ALGÈBRE 1
(COURS DE M1, 2018-2019)
HMMA 115M

COURS 1-2
LOIS DE COMPOSITION, MONOIDES, GROUPES, ANNEAUX, CATÉGORIES

Loi de composition

Definition. Soit E un ensemble. On appelle loi de composition sur E une application f de $E \times E$ dans E. La valeur $f(x, y)$ de f pour un couple $(x, y) \in E \times E$ s'appelle le composé de x et de y pour cette loi. Un ensemble muni d'une loi de composition e'est appelé un *magma*.

Exemples
Les applications

$$(X, Y) \to X \cup Y$$

et

$$(X, Y) \to X \cap Y$$

sont des lois de composition sur l'ensemble des parties d'un ensemble E.

Monoïdes

Definition. Un *monoïde* est un triple (M, μ, e), où M est un ensemble, μ est une application (la loi de composition)

$$\mu : M \times M \to M,$$

$e \in M$, avec les axiomes suivants

* Associativité de la loi de composition μ :

$$\forall x, y, z \in M,\ \mu(x, \mu(y, z)) = \mu(\mu(x, y), z).$$

* e est un élément neutre : $\forall x \in M,\ \mu(x, e) = \mu(e, x) = x$;

Il s'agit d'un *demi-groupe* si l'on ne suppose pas, d'existence d'un élément neutre.

Souvent la multiplication μ est noté par un point ou simlement par juxtaposition.

Elément e est unique : si e' est un autre élément neutre, alors nous avons

$$e' = e'e = e.$$

Definition. Un monoïde M est commutatif si l'on a $xy = yx$ pour x, y dans M.

Exemples
1. L'ensemble des parties d'un ensemble E, muni de l'union ensembliste, est un monoïde, dont l'ensemble vide est l'élément neutre. Le même ensemble muni de l'intersection ensembliste est aussi un monoïde dont E est l'élément neutre.
2. L'ensemble des entiers naturels, muni de l'addition, est un monoïde, dont 0 est l'élément neutre.
3. L'ensemble des entiers naturels strictement positifs, muni de la multiplication, est un monoïde d'élément neutre 1.
4. L'ensemble des entiers naturels muni de la loi Max qui a deux entiers associe le plus grand des deux est un monoïde de neutre 0.

Si M et M' sont deux monoïdes un *morphisme* de monoïdes est une application

$$\phi : M \to L$$

avec les conditions

$$\forall x, y \in M,\ \phi(xy) = \phi(x)\phi(y),$$
$$\phi(e_M) = \phi(e_L).$$

Exemple
Si l'on munit l'ensemble des entiers naturels de la loi Max, l'application

$$n \mapsto n + 1$$

est un morphisme de demi-groupes mais n'est pas un morphisme de monoïdes.

Si X et Y sont deux sous-ensembles d'un monoïde M l'ensemble XY est défini par

$$XY = \{xy \mid\ x \in X, y \in Y\}.$$

Cette définition donne la stucture d'un monoïde sur l'ensemble $\mathcal{P}(M)$ de tous les sous-ensembles de M. Elément neutre de ce monoïde est un ensemble $\{e\}$.
Un sous-monoïde d'un monoïde M est un sous-ensemble T de M vérifiant :

$$TT \subset T, \quad e \in T.$$

Exemple
Le sous-ensemble de $\mathcal{P}(M)$ qui se compose de sous-ensembles non-vide de M est un sous-monoïde de $\mathcal{P}(M)$.

Monoïdes libres

Si A est un ensemble, appelé *alphabet*, l'ensemble des suites finies d'éléments de A,

$$m = (a_1, \ldots, a_n), \quad n \geq 0,$$

appelées *mots* muni de l'opération de concaténation est un monoïde noté A^* et appelé monoïde *libre* sur A. L'entier n est appelé la *longueur* du mot m et noté par $l(m)$ ou simplement par $|m|$. Si

$$m' = (b_1, \ldots, b_k)$$

est un outre mot le produit mm' est définit par concatenation

$$mm' = (a_1, \ldots, a_n, b_1, \ldots, b_k)$$

Le suite du longuer 0, qui est une suite vide, est un élément neutre pour se produit. Il y a une inclusion canonique

$$A \xrightarrow{\subset} A^*$$

où une lettre $a \in A$ est indetifié avec la suite (a) de longueur 1.

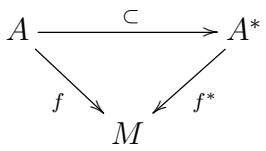
Proposition 1. *Soit M un monoïde et*

$$f : A \to M$$

est une application (ensembiste). Alors il existe une seule morphisme de monoïdes

$$f^* : A^* \to M$$

telle que le diagramme suivant



est commutatif

Definition. Un *langage* sur un alphabet A est un sous-ensemble de monoïde A^*, on suppose souvant que l'alphabet A est fini. L'ensemble de tous les langage sur l'alphabet A forment un monoïde.

En informatique théorique, les monoïdes et plus particulièrement le monoïde libre sont parmi les structures les plus utilisées.

Groupes

Definition. Un groupe $\mathcal{G}$ est un monoïde tel que pour chaque son élément $g \in \mathcal{G}$ il existe un élément $h \in \mathcal{G}$ tel que $g \cdot h = h \cdot g = e$, h est dit inverse de g et on le note g^{-1}.

On définit homomorphisme, isomorphhisme et automorphisme.

On appelle *ordre* d'un élément a d'un groupe $(G, \cdot)$ le plus petit positif n tel que $a^n = e$; notation $|a| = n$; si $a^n \neq e \; \forall \, n > 0$ on dit que l'ordre de a est égale à infini : $|a| = \infty$.

Un groupe G est *sans torsion* si pour tout $g \neq e$ l'ordre de g est infini.

La cardinalité d'un groupe comme un ensemble est appelée l'*ordre* du group, la notation $|G|$.

Exemples de groupes

1. Soit M un ensemble, soit $S(M)$ l'ensemble de toutes les bijections de M. Avec l'opération de composition de bijections $S(M)$ devient un groupe. Si M est cardinalité finie on peut l'identifier avec l'ensemble $\{1, \ldots, n\}$, le groupe $S(M)$ est un groupe des permutation de degré n ou groupe symétrique $S(n)$ d'indice n.

Chaque élément de $S(n)$ peut être pésenter sous la forme, comme une permutation :

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$$

Alors $|S(n)| = n!$.

Anneaux

Definition. On appelle *anneau* un ensemble A muni de deux lois de composition appelées respectivement addition et multiplication, satisfaisant aux axiomes suivants :

(AN I) Pour l'addition, A est un groupe commutatif.

(AN II) La multiplication est associative et possède un élément neutre.

(AN III) La multiplication est distributive par rapport à l'addition.

On dit que l'anneau A est commutatif si sa multiplication est commutative.

Dans la suite, on note

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

l'addition et

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

la multiplication ; on note 0 l'élément neutre de l'addition et 1 celui de la multiplication. Enfin, on note $-x$ l'opposé de x pour l'addition. Les axiomes d'un anneau s'expriment donc par les

identités suivantes :

1) $x + (y + z) = (x + y)$ (associativité de l'addition) ,
2) $x + y = y + x$ (commutativité de l'addition),
3) $0 + x = x + 0 = x$ (zéro) ,
4) $x + (-x) = (-x) + x = 0$ (opposé) ,
5) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (associativité de la multiplication),
6) $x \cdot 1 = 1 \cdot x$ (élément unité) ,
7) $(x + y) \cdot z = x \cdot z + y \cdot z$ (distributivité) ,
8) $x \cdot (y + z) = x \cdot y + x \cdot z)$ (distributivité) .

Enfin l'anneau A est commutatif si l'on a $xy = yx$ pour x, y dans A.

Exemples d'anneaux

1. Anneau nul. Soit A un anneau. Pour qu'on ait $0 = 1$ dans A, il faut et il suffit que A soit réduit à un seul élément. En effet, la condition est évidemment suffisante. D'autre part, si $0 = 1$, on a, pour tout $x \in A$, $x = x \cdot 1 = x \cdot 0 = 0$. Un tel anneau s'appelle un anneau nul.

2. Anneau des entiers rationnels $\mathbb{Z}$ est un anneau commutatif.

3. Anneau de fonctions réelles. Soit I un intervalle de l'ensemble $\mathbb{R}$ des nombres réels et soit A l'ensemble des fonctions continues définies dans I et à valeurs réelles. On définit la somme $f + g$ et le produit fg de deux fonctions f et g par

$$(f + g)(t) = f(t) + g(t), \quad (fg)(t) = f(t)g(t), \quad (t \in I).$$

4. Anneau des endomorphismes d'un groupe commutatif. Soit G un groupe commutatif, noté additivement. On note E l'ensemble des endomorphismes de G. Etant donnés f et g dans E, on définit les applications $y + g$ et fg de G dans G par

$$(f + g)(x) = f(x) + g(x), (fg)(x) = f(g(x))(x \in G).$$

$f + g$ est un endomorphisme de G, et il en est évidemment de même de $fg = f \circ g$. E est un groupe (commutatif) pour l'addition. La multiplication est évidemment associative et admet l'élément neutre Id_G. Par ailleurs, pour f, g et h dans E, posons $\phi = f(g+h)$; pour tout $x \in G$, on a

$$\phi(x) = f((g + h)(x) = f(g(x) + h(x))) = f(g(x)) + f(h(x))$$

car f est un endomorphisme de G ; on a donc $\phi = fg + fh$, et il est clair que $(g + h)f = gf + hf$. Par suite, E est un anneau (non commutatif en général) qu'on appelle anneau des endomorphismes de G.

On obtient un anneau commutatif dont l'élément unité est la constante l.

Corps

Definition. On dit qu'un anneau K est un corps s'il n'est pas réduit à 0 et si tout élément non nul de K est inversible.

Exemples de groupes (suite)

2. Groupes matriciels.

Le groupe général linéaire de degré n d'un anneau commutatif unitaire (ou d'un corps) K est le groupe des matrices $n \times n$ inversibles à coefficients dans K, muni de la multiplication matricielle. On le note $GL_n(K)$, ou GL_n, ou $GL(n, K)$.

Le groupe spécial linéaire d'ordre n d'un anneau commutatif unitaire (ou d'un corps) K, noté $SL(n,K)$, est le groupe des matrices de déterminant 1.

On appelle matrice triangulaire supérieure toute matrice carrée $M = (m_{i,j})$ d'ordre n telle que, si $j < i$, alors $m_{i,j} = 0$. On note par $T(n,K)$ l'ensemble des matrices triangulaires supérieures inversibles.

On dit qu'une matrice triangulaire est unitriangulaire, si $m_{i,i} = 1$. On note par $UT(n,K)$ l'ensemble des matrices unitriangulaires supérieures inversibles.

Sous-groupes

Definition. Soit H un sous-ensemble d'un groupe G. On dit que $(H,\cdot)$ est un sous-groupe de $(G,\cdot)$ si $(H,\cdot)$ est un groupe dont la loi $\cdot$ s'obtient par restriction de $\cdot$ à $H \times H$.

On dit qu'un sous-groupe H d'un groupe G est normal (ou distingué) dans G s'il est stable par conjugaison, c'est-à-dire si :

$$\forall h \in H,\ \forall x \in G, \qquad xhx^{-1} \in H.$$

On note alors $H \trianglelefteq G$.

Une façon équivalente de définir un sous-groupe distingué est de dire que les classes à droite et à gauche de H dans G coïncident, c'est-à-dire :

$$\forall x \in G, \qquad xH = Hx.$$

Exemple

Le groupe $SL(n,K)$ est un sous-groupe distingué de $GL(n,K)$.

Catégories

Definition. Une *catégorie* $\mathcal{C}$ se compose

* d'une classe dont les éléments sont appelés objets,

* d'un ensemble $\mathrm{Hom}\big(A,B\big)$, pour chaque paire d'objets A et B, dont les éléments f sont appelés morphismes (ou flèches) entre A et B, et sont parfois notés $f : A \to B$,

* d'un morphisme $\mathrm{id}_A : A \to A$, pour chaque objet A, appelé identité sur A,

* d'un morphisme $g \circ f : A \to C$ pour toute paire de morphismes $f : A \to B$ et $g : B \to C$, appelé composée de f et g, tel que :

* la composition est associative : pour tous morphismes $f : c \to d, g : b \to c$ et $h : a \to b$, $(f \circ g) \circ h = f \circ (g \circ h)$,

* les identités sont des éléments neutres de la composition : pour tout morphisme $f : A \to B$, $\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$.

Exemples

1. La catégorie (Ens), dont les objets sont les ensembles, et les flèches les applications, avec la composition usuelle des applications.

2. La catégorie (Top), dont les objets sont les espaces topologiques, et les flèches les applications continues, avec la composition usuelle.

3. La catégorie (Mon), dont les objets sont les monoïdes et les flèches les morphismes, avec la composition usuelle.

4. La catégorie (Grp), dont les objets sont les groupes et les flèches les morphismes, avec la composition usuelle.

5. On se donne un monoïde $(M,\cdot,e)$, et on définit la catégorie $\mathcal{M}$ ainsi :
objets : un seul ;
flèches : les éléments du monoïde, elles partent toute de l'unique objet pour y revenir ;
composition : donnée par la loi du monoïde (l'identité est donc la flèche associée à e).

6. On se donne un ensemble E muni d'une relation réflexive et transitive R, et on définit la catégorie associée $\mathcal{E}$ ainsi :

objets : les éléments de l'ensemble ;

flèches : pour tous objets a et b, il existe une flèche de a vers b si et seulement si aRb (et pas de flèche sinon) ;

composition : la composée de deux flèches est la seule flèche qui réunit les deux extrémités (la relation est transitive) ; l'identité est la seule flèche qui relie un objet à lui-même (la relation est réflexive).

Définition. Soit $\mathcal{C}$ une catégorie. On appelle catégorie opposée de $\mathcal{C}$ la catégorie, notée $\mathcal{C}^{op}$, dont les objets sont les mêmes que ceux de $\mathcal{C}$ et telle que si X, Y sont des objets de $\mathcal{C}^{op}$, on a

$$\mathrm{Hom}_{\mathcal{C}^{op}}\big(X, Y\big) = \mathrm{Hom}_{\mathcal{C}}\big(Y, X\big)$$

Foncteurs

Définition. Un foncteur (covariant) F d'une catégorie $\mathcal{C}$ vers une catégorie $\mathcal{D}$,

$$F : \mathcal{C} \longrightarrow \mathcal{D}$$

est la donnée

a) Pour tout objet X de $\mathcal{C}$ d'un objet F(X) de $\mathcal{D}$.

b) Pour tout couple d'objets (X, Y) de $\mathcal{C}$ et tout $f \in \mathrm{Hom}_{\mathcal{C}}\big(Y, X\big)$, d'un $F(f) \in \mathrm{Hom}_{\mathcal{D}}\big(F(X), F(Y)\big)$ tel que
   - pour tout objet X de $\mathcal{C}$, on a $F(1_X) = 1_{F(X)}$;
   - pour tout $f \in \mathrm{Hom}_{\mathcal{C}}\big(X, Y\big)$, pour tout $g \in \mathrm{Hom}_{\mathcal{C}}\big(Y, X\big)$, on a $F(g \circ f) = F(g) \circ F(f)$.

Références

[1] Bourbaki, N. *Éléments de mathématique. Algèbre. Chapitres 1 à 3.* Hermann, Paris, 1970. xiii+635 pp.

[2] MacLane, S. *Categories for the working mathematician.* Graduate Texts in Mathematics, Vol. 5. Springer-Verlag, New York-Berlin, 1971. ix+262 pp.

Département des Sciences Mathématiques, Université de Montpellier, Place Eugéne Bataillon, 34095 Montpellier cedex 5, France

E-mail address: vershini@math.univ-montp2.fr

ALGÈBRE 1
(COURS DE M1, 2018-2019)
HMMA 115M

COURS 3

Anneaux

Lorsqu'on parle d'éléments inversibles, d'éléments permutables, etc dans un anneau A, toutes ces notions sont relatives à la multiplication dans A.

Pour la loi induite par la multiplication, l'ensemble des éléments inversible est un groupe appelé *groupe multiplicatif* de A, noté parfois A^*.

Soient x, y dans A. On dit que x est *multiple à gauche* (resp. *à droite*) de y s'il existe $y' \in A$ tel que $x = y'y$ (resp. $x = yy'$) ; on dit encore que y est *diviseur à droite* (resp. *à gauche*) de x. Lorsque A est commutatif, il est inutile de préciser « à gauche » ou « à droite ».

Definition. Soit $x \in A$. On dit que x est *nilpotent* s'il existe un entier $n > 0$ tel que $x^n = 0$. Alors l'élément $1 - x$ est inversible, d'inverse égal à $1 + x + x^2 + \cdots + x^{n-1}$.

Comme A est un groupe commutatif pour l'addition, on a défini l'élément nx pour $n \in \mathbb{Z}$ et $x \in A$.

Proposition 1 (Formule du binôme)**.** *Soient x et y deux éléments permutables d'un anneau A. On a :*

$$(x+y)^n = \sum_{p=0}^{n} C_n^p x^p y^{n-p}.$$

Definition. Soient A et B deux anneaux. On appelle *morphisme*, ou *homomorphisme*, de A dans B toute application f de A dans B satisfaisant aux relations :

$$f(x+y) = f(x) + f(y), \quad f(xy) = f(x).(y), \quad f(1) = 1,$$

quels que soient x, y dans A.

Le composé de deux homomorphismes d'anneaux est un homomorphisme d'anneaux. Une application identique est aussi un homomorphisme d'anneaux. Alors il s'agit de *catégorie des anneaux*.

Soient A et B deux anneaux et f une application de A dans B ; pour que f soit un isomorphisme, il faut et il suffit que ce soit un homomorphisme bijectif ; dans ce cas, f^{-1} est un homomorphisme de B dans A. Un homomorphisme d'un anneau A dans lui-même s'appelle un *endomorphisme* de A.

Soit $f : A \to B$ un homomorphisme d'anneaux. L'application f est un homomorphisme du groupe additif de A dans le groupe additif de B ; en particulier, on a $f0) = 0$ et $f(-x) = -f(x)$ pour tout $x \in A$. L'image par f d'un élément inversible de A est un élément inversible de B, et la restriction de f au groupe multiplicatif de A est un homomorphisme de ce groupe dans le groupe multiplicatif de B.

Exemples

1. Soit A un anneau. On voit immédiatement que l'application

$$n \mapsto n.1$$

de $\mathbb{Z}$ dans A est l'unique homomorphisme de $\mathbb{Z}$ dans A. En particulier, l'application identique de $\mathbb{Z}$ est un endomorphisme de l'anneau $\mathbb{Z}$.

Prenons en particulier pour A l'anneau des endomorphismes du groupe additif $\mathbb{Z}$. L'application $n \mapsto n.1$ de $\mathbb{Z}$ dans A est un isomorphisme de $\mathbb{Z}$ sur A.

2. Soit a un élément inversible d'un anneau A. L'application

$$x \mapsto axa^{-1}$$

est un endomorphisme de A car on a

$$a(x+y)a^{-1} = axa^{-1} + aya^{-1},$$
$$a(xy)a^{-1} = (axa^{-1})(aya^{-1}).$$

Elle est bijective, car la relation $x' = axa^{-1}$ équivaut à $x = a^{-1}x'a$. C'est donc un automorphisme de l'anneau A, appelé *automorphisme intérieur* associé à a.

Sous-anneaux

Definition. Soit A un anneau. On appelle *sous-anneau* de A toute partie B de A qui est un sous-groupe de A pour l'addition, qui est stable pour la multiplication et contient l'unité de A.

Les conditions précédentes peuvent s'écrire

$$0 \in B, \quad B + B \subset B, \quad -B \subset B, \quad B.B \subset B, \quad 1 \in B.$$

Si B est un sous-anneau de A, on le munit de l'addition et de la multiplication induites par celles de A, qui en font un anneau. L'injection canonique de B dans A est un homomorphisme d'anneaux.

Exemples

1. Tout sous-groupe du groupe additif $\mathbb{Z}$ qui contient 1 est égal à $\mathbb{Z}$. Donc $\mathbb{Z}$ est le seul sous-anneau de $\mathbb{Z}$.

2. Soient A un anneau et (A_i) $i \in I$ une famille de sous-anneaux de A ; il est immédiat que $\cap_{i\in I} A_i$ est un sous-anneau de A. En particulier, l'intersection de tous les sous-anneaux de A contenant une partie X de A est un sous-anneau qui est appelé le *sous-anneau* de A *engendré par* X.

Definition. Soit A un anneau. On appelle le *centre* de A sous-ensemble de A composé de tous les éléments $a \in A$ tels que $ax = xa$ pour tout $x \in A$.

Le centre est un sous-anneau de A.

Definition. Soit A un anneau et M un monoïde. L'*anneau du monoïde* M, noté par $A[M]$ est l'ensemble des applications de M dans A de support fini (c'est-à-dire nulles sauf sur une partie finie de M), muni de la multiplication définie par :

$$(fg)(m) = \sum_{x,y\in M, xy=m} f(x)g(y).$$

Si l'on identifie chaque élément m de M avec la fonction caractéristique du singleton $\{m\}$, M s'identifie à une partie de $A[M]$ et $A[M]$ est muni du produit qui étend (par bilinéarité) la loi de monoïde de M. Plus explicitement, un élément de $A[M]$ est noté

$$f = \sum_{m\in M} f_m m, \quad f_m \in A,$$

où les éléments f_m sont presque tous nuls, et le produit de deux tels éléments est donné par :

$$\left(\sum_{x\in M} f_x x\right)\left(\sum_{y\in M} g_y y\right) = \sum_{m\in M}\left(\sum_{x,y\in M, xy=m} f_x g_y\right) m.$$

Si M est un groupe, $A[M]$ est appelée l'*anneau du groupe* M.

L'anneau A est un sous-anneau de $A[M]$. Plus général : si L est un sous-monoïde de M alors $A[L]$ est un sous-anneau de $A[M]$.

Exemples

1. Soit A un anneau et N est un monoïde libre engenré par une lettre x (isomorphe à monoïde de nombres naturels $\mathbb{N}$), alors $A[N] = A[x]$ est l'*anneau de polynômes par rapport au indéterminée* x *à coefficients dans* A.

2. Soit A un anneau et M est un monoïde libre commutatif engenré par lettres x_i, $i \in I$, (isomorphe à somme directe de monoïdes de nombres naturels $\mathbb{N}$), alors $A[M] = A[x_i], i \in I$, est l'*anneau de polynômes par rapport au indéterminées* x_i, $i \in I$ *à coefficients dans* A.

Idéaux

Definition. Soit A un anneau. On dit qu'une partie α de A est un *idéal à gauche* (resp. *à droite*) si α est un sous-groupe du groupe additif de A et si les relations $a \in A$, $x \in \alpha$ entraînent $ax \in \alpha$ (resp. $xa \in \alpha$). On dit que α est un *idéal bilatère* de A si a est à la fois un idéal à gauche et un idéal à droite de A.

Dans un anneau commutatif, les trois espèces d'idéaux se confondent ; on les appelle simplement idéaux.

La définition d'un idéal à gauche se traduit par les relations

$$0 \in \alpha, \quad \alpha + \alpha \subset \alpha, \quad A.\alpha \subset \alpha,$$

la relation $-\alpha \subset \alpha$ résultant de la formule $(-1).x = -x$ et de $A.\alpha \subset \alpha$. Pour tout $x \in A$, soit γ_x l'application $a \mapsto xa$ de A dans A ; l'application $x \mapsto \gamma_x$ définit l'action de A sur le groupe additif $< A, + >$. Les idéaux à gauche de A ne sont autres que les sous-groupes de $< A, + >$ stables pour cette action.

Exemples

1. Soit A un anneau. L'ensemble A est un idéal bilatère de A ; il en est de même de l'ensemble réduit à 0, qu'on appelle l'idéal nul et qu'on écrit parfois 0 ou (0) au lieu de $\{0\}$.

2. Pour tout élément a de A, l'ensemble $A.a$ des multiples à gauche de a est un idéal à gauche ; de même l'ensemble $a.A$ est un idéal à droite. Lorsque a est dans le centre de A, on a $A.a = a.A$; cet idéal s'appelle l'*idéal principal engendré par* a et se note (a). On a $(a) = A$ si et seulement si a est inversible.

3. Soit M une partie de A. L'ensemble des éléments $x \in A$ tels que $xy = 0$ pour tout $y \in M$ est un idéal à gauche de A qu'on appelle l'*annulateur à gauche* de M. On définit de manière analogue l'annulateur à droite de M.

4. Toute intersection d'idéaux à gauche (resp. à droite, bilatères) de A est un idéal à gauche (resp. à droite, bilatère). Etant donnée une partie X de A, il existe donc un plus petit idéal à gauche (resp. à droite, bilatère) contenant X ; on l'appelle l'idéal à gauche (resp. à droite, bilatère) *engendré* par X.

Proposition 2. *Soient A un anneau, (x_λ), $\lambda \in L$ une famille d'éléments de A, α (resp. β) l'ensemble des sommes finies*

$$\sum_{\lambda \in L} a_\lambda x_\lambda \ a_\lambda \in A$$

$$(resp. \quad \sum_{\lambda \in L} a_\lambda x_\lambda b_\lambda \ a_\lambda, b_\lambda \in A).$$

Alors α (resp. β) est l'idéal à gauche (resp. bilatère) de A engendré par l'ensemble des x_λ.

Definition. Soit

$$f : A \to B$$

un homomorphisme d'anneaux. Son *noyau* est le noyau en tant qu'homomorphism des groupes.

Proposition 3. *Le noyau d'un homomorphisme d'anneaux*

$$f : A \to B$$

est un idéal bilatère.

Soit α un idéal à gauche de A. Les conditions $1 \notin \alpha$, $\alpha \neq A$ sont évidemment équivalentes.

Definition. Soit A un anneau. On dit qu'un idéal à gauche α est *maximal* s'il est un élément maximal de l'ensemble des idéaux à gauche distincts de A.

Théorème 1 (Krull)**.** *Soient A un anneau et α un idéal à gauche de A distinct de A. Il existe un idéal à gauche maximal μ de A contenant α.*

Démonstration. On utilise lemme de Zorn. □

Rappel sur Lemme de Zorn

Définition. Une *relation d'ordre (partiel)* sur un ensemble X est une partie R de $X \times X$ telle que
- $(x, x) \in R$, pour tout $x \in X$;
- $(x, y) \in R,\ (y, x) \in R => x = y$;
- $(x, y) \in R,\ (y, z) \in R => (x, z) \in R$.

On note $x \leq y$ au lieu de $(x, y) \in R$.

Exemples

1. L'ordre usuel sur $\mathbb{R}$ est *total* : $\forall x, y \in R$, on a $x \leq y$ ou $y \leq x$.
2. L'inclusion $A \subset B$ définit un ordre sur les parties d'un ensemble.

Définition. Soient X un ensemble ordonné, A une partie non vide de X et $x \in X$;
- x *majore* (resp. *minore*) A si $y \leq x\ \forall\ y \in A$ (resp. si $y \geq x\ \forall\ y \in A$) ;
- x est une *borne supéerieure* (resp. *inférieure*) de A si x majore A et si $x \leq y$, pour tout majorant y de A (resp. si x minore A et si $x \geq y$, pour tout minorant y de A).

Définition. Dans un ensemble ordonné, un élément *maximal* est un élément tel qu'il n'existe aucun autre élément de cet ensemble qui lui soit supérieur, c'est-à-dire que a est dit élément maximal d'un ensemble ordonnné X si a est un élément de X tel que pour tout x appartenant à X, $a \leq x$ implique $a = x$.

Lemme de Zorn. *Soit X un ensemble (partiellement) ordonné. Supposons que toute partie (non vide) totalement ordonnée admette une borne supérieure. Alors X possède un élément maximal.*

Références

[1] Bourbaki, N. *Éléments de mathématique. Algèbre. Chapitres 1 à 3.* Hermann, Paris 1970 xiii+635 pp.

[2] Lang, S. *Algèbre.* Dunod, Paris, 2004, 926 pp.

Département des Sciences Mathématiques, Université de Montpellier, Place Eugéne Bataillon, 34095 Montpellier cedex 5, France

E-mail address: vershini@math.univ-montp2.fr

ALGÈBRE 1
(COURS DE M1, 2018-2019)
HMMA 115M

COURS 4

Anneaux (suite)

Proposition 1. *Soient A un anneau, (α_λ), $\lambda \in L$ une famille d'idéaux à gauche de A. L'idéal à gauche engendré par*

$$\bigcup_{\lambda\in L} \alpha_\lambda$$

se compose des sommes finies

$$\sum_{\lambda\in L} y_\lambda, \quad y_\lambda \in \alpha_\lambda.$$

Définition. On dit que l'idéal α engendré par $\cup_{\lambda\in L}\alpha_\lambda$ est la *somme des idéaux à gauche* α_λ et on le note

$$\sum_{\lambda\in L} \alpha_\lambda.$$

Corollaire 1. *La somme $\alpha_1+\alpha_2$ de deux idéaux à gauche se compose des sommes a_1+a_2 avec $a_1 \in \alpha_1$ et $a_2 \in \alpha_2$.*

Idéaux de $\mathbb{Z}$

Un idéal de $\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$, donc de la forme $n.\mathbb{Z}$ avec $n \geq 0$; réciproquement, pour tout entier $n \geq 0$, l'ensemble $n.\mathbb{Z}$ est un idéal, l'idéal principal (n). Donc tout idéal de $\mathbb{Z}$ est principal, et se représente de manière unique sous la forme $n.\mathbb{Z}$ avec $n \geq 0$. L'idéal (1) est égal à $\mathbb{Z}$, l'idéal (0) est réduit à 0, et les idéaux distincts de $\mathbb{Z}$ et $\{0\}$ sont donc de la forme $n.\mathbb{Z}$ avec $n > 1$. Si $m \geq 1$ et $n \geq 1$, on a $m.\mathbb{Z} \supset n.\mathbb{Z}$ si et seulement si $n \in m.\mathbb{Z}$, c'est-à-dire si m divise n. Par suite, pour que l'idéal $n.\mathbb{Z}$ soit maximal, il faut et il suffit qu'il n'existe aucun entier $m > 1$ distinct de n divisant n ; autrement dit, les idéaux maximaux de $\mathbb{Z}$ sont les idéaux de la forme $p.\mathbb{Z}$ où p est un nombre premier.

Soient m et n deux entiers ≥ 1. L'idéal $m.\mathbb{Z}+n.\mathbb{Z}$ est principal, d'où l'existence d'un entier $d \geq 1$ caractérisé par $d.\mathbb{Z} = m.\mathbb{Z}+n.\mathbb{Z}$; pour tout entier $r \geq 1$, la relation « r divise d » équivaut à $r.\mathbb{Z} \supset d.\mathbb{Z}$, donc à « $r.\mathbb{Z} \supset m.\mathbb{Z}$ et $r.\mathbb{Z} \supset n.\mathbb{Z}$ » c'est- à-dire à « r divise m et n ». On voit donc que les diviseurs communs à m et n sont les diviseurs de d et que d est par suite le plus grand des diviseurs ≥ 1 communs à m et n ; on appelle d *le plus grand commun diviseur* (en abrégé p.g.c.d.) de m et n. Comme $d.\mathbb{Z} = m.\mathbb{Z}+n.\mathbb{Z}$, il existe deux entiers x et y tels que $d = mx+ny$. On dit que m et n sont *étrangers* ou *premiers entre eux* si leur p.g.c.d. est égal à 1. Il revient au même de supposer qu'il existe des entiers x et y tels que $mx + ny = 1$. L'intersection des idéaux $m.\mathbb{Z}$ et $n.\mathbb{Z}$ n'est pas nulle car elle contient mn, donc est de la forme $r.\mathbb{Z}$ avec $r \geq 1$. En raisonnant comme précédemment, on voit que les multiples de r sont les multiples communs à m et n, et que r est le plus petit des entiers ≥ 1 multiples communs de m et n ; on l'appelle *le plus petit commun multiple* (p.p.c.m.) de m et n.

Caractéristique

Proposition 2. *Soit A un anneau. Alors il existe un unique morphisme d'anneaux f de $\mathbb{Z}$ dans A.*

Il faut noter que l'image de f est le sous-anneau de A engendré par 1. Cette image est isomorphe à $\mathbb{Z}/\ker f$. Or, tout idéal de $\mathbb{Z}$ est de la forme (n), avec $n \in \mathbb{N}$. Posons donc $\ker f = (n)$. Si $n = 0$, l'image de f est isomorphe à $\mathbb{Z}$, et on dira que A est de *caractéristique nulle*. Si n est fini, on dit que A est de *caractéristique* n. Dans ce cas, n est le plus petit entier strictement positif tel que la somme de $n1_A$ vaut 0_A. L'image de $\mathbb{Z}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Anneaux quotients

Définition. Soit E un ensemble. On dit qu'une loi de composition T et une relation d'équivalence R dans E sont compatibles si les relations $x \equiv x'(\mathrm{mod}\, R)$ et $y \equiv y' \,\mathrm{mod}\, R)$ pour x, x', y, y' dans E) entraînent $xTy \equiv x'Ty'(\mathrm{mod}\, R)$; la loi de composition sur l'ensemble quotient E/R qui, aux classes d'équivalence de x et de y, fait correspondre la classe d'équivalence de xTy, s'appelle la *loi quotient* de la loi T par R.

Soit A un anneau. Si α est un idéal bilatère de A, on dit que deux éléments x et y de A sont *congrus modulo* α et l'on écrit $x \equiv y(\mathrm{mod}\,.\alpha)$ a) ou $x \equiv y(\alpha)$ si $x - y \in \alpha$. On a là une relation d'équivalence dans A. Les relations $x \equiv y(\alpha)$ et $x' \equiv y'(\alpha)$ entraînent $x+x' \equiv y+y'(\alpha)$, $xx' \equiv xy'(\alpha)$, car α est idéal à gauche, et $xy' \equiv yy'(\alpha)$ car a est idéal à droite, d'où $xx' \equiv yy'(\alpha)$. Réciproquement, si R est une relation d'équivalence sur A compatible avec l'addition et la multiplication, l'ensemble α des éléments x tels que $x \equiv 0 \,\mathrm{mod}\,.R$ est un idéal bilatère et la relation $x \equiv y \,\mathrm{mod}\,.R$ équivaut à $x \equiv y \,\mathrm{mod}\,.\alpha$.

Soient A un anneau et α un idéal bilatère de A. On note A/α l'ensemble quotient de A par la relation d'équivalence $x \equiv y(\mathrm{mod}\,\alpha)$, muni de l'addition et de la multiplication quotients de celles de A. Montrons que A/α est un anneau :

a) Pour l'addition, A/α est le groupe commutatif quotient du groupe additif de A par le sous-groupe α.

b) Pour la multiplication, A/α est un monoïde.

c) Distributivité on montre directement.

Définition. Soient A are anneau et α un idéal bilatère de A. On appelle *anneau quotient* de A par α et l'on note A/α l'ensemble quotient de A par la relation d'équivalence $x \equiv y(\alpha)$, muni de l'addition et de la multiplication quotients de celles de A.

L'anneau $A/0$ est isomorphe à A, et A/A est un anneau nul.

Exemple. Pour tout entier $n \geq 1$, l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ s'appelle *anneau des entiers modulo* n ; il a n éléments, qui sont les classes modulo n des entiers $0, 1, 2, ..., n-1$. Pour $n = 1$, on obtient un anneau nul.

Théorème 1. *Soient A un anneau et α un idéal bilatère de A.*

a) L'application canonique π de A sur A/α est un homomorphisme d'anneaux.

b) Soient B un anneau et f un homomorphisme de A dans B. Si $f(\alpha) = \{0\}$, il existe un homomorphisme $\bar{f}$ de A/α dans B et un seul tel que $\bar{f} = f \circ \pi$.

Théorème 2. *Soient A et B des anneaux, f un homomorphisme de A dans B.*

a) Le noyau α de f est un idéal bilatère de A.

b) L'image $B' = f(A)$ de f est un sons-anneau de B.

c) Soient $\pi : A \to A/\alpha$ et $i : B' \to B$ les morphismes canoniques. Il existe un morphisme $\bar{f}$ de A/α dans B' et un seul tel que $f = i \circ \bar{f} \circ \pi$, et $\bar{f}$ est un isomorphisme.

Sous-anneaux et idéaux dans un anneau quotient

Proposition 3. *Soient A et A' deux anneaux, f un homomorphisme de A dans A', et α le noyau de f.*

a) Soit B' un sous-anneau de A'. Alors $B = f^{-1}(B')$ est un sous-anneau de A contenant α. Si f est surjectif, on a $f(B) = B'$, et $f|B$ définit par passage au quotient un isomorphisme de B/α sur B'.

b) Soit β' un idéal à gauche (resp. à droite, bilatère) de A'. Alors $\beta = f^{-1}(\beta')$ est un idéal à gauche (resp. à droite, bilatère) de A contenant α.

c) Si β' un idéal bilatère de A', l'application composée du morphisme canonique $A' \to A'/\beta'$ et de $f : A \to A'$ définit, par passage au quotient, un morphisme injectif $\bar{f}$ de A/β dans A'/β'. Si f est surjectif, $\bar{f}$ est un isomorphisme de A/β sur A'/β'.

d) Supposons f surjectif. Soit Φ l'ensemble des sous-anneaux (resp. idéaux à gauche, idéaux à droite, idéaux bilatères) de A contenant α. Soit Φ' l'ensemble des sous-anneaux (resp. idéaux à gauche, idéaux à droite, idéaux bilatères) de A'. Les applications

$$B \mapsto f(B)$$

et

$$B' \mapsto f^{-1}(B')$$

sont des bijections réciproques de Φ sur Φ' et de Φ' sur Φ.

Corollaire 2. *Soient A un anneau et α un idéal bilatère de A.*

a) Tout idéal à gauche (resp. à droite, bilatère) de A/α s'écrit de manière unique sous la forme β/α, où β est un idéal à gauche (resp. à droite, bilatère) de A contenant α.

b) Si β est bilatère, l'homomorphisme composé

$$A \to A/\alpha \to (A/\alpha)/(\beta/\alpha)$$

définit par passage au quotient un isomorphisme de A/β sur $(A/\alpha)/(\beta/\alpha)$.

Multiplication des idéaux

Soient A un anneau, α et β des idéaux bilatères de A. L'ensemble des éléments de la forme

$$x_1y_1 + \cdots + x_ny_n \quad \text{avec } n \geq 0,\ x_i \in \alpha \text{ et } y_i \in b \quad \text{pour } 1 \leq i \leq n,$$

est évidemment un idéal bilatère de A, qu'on note $\alpha\beta$ et qu'on appelle le *produit* des idéaux bilatères α et β. Pour cette multiplication, l'ensemble des idéaux bilatères de A est un monoïde, ayant pour élément unité l'idéal bilatère A. Si α, β et γ sont des idéaux bilatères de A, on a

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma, \quad (\beta + \gamma)\alpha = \beta\alpha + \gamma\alpha.$$

On a

$$\alpha(0) = (0)\alpha = (0).$$

Si A est commutatif, la multiplication des idéaux est commutative.

On a

$$\alpha\beta \subset \alpha A \subset \alpha \text{ et } \alpha\beta \subset A\beta \subset \beta,$$

donc

$$\alpha\beta \subset \alpha \cap \beta. \tag{1}$$

Définition. Un *demi-anneau*, ou un *semi-anneau*, est une structure algébrique $(E, +, \times, 0, 1)$ telle que

1) $(E, +, 0)$ constitue un monoïde commutatif ;
2) $(E, \times, 1)$ forme un monoïde ;
3) $\times$ est distributif par rapport à $+$;
4) 0 est *absorbant* pour le produit, autrement dit : pour tout $x \in E$ $x \times 0 = 0 \times x = 0$.

Un demi-anneau est commutatif quand son produit est commutatif.

Remarque. Contrairement à ce qui se passe avec les anneaux, on ne peut démontrer à partir des autres axiomes que 0 est un élément absorbant.

Proposition 4. *L'ensemble des idéaux bilatères d'un anneau forme une structure de semi-anneau.*

Produit d'anneaux

Soit $(A_i)i \in I$ une famille d'anneaux. Soit A l'ensemble produit $\prod_{i\in I} A_i$. Sur A, on définit une addition et une multiplication par les formules

$$(x_i) + (y_i) = (x_i + y_i), \quad (x_i) \cdot (y_i) = (x_i \cdot y_i).$$

On vérifie immédiatement que A est un anneau (dit *produit* des anneaux A_i) ayant pour zéro l'élément $0 = (0_i)_{i\in I}$ où 0_i est le zéro de A_i, et pour unité $1 = (1_i)_{i\in I}$ où 1_i est l'unité de A_i. Si les A_i sont commutatifs, il en est de même de A. Si C_i, est le centre de A_i, le centre de A est $\prod_{i\in I} C_i$.

Pour tout $i \in I$, la projection pr_i de A sur A_i est un homomorphisme d'anneaux. Si B est un anneau et $f_i : B \to A_i$ une famille d'homomorphismes, il existe un unique homomorphisme $f : B \to A$ tel que $f_i = \mathrm{pr}_i \circ f$ pour tout $i \in I$; il est donné par $f(b) = (f_i(b))_{i\in I}$.

Pour tout $i \in I$, soit α_i un idéal à gauche de A_i. Alors $\alpha = \prod_{i\in I} \alpha_i$ est un idéal à gauche de A. On a un énoncé analogue pour les idéaux à droite, les idéaux bilatères et les sous-anneaux. Supposons que a_i soit un idéal bilatère pour tout $i \in I$, et notons f_i l'application canonique de A_i sur A_i/α_i. Alors l'application

$$f : (x_i)_{i\in I} \mapsto (f(x_i))_{i\in I}$$

de $\prod_{i\in I} A_i$ sur $\prod_{i\in I}(A_i/\alpha_i)$ est un homomorphisme d'anneaux de noyau$\prod_{i\in I} \alpha_i$, donc définit par passage au quotient un isomorphisme de $\prod_{i\in I}(A_i/\alpha_i)/(\prod_{i\in I} \alpha_i)$ sur $\prod_{i\in I}(A_i/\alpha_i)$.

Définition. Soit A un anneau. On dit que deux idéaux α et β de A sont premiers entre eux si $\alpha + \beta = A$. Ceci est possible si et seulement s'il existe $a \in \alpha$, $b \in \beta$ tels que $a + b = 1$.

Théorème 3 (Théorème chinois)**.** *Soit A un anneau et soient α et β deux idéaux propres de A et soit :*

$$\phi : A/\alpha \cap \beta \to A/\alpha \times A/\beta$$

le morphisme naturel qui envoie $\bar{x} \in A/(\alpha \cap \beta)$ sur $(\bar{x}_\alpha, \bar{x}_\beta) \in A/\alpha \times A/\beta$. Si α et β sont premiers entre eux alors ϕ est un isomorphisme.

Corollaire 3. *Soit A un anneau et soient α_1, α_2, ..., α_k des idéaux propres de A tels que α_i et α_j sont premiers entre eux si $i \neq j$ et posons $\alpha = \cap_{i=1}^k \alpha_i$. Alors on a un isomorphisme comme au point (a) :*

$$\phi : A/\alpha \cong A/\alpha_1 \times A/\alpha_2 \times \cdots \times A/\alpha_k.$$

Références

[1] Bourbaki, N. *Éléments de mathématique. Algèbre. Chapitres 1 à 3.* Hermann, Paris 1970 xiii+635 pp.

[2] Lang, S. *Algèbre*. Dunod, Paris, 2004, 926 pp.

Département des Sciences Mathématiques, Université de Montpellier, Place Eugéne Bataillon, 34095 Montpellier cedex 5, France

E-mail address: vladimir.verchinine@umontpellier.fr

ALGÈBRE 1
(COURS DE M1, 2018-2019)
HMMA 115M

COURS 5

Anneaux commutatifs, anneaux des fractions

Monoïde des fractions d'un monoïde commutatîf

Soient E un monoïde commutatif, S une partie de E et S' le sous-monoïde de E engendré par S.

Lemme 1. *Dans $E \times S'$, la relation $R(x, y)$ que voici :*
«il existe a, b dans E et p, q, s dans S' tels que $x = (a, p)$, $y = (b, q)$, et $aqs = bps$»
est une relation d'équivalence compatible avec la loi du monoïde produit $E \times S'$.

Définition. Soient E un monoïde commutatif, S une partie de E et S' le sous-monoïde de E engendré par S. On note E_S et l'on appelle *monoïde des fractions de E associé à S* (ou *à dénominateurs dans S*) le monoïde quotient $(E \times S')/R$, où la relation d'équivalence R est décrite comme dans le lemme 1.

Pour $a \in E$ et $b \in S'$, la classe de (a, p) modulo R se note en général a/p et s'appelle la *fraction de numérateur a et dénominateur p*. On a donc par définition

$$(a/p).(a'/p') = aa'/pp'.$$

Les fractions a/p et a'/p' sont égales si et seulement s'il existe s dans S' avec $spa' = sp'a$; En particulier, on a $a/p = sa/sp$ pour $a \in A$ et s, p dans S'. L'élément neutre de E_S est la fraction e/e. On posera $a/e = \epsilon(a)$ pour tout $a \in E$. Ce qui précède montre que ϵ est un homomorphisme de E dans E_S, dit *canonique*. Pour tout $p \in S'$, on a

$$(p/e).(e/p) = e/e,$$

donc e/p est inverse de $\epsilon(p) = p/e$; tout élément de $\epsilon(S')$ est donc inversible. On a $a/p = (a/e)(e/p)$, d'où

$$a/p = \epsilon(a).s\epsilon(p)^{-1}$$

pour $a \in A$ et $p \in S$; le monoïde E_S est donc engendré par $\epsilon(E) \cup \epsilon(S)^{-1}$.

Définition. Un élément a d'un magma E est dit *simplifiable* ou *régulier*) *à gauche* (resp. *à droite*) si la translation à gauche (resp. à droite) par a est injective. Un élément simplifiable à gauche et à droite est appelé élément simplifiable (ou régulier).

Proposition 1. *Soient E un monoïde et x un élément de E. Si x est inversible à gauche, il est simplifiable à gauche. En particulier, si x est inversible, les translations à gauche et à droite par x sont bijectives.*

Proposition 2. *(i) Soient E un monoïde et $a, b \in E$; pour qu'on ait $\epsilon(a) = \epsilon(b)$, il faut et il suffit qu'il existe $s \in S'$ avec $sa = sb$.*
(ii) Pour que ϵ soit injectif il faut et il suffit que tout élément de S soit simplifiable.
(iii) Pour que ϵ soit bijectif il faut et il suffit que tout élément de S soit inversible.

Théorème 1. *Soient E un monoïde commutatif, S une partie de E, E_S le monoïde de fractions associé à S et $\epsilon : E \to E_S$ l'homomorphisme canonique. Soit de plus f un homomorphisme de E dans un monoïde F (non nécessairement commutatif), tel que tout élément de $f(S)$ soit inversible dans F. Il existe un homomorphisme $\bar{f}$ et un seul de E_S dans F tel que $f = \bar{f} \circ \epsilon$.*

Exemples des monoïde des fractions

1. Soit $\bar{E} = E_E$. Comme le monoïde $\bar{E}$ est engendré par l'ensemble $\epsilon(E) \cup \epsilon(E)^{-1}$ qui se compose d'éléments inversibles, tout élément de $\bar{E}$ est inversible. Autrement dit, $\bar{E}$ est un groupe commutatif. De plus d'après le Th. 1, tout homomorphisme f de E dans un groupe G se factorise de manière unique sous la forme $f = \bar{f} \circ \epsilon$ où $\bar{f} : E \to G$ est un homomorphisme. On dit que E est le *groupe des fractions* de E (ou *groupe des différences* de E dans le cas de la notation additive).

2. Soit $\Phi = E_S$, où S se compose des éléments simplifiables de E. D'après Proposition 2 (ii), l'homomorphisme canonique de E dans Φ est injectif ; on en profitera pour identifier E à son image dans Φ. Par suite, E est un sous-monoïde de Φ, tout élément simplifiable de E a un inverse dans Φ, et tout élément de Φ est de la forme $a/p = a.p^{-1}$ avec $a \in E$ et $p \in S$; on a $a/p = a'/p'$ si et seulement si l'on a $ap' = pa'$. On voit facilement que les éléments inversibles de Φ sont les fractions a/p avec a et p simplifiables et que p/a est l'inverse de a/p.

3. Entiers rationnels.

Considérons le monoïde commutatif $\mathbb{N}$ des entiers naturels, la loi de composition étant l'addition ; tous les éléments de $\mathbb{N}$ sont simplifiables pour cette loi. Le groupe des différences de $\mathbb{N}$ se note $\mathbb{Z}$; ses éléments sont appelés les entiers rationnels ; sa loi s'appelle addition des entiers rationnels et se note encore + . L'homomorphisme canonique de $\mathbb{N}$ dans $\mathbb{Z}$ est injectif, et nous identifierons chaque élément de $\mathbb{N}$ à son image dans $\mathbb{Z}$. Les éléments de $\mathbb{Z}$ sont, par définition, les classes d'équivalence déterminées dans $\mathbb{N} \times \mathbb{N}$ par la relation $m_1 + n_2 = m_2 + n_1$ entre (m_l, n_1) et (m_2, n_2) ; un élément m de $\mathbb{N}$ est identifié avec la classe formée des éléments $(m + n, n)$ où $n \in \mathbb{N}$; il admet pour opposé dans Z la classe des éléments $(n, m + n)$. Tout élément (p, q) de $\mathbb{N} \times \mathbb{N}$ peut s'écrire sous la forme $(m + n, n)$ si $p \geq q$, sous la forme $(n, m + n)$ si $p \leq q$; il s'ensuit que $\mathbb{Z}$ est la réunion de $\mathbb{N}$ et de l'ensemble des opposés des éléments de $\mathbb{N}$. L'élément neutre 0 est le seul élément de $\mathbb{N}$ dont l'opposé appartienne à $\mathbb{N}$. Pour tout entier naturel m, on note $-m$ l'entier rationnel opposé de m, et on note $-\mathbb{N}$ l'ensemble des éléments $-m$ pour $m \in N$. On a

$$\mathbb{Z} = \mathbb{N} \cup (-N) \text{ et } \mathbb{N} \cap (-\mathbb{N}) = 0.$$

Pour $m \in \mathbb{N}$, on a $m = -m$ si et seulement si $m = 0$.

Anneaux de fractions

Théorème 2. *Soient A un anneau commutatif et S une partie de A. Soit A_S le monoïde des fractions de A à dénominateurs dans S. Soit $\epsilon : A \to A_S$ le morphisme canonique. Il existe sur A_S une addition et une seule satisfaisant aux conditions suivantes :*

a) A_S, muni de cette addition et de sa multiplication, est un anneau commutatif ;

b) ϵ est un homomorphisme d'anneaux.

Définition. L'anneau défini au th. 2 s'appelle *anneau des fractions de A associé à S*, ou ıà dénominateurs dans S, et se note $A[S^{-1}]$. Le zéro $A[S^{-1}]$ est $0/1$, l'unité de $A[S^{-1}]$ est $1/1$.

Si S est l'ensemble des éléments simplifiables de A, l'anneau $A[S^{-1}]$ s'appelle *l'anneau total des fractions de A*. On identifie alors A à un sous-anneau de $A[S^{-1}]$. grâce a l'application ϵ, qui est alors injective.

Théorème 3. *Soient A un anneau commutatif, S une partie de A, B un anneau, f un homomorphisme de A dans B tel que tout élément de $f(S)$ soit inversible. Il existe un homomorphisme $\bar{f}$ de $A[S^{-1}$ dans B et un seul tel que $f = \bar{f} \circ \epsilon$.*

Le corps des nombres rationnels

Définition. On appelle *corps des nombres rationnels*, et l'on désigne par $\mathbb{Q}$,, le corps des fractions de l'anneau $\mathbb{Z}$ des entiers rationnels. Les éléments de $\mathbb{Q}$ sont appelés *nombres rationnels*.

Tout nombre rationnel est donc une fraction de la forme a/b où a et b sont des entiers rationnels avec $b \neq 0$ (et même $b > 0$ comme le prouve la relation $a/b = (-a)/(-b)$).

Corps

Théorème 4. *Soit A un anneau. Les conditions suivantes sont équivalentes :*
a) A est un corps ;
b) A est non réduit à 0, et les seuls idéaux à gauche de A sont 0 et A.

Corollaire 1. *Soient A un anneau et α un idéal bilatère de A. Pour que l'anneau A/α soit un corps, il faut et il suffit que α soit un idéal à gauche maximal de A.*

Corollaire 2. *Soit A un anneau commutatifnon réduit à 0. Il existe un homomorphisme de A sur un corps commutatif.*

Corollaire 3. *Soit a un entier ≥ 0. Pour que l'anneau $\mathbb{Z}/a\mathbb{Z}$ soit un corps, il faut et il suffit que a soit premier.*

Pour p premier, le corps $\mathbb{Z}/p\mathbb{Z}$ se note $\mathbb{F}_p$.

Théorème 5. *Soient K un corps et A un anneau non réduit à 0. Si f est un homomorphisme de K dans A, alors le sous-anneau $f(K)$ de A est un corps et f définit un isomorphisme de K sur (K).*

Anneaux intègres

Définition. On dit qu'un anneau A est *intègre* (ou que A est un anneau *d'intégrité*) s'il est commutatif, non réduit à 0, et si le produit de deux éléments non nuls de A est non nul.

L'anneau $\mathbb{Z}$ des entiers rationnels est intègre : il est commutatif, non réduit à 0 ; le produit de deux entiers > 0 est non nul ; tout entier non nul est de la forme a ou $-a$ avec $a > 0$, et l'on a $(-a)b = -ab$, $(-a)(-b) = ab$ pour $a > 0$, $b > 0$, d'où notre assertion.

Proposition 3. *La caractéristique d'un anneau intègre est soit nulle, soit un nombre premier.*

Tout corps commutatif est un anneau intègre. Un sous-anneau d'un anneau intègre est intègre. En particulier, un sous-anneau d'un corps commutatif est intègre. Nous allons montrer que réciproquement tout anneau intègre A est isomorphe à un sous-anneau d'un corps commutatif. Rappelons que l'on a identifié A à un sous-anneau de son anneau total des fractions. Notre assertion résulte alors de la proposition suivante :

Proposition 4. *Si A est un anneau intègre, l'anneau total des fractions K de A est un corps commutatif.*

Démonstration. L'anneau K est commutatif. Il est non réduit à 0 puisque $A \neq \{0\}$. Comme A est intègre, tout élément non nul de A est simplifiable, et K se compose des fractions a/b avec $b \neq 0$. Or $a/b = 0$ entraîne $a \neq 0$, et la fraction b/a est alors inverse de a/b. □

Définition. L'anneau total des fractions d'un anneau intègre s'appelle son *corps des fractions.*

On identifie un tel anneau à son image dans son corps des fractions.

Proposition 5. *Soient B un anneau non réduit à 0, A un sous-anneau commutatif de B tel que tout élément non nul de A soit inversible dans B.*
a) A est intègre.
b) Soit A' le corps des fractions de A. L'injection canonique de A dans B se prolonge de manière unique en un isomorphisme f de A' sur un sous-corps de B.
c) Les éléments de $f(A')$ sont les xy^{-1} où $x \in A, y \in A, y \neq 0$.

Idéaux premiers

Proposition 6. *Soient A un anneau commutatif, ρ un idéal de A. Les conditions suivantes sont équivalentes :*

a) l'anneau A/ρ est intègre ;

b) $A \neq \rho$ et, si $x \in A \setminus \rho$ et $y \in A \setminus \rho$, on a $xy \in A \setminus \rho$;

c) ρ est le noyau d'un homomorphisme de A dans un corps.

Définition. Dans un anneau commutatif A, on appelle idéal *premier* un idéal ρ vérifiant les conditions de la prop. 3.

Exemples

1. Soit A un anneau commutatif. Si μ est un idéal maximal de A, μ est premier ; en effet, l'anneau A/μ est un corps.

2 Si A est un anneau intègre, l'idéal $\{0\}$ de A est premier (mais non maximal en général, comme le prouve l'exemple de l'anneau $\mathbb{Z}$).

Éléménts irréductibles et premiers

Définition. Soit A un anneau commutatif intègre. Si $a \in A \setminus \{0\}$, on dit que a est *irréductible* (parfois on dit *indécomposable*) s'il vérie :

(i) a n'est pas inversible et

(ii) si $x, y \in A$ sont tels que $xy = a$, alors soit x est inversible, soit y est inversible.

Si $a \in A \setminus \{0\}$, on dit que a est *premier* s'il vérie :

(i) a n'est pas inversible et

(ii) si $x, y \in A$ sont tels que a divise xy, alors a divise x ou a divise y.

En particulier, tout élément premier est indécomposable. La réciproque est fausse.

Exemple

Soit $A = \mathbb{Z}[i\sqrt{3}]$. L'éléments 2, est irréductible, mais non premier.

Soient $x, y \in A$ où A est un anneau intègre. On dit que x, y admettent un plus petit commun multiple (PPCM) s'il existe $m \in A$ tel que $x|m$, $y|m$ et tout élément m' de A tel que $x|m'$ et $y|m'$ vérife $m|m'$. Un tel m est alors unique à multiplication par un élément inversible près. On dit que m est un *plus petit commun multiple* (un PPCM) de x et y, mais, le plus souvent, par abus de langage, on dit que c'est "le" plus petit commun multiple (le PPCM).

On dit que x, y admettent un *plus grand commun diviseur* (PGCD) s'il existe $d \in A$ tel que $d|x$, $d|y$ et tout élément d' de A tel que $d'|x$ et $d'|y$ vérife $d'|d$. Un tel d est alors unique à multiplication par un élément inversible près. On dit que d est un plus grand commun diviseur (un PGCD) de x et y, mais, le plus souvent, par abus de langage, on dit que c'est "le" plus grand commun diviseur (le PGCD).

Références

[1] Bourbaki, N. *Éléments de mathématique. Algèbre. Chapitres 1 à 3.* Hermann, Paris 1970 xiii+635 pp.

[2] Lang, S. *Algèbre.* Dunod, Paris, 2004, 926 pp.

Département des Sciences Mathématiques, Université de Montpellier, Place Eugéne Bataillon, 34095 Montpellier cedex 5, France

E-mail address: vershini@math.univ-montp2.fr

ALGÈBRE 1
(COURS DE M1, 2018-2019)
HMMA 115M

COURS 6

MODULES

Définition. Etant donné un anneau A, on appelle *module à gauche* sur A (ou A-*module à gauche*), un ensemble E muni d'une structure algébrique définie par la donnée :

1) d'une loi de groupe commutatif dans E (notée additivement dans ce qui suit) ;

2) d'une loi d'action $(a, x) \to ax$, dont le domaine d'opérateurs est l'anneau A, et qui satisfait aux axiomes suivants :

(M_I) $a(x + y) = (ax) + (ay)$ quels que soient $a \in A$, $x \in E$, $y \in E$;

(M_{II}) $(a + b)x = (ax) + (bx)$ quels que soient $a \in A$, $b \in A$, $x \in E$;

(M_{III}) $a(bx) = (ab)x$ quels que soient $a \in A$, $b \in A$, $x \in E$;

(M_{IV}) $1x = x$ pour tout $x \in E$.

De même façon on définit *module à droite*. Si A est commutaif il n'y a pas de diference entre notions module à gauche et module à droite. Dans ce cas on dit A-*module*.

Si E est A-module à gauche et B-module à droite on dit que E est un (A, B)-*bimodule*.

Exemples

1. Soit ϕ un homomorphisme d'un anneau A dans un anneau B ; l'application $(a, x) \mapsto \phi(a)x$ (resp. $(a, x) \mapsto x\phi(a)$) de $A \times B$ dans B définit sur B une structure de A-module à gauche (resp. à droite). Quand on prend en particulier pour cp l'application identique de A on obtient sur A une structure canonique de A-module à gauche (resp. à droite) ; on notera A_g, (resp. A_d) l'ensemble A muni de cette structure, pour éviter des confusions.

2. Espaces vectoriels.

3. Idéaux.

4. Chaque groupe abélien est un module sur $\mathbb{Z}$.

5. Soient E un groupe commutatif noté additivement, End E l'anneau des endomorphismes de E : on rappelle que le produit fg de deux endomorphismes est par définition l'endomorphisme composé $f \circ g$. La loi d'action

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

entre opérateurs $f \in \operatorname{End} E$ et éléments $x \in E$ définit sur E une structure canonique de End E-module à gauche.

Applications linéaires

Étant donnés deux A-modules à gauche (resp. à droite) E et F, on notera $\operatorname{Hom}(E, F)$ ou $\operatorname{Hom}_A(E, F)$ l'ensemble des applications linéaires de E dans F.

Proposition 1. *L'ensemble* $\operatorname{Hom}(E, F)$ *est un groupe commutatif. Soit A un anneau commutatif, soit*

$$f : E \to F$$

morphisme de modules. Alors λf est un morphisme de modules et avec cette multiplication on définit la structure de A-module sur $\operatorname{Hom}(E, F)$.

Sous-modules ; modules quotients

Soient E un A-module, M une partie de E ; pour que la structure de A-module de E induise sur M une structure de A-module, il faut et il suffit que M soit un sous-groupe stable par rapport à multiplications par éléments de A :

$$\alpha m \in M, \quad \alpha \in A,\ m \in M.$$

Lorsqu'il en est ainsi, M vérifie évidemment les axiomes $M_I - M_{IV}$; alors M, muni de cette structure est appelé *sous-module* de E ; l'injection canonique $M \hookrightarrow E$ est une application linéaire. Lorsque E est un espace vectoriel, ses sous-modules s'appellent aussi sous-espaces vectoriels.

Exemples

1. Dans un module quelconque E, l'ensemble réduit à 0 est un sousmodule (sous-module nul, souvent noté 0 par abus de notation).
2. Soit A un anneau. Les sous-modules de A_g, (resp. A_d) ne sont autres que les idéaux à gauche (resp. idéaux à droite) de l'anneau A.
3. Soient E un A-module, x un élément de E, α un idéal à gauche de A. L'ensemble des éléments ax, où a parcourt α, est un sous-module de E, qu'on note αx.
4. Dans un groupe commutatif G, considéré comme $\mathbb{Z}$-module, tout sous-groupe de G est aussi un sous-module.

Soient E un A-module, M un sous-module, E/M le groupe quotient. Soient $x \in E$ et $\bar{x}$ le classe d'équivalence de x dand E/M : $\bar{x} = x + M$. On définit la multiplication de $\bar{x}$ à gauche par $a \in A$ par formule

$$a\bar{x} = ax + M.$$

Cette formule définit correctement la structure de A-module sur E/M.

Exemple

Tout idéal à gauche α dans un anneau A définit un module quotient A_g/α du A-module à gauche A_g ; par abus de notation, ce module quotient s'écrit souvent A/α.

Produits de modules

Soit (E_i), $i \in I$, une famille de modules sur un même anneau A. On vérifie immédiatement que, sur l'ensemble produit $E = \prod_{i\in I} E_i$ le produit des structures de module des E_i est une structure de A-module : si $x = (x_i)$, $y = (y_i)$ sont deux éléments de E, on a donc

$$\begin{cases} x + y = (x_i, y_i), \\ ax + y = (ax_i) \quad \text{pour tout } a \in A. \end{cases} \tag{1}$$

Muni de cette structure, l'ensemble E est appelé le module produit des modules E. Les formules (1) expriment que les projections $pr_i : E \to E_i$ sont des applications linéaires ; ces applications sont évidemment surjectives.

Proposition 2. *Soit $E = \prod_{i\in I} E_i$ le produit d'une famille de A-modules $(E_i)_{i\in I}$. Pour tout A-module F et toute famille d'applications linéaires $f : F \to E_i$, il existe une application f de F dans E et une seule, telle que $\mathrm{pr}_i \circ f = f_i$ pour tout $i \in I$ et cette application est linéaire.*

Somme directe de modules

Soient $(E_i)_{i\in I}$ une famille de A-modules, $F = \prod E_i$ leur produit. L'ensemble E des $x \in F$ tels que $\mathrm{pr}_i\, x = 0$ sauf pour un nombre fini d'indices est évidemment un sous-module de F, qu'on appelle la *somme directe* de la famille de modules $(E_i)_{i\in I}$ et que l'on note $\oplus_{i\in I} E_i$. Lorsque I est fini, on a donc $\oplus_{i\in I} E_i = \prod_{i\in I} E_i$

Pour tout $k \in I$, soit j_k l'application $E_k \to F$ qui, à tout $x_k \in E_k$, fait correspondre l'élément de F tel que $\mathrm{pr}_i(j_k(x_k)) = 0$ pour $i \neq k$ et $\mathrm{pr}_k(j_k(xk)) = x_k$; il est immédiat que j_k est une application linéaire injective de E_k dans la somme directe E des E_i, que nous appellerons l'injection canonique ; le sous-module $j_k(E_k)$ de E, isomorphe à E_k, est appelé le sous-module composant de E.

Proposition 3. *Soient $(E_i)_{i\in I}$ une famille de A-modules, M un A-module, et pour tout $i \in I$, soit $f_i : E_i \to M$ une application linéaire. Il existe alors une application linéaire*

$$g : \oplus_{i\in I} E_i \to M$$

et une seule telle que, pour tout $i \in I$, on ait :

$$g \circ j_i = f_i.$$

Suites exactes

Définition. Soient F, G, H trois A-modules ; soit f un homomorphisme de F dans G et soit g un homomorphisme de G dans H. On dit que le couple (f, g) est une *suite exacte* si l'on a

$$g^{-1}(0) = f(F)$$

autrement dit, si le noyau de g est égal à l'image de f.

On dit aussi que le diagramme

$$F \xrightarrow{f} G \xrightarrow{g} H$$

est une suite exacte.

Considérons de même un diagramme formé de quatre A-modules et de trois homomorphismes :

$$E \xrightarrow{f} F \xrightarrow{g} G \xrightarrow{h} H. \tag{2}$$

On dit que ce diagramme est exact en F si le diagramme

$$E \xrightarrow{f} F \xrightarrow{g} G$$

est exact ; on dit qu'il est exact en G si

$$F \xrightarrow{g} G \xrightarrow{h} H.$$

est exact. Si le diagramme (2) est exact en F et en G, on dit simplement qu'il est exact, ou encore que c'est une suite exacte. On définit de même les suites exactes à un nombre quelconque de termes.

Dire qu'on a une suite exacte

$$0 \to E \xrightarrow{f} F \xrightarrow{g} G \to 0$$

signifie que f est injectif, g surjectif et que la bijection canonique associée à g est un isomorphisme de $F/f(E)$ sur G. On dit encore alors que le triplet (F, f, g) est une extension du module G par le module E.

Définition. Soient A et B des ensembles, f une application injective (resp. surjective) de A dans B. Toute application r (resp. s) de B dans A telle que $r \circ f$ (resp. $f \circ s$) soit l'application identique de A (resp. B) est appelée une *rétraction* (resp. *section*) associée à f.

Proposition 4. *Étant donnée une suite exacte de A-modules*

$$0 \to E \xrightarrow{f} F \xrightarrow{g} G \to 0 \tag{3}$$

les conditions suivantes sont équivalentes :

a) Il existe une rétraction linéaire $r : F \to E$ associée à f.

b) Il existe une section linéaire $s : G \to F$ associée à g.

Lorsqu'il en est ainsi, $f + s : E \oplus G \to F$ et $(r, g) : F \to E \times G$ sont des isomorphismes.

Définition. Lorsque la suite exacte (3) vérifie les conditions de la prop. 4, on dit qu'elle est *scindée* ou que (F, f, g) est une *extension triviale* de G par E.

Propriétés de $\mathrm{Hom}_A(E, F)$ relatives aux suites exactes

Théorème 1. *Soient A un anneau, E', E, E'' trois A-modules, $u : E' \to E$, $v : E \to E''$ deux homomorphismes. On suppose que la suite*

$$E' \xrightarrow{u} E \xrightarrow{v} E'' \to 0$$

est exacte. Alors la suite

$$0 \to \mathrm{Hom}(E'', F) \xrightarrow{\bar{v}} \mathrm{Hom}(E, F) \xrightarrow{\bar{u}} \mathrm{Hom}(E', F)$$

(où on a posé $\bar{u} = \mathrm{Hom}(u, 1_F)$, $\bar{v} = \mathrm{Hom}(v, 1_F)$) est exacte.

Proposition 5. *Si la suite exacte d'applications linéaires*

$$0 \to E' \xrightarrow{u} E \xrightarrow{v} E'' \to 0$$

est scindée, la suite

$$0 \to \mathrm{Hom}(E'', F) \xrightarrow{\bar{v}} \mathrm{Hom}(E, F) \xrightarrow{\bar{u}} \mathrm{Hom}(E', F) \to 0$$

est exacte et scindée.

Théorème 2. *Soient A un anneau, F', F, F'' trois A-modules, $u : F' \to F$, $v : F \to F''$ deux homomorphismes. On suppose que la suite*

$$0 \to F' \xrightarrow{u} F \xrightarrow{v} F''$$

est exacte. Alors la suite

$$0 \to \mathrm{Hom}(E, F') \xrightarrow{\bar{v}} \mathrm{Hom}(E, F) \xrightarrow{\bar{u}} \mathrm{Hom}(E, F'')$$

(où on a posé $\bar{u} = \mathrm{Hom}(1_E, u)$, $\bar{v} = \mathrm{Hom}(1_E, v)$) est exacte.

Proposition 6. *Si la suite exacte d'applications linéaires*

$$0 \to F' \xrightarrow{u} F \xrightarrow{v} F'' \to 0$$

est scindée, la suite

$$0 \to \mathrm{Hom}(E, F') \xrightarrow{\bar{v}} \mathrm{Hom}(E, F) \xrightarrow{\bar{u}} \mathrm{Hom}(E, F'') \to 0$$

est exacte et scindée.

Références

[1] Bourbaki, N. *Éléments de mathématique. Algèbre. Chapitres 1 à 3.* Hermann, Paris 1970 xiii+635 pp.

[2] Lang, S. *Algèbre.* Dunod, Paris, 2004, 926 pp.

Département des Sciences Mathématiques, Université de Montpellier, Place Eugéne Bataillon, 34095 Montpellier cedex 5, France

E-mail address: vershini@math.univ-montp2.fr

ALGÈBRE 1
(COURS DE M1, 2018-2019)
HMMA 115M

COURS 7

MODULES (suite)

Familles libres. Bases

Soient A un anneau, T un ensemble, et considérons le A-module $A_g^{(T)}$ qui est la somme directe externe d'une famille (M_t), $t \in T$, de A-modules tous égaux à A_g. Pour tout $t \in T$ on a une injection canonique $j_t : A_g \hookrightarrow A_g^{(T)}$. On a $j_t(1) = e_t$, de sorte que $e_t = \delta_{t,u}$, $u \in T$ où $\delta_{t,u}$ est égal à 0 si $u \neq t$, à 1 si $u = t$ ("symbole de Kronecker"). Tout $x = (x_t)_{t\in T} \in A_g^{(T)}$ s'écrit donc d'une seule manière :

$$x = \sum_{t\in T} x_t e_t.$$

L'application $\varphi : t \to e_t$ de T dans $A_g^{(T)}$ est dite canonique ; elle est injective.

Proposition 1. *Pour tout A-module E et toute application $f : T \to E$ il existe une application A-linéaire et une seule $h : A_g^{(T)} \to E$ telle que $f = h \circ \varphi$.*

On a par définition

$$h(\sum_{t\in T} x_t e_t) = \sum_{t\in T} x_t f(t).$$

Le noyau R de h est l'ensemble des $(x_t)_{t\in T} \in A_g^{(T)}$ tels que l'on ait

$$\sum_{t\in T} x_t f(t) = 0.$$

On dit que le module R est le *module des relations linéaires entre les éléments de la famille* $(f(t))_{t\in T}$. On a la suite exacte

$$0 \to R \to A_g^{(T)} \xrightarrow{h} E.$$

Corollaire 1. *Soient T, T' deux ensembles, $h : T \to T'$ une application. Il existe alors une application A-linéaire $\psi : A(T) \to A(T')$ et une seule rendant commutatif le diagramme*

$$\begin{array}{ccc} T & \xrightarrow{\quad h \quad} & T' \\ \Big\downarrow{\scriptstyle \varphi} & & \Big\downarrow{\scriptstyle \varphi'} \\ A^{(T)} & \xrightarrow{\quad \psi \quad} & A^{(T')}. \end{array}$$

où φ et φ' sont les applications canoniques.

Corollaire 2. *Pour qu'une famille $(a_t)_{t\in T}$ d'éléments d'un A-module E soit un système générateur de E, il faut et il suffit que l'application linéaire $A_g^{(T)} \to E$ déterminée par cette famille soit surjective.*

Définition. On dit qu'une famille $(a_t)_{t\in T}$ d'éléments d'un A-module E est une *famille libre* (resp. est une *base* de E) si l'application linéaire $A_g^{(T)} \to E$ déterminée par cette famille est injective (resp. bijective). On dit qu'un module est *libre* s'il possède une base.

En particulier, un groupe commutatif G est libre si G (noté additivement) est un $\mathbb{Z}$-module libre.

Corollaire 3. *Soient E un A-module libre, $(a_t)_{t\in T}$ une base de E, F un A-module, $(b_t)_{t\in T}$ une famille d'éléments de F. Il existe une application linéaire $f : E \to F$ et une seule telle que l'on ait*

$$f(a_t) = b_t \text{ pour tout } t \in T. \tag{1}$$

Pour que f soit injective (resp. surjective), il faut et il suffit que (b_t) soit une famille libre dans F (resp. un système générateur de F).

Lorsqu'une famille $(a_t)_{t\in T}$ n'est pas libre, on dit qu'elle est *liée*. Dire que la famille $(a_t)_{t\in T}$ est libre signifie que la relation

$$\sum_{t\in T} \lambda_t a_t = 0$$

(où la famille (λ_t) est à support fini) entraîne $\lambda_t = 0$ pour tout $t \in T$; dire que $(a_t)_{t\in T}$ est une base de E signifie que tout $x \in E$ s'écrit d'une manière et d'une seule sous la forme

$$x = \sum_{t\in T} \xi_t a_t;$$

pour tout $t \in T$, on dit alors que ξ_t est la *composante* (ou la *coordonnée*) *d'indice t de x par rapport à la base* (a_t) ; l'application $x \mapsto \xi_t$ de E dans A_g est linéaire.

Produit tensoriel de deux modules

Soient A un anneau, E un A-module à droite, F un A-module à gauche. Considérons le $\mathbb{Z}$-module (groupe abélien) C des combinaisons linéaires formelles des éléments de $E \times F$ à coefficients dans $\mathbb{Z}$, dont on peut considérer qu'une base est formée des couples (x, y), où $x \in E$ et $y \in F$. Soit D le sous-$\mathbb{Z}$-module de C engendré par les éléments de l'un des types suivants :

$$\begin{cases} (x_1 + x_2, y) - (x_1, y) - (x_2, y), \\ (x, y_1 + y_2) - (x, y_1) - (x, y_2), \\ (x\lambda, y) - (x, \lambda y), \end{cases} \tag{2}$$

où x, x_1, x_2 sont dans E, y, y_1, y_2 dans F et λ dans A.

Définition. On appelle *produit tensoriel* du A-module à droite E et du A-module à gauche F, et on note $E \otimes_A F$ (ou simplement $E \otimes F$ si aucune confusion n'est à craindre) le $\mathbb{Z}$-module quotient C/D (quotient du $\mathbb{Z}$-module C des combinaisons linéaires formelles d'éléments de $E \times F$ à coefficients dans $\mathbb{Z}$, par le sous-module D engendré par les éléments de l'un des types (2). Pour $x \in E$ et $y \in F$, on note $x \otimes y$ et on appelle *produit tensoriel* de x et de y l'élément de $E \otimes_A F$ image canonique de l'élément (x, y) de C.

L'application $\phi : (x, y) \to x \otimes y$ de $E \times F$ dans $E \otimes_A F$ est dite *canonique*. C'est une application $\mathbb{Z}$-bilinéaire qui vérifie les conditions ssuivantes :

$$\phi(x\lambda, y) = \phi(x, \lambda y) \tag{3}$$

Proposition 2. *a) Soit g une application $\mathbb{Z}$-linéaire de $E \otimes_A F$ dans un $\mathbb{Z}$-module G. L'application*

$$(x, y) \mapsto f(x, y) = g(x \otimes y)$$

de $E \times F$ dans G est $\mathbb{Z}$-bilinéaire et vérifie les conditions (3).

b) Réciproquement, soit f une application $\mathbb{Z}$-bilinéaire de $E\times F$ dans un $\mathbb{Z}$-module G, vérifiant les conditions (3). Il existe alors une application $\mathbb{Z}$-linéaire g de $E\otimes_A F$ dans G et une seule telle que $f(x,y)=g(x\otimes y)$ pour $x\in E, y\in F$.

Définition. Un $(A-B)$-*bimodule* est un ensemble M muni à la fois d'une structure de module à gauche sur un anneau A et d'une structure de module à droite sur un anneau B vérifiant

$$\forall a\in A,\quad \forall x\in M,\quad \forall b\in B,\quad a.(x.b)=(a.x).b.$$

On ce note ${}_AM_B$.

Exemples

(1) Tout A-module à droite est aussi un $(\mathbb{Z}-A)$-bimodule.

(2) A est un $(A-A)$ bimodule.

(3) Si A est commutatif, tout A-module peut être vu comme un $(A-A)$-bimodule.

Proposition 3. *Soient A, B deux anneaux, M un (A-B)-bimodule, N un B-module à gauche. Alors le produit tensoriel ${}_AM_B\otimes_B N$ a la structure canonique du A-module à gauche définit par :*

$$a(x\otimes y)=(ax\otimes y)$$

Proposition 4. *Si E est un A-module à droite, l'application $h: x\mapsto x\otimes 1$ de E dans $E\otimes_A ({}_gA_d)$ est un isomorphisme de A-modules à droite, dont l'isomorphisme réciproque f est tel que $f(x\otimes\lambda)=x\lambda$ pour $x\in E$, $\lambda\in A$.*

Produit tensoriel de deux applications linéaires

Soient A un anneau, E, E' deux A-modules à droite, F, F' deux $A-$modules à gauche, $u: E\to E'$ et $v: F\to F'$ deux applications A-linéaires. On vérifie immédiatement que l'application

$$(x,y)\mapsto u(x)\otimes v(y)$$

de $E\times F$ dans $E'\otimes_A F'$ est $\mathbb{Z}$-bilinéaire et satisfait aux conditions (3). En vertu de la prop. 2, il existe donc une application $\mathbb{Z}$-linéaire et une seule

$$w: E\otimes_A F\to E'\otimes_A F'$$

telle que

$$w(x\otimes y)=u(x)\otimes v(y) \tag{4}$$

pour $x\in E$, $y\in F$. Cette application se note $u\otimes v$ (lorsqu'il n'en résulte pas de confusion) et s'appelle le *produit tensoriel* des applications linéaires u et v.

On déduit de (4) que $(u,v)\mapsto u\otimes v$ est une application $\mathbb{Z}$-bilinéaire dite canonique :

$$\mathrm{Hom}_A(E,E')\times\mathrm{Hom}_A(F,F')\to\mathrm{Hom}_{\mathbb{Z}}(E\otimes_A F, E'\otimes_A F').$$

Proposition 5. *Soient E'' un A-module à droite, F'' un A-module à gauche, $u': E'\to E''$, $v': F'\to F''$ des applications A-linéaires ; il résulte de (4). Alors on a*

$$(u'\circ u)\otimes(v'\circ v)=(u'\otimes v')\circ(u\otimes v)$$

Produit tensoriel de deux modules sur un anneau commutatif

Soit C un anneau commutatif ; commutativité permettent de définir sur le produit tensoriel $E\otimes_C F$ la structure de C-module, telle que

$$\gamma(x\otimes y)=(\gamma x)\otimes y=(x\otimes\gamma y),\quad \gamma\in C,\ x\in E,\ y\in F.$$

Définition. Pour tout C-module G, les applications $\mathbb{Z}$-bilinéaires f de $E \times F$ dans G pour lesquelles on a

$$f(\lambda x, y) = f(x, \lambda y) = \lambda f(x, y) \text{ pour } \ x \in E, y \in F, \lambda \in C, \tag{5}$$

sont appelées *C-bilinéaires*, et forment un C-module que l'on note $\mathcal{L}(E, F; G)$.

Proposition 6. *Soient C anneau commutatf, E, F, G C-modules.*

a) Soit g une application linéaire du module $E \otimes_C F$ dans G. L'application $f : (x, y) \mapsto g(x \otimes y)$ de $E \times F$ dans G est C-bilinéaire, vérifie les relations (5).

b) Réciproquement, soit f une application C-bilinéaire de $E \times F$ dans G, vérifiant les conditions (5). Il existe alors une application linéaire et une seule g du C-module $E \otimes_C F$ dans le C-module G telle que l'on ait $f(x, y) = g(x \otimes y)$ pour $x \in E$, $y \in F$.

Corollaire 4. *La prop. 6 définit un isomorphisme canonique de C-modules*

$$\mathcal{L}(E, F; G) \to \mathrm{Hom}_C(E \otimes_C F, G).$$

Références

[1] Bourbaki, N. *Éléments de mathématique. Algèbre. Chapitres 1 à 3.* Hermann, Paris 1970 xiii+635 pp.

[2] Lang, S. *Algèbre.* Dunod, Paris, 2004, 926 pp.

Département des Sciences Mathématiques, Université de Montpellier, Place Eugéne Bataillon, 34095 Montpellier cedex 5, France

E-mail address: vershini@math.univ-montp2.fr

ALGÈBRE 1
(COURS DE M1, 2018-2019)
HMMA 115M

COURS 8

MATRICES

Définition. Soient I, K, H trois ensembles ; on appelle *matrice de type* (I, K) *à éléments dans* H (ou *matrice de type* (I, K) *sur* H) toute famille $M = (m_{i,k})_{(i,k)\in I\times K}$ d'éléments de H dont l'ensemble d'indices est le produit $I \times K$. Pour tout $i \in I$, la famille $(m_{i,k})_{k\in K}$ est appelée la *ligne d'indice* i de M ; pour tout $k \in K$, la famille $(m_{i,k})_{i\in I}$ est appelée la *colonne d'indice* k de M.

Si I (resp. K) est fini, on dit que M est une matrice ayant un nombre fini de lignes (resp. de colonnes). L'ensemble des matrices de type (I, K) sur H s'identifie au produit $H^{I\times K}$.

Si I et K sont finis, on imagine les éléments de la matrice disposés dans les cases d'un tableau rectangularectangulaire ayant p lignes (rangées horizontales) et q colonnes (rangées verticales) :

$$M = \begin{pmatrix} m_{1,1} & m_{1,2} & \dots & m_{1,q} \\ m_{2,1} & m_{2,2} & \dots & m_{2,q} \\ \cdot & \cdot & \dots & \cdot \\ m_{p,1} & m_{p,2} & \dots & m_{p,q} \end{pmatrix}.$$

Définition. On appelle *transposée* d'une matrice $M = (m_{i,k})_{(i,k)\in I\times K}$ et on note ${}^tM$ la matrice $M' = (m'_{k,i})_{(k,i)\in K\times I}$ sur H donnée par $m'_{k,i} = m_{i,k}$, pour tout $(i, k) \in I \times K$.

Matrices sur un groupe commutatif

Soit G un groupe commutatif (noté additivement). L'ensemble des matrices sur G, ayant des ensembles d'indices donnés I, K, est muni d'une structure de groupe commutatif, puisque c'est l'ensemble des applications de $I \times K$ dans G ; ce groupe est noté additivement, de sorte que si $M = (m_{i,k})$ et $M' = (m'_{k,i})$ sont deux de ses éléments, on a

$$M + M' = (m_{i,k} + m'_{k,i}).$$

L'élément neutre de ce groupe est donc la matrice dont tous les éléments sont nuls (dite *matrice nulle*).

Matrices sur un anneau

Les matrices qui sont les plus importantes en Mathématique sont les matrices sur un anneau. L'ensemble $A^{I\times K}$ des matrices sur A, correspondant à des ensembles d'indices I, K, est alors canoniquement muni d'une structure de (A, A)-bimodule

Étant données deux matrices

$$M = (m_{i,k})_{(i,k)\in I\times K}, \quad M' = (m'_{k,l})_{(k,l)\in K\times L}$$

sur A, telles que l'ensemble K des indices des colonnes de M soit fini et égal à l'ensemble des indices des lignes de M', on appelle *produit de* M *et* M' et on note MM' la matrice

$$(\sum_{k\in K} m_{i,k}m'_{k,l})_{(i,l)\in I\times L} \tag{1}$$

sur A.

On vérifie aussitôt les formules de distributivité

$$\begin{cases}(M+N)M' = MM' + NM', \\ M(M'+N') = MM' + MN'\end{cases} \tag{2}$$

les ensembles d'indices étant tels que les sommes et produits écrits soient définis.

Si $M = (m_{i,k})$, $M' = (m_{k,l})$, $M'' = (m''_{l,s})$ sont des matrices sur A, on a

$$M(M'M'') = (MM')M''$$

lorsque les produits des deux membres sont définis.

Matrices et applications linéaires

Soient A un anneau, E un A-module (à droite ou à gauche) admettant une base $(e_i)_{i\in I}$. Pour tout élément $x \in E$, on appelle *matrice de x par rapport à la base* $(e_i)_{i\in I}$ et on note $M(x)$ ou $\mathbf{x}$ (ou même parfois x lorsqu'il n'en résulte pas de confusion), la matrice colonne formée des composantes x_i $(i \in I)$ de x par rapport à $(e_i)_{i\in I}$.

Considérons maintenant deux A-modules (à gauche ou à droite) E et F ayant des bases $(e_i)_{i\in I}$ et $(f_k)_{\in K}$ respectivement. Pour une application u de E dans F, nous allons définir la matrice de u par rapport aux bases $(e_i)_{i\in I}$ et $(f_k)_{\in K}$, dans chacun des cas suivants :

(D) E et F sont des A-modules à droite, u est A-linéaire.

(G) E et F sont des A-modules à gauche, u est A-linéaire.

Définition. Dans chacun des deux cas précédents, on appelle *matrice de u par rapport aux bases* $(e_i)_{i\in I}$ et $(f_k)_{\in K}$ la matrice

$$M(u) = (u_{k,i})_{(k,i)\in K\times I}$$

telle que

$$u(e_i) = \sum_{k\in K} u_{k,i} f_k \text{ pour modules à gauche,} \tag{3}$$

et

$$u(e_i) = \sum_{k\in K} f_k u_{k,i} \text{ pour modules à droite.} \tag{4}$$

La colonne d'indice i de $M(u)$ est donc égale à $M(u(e_i))$.

Proposition 1. *Soient E, F, G trois modules à droite (resp. à gauche) sur un anneau A, $(e_i)_{i\in I}$, $(f_k)_{k\in K}$, $(g_l)_{l\in L}$ des bases finies respectives de E, F, G, $u : E \to F$, $v : F \to G$ deux applications linéaires, $M(u)$ la matrice de u relative aux bases (e_i), (f_k), $M(v)$ la matrice de v relative aux bases (f_k), (g_l), $M(v\circ u)$ la matrice de $v\circ u$ relative aux bases $(e_i), (g_l)$; on a alors*

$$M(v\circ u) = M(v)M(u).$$

Problème de détérminant pour anneaux non-commutatifs

Soit A un anneau non-commutatif. Il n'y a pas de fonction

$$\det : M_2(A) \to A$$

telle que

– det est bilinéaire par rapport à colonnes,
– det est égale à zeo si deux colonnes sont égaux,
– det est égale à 1 pour matrice identité.

Si on suppose que telle fonction existe on a pour tous $x, y \in A$

$$xy = xy \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = x \det \begin{pmatrix} 1 & 0 \\ 0 & y \end{pmatrix} = \det \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} =$$
$$= y \det \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = yx \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = yx.$$

Si on définit une fonction

$$\det : M_2(A) \to A$$

par

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

il n'y a pas de propriété

$$\det(AB) = \det(A) \det(B) :$$

$$\det \left(\begin{pmatrix} 1 & 0 \\ 0 & y \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \right) = xy$$
$$\det \begin{pmatrix} 1 & 0 \\ 0 & y \end{pmatrix} \det \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = yx.$$

MATRICES SUR UN ANNEAU COMMUTATIF

Soit A un anneau commutatif. On définit $GL_n(A)$ comme ensemble des éléments inversibles de l'anneau de matrices carrées $M_n(A)$. Pour les matrices carrées on peut définir le déterminant par la formule habituelle, c'est un élément de A. Les méthodes de calcul des déterminants sont les mêmes (à condition de ne pas utiliser des inverses d'éléments de A non inversibles). En particulier, le développement par rapport à une ligne se fait de la même façon, le déterminant de la transposée est égal au déterminant de la matrice,

$$\det(XY) = \det(X) \det(Y)$$

etc. On peut donc définir la *comatrice* $\mathrm{com}(M)$ d'une matrice carrée M comme sur un corps, et $\mathrm{com}(M)$ est à coefficients dans A (car ses coefficients sont du type $(-1)^{i+j}\Delta_{i,j}$ où $\Delta_{i,j}$ est le mineur associé à l'élément $m_{i,j}$ de M). On a alors, par le même calcul que sur un corps, la :

Proposition 2. *On a*

$$M^t \mathrm{com}(M) = \det(M) Id.$$

D'où :

Corollaire 1. *Une matrice M est inversible dans $M_n(A)$ si et seulement si $\det(M) \in A^\times$.*

Corollaire 2. *Si $\det(M) \in A^\times$, alors le système $MX = Y$ a une solution et une seule.*

La réciproque n'est pas vraie, par exemple

$$\begin{cases} 2x = 2 \\ 5y = 5 \end{cases}$$

a bien une solution $(x, y) = (1, 1)$ dans $\mathbb{Z}$, alors que le déterminant de la matrice du système vaut 10 et pas ± 1.

On définit le polynôme caractéristique de matrice M comme dans le cas de matrices sur un corps $P_M(X) := \det(XId - M)$.

Théorème 1 (Cayley-Hamilton)**.** *Soient A un anneau, $M \in M_n(A) \setminus \{0\}$ et P_M le polynôme caractéristique de M. Alors $P_M(M) = 0$.*

Démonstration. Par définition, $P_M(X) = \det(XId - M)$. Remarquer que $XId - M$ est une matrice à cofficients dans l'anneau $A[X]$. On a donc

$$(XId - M)^t \operatorname{com}(XId - M) = \det(XId - M)Id = P_M(X)Id = P_M(XId)$$

Maintenant $XId - M \mid P_M(XId) - P_M(M)$ parce que $XId - M \mid X^kId - M^k$ par la formule :

$$(XId - M)\sum_{i=0}^{k-1} X^i M^{k-1-i} = X^kId - M^k$$

Donc $XId - M \mid P_M(XId)$, et $XId - M \mid P_M(XId) - P_M(M)$, ce qui implique $XId - M \mid P_M(M)$. On peut écrire $(XId - M)B(X) = P_M(M)$, où $B(X)$ est une matrice avec des coefficients $b_{i,j} \in A[X]$. Du fait que les coefficients de $P_M(M)$ sont constants, cela implique qu'ils sont tous nuls. En effet, si b_{i_0,j_0} est un polynôme de degré $\deg(b_{i_0,j_0})$ maximal parmi les $b_{i,j}$, le coefficient de $P_M(M)$ en position i_0, j_0 est de degré $\deg(b_{i_0,j_0}) + 1$ (c'est une somme contenant Xb_{i_0,j_0} et puis des polynômes de degré strictement inférieur). □

Références

[1] Bourbaki, N. *Éléments de mathématique. Algèbre. Chapitres 1 à 3.* Hermann, Paris 1970 xiii+635 pp.

[2] Lang, S. *Algèbre.* Dunod, Paris, 2004, 926 pp.

Département des Sciences Mathématiques, Université de Montpellier, Place Eugéne Bataillon, 34095 Montpellier cedex 5, France

E-mail address: vershini@math.univ-montp2.fr

ALGÈBRE 1
(COURS DE M1, 2018-2019)
HMMA 115M

COURS 9

ALGÈBRES

Définition d'une algèbre

Définition. Soit A un anneau commutatif. On appelle algèbre sur A (ou A-algèbre, ou simplement algèbre lorsqu aucune confusion n'est à craindre), un ensemble E muni d'une structure définie par les données suivantes :

1) une structure de A-module sur E ;

2) une application A-bilinéaire m de $E \times E$ dans E.

L'application $m : (x, y) \to m(x, y)$ de $E \times E$ dans E qui intervient dans cette définition est appelée la *multiplication* dans l'algèbre E ; on la note d'ordinaire $(x, y) \mapsto x \cdot y$, ou simplement $(x, y) \mapsto xy$.

Diagrammes exprimant l'associativité et la commutativité d'une algèbre

Soit A un anneau commutatif, E un A-module ; la donnée d'une application bi-linéaire de $E \times E$ dans E équivaut à celle d'une application A-linéaire :

$$m : E \otimes_A E \to E.$$

Une structure de A-algèbre sur E est donc définie par la donnée d'une structure de A-module sur E et d'une application A-linéaire de $E \otimes_A E$ dans E.

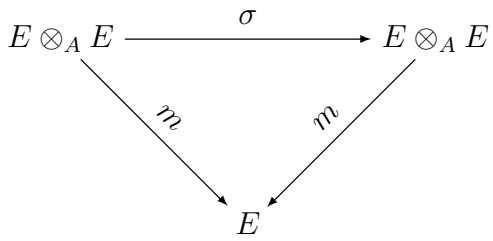
Soit E' une seconde A-algèbre, et soit $m' : E' \otimes_A E' \to E'$ l'application A-linéaire définissant la multiplication de E'. Une application $f : E \to E'$ est un homomorphisme de A-algèbres si et seulement si f est une application A-linéaire qui rend commutatif le diagramme

$$\begin{array}{ccc} E \otimes_A E & \xrightarrow{f \otimes f} & E' \otimes_A E' \\ \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle m'} \\ E & \xrightarrow{\quad f \quad} & E'. \end{array}$$

Pour qu'une A-algèbre E soit *associative*, il faut et il suffit que le diagramme d'applications A-linéaires

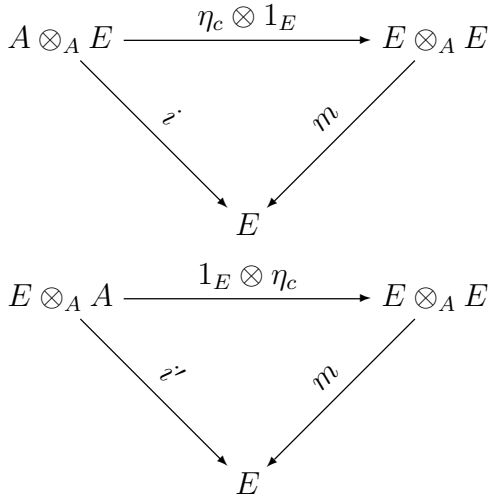
$$\begin{array}{ccc} E \otimes_A E \otimes_A E & \xrightarrow{m \otimes 1_E} & E \otimes_A E \\ \downarrow{\scriptstyle 1_E \otimes m} & & \downarrow{\scriptstyle m} \\ E \otimes_A E & \xrightarrow{\quad m \quad} & E \end{array}$$

soit commutatif. De même, pour que l'algèbre E soit *commutative*, il faut et il suffit que le diagramme d'applications A-linéaires



soit commutatif, en notant σ l'application A-linéaire canonique définie par $\sigma(x \otimes y) = y \otimes x$ pour $x \in E$, $y \in E$.

Pour tout $c \in E$, notons η_c l'application A-linéaire de A dans E définie par la condition $\eta_c = c$. Pour que c soit élément unité de E, il faut et il suffit que les deux diagrammes



soient commutatifs (i et i' désignant les isomorphismes canoniques). Dans ce cas l'algèbre est appelée *unitaire*.

Exemples d'algèbres

1. Algèbre d'un monoïde.

2. Algèbre de polynômes.

3. Algèbres de matrices à coefficients dans un anneau commutatif $M_n(A)$.

4. Algèbre de chemins.

Étant donné un carqois (graphe orienté) Γ et un anneau commutatif A, on peut définir une *algèbre de chemins* (du carquois Γ) $A\Gamma$ comme l'algèbre dont la A-base est donnée par les suites finies d'arcs consécutifs de Γ (et le chemin nul), la composition étant naturelle si les chemins considérés peuvent être mis bout à bout, et donnant l'objet nul sinon.

5. Algèbres de Lie.

Soit A un anneau commutatif.

Définition. Une algèbre L sur A s'appelle *algèbre de Lie* sur A si sa multiplication (notée par $(x, y) \mapsto [x, y]$) vérifie les conditions suivantes :

(1) $[x, x] = 0$

(2) $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ pour tout x, y, z en L.

Proposition 1. *Soit E une algèbre associative sur un anneau commutatif A. On pose pour tout $x, y \in E$, $[x, y] = xy - yx$ (c'est le commutateur des deux éléments x et y). Alors $(E, [\ ,\ ])$ est une algèbre de Lie sur A.*

Références

[1] Bourbaki, N. *Éléments de mathématique. Algèbre. Chapitres 1 à 3.* Hermann, Paris 1970 xiii+635 pp.

[2] Lang, S. *Algèbre*. Dunod, Paris, 2004, 926 pp.

Département des Sciences Mathématiques, Université de Montpellier, Place Eugéne Bataillon, 34095 Montpellier cedex 5, France

E-mail address: vershini@math.univ-montp2.fr

ALGÈBRE 1
(COURS DE M1, 2018-2019)
HMMA 115M

COURS 10

Radicaux

Définition. Soit A un anneau commutatif. Si I est un idéal de A, on appelle le *radical* de I et on note $\mathrm{rad}(I)$ l'ensemble des éléments x de A tel qu'il existe $n \in N^*$ tel que $x^n \in I$.

Proposition 1. *(a) Radical de I $\mathrm{rad}(I)$ est un idéal de A qui contient I.*
(b) $\mathrm{rad}(\mathrm{rad}(I)) = \mathrm{rad}(I)$.
(c) Si I et J sont deux idéaux de A, alors $\mathrm{rad}(I \cap J) = \mathrm{rad}(IJ) = \mathrm{rad}(I) \cap \mathrm{rad}(J)$.
$\mathrm{rad}(I + J) = \mathrm{rad}(\mathrm{rad}(I) + \mathrm{rad}(J))$.

Définition. Un idéal qui est égal à son radical s'appelle *saturé*.

Corollaire 1. *Tout idéal de A est inclus dans un idéal saturé.*

Proposition 2. *Soit A un anneau commutatif. L'ensemble de tous les éléments nilpotents de A est un idéal de A.*

Définition. L'idéal de proposition **??** est appelé le *nilradical* de A, noté $\mathrm{Nilrad}(A)$, ou $\mathrm{Nil}(A)$.

Corollaire 2. $\mathrm{rad}(0) = \mathrm{Nilrad}(A)$.

Proposition 3. *Nilradical d'un anneau commutatif A est l'intersection de tous les idéaux premiers de A.*

Soit R un anneau (qui n'est pas nécessairement commutatif).
Définition. L'intersection de tous les idéaux à gauche maximaux de R est appelé le *radical de Jacobson* de R, noté $\mathrm{J}(R)$.

Pour chaque anneau commutatif nilradical est une partie de radical de Jacobson.

Proposition 4. *Un élément x appartient au radical de Jacobson de l'anneau commutatif A si et seulement si $1 - xy$ est inversible dans A pour tout y de A.*

Anneaux euclidiens et factoriels

Définition. Soit A un anneau commutatif. On dit que A est *euclidien* si
(1) A est intègre,
(2) il existe un application

$$N : A \to \mathbb{N}$$

telle que $N(a) = 0$ si et seulement si $a = 0$ et, pour tous $a, b \in A \setminus \{0\}$, il existe $q, r \in A$ tels que

$$a = bq + r \text{ et } N(r) < N(b).$$

On dit que N est un *stathme* sur A.

On dit que A est *principal* si
(1) A est intègre,
(2) tout idéal de A est principal.

On dit que A est *factoriel* si
(1) A est intègre,

(2) il existe un ensemble P d'éléments irréductibles de A tels que :
(i) tout élément $x \in A \setminus \{0\}$ admet une décomposition

$$x = u \prod_{i=1}^{k} p_i^{a_i}$$

avec $u \in A^\times$, $a_i \in N^*$ et $p_i \in P$ distincts,
(ii) si un élément $x \in A \setminus \{0\}$ admet deux décompositions

$$x = u \prod_{i=1}^{k} p_i^{a_i} = u' \prod_{i=1}^{k'} q_j^{b_j}$$

avec $u, u' \in A^\times$, $a_i, b_j \in N^*$ et $p_i \in P$ distincts et $q_j \in P$ distincts alors on a $k = k'$, $u = u'$ et il existe une permutation σ de $\{1, 2, \ldots, k\}$ telle que $p_i = q_{\sigma(i)}$ et $a_i = b_\sigma(i)$.

On peut écrire tout élément x d'un anneau factoriel

$$x = u \prod_{p \in P} p^{a_p},$$

avec $u \in A^\times$ et les $a_p \in \mathbb{N}$ tous nuls sauf un nombre fini. Alors, avec cette notation, on a : si

$$y = u' \prod_{p \in P} p^{b_p},$$

on a

$$xy = uu' \prod_{p \in P} p^{a_p + b_p}.$$

Si K est le corps de fractions de A, alors tout élément x de K s'écrit

$$x = u \prod_{p \in P} p^{a_p},$$

avec avec $u \in A^\times$ et les $a_p \in \mathbb{Z}$ tous nuls sauf un nombre fini.

On dit que $a, b \in A$ sont *associés*, s'il existe un élément inversible $u \in A$ tel que $a = ub$.

Soit A un anneau factoriel, P comme dans la définition. Alors P contient un et un seul élément de chaque classe d'association d'éléments irréductibles de A. Aussi, si P' est un ensemble d'éléments de A contenant un représentant de chaque classe d'association d'éléments irréductibles de A et rien d'autre, P' vérifie aussi les conditions de la définition. On dit qu'un tel P' est un système minimal de générateurs irréductibles. On dira par la suite "soit (A, P) un anneau factoriel", sous-entendu que A est un anneau factoriel et P un système minimal de générateurs irréductibles.

Exemples

Un corps commutatif est toujours un anneau euclidien pour le stathme qui vaut 1 sur tout élément non nul.

Voici trois types classiques moins triviaux d'anneaux euclidiens :

(1) L'anneau $\mathbb{Z}$. On posera $N(x) = |x|$.

Théorème 1 (Algorithme de division)**.** *Etant donnés entiers a et b avec $b > 0$ il existe deux entiers uniques q et r tels que*

$$a = bq + r \ \text{ et } \ 0 \leq r < b.$$

Théorème 2 (Algorithme de division modifié)**.** *Etant donnés entiers a et b avec $b > 0$ il existe deux entiers uniques q et r tels que*

$$a = bq + r \ \text{ et } \ -b/2 < r \leq b/2.$$

(2) L'anneau $K[X]$ où K est un corps commutatif. On posera $N(P) = \deg P + 1$ si $P \neq 0$.

Entiers de Gauss

L'anneau $\mathbb{Z}[i] := \{a + ib,\ a, b \in \mathbb{Z}\}$ comme sous-anneau de $\mathbb{C}$. On pose ici

$$N(a + ib) = (a + ib)(a - ib) = a^2 + b^2.$$

Théorème 3 (Algorithme de division pour entiers de Gauss)**.** *Etant donnés entiers de Gauss α et β avec $\beta \neq 0$ il existe deux entiers de Gauss γ et ρ tels que*

$$\alpha = \beta\gamma + \rho \text{ et } N(\rho) \leq 1/2N(\beta).$$

Théorème 4. *Un anneau euclidien est toujours principal.*

Proposition 5. *Dans un anneau principal A, tout élément irréductible est premier.*

Théorème 5. *Un anneau principal est toujours factoriel.*

Contrexemples.

Les anneaux $\mathbb{Z}[i\sqrt{3}]$, $\mathbb{Z}[i\sqrt{5}]$, etc, sont intègres mais pas factoriels.

Définition. Soit A un anneau intègre. Deux éléments a et b de A sont dits *premiers entre eux* si tout diviseur commun à a et b est inversible.

Théorème 6. *Soit (A, P) un anneau factoriel. Si*

$$x = u \prod_{p \in P} p^{a_p} \in A \setminus \{0\}, \quad y = u' \prod_{p \in P} p^{b_p} \in A \setminus \{0\},$$

avec $u, u' \in A^\times$ et les $a_p, b_p \in \mathbb{N}$. Alors, on a :

(a) *$x|y$ si et seulement si $a_p \leq b_p$ pour tous $p \in P$.*

(b) *$d := \prod_{p \in P} p^{\min(a_p, b_p)}$ est un PGCD de x et y.*

(c) *$m := \prod_{p \in P} p^{\max(a_p, b_p)}$ est un PPCM de x et y.*

(d) *Dans A, tout élément irréductible est premier.*

(e) *On a dans A le lemme de Gauss : soient $a, b, c \in A$ tels que a divise bc mais a est premier avec b. Alors a divise c.*

(f) *On a dans A le lemme d'Euclide : soient $a, b, c \in A$ tels que a est irreductible et il divise bc. Alors a divise b ou c.*

Si A est principal, $\mathrm{PGCD}(x, y) = d$ et $\mathrm{PPCM}(x; y) = m$ sont définis aussi par $(x) \cap (y) = (d)$ et $(x, y) = (m)$.

Théorème 7. *Soit A un anneau principal. Alors A verifie :*

(a) *le théorème de Bézout : si $a, b \in A$ sont premiers entre eux alors il existe $u, v \in A$ tels que $au + bv = 1$,*

(b) *tout idéal premier non nul de A est maximal.*

Références

[1] Lang, S. *Algèbre*. Dunod, Paris, 2004, 926 pp.

Département des Sciences Mathématiques, Université de Montpellier, Place Eugéne Bataillon, 34095 Montpellier cedex 5, France

E-mail address: vershini@math.univ-montp2.fr

ALGÈBRE 1
(COURS DE M1, 2018-2019)
HMMA 115M

COURS 11

Nombres premier de Gauss (de l'anneau $Z[i]$) et théorème des deux carrés.

On note $\mathbb{Q}(i)$ le sous-ensemble de $\mathbb{C}$ formé de nombres complexes $a+ib$ tels que $a,b\in\mathbb{Q}$. Alors $\mathbb{Q}(i)$ est stable par addition et multiplication ; c'est donc un sous-anneau de $\mathbb{C}$. C'est en fait un sous-corps de $\mathbb{C}$ comme on peut le vérifer en écrivant, pour $a,b\in\mathbb{Q}$ tels que $a^2+b^2\neq 0$,

$$\frac{1}{a+ib}=\frac{a-ib}{a^2+b^2}=\frac{a}{a^2+b^2}-i\frac{b}{a^2+b^2}\in\mathbb{Q}(i).$$

On pose :

$$N:\mathbb{Q}(i)\to\mathbb{Q}_+,\quad N(z)=N(a+ib)=z\bar{z}=a^2+b^2.$$

On appelle N la norme sur $\mathbb{Q}(i)$. Elle est multiplicative au sens où $N(zz')=N(z)N(z')$. L'anneau des entiers de Gauss $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{Q}(i)$.

Théorème 1. *a) Le corps de fractions de $\mathbb{Z}[i]$ est $\mathbb{Q}(i)$.*
b) Les éléments inversibles de $\mathbb{Z}[i]$ sont les éléments de norme 1, soit $\{1,-1,i,-i\}$.

Définition. Un nombre premier de Gauss est un élément premier (irréductible) de $\mathbb{Z}[i]$.

Proposition 1. *Tout nombre premier de Gauss divise un nombre premier usuel.*

Démonstration. Il divise sa norme donc (d'après le lemme d'Euclide dans $\mathbb{Z}[i]$) au moins l'un des facteurs premiers (dans $\mathbb{Z}$) de celle-ci. □

Proposition 2. *Le nombre 2 n'est pas un nombre premier de Gauss, $\pm(1\pm i)$ sont des nombres premiers de Gauss.*

Démonstration. $2=(1+i)(1-i)$. □

Si d est un entier, on note $\phi(d)$ le nombre des entiers x te'ls que

$$\phi(d)=\begin{cases}1\leq x\leq d,\\ x \text{ est premier à } d.\end{cases}$$

On appelle $\phi(d)$ *l'indicatrice d'Euler* de d.

Proposition 3. *Le nombre de générateurs du groupe $\mathbb{Z}/d\mathbb{Z}$ est égal à $\phi(d)$.*

Proposition 4. *Soit G un groupe fini, $|G|=n$. Si pour tout $d|n$, $\mathrm{card}\{x\in G|x^d=1\}\leq d$, alors G est cyclique.*

Démonstration. On fixe $d|n$. Soit G_d un sous-ensemble des éléments de G d'ordre d. On suppose que $G_d\neq\emptyset$, alors il existe $y\in G_d$; $\langle y\rangle\subset\{x\in G|x^d=1\}$. Le sous-groupe y est de cardinalité d, alors aprés l'hypothèse de la proposition on a $\langle y\rangle=\{x\in G|x^d=1\}$. Alors G_d est l'ensemble de générateurs du groupe cyclique $\langle y\rangle$ d'ordre d, et $\mathrm{card}(G_d)=\phi(d)$. Alors nous avons montré que G_d soit vide soit de cardinalité $\phi(d)$ pour tout $d|n$. Alors on a :

$$n=|G|=\sum_{d|n}\mathrm{card}(G_d)\leq\sum_{d|n}\phi(d)=n.$$

La dernière égalité $\sum_{d|n} \phi(d) = n$ est déduite du même argument appliqué en cas où G est le groupe cyclique d'ordre n.

Alors $\text{card}(G_d) = \phi(d)$ pour tout $d|n$, en particulier $G_n \neq \emptyset$ et G est cyclique. □

Corollaire 1. *Dans un groupe cyclique fini G le nombre d'éléments d'ordre d où d est un diviseur de $|G|$ est égale à $\phi(d)$.*

Corollaire 2. *Si K est un corps fini, alors le groupe multiplicatif K^* est cyclique.*

Théorème 2. *Un nombre premier $p \in \mathbb{N}$ est un élément premier de $\mathbb{Z}[i]$ si et seulement si $p \equiv 3 \mod 4$.*

Démonstration. Soit $p \in \mathbb{N}$ premier tel que $p \equiv 3 \mod 4$. Supposons par l'absurde que p n'est pas premier dans $\mathbb{Z}[i]$. Comme $\mathbb{Z}[i]$ est principal, p est réductible. Écrivons $p = zu$, avec z et u non inversibles, soit $N(z) > 1$ et $N(u) > 1$. On a $p^2 = N(p) = N(z)N(u)$. Comme on est dans $\mathbb{N}$ et que p est premier, on doit avoir $p = N(z) = N(u)$. Mais une norme $N(z)$ est une somme de deux carrés, qui ne peut jamais être congrue à 3 modulo 4 :

$$(2k+1)^2 + (2m)^2 = 4(k^2 + k + m) + 1.$$

Donc p n'est pas réductible, il est premier.

Soit maintenant $p \in \mathbb{Z}$ premier tel que $p \equiv 1 \mod 4$. Le groupe $G := (\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique car $\mathbb{Z}/p\mathbb{Z}$ est un corps fini, 4 divise $|G|$ donc par Proposition **??**, G a un seul élément d'ordre 2, c'est $\overline{p-1}$ ($(p-1)^2 = p^2 + 2p + 1$), et deux éléments d'ordre 4 qu'on note $\bar{y}$. En particulier, on doit avoir $y^2 = \overline{p-1}$ soit $\bar{y}^2 + \bar{1} \equiv p \mod p$. Alors, p divise $\bar{y}^2 + \bar{1}$ et alors dans $Z[i]$, $p|(y+i)(y-i)$. Comme $p(a+ib) = pa + ipb$ on voit que p ne divise pas $y - i$ (car $pb = 1$ impossible). Comme p divise le produit pourtant, il s'ensuit que p n'est pas premier (dans $Z[i]$). □

Corollaire 3. Le théorème des deux carrés. *Soit $p \in \mathbb{Z}$ un nombre premier. Alors p s'écrit comme somme de deux carrés si et seulement si $p = 2$ ou $p \equiv 1 \mod 4$. La présentation comme somme de deux carrés est unique pour chaque p.*

Théorème 3. *Les nombres premiers de Gauss sont :*
$\pm(1 \pm i)$;
pour tout nombre premier p congru à 1 modulo 4 : les huit entiers de Gauss de norme p ;
pour tout nombre premier p congru à 3 modulo 4 : $\pm p$ et $\pm ip$.

Démonstration. Si p est somme de deux carrés, alors $p = a^2 + b^2 = (a+bi)(a-ib)$, $(a+bi)$ et $(a-bi)$ sont irréductibles dans $\mathbb{Z}[i]$, puisque leur norme p est irréductible dans $\mathbb{Z}$. Les nombres premiers de Gauss qui divisent p sont donc $(a+bi)$ et $(a-bi)$, et leurs produits par les unités i, -1 et $-i$ (ces huit nombres sont distincts, sauf si $p = 2$). □

Théorème 4. *Un entier est somme de deux carrés si et seulement si chacun de ses facteurs premiers de la forme $4k+3$ intervient à une puissance paire.*

Références

[1] Lang, S. *Algèbre*. Dunod, Paris, 2004, 926 pp.

[2] Perrin, D. *Cours d'Algèbre*. Ellipses, Paris, 1996, 207 pp.

Département des Sciences Mathématiques, Université de Montpellier, Place Eugéne Bataillon, 34095 Montpellier cedex 5, France
E-mail address: vershini@math.univ-montp2.fr

ALGÈBRE 1
(COURS DE M1, 2018-2019)
HMMA 115M

COURS 12

Rappel sur les espaces topologiques

Définition. Un *espace topologique* est un couple (E, τ), où E est un ensemble et τ un ensemble de parties de E que l'on définit comme les ouverts de (E, τ), vérifiant les propriétés suivantes :
- L'ensemble vide et E appartiennent à τ.
- Toute réunion d'ouverts est un ouvert, c'est-à-dire si $(U_i)_{i\in I}$ est une famille (finie ou infinie, dénombrable ou non dénombrable) d'éléments de τ, alors
$$\bigcup_{i\in I} U_i \in \tau.$$
- Toute intersection finie d'ouverts est un ouvert, c'est-à-dire si $U_1, \ldots, U_n$ sont des éléments de τ $(n > 0)$, alors
$$U_1 \cap \ldots \cap U_n \in \tau.$$

L'ensemble τ, qui est un ensemble de parties de E, est alors appelé une topologie sur E.

Un *fermé* d'une topologie est défini comme le complémentaire d'un ouvert.

L'intérieur ; adhérence.

Sous-ensembles dense ; espaces séparables ; droite réelle $\mathbb{R}$ est séparable.

Définition. Soit X un espace topologique et A un sous-ensemble de X, A est *nulle part dense* dans X si l'intérieur de l'adhérence de A est vide.

Définition. On dit qu'un espace topologique X est de Kolmogorov, ou vérifie la propriété T_0, si pour deux points distincts quelconques de X, l'un (au moins) des deux points admet un voisinage qui ne contient pas l'autre point.

Applications continues

Définition. Soit X et Y deux espaces topologiques, $f : X \to Y$ est une application, $x \in X$. L'application f est *continue* dans x si pour tout voisinage V de $f(x)$ l'image inverse $f^{-1}(V)$ est un voisinage de x.

Si X et Y sont deux espaces métriques cette définition est équivalente à suivante : l'application f est *continue* dans x si pour chaque $\epsilon > 0$ il existe $\delta > 0$ tel que pour tout $z \in X$, tel que $d_X(x, z) < \delta$ on a $d_Y(f(x), f(z)) < \epsilon$.

Définition. Soit X et Y sont deux espaces métriques, l'application $f : X \to Y$ est *uniformément continue* si pour chaque $\epsilon > 0$ il existe $\delta > 0$ tel que pour touts $x, z \in X$, tel que $d_X(x, z) < \delta$ on a $d_Y(f(x), f(z)) < \epsilon$.

Exemple

L'application $x \to x^2$ de $\mathbb{R}$ vers $\mathbb{R}$ est continue, mais pas uniformément continue.

Proposition 1. *Si x_0 est un point adhérent à un ensemble $A \subset X$ d'un espace topologique X, et si l'application $f : X \to Y$ est continue au point x_0, alors $f(x_0)$ est adhérent à $f(A)$.*

Théorème 1. *Soit X et Y deux espaces topologiques, $f : X \to Y$ est une application. Les propriétés suivantes sont équivalentes :*

a) l'application $f : X \to Y$ est continue ;

b) pour tout sous-ensemble $A \subset X$ de X, $f(\overline{A}) \subset \overline{f(A)}$;

c) pour tout sous-ensemble fermé $F \subset Y$ de Y, $f^{-1}(F)$ est un ensemble férmé dans Y ;
d) pour tout sous-ensemble ouvert $A \subset Y$ de Y, $f^{-1}(A)$ est un ensemble ouvert dans Y.

Spectre d'anneau

Proposition 2. *Soitent A un anneau commutaif, P un idéal premier de A, I_j, $j \in \{1, 2, \ldots, n\}$, une famille finie des idéaux de A. Soit*

$$I = I_1 \ldots I_j \ldots I_n.$$

Alors $I \subset P$ implique qu'il existe j tel que $I_j \subset P$.

Soit A un anneau commutaif, soit X l'ensemble de tous les idéaux premier de A. Pour chaque sous-ensemble E de A, on note $V(E)$ l'ensemble de tous les idéaux premiers de A qui contiennent E.

Proposition 3.
- *i) Si I est un idéal engendré par E, alors $V(E) = V(I) = V(rad(I))$.*
- *ii) $V(0) = X, V(1) = \emptyset$.*
- *iii) Si $(E_j), j \in J$ est une famille de sous-ensembles de A, alors*

$$V(\cup_{j\in J} E_j) = \cap_{j\in J} V(E_j).$$

- *iv) $V(I \cap K) = V(IK) = V(I) \cup V(K)$ pour tous les idéaux I, K de A.*

Corollaire 1. *Les ensembles $V(E$, $E \subset A$ satisfont des axiomes pour des ensembles férmés dans un espace topologique.*

Définition. La topologie de Corolaire 1 est appelé la *topologie de Zariski*. L'espace X avec la topologie de Zariski est appelé le *spectre* de A et on le note $\mathrm{Spec}(A)$.

Exemples : $\mathrm{Spec}(\mathbb{Z})$, k - corps commutaif.

Proposition 4. *Soit $f : A \to B$ un homomorphisme des anneaux commutatifs. Alors l'image inverse d'un idéal premier dans B est un idéal premier dans A.*

Proposition 5. *Soit $f : A \to B$ un homomorphisme des anneaux commutatifs. Soit P un idéal premier dans B Alors l'application*

$$P \mapsto f^{-1}(P)$$

induit l'application continue

$$\mathrm{Spec}(f) : \mathrm{Spec}(B) \to \mathrm{Spec}(A).$$

Théorème 2. Spec *est un foncteur contravariant de la cathègorie des anneaux commutatifs vers la catégorie des espaces topologiques.*

Références

[1] Bourbaki, N. *Éléments de mathématique. Topologie générale. Chapitres 1 à 4.* Hermann, Paris, 1971. xv+357 pp.

[2] Lang, S. *Algèbre.* Dunod, Paris, 2004, 926 pp.

Département des Sciences Mathématiques, Université de Montpellier, Place Eugéne Bataillon, 34095 Montpellier cedex 5, France

E-mail address: vershini@math.univ-montp2.fr

ALGÈBRE 1
(COURS DE M1, 2018-2019)
HMMA 115M

COURS 13

POLYNÔMES

Anneaux de polynômes à une indéterminée

Soit A un anneau commutatif, $A[X]$ est une A-algèbre de polynômes à une indéterminée.

Proposition 1 (Propriété universelle d'algèbre de polynômes)**.** *Soient B une A-algèbre et b un élément de B. Il existe un homomorphisme de A-algèbres unique*

$$\phi : A[X] \to B$$

tel que $\phi(X) = b$.

Proposition 2. *Soient $P, S \in A[X]$ non nuls.*

$$P(X) = \sum_{i=1}^{k} a_i X^i, \quad S(X) = \sum_{j=1}^{m} b_j X^j.$$

Alors

$$\deg(PS) \leq \deg(P) + \deg(S)$$

Si $a_k b_m \neq 0$ (par exemple si A est integre ou l'un de $\{a_k, b_m\}$ est inversible), alors

$$\deg(PS) = \deg(P) + \deg(S)$$

Proposition 3. *Soient $P, S \in A[X]$ comme en Proposition **??**. Soit A est integre ou a_k est inversible. Si P divise S, alors*

$$\deg(P) \leq \deg(S).$$

Proposition 4. (a) *L'anneau $A[X]$ est intègre si et seulement si l'anneau A est intègre.*

(b) *Si A est intègre, alors $A[X]^\times = A^\times$.*

Proposition 5. (a) *Si A est un corps commuatif, alors l'anneau $A[X]$ est euclidien et alors principal.*

(b) *Si $A[X]$ est pricipal, alors l'anneau A est un corps commutatif.*

Soient (A, P) un anneau factoriel et K son corps de fractions. Si $P \in A[X]$ on note $c(P)$ le PGCD des coefficients de P (il est défini à association près). On l'appelle le *contenu* de P. On dit que P est *primitif* si $c(P)$ est inversible. Tout $P \in A[X] \setminus \{0\}$ s'écrit $P = c(P)S$ avec $S \in A[X] \setminus \{0\}$ primitif.

Proposition 6. (a) *Soit $P \in A[X] \setminus \{0\}$ un polynôme primitif et $\alpha \in K$ tel que $\alpha P \in A[X] \setminus \{0\}$ et est primitif. Alors $\alpha \in A^\times$.*

(b) *Si $P \in K[X] \setminus \{0\}$, il existe un élément $k_P \in K^\times$ tel que $k_P P$ ait des coefficients dans A et soit primitif. Un tel k_P est unique à multiplication par un inversible de A près.*

(c) *Si $F, G \in A[X]$ sont primitifs, alors FG est primitif.*

(d) *Si $F, G \in A[X]$, alors $c(FG) = c(F)c(G)$.*

Théorème 1. *Si A est factoriel, les éléments irréductibles de $A[X]$ sont exactement les éléments de A qui sont irréductibles dans A et les polynômes primitifs qui sont irréductibles dans $K[X]$.*

Proposition 7. *Soit A un anneau commutatif et soient $P, S \in A[X]$ non nuls tels que le coefficient dominant de S est inversible dans A. Alors on peut faire la division euclidienne de P par S : il existe un unique couple $(U, R) \in A[X] \times A[X]$ tels que*

$$P = US + R$$

et $\deg(R) < \deg(S)$.

Théorème 2. *Soit A un anneau factoriel et K le corps de fractions de A. Soient $P, S \in A[X]$ tels que :*
- P divise S dans $K[X]$ et
- P est primitif.
Alors P divise S dans $A[X]$.

Théorème 3. *Si A est factoriel, $A[X]$ est factoriel.*

Remarquer que la réciproque est aussi vraie. Si $A[X]$ est factoriel et P est son système minimal de générateurs irréductibles, alors $P \cap A$ est un système minimal de générateurs irréductibles pour A et l'unicité de ceci vient de l'unicité de cela.

Anneaux de polynômes à plusieurs indéterminées

Soit A un anneau commutatif unitaire. On s'intéresse aux anneaux de polynômes en plusieurs indéterminées $A[X_1, X_2, \dots X_n]$ sur A. On appelle *monôme* un polynôme du type

$$\lambda \prod_{1 \leq i \leq n} X_i^{k_i}, \text{ où } \lambda \in A \setminus \{0\}$$

et *monôme unitaire* un polynôme du type

$$\prod_{1 \leq i \leq n} X_i^{k_i}.$$

Alors $P \in A[X_1, X_2, \dots, X_n]$ s'écrit de façon unique comme combinaison linéaire à coefficients dans A de monômes unitaires distincts. On appelle usuellement monôme de P un monôme unitaire qui apparait effectivement (i.e. avec un coefficient non nul) dans cette combinaison linéaire. Par définition, le *degré total* d'un monôme unitaire $\prod_{1 \leq i \leq n} X_i^{k_i}$. est $\sum_i k_i$ et le *degré partiel* en X_j est a_j. Si $P \in A[X_1, X_2, \dots, X_n]$ on appelle *degré total* de P (parfois juste "degré"), noté $\deg(P)$, le maximum des degrés des monômes de P, et le *degré partiel* de P en X_j, noté $\deg_j(P)$, le maximum des degrés en X_j des monômes de P. Remarquer que, si on pose $B := A[X_1, \dots, X_{n-1}]$, alors $A[X_1, \dots X_n] \cong B[X]$. Ceci permet d'obtenir par récurrence des résultats sur $A[X_1, \dots X_n]$ à partir des résultats sur les anneaux de polynômes en une variable.

Proposition 8.
(a) *L'anneau $A[X_1, \dots X_n]$ est intègre si et seulement si l'anneau A est intègre.*
(b) *Si A est intègre, alors on a* $\deg(PS) = \deg(P) + \deg(S)$, *et* $\deg_j(PS) = \deg_j(P) + \deg_j(S)$.
(c) *L'anneau $A[X_1, \dots X_n]$ est factoriel si et seulement si A est factoriel.*
(d) *Si $n \geq 2$, alors $A[X_1, \dots X_n]$ n'est jamais principal.*

Remarque. Soit A un anneau commutatif quelconque : si $P, S \in A[X_1, X_2, \dots, X_n]$, si $\deg_n(S) \geq 1$ et le coefficient dominant de S en tant que polynôme de X_n (à coefficients dans $A[X_1, X_2, \dots, X_{n-1}]$ est dans $A^\times$, alors il existe un unique couple (H, R) de polynômes tel que

$$P = HS + R$$

etdeg$(R) <$ deg(S). Ceci n'est que la division par un polynôme unitaire dans $B[X_n]$, où $B = A[X_1, X_2, \ldots, X_{n-1}]$. Par exemple, si $P \in A[X_1, X_2, X_3]$ quelconque et

$$S(X_1, X_2, X_3) = X_1^2 X_2 + X_2^2 + X_3 X_1 + X_1^2,$$

on peut faire une division euclidienne de P par S par rapport à X_2, mais en général pas par rapport à X_3 ou X_1.

Polynômes homogènes.

Un polynôme $P, S \in A[X_1, X_2, \ldots, X_n]$ est dit *homogène de degré* m si P est non nul et tous les monômes de P sont de même degré, égal à m. Une combinaison linéaire de polynômes homogènes de degré m est soit nulle, soit homogène de degré m. Tout polynôme P non nul de $A[X_1, X_2, \ldots, X_n]$ s'écrit de façon unique comme somme de polynômes homogènes

$$P = \sum_{i=0}^{\deg(P)} P_i$$

avec P_i homogène de degré i.

On suppose que A est intègre. Alors $A[X_1, X_2, \ldots, X_n]$ est intègre. Si P et S sont homogènes de degré m et n respectivement, leur produit est homogène de degré $m + n$.

Proposition 9. *Soit $P \neq 0$ un polynôme homogène et supposons que $P = SR$ où S et R sont deux polynômes. Alors S et R sont homogènes.*

Soit $P \in A[X_1, X_2, \ldots, X_n] \setminus \{0\}$ un polynôme. Alors P est homogène de degré m si et seulement si, dans l'anneau de polynômes à $n + 1$ indéterminées $A[X_1, X_2, \ldots, X_n, t]$ on a l'égalité

$$P(tX_1, tX_2, \ldots, tX_n, t) = t^m P(X_1, X_2, \ldots, X_n).$$

Polynômes symétriques.

Soit $\mathcal{S}_n$ le group symétrique de n lettres, $\sigma \in \mathcal{S}_n$. Pour tout $P \in A[X_1, X_2, \ldots, X_n]$ on pose

$$P_\sigma := P(X_{\sigma(1)}, X_{\sigma(2)}, \ldots X_{\sigma(n)}).$$

C'est une action du groupe $\mathcal{S}_n$ sur $A[X_1, X_2, \ldots, X_n]$. Un polynôme $P \in A[X_1, X_2, \ldots, X_n]$ est dit *symétrique* si $P_\sigma = P$ pour tous $\sigma \in \mathcal{S}_n$. Les polynômes symétriques forment une sous-algèbre de $A[X_1, X_2, \ldots, X_n]$.

On appelle *polynômes symétriques élémentaires* en $X_1, X_2, \ldots X_n$ les n polynômes suivants :

$$\begin{aligned}
s_1 &= X_1 + X_2 + \cdots + X_n, \\
s_2 &= \sum_{1 \leq i < j \leq n} X_i X_j, \\
&\ldots\ldots\ldots\ldots \\
s_k &= \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} X_{i_1} X_{i_2} \ldots X_{i_k}, \\
&\ldots\ldots\ldots\ldots \\
s_n &= \prod_{i=1}^{n} X_i.
\end{aligned}$$

Plus précisément, on dit que s_k est le *k-ème polynôme symétrique élémentaire* en $X_1, X_2, \ldots, X_n$. Remarquer que s_k est homogène de degré k, il a C_n^k monômes, et qu'en faisant $X_n = 0$ dans s_k on obtient le k-ème polynôme symétrique élémentaire en $X_1, X_2, \ldots, X_{n-1}$.

Si $P \in A[X_1, X_2, \ldots, X_n]$ est un monôme du type $\prod_{i=1}^n X_i^{m_i}$, on appelle poids de P l'entier $\sum_{i=1}^n i m_i$. Si $P \in A[X_1, X_2, \ldots, X_n]$ est non nul, on appelle poids de P le poids maximal de ses monômes. Remarquer que le degré de $P(s_1, s_2, \ldots, s_n)$ est inférieur ou égal au poids de P.

Théorème 4. *Soit $P \in A[X_1, X_2, \ldots, X_n]$ un polynôme symétrique de degré d. Alors il existe un unique polynôme $T \in A[X_1, X_2, \ldots, X_n]$ tel que*

$$P(X_1, X_2, \ldots, X_n) = T(s_1, s_2, \ldots, s_n),$$

et T est de poids d. Donc la sous-algèbre $A[X_1, X_2, \ldots, X_n]_S$ de $A[X_1, X_2, \ldots, X_n]$ formée de polynômes symétriques est une algèbre de polynômes en $s_1, s_2, \ldots s_n$.

Références

[1] Lang, S. *Algèbre*. Dunod, Paris, 2004, 926 pp.

Département des Sciences Mathématiques, Université de Montpellier, Place Eugéne Bataillon, 34095 Montpellier cedex 5, France
E-mail address: vershini@math.univ-montp2.fr

ALGÈBRE 1
(COURS DE M1, 2018-2019)
HMMA 115M

COURS 14

Racines des polynômes à une indéterminée

Proposition 1. *Soit A un anneau commutatif et $P \in A[X]$ un polynôme non nul. Si $a \in A$ alors il y a équivalence entre :*
(i) $P(a) = 0$,
(ii) $X - a$ divise P dans $A[X]$.

À partir de maintenant, l'anneau A sera intègre. Si $P \in A[X] \setminus \{0\}$ et a est une racine de P on appelle multiplicité de a dans P l'entier m tel que $(X-a)^m$ divise P mais $(X-a)^{m+1}$ ne divise pas P. Une multiplicité est alors définie, inférieure ou égale à $\deg(P)$. On dit parfois que la multiplicité de a est zéro quand a n'est pas racine de P. On dit qu'une racine a de P est racine simple si la multiplicité de a est 1. La dérivée formelle d'un polynôme $P(X) = \sum_{i=0}^{n} a_i X^i$ est par définition le polynôme

$$P'X) = \sum_{i=1}^{n} i a_i X^{i-1}.$$

Ici, comme d'habitude, ia_i est à prendre comme la somme à i termes $a_i + a_i + \cdots + a_i$ dans A.

Proposition 2. *Si l'anneau A est de caractéristique nulle, alors*

$$\deg(P') = \deg(P) - 1.$$

Remarque. Le polynôme $P(X) = X^p$ de $\mathbb{F}_p[X]$ a une dérivée formelle nulle. Ainsi, l'hypothèse sur la caractéristique est importante.

Proposition 3. *Soient $P \in A[X] \setminus \{0\}$ et a une racine de P dans A.*
(a) On a : a est racine simple de P si et seulement si $P'(a) \neq 0$.
(b) Si a est une racine de P de multiplicité m, alors

$$P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0.$$

Si, de plus, la caractéristique de A est nulle, on a $P^{(m)}(a) \neq 0$.

Remarque. Le polynôme $P(X) = X^p$ de $\mathbb{F}_p[X]$ a une dérivée formelle nulle, donc 0 est racine de toutes ses dérivées. Toutefois, 0 est racine de multiplicité p de P. Donc l'hypothèse sur la caractéristique dans (b) est importante.

Proposition 4. *Soient A un anneau commutatif intègre et $P \in A[X]$ un polynôme de degré $n \geq 1$. Alors P a au plus n racines dans A. Si $x_1, x_2, \ldots, x_k$ sont les racines (distinctes) de P dans A et $m_1, m_2, \ldots, m_k$ leurs multiplicités, alors P s'écrit*

$$P(X) = \prod_{i=1}^{k} (X - x_i)^{m_i} R(X)$$

où $R \in A[X]$ n'a aucune racine dans A.

Soit A un anneau commutatif intègre. On dit que $P \in A[X] \setminus \{0\}$ est *scindé* sur A si P peut s'écrire comme produit de polynômes de degré 1 sur A, autrement dit si le polynôme R de la proposition est de degré zéro.

Si K est un corps, on dit que K est *algébriquement clos* si tout polynôme de degré ≥ 1 à coefficients dans K est scindé sur K. Ceci équivaut à ce que tout polynôme irréductible à coefficients dans K soit de degré 1. Par un théorème qu'on ne démontrera pas ici, pour tout corps K il existe un corps $\bar{K}$ tel que

$K \subset \bar{K}$,

$\bar{K}$ est algébriquement clos et tout corps algébriquement clos qui contient K contient un corps isomorphe à $\bar{K}$.

On dit que $\bar{K}$ est une *clôture algébrique* de K. Le corps $\bar{K}$ est unique à isomorphisme près.

Remarquer que, puisque A est intègre, il est inclus dans un corps de fracvctions de A : $K = Fr(A)$. Il est donc inclus aussi dans un corps algébriquement clos $\bar{K}$ qui contient toutes les racines de tous les polynômes à coefficients dans A.

Proposition 5. *Soit A un anneau factoriel. Soit $P \in A[X]$ non nul,*

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0.$$

(a) Soit $a \in A$ une racine de P. Alors $a|a_0$.

(b) Soit $x_0 \in Fr(A)$ une racine de P dans le corps de fractions $Fr(A)$ de A. Posons $x_0 = \frac{a}{b}$ avec $a, b \in A$ premiers entre eux. Alors $a|a_0$ et $b|a_n$. En particulier, si le coefficient dominant de P est 1, alors toute racine de P dans $Fr(A)$ est dans A.

Algèbre de séries formelles

Soit A un anneau commutatif. On désigne par A[[X]] l'anneau des "sommes formelles"

$$S(X) := \sum_{n=0}^{+\infty} a_n X^n,$$

avec $a_i \in A$ et muni d'une addition et d'une multiplication de la façon suivante : soit $T(X) = \sum_{n=0}^{+\infty} b_n z^n$ l'autre séries formelle, l'addition est définie par

$$(S+T)(X) = \sum_{n=0}^{+\infty} (a_n + b_n) X^n.$$

et la multiplication par

$$S(X)T(X) = (\sum_{n=0}^{+\infty} a_n)(\sum_{n=0}^{+\infty} b_n) = \sum_{n=0}^{+\infty} c_n X^n$$

où $c_n = \sum_{k=0}^{n} a_k b_{n-k}$.

L'anneau $A[[X]]$ est une A-algèbre pour la multiplication par les scalaires $a \in A$:

$$aS(X) = a \sum_{n=0}^{+\infty} a_n X^n = \sum_{n=0}^{+\infty} a a_n X^n.$$

C'est l'*algèbre de séries formelles à coefficients dans A.*

Définition. On appelle *valuation* une application d'un anneau commutatif A non nul vers un groupe abélien totalement ordonné $(G, +, <)$ union l'infini

$$v : A \longrightarrow G \cup \{\infty\}$$

qui vérifie les propriétés suivantes :

(1) $\forall x \in A,\ v(x) = \infty \Longleftrightarrow x = 0$;

(2) $\forall x, y \in A,\ v(xy) = v(x) + v(y)$;

(3) $v(x+y) \geqslant \min(v(x), v(y))$,

Si

$$S(X) = \sum_{n=0}^{+\infty} a_n X^n,$$

est une série formelle, on définit $o(S)$ la valuation de S comme le plus petit entier $k \in N$ tel que $a_k \neq 0$, avec la convention que, si $S = 0$, on pose $o(S) = +\infty$. Propriétés (1) et (3) sont satistaites. Si on ne suppose pas que A est integre on a

$$o(ST) \geq o(S) + o(T)$$

pour toutes $S, T \in A[[X]]$ en général, et $o(ST) = o(S) + o(T)$ pour toutes $S, T \in A[[X]]$ si A est intègre.

La structure d'anneau $A[[X]]$ est inspirée de celle de l'anneau de polynômes $A[X]$. Ainsi $A[X]$ est (isomorphe à) une sous-algèbre de l'algèbre de séries formelles, en identifiant toute série formelle dont tous les coefficients sont nuls à partir d'un certain rang au polynôme associé. Si $P, R \in A[[X]]$, il n'est pas aisé de définir, comme pour les polynômes, $P \circ R(X) = P(Q(X))$ (dite *substitution* de R dans P). On peut quand-même le faire dans certains cas.

Définition. Soient

$$P(X) := \sum_{n=0}^{+\infty} a_n X^n, R(X) = \sum_{n=0}^{+\infty} b_n X^n \in A[[X]]$$

telles que $b_0 = 0$. Alors on définit $P \circ R$ comme la série

$$\sum_{n=0}^{+\infty} c_n X^n,$$

avec $c_n = \sum_{i=0}^{n} a_i u_i$, où par définition u_i est le coefficient de X^i dans $\sum_{j=1}^{n} (b_j X^j)^i$. On dit qu'on a fait la *substitution* de R dans P.

La substitution a les propriétés : si $S, S_0, T, T_0 \in A[[X]]$ sont telles que les termes constants de T et T_0 sont nuls, alors

$$(S + S_0) \circ T = S \circ T + S_0 \circ T$$
$$S S_0 \circ T = (S \circ T)(S_0 \circ T)$$
$$(S \circ T) \circ T_0 = S \circ (T \circ T_0).$$

Remarquer que si les termes constants de T et T_0 sont nuls, il en est de même de celui de $T \circ T_0$ donc la dernière égalité a un sens.

Théorème 1. *Un élément $S = \sum_{n=0}^{+\infty} a_n X^n$, de $A[[X]]$ est inversible si et seulement si $a_0 \in A^\times$.*

Théorème 2. *(a) $A[[X]]$ est intègre si et seulement si A est intègre.*
(b) $A[[X]]$ est un anneau principal si et seulement si A est un corps.
(c) Si A est un corps, tout idéal de $A[[X]]$ est de la forme (X^k), $k \in \mathbb{N}$.

On peut définir également la dérivée d'une série formelle $S = \sum_{n=0}^{+\infty} a_n X^n$ comme la série formelle

$$S' = \sum_{n=1}^{+\infty} n a_n X^{n-1}.$$

Topologie

Soit v une valuation sur A à valeurs réelles, et $\rho \in]0, 1[$. On associe à v une valeur absolue ultramétrique $|\ |_v$ en posant

$$\forall x \in A^*,\ |x|_v = \rho^{v(x)}.$$

Références

[1] Lang, S. *Algèbre*. Dunod, Paris, 2004, 926 pp.

Département des Sciences Mathématiques, Université de Montpellier, Place Eugéne Bataillon, 34095 Montpellier cedex 5, France
E-mail address: vershini@math.univ-montp2.fr