P \overrightarrow{QP} = 0$ si et seulement si

$$\forall R \in E, \overrightarrow{QR} = \sum \lambda_P \overrightarrow{PR}.$$

3.4.11 Exercices

On suppose dans ces exercices que $2 \neq 0$ dans K.

i) Montrer que les médianes d'un triangle sont concourantes au centre de gravité ou parallèles (si $3 = 0$ dans K).

ii) Montrer qu'un quadruplé (P, Q, R, S) est un parallélogramme si et seulement si le milieu de $\{P, R\}$ est aussi le milieu de $\{Q, S\}$.

iii) Montrer que si $\{P, Q, R\}$ est un triangle et P', Q', R' les milieux des côtés opposés aux aux sommets. Alors, (P', Q', R', Q) est un parallélogramme.

iv) Montrer qu'un endomorphisme p d'un espace affine E est une projection si et seulement si c'est le milieu de Id_E et d'une symétrie s dans $\mathcal{A}(E)$.

3.4.12 Proposition

Pour qu'une partie non-vide F d'un espace affine E soit un sous-espace affine, il faut et suffit que tout barycentre de points de F soit dans F. En fait, le sous-espace affine engendré par une partie non-vide A de E est l'ensemble des barycentres de points de A.
De même, pour qu'une application

$$f : E \to F$$

soit affine, il faut et suffit qu'elle préserve les barycentres.

3.5 Repères affines

3.5.1 Définition

On dit qu'une famille $S \to E$ est *affinement génératrice* (resp. *affinement libre*, resp. un *repère affine* si c'est une famille génératrice (resp. une famille libre, resp. une base) de $\hat{E}$. Les *coordonnées barycentriques* d'un point P dans un repère affine sont les composantes de P, vu comme vecteur de $\hat{E}$.

3.5.2 Remarque

Considérons une famille $\{P_s\}_{s\in S}$ d'éléments de E et fixons $s_0 \in S$. On pose $S_0 = S\backslash\{s_0\}$ et on considère la famille $\{\overrightarrow{P_{s_0}P_s}\}_{s\in S_0}$ de $\vec{E}$. Alors, $S \to E$ est affinement génératrice (resp. affinement libre, resp. un repère affine) si et seulement si $S_0 \to \vec{E}$ est une famille génératrice (resp.une famille libre libre, resp. une base).

3.5.3 Proposition

Soient E et F deux espaces affines et $S \to E$ un repère affine de E. Alors, toute application $S \to F$ se prolonge de manière unique en une application affine $E \to F$.

3.5.4 Exercice

On suppose que $3 \neq 0$ dans K. Soit E un plan affine muni d'un repère affine (A, B, C) et G le centre de gravité du repère.
Si P est un point de E distinct de G, de coordonnées (a, b, c), on note D_P la droite d'équation $ax + by + cz = 0$ dans E.

i) Montrer que D_P ne passe pas par G et que toute droite ne passant pas par G est de la forme D_P pour un unique P.
ii) Montrer que trois points P, Q, R distincts de G sont alignés si et seulement si les droites D_P, D_Q, D_R sont parallèles ou concourantes.
iii) Soient $P \neq Q \in E$ distincts de G. Montrer que $D_P \parallel D_Q$ si et seulement si $G \in (PQ)$.
iv) Soient $P \neq Q \in E$ avec $G \notin (PQ)$. Montrer que $(PQ) = D_R$ avec $R = D_P \cap D_Q$.

3.6 Caractérisation des applications affines

3.6.1 Remarque

Si σ est un automorphisme de K et E un espace vectoriel sur K, on note E^σ le K-espace vectoriel obtenu par restriction des scalaires

$$\sigma^{-1} : K \to K$$

(on a aussi $E^\sigma \simeq K_{\underset{\sigma}{\searrow}} \otimes_K E$). En tant que groupes additifs, E et E^σ sont identiques, mais la multiplication sur E^σ est donnée par $(\lambda, u) \mapsto \sigma^{-1}(\lambda)u$.
En particulier, si E est un espace affine sur K, on peut considérer l'espace affine E^σ dont l'ensemble sous-jacent est E muni de l'action du groupe additif de $\vec{E}^\sigma$ qui n'est autre que celui de E.

3.6.2 Définition

Si σ est un automorphisme de K, on dit qu'une application linéaire (resp. affine) $f : E^\sigma \to F$ est une *application σ-linéaire (resp. σ-affine)* $E \to F$. Dans le cas vectoriel, cela signifie que f est un homomorphisme de groupes tel que

$$f(\lambda u) = \sigma(\lambda) f(u).$$

Si σ n'est pas précisé, on dit *application semi-linéaire (resp. semi-affine).*

3.6.3 Théorème

Soient E et F deux espaces affines de même dimension finie au moins deux. Une bijection

$$f : E \to F$$

est semi-affine si et seulement si elle transforme tout couple de droites parallèles en couple de droites parallèles.

3.6.4 Proposition

Soit E un espace affine sur $K \neq \mathbf{F}_2$ et $P_0, \ldots, P_n \in E$. Alors, $P \in (P_0 \cdots P_n)$ si et seulement s'il existe $Q \in (P_0 P_1)$ et $R \in (P_1 \cdots P_n)$ tels que $P \in (QR)$.

3.6.5 Corollaire

Soit E un espace affine sur $K \neq \mathbf{F}_2$ et $F \subset E$ non-vide. Alors, F est un sous-espace affine de E si et seulement si pour tout $P, Q \in F$, on a $(PQ) \subset F$.

3.6.6 Corollaire

Soient E et F deux espaces affines sur $K \neq \mathbf{F}_2$ et $f : E \to F$ une application telle que pour tout $P, Q \in E$, on ait

$$f(PQ) \subset (f(P)f(Q))(\text{resp. } \supset, \text{ resp. } =).$$

Alors, pour tout $P_0, \ldots, P_n \in E$, on a

$$f(P_0 \cdots P_n) \subset (f(P_0) \cdots f(P_n))(\text{resp. } \supset, \text{resp. } =).$$

3.6.7 Théorème fondamental de la géométrie affine

Soient E et F deux espaces affines de même dimension finie au moins deux sur $K \neq \mathbf{F}_2$. Une bijection $f : E \to F$ est semi-affine si et seulement si elle transforme trois points alignés en trois points alignés.

3.6.8 Remarque

Comme $\mathbf{R}$ n'a pas d'automorphisme non-triviaux, on peut, lorsque $K = \mathbf{R}$ remplacer "semi-affine" par "affine" dans les deux théorèmes précédents.

3.7 Géométrie affine sur un corps ordonné

Dans ce paragraphe, K est un corps ordonné, c'est à dire, muni d'un ordre tel que les translations $x \mapsto x + a$ soient croissantes et $x, y \geq 0 \Rightarrow xy \geq 0$.

3.7.1 Définition

Soit H un hyperplan d'un espace affine E sur K d'équation $f = 0$. On dit alors que

$$\{P \in E, f(P) \geq 0\}$$

est un *demi-espace fermé* de $bord H$.
On définit de manière analogue les *demi-espaces ouverts*.
On dit *demi-droite* ou *demi-plan* si E est une droite ou un plan.

3.7.2 Définition

Si $P, Q \in E$, le *segment fermé* $[P, Q]$ d'*extrémités* P et Q est l'ensemble des barycentres de P et Q affectés de coefficients $\lambda, \mu \geq 0$.
On définit de manière analogue les *segments semi-ouverts* $[P, Q[$ et $]P, Q]$ ainsi que le *segment ouvert* $]P, Q[$.
Enfin, une partie S d'un espace affine E sur K est *convexe* si pour tout $P, Q \in X$, on a

$$[P, Q] \subset S.$$

3.7.3 Proposition

i) Une partie d'un espace affine E sur K est convexe si et seulement si elle est stable par barycentres à coefficients positifs.

ii) L'image d'un convexe par une application affine est convexe.

iii) Toute intersection de convexes est convexe.

iv) Tout espace affine, segment, ou demi-espace est convexe.

3.7.4 Définition

Le plus petit convexe contenant une partie S de E est l'*enveloppe convexe* de S.

3.7.5 Exemple

Les parties convexes d'une droite sont la droite, les segments et les demi-droites. Un segment fermé est l'enveloppe convexe de ses extrémités.

3.7.6 Définition

Soient $\{P_0, \ldots, P_n\}$ et $\{Q_0, \ldots, Q_n\}$ deux repères affines d'un espace affine E et f l'unique application affine qui échange ces repères. On dit que ces repères ont même *orientation* si $\det(f) \geq 0$.
Orienter E, c'est choisir une classe de repères ayant même orientation.

3.8 Espaces projectifs et sous-espaces

3.8.1 Définition

Une structure d'*espace projectif* sur un ensemble X est la donnée d'une bijection

$$(E_X \backslash 0)/K^* \simeq X,$$

où E_X est un espace vectoriel et K^* agit par multiplication. De manière équivalente, c'est la donnée de l'application

$$\pi_X : E_X \backslash 0 \to X, u \mapsto P$$

qui induit cette bijection.
Les composantes $(x_i)_{i \in I}$ de u relativement à une base donnée sont des *coordonnées homogènes* de P relativement à cette base (celles ci sont définies à multiplication près par un scalaire non-nul).
La *dimension* de X est $\dim X = \dim E_X - 1$. On parle de *droite projective*ou de *plan projectif* si la dimension est 1 ou 2. Enfin, les éléments de X sont les *points* de l'espace projectif.

3.8.2 Exemples

Soit E un espace vectoriel sur K et $\mathbf{P}(E)$ l'ensemble des droites vectorielles de E. La surjection $\pi : E\backslash 0 \to \mathbf{P}(E)$ qui envoie un vecteur u sur la droite vectorielle de E dirigée par u munit $\mathbf{P}(E)$ d'une structure d'espace projectif. C'est l'espace projectif sur E. On écrit $\mathbf{P}^n(K) := \mathbf{P}(K^{n+1})$.
De même, l'ensemble $\check{\mathbf{P}}(E)$ des hyperplans vectoriels de E est muni d'une structure d'espace projectif par

$$\check{E}\backslash 0 \to \check{\mathbf{P}}(E), \varphi \to \ker \varphi.$$

L'application

$$K^2\backslash 0 \to K \cup \{\infty\},$$
$$(x, y) \mapsto \frac{x}{y} \text{ si } y \neq 0 \text{ et } \infty \text{ sinon,}$$

fait de $K \cup \{\infty\}$ une droite projective.
Plus généralement, on peut munir

$$K^n \cup K^{n-1} \dots K \cup \infty$$

d'une structure d'espace projectif de dimension n.

3.8.3 Définition

Soit X un espace projectif et F un sous-espace vectoriel de E_X. Alors π_X induit une bijection

$$\pi_Y : (F\backslash 0)/K^* \simeq Y,$$

ou Y est une partie de X. On dit alors que Y est un *sous-espace projectif* de X. On dit *hyperplan projectif* si F est un hyperplan de E.

3.8.4 Exemples

Si $X := \mathbf{P}(E)$, on a tout simplement $Y = \mathbf{P}(F)$.
Les droites de $X := K^2 \cup K \cup \infty$ sont la droite à l'infini $K \cup \infty$ et les droites de K^2 complétées par leur pentes, c'est à dire, d'une part les $D \cup \infty_D$ ou D est une droite de K^2 d'équation $y = ax + b$ et $\infty_D = a \in K$ et, d'autre part, les $D \cup \infty$ ou D est une droite verticale dans K^2 d'équation $x = c$.

3.8.5 Proposition

Soit X un espace projectif. L'application $Y \mapsto E_Y$ est une bijection de l'ensemble des sous-espaces projectifs de X sur l'ensemble des sous-espaces vectoriels de E. Cette bijection préserve l'inclusion et l'intersection.

3.8.6 Corollaire

Toute intersection de sous-espaces projectifs de X est un sous-espace projectif. En particulier, si $S \subset X$, il existe un plus petit sous-espace projectif Y contenant S.

3.8.7 Définition

On dit alors que Y est le sous-espace projectif *engendré*par S ou que S est un ensemble de *générateurs* de Y. On écrit aussi $Y = (S)$.

3.8.8 Proposition (Théorème d'incidence)

Soient Y et Z deux sous-espaces projectifs de X. Alors

$$\dim(Y \cup Z) + \dim Y \cap Z = \dim Y + \dim Z.$$

3.8.9 Exemples

i) Par deux points distincts d'un espace projectif, il passe une droite et une seule.

ii) Deux droites distinctes du plan projectif se coupent en un point et un seul.

3.8.10 Définition

On dit que des points sont *alignés* s'ils sont situés sur une même droite. On dit que des droites sont *concourantes*si leur intersection est non-vide. On appelle *triangle* un ensemble de trois points non-alignés. Ces points sont les *sommets*. Étant donné un sommet, la droite passant par les deux autres sommets est le *côté opposé*.

3.9 Applications projectives

3.9.1 Remarque

Soient X, Y deux espaces projectifs et $g : E_X \to E_Y$ une application linéaire. On sait alors qu'il existe un unique sous-espace projectif Z de X tel que $\ker g = E_Z$. Alors g induit une application

$$g : E_X \backslash E_Z \to E_Y \backslash 0$$

compatible avec l'action de K^* qui, à son tour, induit une fonction $f : X \to Y$ définie sur le complémentaire de Z.

3.9.2 Définition

On dit alors que la fonction f est une *application projective*de X vers Y et que Z est son *noyau*. On note $\mathcal{P}(X, Y)$ leur ensemble.
On dit *homographie* si g est injective (auquel cas le noyau est vide) et on note $GP(X)$ l'ensemble des homographies de X sur lui même. On écrit plutôt $PGL(E)$ si $X = \mathbf{P}(E)$ et $PGL^n(K)$ si $X = \mathbf{P}^n(K)$.
Enfin, on dit que X et Y sont *isomorphes*'il existe une homographie de X sur Y.

3.9.3 Exemples

Une homographie

$$K \cup \infty \to K \cup \infty$$

est une application de la forme

$$z \mapsto \frac{az+b}{cz+d}$$

avec $ad - bc \neq 0$. Bien sûr $-d/c \mapsto \infty$ et $\infty \mapsto a/c$.
Supposons que $\dim X < \infty$ et soient $Y, Z \subset X$ des sous-espaces projectifs disjoints tels que

$$\dim Y + \dim Z = \dim X - 1.$$

Si $P \in X \backslash Y$, on a $(P, Y) \cap Z = Q$ et la fonction $P \mapsto Q$ est une application projective appelée *projection conique*. En fait, elle correspond a la projection sur E_Z de direction E_Y.

3.9.4 Remarque

On a X isomorphe à Y si et seulement si E_X est isomorphe à E_Y. En particulier, X est canoniquement isomorphe à $\mathbf{P}(E_X)$, ce qui permet, en pratique de ne considérer que les espaces projectifs de cette forme. Par exemple, on a

$$K \cup \infty \simeq \mathbf{P}^1(K).$$

3.9.5 Proposition

i) La composée de deux applications projectives est une application projective.

ii) L'application évidente

$$L(E_X, E_Y) \to \mathcal{P}(X, Y)$$

munit l'ensemble des applications projectives non-vides d'une structure d'espace projectif.

iii) On a une suite exacte

$$0 \to K^* \to GL(E_X) \to GP(X) \to 1.$$

3.9.6 Proposition

Soit $f : X \to Y$ une application projective de noyau Z. Si $T \subset X$ est un sous-espace projectif, alors $f(T)$ est un sous-espace projectif de Y. De même, si T est un sous-espace projectif de Y, alors $f^{-1}(T) \cup Z$ est un sous-espace projectif de X.

3.9.7 Définition

Si X est un espace projectif et $\check{X}$ l'ensemble des hyperplans de X, on a une bijection

$$\check{\mathbf{P}}(E_X) \simeq \check{X}$$

qui munit $\check{X}$ d'une structure d'espace projectif. C'est l'*espace projectif dual* de X.

3.9.8 Remarque

Si E est un espace vectoriel et $F \subset E$ un sous-espace vectoriel, alors

$$F^{\perp} = \{\varphi \in \check{E}, F \subset \ker \varphi\}$$

est un sous-espace vectoriel de $\check{E}$. Si $\dim E < \infty$, l'application $F \to F^{\perp}$ est une bijection décroissante de l'ensemble des sous-espaces vectoriels de E sur celui des sous-espaces vectoriels de $\check{E}$.
On en déduit que si X est un espace projectif de dimension finie, on a une bijection décroissante $Y \mapsto Y^{\perp}$ entre l'ensemble des sous-espaces projectifs de X et celui des sous-espaces projectifs de $\check{X}$ (*corrélation*).
On dit que deux assertions sont *duales* si elles se déduisent l'une de l'autre par cette transformation.

3.9.9 Exemples

Dans un plan projectif, les deux assertions de l'exemple 3.8.9 sont duales.
L'assertion duale de "trois points sont alignés"est "trois droites sont concourantes".
Enfin, si on se donne un triangle

$$\{P, Q, R\} \subset X,$$

on lui associe le triangle

$$\{(QR), (RP), (PQ)\} \subset \check{X}$$

appelé *triangle dual*.

3.10 Repères projectifs

3.10.1 Définition

Soient $\{u_i\}_{i\in I}$ une famille de vecteurs non-nuls de E_X et $\{P_i\}_{i\in I}$ son image par π_X. On dit que $\{P_i\}_{i\in I}$ est *projectivement libre* (resp. *génératrice*) si $\{u_i\}_{i\in I}$ est libre (resp. génératrice).
Enfin, on dit que $\{P_i\}_{i\in I}$ est un *repère* si la famille est génératrice, *n'est pas libre* mais que toute sous-famille propre est libre.

3.10.2 Exemple

Dans $\mathbf{P}^n(K)$, on peut prendre tous les points de coordonnées homogènes $(0, \ldots, 0, 1, 0, \ldots, 0)$ et celui de coordonnées $(1, \ldots, 1)$. Dans $K \cup \infty$, on prend $\infty, 0, 1$ comme repère canonique.

3.10.3 Proposition

Soient $\{P_i\}_{i=0}^{n+1}$ et $\{P'_i\}_{i=0}^{n+1}$ des repères de X et X' respectivement. Alors, il existe une unique application projective $f : X \to X'$ telle que, pour tout $i = 0, \ldots, n+1$ on ait $f(P_i) = P'_i$ et c'est un isomorphisme.

3.10.4 Définition

Soient X une droite projective,

$$P, Q, R, S \in X$$

distincts et

$$f : X \to K \cup \infty$$

l'homographie telle que

$$f(P) = \infty, f(Q) = 0, f(R) = 1.$$

Alors,

$$[P, Q, R, S] := f(S) \in K \backslash \{0, 1\}$$

est le *birapport* ou *rapport anharmonique*. On dit que les points sont en *division harmonique* si

$$[P, Q, R, S] = -1.$$

3.10.5 Exercice

Montrer que si $a, b, c, d \in K$ sont distincts,

$$[a, b, c, d] = \frac{\frac{c-a}{c-b}}{\frac{d-a}{d-b}}.$$

3.10.6 Vrai théorème de Thales

Soient X et X' deux droites projectives. Pour qu'il existe une homographie $f : X \to X'$ envoyant quatre points distincts donnés de X sur quatre points distincts donnés de X', il faut et suffit qu'ils aient même birapport.

3.11 Espaces affines et projectifs

3.11.1 Remarque

Soient E un espace vectoriel et H un hyperplan de E. Considérons l'application canonique

$$L(E/H, H) \to L(E), \Phi \mapsto \underline{\Phi} := i \circ \Phi \circ p,$$

où

$$p : E \to E/H, i : H \to E$$

sont la projection et l'inclusion, respectivement. L'application

$$L(E/H, H) \to L(E), \Phi \mapsto \mathrm{Id}_E + \underline{\Phi}$$

est un homomorphisme de monoïdes et induit donc un homomorphisme de groupes

$$L(E/H, H) \to GL(E).$$

Remarquons aussi que, par construction, H est stable par $\mathrm{Id}_E + \underline{\Phi}$.

3.11.2 Proposition

Soient X un espace projectif (non vide), Z un hyperplan dans X et $U := X\backslash Z$. L'homomorphisme de groupes

$$L(E_X/E_Z, E_Z) \to GL(E_X) \to GP(X) \subset S(X)$$

est à valeurs dans $S(U)$ et munit U d'une structure d'espace affine (avec $\vec{U} = L(E_X/E_Z, E_Z)$).

3.11.3 Remarque

Si F est un sous-espace affine de E_X parallèle à E_Z ne passant pas par l'origine, alors π_X induit un isomorphisme d'espaces affines $F \simeq U$. Mais l'isomorphisme $E_Z \simeq \vec{U}$ dépend du choix de F.

3.11.4 Définition

Si E est un espace affine, le *complété projectif* de E est $\bar{E} := \mathbf{P}(\hat{E})$ et le *lieu à l'infini* de E est

$$\infty_E := \mathbf{P}(\vec{E}).$$

On dit aussi que E est la *partie affine* de $\bar{E}$.

3.11.5 Corollaire

Soit E un espace affine. Alors, l'application composée

$$i : E \hookrightarrow \hat{E}\backslash\{0\} \to \bar{E}$$

induit un isomorphisme d'espaces affines

$$E \simeq \bar{E}\backslash\infty_E.$$

Réciproquement, si Z un hyperplan d'un espace projectif X et $U := X\backslash Z$, alors $\bar{U} \simeq X$ et $\infty_U \simeq Z$.

3.11.6 Proposition

Soient X (resp. X') un espace projectif, Z (resp. Z') un hyperplan dans X et U (resp. U') son complémentaire.
Alors, la restriction induit une bijection entre l'ensemble des applications projectives

$$f : X \to X'$$

telles que

$$f(Z) \subset Z', f(X) \not\subset Z',$$

et l'ensemble des applications affines $U \to U'$. On note $g \mapsto \bar{g}$ l'application réciproque.

3.11.7 Remarque

Si $g : E \to F$ est une application affine, alors $\bar{g}$ est induite par $\hat{g}$.

3.11.8 Corollaire

Soient X un espace projectif, Z un hyperplan dans X et $U := X \backslash Z$. Alors, l'application $g \mapsto \bar{g}$ induit un isomorphisme entre $GA(U)$ et le sous groupe des $f \in GP(X)$ qui laissent Z invariant.

3.11.9 Proposition

Soient X un espace projectif, Z un hyperplan dans X et $U := X \backslash Z$. Alors, l'application

$$Y \mapsto V := Y \cap U$$

est une bijection de l'ensemble des sous-espaces projectifs de X qui ne sont pas contenus dans Z sur l'ensemble des sous-espaces affines V de U. Celle-ci est croissante et préserve l'intersection.

3.11.10 Remarque

On a des isomorphismes canoniques $\bar{V} \simeq Y$ et $\infty_V := Y \cap Z$. On dit aussi que V est la *partie affine* de Y (relativement à Z).

3.11.11 Corollaire

Si V est engendré par S comme sous-espace affine, alors $\bar{V}$ est engendré par S comme sous-espace projectif.
Soient V et V' deux sous-espaces affines de U. Alors, $V \parallel V'$ si et seulement si $\infty_V = \infty_{V'}$.
Si $\dim X > 0$, alors $Dil(U)$ (resp. $Tr(U)$) correspond aux $\bar{f}$ qui laissent invariants tous les points de Z (resp. et seulement ceux-ci à part Id_X).

3.11.12 Exemple

Soit X une droite projective et P, Q, R, S quatre points distincts. On choisit un point à l'infini. Si celui-ci est distinct des 4 autres points, on a

$$[P, Q, R, S] = \frac{\overline{\overline{PR}}}{\overline{\overline{QR}}} \Big/ \frac{\overline{\overline{PS}}}{\overline{\overline{QS}}}.$$

Si on prend P comme point à l'infini, alors

$$[P, Q, R, S] = \frac{\overline{QS}}{\overline{QR}}.$$

En particulier, dans ce cas, les point sont en division harmonique si et seulement si Q est le milieu de $\{R, S\}$ lorsque $2 \neq 0$ dans K.

3.12 Théorèmes de Desargues et Pappus

3.12.1 **Proposition** (Vrai théorème de Desargues)

Soient $T := \{P, Q, R\}$ et $T' := \{P', Q', R'\}$ deux triangles d'un plan projectif. On suppose

$$P \neq P', Q \neq Q', R \neq R'$$

et

$$(PQ) \neq (P'Q'), (PR) \neq (P'R'), (QR) \neq (Q'R').$$

On note P'' le point d'intersection de (QR) et de $(Q'R')$ et on définit de manière analogue Q'' et R''.
Alors, les points P'', Q'' et R'' sont alignés si et seulement si les droites (PP'), (QQ') et (RR') sont concourantes.

3.12.2 **Corollaire** (Théorème de Desargues, cas affine, suite)

Soient $T := \{P, Q, R\}$ et $T' := \{P', Q', R'\}$ deux triangles d'un plan affine avec

$$P \neq P', Q \neq Q', R \neq R'.$$

Supposons que les côtés opposés à P dans T et à P' dans T', respectivement, se coupent en P''. Définissons de manière analogue Q'' et R''.
Alors, les points P'', Q'' et R'' sont alignés si et seulement si les droites (PP'), (QQ') et (RR') sont parallèles ou concourantes.

3.12.3 **Proposition** (Vrai théorème de Pappus)

Soient P, Q, R, P', Q', R' six points du plan projectifs tels que

$$P' \neq Q, R; Q' \neq P, R; R' \neq P, Q$$

et que

$$(QR') \neq (Q'R); (PQ') \neq (P'Q); (PR') \neq (P'R).$$

On note P'' le points d'intersection de (QR') et de $(Q'R)$ et on définit les points Q'' et R'' de manière analogue.
Si P, Q, R d'une part et P', Q', R' d'autre part, sont alignés, alors P'', Q'', R'' sont alignés.

3.12.4 **Corollaire** (Théorème de Pappus, cas affine, suite)

Soient P, Q, R, P', Q', R' six points du plan affines tels que

$$P' \neq Q, R, Q' \neq P, R, R' \neq P, Q.$$

On suppose que (QR') et $(Q'R)$ se coupent en un point P'' et on définit les points Q'' et R'' de manière analogue.
Si P, Q, R d'une part et P', Q', R' d'autre part, sont alignés, alors P'', Q'', R'' sont alignés.

3.12.5 **Corollaire** (Théorème de Pappus dual)

Soient P, Q, R, P', Q', R' six points distincts d'un plan projectif. Supposons que les trois droites

$$(PR'), (RQ'), (QP')$$

sont concourantes et que les trois droites

$$(PQ'), (QR'), (RP')$$

le soient aussi. Alors, les trois droites

$$(PP'), (QQ'), (RR')$$

sont aussi concourantes.

3.12.6 **Corollaire** (Théorème de Pappus dual, cas affine)

Soient P, Q, R, P', Q', R' six points distincts d'un plan affine. Supposons que les trois droites

$$(PR'), (RQ'), QP')$$

sont concourantes ou parallèles et que les trois droites

$$(PQ'), (QR'), (RP')$$

le soient aussi. Alors, les trois droites

$$(PP'), (QQ'), (RR')$$

sont aussi concourantes ou parallèles.

3.13 Caractérisation des applications projectives

3.13.1 Proposition

Soit X un espace projectif et $P_0, \ldots, P_n \in X$. Alors, $P \in (P_0 \cdots P_n)$ si et seulement s'il existe $R \in (P_1 \cdots P_n)$ tels que $P \in (P_0 R)$.

3.13.2 Corollaire

Soit X un espace projectif et $Y \subset X$ non-vide. Alors, Y est un sous-espace projectif de X si et seulement si pour tout $P, Q \in Y$, on a $(PQ) \subset Y$.

3.13.3 Corollaire

Soient X et Y deux espaces projectifs et

$$f : X \to Y$$

une application telle que pour tout $P, Q \in X$, on ait

$$f(PQ) \subset (f(P)f(Q))(\text{ resp. } \supset,\ \text{resp. } =).$$

Alors, pour tout $P_0, \ldots, P_n \in X$, on a

$$f(P_0 \cdots P_n) \subset (f(P_0) \cdots f(P_n))(\text{ resp. } \supset,\ \text{resp. } =).$$

3.13.4 Remarque

Soit σ un automorphisme de K et X un espace projectif sur K. On note X^σ l'espace projectif donné par $\pi_X^\sigma : E_X^\sigma \backslash 0 \to E_X \backslash 0 \to X$.

3.13.5 Définition

Soit σ un automorphisme de K. Une *application σ-projective* (resp. une *σ-homographie*) $X \to Y$ est une application projective (resp. une homographie) $X^\sigma \to Y$.
Lorsque σ n'est pas précisé, on dit *application semi-projective*ou *semi-homographie*.

3.13.6 Théorème

Soient X et Y deux espaces projectifs de même dimension finie au moins 2. Une application

$$f : X \to Y$$

est une semi-homographie si et seulement si c'est une bijection qui transforme trois points alignés en trois points alignés.

Chapitre 4

Le langage des catégories

4.1 Définition et exemples

On parlera ci dessous de collections qui ne forment pas nécessairement des ensembles mais on utilisera tout de même les notations habituelles de la théorie des ensembles.

4.1.1 Définition

Une *catégorie* $\mathcal{C}$ consiste en

a) Une collection d'*objets* X.

b) Pour tout $X, Y \in \mathcal{C}$, d'un ensemble de *morphismes* $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ (si $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$, on dit que X est la *source* de f, que Y est son *but*et on écrit $f : X \to Y$).

c) Pour tout $X, Y, Z \in \mathcal{C}$, une loi de *composition*

$$\mathrm{Hom}_{\mathcal{C}}(X, Y) \times \mathrm{Hom}_{\mathcal{C}}(Y, Z) \to \mathrm{Hom}_{\mathcal{C}}(X, Z)$$

$$(f, g) \mapsto g \circ f.$$

On exige de plus que les propriétés suivantes soient satisfaites :

i)

$$\forall X \in \mathcal{C}, \exists\, \mathrm{Id}_X : X \to X,$$

$$\forall f : X \to Y, f \circ \mathrm{Id}_X = f$$

et

$$\forall f : Y \to X, \mathrm{Id}_X \circ f = f$$

(celui-ci est alors unique et s'appelle l'*identité*).

ii)

$$\forall f : X \to Y, g : Y \to Z, h : Z \to T,$$

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

4.1.2 Exemples

i) On a tout d'abord la catégorie **Ens** dont les objets sont les ensembles, les morphismes sont les applications et la composition se fait de la manière habituelle.

On dispose de même de la catégorie a catégorie **Mon** des monoïdes et de la catégorie **Gr** des groupes.

ii) Si G est un monoïde, on peut considérer les catégories G-**Ens** et **Ens**-G des ensembles munis d'une action à gauche ou a droite.

Si A est un anneau, on peut considérer les catégories A-**Mod** des A-modules à gauche et **Mod**-A des A-modules à droite.

En particulier, on a la catégorie **Ab** des groupes abéliens et, si K est un corps la catégorie K-**ev** des K-espaces vectoriels. Ou la catégorie K–**evf** des espaces vectoriels de dimension finie sur un corps K.

On peut aussi regarder, si A est un anneau, la catégorie $\mathbf{Mat}_A$ dont les objets sont les entiers naturels et les morphismes $m \to n$ les matrices à n lignes et m colonnes à coefficients dans A. La composition est alors donnée par la multiplication des matrices.

iii) Si A est un anneau commutatif, on peut considérer la catégories A-**Alg** des A-algèbres (centrales), et en particulier, la catégorie **Ann** des anneaux. On pourra aussi considérer la catégorie **Com** des anneaux commutatifs.

iv) On peut aussi considérer la catégorie **Top** dont les objets sont les espaces topologiques et les morphismes sont les applications continues.

Bien sûr, il y a aussi les catégories **Met** et **Comp** des espaces métriques et des espaces complets, les morphismes étant les applications uniformément continues.

v) On dispose de la catégorie **GrT** des groupes topologiques (avec homomorphismes continus), de la catégorie **R-evt** des **R**-espaces vectoriels topologiques (avec applications linéaires continues).

De même, on peut regarder les catégories **R-evn** (resp. **Ban**) des **R**-espaces vectoriels normés (resp. des Banach) avec les applications linéaires contractantes.

vi) Si G est un monoïde, on peut considérer la catégorie **G** qui a pour seul objet G, dont les morphismes sont les éléments de G et où la composition est la multiplication.

vii) On peut considérer un ensemble ordonné $(I, \leq)$ comme une catégorie. En effet, les objets sont les éléments de I et pour tout $i, j \in I$, il y a un unique morphisme $i \to j$ si $i \leq j$ et aucun sinon.

Comme cas particulier, on peut prendre un espace topologique X et la catégorie $\mathbf{Ouv}(X)$ des ouverts de X.

4.1.3 Définition

Une catégorie est *petite* si ses objets forment un ensemble.
Elle est *finie* s'il y a un nombre fini de morphismes (et donc d'objets).

4.1.4 Exemple

Un ensemble ordonné $(I, \leq)$, et donc en particulier la catégorie $\mathbf{Ouv}(X)$ si X est un espace topologique, est une petite catégorie. De même, si G est un monoïde, la catégorie $\mathbf{G}$ est petite. Aussi, si A est un anneau, $\mathbf{Mat}_A$ est petite.

4.1.5 Définition

Si $\mathcal{C}$ et $\mathcal{C}'$ sont deux catégories, la *catégorie produit* $\mathcal{C} \times \mathcal{C}'$ est la catégorie dont les objets sont les couples (X, X') avec $X \in \mathcal{C}$ et $X' \in \mathcal{C}'$ et les morphismes sont les couples de morphismes. La composition est définie de manière évidente.

4.1.6 Définition

La *catégorie opposée*ou *duale* à $\mathcal{C}$ est la catégorie $\mathcal{C}^{op}$ qui a les mêmes objets que $\mathcal{C}$ avec pour tout X, Y,

$$\mathrm{Hom}_{\mathcal{C}^{op}}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X).$$

La composition est définie de manière évidente.

4.1.7 Exemple

La catégorie duale de $(I, \leq)$ est $(I, \geq)$.

4.1.8 Définition

Une *sous-catégorie* $\mathcal{C}'$ d'une catégorie $\mathcal{C}$ est une catégorie dont les objets forment une sous-collection de celle des objets de $\mathcal{C}$, pour $X, Y \in \mathcal{C}'$, les morphismes $X \to Y$ forment une partie de $\mathrm{Hom}_{\mathcal{C}}(X, Y)$, la composition est induite par celle de $\mathcal{C}$ et les identités sont celles de $\mathcal{C}$. On écrit parfois $\mathcal{C} \subset \mathcal{C}'$.
On dit que la sous-catégorie est *pleine* si

$$\forall X, Y \in \mathcal{C}', \mathrm{Hom}_{\mathcal{C}'}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(X, Y).$$

4.1.9 Exemples

La catégorie **Ab** est une sous-catégorie pleine de **Gr** qui est elle même une sous-catégorie pleine de **Mon**. De même, la catégorie **Com** est une sous-catégorie pleine de **Ann**.
Si $H \subset G$ est un sous-monoïde, alors $\mathbf{H} \subset \mathbf{G}$.
Si K est un corps, K–**evf** est une sous-catégorie pleine de K–**ev**.
Enfin, **Comp** est une sous-catégorie pleine de **Met**.

4.2 Structure interne

4.2.1 Définitions

On dit que

$$f \in \mathrm{End}_{\mathcal{C}}(X) := \mathrm{Hom}_{\mathcal{C}}(X, X)$$

est un *endomorphisme* de X.
Soit $f : X \to Y$ un morphisme.
Une *rétraction* ou un *inverse à gauche*pour f est un morphisme $g : Y \to X$ tel que $g \circ f = \mathrm{Id}_X$.
Une *section*ou un *inverse à droite*pour f est un morphisme $g : Y \to X$ tel que g soit une rétraction pour f dans $\mathcal{C}^{op}$.

4.2.2 Proposition

Si $f : X \to Y$ possède à la fois une rétraction g et une section h, alors celles-ci sont uniques et on a $h = g$.

4.2.3 Définitions

On dit alors que f est un *isomorphisme*. On écrit $f : X \tilde{\to} Y$ et on pose $f^{-1} := g$, c'est l'*inverse*de f.
On dit que $f : Y \to X$ est un *monomorphisme*si

$$\forall g \neq h : Z \to Y, f \circ g \neq f \circ h.$$

On dit que c'est un *épimorphisme* si c'est un monomorphisme dans $\mathcal{C}^{op}$.

4.2.4 Exemples

i) Dans **Ens**, un isomorphisme est une bijection. De plus, un mono- (resp. épi-) morphisme est une application injective (resp. surjective) et elle possède toujours un inverse à gauche (resp. droite).

ii) Dans A-**Mod**, les mono- (resp. épi-, resp. iso-) morphismes sont les morphismes injectifs (resp. surjectifs, resp. bijectifs). Mais un mono- (resp. épi-) morphisme n'a pas nécessairement d'inverse à gauche (resp. droite).

iii) Dans **Top**, les mono- (resp. épi-) morphismes sont les morphismes injectifs (resp. surjectifs) mais ils n'ont pas nécessairement de rétraction (resp. section). En fait, une application continue bijective n'est pas nécessairement un homéomorphisme (c'est à dire un isomorphisme).

iv) Dans **Ann**, les mono- (resp. iso-) morphismes sont les morphismes injectifs (resp. bijectifs). Un morphisme surjectif est un épimorphisme, mais il existe des monomorphismes qui sont aussi des épimorphismes mais ne sont pas bijectifs ($\mathbf{Z} \to \mathbf{Q}$ par exemple).

4.2.5 Proposition

i) Un morphisme qui possède une rétraction est toujours un monomorphisme (et dual).

ii) Le composé de deux monomorphismes est un monomorphisme (et dual).

iii) Si $g \circ f$ est un monomorphisme, f aussi (et dual).

4.3 Propriétés universelles

4.3.1 Définition

Un objet $X \in \mathcal{C}$ est *final* si

$$\forall Y \in \mathcal{C}, \exists! f : Y \to X.$$

Un objet de $\mathcal{C}$ est dit *initial* si c'est un objet final de $\mathcal{C}^{op}$.

4.3.2 Exemples

Dans **Ens** ou **Top**, un objet est final si et seulement si l'ensemble sous-jacent possède un unique élément. Et $\emptyset$ est l'unique objet initial.
Dans A-**Mod**, un objet est initial si et seulement s'il est final si et seulement s'il est réduit à zéro.
Dans **Ann**, un objet est final si et seulement s'il est réduit à zéro, et $\mathbf{Z}$ est un objet initial.
Dans $(I, \leq)$ un objet initial (resp. final) n'est autre qu'un plus petit (resp. grand) élément.

4.3.3 Proposition

Un objet final est unique à unique isomorphisme près (et dual).

4.3.4 Définition

Soit $(X_i)_{i \in I}$ une famille d'objets de $\mathcal{C}$. Un *produit* des X_i est un objet X, muni de *projections* $p_i : X \twoheadrightarrow X_i$, tel que

$$\forall (f_i : Y \to X_i)_{i \in I}, \exists! f : Y \to X,$$

$$\forall i \in I, p_i \circ f = f_i.$$

La notion duale est celle de *somme*.

4.3.5 Exemples

Dans **Ens**, le produit est le produit cartésien et la somme est l'union disjointe.
Dans **Top**, on trouve les mêmes objets avec la topologie appropriée.
Dans A-**Mod**, le produit et la somme sont le produit cartésien et la somme directe.
Dans A-**Alg**, le produit est le produit cartésien et la somme est le produit tensoriel.
Enfin, dans $(I, \leq)$ le produit d'une famille est la borne inférieure si elle existe.

4.3.6 Proposition

i) Si on se donne une famille de morphismes

$$(f_i : X_i \to Y_i)_{i \in I}$$

et si X (resp. Y) est le produit des X_i (resp. Y_i) avec projections p_i (resp. q_i),

$$\exists! f : X \to Y, \forall i \in I, q_i \circ f = f \circ p_i$$

(et dual).

ii) Si X (resp. X') est un produit des X_i avec projections p_i (resp. p'_i), il existe un unique isomorphisme

$$f : X \tilde{\to} X'$$

tel que

$$\forall i \in I, p'_i \circ f = p_i$$

(et dual).

4.3.7 Remarque

Soit Y un produit de X par lui même avec projections p_1, p_2. Alors,

$$\exists! \delta_X : X \to Y, p_1 \circ \delta = p_2 \circ \delta = Id_X.$$

C'est un monomorphisme appelé *plongement diagonal*.

4.3.8 Définition

Un *noyau* de

$$f_1, f_2 : X \to Y$$

est un objet Z muni d'un morphisme $i : Z \to X$ tel que

$$f_1 \circ i = f_2 \circ i$$

et

$$\forall g : T \to X, f_1 \circ g = f_2 \circ g \Rightarrow$$
$$\exists! h : T \to Z, g = i \circ h.$$

On dit alors que la suite

$$Z \to X \underset{\longrightarrow}{\overset{f_1}{\longrightarrow}} Y$$

est *exacte à gauche*.
On définit dualement les notions de *conoyau*et de *suite exacte à droite*.

4.3.9 Exemples

Dans **Ens**, le noyau de $f, g : E \to F$ est

$$\{x \in E, f(x) = g(x)\}$$

et le conoyau est le quotient de F par la plus petite relation d'équivalence telle que $f(x) \sim g(x)$ si $x \in E$.
Dans **Top**, on trouve les mêmes ensembles avec la topologie appropriée.
Dans A-**Mod**, le noyau de $f, g : M \to N$ est $\ker(g - f)$ et le conoyau est

$$\operatorname{coker}(g - f) := N/\operatorname{Im}(g - f).$$

4.3.10 Proposition

i) Si $i : Z \to X$ (resp. $i' : Z' \to X'$) fait de Z (resp. Z') un noyau de

$$f, g : X \to Y$$

(resp.

$$f', g' : X' \to Y')$$

et si

$$\varphi : X \to X', \psi : Y \to Y'$$

sont deux morphismes tels que

$$\psi \circ f = f' \circ \varphi \text{ et } \psi \circ g = g' \circ \varphi,$$

il existe un unique $\lambda : Z \to Z'$ tel que

$$i' \circ \lambda = \varphi \circ i$$

(et dual).

ii) Si $i : Z \to X$ et $i' : Z' \to X'$ font de Z et Z' des noyaux de

$$f, g : X \to Y,$$

il existe un unique isomorphisme $\lambda : Z \tilde{\to} Z'$ tel que $i' \circ \lambda = i$ (et dual).

iii) Si $i : Z \to X$ fait de Z un noyau de

$$f, g : X \to Y,$$

c'est un monomorphisme (et dual).

iv) Soient
$$f, g : X \to Y$$
deux morphismes et $j : Y \to Y'$ un monomorphisme, alors Z est un noyau de f, g si et seulement si c'est un noyau de
$$j \circ f, j \circ g : X \to Y'$$
(et dual).

4.3.11 Définition

Un *produit fibré* de
$$f_1 : X_1 \to Y, f_2 : X_2 \to Y$$
est un objet X muni de deux *projections*
$$p_1 : X \twoheadrightarrow X_1, p_2 : X \twoheadrightarrow X_2$$
tel que
$$f_1 \circ p_1 = f_2 \circ p_2$$
et
$$\forall g_1 : Z \to X_1, g_2 : Z \to X_2,$$
$$(f_1 \circ g_1 = f_2 \circ g_2 \Rightarrow$$
$$\exists! g : Z \to X, g_1 = p_1 \circ g \text{ et } g_2 = p_2 \circ g).$$
On dit alors que le carré
$$\begin{array}{ccc} X & \longrightarrow & X_1 \\ \downarrow & & \downarrow \\ X_2 & \longrightarrow & Y \end{array}$$
est *cartésien*. On définit dualement les notions de *somme amalgamée*et de *carré co-cartésien*.

4.3.12 Exemples

Le produit fibré de
$$f_1 : X_1 \to Y, f_2 : X_2 \to Y$$
dans **Ens**, **Top** ou A-**Mod** est
$$\{(x_1, x_2) \in X_1 \times X_2, f_1(x_1) = f_2(x_2)\}$$
avec la structure induite dans les deux derniers cas.
La somme amalgamée de deux morphismes d'anneaux commutatifs $f : A \to B$ et $g : A \to C$ est $B \otimes_A C$.
Dans **Ens**, **Top** ou A-**Mod**, si $Z \subset X$, le diagramme
$$\begin{array}{ccc} f^{-1}(Z) & \hookrightarrow & X \\ \downarrow & & \downarrow f \\ Z & \hookrightarrow & Y \end{array}$$
est cartésien.

4.3.13 Proposition

i) Si
$$p_1 : X \to X_1, p_2 : X \to X_2$$
font de X un produit fibré de
$$f_1 : X_1 \to Y, f_2 : X_2 \to Y,$$
si
$$p'_1 : X' \to X'_1, p'_2 : X' \to X'_2$$
font de X' un produit fibré de
$$f'_1 : X'_1 \to Y', f'_2 : X'_2 \to Y'$$
et si
$$\psi : Y \to Y', \varphi_1 : X_1 \to X'_1, \varphi_2 : X_2 \to X'_1$$
sont tels que
$$\psi \circ f'_1 = f_1 \circ \varphi_1 \text{ et } \psi \circ f'_2 = f_2 \circ \varphi_2,$$
alors, il existe un unique $\varphi : X \to X'$ tel que
$$p'_1 \circ \varphi = \varphi_1 \circ p_1 \text{ et } p'_2 \circ \varphi = \varphi_2 \circ p_2$$
(et dual).

ii) Si X et X' sont des produits fibrés de
$$f_1 : X_1 \to Y, f_2 : X_2 \to Y$$
avec projections p_1, p_2 dans le premier cas et p'_1, p'_2 dans le second, il existe un unique isomorphisme $\varphi : X \tilde{\to} X'$ tel que
$$p'_1 \circ \varphi = p_1 \text{ et } p'_2 \circ \varphi = p_2$$
(et dual).

iii) Dans un diagramme cartésien
$$\begin{array}{ccc} X' & \xrightarrow{f'} & Y' \\ \downarrow & & \downarrow \\ X & \xrightarrow{f} & Y \end{array},$$
si f est un monomorphisme, f' aussi (et dual).

iv) Un morphisme $f : X \to Y$ est un monomorphisme si et seulement si le diagramme
$$\begin{array}{ccc} X & \xrightarrow{\mathrm{Id}_X} & X \\ \downarrow \mathrm{Id}_X & & \downarrow f \\ X & \xrightarrow{f} & Y \end{array},$$
est cartésien (et dual).

4.3.14 Remarque

Si $f : X \to Y$ est un morphisme et si le produit $X \times Y$ existe, il existe un unique

$$\Gamma : X \to X \times Y,$$

tel que

$$p_X \circ \Gamma = \mathrm{Id}_X \text{ et } p_Y \circ \Gamma = f.$$

C'est le *graphe* de f et si $Y \times Y$ existe, on a un diagramme cartésien

$$\begin{array}{ccc} X & \overset{\Gamma}{\hookrightarrow} & X \times Y \\ \downarrow f & & \downarrow f \times \mathrm{Id}_Y \\ Y & \overset{\delta}{\hookrightarrow} & Y \times Y \end{array} .$$

4.3.15 Proposition

i) Si $\mathcal{C}$ possède un objet final 0, alors un produit de X et Y n'est autre qu'un produit fibré au dessus de 0 (et dual). De plus 0 est le produit vide (et dual).

ii) Si X est un produit de X_1 et X_2 avec projections p_1, p_2, alors un noyau de

$$f_1 \circ p_1, f_2 \circ p_2 : X \to Y$$

est un produit fibré de

$$f_1 : X_1 \to Y, f_2 \to Y$$

(et dual).

iii) Si Z est un produit de Y par lui même avec projections p_1, p_2, et si

$$f_1, f_2 : X \to Y,$$

il existe un unique $f : X \to Z$ tel que

$$p_1 \circ f = f_1 \text{ et } p_2 \circ f = f_2$$

et alors, un produit fibré de f et de δ_Y est un noyau de f_1, f_2 (et dual).

4.4 Foncteurs

4.4.1 Définition

Un *foncteur (covariant)* $F : \mathcal{C} \to \mathcal{C}'$ est une opération qui associe à tout $X \in \mathcal{C}$ un objet

$$F(X) \in \mathcal{C}$$

et a tout $f : X \to Y$ un morphisme

$$F(f) : F(X) \to F(Y).$$

On demande que soient satisfaites les propriétés suivantes :

i)
$$\forall X \in \mathcal{C}, F(\mathrm{Id}_X) = \mathrm{Id}_{F(X)}\,.$$

ii)
$$\forall f : X \to Y, g : Y \to Z, F(g \circ f) = F(g) \circ F(f).$$

Un *foncteur contravariant* $F : \mathcal{C} \to \mathcal{C}'$ est un foncteur (covariant) $F : \mathcal{C}^{op} \to \mathcal{C}'$.

4.4.2 Exemples

i) On dispose des foncteurs "oubli" évidents

$$A\text{-}\mathbf{Mod} \to \mathbf{Ens}, \mathbf{Ann} \to \mathbf{Ab}, \mathbf{Ann} \to \mathbf{Mon}, ...$$

Ou si $A \to B$ est un morphisme d'anneaux, B-**Mod** $\to$ A-**Mod**, de restriction des scalaires. De même, on a les foncteurs "oubli"

$$\mathbf{Top} \to \mathbf{Ens}, \mathbf{R\text{-}evn} \to \mathbf{R\text{-}ev}, ...$$

ii) On a le foncteur d'abélianisation

$$\mathbf{Gr} \to \mathbf{Ab}, G \mapsto G^{ab} := G/[G, G].$$

On peut aussi considérer les foncteurs de complétion

$$X \mapsto \hat{X}, \mathbf{Met} \to \mathbf{Comp}, \mathbf{R\text{-}evn} \to \mathbf{Ban}.$$

Où encore les foncteurs

$$X \mapsto X^{disc}, X \mapsto X^{gross}, \mathbf{Ens} \to \mathbf{Top}$$

qui munissent un ensemble de la topologie discrète ou grossière.

iii) On dispose du foncteur "module libre"

$$E \mapsto A^{(E)}, \mathbf{Ens} \to A\text{-}\mathbf{Mod}$$

et du foncteur "monoïde abélien libre"

$$E \mapsto \mathbf{N}^{(E)}, \mathbf{Ens} \to \mathbf{Mon}.$$

On a aussi le foncteur "algèbre du monoïde"

$$G \mapsto A^{(G)}, \mathbf{Mon} \to A\text{-}\mathbf{Alg}$$

si A est un anneau commutatif ou encore "algèbre de polynômes"

$$E \mapsto A[E], \mathbf{Ens} \to A\text{-}\mathbf{Alg}.$$

iv) On a le foncteur évident $\mathbf{Mat}_A \to A\text{-}\mathbf{Mod}$. On a aussi les foncteurs $GL_n : \mathbf{Ann} \to \mathbf{Gr}$ et en particulier, le foncteur $A \mapsto A^*$. Enfin, on peut regarder le foncteur de dualité

$$M \mapsto \check{M} := \mathrm{Hom}_A(M, A)$$

de A-**Mod** dans lui même si A est un anneau commutatif.

v) Si A est un anneau, on peut définir des foncteurs

$$\mathrm{Hom} : A\text{-}\mathbf{Mod}^{op} \times \mathbf{Ab} \to \mathbf{Mod}\text{-}A$$

et

$$\otimes : \mathbf{Mod}\text{-}A \times A\text{-}\mathbf{Mod} \to \mathbf{Ab}.$$

Bien sûr, si A est commutatif, on obtient des foncteurs

$$A\text{-}\mathbf{Mod}^{op} \times A\text{-}\mathbf{Mod} \to A\text{-}\mathbf{Mod}$$

et

$$\otimes : A\text{-}\mathbf{Mod} \times A\text{-}\mathbf{Mod} \to A\text{-}\mathbf{Mod}.$$

Si $A \to B$ est un morphisme d'anneaux, on a le foncteur d'extension des scalaires

$$A\text{-}\mathbf{Mod} \to B\text{-}\mathbf{Mod}, M \to B \otimes_A M.$$

vi) Un foncteur covariant $(I, \leq) \to (J, \leq)$ est une application croissante. Toute application continue $f : X \to Y$ fournit un foncteur

$$f^{-1} : Ouv(Y) \to Ouv(X).$$

On peut considérer la catégorie **Cat** des petites catégories et des foncteurs. On a alors un foncteur

$$\mathbf{Top}^{op} \to \mathbf{Cat}, X \mapsto Ouv(X), f \mapsto f^{-1}.$$

4.4.3 Définition

Si $F : \mathcal{C} \to \mathcal{C}'$ et $G : \mathcal{C}' \to \mathcal{C}''$ sont deux foncteurs, on défini leur *composé*

$$G \circ F : \mathcal{C} \to \mathcal{C}''$$

par

$$(G \circ F)(X) = G(F(X)) \text{ et } (G \circ F)(f) = G(F(f)).$$

Aussi, si $\mathcal{C}$ est une catégorie, le foncteur *identité*

$$\mathrm{Id}_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$$

est défini par

$$\mathrm{Id}_{\mathcal{C}}(X) = X \text{ et } \mathrm{Id}_{\mathcal{C}}(f) = f.$$

4.4.4 Remarques

i) Si $\mathcal{C}' \subset \mathcal{C}$, on a un foncteur d'inclusion $\mathcal{C}' \hookrightarrow \mathcal{C}$.

ii) Si $\mathcal{C}$ et $\mathcal{C}'$ sont deux catégories, on dispose du foncteur évident de "projection"

$$\mathcal{C} \times \mathcal{C}' \to \mathcal{C}.$$

De même, si on fixe $X \in \mathcal{C}$, on peut considérer le foncteur

$$\mathcal{C}' \to \mathcal{C} \times \mathcal{C}', Y \mapsto (X, Y), f \mapsto (\mathrm{Id}_X, f)$$

(et symétriquement).

iii) Si $\mathcal{C}$ est une catégorie, on peut considérer le foncteur

$$\mathrm{Hom} : \mathcal{C}^{op} \times \mathcal{C} \to \mathbf{Ens}$$

qui envoie (X, Y) sur $\mathrm{Hom}(X, Y)$, et un couple

$$(f : X' \to X, g : Y \to Y')$$

de morphismes de $\mathcal{C}$, sur l'application

$$\mathrm{Hom}(X, Y) \to \mathrm{Hom}(X', Y'), h \mapsto g \circ h \circ f.$$

Par composition, on obtient des foncteurs

$$h^X : \mathcal{C} \to \mathbf{Ens}, Y \mapsto \mathrm{Hom}(X, Y)$$

et

$$h_Y : \mathcal{C}^{op} \to \mathbf{Ens}, X \mapsto \mathrm{Hom}(X, Y).$$

iv) Il revient au même de se donner un foncteur (covariant) $F : \mathcal{C} \to \mathcal{C}'$ ou un foncteur (covariant) $F : \mathcal{C}^{op} \to \mathcal{C}'^{op}$. Cela permet de définir le composé de deux foncteurs contravariants ou de deux foncteurs de différentes variances.

Remarquons pour finir que l'on a toujours

$$H \circ (G \circ F) = (H \circ G) \circ F.$$

4.4.5 Remarque

Un foncteur préserve les sections, les rétractions par dualité et donc aussi les isomorphismes. Mais il ne préserve pas toujours les monomorphismes, ni les épimorphismes.

4.4.6 Définition

Un foncteur $F : \mathcal{C} \to \mathcal{C}'$ est *fidèle*(resp. *pleinement fidèle*)si pour tout $X, Y \in \mathcal{C}$, l'application

$$\mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{C}'}(F(X), F(Y))$$

est injective (resp. bijective).
Il est *essentiellement surjectif* si tout objet de $\mathcal{C}'$ est isomorphe à un objet de la forme $F(X)$.
Une catégorie $\mathcal{C}$ est *concrète* s'il existe un foncteur fidèle $\mathcal{C} \to \mathbf{Ens}$ appelé foncteur oubli.

4.4.7 Exemples

Les catégories A-**Mod**, **Ann**, **Mon**, **Top**, **R-evn**, etc. sont concrètes. Le foncteur $\mathbf{Mat}_A \to A$-**mod** est pleinement fidèle. Le foncteur $\mathbf{Mat}_K \to K$-**evf** est essentiellement surjectif.

4.4.8 Proposition

i) Le composé de deux foncteurs (pleinement) fidèles est (pleinement) fidèle.

ii) Un foncteur d'inclusion $\mathcal{C}' \hookrightarrow \mathcal{C}$ est toujours fidèle. Il est pleinement fidèle s'il fait de $\mathcal{C}'$ une sous-catégorie pleine de $\mathcal{C}$.

iii) Si F est pleinement fidèle et $F(X)$ isomorphe à $F(Y)$, alors X est isomorphe à Y.

iv) Si F est fidèle et $F(f)$ est un monomorphisme, alors f aussi (et dual).

4.4.9 Exemple

Dans une catégorie concrète, tout morphisme injectif (resp. surjectif) est un mono- (resp. épi-) morphisme.

4.5 Transformations naturelles

4.5.1 Définition

Soient $F, G : \mathcal{C} \to \mathcal{C}'$ deux foncteurs. Une *transformation naturelle*

$$\alpha : F \to G$$

est une collection de morphismes

$$\alpha_X : F(X) \to G(X)$$

pour $X \in \mathcal{C}$ telle que

$$\forall f : X \to Y, G(f) \circ \alpha_X = \alpha_Y \circ F(f).$$

4.5.2 Exemples

i) Le déterminant
$$\det_A : GL_n(A) \to A^*$$
défini une transformation naturelle entre le foncteur GL_n et le foncteur $A \mapsto A^*$ de **Ann** $\to$ **Gr**.

ii) De même, la projection $G \twoheadrightarrow G^{ab}$ est naturelle (entre le foncteur $\mathrm{Id}_{\mathbf{Gr}}$ et le foncteur composé du foncteur d'abélianisation **Gr** $\to$ **Ab** et du foncteur d'inclusion **Ab** $\hookrightarrow$ **Gr**).

iii) Si A est un anneau commutatif, le morphisme de M dans son bidual
$$M \to \check{\check{M}}, m \mapsto (u \mapsto u(m))$$
est naturel (entre le foncteur Id sur A-**Mod** et le foncteur bidual, second itéré du foncteur dual).

4.5.3 Définitions

La transformation
$$\mathrm{Id}_F : F \to F$$
définie par
$$\mathrm{Id}_{FX} = \mathrm{Id}_{F(X)}$$
est l'*identité naturelle*
La *composée*de
$$\alpha : F \to G \text{ et } \beta : G \to H$$
est donnée par
$$(\beta \circ \alpha)_X = \beta_X \circ \alpha_X.$$
On dit que $\alpha : F \to G$ est un *isomorphisme naturel*s'il existe $\beta : G \to F$ tel que
$$\beta \circ \alpha = \mathrm{Id}_F \text{ et } \alpha \circ \beta = \mathrm{Id}_G\,.$$
On dit qu'un foncteur $F : \mathcal{C} \to \mathcal{C}'$ est une *équivalence de catégories* s'il existe $G : \mathcal{C}' \to \mathcal{C}$ tel que
$$G \circ F \simeq \mathrm{Id}_{\mathcal{C}} \text{ et } F \circ G \simeq \mathrm{Id}_{\mathcal{C}'}\,.$$

4.5.4 Exemples

i) Si A est un anneau commutatif et M un A-module libre de rang fini, l'isomorphisme de bidualité $M \tilde{\to} \check{\check{M}}$ est naturel.
Par contre, bien que, si K est un corps, le foncteur dual $M \mapsto \check{M}$ est une équivalence de catégories de K-**evf** dans lui même, il n'y a pas d'isomorphisme naturel $M \tilde{\to} \check{M}$ dans K-**evf**.

ii) Le foncteur
$$\mathbf{Mat}_K \to K\text{-}\mathbf{evf}, n \to K^n$$
est une équivalence de catégories.

iii) Soit A-**Op** la catégorie des A-modules à opérateurs : les objets sont les couples (M, u) avec
$$M \in A\text{-}\mathbf{Mod} \text{ et } u \in \mathrm{End}_A(M).$$
Un morphisme $(M, u) \to (N, v)$ est un homomorphisme $f : M \to N$ tel que $f \circ u = v \circ f$.
Alors A-**Op** est équivalente à $A[X]$-**Mod**.

4.5.5 Remarques

Pour des transformations naturelles, on a toujours
$$(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma).$$
Une transformation naturelle α est un isomorphisme si et seulement si pour tout X, α_X en est un.
Enfin, si $f : X \to Y$ est un morphisme dans une catégorie $\mathcal{C}$, on a une transformation naturelle $h^f : h^Y \to h^X$ donnée par
$$\mathrm{Hom}(Y, Z) \to \mathrm{Hom}(X, Z), g \to g \circ f.$$
et de même, $h_f : h_X \to h_Y$ donnée par
$$\mathrm{Hom}(Z, X) \to \mathrm{Hom}(Z, Y), g \to f \circ g.$$

4.5.6 Théorème

Un foncteur est une équivalence de catégories si et seulement s'il est pleinement fidèle et essentiellement surjectif.

4.6 Foncteurs représentables

4.6.1 Définition

On dit qu'un foncteur $F : \mathcal{C} \to \mathbf{Ens}$ est *représentable* par $X \in \mathcal{C}$ s'il est naturellement isomorphe au foncteur h^X.

4.6.2 Exemples

i) Le foncteur "oubli" sur **Gr** est représentable par **Z**.
Le foncteur "oubli" sur A-**Mod** est représentable par A.
Le foncteur "oubli" sur **Top** est représentable par 0.
Le foncteur "oubli" sur A-**Alg** est représentable par $A[T]$.
Le foncteur "oubli" sur la catégorie **Grf** des groupes finis n'est pas représentable.

ii) Si A est un anneau commutatif et $S \subset A$, le foncteur

$$B \to \{\phi : A \to B, \phi(S) \subset B^*\}$$

est représentable par $A[S^{-1}]$.

iii) Le foncteur

$$P \to \mathrm{Bil}((M,N),P)$$

est représentable par $M \otimes_A N$.

4.6.3 Théorème (Lemme de Yoneda)

Soit $F : \mathcal{C} \to \mathbf{Ens}$ un foncteur et $X \in \mathcal{C}$. Alors, les transformations naturelles $h^X \to F$ forment un ensemble noté $\mathrm{Hom}(h^X, F)$.
De plus, on a une bijection

$$F(X) \simeq \mathrm{Hom}(h^X, F)$$

donnée comme suit :
A $s \in F(X)$, on associe la transformation naturelle $\alpha : h^X \to F$ définie par

$$\alpha_Y : h^X(Y) \to F(Y), f \mapsto F(f)(s)$$

pour $Y \in \mathcal{C}$. La réciproque est donnée par

$$\alpha \mapsto \alpha_X(\mathrm{Id}_X).$$

4.6.4 Proposition

i) Un foncteur $F : \mathcal{C} \to \mathbf{Ens}$ est représentable par $X \in \mathcal{C}$ si et seulement si

$$\exists s \in F(X), \forall Y \in \mathcal{C}, \forall t \in F(Y),$$

$$\exists! f : X \to Y, F(f)(s) = t.$$

ii) Si X et X' représentent le même foncteur à l'aide de s et s', il existe un unique isomorphisme $f : X \tilde{\to} X'$ tel que $F(f)(s) = s'$.

4.6.5 Définition

Avec les notations du (i) ci dessus, on dit que X, muni de s, est *universel*pour les $t \in F(Y)$ dans $\mathcal{C}$.

4.6.6 Exemples

On voit que $M \otimes_A N$ est universel pour les applications bilinéaires $M \times N \to P$.
Ou encore, que $A[T]$ est universel pour les éléments de A-algèbres.
Un autre exemple est donné par le corps de rupture d'un polynôme irréductible qui est universel pout les racines de ce polynômes dans une extension du corps.

4.6.7 Proposition

i) Un objet est final si et seulement s'il représente le foncteur contravariant

$$Y \mapsto 0$$

(et dual).

ii) Un objet est un produit des X_i si et seulement s'il représente le foncteur

$$Y \mapsto \prod \mathrm{Hom}(Y, X_i)$$

(et dual).

iii) Un objet est un noyau de

$$f, g : X \to Y$$

si et seulement s'il représente le foncteur

$$Z \mapsto \ker(h_f^Z, h_g^Z : \mathrm{Hom}(Z, X) \to \mathrm{Hom}(Z, Y))$$

(et dual).

iv) Un objet est un produit fibré de

$$f_1 : X_1 \to Y, f_2 : X_2 \to Y$$

si et seulement s'il représente le foncteur

$$Z \mapsto \mathrm{Hom}(Z, X_1) \times_{\mathrm{Hom}(Z,Y)} \mathrm{Hom}(Z, X_2)$$

(et dual).

4.7 Diagrammes et limites

4.7.1 Définition

Soit $\mathcal{C}$ une catégorie quelconque et I une petite catégorie.
Un *diagramme commutatif* de base I dans $\mathcal{C}$ est un foncteur $D : I \to \mathcal{C}$ ou I est une petite catégorie.
Un *morphisme* entre deux diagrammes commutatifs est une transformation naturelle.

4.7.2 Remarque

Se donner un diagramme commutatif de base I dans $\mathcal{C}$ revient à se donner une famille $(X_i)_{i \in I}$ d'objet de $\mathcal{C}$ et pour tout $u : i \to j$ un morphisme

$$f_u : X_i \to X_j$$

tel que

$$\forall v : j \to k, f_{v \circ u} = f_v \circ f_u.$$

On voit alors qu'un morphisme de diagrammes $(X_i, f_u) \to (Y_i, g_u)$ est la donnée de morphismes $h_i : X_i \to Y_i$ satisfaisant pour tout $u : i \to j$, $g_u \circ h_i = h_j \circ f_u$.

4.7.3 Remarque

Les diagrammes commutatifs de base I dans $\mathcal{C}$ forment une catégorie $\mathcal{C}^I$ avec les transformations naturelles pour morphismes. On identifie $\mathcal{C}$ avec $\mathcal{C}^0$, ou 0 désigne la catégorie triviale.

4.7.4 Proposition

i) Si I est une petite catégorie et $F : \mathcal{C} \to \mathcal{C}'$ un foncteur, il existe un unique foncteur

$$F^I : \mathcal{C}^I \to \mathcal{C}'^I$$

tel que

$$F^I(D) = F \circ D$$

si $D \in C^I$ et

$$F^I(T)_i = F(T_i)$$

si T est un morphisme de $\mathcal{C}^I$ et $i \in I$.
On a toujours $(G \circ F)^I = G^I \circ F^I$.

ii) Si $\lambda : I \to J$ est un morphisme entre petites catégories et $\mathcal{C}$ une catégorie quelconque, il existe un unique foncteur

$$\lambda^* : \mathcal{C}^J \to \mathcal{C}^I$$

tel que

$$\lambda^*(D) = D \circ \lambda$$

si $D \in \mathcal{C}^J$ et

$$\lambda^*(T)_i = T_{\lambda(i)}$$

si T est un morphisme de $\mathcal{C}^J$ et $i \in I$.
On a toujours $(\mu \circ \lambda)^* = \lambda^* \circ \mu^*$.

iii) Si I et J sont deux petites catégories et $\mathcal{C}$ une catégorie quelconque, le foncteur

$$\left(C^I\right)^J \to C^{I \times J}$$

qui envoie $D \in \left(C^I\right)^J$ sur le foncteur

$$(i, j) \mapsto D(j)(i)$$

et

$$(u : i \to i', v : j \to j') \mapsto D(j')(u) \circ D(v)_i$$

est une équivalence de catégories.

4.7.5 Définitions

Le foncteur associé au "foncteur final"

$$0_I : I \to 0,$$

est le *foncteur diagonal*

$$0_I^* : C = C^0 \to C^I$$

qui envoie X sur le *diagramme constant*

$$\underline{X} := 0_I^*(X).$$

4.7.6 Définitions

Si D est un diagramme commutatif de base I dans $\mathcal{C}$ et si le foncteur

$$h^D \circ 0_I^* : Y \to \mathrm{Hom}(D, \underline{Y})$$

est représentable par X, on dit que X est la *limite inductive* de D et on écrit $X = \varinjlim D$.
Si X est la limite inductive d'un diagramme D dans $\mathcal{C}^{op}$, on dit que X est la *limite projective* de D et on écrit $X = \varprojlim D$.
On dit qu'une limite est *finie* si I est une catégorie finie.

4.7.7 Remarques

Par définition, dire que $X = \varprojlim D$ signifie qu'il existe un morphisme $S : \underline{X} \to D$ tel que si $Y \in \mathcal{C}$ et $T : \underline{Y} \to D$ est un morphisme, alors il existe un unique $g : Y \to X$ tel que $T = g \circ S$.
On dispose bien sûr de la notion de limite sur un ensemble ordonné $(I, \leq)$. Si celui-ci est filtrant (resp. cofiltrant), on parle de *limite inductive filtrante*(resp.*projective cofiltrante*).

4.7.8 Remarque

En reprenant les notations ci-dessus, on voit que

$$X = \varprojlim(X_i, f_u)$$

s'il existe une famille

$$(p_i : X \to X_i)_{i \in I}$$

de morphismes de $\mathcal{C}$ tels que

$$\forall u : i \to j, f_u \circ p_i = p_j,$$

et telle que pour toute famille

$$(g_i : Y \to X_i)_{i \in I}$$

de morphismes de $\mathcal{C}$ satisfaisant

$$\forall u : i \to j, f_u \circ g_i = g_j,$$

il existe un unique morphisme $g : Y \to X$ tel que pour tout $i \in I$, on ait $g_i = p_i \circ g$. En particulier, on voit que l'objet final, les produits, les noyaux et les produits fibrés sont des limites projectives. Dualement, l'objet initial, les sommes, les conoyaux et les sommes amalgamées sont des limites inductives.

4.7.9 Exemples

Toutes les limites projectives et inductives existent dans **Ens**, **Top**, **Gr**, A-**Mod** ou **Ann**.

4.7.10 Proposition

Si toutes les limite projectives de base I existent dans $\mathcal{C}$, il existe un unique foncteur

$$\varprojlim_I : \mathcal{C}^I \to \mathcal{C}$$

qui envoie le diagramme D sur $\varprojlim D$ et le morphisme $T : D \to E$ sur l'unique morphisme

$$f : X := \varprojlim D \to Y := \varprojlim E$$

rendant commutatif le diagramme

$$\begin{array}{ccc} \underline{X} & \xrightarrow{\underline{f}} & \underline{Y} \\ \downarrow & & \downarrow \\ D & \xrightarrow{T} & E \end{array}$$

(et dual).

4.7.11 Lemme

Soit (X_i, f_u) un diagramme de $\mathcal{C}$. Si

$$X' := \prod_i X_i \text{ et } X'' := \prod_{u:i\to j} X_j,$$

on note

$$p : X' \to X$$

l'unique morphisme qui, composé avec la projection $X'' \twoheadrightarrow X_j$ donne la projection $X' \twoheadrightarrow X_j$, et

$$f : X' \to X'',$$

l'unique morphisme qui, composé avec la projection $X'' \twoheadrightarrow X_j$ donne la composée de la projection $X' \twoheadrightarrow X_i$ et de $f_u : X_i \to X_j$. Si $X = \ker(p, f)$, c'est la limite projective de (X_i, f_u).

4.7.12 Proposition

i) Si tous les noyaux et tous les produits (resp. finis) existent dans $\mathcal{C}$, toutes les limites projectives (resp. finies) existent dans $\mathcal{C}$ (et dual).

ii) Si $\mathcal{C}$ possède un objet final et si tous les produits fibrés existent dans $\mathcal{C}$, toutes les limites projectives finies existent dans $\mathcal{C}$ (et dual).

4.8 Foncteurs Exacts

4.8.1 Définition

Un foncteur $F : \mathcal{C} \to \mathcal{C}'$ est *continu à gauche* (resp. *exact à gauche*)s'il préserve les limites projectives (resp. finies).
On définit dualement la notion de foncteur *continu à droite*(resp. *exact à droite*).
Si les deux conditions sont satisfaites, on dit foncteur *continu*(resp. *exact*).
Attention : la notion de foncteur continu à un autre sens en théorie des Topos.

4.8.2 Exemples

i) Le foncteur "oubli" **Top** $\to$ **Ens**, le foncteur $X \mapsto X^{disc}$ et le foncteur de restriction des scalaires B-**Mod** $\to$ A-**Mod** associé à un homomorphisme d'anneaux $A \to B$ sont continus.

ii) Le foncteur $X \mapsto X^{gross}$, les foncteurs "oubli" en général, les foncteurs d'inclusion et le foncteur

$$N \to \mathrm{Hom}_{\mathbf{Z}}(M, N) : \mathbf{Ab} \to \mathbf{Mod}\text{-}A,$$

si $M \in A$-**Mod**, sont continus à gauche.

iii) Le foncteur d'extension des scalaires

$$A\text{-}\mathbf{Mod} \to B\text{-}\mathbf{Mod},$$

le foncteur $A \mapsto A^{(E)}$, le foncteur $G \to A^{(G)}$, les foncteurs

$$X \mapsto \hat{X}, G \mapsto G^{ab}, N \to M \otimes_A N$$

sont continus à droite.

iv) Si S est une partie multiplicative d'un anneau commutatif A, le foncteur

$$M \to S^{-1}M, A\text{-}\mathbf{Mod} \to S^{-1}A\text{-}\mathbf{Mod}$$

est exact.

4.8.3 Proposition

i) Si tous les noyaux et les produits (resp. finis) existent dans $\mathcal{C}$ et sont préservés par F, alors alors F est continu (resp. exact) à gauche (et dual).

ii) Si $\mathcal{C}$ possède un objet final préservé par F et si tous les produits fibrés existent dans $\mathcal{C}$ et sont préservés par F, alors alors F est exact à gauche (et dual).

4.8.4 Proposition

i) Le composé de deux foncteurs continus (resp. exacts) à gauche est continu (resp. exact) à gauche (et dual).

ii) Un foncteur exact à gauche préserve les monomorphismes (et dual).

iii) Le foncteur
$$h_X : \mathcal{C} \to \mathbf{Ens}, Y \mapsto \mathrm{Hom}(Y, X)$$
est exact à gauche.

4.8.5 Exemple

Soit G un groupe et $\mathcal{F}$ un ensemble de sous-groupes de G ordonné par inclusion. On dispose d'un diagramme commutatif évident
$$D : \mathcal{F} \to \mathbf{Ens}, H \to G/H.$$
Et on peut considérer sa limite projective
$$\hat{G}^{/\mathcal{F}} = \varprojlim G/H$$
et l' application canonique
$$\iota : G \to \hat{G}^{/\mathcal{F}}.$$
Comme le foncteur *disc* préserve les limites projectives, si on munit G/H de la topologie discrète pour $H \in \mathcal{F}$, on voit que $\hat{G}^{/\mathcal{F}}$ est muni d'une structure d'espace topologique et que ι est continu.
Pour la même raison, si les sous-groupes sont distingués, $\hat{G}^{/\mathcal{F}}$ est muni d'une structure de groupe et ι est un homomorphisme de groupes.
Enfin, si les deux conditions sont satisfaites, on obtient un groupe topologique et un homomorphisme de groupes topologiques.
Par exemple, on peut considérer l'ensemble $\mathcal{N}$ de tous les sous-groupes distingués d'indice fini N de G. On dit alors que
$$\hat{G} := \hat{G}^{/\mathcal{F}}$$
est le *complété profini*de G. On dit que G est un *groupe profini*si $G \tilde{\to} \hat{G}$. Par exemple, le groupe de Galois d'une extension galoisienne (infinie) est un groupe profini.
Si A est un anneau, M un A-module, et $\mathfrak{a}$ un idéal bilatère de A, on peut prendre pour $\mathcal{F}$ la famille des $\mathfrak{a}^n M$ et on écrit
$$\hat{M}^{\mathfrak{a}} := \varprojlim M/\mathfrak{a}^n M.$$
On dit que c'est le *complété*de M le long de $\mathfrak{a}$. Toujours parce que les foncteurs en question sont continus à gauche, on voit que $\hat{A}^{\mathfrak{a}}$ est un anneau topologique et que $\hat{M}^{\mathfrak{a}}$ est un $\hat{A}^{\mathfrak{a}}$-module topologique.
Un exemple classique est fourni par l'anneau des entiers p-adiques
$$\mathbf{Z}_p := \varprojlim \mathbf{Z}/p^n$$

pour p premier. Un autre est donné par

$$A[[X_1, \ldots, X_n]]$$

qui est le complété de $A[X_1, \ldots, X_n]$ le long de l'idéal $(X_1, \ldots, X_n)$.

4.9 Foncteurs adjoints

4.9.1 Définition

On dit qu'un foncteur $F : \mathcal{C} \to \mathcal{C}'$ est *adjoint à gauche* à un foncteur $G : \mathcal{C}' \to \mathcal{C}$ si on a un isomorphisme naturel de foncteurs

$$\mathcal{C}^{op} \times \mathcal{C}' \to \mathbf{Ens}$$

$$\mathrm{Hom}(F(X), X') \tilde{\to} \mathrm{Hom}(X, G(X')).$$

On dit aussi que G est *adjoint à droite* à F.

4.9.2 Exemples

i) Le foncteur oubli **Top** $\to$ **Ens** a pour adjoint à gauche (resp. droite) le foncteur $E \mapsto E^{disc}$ (resp. $E \mapsto E^{gross}$).
Le foncteur oubli A-**Mod** $\to$ **Ens** a pour adjoint à gauche le foncteur $E \mapsto A^{(E)}$.
Le foncteur oubli A-**Alg** $\to$ **Mon** a pour adjoint à gauche le foncteur $G \mapsto A^{(G)}$.

ii) Le foncteur $G \mapsto G^{ab}$ est adjoint à gauche au foncteur d'inclusion **Ab** $\hookrightarrow$ **Gr**.
Le foncteur $X \mapsto \hat{X}$ est adjoint à gauche au foncteur d'inclusion

$$\mathbf{Comp} \hookrightarrow \mathbf{Met} \text{ ou } R\text{-}\mathbf{evn} \hookrightarrow \mathbf{Ban}.$$

iii) Si M est un A-module à gauche, le foncteur

$$N \to M \otimes_A N$$

est adjoint au foncteur

$$N \to \mathrm{Hom}(M, N).$$

Le foncteur extension des scalaires est adjoint à gauche au foncteur de restriction des scalaires.

4.9.3 Définition

Si F est adjoint à gauche à G, on note α^X l'image de $Id_{F(X)}$ sous l'isomorphisme

$$\mathrm{Hom}(F(X), F(X)) \tilde{\to} \mathrm{Hom}(X, G(F(X)))$$

et β^X l'antécédent de $Id_{G(X')}$ sous l'isomorphisme

$$\mathrm{Hom}(F(G(X'), X') \tilde{\to} \mathrm{Hom}(G(X'), G(X')).$$

On dit que les transformations naturelles

$$\alpha : \mathrm{Id}_{\mathcal{C}} \to G \circ F$$

et

$$\beta : F \circ G \to \mathrm{Id}_{\mathcal{C}'}$$

sont les *morphismes d'adjonction*.

4.9.4 Exemples

Les morphismes d'adjonction associés au foncteur oubli **Top** $\to$ **Ens** sont l'identité et les applications continues évidentes

$$X^{disc} \to X \text{ et } X \to X^{disc}.$$

Les morphismes d'adjonction associés au foncteur oubli A-**Mod** $\to$ **Ens** sont le morphisme d'inclusion $E \hookrightarrow A^{(E)}$ et le morphisme évident $A^{(M)} \to M$.
Les morphismes d'adjonction associés au foncteur d'inclusion **Ab** $\hookrightarrow$ **Gr** sont l'identité et le morphisme naturel $G \to G^{ab}$.
Les morphismes d'adjonction associés à la complétion sont l'identité et l'inclusion.
Les morphismes d'adjonction associés aux foncteurs de restriction et d'extension des scalaires sont l'identité et le morphisme évident

$$B \otimes_A M \to M, b \otimes m \to bm.$$

4.9.5 Proposition

Le foncteur $F : \mathcal{C} \to \mathcal{C}'$ est adjoint à gauche au foncteur $G : \mathcal{C}' \to \mathcal{C}$ si et seulement s'il existe

$$\alpha : \mathrm{Id}_{\mathcal{C}} \to G \circ F \text{ et } \beta : F \circ G \to \mathrm{Id}_{\mathcal{C}'}$$

tels que les composés

$$F \xrightarrow{\alpha} F \circ G \circ F \xrightarrow{\beta} F$$

et

$$G \xrightarrow{\beta} G \circ F \circ G \xrightarrow{\alpha} G$$

soient les identités de F et de G. Les morphismes α et β sont alors les morphismes d'adjonction.

4.9.6 Proposition

i) Deux adjoins à gauche d'un même foncteur sont isomorphes (et dual).
ii) Si $F : \mathcal{C} \to \mathcal{C}'$ et $F' : \mathcal{C}' \to \mathcal{C}''$ sont adjoints à gauche à G et G' respectivement, alors $F' \circ F$ est adjoint à gauche à $G \circ G'$.
iii) Un foncteur $G : \mathcal{C}' \to \mathcal{C}$ possède un adjoint F à gauche si et seulement si pour tout $X \in \mathcal{C}$, le foncteur $h^X \circ G$ est représentable. Il est alors représenté par $F(X)$ (et dual).
iv) Toutes les limites projectives de base I existent dans $\mathcal{C}$ si et seulement si le foncteur $X \to \underline{X}$ possède un adjoint à droite G et alors $G = \varprojlim_I$ (et dual).

4.9.7 Lemme (d'extension de Kan)

Soit $\lambda : I \to J$ un morphisme de petites catégories.
Pour tout $j \in J$, on note I/j la catégorie dont les objets sont les couples

$$(i, v : \lambda(i) \to j)$$

et les flèches

$$(i, v) \to (i', v')$$

sont les $u : i \to i'$ tels que $v' \circ \lambda(u) = v$. On note encore $j : I/j \to I$ le morphisme $(i, v) \mapsto i$.
Alors, $\lambda^* : \mathcal{C}^J \to \mathcal{C}^I$ possède un adjoint $\lambda_!$ à gauche si et seulement si pour tout $D \in \mathcal{C}^I$ et tout $j \in J$, $\varinjlim_{I/j} j^*D$ existe.
On a alors $\lambda_! D = \varinjlim_{I/j} j^*D$.

4.9.8 Proposition

i) Si $F : \mathcal{C} \to \mathcal{C}'$ est adjoint à gauche à G et si I est une petite catégorie, alors F et G induisent une adjonction entre $\mathcal{C}^I$ et $\mathcal{C}'^I$.

ii) Un foncteur ayant un adjoint à gauche est continu à gauche (et dual).

iii) Soit $F : \mathcal{C} \to \mathcal{C}'$ un foncteur ayant un adjoint G à droite. Alors, G est fidèle (resp. pleinement fidèle) si et seulement si le morphisme d'adjonction

$$\beta : F \circ G \to \mathrm{Id}_{\mathcal{C}'}$$

est un monomorphisme (resp. isomorphisme) (et dual).

iv) Soit $F : \mathcal{C} \to \mathcal{C}'$ un foncteur ayant un adjoint pleinement fidèle G à droite et D un diagramme de $\mathcal{C}'$. Si

$$X = \varinjlim(G \circ D),$$

alors $F(X) = \varinjlim D$ et si

$$Y = \varprojlim(G \circ D),$$

alors $F(Y) = \varprojlim D$ (et dual).

4.9.9 Exemple

On sait que le foncteur d'inclusion $\mathbf{Ab} \hookrightarrow \mathbf{Gr}$ est pleinement fidèle a pour adjoint à droite le foncteur $G \to G^{ab}$.
Si D est un diagramme de groupes abéliens et G sa limite projective (resp. inductive) dans $\mathbf{Gr}$, alors sa limite projective (resp. inductive) dans $\mathbf{Ab}$ est G^{ab}.
Par exemple, si G est le produit libre de deux groupes abéliens G_1 et G_2, alors G^{ab} est la somme directe de G_1 et G_2.

4.10 Catégories additives

4.10.1 Définitions

Une *structure pré-additive* sur une catégorie $\mathcal{C}$ est la donnée pour tout $M, M' \in \mathcal{C}$, d'une structure de groupe abélien sur $\mathrm{Hom}_{\mathcal{C}}(M, M')$ de telle sorte que pour tout $M, M', M'' \in \mathcal{C}$, l'application de composition

$$\mathrm{Hom}_{\mathcal{C}}(M, M') \times \mathrm{Hom}_{\mathcal{C}}(M', M'') \to \mathrm{Hom}_{\mathcal{C}}(M, M'')$$

soit bilinéaire.
On dit qu'un objet M est *nul* si $\mathrm{Id}_M = 0$.
On dit qu'un objet M est *somme directe* de M_1 et M_2 s'il existe

$$p_k : M \to M_k, i_k : M_k \to M, k = 1, 2$$

tels que

$$p_k \circ i_k = \mathrm{Id}_{M_k}, k = 1, 2 \text{ et } i_1 \circ p_1 + i_2 \circ p_2 = \mathrm{Id}_M .$$

4.10.2 Remarque

Il revient au même de munir $\mathcal{C}$ ou $\mathcal{C}^{op}$ d'une structure pré-additive et les notions d'objets nuls et de sommes directes sont autoduales.

4.10.3 Proposition

Supposons que $\mathcal{C}$ est munie d'une structure pré-additive. Alors,
Un objet est nul si et seulement s'il est final (dual).
Un objet M est somme directe de M_1 et M_2 si et seulement si c'est un produit de M_1 et M_2 avec projections p_1, p_2 (dual).

4.10.4 Définition

On dit que $\mathcal{C}$ est une *catégorie additive* s'il existe une structure pré-additive pour laquelle il y a un objet nul 0 et toutes les sommes directes existent.

4.10.5 Remarques

Les catégories A-**Mod**, K-**evf**, $\mathbf{Mat}_A$, **R-evt**, **R-evn** et **Ban** sont additives.
Si $\mathcal{C}$ est une catégorie additive, elle possède une unique structure pré-additive.
Si $\mathcal{C}$ est une catégorie additive, $\mathcal{C}^{op}$ aussi.

4.10.6 Proposition

Soit $\mathcal{C}$ une catégorie additive. Alors,

i) Un morphisme $f : M \to N$ est un monomorphisme si et seulement si chaque fois que $f \circ u = 0$, on a $u = 0$ (et dual).

ii) Dans un diagramme cartésien

$$\begin{array}{ccc} M' & \xrightarrow{f'} & N' \\ \downarrow & & \downarrow \\ M & \xrightarrow{f} & N \end{array},$$

f est un monomorphisme si et seulement si f' en est un (et dual).

4.10.7 Remarque

Si $\mathcal{C}$ est une catégorie additive, on a un foncteur

$$\mathrm{Hom} : \mathcal{C}^{op} \times \mathcal{C} \to \mathbf{Ab}.$$

4.10.8 Définition

Un foncteur $F : \mathcal{C} \to \mathcal{C}'$ entre deux catégories additives est *additif* si pour tout $M, N \in \mathcal{C}$ l'application

$$\mathrm{Hom}(M, N) \to \mathrm{Hom}(F(M), F(N))$$

est un homomorphisme de groupes.

4.10.9 Exemples

Les foncteurs Hom_A et $\otimes_A$ sont additifs. Les foncteurs de restriction et d'extension des scalaires sont aussi additifs.

4.10.10 Proposition

i) Si $\mathcal{C}$ est une catégorie additive, les foncteurs h^M et h_N sont additifs.

ii) Un foncteur est additif si et seulement s'il préserve les sommes directes (et l'objet nul).

iii) Le composé de deux foncteurs additifs est additif.

4.10.11 Remarque

Soit $\mathcal{C}$ une catégorie additive et $G : \mathcal{C}' \to \mathcal{C}$ un foncteur pleinement fidèle ayant un adjoint F à gauche. Alors $\mathcal{C}'$ est additive.

4.10.12 Définition

Soit $\mathcal{C}$ une catégorie additive. On défini le *noyau*$\ker f$ de $f : M \to N$ comme étant le noyau de f et 0 (s'il existe). On définit le *conoyau* $\operatorname{coker} f$ dualement. Ceux-ci sont bien sûr définis à (unique) isomorphisme près.
On dit que $\mathcal{C}$ est *exacte* si tout morphisme possède un noyau et un conoyau. On note alors M/N le conoyau d'un monomorphisme $N \hookrightarrow M$.

4.10.13 Remarques

Les catégories A-**Mod**, K-**evf**, **R-evt**, **R-evn** et **Ban** sont exactes mais pas $\mathbf{Mat_Z}$.
Si $\mathcal{C}$ est exacte, $\mathcal{C}^{op}$ aussi.
Dans une catégorie exacte, toutes les limites finies existent.

4.10.14 Proposition

Soit $\mathcal{C}$ une catégorie exacte. Alors,

i) On a $\ker \mathrm{Id}_M = 0$ et
$$\ker(0 : M \to N) = M$$
(et dual).

ii) Si g est un monomorphisme, alors
$$\ker(g \circ f) = \ker f$$
(et dual).

iii) Un morphisme est un monomorphisme si et seulement si son noyau est nul (et dual).

iv) Si $f : M \to N$ est un morphisme, la projection
$$M \twoheadrightarrow M/\ker f$$
a pour noyau $\ker f$ (dual).

4.11 Catégories abéliennes

4.11.1 Définition

On dit qu'une catégorie exacte $\mathcal{C}$ est *abélienne* si tout monomorphisme (resp. épimorphisme) est un noyau (resp. conoyau).

4.11.2 Remarque

Les catégories A-**Mod** et K-**evf** et **Ban** sont abéliennes mais pas **R-evt** ni **R-evn**.
Si $\mathcal{C}$ est abélienne, $\mathcal{C}^{op}$ aussi.

4.11.3 Proposition

Soit $\mathcal{C}$ une catégorie abélienne. Alors,

i) Si $f : N \hookrightarrow M$ est un monomorphisme, N est le noyau de $M \to M/N$ (dual).

ii) Tout morphisme $f : M \to N$ se factorise de manière unique à isomorphisme près en un épimorphisme $M \to \operatorname{Im} f$ suivi d'un monomorphisme $\operatorname{Im} f \to N$. On a
$$\operatorname{Im} f = \ker(N \to \operatorname{coker} f)$$
(et dual).

iii) Tout homomorphisme qui est à la fois un monomorphisme et un épimorphisme est un isomorphisme.

iv) Dans un diagramme cartésien
$$\begin{array}{ccc} M' & \xrightarrow{f} & N' \\ \downarrow & & \downarrow \\ M & \xrightarrow{f'} & N \end{array},$$
si f est un épimorphisme, alors f' aussi et le diagramme est cocartésien (et dual).

4.11.4 Définition

On dit que la suite
$$0 \to M' \to M \xrightarrow{f} M''$$
est *exacte (à gauche)* si la suite
$$M' \to M \underset{0}{\overset{f}{\rightrightarrows}} M''$$
est exacte à gauche. On définit dualement la notion de *suite exacte à droite*.
On dit qu'une suite
$$0 \to M' \to M \to M'' \to 0$$
est *exacte* si elle est exacte à droite et à gauche.
Une suite
$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$
est *scindées*'il existe un isomorphisme
$$f : M' \bigoplus M'' \xrightarrow{\sim} M$$
tel que
$$p \circ f : M' \bigoplus M'' \to M''$$
et
$$f^{-1} \circ i : M' \to M' \bigoplus M''$$
soient les morphismes canoniques.

4.11.5 Exemple

Un anneau commutatif intègre est un corps si et seulement si toutes les suites exactes de A-modules sont scindées.

4.11.6 Proposition

Une suite

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

est scindée si et seulement si elle est exacte et p possède une section (et dual).

4.11.7 Proposition

i) Un foncteur entre catégorie abéliennes est exact à gauche si et seulement si il est additif et préserve les suites exactes à gauche (et dual).

ii) Si un foncteur additif G possède un adjoint F à gauche, celui ci est aussi additif et on a un isomorphisme de bifoncteurs à valeur dans **Ab** (et dual).

iii) Soit $\mathcal{C}$ une catégorie abélienne et $G : \mathcal{C}' \to \mathcal{C}$ un foncteur pleinement fidèle ayant un adjoint F à gauche. Alors $\mathcal{C}'$ est abélienne.

Bibliographie

[1] M.F. Atiyah, I.G. Mac Donald, *Introduction to commutative Algebra*. Addison-Wesley, Reading, Mass (1969).

[2] A. Bigard, *Géométrie, cours et exercices corrigés pour le Capes et l'agrégation*. Masson, Paris (1998)

[3] N. Bourbaki, *Éléments de mathématiques. Théorie des ensembles*. Diffusion C.C.L.S. Paris (1970)

[4] P.M. Cohn, *Algebra*. John Wiley & sons.

[5] J. Frenkel, *Géométrie pour l'élève professeur*. Hermann, Paris (1973)

[6] J. Huisman, *Algèbre commutative*, polycopié de l'université de Rennes I (1998)

[7] J.-P. Lafon, *Les formalismes fondamentaux de l'algèbre commutative*. Collection Enseignement des sciences, 20. Hermann (1974)

[8] J.-P. Lafon, *algèbre commutative, Langages géométriques et algébriques*. Collection Enseignement des sciences, 24. Hermann (1977)

[9] S. Lang, *Algebra*. Addison-Wesley, Reading, Massachusets (1965)

[10] S. Lang, *Algebraic structures*. Addison-Wesley, Reading, Massachusets (1967)

[11] J. R. Strooker, *Introduction to catégories, homological algebra and sheaf cohomology*. Cambridge University Press (1978)

Index

G-ensemble, 11
G-ensemble à droite, 11
σ-homographie, 76
élément algébrique, 38
élément d'un ensemble, 2
élément irréductible, 35
élément maximal, 7
élément minimal, 7
élément neutre, 8
élément nilpotent, 31
élément nul, 8
élément premier, 35
élément régulier, 32
élément séparable, 41
élément transcendant, 38
élément unité, 8
éléments conjugués, 38
éléments premiers entre eux, 36
épimorphisme, 81
équivalence, 2
équivalence de catégories, 92

action de groupe, 11
action fidèle, 12
action libre, 12
action par endomorphismes, 13
action simple, 12
action transitive, 12
algèbre, 26
algèbre de polynômes, 27
algèbre de type fini, 35
algèbre engendrée, 27
algèbre extérieure, 51
algèbre symétrique, 50
algèbre tensorielle, 50
anneau, 18
anneau commutatif, 18
anneau de fractions, 33
anneau euclidien, 36
anneau factoriel, 35
anneau intègre, 32
anneau local, 33
anneau noethérien, 34
anneau principal, 36
anneau réduit, 32
antécédent d'un élément, 3
appartenir à un ensemble, 2
application, 4
application σ-affine, 64
application σ-linéaire, 64
application σ-projective, 76
application affine, 55
application bijective, 4
application bilinéaire, 43
application compatible à des relations, 6
application croissante, 6
application injective, 4
application multilinéaire, 49
application multilinéaire alternée, 51
application multilinéaire symétrique, 51
application polynomiale, 28
application projective, 68
application semi-affine, 64
application semi-linéaire, 64
application semi-projective, 76
application surjective, 4
assertions duales, 69
automorphisme d'un espace affine, 55
automorphisme de monoïde, 8

barycentre, 62
base d'un module, 24
base duale, 47
birapport, 71
bord d'un demi-espace, 65

borne inférieure, 7
borne supérieure, 7
but d'un morphisme, 78
but d'une relation, 3

côté opposé, 57, 68
cardinal, 5
carré cartésien, 85
carré cocartésien, 85
catégorie, 78
Catégorie abélienne, 106
catégorie additive, 104
catégorie concrète, 91
catégorie duale, 80
Catégorie exacte, 106
catégorie finie, 79
catégorie opposée, 80
catégorie produit, 79
centre d'un monoïde, 9
centre d'une homothétie, 58
centre de gravité, 62
clôture algébrique, 40
classe d'un élément, 6
coefficient dominant d'un polynôme, 29
coefficients d'un barycentre, 62
complété d'un module, 100
complété profini d'un groupe, 100
complété projectif d'un espace afine, 72
composée d'extensions de corps, 38
composition de foncteurs, 89
composition de morphismes, 78
composition de relations, 3
composition de transformations naturelles, 92
conjonction, 2
conoayu d'un couple de morphisme, 83
conoyau d'un morphisme, 106
contenir un ensemble, 2
coordonnées barycentriques, 62
coordonnées d'un point, 54
coordonnées homogènes, 66
corps, 32
corps algébriquement clos, 40
corps de décomposition, 40
corps de rupture, 39
corps résiduel d'un anneau local, 33
corrélation, 69
correspondance, 3
couple, 3

déterminant d'un homomorphisme, 52
déterminant d'un module, 52
déterminant d'une suite de vecteurs, 52
degré d'un polynôme, 29
degré d'une extension de corps, 38
degré de séparabilité, 41
demi-droite, 65
demi-espace fermé, 65
demi-espace ouvert, 65
demi-plan, 65
diagramme commutatif, 95
diagramme constant, 97
dilatation, 55
dimension d'un espace affine, 54
dimension d'un espace projectif, 66
dimension d'un espace vectoriel, 32
disjonction, 2
diviseur de zéro, 31
division harmonique, 71
domaine de définition, 3
droite affine, 54
droite projective, 66
droites concourantes, 57, 68

endomorphisme, 80
endomorphisme d'un espace affine, 55
endomorphisme de monoïde, 8
ensemble, 2
ensemble défini en compréhension, 2
ensemble défini en extension, 2
ensemble de générateurs d'un espace projectif, 67
ensemble de générateurs d'un groupe, 10
ensemble de générateurs d'un monoïde, 9
ensemble inductif, 7
ensemble quotient, 6
ensemble vide, 2
ensembles égaux, 2
ensembles disjoints, 2

entiers naturels, 5
enveloppe convexe, 65
enveloppe vectorielle d'un espace affine, 60
espace affine, 54
espace affine engendré par une partie, 57
espace directeur d'un espace affine, 54
espace projectif, 66
espace projectif dual, 69
espace projectif engendré par une partie, 67
espace vectoriel, 32
espaces faiblement parallèles, 57
espaces parallèles, 57
espaces projectifs isomorphes, 68
espaces supplémentaires, 57
extension algébrique de corps, 38
extension de corps, 38
extension de corps intermédiaire, 38
extension finie de corps, 38
extension galoisienne de corps, 41
extension normale de corps, 40
extension séparable de corps, 41
extension scindée, 13
extrémité d'un segment, 65

famille affinement génératrice, 62
famille affinement libre, 62
famille génératrice, 24
famille libre, 24
famille projectivement génératrice, 70
famille projectivement libre, 70
foncteur additif, 105
foncteur adjoint à droite, 101
foncteur adjoint à gauche, 101
foncteur continu, 99
foncteur continu à droite, 99
foncteur continu à gauche, 99
foncteur contravariant, 87
foncteur covariant, 87
foncteur diagonal, 97
foncteur essentiellement surjectif, 91
foncteur exact, 99
foncteur exact à droite, 99
foncteur exact à gauche, 99
foncteur fidèle, 91
foncteur identité, 89
foncteur pleinement fidèle, 91
foncteur représentable, 93
fonction, 4
forme affine, 55

graduation, 49
graphe d'un morphisme, 86
graphe d'une relation, 3
groupe, 10
groupe alterné, 11
groupe de Galois, 42
groupe engendré par une partie, 10
groupe profini, 100
groupe symétrique, 11

homographie, 68
homomorphisme d'algèbres, 26
homomorphisme d'anneaux, 18
homomorphisme de groupes, 10
homomorphisme de modules, 19
homomorphisme de monoïdes, 8
homothétie, 55
hyperplan, 56
hyperplan projectif, 67

idéal, 20
idéal bilatère, 20
idéal maximal, 32
idéal premier, 32
idéal principal, 21
idéal radical, 32
Identité, 78
identité, 3
Identité naturelle, 92
image d'un élément, 3
image d'une application, 3
image d'une partie, 4
image réciproque d'une partie, 4
implication, 2
inclusion, 2
intersection, 2
inverse, 10
inverse à droite, 10

inverse à droite d'un morphisme, 80
inverse à gauche, 10
inverse à gauche d'un morphisme, 80
inverse d'un morphisme, 81
isomorphisme, 81
isomorphisme d'anneaux, 18
isomorphisme d'espaces affines, 55
isomorphisme de modules, 19
isomorphisme de monoïdes, 8
isomorphisme naturel, 92

lieu à l'infini d'un espace affine, 72
limite finie, 97
limite inductive, 97
limite inductive filtrante, 97
limite projective, 97
limite projective filtrante, 97
localisé d'un module, 30
loi associative, 8
loi de composition, 8
loi de composition interne, 8
loi opposée, 8

médiane d'un triangle, 62
majorant, 7
mesure algébirque d'un bipoint, 58
milieu d'un bipoint, 62
minorant, 7
module, 19
module à droite, 19
module de matrices, 24
module de type fini, 21
module dual, 47
module engendré, 21
module libre, 24
module monogène, 21
module noethérien, 34
monoïde, 8
monoïde engendré par une partie, 9
monomorphisme, 81
morphisme, 78
morphisme d'extensions de corps, 38
morphisme de diagrammes commutatifs, 95
morphismes d'adjonction, 102

norme d'une extension de corps, 39
noyau d'un couple de morphismes, 83
noyau d'un homomorphisme, 9
noyau d'un morphisme, 106
noyau d'une application projective, 68

objet d'une catégorie, 78
objet final, 81
objet initial, 82
objet nul, 104
objet universel, 94
opposé, 10
orbite, 12
ordre partiel, 7
ordre total, 7
orientation d'un espace, 66
orientation d'un repère, 66

paire, 2
parallélogramme, 58
partie affine d'un espace projectif, 72, 73
partie convexe, 65
partie d'un ensemble, 2
partie multiplicative d'un anneau, 30
partition d'un ensemble, 2
petite catégorie, 79
plan affine, 54
plan projectif, 66
plongement diagonal, 83
plus grand élément, 7
plus grand diviseur commun, 36
plus petit élément, 7
point d'un espace affine, 54
point d'un espace projectif, 66
point massique, 61
points alignés, 57, 68
polynôme caractéristique d'un endomorphisme, 52
polynôme minimal, 38
polynôme minimal d'un endomorphisme, 52
polynôme séparable, 41
polynôme unitaire, 29
produit d'anneaux, 23
produit d'ensemble, 3

produit d'objet, 82
produit de modules, 23
produit fibré, 84
produit semi-direct, 13
produit tensoriel, 44
projection, 6, 82, 84
projection affine, 58
projection conique, 68
prolongement d'une relation, 3

quantificateur existenciel, 2
quantificateur universel, 2

rétraction d'un morphisme, 80
radical d'un idéal, 32
rang d'un module, 24
rapport anharmonique, 71
rapport d'une dilatation, 55
relation, 3
relation antisymétrique , 5
relation d'équivalence, 6
relation d'ordre, 6
relation de Chasles, 54
relation de préordre, 6
relation induite, 3
relation réciproque, 3
relation réflexive, 5
relation symétrique, 5
relation transitive, 5
relation vide, 3
repére cartésien, 54
repère affine, 62
repère projectif, 70
restriction d'une relation, 3
restriction des scalaires, 20

section d'un morphisme, 80
segment fermé, 65
segment ouvert, 65
segment semi-ouvert, 65
semi-homographie, 76
signature d'une permutation, 11
singleton, 2
somme amalgammée, 85
somme d'objets, 82
somme de modules, 23
somme directe, 104
sommet d'un triangle, 57, 68
source d'un morphisme, 78
source d'une relation, 3
sous-algèbre, 26
sous-anneau, 18
sous-catégorie, 80
sous-catégorie pleine, 80
sous-ensemble, 2
sous-espace affine, 56
sous-espace projectif, 67
sous-extension de corps, 38
sous-groupe, 10
sous-module, 20
sous-monoïde, 9
sous-monoïde distingué, 12
stabilisateur, 12
structure pré-additive, 104
suite exacte, 13, 107
suite exacte à droite, 107
suite exacte à droite de morphismes, 83
suite exacte à gauche, 107
suite exacte à gauche de morphismes, 83
suite exacte courte, 13
suite exacte scindée, 107
symétrie affine, 58

trace d'un homomorphisme, 47
trace d'une extension de corps, 39
transformation naturelle, 91
translation, 55
transposé d'un homomorphisme, 47
triangle, 57, 68
triangle dual, 70
triplet, 3

union, 2
union disjointe, 3

valuation discrète, 34