

Algèbre I — Master 1

Séance 2 — Révisions de théorie des anneaux

Quotients, factorisation, localisation et conditions de finitude

But de la séance. Revoir les constructions d'anneaux qui seront utilisées dans la théorie des modules : idéaux et quotients, anneaux euclidiens, principaux et factoriels, localisation, noethérianité et artinianité. L'algèbre de groupe fournira la transition vers les représentations.

Table des matières

1 Anneaux, morphismes et algèbres	2
1.1 Éléments remarquables	2
2 Idéaux et anneaux quotients	3
2.1 Idéaux	3
2.2 Quotients et propriété universelle	3
2.3 Idéaux premiers, maximaux et radicaux	3
3 Anneaux euclidiens, principaux et factoriels	4
3.1 Divisibilité, irréductibles et éléments premiers	4
3.2 Domaines euclidiens	4
3.3 Domaines principaux	5
3.4 Domaines factoriels	5
4 Localisation	6
4.1 Construction par fractions	6
4.2 Propriété universelle	6
4.3 Exemples	7
4.4 Idéaux et spectre après localisation	7
5 Anneaux noethériens et artiniens	7
5.1 Conditions de chaîne	7
5.2 Théorème de la base de Hilbert	8
5.3 Anneaux artiniens	9
6 Algèbres de monoïdes et de groupes	9
7 Transition vers les modules	9
8 Compléments	10
8.1 Théorème chinois et idempotents	10
8.2 Structure des anneaux artiniens commutatifs	10
8.3 Théorème de Wedderburn–Artin	11
8.4 Dimension de Krull et anneaux locaux réguliers	11
À retenir	11

1. Anneaux, morphismes et algèbres

Dans tout le cours, les anneaux sont unitaires et les morphismes d'anneaux préservent l'unité.

Définition 1.1. Un *anneau* est un groupe abélien $(A, +)$ muni d'une multiplication associative et distributive par rapport à l'addition, possédant un élément neutre 1_A . Il est *commutatif* si $ab = ba$ pour tous $a, b \in A$.

Voici les exemples qui interviendront le plus souvent :

- $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, les corps $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{F}_p$;
- les anneaux de polynômes $A[T]$ et $A[T_1, \dots, T_n]$, ainsi que l'anneau de séries formelles $A[[T]]$;
- l'anneau $M_n(A)$ des matrices carrées, non commutatif dès que $n \geq 2$ et $A \neq 0$;
- l'anneau $\text{End}_A(M)$ des endomorphismes d'un A -module M , avec la composition ;
- le produit $A \times B$, muni des opérations composante par composante ;
- l'algèbre de groupe $\mathbf{k}[G]$;
- l'anneau A^X des fonctions $X \rightarrow A$, avec les opérations ponctuelles.

Définition 1.2. Soit A un anneau commutatif. Une *A-algèbre* est un anneau B muni d'un morphisme $A \rightarrow B$ dont l'image est contenue dans le centre $Z(B)$. Si B est commutatif, cette dernière condition est automatique.

Ainsi, un morphisme d'anneaux commutatifs $A \rightarrow B$ permet de multiplier les éléments de B par les éléments de A , suivant $a \cdot b = f(a)b$.

1.1. Éléments remarquables

Soit A un anneau.

- Une *unité* est un élément possédant un inverse multiplicatif. Les unités forment un groupe $A^\times$.
- Un élément a est *nilpotent* s'il existe $n \geq 1$ tel que $a^n = 0$.
- Un élément e est *idempotent* si $e^2 = e$.
- Un anneau commutatif non nul est un *domaine intègre* s'il ne possède aucun diviseur de zéro.
- Un *corps* est un anneau commutatif non nul dans lequel tout élément non nul est inversible.

Les idempotents centraux codent des décompositions. Si $e^2 = e$ et $e \in Z(A)$, l'application

$$A \longrightarrow eA \times (1 - e)A, \quad a \longmapsto (ea, (1 - e)a),$$

est un isomorphisme d'anneaux. Ce phénomène réapparaîtra dans la décomposition des modules et des algèbres semi-simples.

2. Idéaux et anneaux quotients

2.1. Idéaux

Dans un anneau non nécessairement commutatif, on distingue les idéaux à gauche, à droite et bilatères. Un sous-groupe additif $I \subseteq A$ est un idéal à gauche si $aI \subseteq I$ pour tout $a \in A$, et un idéal à droite si $Ia \subseteq I$. Il est bilatère s'il est à la fois idéal à gauche et idéal à droite. Dans un anneau commutatif, ces trois notions coïncident.

Si $S \subseteq A$, l'idéal bilatère engendré par S est constitué des sommes finies

$$\sum_i a_i s_i b_i, \quad a_i, b_i \in A, \quad s_i \in S.$$

Dans le cas commutatif, il s'agit simplement des sommes $\sum_i a_i s_i$.

2.2. Quotients et propriété universelle

Si I est un idéal bilatère, le groupe abélien quotient A/I devient un anneau pour la multiplication

$$(a + I)(b + I) = ab + I.$$

Le caractère bilatère de I est précisément ce qui rend cette multiplication bien définie. La projection $\pi: A \rightarrow A/I$ est un morphisme d'anneaux de noyau I . Réciproquement, le noyau de tout morphisme d'anneaux est un idéal bilatère.

Proposition 2.1 (Propriété universelle du quotient). *Soit $f: A \rightarrow B$ un morphisme d'anneaux tel que $I \subseteq \text{Ker}(f)$. Il existe un unique morphisme $\bar{f}: A/I \rightarrow B$ tel que $f = \bar{f} \circ \pi$. Il est donné par $\bar{f}(a + I) = f(a)$.*

Exemple 2.2.

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(n), \quad \mathbf{k}[T]/(T^n - 1), \quad \mathbf{k}[T_1, \dots, T_r]/I.$$

Si $P \in \mathbf{k}[T]$ est non constant, $\mathbf{k}[T]/(P)$ est un corps si et seulement si P est irréductible.

Théorème 2.3 (Correspondance des idéaux). *Les idéaux de A/I sont en bijection avec les idéaux de A contenant I :*

$$J \longmapsto J/I, \quad \bar{J} \longmapsto \pi^{-1}(\bar{J}).$$

Cette correspondance préserve les inclusions ainsi que les idéaux premiers et maximaux.

2.3. Idéaux premiers, maximaux et radicaux

Dans cette sous-section, A est commutatif.

Définition 2.4. Un idéal propre $\mathfrak{p} \subsetneq A$ est *premier* si $ab \in \mathfrak{p}$ implique $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$. Cela équivaut à dire que $A/\mathfrak{p}$ est un domaine intègre.

Un idéal propre $\mathfrak{m} \subsetneq A$ est *maximal* s'il n'existe aucun idéal strictement compris entre $\mathfrak{m}$ et A . Cela équivaut à dire que $A/\mathfrak{m}$ est un corps.

Tout idéal maximal est premier. La réciproque est fausse : (0) est premier mais non maximal dans $\mathbb{Z}$.

Exemple 2.5. Les idéaux premiers de $\mathbb{Z}$ sont (0) et les (p) , où p est premier ; les idéaux maximaux sont les (p) . Dans $\mathbf{k}[T]$, les idéaux maximaux sont engendrés par les polynômes irréductibles. Si $\mathbf{k}$ est algébriquement clos, ils sont donc de la forme $(T - a)$.

Définition 2.6. Le *radical* d'un idéal I est

$$\sqrt{I} = \{a \in A \mid a^n \in I \text{ pour un certain } n \geq 1\}.$$

Le nilradical $\sqrt{(0)}$ est l'ensemble des éléments nilpotents.

On admettra la description fondamentale

$$\sqrt{I} = \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p},$$

où l'intersection porte sur les idéaux premiers contenant I . En particulier, le nilradical est l'intersection de tous les idéaux premiers de A .

3. Anneaux euclidiens, principaux et factoriels

Dans toute cette section, A est un domaine intègre.

3.1. Divisibilité, irréductibles et éléments premiers

On dit que a *divise* b , et l'on écrit $a \mid b$, s'il existe $c \in A$ tel que $b = ac$. Deux éléments a, b sont *associés* si $a = ub$ pour une unité $u \in A^\times$; cela équivaut à $(a) = (b)$.

Définition 3.1. Un élément $p \in A$, non nul et non inversible, est

- *irréductible* si $p = ab$ implique que a ou b est une unité ;
- *premier* si $p \mid ab$ implique $p \mid a$ ou $p \mid b$.

Tout élément premier est irréductible. La réciproque peut être fausse. Par exemple, dans $\mathbb{Z}[\sqrt{-5}]$, l'élément 2 est irréductible mais non premier, car 2 divise $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$ sans diviser aucun des deux facteurs.

3.2. Domaines euclidiens

Définition 3.2. Un domaine A est *euclidien* s'il existe une application

$$\delta: A \setminus \{0\} \longrightarrow \mathbb{N}$$

telle que, pour tous $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ vérifiant

$$a = bq + r, \quad r = 0 \quad \text{ou} \quad \delta(r) < \delta(b).$$

L'algorithme d'Euclide calcule alors un plus grand commun diviseur par divisions successives ; en remontant les égalités, on obtient l'identité de Bézout $d = ax + by$.

Exemple 3.3. 1. $\mathbb{Z}$ est euclidien pour $\delta(n) = |n|$.

2. $\mathbf{k}[T]$ est euclidien pour $\delta(P) = \deg(P)$.

3. L'anneau des entiers de Gauss $\mathbb{Z}[i]$ est euclidien pour la norme $N(a + ib) = a^2 + b^2$. La division avec reste s'obtient en approchant les parties réelle et imaginaire d'un nombre complexe par des entiers.

4. Tout corps est euclidien, de manière triviale.

3.3. Domaines principaux

Définition 3.4. Un *domaine principal*, ou *PID*, est un domaine intègre dans lequel tout idéal est principal, c'est-à-dire de la forme $(a) = aA$.

Théorème 3.5. *Tout domaine euclidien est principal.*

Démonstration. Soit $I \neq (0)$ un idéal. Choisissons $d \in I \setminus \{0\}$ tel que $\delta(d)$ soit minimale. Pour $a \in I$, écrivons $a = dq + r$ avec $r = 0$ ou $\delta(r) < \delta(d)$. Comme $r = a - dq \in I$, la minimalité impose $r = 0$. Ainsi $I = (d)$. $\square$

Exemple 3.6. $\mathbb{Z}$, $\mathbf{k}[T]$ et $\mathbb{Z}[i]$ sont des PID. Tout corps est un PID, son seul idéal propre étant (0) . En revanche, $\mathbf{k}[X, Y]$ n'est pas principal : l'idéal (X, Y) ne peut être engendré par un seul polynôme. Le quotient $\mathbb{Z}/n\mathbb{Z}$ pour n composé n'est pas un PID suivant notre convention, car ce n'est pas un domaine.

La réciproque « principal implique euclidien » est fausse. Les exemples sont moins élémentaires ; un exemple classique dû à Motzkin est l'anneau des entiers $\mathbb{Z}[(1 + \sqrt{-19})/2]$, qui est principal mais non euclidien.¹

3.4. Domaines factoriels

Définition 3.7. Un *domaine factoriel*, ou *UFD*, est un domaine dans lequel tout élément non nul et non inversible s'écrit comme produit d'irréductibles, cette écriture étant unique à permutation et multiplication des facteurs par des unités près.

Théorème 3.8. *Dans un domaine principal, tout irréductible est premier et toute suite strictement croissante d'idéaux est stationnaire. Il en résulte que tout PID est factoriel. Ainsi*

$$\text{euclidien} \implies \text{principal} \implies \text{factoriel}.$$

Idée de la preuve. Si p est irréductible et $p \mid ab$, considérons l'idéal $(p, a) = (d)$. Comme $d \mid p$, l'irréductibilité de p donne soit d inversible, soit d associé à p . Dans le second cas $p \mid a$. Dans le premier, Bézout donne $up + va = 1$; en multipliant par b , on obtient $p \mid b$.

L'existence d'une factorisation découle de la condition de chaîne ascendante sur les idéaux principaux : sinon, une succession de factorisations propres produirait une chaîne strictement croissante $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$. L'unicité résulte du fait que les irréductibles sont premiers. $\square$

Théorème 3.9 (Lemme de Gauss). *Si A est factoriel, alors $A[T]$ est factoriel. Par récurrence, $A[T_1, \dots, T_n]$ est factoriel.*

Ainsi $\mathbf{k}[X, Y]$ est factoriel mais non principal : la seconde implication de la chaîne précédente n'est pas réversible. Quant à $\mathbb{Z}[\sqrt{-5}]$, il n'est pas factoriel, puisque

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

donne deux décompositions incompatibles en irréductibles.

Remarque 3.10. Le résultat sur les PID qui sera décisif aux séances suivantes est le suivant : tout sous-module d'un module libre de rang fini sur un PID est libre. Il mène à la forme normale de Smith et au théorème de structure des modules de type fini.

¹T. Motzkin, *The Euclidean algorithm*, Bull. Amer. Math. Soc. **55** (1949), 1142–1146.

4. Localisation

La localisation force une famille d'éléments à devenir inversibles. Elle englobe la construction du corps des fractions, mais permet aussi d'étudier un anneau au voisinage d'un idéal premier.

4.1. Construction par fractions

Définition 4.1. Une partie $S \subseteq A$ d'un anneau commutatif est *multiplicative* si $1 \in S$ et si $s, t \in S$ implique $st \in S$. Nous supposons $0 \notin S$.

Sur $A \times S$, on pose

$$(a, s) \sim (a', s') \iff \text{il existe } t \in S \text{ tel que } t(as' - a's) = 0.$$

C'est une relation d'équivalence. On note a/s la classe de (a, s) . Les formules

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}, \quad \frac{a}{s} \frac{a'}{s'} = \frac{aa'}{ss'}$$

font de l'ensemble des classes un anneau, noté $S^{-1}A$. Si A est intègre, la relation d'équivalence se simplifie en $as' = a's$.

Le morphisme canonique

$$\iota: A \longrightarrow S^{-1}A, \quad a \longmapsto a/1,$$

n'est pas toujours injectif :

$$\text{Ker}(\iota) = \{a \in A \mid sa = 0 \text{ pour un certain } s \in S\}.$$

Chaque $s \in S$ devient inversible, d'inverse $1/s$.

Exemple 4.2. Prenons $A = \mathbb{Z}/6\mathbb{Z}$ et $S = \{1, 2, 4\}$. Dans $S^{-1}A$, la classe de 2 devient inversible. Comme $2 \cdot 3 = 0$, la classe de 3 devient nulle. On obtient en fait

$$S^{-1}(\mathbb{Z}/6\mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}.$$

Cet exemple montre concrètement pourquoi le morphisme $A \rightarrow S^{-1}A$ peut ne pas être injectif.

4.2. Propriété universelle

Théorème 4.3 (Propriété universelle de la localisation). Soit $f: A \rightarrow B$ un morphisme vers un anneau commutatif tel que $f(s) \in B^\times$ pour tout $s \in S$. Il existe un unique morphisme

$$\tilde{f}: S^{-1}A \longrightarrow B$$

tel que $f = \tilde{f} \circ \iota$. Il est donné par

$$\tilde{f}(a/s) = f(a)f(s)^{-1}.$$

La construction $S^{-1}A$ est donc caractérisée à isomorphisme unique près, indépendamment de sa présentation explicite par fractions.

4.3. Exemples

1. Si A est intègre et $S = A \setminus \{0\}$, on obtient le corps des fractions $\text{Frac}(A)$. Ainsi $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$ et $\text{Frac}(\mathbf{k}[T]) = \mathbf{k}(T)$.
2. Pour $f \in A$, si $S = \{1, f, f^2, \dots\}$, on note la localisation A_f . Par exemple $\mathbf{k}[T]_T = \mathbf{k}[T, T^{-1}]$.
3. Pour un nombre premier p ,

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\}.$$

Ses unités sont les fractions a/b avec $p \nmid a$, et son unique idéal maximal est $p\mathbb{Z}_{(p)}$.

4. Si $\mathfrak{p}$ est un idéal premier de A , le complément $S = A \setminus \mathfrak{p}$ est multiplicatif. On note $A_{\mathfrak{p}} = S^{-1}A$.

Définition 4.4. Un anneau commutatif R est *local* s'il possède un unique idéal maximal.

Proposition 4.5. Pour tout idéal premier $\mathfrak{p} \subseteq A$, l'anneau $A_{\mathfrak{p}}$ est local et son unique idéal maximal est $\mathfrak{p}A_{\mathfrak{p}}$. Un élément a/s est inversible si et seulement si $a \notin \mathfrak{p}$.

4.4. Idéaux et spectre après localisation

Si $I \subseteq A$ est un idéal, son extension dans $S^{-1}A$ est

$$S^{-1}I = IS^{-1}A = \left\{ \frac{a}{s} \mid a \in I, s \in S \right\}.$$

Tout idéal de $S^{-1}A$ est de cette forme, mais plusieurs idéaux de A peuvent avoir la même extension.

Théorème 4.6 (Correspondance des idéaux premiers). Les applications d'extension et de contraction induisent des bijections inverses entre

$$\{\mathfrak{p} \in \text{Spec}(A) \mid \mathfrak{p} \cap S = \emptyset\} \quad \text{et} \quad \text{Spec}(S^{-1}A),$$

données par $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ et $\mathfrak{q} \mapsto \iota^{-1}(\mathfrak{q})$.

Exemple 4.7. Les idéaux premiers de $\mathbb{Z}_{(p)}$ sont (0) et $p\mathbb{Z}_{(p)}$. Les idéaux premiers de A_f correspondent aux idéaux premiers de A ne contenant pas f .

La localisation s'étendra aux modules. Pour un A -module M , on construira $S^{-1}M$ et l'on démontrera l'isomorphisme

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

En particulier, la localisation est un changement des scalaires et elle est un foncteur exact.

5. Anneaux noethériens et artiniens

5.1. Conditions de chaîne

Définition 5.1. Un anneau commutatif A est *noethérien* si toute chaîne croissante d'idéaux

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

est stationnaire. Il est *artinien* si toute chaîne décroissante

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots$$

est stationnaire.

Proposition 5.2. *Pour un anneau commutatif A , les propriétés suivantes sont équivalentes :*

- (i) A est noethérien ;
- (ii) tout idéal de A est de type fini ;
- (iii) toute famille non vide d'idéaux de A possède un élément maximal.

Démonstration. Supposons la condition de chaîne ascendante et soit I un idéal. S'il n'est pas de type fini, on choisit successivement $a_{n+1} \in I \setminus (a_1, \dots, a_n)$, ce qui produit une chaîne strictement croissante : contradiction. Si tous les idéaux sont de type fini, l'union d'une chaîne d'idéaux est engendrée par un nombre fini d'éléments, tous contenus dans un même terme ; la chaîne est donc stationnaire. L'équivalence avec la condition maximale se démontre de façon analogue. $\square$

Exemple 5.3. 1. Tout corps, $\mathbb{Z}$ et tout PID sont noethériens.

- 2. Tout anneau fini est à la fois noethérien et artinien.
- 3. Toute algèbre de dimension finie sur un corps est noethérienne et artinienne : une chaîne d'idéaux est une chaîne de sous-espaces vectoriels. Ainsi $\mathbb{Z}/n\mathbb{Z}$ et $\mathbf{k}[T]/(T^n)$ sont artiniens.
- 4. $\mathbf{k}[T]$ est noethérien mais non artinien, à cause de la chaîne $(T) \subsetneq (T^2) \subsetneq (T^3) \subsetneq \dots$.
- 5. $\mathbf{k}[[T]]$ est noethérien mais non artinien pour la même raison.
- 6. L'anneau $\mathbf{k}[X_1, X_2, \dots]$ n'est pas noethérien, puisque $(X_1) \subsetneq (X_1, X_2) \subsetneq \dots$.

Les quotients et les localisations d'un anneau noethérien sont noethériens. Pour un quotient, cela résulte de la correspondance des idéaux ; pour une localisation, tout idéal est l'extension d'un idéal de A .

5.2. Théorème de la base de Hilbert

Théorème 5.4 (Théorème de la base de Hilbert). *Si A est un anneau commutatif noethérien, alors $A[T]$ est noethérien.*

Démonstration. Soit $I \subseteq A[T]$ un idéal. Pour chaque $n \geq 0$, notons J_n l'idéal de A engendré par les coefficients dominants des polynômes de I de degré au plus n . La suite (J_n) est croissante, donc stationnaire : il existe N tel que $J_n = J_N$ pour $n \geq N$.

Pour chaque $n \leq N$, choisissons un nombre fini de polynômes de I dont les coefficients dominants engendrent J_n ; soit F la réunion finie de ces familles. Nous affirmons que F engendre I . En effet, si $P \in I$ est de degré d , son coefficient dominant appartient à J_d . Une combinaison appropriée des polynômes choisis, multipliés par des puissances de T , permet de soustraire à P un élément de (F) de même terme dominant. On conclut par récurrence sur le degré. $\square$

Corollaire 5.5. *Toute algèbre commutative de type fini sur un anneau noethérien est noethérienne. En particulier, toute $\mathbf{k}$ -algèbre commutative de type fini*

$$\mathbf{k}[T_1, \dots, T_n]/I$$

est noethérienne.

Remarque 5.6. Le théorème ne dit pas que $A[[T]]$ est noethérien ; cette assertion est vraie, mais sa preuve demande un argument supplémentaire.

5.3. Anneaux artiniens

La condition artinienne est beaucoup plus forte que la condition noethérienne.

Théorème 5.7. *Tout anneau commutatif artinien est noethérien.*

La réciproque est fautive, comme le montrent $\mathbb{Z}$, $\mathbf{k}[T]$ et $\mathbf{k}[[T]]$.

Théorème 5.8. *Soit A une $\mathbf{k}$ -algèbre commutative de type fini. Les conditions suivantes sont équivalentes :*

- (i) A est artinienne ;
- (ii) A est de dimension finie comme $\mathbf{k}$ -espace vectoriel ;
- (iii) tout idéal premier de A est maximal.

La dernière condition signifie que la dimension de Krull de A est nulle. Par exemple, $\mathbf{k}[T]/(P)$ est artinien pour tout polynôme non nul P , même si P n'est ni irréductible ni sans facteur carré.

Remarque 5.9. Dans un anneau artinien commutatif, il n'existe qu'un nombre fini d'idéaux maximaux, le nilradical est nilpotent, et l'anneau se décompose en produit fini d'anneaux artiniens locaux. Cette structure sera esquissée dans les compléments.

6. Algèbres de monoïdes et de groupes

Définition 6.1. Soit M un monoïde et A un anneau commutatif. L'*algèbre de monoïde* $A[M]$ est le A -module libre de base $(\delta_m)_{m \in M}$, muni de la multiplication $\delta_m \delta_{m'} = \delta_{mm'}$, étendue par bilinéarité. Si $M = G$ est un groupe, on parle d'*algèbre de groupe*.

Ainsi,

$$\mathbf{k}[\mathbb{N}] \simeq \mathbf{k}[T], \quad \mathbf{k}[\mathbb{Z}] \simeq \mathbf{k}[T, T^{-1}], \quad \mathbf{k}[\mathbb{Z}^n] \simeq \mathbf{k}[T_1^{\pm 1}, \dots, T_n^{\pm 1}].$$

Si $C_n = \langle \sigma \rangle$ est cyclique,

$$\mathbf{k}[C_n] \simeq \mathbf{k}[T]/(T^n - 1), \quad \delta_\sigma \longleftrightarrow T.$$

Pour un groupe fini G , $\mathbf{k}[G]$ est de dimension $|G|$ sur $\mathbf{k}$. Une représentation $\rho: G \rightarrow \mathrm{GL}(V)$ s'étend par linéarité en un morphisme d'algèbres

$$\mathbf{k}[G] \longrightarrow \mathrm{End}_{\mathbf{k}}(V), \quad \sum_{g \in G} a_g \delta_g \longmapsto \sum_{g \in G} a_g \rho(g).$$

Elle définit donc une structure de $\mathbf{k}[G]$ -module sur V . Réciproquement, l'action des éléments δ_g sur un $\mathbf{k}[G]$ -module fournit une représentation de G .

Pour un groupe fini, il faut distinguer l'algèbre de groupe $\mathbf{k}[G]$ de l'anneau $\mathbf{k}^G$ des fonctions $G \rightarrow \mathbf{k}$ muni du produit ponctuel. Après choix des fonctions delta, ils ont le même espace vectoriel sous-jacent, mais leurs multiplications sont différentes :

$$\delta_g \delta_h = \delta_{gh} \quad \text{dans } \mathbf{k}[G], \quad \delta_g \delta_h = \begin{cases} \delta_g & g = h, \\ 0 & g \neq h \end{cases} \quad \text{dans } \mathbf{k}^G.$$

7. Transition vers les modules

Définition 7.1. Un A -module à gauche est un groupe abélien $(M, +)$ muni d'une loi $A \times M \rightarrow M$, $(a, m) \mapsto am$, distributive en chaque variable et telle que

$$(ab)m = a(bm), \quad 1_A m = m.$$

De manière équivalente, c'est un morphisme d'anneaux $A \rightarrow \text{End}_{\mathbb{Z}}(M)$.

Exemples fondamentaux :

- les $\mathbb{Z}$ -modules sont exactement les groupes abéliens ;
- les $\mathbf{k}$ -modules sont les espaces vectoriels sur $\mathbf{k}$;
- un $\mathbf{k}[T]$ -module est un $\mathbf{k}$ -espace vectoriel muni d'un endomorphisme, l'action de T ;
- un $\mathbf{k}[G]$ -module est une représentation linéaire de G ;
- les idéaux à gauche de A sont les sous- A -modules du module régulier ${}_A A$.

Pour un anneau non commutatif, il faut distinguer modules à gauche et modules à droite. Un (A, B) -bimodule est simultanément un A -module à gauche et un B -module à droite, avec

$$(am)b = a(mb).$$

Les bimodules seront les coefficients naturels du produit tensoriel et des changements de scalaires.

8. Compléments

8.1. Théorème chinois et idempotents

Théorème 8.1 (Théorème chinois). Soient $I_1, \dots, I_r$ des idéaux deux à deux comaximaux d'un anneau commutatif A . Le morphisme canonique

$$A \longrightarrow \prod_{i=1}^r A/I_i$$

est surjectif et son noyau est $\bigcap_i I_i = \prod_i I_i$. Par conséquent,

$$A/\bigcap_i I_i \simeq \prod_{i=1}^r A/I_i.$$

Pour $r = 2$, si $x \in I$ et $y \in J$ vérifient $x + y = 1$, la classe de y dans $A/(I \cap J)$ est un idempotent qui vaut 1 modulo I et 0 modulo J . Réciproquement, une décomposition de 1 en idempotents centraux orthogonaux $1 = e_1 + \dots + e_r$ donne une décomposition $A \simeq e_1 A \times \dots \times e_r A$.

8.2. Structure des anneaux artiniens commutatifs

Soit A artinien commutatif, d'idéaux maximaux $\mathfrak{m}_1, \dots, \mathfrak{m}_r$. Son radical de Jacobson et son nilradical coïncident :

$$J(A) = \sqrt{(0)} = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r,$$

et cet idéal est nilpotent. Pour N assez grand, le théorème chinois donne

$$A \simeq \prod_{i=1}^r A/\mathfrak{m}_i^N.$$

Chaque facteur est un anneau artinien local. Ainsi, l'étude des anneaux artiniens commutatifs se ramène à celle des anneaux artiniens locaux.

8.3. Théorème de Wedderburn–Artin

Dans le cadre non commutatif, un anneau est *semi-simple* s'il est semi-simple comme module sur lui-même. Le théorème de Wedderburn–Artin affirme qu'un tel anneau est un produit fini

$$A \simeq \prod_{i=1}^r M_{n_i}(D_i),$$

où les D_i sont des algèbres à division. En particulier, un anneau simple artinien est isomorphe à $M_n(D)$. Cette structure expliquera plus tard la décomposition des algèbres de groupes en caractéristique ne divisant pas l'ordre du groupe.

8.4. Dimension de Krull et anneaux locaux réguliers

La *dimension de Krull* d'un anneau commutatif A est la borne supérieure des longueurs r des chaînes strictes d'idéaux premiers

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r.$$

Un corps est de dimension 0, $\mathbb{Z}$ et $\mathbf{k}[T]$ de dimension 1, et $\mathbf{k}[T_1, \dots, T_n]$ de dimension n .

Si $(A, \mathfrak{m}, \mathbf{k})$ est un anneau local noethérien, on a

$$\dim_{\mathbf{k}}(\mathfrak{m}/\mathfrak{m}^2) \geq \dim(A).$$

L'anneau est dit *local régulier* lorsqu'il y a égalité. Par exemple, $\mathbf{k}[T_1, \dots, T_n]_{(T_1, \dots, T_n)}$ est local régulier de dimension n .

À retenir

- Les idéaux bilatères sont exactement les noyaux des morphismes d'anneaux et permettent de former les quotients.
- La chaîne euclidien $\Rightarrow$ principal $\Rightarrow$ factoriel organise les propriétés de division et de factorisation ; les réciproques sont fausses.
- La localisation $S^{-1}A$ est l'anneau universel dans lequel les éléments de S deviennent inversibles ; ses idéaux premiers correspondent à ceux de A qui évitent S .
- La noethérianité est une condition de finitude des idéaux, stable par quotient, localisation et adjonction d'un nombre fini de variables.
- Une algèbre commutative de type fini sur un corps est artinienne si et seulement si elle est de dimension vectorielle finie.
- Les représentations de G sont exactement les modules sur l'algèbre de groupe $\mathbf{k}[G]$.