

II

Anneaux de Dedekind

1. Localisation et idéaux fractionnaires

Cette section est consacrée à quelques rappels élémentaires d'algèbre commutative.

Soit A un anneau intègre. Notons K son corps des fractions. Rappelons que A est dit *noethérien* si et seulement si toute suite croissante d'idéaux de A est stationnaire. Il est équivalent de dire que tout idéal de A est de type fini.

L'anneau A est dit *intégralement clos* s'il est intègre et si tout élément de K qui est *entier sur A* (c'est-à-dire racine d'un polynôme unitaire à coefficients dans A) est dans A . Par exemple $\mathbf{Z}$ est intégralement clos (mais pas $A = \mathbf{Z} + \mathbf{Z}[\sqrt{-3}]$, en effet $x = (1 + \sqrt{-3})/2$ est solution de l'équation $x^2 - x + 1 = 0$ sans appartenir à A). Lorsque A est contenu dans un corps L , l'ensemble des éléments de L qui sont entiers sur A est un anneau qu'on appelle *clôture intégrale de A dans L* . Dire qu'un élément x de L est entier sur A revient à dire que $A[x]$ est un A -module de type fini.

Soit I un A -module contenu dans K . Posons

$$I^{-1} = \{x \in K/xI \subset A\},$$

$$R(I) = \{x \in K/xI \subset I\}.$$

On dit que I est un *idéal fractionnaire* si $I \neq 0$ et s'il existe $a \in A$ non nul tel que $aI \subset A$, cela revient à dire qu'il existe $a \in K$ tel que $aI \subset A$.

Un idéal fractionnaire I est dit *inversible* s'il vérifie $II^{-1} = A$.

Soient I_1 et I_2 deux idéaux fractionnaires de A contenus dans $a_1^{-1}A$ et $a_2^{-1}A$ respectivement avec $(a_1, a_2) \in (A - \{0\})^2$. Alors $I_1 + I_2$, $I_1 I_2$, $I_1 \cap I_2$ sont des idéaux fractionnaires car ils sont contenus dans $(a_1 a_2)^{-1}A$. De plus $I = \{x \in K/xI_2 \subset I_1\}$ est un idéal fractionnaire. (Preuve : c'est un A -module non nul ; on a $uvI \subset A$ avec $u \neq 0$ vérifiant $uI_1 \subset A$ et $v \in I_2$ non nul.) Il en résulte (par application à $I_1 = I$ et $I_2 = A$ ou $I_2 = I$) que I_1^{-1} et $R(I_1)$ sont des idéaux fractionnaires.

Lorsque A est un anneau noethérien, tout idéal fractionnaire I est de type fini. En effet on a un isomorphisme de A -modules entre I et $aI \subset A$ qui est un idéal de A et qui est donc de type fini.

Soit $\mathcal{P}$ un idéal premier de A . Le *localisé* $A_{(\mathcal{P})}$ de A en $\mathcal{P}$ est le sous-anneau de K formé des éléments de la forme u/v (avec $(u, v) \in A \times (A - \mathcal{P})$). C'est un *anneau local*, c'est-à-dire un anneau contenant un unique idéal maximal. On a $\mathcal{P} = \mathcal{P}A_{(\mathcal{P})} \cap A$. Mentionnons la propriété importante suivante de la localisation :

Lemme 1. — Soit I un idéal de $A_{(\mathcal{P})}$. On a

$$I = (I \cap A)A_{(\mathcal{P})}.$$

Démonstration. — On l'inclusion $(I \cap A)A_{(\mathcal{P})} \subset I$. Réciproquement tout élément de I s'écrit sous la forme u/v avec $(u, v) \in A \times (A - \mathcal{P})$. Comme v est inversible dans $A_{(\mathcal{P})}$, on a $u \in I \cap A$. On a donc $u/v \in (I \cap A)A_{(\mathcal{P})}$.

Tout idéal de $A_{(\mathcal{P})}$ est donc de la forme $IA_{(\mathcal{P})}$ où I est un idéal de A . Cela entraîne que si A est noethérien $A_{(\mathcal{P})}$ est noethérien. Caractérisons les anneaux de valuation discrète.

PROPOSITION 1. — *Soit A un anneau noethérien, intégralement clos et possédant un unique idéal premier non nul $\mathcal{M}$. Alors A est un anneau de valuation discrète.*

Démonstration. — Notons K le corps des fractions de A . Procédons en plusieurs étapes.

Lemme 2. — *Soit $x \in \mathcal{M}$, $x \neq 0$. On a $A[\frac{1}{x}] = K$.*

Démonstration. — Il suffit de prouver que $A[\frac{1}{x}]$ est un corps, c'est-à-dire que tout idéal premier de $A[\frac{1}{x}]$ est nul. Soit $\mathcal{P}$ un idéal premier de $A[\frac{1}{x}]$. Il ne contient pas x qui est inversible dans $A[\frac{1}{x}]$. L'idéal $\mathcal{P} \cap A$ est un idéal premier de A distinct de $\mathcal{M}$ puisque $x \in \mathcal{M}$. On a donc $\mathcal{P} \cap A = \{0\}$. Soit y/x^n un élément de $\mathcal{P}$, où on peut supposer que $y \in A$. On a $y \in \mathcal{P} \cap A = \{0\}$. Cela prouve que $\mathcal{P}$ est nul.

Lemme 3. — *Soit z un élément de A non nul. Soit $x \in \mathcal{M}$. Il existe $n \geq 0$ tel que $x^n \in zA$.*

Démonstration. — Si $z \neq 0$, on a $1/z \in K = A[\frac{1}{x}]$. Il existe donc n tel que $x^n z \in A$.

Lemme 4. — *Soit z un élément de A non nul. Il existe un entier $m \geq 0$ tel que $\mathcal{M}^m \subset zA$.*

Démonstration. — Puisque A est un anneau noethérien, $\mathcal{M}$ est un A -module de type fini. Soient $x_1, x_2, \dots, x_k$ des générateurs de $\mathcal{M}$. Posons $m = kn$, avec n tel que $x_i^n \in zA$ pour tout i , c'est possible d'après le lemme 2. L'idéal $\mathcal{M}^m$ est engendré par les monômes de degré total m en les x_i . Tous les tels monômes contiennent un facteur du type x_i^n ; un tel facteur est dans zA . On en déduit que $\mathcal{M}^m \subset zA$.

Lemme 5. — *On a $\mathcal{M}^{-1} \neq A$.*

Démonstration. — Choisissons m minimal parmi les entiers ≥ 0 tels que $\mathcal{M}^m \subset zA$. Soit $y \in \mathcal{M}^{m-1} - zA$. On a $\mathcal{M}y \subset zA$. Par conséquent on a $y/z \in \mathcal{M}^{-1} - A$.

Lemme 6. — *On a $\mathcal{M}\mathcal{M}^{-1} = A$.*

Démonstration. — C'est un sous A -module de A qui contient $\mathcal{M}$. Il est donc égal à A ou $\mathcal{M}$. Soit t un élément de $\mathcal{M}^{-1} - A$. L'élément t n'est pas entier sur A puisque A est intégralement clos. Pour tout $n > 0$, t^n n'est pas une combinaison linéaire à coefficients dans A des t^i , $i < n$. La suite de A -modules $A \subset A + At \subset A + At + At^2 \subset \dots$ est donc strictement croissante. Cette suite n'est donc contenue dans aucun A -module de type fini, puisque A est noethérien. En particulier elle n'est pas contenue dans $\mathcal{M}^{-1}$, qui est de type fini (en effet c'est un idéal fractionnaire). Par conséquent il existe $n > 0$, que l'on peut choisir minimal, tel que $t^n \notin \mathcal{M}^{-1}$. On a donc que $t^n \mathcal{M}$ n'est pas contenu dans A et *a fortiori* pas contenu dans $\mathcal{M}\mathcal{M}^{-1}$ ni dans $t\mathcal{M}$. Par conséquent $t^{n-1}\mathcal{M}$ n'est pas contenu dans $\mathcal{M}$. L'idéal $\mathcal{M}\mathcal{M}^{-1}$ de A n'est donc pas contenu dans $\mathcal{M}$. Puisque $\mathcal{M}$ est maximal, cela entraîne que $\mathcal{M}\mathcal{M}^{-1} = A$.

Lemme 7. — *L'idéal $\mathcal{M}$ est principal.*

Démonstration. — Puisqu'on a $\mathcal{M}\mathcal{M}^{-1} = A$, il existe un élément u de $A - \mathcal{M}$ qui s'exprime comme le produit d'un élément v de $\mathcal{M}$ par un élément w de $\mathcal{M}^{-1}$. Cet élément u est

inversible puisque $\mathcal{M}$ est un idéal maximal. Soit $t \in \mathcal{M}$. On a $t = twv/u = (tw/u)v$. Comme $w \in \mathcal{M}^{-1}$, tw appartient à A . On a donc $t \in vA$. Par conséquent $\mathcal{M}$ est engendré par v comme A -module. Il est donc principal.

Soit I un idéal propre de A . Il est contenu dans $\mathcal{M} = \pi A$, où π est une uniformisante de $\mathcal{M}$. Donc $\frac{1}{\pi}I$ est un idéal de A contenant strictement I . En itérant ce processus, et en utilisant le fait que A est noethérien, on montre que I est de la forme $\pi^k A$, avec k entier et donc que I est principal. Ainsi, l'anneau A est principal. Cela achève la preuve de la proposition 1.

Citons une autre caractérisation des anneaux de valuation discrète : un anneau intègre, local, noethérien et dont l'idéal maximal est principal est de valuation discrète. Nous ne ferons pas usage de cette caractérisation.

Soit A un anneau noethérien et intégralement clos. Soit $\mathcal{P}$ est un idéal premier minimal et maximal de A . Alors $A_{(\mathcal{P})}$ est un anneau de valuation discrète dont l'idéal maximal n'est autre que $\mathcal{P}A_{(\mathcal{P})}$. Notons $v_{\mathcal{P}}$ la valuation associée. Les idéaux fractionnaires de $A_{(\mathcal{P})}$ sont de la forme $\mathcal{P}^n A_{(\mathcal{P})}$, $n \in \mathbf{Z}$.

Lemme 8. — Supposons que A soit intégralement clos. Alors $A_{(\mathcal{P})}$ est intégralement clos. *Démonstration.* — Soit x un élément K qui est entier sur $A_{(\mathcal{P})}$. Il vérifie

$$x^n + \frac{a_{n-1}}{b}x^{n-1} + \dots + \frac{a_0}{b} = 0,$$

avec $b \in A - \mathcal{P}$ et $a_i \in A$ ($i \in \{0, 1, \dots, n-1\}$). On en déduit que bx est entier sur A . C'est donc un élément de A . Cela entraîne qu'on a $x \in A_{(\mathcal{P})}$.

2. Anneaux de Dedekind

Un *anneau de Dedekind* est un anneau A intègre et noethérien vérifiant l'une au moins des conditions suivantes.

- (ι) A est intégralement clos et tout idéal premier et non nul de A est maximal.
- (ι) Pour tout idéal premier $\mathcal{P}$ non nul de A , $A_{(\mathcal{P})}$ est un anneau de valuation discrète.
- (ι) Tout idéal fractionnaire de A est inversible.

Exemples. — Comme on le verra plus tard, l'anneau des entiers d'un corps de nombres, en particulier $\mathbf{Z}$, est un anneau de Dedekind.

Soit k un corps. L'anneau $k[T]$ est un anneau de Dedekind. En revanche l'anneau $k[T_1, T_2]$ n'est pas de Dedekind puisque les idéaux engendrés par T_1 et T_2 sont non nuls, distincts et premiers.

Un anneau principal (*a fortiori* de valuation discrète) est un anneau de Dedekind. En revanche un anneau de Dedekind n'est pas nécessairement principal ni même factoriel.

PROPOSITION 2. — *Soit A un anneau intègre et noethérien. Les conditions (ι), (ι) et (ι) sont équivalentes pour A .*

Démonstration. — (ι) entraîne (ι) . Cela résulte des propriétés de $A_{(\mathcal{P})}$ déjà établies de la proposition 1 appliquées à $A_{(\mathcal{P})}$. En effet, $A_{(\mathcal{P})}$ est noethérien et intégralement clos. De plus, si $\mathcal{P}$ est un idéal premier non nul de $A_{(\mathcal{P})}$, il est contenu dans un idéal maximal $\mathcal{M}$ de $A_{(\mathcal{P})}$. Ainsi les idéaux $\mathcal{P} \cap A$ et $\mathcal{M} \cap A$ de A sont premiers et emboîtés. Par hypothèse, ils sont égaux. Ainsi on a $\mathcal{P} = (\mathcal{P} \cap A)A_{(\mathcal{P})} = (\mathcal{M} \cap A)A_{(\mathcal{P})} = \mathcal{M}$. Donc $\mathcal{P}$ est maximal. On peut donc appliquer la proposition 1.

$(\iota\iota)$ entraîne $(\iota\iota)$. Soit I un idéal fractionnaire de A . Quitte à remplacer I par aI , avec $a \in A$ et $aI \in A$, on peut supposer que $I \subset A$. Considérons l'idéal II^{-1} . Supposons qu'il soit strictement contenu dans A . Il existe alors un idéal premier $\mathcal{P}$ de A qui le contient. Soit $(a_1, a_2, \dots, a_n)$ un système fini de générateurs de I . Soit x un élément de I de valuation $\mathcal{P}$ -adique minimale. On a $IA_{(\mathcal{P})} = xA_{(\mathcal{P})}$. On peut donc écrire les générateurs de I sous la forme $a_i = xu_i/v_i$, avec $u_i \in A$ et $v_i \in A - \mathcal{P}$.

Posons $v = \prod_i v_i$. C'est un élément de $A - \mathcal{P}$. Puisqu'on a $va_i/x \in A$, on a $v/x \in I^{-1}$. Par conséquent on a $v \in II^{-1}$. Contradiction.

$(\iota\iota)$ entraîne (ι) . Vérifions que A est intégralement clos. Soit x un élément A -entier de K . L'anneau $A[x]$ est de type fini sur A et contenu dans K . C'est donc un idéal fractionnaire. On a $A[x]^2 = A[x]$ et donc

$$A[x] = A[x](A[x]A[x]^{-1}) = A[x]A[x]^{-1} = A.$$

Soit $\mathcal{P}$ un idéal premier de A . Soit $\mathcal{M}$ un idéal maximal qui contient $\mathcal{P}$. L'idéal fractionnaire $\mathcal{M}^{-1}\mathcal{P}$ est contenu dans A . On a donc $(\mathcal{M}^{-1}\mathcal{P})\mathcal{M} = \mathcal{P}$. Puisque $\mathcal{P}$ est un idéal premier on a $\mathcal{P} = \mathcal{M}$ ou $\mathcal{P}\mathcal{M}^{-1} \subset \mathcal{P}$. Il reste à exclure ce dernier cas. Rappelons qu'on a $A \subset \mathcal{M}^{-1}$ et $A \neq \mathcal{M}^{-1}$. Le cas $\mathcal{P}\mathcal{M}^{-1} \subset \mathcal{P}$ entraîne

$$\mathcal{M}^{-1} \subset \mathcal{P}\mathcal{P}^{-1}\mathcal{M}^{-1} \subset \mathcal{P}\mathcal{P}^{-1} = A.$$

Cela est absurde.

Soit A un anneau de Dedekind et $\mathcal{P}$ un idéal maximal de A . Soit I un idéal fractionnaire de K (ou, plus généralement, un sous-ensemble non nul et non vide de K en autorisant la valeur $-\infty$). Posons

$$v_{\mathcal{P}}(I) = \inf_{x \in I} v_{\mathcal{P}}(x) \in \mathbf{Z}.$$

On vérifie que cette quantité est bien définie dans $\mathbf{Z}$.

Soit A un anneau de Dedekind. La multiplication des idéaux fractionnaires de A définit une loi de groupe, puisque tout idéal fractionnaire est inversible dans un anneau de Dedekind. On appelle le groupe ainsi formé par les idéaux fractionnaires *groupe des idéaux* de A . On le notera $\mathcal{I}(A)$.

PROPOSITION 3. — *Le groupe $\mathcal{I}(A)$ est isomorphe au groupe abélien libre engendré par les idéaux premiers non nuls.*

Soit I un idéal fractionnaire de K . Plus précisément on a

$$I = \prod_{\mathcal{P}} \mathcal{P}^{v_{\mathcal{P}}(I)}.$$

Démonstration. — Commençons par un résultat préliminaire.

Lemme 9. — Soit I un idéal de A . C'est un produit d'idéaux premiers de A .

Démonstration. — Soit $\mathcal{P}_1$ un idéal maximal de A contenant I . On a $I \subset I\mathcal{P}_1^{-1} \subset A$. Supposons que I ne soit pas produit d'idéaux maximaux. Une construction itérative permet de construire une suite croissante d'idéaux :

$$I \subset I\mathcal{P}_1^{-1} \subset I\mathcal{P}_1^{-1}\mathcal{P}_2^{-1} \subset \dots \subset A.$$

Cette suite est finie puisque A est noethérien. Cette contradiction donne la preuve du lemme.

Revenons à la démonstration de la proposition 3.

Pour $\mathcal{P}$ idéal maximal de $\mathbf{Z}$, considérons l'application $i_{\mathcal{P}} : \mathcal{I}(A) \longrightarrow \mathcal{I}(A_{(\mathcal{P})})$ qui à I associe $IA_{(\mathcal{P})}$. C'est un homomorphisme de groupes. Soit $\mathcal{P}'$ un idéal premier de A distinct de $\mathcal{P}$. On a $i_{\mathcal{P}}(\mathcal{P}') = A_{(\mathcal{P})}$. En effet tout élément non nul de $\mathcal{P}'$ n'est pas dans l'idéal maximal de $A_{(\mathcal{P})}$; l'idéal de $A_{(\mathcal{P})}$ qu'il engendre est donc égal à $A_{(\mathcal{P})}$.

Démontrons que $\mathcal{I}(A)$ est engendré par les idéaux maximaux de A . Soit I un idéal fractionnaire de A . Soit $t \in A$ tel que $tI \subset A$. D'après le lemme 9, les idéaux de A tI et tA s'expriment comme produits d'idéaux maximaux. Puisque I est inversible, c'est le quotient de ces deux produits.

Démontrons que le sous-groupe de $\mathcal{I}(A)$ engendré par les idéaux premiers est librement engendré. Supposons qu'on ait $\prod_{\mathcal{P}} \mathcal{P}^{r_{\mathcal{P}}} = A$, avec $r_{\mathcal{P}} \in \mathbf{Z}$ et presque toujours nul. Soit $\mathcal{P}_0$ un idéal premier de A tel que $r_{\mathcal{P}_0}$ soit non nul. On a

$$A_{(\mathcal{P}_0)} = i_{\mathcal{P}_0}(A) = i_{\mathcal{P}_0}(\mathcal{P}_0^{r_{\mathcal{P}_0}}) = \mathcal{P}_0^{r_{\mathcal{P}_0}} A_{(\mathcal{P}_0)} \neq A_{(\mathcal{P}_0)}.$$

Soit I un idéal fractionnaire de K . Il s'exprime donc sous la forme

$$I = \prod_{\mathcal{P}} \mathcal{P}^{r_{\mathcal{P}}}.$$

On a

$$i_{\mathcal{P}}(I) = \mathcal{P}^{r_{\mathcal{P}}} A_{(\mathcal{P})} = (\mathcal{P} A_{(\mathcal{P})})^{r_{\mathcal{P}}}.$$

Par conséquent on a

$$r_{\mathcal{P}} = v_{\mathcal{P}}(IA_{(\mathcal{P})}) = v_{\mathcal{P}}(I).$$

Cela achève la démonstration de la proposition 3.

Dans un anneau de Dedekind on n'a pas nécessairement la factorisation unique des éléments de A (car un anneau de Dedekind n'est pas nécessairement factorisation). En revanche la proposition 3 nous assure qu'on a la factorisation unique des idéaux à partir des idéaux premiers.

Les *idéaux fractionnaires principaux* d'un anneau de Dedekind A sont les idéaux de la forme aI avec $a \in K$. Ils forment un sous-groupe de $\mathcal{I}(A)$. Le groupe quotient est le *groupe des classes d'idéaux* de A (ou de K). C'est encore le groupe de Picard de A . Ce

n'est pas nécessairement un groupe fini. Le groupe des éléments inversibles de A est le *groupe des unités* de A (ou de K).

COROLLAIRE 1. — Soit A un anneau de Dedekind de corps de fractions K . Soit $x \in K$. On a $v_{\mathcal{P}}(x) = 0$ pour presque tout idéal maximal $\mathcal{P}$ de A .

COROLLAIRE 2. — Soit A un anneau de valuation discrète. On a $\mathcal{I}(A) \simeq \mathbf{Z}$.

COROLLAIRE 3. — Soit A un anneau de Dedekind. Les applications $i_{\mathcal{P}}$ définissent un isomorphisme de groupes entre $\mathcal{I}(A)$ et la somme directe des groupes $\mathcal{I}(A_{(\mathcal{P})})$, où $\mathcal{P}$ parcourt les idéaux premiers maximaux de A .

Soient I_1 et I_2 des idéaux fractionnaires d'un anneau de Dedekind A . Soit $\mathcal{P}$ un idéal maximal de A . Indiquons les formules suivantes, qui se déduisent de la proposition 3

$$\begin{aligned} v_{\mathcal{P}}(I_1 I_2) &= v_{\mathcal{P}}(I_1) + v_{\mathcal{P}}(I_2), \\ v_{\mathcal{P}}(I_1 + I_2) &= \min(v_{\mathcal{P}}(I_1), v_{\mathcal{P}}(I_2)), \\ v_{\mathcal{P}}(I_1 \cap I_2) &= \max(v_{\mathcal{P}}(I_1), v_{\mathcal{P}}(I_2)), \\ v_{\mathcal{P}}(I_1 I_2^{-1}) &= v_{\mathcal{P}}(I_1) - v_{\mathcal{P}}(I_2). \end{aligned}$$

Le résultat suivant est connu sous le nom de *lemme d'approximation* (c'est une variante du *théorème des restes chinois*).

PROPOSITION 4. — Soit A un anneau de Dedekind de corps de fractions K . Soit I un ensemble fini. Soient $(x_i)_{i \in I}$, $(n_i)_{i \in I}$ et $(\mathcal{P}_i)_{i \in I}$ des familles d'éléments de K , d'entiers et d'idéaux maximaux de A deux à deux distincts respectivement. Il existe alors $y \in K$ tel que $v_{\mathcal{P}_i}(y - x_i) \geq n_i$ pour tout $i \in I$ et $v_{\mathcal{P}}(y) \geq 0$ pour tout $\mathcal{P} \neq \mathcal{P}_i$, $i \in I$.

Démonstration. — Dans un premier temps, on suppose que les x_i appartiennent à A . On peut supposer que les n_i sont ≥ 0 .

Les idéaux $\mathcal{P}_i^{n_i}$ sont deux à deux premiers entre eux lorsque i parcourt I . On a donc un isomorphisme d'anneaux $A / \prod_{i \in I} \mathcal{P}_i^{n_i} \rightarrow \prod_{i \in I} (A / \mathcal{P}_i^{n_i})$, d'après le lemme des restes chinois. L'homomorphisme surjectif qui en résulte $A \rightarrow \prod_{i \in I} (A / \mathcal{P}_i^{n_i})$ permet de conclure.

Ne faisons plus de restriction sur les x_i . On se ramène au cas précédent en posant $x_i = a_i/s$ avec $a_i \in A$ et $s \in A$. On cherche y sous la forme a/s . Il reste à déterminer a par les conditions

$$v_{\mathcal{P}_i}(a - a_i) \geq n_i + v_{\mathcal{P}_i}(s) \text{ et } v_{\mathcal{P}}(a) \geq v_{\mathcal{P}}(s),$$

pour $\mathcal{P}$ distinct des $\mathcal{P}_i$. Cela revient à un problème du type précédent en agrandissant la famille $\mathcal{P}_i$.

Exercice 1. — Dédurre du lemme d'approximation qu'un anneau de Dedekind qui n'a qu'un nombre fini d'idéaux premiers est principal.

Exercice 2. — Soit A un anneau de Dedekind de corps de fractions K . Démontrer que l'application $K^* \rightarrow \mathcal{I}(A)$ qui à a associe l'idéal fractionnaire aA est un homomorphisme de groupes qui a pour noyau le groupe des unités de A et pour conoyau le groupe des classes d'idéaux de A .