Séminaire Dubreil.
Algèbre et théorie
des nombres

Michel Lazard

Théorie des idéaux dans les anneaux de Dedekind

Séminaire Dubreil. Algèbre et théorie des nombres, tome 5-6 (1951-1953), exp. n° 2, p. 1-8

<http://www.numdam.org/item?id=SD_1951-1953__5-6__A2_0>

Faculté des Sciences de Paris
-:-:-:-
Séminaire A. CHÂTELET et P. DUBREIL
(ALGÈBRE ET THÉORIE DES NOMBRES)
THÉORIE DES IDÉAUX
Années 1951-1953
-:-:-:-

Exposé n° 2

II. THÉORIE DES IDÉAUX DANS LES ANNEAUX DE DEDEKIND

par Michel LAZARD

Dans certains anneaux, dits anneaux de Dedekind, il est possible de développer une théorie de la décomposition des idéaux en produits d'idéaux premiers semblable à la décomposition des entiers naturels en produits de facteurs premiers ; les formules de calcul du plus grand commun diviseur (p.g.c.d.) et du plus petit commun multiple (p.p.c.m.) sont tout-à-fait analogues. Ces anneaux sont historiquement à l'origine du concept d'idéal, le plus grand commun diviseur (p.g.c.d.) de deux entiers algébriques était conçu comme un "nombre idéal". Les deux principaux types d'exemples d'anneaux de Dedekind sont :

1° les anneaux d'entiers algébriques dans les extensions algébriques finies du corps des nombres rationnels ;

2° les anneaux de fonctions algébriques entières (par rapport à une certaine variable) dans le corps des fonctions algébriques d'une variable.

D'autres anneaux rencontrés en géométrie algébrique, sont aussi des anneaux de Dedekind.

Définitions et axiomes. - Nous étudierons un anneau $\mathcal{O}$ supposé commutatif et possédant un élément unité (noté 1). Nous conviendrons, une fois pour toute, de ne considérer que des idéaux qui contiennent des éléments non-diviseurs de zéro. Pour simplifier l'exposé, nous nous bornerons aux anneaux d'intégrité (le cas général n'implique pas de modifications aux démonstrations) : nous ne considérons pas $(\mathcal{O})$ comme un idéal.

Un anneau d'intégrité $\mathcal{O}$ sera dit anneau de Dedekind s'il vérifie les trois axiomes suivants :

1° Tout idéal premier de $\mathcal{O}$ est un idéal maximal.

2° tout idéal possède une base finie (ou une formulation équivalente de la condition maximale de Noether).

3° $\mathcal{O}$ est intégralement fermé dans son corps des quotients K.

Autrement dit, tout élément de K entier par rapport à $\mathcal{O}$ appartient à $\mathcal{O}$. Rappelons qu'un élément x de K est dit entier par rapport à $\mathcal{O}$ s'il vérifie une des trois conditions suivantes (qui sont équivalentes si $\mathcal{O}$ est noethérien, c'est-à-dire vérifie l'axiome 2) :

a. x est racine d'une équation algébrique à coefficient dans $\mathcal{O}$, le coefficient de la plus grande puissance étant l'unité ;

b. toutes les puissances (entières positives) de x s'expriment comme des fractions ayant un même dénominateur ;

c. toutes les puissances (entières positives) de x sont contenues dans un sous-anneau de K qui est un sous-$\mathcal{O}$-module engendré par un nombre fini d'éléments.

Considérons la famille P_i des idéaux <u>premiers</u> de $\mathcal{O}$. Nous définirons la famille d'idéaux $\mathfrak{M}$ comme la famille <u>multiplicative</u> engendrée par les P_i. (i parcourt un ensemble d'indice I). Tout élément Q de $\mathfrak{M}$ s'écrit sous la forme :

(1) $$\prod_{i \in I} P_i^{\alpha_i}$$

où les α_i sont des entiers $\geqslant 0$, tous nuls sauf un nombre fini. (On prend le produit des P_i affectés des exposants positifs, et on pose $P_i^0 = \mathcal{O}$).

Nous avons donc une application $(\alpha_i)_{i \in I} \to \prod_{i \in I} P_i^{\alpha_i}$ de l'ensemble $N^{(I)}$ des familles d'entiers $\alpha_i \geqslant 0$, tous nuls, sauf un nombre fini, sur la famille d'idéaux $\mathfrak{M}$.

On définit immédiatement sur $N^{(I)}$ une structure de <u>semi-groupe abélien ordonné</u> (en considérant l'addition et la comparaison terme à terme de deux familles d'exposants de $N^{(I)}$. L'application que nous avons définie de $N^{(I)}$ sur $\mathfrak{M}$ transforme l'opération d'<u>addition</u> dans $N^{(I)}$ en l'opération de <u>multiplication</u> dans $\mathfrak{M}$.

Faisons maintenant appel à l'<u>axiome 1</u>. Rappelons d'abord quelques propriétés des idéaux sans diviseurs communs. Deux idéaux A et B de $\mathcal{O}$ sont dits sans diviseurs communs si $A + B = \mathcal{O}$, ou encore s'il existe $a \in A$ et $b \in B$ tels que $a + b = 1$, ou encore si les congruences $x \equiv a \pmod{A}$ et $x \equiv b \pmod{B}$ peuvent toujours être résolus simultanément dans l'anneau $\mathcal{O}$.

L'intersection de deux idéaux A et B sans diviseurs communs est égale à leur produit : en effet, on a toujours les relations :

(2) $$A\,B \subset A \cap B$$

et

(3) $$(A + B)(A \cap B) \subset A\,B \ ;$$

comme $A + B = \mathcal{O}$, contenant une unité, on en déduit $A \cap B = AB$. Si l'idéal A est sans diviseurs communs avec chacun des deux idéaux B et C, il est sans diviseurs communs avec leur intersection et leur produit.

Il suffit de le démontrer pour le produit BC. Nous avons des relations de la forme :

(4) $$a + b = 1$$

(5) $$a' + c = 1 \quad (\text{avec } a, a' \in A, \ b \in B, \ c \in C)$$

d'où l'on déduit :

(6) $$(a\,a' + a\,c + a'b) + bc = 1 \quad (\text{où } bc \in BC, \ aa' + ac + a'b \in A).$$

Par récurrence on démontre que deux puissances d'idéaux sans diviseurs communs sont sans diviseurs communs, que le produit d'une famille finie d'idéaux sans diviseurs communs deux à deux est égal à leur intersection, etc.

D'après l'axiome 1, tout idéal premier P_i est maximal, c'est-à-dire que quel que soit l'idéal A, $P_i + A = P_i$ si $A \subset P$, ou $P_i + A = \mathcal{O}$, si $A \not\subset P_i$. Autrement dit P_i est sans diviseurs communs avec tout idéal qu'il ne divise pas. En particulier deux puissances d'idéaux premiers distincts sont sans diviseurs communs.

Il résulte de ce qui précède que tout idéal de $\mathfrak{M}$, soit $\prod_{i \in I} P_i^{\alpha_i}$ peut s'écrire comme une intersection : $\bigcap_{i \in I} P_i^{\alpha_i}$.

Soient maintenant $\prod_{i \in I} P_i^{\alpha_i}$ et $\prod_{i \in I} P_i^{\beta_i}$ deux idéaux de la famille $\mathfrak{M}$. Nous avons :

(7) $$\left(\prod_{i \in I} P_i^{\alpha_i}\right) \cap \left(\prod_{i \in I} P_i^{\beta_i}\right) = \left(\bigcap_{i \in I} P_i^{\alpha_i}\right) \cap \left(\bigcap_{i \in I} P_i^{\beta_i}\right)$$
$$= \bigcap_{i \in I} (P_i^{\alpha_i} \cap P_i^{\beta_i}) = \bigcap_{i \in I} P_i^{\max(\alpha_i, \beta_i)}$$

D'autre part, en utilisant la formule de distributivité de la multiplication des idéaux par rapport à leurs somme $(A(B + C) = AB + AC)$, nous obtenons :

$$(8)\quad \begin{aligned}(\prod_{i\in I} P_i^{\alpha_i}) + (\prod_{i\in I} P_i^{\alpha_i}) &= (\prod_{i\in I} P_i^{\min(\alpha_i, \beta_i)})(\prod_{i\in I} P_i^{\alpha_i - \min(\alpha_i, \beta_i)}) \\ &+ \dots (\prod_{i\in I} P_i^{\min(\alpha_i, \beta_i)})(\prod_{i\in I} P_i^{\beta_i - \min(\alpha_i, \beta_i)}) \\ &= (\prod_{i\in I} P_i^{\min(\alpha_i, \beta_i)})(\prod_{i\in I} P_i^{\alpha_i - \min(\alpha_i, \beta_i)} + \prod_{i\in I} P_i^{\beta_i - \min(\alpha_i, \beta_i)}) \\ &= \prod_{i\in I} P_i^{\min(\alpha_i, \beta_i)},\end{aligned}$$

car les idéaux $\prod_{i\in I} P_i^{\alpha_i - \min(\alpha_i, \beta_i)}$ et $P_i^{\beta_i - \min(\alpha_i, \beta_i)}$ sont sans diviseurs communs.

Nous sommes donc parvenus, en nous appuyant seulement sur l'axiome 1, au résultat suivant :

La famille multiplicative $\mathfrak{M}$ est fermée par rapport aux opérations de la somme et de l'intersection (sous-treillis du treillis des idéaux) ;

L'application de $I^{(N)}$ sur $\mathfrak{M}$ transforme la borne supérieure de deux éléments de $I^{(N)}$ en intersection (c'est-à-dire borne inférieure ou p.p.c.m.) des idéaux correspondants, et la borne inférieure de deux éléments de $I^{(N)}$ en somme (c'est-à-dire borne supérieure ou p.g.c.d.) des idéaux correspondants.

Montrons maintenant, en faisant intervenir l'axiome 2, que l'application de $I^{(N)}$ sur $\mathfrak{M}$ est biunivoque.

Supposons qu'on ait :

$$(9)\quad \prod_{i\in I} P_i^{\alpha_i} = \prod_{i\in I} P_i^{\beta_i}$$

sans avoir, pour tout i, $\alpha_i = \beta_i$. Alors, d'après les résultats déjà obtenus on aurait

$$(10)\quad \prod_{i\in I} P_i^{\min(\alpha_i, \beta_i)} = \prod_{i\in I} P_i^{\max(\alpha_i, \beta_i)} = (\prod_{i\in I} P_i^{|\alpha_i - \beta_i|}) \prod_{i\in I} P_i^{\min(\alpha_i, \beta_i)}$$

Or, dans un anneau $\mathcal{O}$, commutatif possédant un élément unité, si l'on a un idéal $A \neq \mathcal{O}$ et un idéal B possédant une base finie, la relation $AB = B$ implique que tout élément de B est diviseur de 0 dans $\mathcal{O}$. Soit en effet w_j

$(1 \leq j \leq n)$ une base de B . $AB = B$ est équivalent à l'existence d'un système d'équations

$$\sum_{1 \leq k \leq n} (a_{jk} - \delta_{jk}) w_j = 0$$

$(1 \leq j \leq n \; ; \; a_{jk} \in A \; ; \; \delta_{jk} = 1$ si $i = j$, $\delta_{jk} = 0$ si $i \neq j)$.

Désignant par Δ le déterminant $||a_{jk} - \delta_{jk}||$, on obtient

$$\Delta w_j = 0 \text{ pour tout } j \text{ , donc } \Delta B = 0 \text{ , } \Delta = 1 \pmod{A} \text{ , donc } \neq 0 .$$

Dans le cas qui nous intéresse, il suffit de poser $A = \prod_{i \in I} P_i^{|\alpha_i - \beta_i|}$ et $B = \prod_{i \in I} P_i^{\min(\alpha_i , \beta_i)}$ pour aboutir à une contradiction si $\alpha_i \neq \beta_i$ pour un certain i ; en effet, dans ce cas $A \neq \mathcal{O}$; B possède une base finie (d'après l'axiome 2), et contient des éléments non-diviseurs de zéro. Par conséquent l'application de $I^{(N)}$ sur $\mathfrak{M}$ est <u>biunivoque</u>.

Montrons maintenant qu'étant donné un idéal $A \subset \mathcal{O}$, il existe un idéal Q de la famille $\mathfrak{M}$ tel que $Q \subset A$. Raisonnons par l'absurde : si tout idéal A ne vérifiait pas cette propriété, il existerait, dans la famille des idéaux ne la vérifiant pas, un idéal maximal (par rapport aux autres idéaux de cette famille). Soit A un tel idéal. A n'est pas premier, sans quoi il appartiendrait à la famille $\mathfrak{M}$ et $A \subset A$. Il existe donc des éléments b et c n'appartenant pas à A , tels que $bc \in A$. Mais alors

$$(11) \qquad (A , a)(A , b) \subset A .$$

D'après le choix de A , les idéaux (A , a) et (A , b) qui contiennent strictement l'idéal A , vérifient la propriété étudiée, c'est-à-dire qu'il existe Q_1 et Q_2 appartenant à la famille tels que

$$(12) \qquad Q_1 \subset (A , a) \text{ et } Q_2 \subset (A , b) .$$

Il en résulte que $Q_1 Q_2 \subset (A , a)(A , b) \subset A$ et A contient l'idéal $Q_1 Q_2$ de la famille $\mathfrak{M}$, contrairement à l'hypothèse.

Parmi les idéaux Q de la famille $\mathfrak{M}$ contenues dans un idéal A , il en existe un plus grand que tous les autres (car, d'après l'axiome 2, toute somme d'idéaux est une somme finie, et la famille $\mathfrak{M}$ est fermée par rapport aux sommes finies).

Il existe donc un idéal $\prod_{i \in I} P_i^{\alpha_i}$ tel que $\prod_{i \in I} P_i^{\beta_i} \subset A$ soit équivalent à

$\beta_i \geq \alpha_i$ (pour tout i)

Tout idéal $\prod_{i \in I} P_i^{\gamma_i}$ contenant A est tel que $\gamma_i \leq \alpha_i$. Il n'en existe donc qu'un nombre fini, et leur intersection, qui appartient encore à la famille $\mathfrak{M}$, est le plus petit d'entre eux. Nous obtenons donc, pour chaque idéal A, un "encadrement" le meilleur possible par des idéaux Q_1 et Q_2 de la famille $\mathfrak{M}$:

$$Q_1 \subset A \subset Q_2 \quad . \tag{13}$$

Remarquons que si $A \neq \mathcal{O}$, $Q_2 \neq \mathcal{O}$ (en effet, A est alors contenu dans au moins un idéal premier). Notre but est de démontrer que la famille $\mathfrak{M}$ est constituée par tous les idéaux de $\mathcal{O}$, ou encore que dans l'encadrement précédent $Q_1 = A = Q_2$.

Remarquons que la famille $\mathfrak{M}$ est, par rapport à la multiplication, un semi-groupe abélien (chaque élément est régulier). Il est donc possible, abstraitement de plonger l'ensemble $\mathfrak{M}$ dans un groupe abélien, où la multiplication coïncide avec la multiplication déjà introduite dans $\mathfrak{M}$.

Nous montrerons que le groupe abélien en question (défini à un isomorphisme près si on le suppose engendré par $\mathfrak{M}$) peut être "réalisé" par une famille de $\mathcal{O}$-modules (dits encore "idéaux fractionnaires") dans le corps des quotients K de $\mathcal{O}$. Rappelons la définition d'un $\mathcal{O}$-module contenu dans K : c'est un sous-groupe additif de K, soit A tel que $\mathcal{O}A = A$ (c'est-à-dire que le produit d'un élément de A par un élément de $\mathcal{O}$ appartient à A). Le produit de deux $\mathcal{O}$-modules de K se définit comme le produit de deux idéaux dans $\mathcal{O}$. (Ces idéaux ne sont pas autre chose que les $\mathcal{O}$-module contenus dans $\mathcal{O}$).

Il suffit, pour montrer que notre "réalisation" de la symétrisation de $\mathfrak{M}$ par des $\mathcal{O}$-modules est possible, de montrer que les générateurs P_i de $\mathfrak{M}$ possèdent des inverses $\tilde{P}_i$. Précisons : il s'agit de trouver des $\mathcal{O}$-modules $\tilde{P}_i$ tels que $P_i \tilde{P}_i = \mathcal{O}$ (c'est-à-dire l'élément neutre de $\mathfrak{M}$). Pour tout P_i, l'ensemble des éléments x de K tels que $x P_i \subset \mathcal{O}$ forment un $\mathcal{O}$-module que nous noterons P_i^{-1}, et l'on a :

$$P_i \subset P_i P_i^{-1} \subset \mathcal{O} ,$$

par conséquent

$$P_i P_i^{-1} = P_i \quad \text{ou} \quad P_i P_i^{-1} = \mathcal{O} .$$

Etablissons d'abord que P_i^{-1} contient un élément n'appartenant pas à $\mathcal{O}$. Soit a un élément non nul de l'idéal P_i. L'idéal principal (a) contient un plus grand idéal de la famille $\mathfrak{M}$. Parmi les facteurs premiers de ce dernier idéal figure nécessairement l'idéal premier P_i. On peut donc écrire :

$$P_i Q \subset (a) \quad \text{et} \quad Q \not\subset (a) . \tag{14}$$

Soit b un élément de Q tel que $b \notin (a)$. Alors $P_i(b) \subset (a)$, ou ce qui est équivalent $\frac{b}{a} \in P_i^{-1}$. Mais $b \notin (a)$ est équivalent à $\frac{b}{a} \notin \mathcal{O}$. Donc $\frac{b}{a}$ n'appartient pas à $\mathcal{O}$.

Faisons maintenant appel à l'axiome 3 pour démontrer que $P_i(P_i^{-1})^n = \mathcal{O}$. Si cela était faux, on aurait $P_i(P_i^{-1})^n = P_i$ et, par conséquent (récurrence sur n) $P_i(P_i^{-1})^x = P_i$ pour tout entier positif n. Soit alors $a \in P_i$, $a \neq 0$, et $x \in P_i^{-1}$, $x \notin \mathcal{O}$, on aurait $a x^n \in \mathcal{O}$ pour tout entier positif n, et par conséquent x serait entier par rapport à $\mathcal{O}$, donc (d'après l'axiome 3) appartiendrait à $\mathcal{O}$ contrairement à l'hypothèse. Par conséquent P_i^{-1} fournit l'inverse de P_i que nous cherchions, et l'on peut désormais considérer le <u>groupe abélien</u> des $\mathcal{O}$-modules $\prod_{i \in I} P_i^{\alpha_i}$ où les α_i sont tous seuls, sauf un nombre fini, qui peuvent prendre des valeurs entières <u>positives</u> ou <u>négatives</u>.

Soit $Q_1 \subset A \subset Q_2$ le meilleur encadrement d'un idéal A par des idéaux de la famille $\mathfrak{M}$; comme la multiplication par un $\mathcal{O}$-module respecte évidemment les relations d'inclusions, on en déduit :

$$Q_1 Q_2^{-1} \subset A Q_2^{-1} \subset \mathcal{O} .$$

Si l'idéal $A Q_2^{-1}$ était différent de $\mathcal{O}$, on trouverait Q_3 dans la famille $\mathfrak{M}$ telle que $A Q_2^{-1} \subset Q_3 \subsetneq \mathcal{O}$, d'où l'on déduirait $A \subset Q_2 Q_3 \subsetneq Q_2$. Par conséquent $A Q_2^{-1} = \mathcal{O}$ et $Q_1 = A = Q_2$.

Notre famille $\mathfrak{M}$ est donc formée par tous les idéaux de l'anneau $\mathcal{O}$, et nous avons vu comment la théorie de la divisibilité des idéaux, le calcul de leur p.g.c.d., etc. sont analogues à la théorie de la divisibilité des entiers naturels.

Démontrons maintenant une réciproque, qui établit en quelque sorte la nécessité des trois axiomes : si dans l'anneau $\mathcal{O}$ (anneau d'intégrité si l'on ne veut pas se restreindre à n'envisager que les idéaux qui contiennent des non-diviseurs de zéro) tout idéal A est un produit d'une famille finie d'idéaux premiers :

$A = \prod_{i \in I} P_i^{\alpha_i}$ et si A n'est contenu dans $B = \prod_{i \in I} P_i^{\beta_i}$ que lorsque $\beta_i \leq \alpha_i$ (pour tout i), l'anneau $\mathcal{O}$ vérifie les axiomes 1, 2 et 3.

La vérification des axiomes 1 et 2 est immédiate. Indiquons celle de l'axiome 3. Soit n dans le corps des quotients K de $\mathcal{O}$, entier par rapport à $\mathcal{O}$. Par hypothèse les puissances $x^0 = 1$, x, x^2, ... de x engendrent un $\mathcal{O}$-module L dans K tel que $L^2 = L$ et que $aL \subset \mathcal{O}$ pour un certain élément a de $\mathcal{O}$. Alors $(La)^2 = (La).a$ et, chaque idéal (La en particulier) étant régulier par rapport à la multiplication des idéaux, on obtient en simplifiant : $La = (a)$, ce qui est équivalent à $L = \mathcal{O}$. Donc $n \in \mathcal{O}$ et l'axiome 3 est vérifié.