Idéaux inversibles – Anneaux de Dedekind

Lionel Ducos août 2009

Table des matières

11.1 Introduction

Remarque. Les structures algébriques dont nous allons parler n'étaient évidemment pas usitées au XIX^e siècle. Mais, pour comprendre le cœur du problème, il nous paraît commode de nous exprimer avec le langage actuel.

Les anneaux de Dedekind prennent naissance dans la théorie des nombres. Il est maintenant bien connu que, pour résoudre certains problèmes concernant les nombres entiers relatifs, travailler uniquement avec l'anneau $\mathbb{Z}$ est maladroit, voire totalement insuffisant. Au cours des XVIII^e et XIX^e siècles, de grands mathématiciens comme Euler, Gauss, Eisenstein, Dirichlet, Legendre, Kummer, Kronecker, et Dedekind bien sûr, participent à l'élaboration progressive de ce qu'on nomme de nos jours les anneaux de Dedekind. Cela commence par le désir de retrouver dans les anneaux de nombres le théorème fondamental de l'arithmétique.

Théorème 11.108 ((Théorème fondamental de l'arithmétique).) *Tout entier naturel non nul s'écrit comme produit de nombres premiers, et cela de manière unique (à l'ordre des facteurs près).*

Définition 11.109 *Un **anneau de nombres** est un sous-anneau de $\mathbb{C}$ formé d'éléments **algébriques** sur $\mathbb{Z}$ (c'est-à-dire racines d'un polynôme non nul à coefficients dans $\mathbb{Z}$).*

Dans la pratique, on considère souvent des anneaux de nombres constitués uniquement d'éléments *entiers* sur $\mathbb{Z}$ et appartenant à une extension de $\mathbb{Q}$ de dimension finie.

Définition 11.110 *On note $A \subset B$ deux anneaux commutatifs. On dit qu'un élément $x \in B$ est* ***entier*** *sur A lorsque x est racine d'un polynôme unitaire à coefficients dans A.*

Définition 11.111 *La* ***fermeture intégrale*** *d'un corps de nombres $\mathcal{K}$ est le sous-anneau de $\mathcal{K}$ formé par tous les éléments de $\mathcal{K}$ entiers sur $\mathbb{Z}$.*

Toutefois, cette propriété *factorielle* de l'anneau $\mathbb{Z}$ énoncée dans le théorème 11.108 n'est réalisée que très rarement de manière générale dans les anneaux intègres : les classes des anneaux *euclidiens*, ou *principaux*, ou « simplement » *factoriels*, sont malheureusement très petites, et, en particulier, exceptionnels sont les anneaux de nombres factoriels. Les anneaux intègres *noethériens*, quant à eux, forment une très large classe, et possèdent déjà la « moitié » de la propriété de factorisation.

> Rappel de la proposition **??** Dans un anneau intègre noethérien, tout élément non nul s'écrit comme produit d'éléments irréductibles.

Mais cette moitié n'est pas suffisante : il manque l'incontournable unicité de cette décomposition. Par exemple, dans l'anneau de nombres $\mathbb{Z}[i\sqrt{3}] = \{a + bi\sqrt{3} \mid a, b \in \mathbb{Z}\}$, on a les égalités

$$(1 + i\sqrt{3})(1 - i\sqrt{3}) = 4 = 2.2$$

mais les éléments 2, $1+i\sqrt{3}$, $1-i\sqrt{3}$, bien qu'irréductibles dans $\mathbb{Z}[i\sqrt{3}]$, sont loin d'être égaux à un inversible près (les seuls inversibles de $\mathbb{Z}[i\sqrt{3}]$ sont ± 1). De même, les très utiles anneaux cyclotomiques $\mathbb{Z}[\xi]$, où $\xi \in \mathbb{C}$ est une racine n-ième de l'unité, ne possèdent pas en général le caractère *factoriel* que les mathématiciens recherchaient tant.

Cependant, le tableau n'est pas totalement noir car certains anneaux de nombres, comme ceux des entiers de Gauss $\mathbb{Z}[i]$ ou de Dirichlet $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, ont d'excellentes propriétés *euclidiennes* (bien que le second possède une infinité d'éléments inversibles). Concernant les anneaux cyclotomiques, Kummer a l'intuition qu'il y a « comme un manque » d'éléments dans ces anneaux pour assurer l'unicité de la factorisation en irréductibles (ou premiers). Il invente alors les *nombres idéaux*, ce qui lui permet d'annoncer que, dans tout anneau cyclotomique, tout élément non nul s'écrit comme produit unique de nombres premiers idéaux. Enfin, Dedekind entreprend de généraliser ce résultat de Kummer à une grande classe d'anneaux commutatifs, comme les anneaux d'entiers (ou fermetures intégrales) et les anneaux qui interviennent dans la théorie des surfaces de Riemann. Pour cela, Dedekind développe les notions d'*idéal*, d'*idéal principal*, d'*idéal fractionnaire*, etc. Finalement, les anneaux de Dedekind se révèlent relativement fréquents (contrairement aux anneaux principaux, ou factoriels) car présents dans toute l'algèbre commutative, et entre autres, *via* l'intermédiaire des anneaux à valuation discrète (c'est-à-dire anneaux locaux principaux), sont aussi utilisés en géométrie algébrique.

On constate que toutes les propriétés d'un anneau de Dedekind viennent de la qualité de ses idéaux. En effet, tous les idéaux non nuls d'un anneau de Dedekind sont *inversibles*, et cela provoque rapidement une excellente arithmétique sur les idéaux. C'est pourquoi nous commençons par étudier les idéaux inversibles dans leur généralité. Le lecteur pourra trouver d'autres approches dans [Sam] p. 58, [Ser] p. 21, [Mal] p. 132, [Mat] p. 82, ou même [Bou] p. 216.

11.2 Idéaux inversibles

11.2.1 Définition et premières propriétés

Rappel.(voir exemple **??**) L'anneau total des fractions d'un anneau commutatif A est l'anneau localisé $S^{-1}A$ où S est la partie multiplicative formée par tous les éléments réguliers de A. L'anneau total des fractions est toujours un anneau contenant A, et donc un A-module. En particulier, il s'agit du corps des fractions de A lorsque A est intègre.

Définition 11.112 *On note A un anneau commutatif. On appelle **idéal fractionnaire** un sous-A-module de l'anneau total des fractions, s'écrivant $a^{-1}\mathcal{J}$ où a est un élément régulier de l'anneau A et $\mathcal{J}$ un idéal de l'anneau A.*

Les idéaux de A sont des idéaux fractionnaires (prendre $a = 1$), et, réciproquement, un idéal fractionnaire inclus dans A est un idéal de A (puisque A-module).

Notation On note A un anneau commutatif et B son anneau total des fractions. Pour deux A-modules $\mathcal{I}, \mathcal{J}$ inclus dans B, on note $\mathcal{I}.\mathcal{J}$ le sous-A-module de B engendré par les produits $i.j$ avec $i \in \mathcal{I}$ et $j \in \mathcal{J}$. Autrement dit, le sous-A-module $\mathcal{I}.\mathcal{J}$ est formé de combinaisons linéaires à coefficients dans A de produits ij avec $i \in \mathcal{I}$ et $j \in \mathcal{J}$.

Cette notation est justifiée car elle prolonge de manière naturelle le produit des idéaux de A.

Définition 11.113 *On note A un anneau commutatif. Un idéal fractionnaire $\mathcal{I}$ est dit **inversible** lorsqu'il existe un idéal fractionnaire $\mathcal{J}$ tel que $\mathcal{I}.\mathcal{J} = A$.*

Un idéal $\mathcal{I}$ de A est inversible si et seulement s'il existe un idéal $\mathcal{J}$ de A et un élément régulier $a \in \mathcal{I}$ tels que $\mathcal{I}.\mathcal{J} = \langle a \rangle$. En particulier, tout idéal de A engendré par un élément régulier est inversible. Par exemple, les idéaux non nuls de $\mathbb{Z}$ sont donc inversibles dans l'ensemble des idéaux fractionnaires de $\mathbb{Z}$.

Proposition 11.114 *L'ensemble des idéaux fractionnaires inversibles est un groupe commutatif pour la multiplication des idéaux fractionnaires.*

Démonstration Si a et b sont réguliers, alors on a $a^{-1}\mathcal{I}.b^{-1}\mathcal{J} = (ab)^{-1}(\mathcal{I}.\mathcal{J})$ où ab est régulier. Ainsi la multiplication est manifestement une loi interne commutative. Elle est aussi clairement associative et d'élément neutre A. Et, par hypothèse, tout élément de l'ensemble est inversible ! □

Proposition 11.115 *On note A un anneau commutatif, $\mathcal{I}, \mathcal{J}$ deux A-modules inclus dans l'anneau total des fractions de A. Si $\mathcal{I}.\mathcal{J} = A$, alors*
- *les idéaux $\mathcal{I}$ et $\mathcal{J}$ sont deux A-modules de type fini ;*
- *les idéaux $\mathcal{I}$ et $\mathcal{J}$ sont deux idéaux fractionnaires de A, inverses l'un de l'autre.*

En particulier, tout idéal inversible de A est un idéal de type fini.

Démonstration On a $\mathcal{I}.\mathcal{J} = A$, on peut donc écrire $1 = i_1 j_1 + \cdots + i_n j_n$ avec $i_k \in \mathcal{I}$ et $j_k \in \mathcal{J}$ pour tout k. Montrons que $\mathcal{I} = \langle i_1, \ldots, i_n \rangle$ et $\mathcal{J} = \langle j_1, \ldots, j_n \rangle$ en tant que A-modules. On a évidemment $\langle i_1, \ldots, i_n \rangle \subset \mathcal{I}$ et $\langle j_1, \ldots, j_n \rangle \subset \mathcal{J}$. Mais $1 \in \langle i_1, \ldots, i_n \rangle \langle j_1, \ldots, j_n \rangle$, donc

$$\mathcal{J} = \mathcal{J}.1 = \mathcal{J} \langle i_1, \ldots, i_n \rangle \langle j_1, \ldots, j_n \rangle \subset \mathcal{J}.\mathcal{I}. \langle j_1, \ldots, j_n \rangle = \langle j_1, \ldots, j_n \rangle$$

et, de même, $\mathcal{I} \subset \langle i_1, \ldots, i_n \rangle$. Ainsi, nous obtenons des systèmes générateurs finis de $\mathcal{I}$ et $\mathcal{J}$. Enfin, étant donné que ces systèmes générateurs sont finis, il existe un dénominateur commun pour leurs éléments, si bien qu'en fait $\mathcal{I}$ et $\mathcal{J}$ sont des idéaux fractionnaires de A (inverses l'un de l'autre par définition). □

Proposition 11.116 *On note $\mathcal{I}, \mathcal{J}$ deux idéaux fractionnaires d'un anneau commutatif A non nul. Leur produit $\mathcal{I}.\mathcal{J}$ est inversible si et seulement si $\mathcal{I}$ et $\mathcal{J}$ le sont.*

Démonstration La réciproque étant déjà connue, il suffit de prouver que $\mathcal{I}$ et $\mathcal{J}$ sont inversibles lorsque $\mathcal{I}.\mathcal{J}$ l'est. Mais cela est assez évident : le produit $\mathcal{I}.\mathcal{J}$ est inversible donc il existe un idéal fractionnaire $\mathcal{K}$ tel que $\mathcal{I}\mathcal{J}\mathcal{K} = A$, ce qui donne un inverse $\mathcal{J}\mathcal{K}$ de $\mathcal{I}$ et un inverse $\mathcal{I}\mathcal{K}$ à $\mathcal{J}$. □

En raison de ce résultat, l'étude des idéaux fractionnaires inversibles revient à l'étude des idéaux inversibles inclus dans l'anneau A. En effet, comme tout élément régulier a engendre un idéal inversible, on voit que, pour tout idéal $\mathcal{J} \subset A$, l'inversibilité de $a^{-1}\mathcal{J}$ est équivalente à celle de $\mathcal{J}$. C'est pourquoi, nous allons nous concentrer plus particulièrement sur l'étude des idéaux inversibles inclus dans A.

Lemme 11.117 ((Cas particulier du lemme de simplification).) *On note $\mathcal{I}$, $\mathcal{J}$, $\mathcal{J}'$ trois idéaux d'un anneau commutatif A tels que $\mathcal{I}\mathcal{J} \subset \mathcal{I}\mathcal{J}'$. Si $\mathcal{I}$ est inversible, alors $\mathcal{J} \subset \mathcal{J}'$.*

Démonstration Il suffit de multiplier l'inclusion $\mathcal{I}\mathcal{J} \subset \mathcal{I}\mathcal{J}'$ par l'inverse de $\mathcal{I}$. □

11.2.2 Opérations arithmétiques

Une des qualités des idéaux inversibles réside dans l'arithmétique sur les idéaux à laquelle ils donnent naissance.

Proposition 11.118 *On note $\mathcal{I}$ un idéal inversible d'un anneau commutatif A. Pour tout idéal $\mathcal{K} \subset \mathcal{I}$, il existe un unique idéal $\mathcal{J}$ tel que $\mathcal{I}\mathcal{J} = \mathcal{K}$. Cet idéal $\mathcal{J}$ sera noté $(\mathcal{K} \div \mathcal{I})$.*

Démonstration Existence de $\mathcal{J}$: posons $\mathcal{J} = \mathcal{I}^{-1}\mathcal{K}$. Alors $\mathcal{J} \subset \mathcal{I}^{-1}\mathcal{I} = A$ donc $\mathcal{J}$ est un idéal de A, et bien sûr $\mathcal{I}\mathcal{J} = \mathcal{K}$. L'unicité de $\mathcal{J}$ vient du lemme 11.117 de simplification. □

Lemme 11.119 *On note $\mathcal{I}, \mathcal{J}, \mathcal{K}$ des idéaux d'un anneau commutatif. On suppose $\mathcal{J} \subset \mathcal{K}$.*
Si $\mathcal{I}$ est inversible, alors $(\mathcal{J} \div \mathcal{I}) \subset (\mathcal{K} \div \mathcal{I})$.
Si $\mathcal{J}$ et $\mathcal{K}$ sont inversibles, alors $(\mathcal{I} \div \mathcal{J}) \supset (\mathcal{I} \div \mathcal{K})$.

Démonstration Pour la première inclusion, on a $(\mathcal{J} \div \mathcal{I})\mathcal{I} = \mathcal{J} \subset \mathcal{K} = (\mathcal{K} \div \mathcal{I})\mathcal{I}$ et le lemme 11.117 de simplification permet de conclure. Pour la seconde inclusion, on a $(\mathcal{I} \div \mathcal{J})\mathcal{J}\mathcal{K} = \mathcal{I}\mathcal{K} \supset \mathcal{I}\mathcal{J} = (\mathcal{I} \div \mathcal{K})\mathcal{K}\mathcal{J}$ et le lemme 11.117 de simplification (par $\mathcal{K}\mathcal{J}$) permet de conclure. □

Lemme 11.120 *On note $\mathcal{J}, \mathcal{K}$ deux idéaux d'un anneau commutatif. Si $\mathcal{J} + \mathcal{K}$ est inversible, alors*

$$(\mathcal{J} \div (\mathcal{J} + \mathcal{K})) \ + \ (\mathcal{K} \div (\mathcal{J} + \mathcal{K})) \ = \ A.$$

Démonstration Posons $\mathcal{I} = (\mathcal{J} \div (\mathcal{J}+\mathcal{K})) + (\mathcal{K} \div (\mathcal{J}+\mathcal{K}))$. Comme $(\mathcal{J} \div (\mathcal{J}+\mathcal{K})).(\mathcal{J}+\mathcal{K}) = \mathcal{J}$ et $(\mathcal{K} \div (\mathcal{J}+\mathcal{K})).(\mathcal{J}+\mathcal{K}) = \mathcal{K}$ car $\mathcal{J}+\mathcal{K}$ est inversible, il vient naturellement $\mathcal{I}(\mathcal{J}+\mathcal{K}) = \mathcal{J}+\mathcal{K}$. Le lemme 11.117 de simplification montre que $\mathcal{I} = A$. □

Proposition 11.121 *On note $\mathcal{J},\mathcal{K}$ deux idéaux d'un anneau commutatif. Si $\mathcal{J}+\mathcal{K}$ est inversible, alors*

$$\begin{array}{lll} & & (\mathcal{J}+\mathcal{K})(\mathcal{J}\cap\mathcal{K}) = \mathcal{J}\mathcal{K} \\ \forall\, n\in\mathbb{N} & & (\mathcal{J}+\mathcal{K})^n = \mathcal{J}^n+\mathcal{K}^n \\ \\ \forall\, \mathcal{I}\subset A & & \mathcal{I}(\mathcal{J}\cap\mathcal{K}) = \mathcal{I}\mathcal{J}\cap\mathcal{I}\mathcal{K} \\ & et & \mathcal{I}+(\mathcal{J}\cap\mathcal{K}) = (\mathcal{I}+\mathcal{J})\cap(\mathcal{I}+\mathcal{K}) \\ & et & \mathcal{I}\cap(\mathcal{J}+\mathcal{K}) = (\mathcal{I}\cap\mathcal{J})+(\mathcal{I}\cap\mathcal{K}) \\ \\ \forall\, \mathcal{I}\ inversible\ \supset \mathcal{J}+\mathcal{K} & & ((\mathcal{J}+\mathcal{K})\div\mathcal{I}) = (\mathcal{J}\div\mathcal{I})+(\mathcal{K}\div\mathcal{I}) \\ & et & ((\mathcal{J}\cap\mathcal{K})\div\mathcal{I}) = (\mathcal{J}\div\mathcal{I})\cap(\mathcal{K}\div\mathcal{I}). \end{array}$$

Si, de plus, $\mathcal{J}$ et $\mathcal{K}$ sont inversibles, alors $\mathcal{J}\cap\mathcal{K}$ est inversible et

$$\begin{array}{lll} \forall\, \mathcal{I}\subset\mathcal{J}\cap\mathcal{K} & & (\mathcal{I}\div(\mathcal{J}\cap\mathcal{K})) = (\mathcal{I}\div\mathcal{J})+(\mathcal{I}\div\mathcal{K}) \\ & et & (\mathcal{I}\div(\mathcal{J}+\mathcal{K})) = (\mathcal{I}\div\mathcal{J})\cap(\mathcal{I}\div\mathcal{K}). \end{array}$$

Toutes ces égalités sont exactement les généralisations de propriétés arithmétiques bien connues dans $\mathbb{Z}$, qui sont les suivantes, en remarquant que $\mathrm{pgcd}(j,k) = j\mathbb{Z}+k\mathbb{Z}$ et $\mathrm{ppcm}(j,k) = j\mathbb{Z}\cap k\mathbb{Z}$.

Proposition 11.122 *On considère j,k deux entiers. Alors*

$$\begin{array}{lll} & & \mathrm{pgcd}(j,\ k).\,\mathrm{ppcm}(j,\ k) = j.k \\ \forall\, n\in\mathbb{N} & & \mathrm{pgcd}(j,\ k)^n = \mathrm{pgcd}(j^n,\ k^n) \\ \\ \forall\, i\in\mathbb{Z} & & i.\,\mathrm{ppcm}(j,\ k) = \mathrm{ppcm}(i.j,\ i.k) \\ & et & \mathrm{pgcd}(i,\ \mathrm{ppcm}(j,\ k)) = \mathrm{ppcm}(\mathrm{pgcd}(i,\ j),\ \mathrm{pgcd}(i,\ k)) \\ & et & \mathrm{ppcm}(i,\ \mathrm{pgcd}(j,\ k)) = \mathrm{pgcd}(\mathrm{ppcm}(i,\ j),\ \mathrm{ppcm}(i,\ k)). \end{array}$$

Pour tout i diviseur commun de j et k, on a

$$\begin{array}{c} \mathrm{pgcd}(j,\ k)/i = \mathrm{pgcd}(j/i,\ k/i) \\ \mathrm{ppcm}(j,\ k)/i = \mathrm{ppcm}(j/i,\ k/i). \end{array}$$

Si, de plus, j et k sont non nuls, alors, pour i multiple commun de j et k, on a

$$\begin{array}{c} i/\,\mathrm{ppcm}(j,\ k) = \mathrm{pgcd}(i/j,\ i/k) \\ i/\,\mathrm{pgcd}(j,\ k) = \mathrm{ppcm}(i/j,\ i/k). \end{array}$$

Démonstration de la proposition11.121 On commence par remarquer que, dans toutes ces égalités à démontrer, une inclusion est toujours évidente :

$$\begin{array}{lll} & & (\mathcal{J}+\mathcal{K})(\mathcal{J}\cap\mathcal{K}) \subset \mathcal{J}\mathcal{K} \\ \forall\, n\in\mathbb{N} & & (\mathcal{J}+\mathcal{K})^n \supset \mathcal{J}^n+\mathcal{K}^n \\ \\ \forall\, \mathcal{I}\subset A & & \mathcal{I}(\mathcal{J}\cap\mathcal{K}) \subset \mathcal{I}\mathcal{J}\cap\mathcal{I}\mathcal{K} \\ & \text{et} & \mathcal{I}+(\mathcal{J}\cap\mathcal{K}) \subset (\mathcal{I}+\mathcal{J})\cap(\mathcal{I}+\mathcal{K}) \\ & \text{et} & \mathcal{I}\cap(\mathcal{J}+\mathcal{K}) \supset (\mathcal{I}\cap\mathcal{J})+(\mathcal{I}\cap\mathcal{K}) \\ \\ \forall\, \mathcal{I}\ \text{inversible}\ \supset \mathcal{J}+\mathcal{K} & & ((\mathcal{J}+\mathcal{K})\div\mathcal{I}) \supset (\mathcal{J}\div\mathcal{I})+(\mathcal{K}\div\mathcal{I}) \\ & \text{et} & ((\mathcal{J}\cap\mathcal{K})\div\mathcal{I}) \subset (\mathcal{J}\div\mathcal{I})\cap(\mathcal{K}\div\mathcal{I}). \end{array}$$

Si, de plus, $\mathcal{J}$ et $\mathcal{K}$ sont inversibles et $\mathcal{J}\cap\mathcal{K}$ est inversible, alors

$$\begin{array}{rll} \forall\, \mathcal{I}\subset\mathcal{J}\cap\mathcal{K} & & (\mathcal{I}\div(\mathcal{J}\cap\mathcal{K}))\supset(\mathcal{I}\div\mathcal{J})+(\mathcal{I}\div\mathcal{K}) \\ & \text{et} & (\mathcal{I}\div(\mathcal{J}+\mathcal{K}))\subset(\mathcal{I}\div\mathcal{J})\cap(\mathcal{I}\div\mathcal{K}). \end{array}$$

Il ne reste qu'à prouver les inclusions inverses et l'inversibilité de $\mathcal{J}\cap\mathcal{K}$.

- On a
$$(\mathcal{J}\div(\mathcal{J}+\mathcal{K}))\mathcal{K}\subset\mathcal{K}\cap(\mathcal{J}\div(\mathcal{J}+\mathcal{K}))(\mathcal{J}+\mathcal{K})=\mathcal{K}\cap\mathcal{J}.$$
donc $(\mathcal{J}\div(\mathcal{J}+\mathcal{K}))\mathcal{K}\mathcal{J}\subset(\mathcal{K}\cap\mathcal{J})\mathcal{J}$. De manière symétrique, $(\mathcal{K}\div(\mathcal{J}+\mathcal{K}))\mathcal{K}\mathcal{J}\subset(\mathcal{K}\cap\mathcal{J})\mathcal{K}$. Or, $(\mathcal{J}\div(\mathcal{J}+\mathcal{K}))\ +\ (\mathcal{K}\div(\mathcal{J}+\mathcal{K}))=A$ car $\mathcal{K}+\mathcal{J}$ est inversible. Ainsi on obtient l'inclusion voulue :
$$\mathcal{J}\mathcal{K}=\mathcal{J}\mathcal{K}((\mathcal{J}\div(\mathcal{J}+\mathcal{K}))+(\mathcal{K}\div(\mathcal{J}+\mathcal{K})))\subset(\mathcal{K}\cap\mathcal{J})\mathcal{J}+(\mathcal{K}\cap\mathcal{J})\mathcal{K}=(\mathcal{K}\cap\mathcal{J})(\mathcal{J}+\mathcal{K}).$$
- On a $(\mathcal{J}\div(\mathcal{J}+\mathcal{K}))^n(\mathcal{J}+\mathcal{K})^n=\mathcal{J}^n$ et $(\mathcal{K}\div(\mathcal{J}+\mathcal{K}))^n(\mathcal{J}+\mathcal{K})^n=\mathcal{K}^n$. Or, $A=(\mathcal{J}\div(\mathcal{J}+\mathcal{K}))\ +\ (\mathcal{K}\div(\mathcal{J}+\mathcal{K}))$ donc $A=(\mathcal{J}\div(\mathcal{J}+\mathcal{K}))^n+(\mathcal{K}\div(\mathcal{J}+\mathcal{K}))^n$. Ainsi, en multipliant par $(\mathcal{J}+\mathcal{K})^n$, on obtient l'égalité $(\mathcal{J}+\mathcal{K})^n=\mathcal{J}^n+\mathcal{K}^n$.
- On sait que $(\mathcal{J}\cap\mathcal{K})(\mathcal{J}+\mathcal{K})=\mathcal{J}\mathcal{K}$, donc
$$\mathcal{I}(\mathcal{J}\cap\mathcal{K})(\mathcal{J}+\mathcal{K})=\mathcal{I}\mathcal{J}\mathcal{K}\supset(\mathcal{I}\mathcal{J}\cap\mathcal{I}\mathcal{K})(\mathcal{J}+\mathcal{K})$$
et le lemme 11.117 de simplification (par $\mathcal{J}+\mathcal{K}$) donne l'inclusion voulue.
- On a
$$((\mathcal{I}+\mathcal{J})\cap(\mathcal{I}+\mathcal{K}))(\mathcal{J}+\mathcal{K})\subset(\mathcal{I}+\mathcal{K})\mathcal{J}+(\mathcal{I}+\mathcal{J})\mathcal{K}=\mathcal{I}(\mathcal{J}+\mathcal{K})+\mathcal{J}\mathcal{K}=(\mathcal{I}+(\mathcal{J}\cap\mathcal{K}))(\mathcal{J}+\mathcal{K})$$
et le lemme 11.117 de simplification (par $\mathcal{J}+\mathcal{K}$) donne l'inclusion voulue.
- On a $(\mathcal{J}\div(\mathcal{J}+\mathcal{K}))(\mathcal{I}\cap(\mathcal{J}+\mathcal{K}))\subset\mathcal{J}\cap\mathcal{I}$ et $(\mathcal{K}\div(\mathcal{J}+\mathcal{K}))(\mathcal{I}\cap(\mathcal{J}+\mathcal{K}))\subset\mathcal{K}\cap\mathcal{I}$. Or, $(\mathcal{J}\div(\mathcal{J}+\mathcal{K}))\ +\ (\mathcal{K}\div(\mathcal{J}+\mathcal{K}))=A$ donc on obtient l'inclusion voulue $(\mathcal{I}\cap(\mathcal{J}+\mathcal{K}))\subset(\mathcal{J}\cap\mathcal{I})+(\mathcal{K}\cap\mathcal{I})$.
- On a
$$((\mathcal{J}\div\mathcal{I})+(\mathcal{K}\div\mathcal{I})).\mathcal{I}=(\mathcal{J}\div\mathcal{I}).\mathcal{I}+(\mathcal{K}\div\mathcal{I}).\mathcal{I}=\mathcal{J}+\mathcal{K}=((\mathcal{J}+\mathcal{K})\div\mathcal{I}).\mathcal{I}$$
et le lemme 11.117 de simplification (par $\mathcal{I}$) donne l'égalité voulue.
- On a
$$((\mathcal{J}\div\mathcal{I})\cap(\mathcal{K}\div\mathcal{I})).\mathcal{I}\subset\mathcal{J}\cap\mathcal{K}=((\mathcal{J}\cap\mathcal{K})\div\mathcal{I}).\mathcal{I}$$
et le lemme 11.117 de simplification (par $\mathcal{I}$) donne l'inclusion voulue.
- L'égalité $\mathcal{J}\mathcal{K}=(\mathcal{J}+\mathcal{K})(\mathcal{J}\cap\mathcal{K})$ prouve que si $\mathcal{J},\mathcal{K},\mathcal{J}+\mathcal{K}$ sont inversibles, alors $(\mathcal{J}\cap\mathcal{K})$ l'est aussi.
- On a
$$((\mathcal{I}\div\mathcal{J})+(\mathcal{I}\div\mathcal{K})).(\mathcal{J}\cap\mathcal{K})\subset(\mathcal{I}\div\mathcal{J}).\mathcal{J}+(\mathcal{I}\div\mathcal{K}).\mathcal{K}=\mathcal{I}=(\mathcal{I}\div(\mathcal{J}\cap\mathcal{K})).(\mathcal{J}\cap\mathcal{K})$$
et le lemme 11.117 de simplification (par $\mathcal{J}\cap\mathcal{K}$) donne l'inclusion voulue.
- On a
$$((\mathcal{I}\div\mathcal{J})\cap(\mathcal{I}\div\mathcal{K})).(\mathcal{J}+\mathcal{K})\subset(\mathcal{I}\div\mathcal{J}).\mathcal{J}+(\mathcal{I}\div\mathcal{K}).\mathcal{K}=\mathcal{I}=(\mathcal{I}\div(\mathcal{J}+\mathcal{K})).(\mathcal{J}+\mathcal{K})$$
et le lemme 11.117 de simplification (par $\mathcal{J}+\mathcal{K}$) donne l'inclusion voulue.

□

Proposition 11.123 *On note A un anneau commutatif. On considère $\mathcal{I}_1, \ldots, \mathcal{I}_k \subset A$ des idéaux deux à deux comaximaux. Alors on a*

$$\begin{array}{ccccccc} \mathcal{I}_1^{\max(\alpha_1,\beta_1)} & \cdots & \mathcal{I}_k^{\max(\alpha_k,\beta_k)} & = & \mathcal{I}_1^{\alpha_1}\cdots\mathcal{I}_k^{\alpha_k} & \cap & \mathcal{I}_1^{\beta_1}\cdots\mathcal{I}_k^{\beta_k} \\ \mathcal{I}_1^{\min(\alpha_1,\beta_1)} & \cdots & \mathcal{I}_k^{\min(\alpha_k,\beta_k)} & = & \mathcal{I}_1^{\alpha_1}\cdots\mathcal{I}_k^{\alpha_k} & + & \mathcal{I}_1^{\beta_1}\cdots\mathcal{I}_k^{\beta_k}. \end{array}$$

On définit l'application

$$\begin{array}{rccc} \phi: & \mathbb{N}^k & \longrightarrow & \{\text{idéaux de } A\} \\ & \alpha & \longmapsto & \mathcal{I}_1^{\alpha_1}\cdots\mathcal{I}_k^{\alpha_k}. \end{array}$$

*Si, de plus, les idéaux $\mathcal{I}_1, \ldots, \mathcal{I}_k$ sont propres et inversibles, alors ϕ est injective et strictement décroissante : $\phi(\alpha) \subsetneq \phi(\beta) \Longleftrightarrow \alpha > \beta$ pour l'ordre produit (voir définition **??**).*

Démonstration Pour trois idéaux quelconques $\mathcal{I}, \mathcal{J}, \mathcal{K} \subset A$ et $m, n, p \in \mathbb{N}$,
– si $\mathcal{I}$ et $\mathcal{J}$ sont comaximaux, alors $\mathcal{I}^m + \mathcal{J} = A$; $\mathcal{I}\mathcal{J} = \mathcal{I} \cap \mathcal{J}$; $\mathcal{J} + \mathcal{I}\mathcal{K} = \mathcal{J} + \mathcal{K}$;
– si $\mathcal{I}$ et $\mathcal{J}$ sont comaximaux, et $\mathcal{I}$ et $\mathcal{K}$ aussi, alors $\mathcal{I} + \mathcal{J}\mathcal{K} = A$ donc $\mathcal{I} + (\mathcal{J} \cap \mathcal{K}) = A$, et

$$\mathcal{I}^n\mathcal{J} \cap \mathcal{I}^p\mathcal{K} = (\mathcal{I}^n \cap \mathcal{J}) \cap (\mathcal{I}^p \cap \mathcal{K}) = \mathcal{I}^{\max(n,p)} \cap (\mathcal{J} \cap \mathcal{K}) = \mathcal{I}^{\max(n,p)}(\mathcal{J} \cap \mathcal{K})$$

$$\mathcal{I}^n\mathcal{J} + \mathcal{I}^p\mathcal{K} = \mathcal{I}^{\min(n,p)}(\mathcal{I}^{n-\min(n,p)}\mathcal{J} + \mathcal{I}^{p-\min(n,p)}\mathcal{K}) = \mathcal{I}^{\min(n,p)}(\mathcal{J} + \mathcal{K}).$$

Ces dernières lignes prouvent (à l'aide d'une récurrence) les égalités annoncées. Enfin, pour démontrer le caractère injectif de ϕ, on utilise (dans une récurrence) le lemme 11.117 de simplification. □

11.2.3 Généralisation

Définition 11.124 *On note A un anneau commutatif et M, N deux sous-modules d'un même A-module. On définit l'**idéal transporteur** de M dans N par $(N : M) = \{x \in A \mid xM \subset N\}$. L'idéal transporteur $(\{0\} : M)$ est l'**idéal annulateur** de M.*

Si $\mathcal{I}, \mathcal{J}$ sont deux idéaux de l'anneau A, alors $\mathcal{I}, \mathcal{J}$ sont en particulier deux sous-A-modules de A et $(\mathcal{I} : \mathcal{J}) = \{x \in A \mid x\mathcal{J} \subset \mathcal{I}\}$.

> Remarque. Les égalités $(\mathcal{I} : \mathcal{J}) = ((\mathcal{I} \cap \mathcal{J}) : \mathcal{J}) = (\mathcal{I} : (\mathcal{I} + \mathcal{J}))$ sont assez claires. Par ailleurs, le produit $(\mathcal{I} : \mathcal{J}).\mathcal{J}$ est inclus dans $\mathcal{I}$, sans lui être égal en général.

Proposition 11.125 *Si $\mathcal{J}$ est un idéal inversible de A et $\mathcal{I} \subset \mathcal{J}$, alors $(\mathcal{I} : \mathcal{J}) = (\mathcal{I} \div \mathcal{J})$.*

Démonstration On a bien sûr $(\mathcal{I} \div \mathcal{J}) \subset (\mathcal{I} : \mathcal{J})$ car $(\mathcal{I} \div \mathcal{J}).\mathcal{J} = \mathcal{I}$. Par ailleurs, on a aussi $(\mathcal{I} : \mathcal{J}).\mathcal{J} \subset \mathcal{I} = (\mathcal{I} \div \mathcal{J}).\mathcal{J}$ et le lemme 11.117 de simplification (par $\mathcal{J}$) prouve l'inclusion $(\mathcal{I} : \mathcal{J}) \subset (\mathcal{I} \div \mathcal{J})$. □

Corollaire 11.126 *On considère deux idéaux $\mathcal{J}, \mathcal{K}$ d'un anneau commutatif. Si $\mathcal{J} + \mathcal{K}$ est inversible, alors $1 \in (\mathcal{J} : \mathcal{K}) + (\mathcal{K} : \mathcal{J})$.*

Remarque. La définition des anneaux arithmétiques (généralisant les anneaux de Dedekind sans hypothèse d'intégrité, ni de noethérianité) repose uniquement sur cette relation : un anneau commutatif A est dit *arithmétique* lorsque, pour tout couple $(\mathcal{J},\mathcal{K})$ d'idéaux de type fini de A, on a $1 \in (\mathcal{J} : \mathcal{K}) + (\mathcal{K} : \mathcal{J})$ (voir définition **??** et lemme **??**).

Démonstration On a $(\mathcal{J} : \mathcal{K}) = (\mathcal{J} : (\mathcal{J}+\mathcal{K})) = (\mathcal{J} \div (\mathcal{J}+\mathcal{K}))$ et de même $(\mathcal{K} : \mathcal{J}) = (\mathcal{K} : (\mathcal{J}+\mathcal{K})) = (\mathcal{K} \div (\mathcal{J}+\mathcal{K}))$. Mais on sait déjà que $1 \in (\mathcal{J} \div (\mathcal{J}+\mathcal{K})) \ + \ (\mathcal{K} \div (\mathcal{J}+\mathcal{K}))$ (voir lemme 11.120). □

Théorème 11.127 *Si $\mathcal{K}$ et $\mathcal{J}$ sont deux idéaux de A tels que $(\mathcal{K} : \mathcal{J}) + (\mathcal{J} : \mathcal{K}) = A$, alors, en tant que A-modules,*

$$A/\mathcal{K} \times A/\mathcal{J} \ \simeq \ A/(\mathcal{K}+\mathcal{J}) \times A/(\mathcal{K} \cap \mathcal{J}).$$

En particulier, si $\mathcal{K}+\mathcal{J} = A$ alors $A/\mathcal{K} \times A/\mathcal{J} \simeq A/\mathcal{K}\mathcal{J}$.

Démonstration On écrit $1 = a + b$ avec $a \in (\mathcal{J} : \mathcal{K})$ et $b \in (\mathcal{K} : \mathcal{J})$. On considère alors l'application

$$\begin{array}{rccc} \phi : & A/\mathcal{K} \times A/\mathcal{J} & \longrightarrow & A/(\mathcal{K}+\mathcal{J}) \times A/(\mathcal{K} \cap \mathcal{J}) \\ & (x \ , \ y) & \longmapsto & (x+y \ , \ ax - by). \end{array}$$

ϕ est un morphisme de A-modules bien défini, car d'une part (première composante) $\mathcal{K}+\mathcal{J}$ contient $\mathcal{K}$ et $\mathcal{J}$ et d'autre part (seconde composante) $\mathcal{K} \cap \mathcal{J}$ contient $a\mathcal{K}$ et $b\mathcal{J}$. Enfin ϕ est bijectif car d'inverse

$$\begin{array}{rccc} \phi^{-1} : & A/\mathcal{K} \times A/\mathcal{J} & \longleftarrow & A/(\mathcal{K}+\mathcal{J}) \times A/(\mathcal{K} \cap \mathcal{J}) \\ & (bx+y \ , \ ax-y) & \longleftarrow\!\shortmid & (x \ , \ y). \end{array}$$

Cela est aussi un morphisme de A-modules, car d'une part (première composante) $\mathcal{K}$ contient $\mathcal{K} \cap \mathcal{J}$ et $b(\mathcal{K}+\mathcal{J})$ et d'autre part (seconde composante) $\mathcal{J}$ contient $\mathcal{K} \cap \mathcal{J}$ et $a(\mathcal{K}+\mathcal{J})$. □

11.2.4 Inversibilité et idéaux premiers

Proposition 11.128 *Dans un anneau commutatif, un idéal premier inversible est un élément maximal (pour l'inclusion) parmi les idéaux propres inversibles.*

Démonstration On note $\mathfrak{p}$ un idéal premier inversible d'un anneau commutatif A. Pour tout idéal inversible $\mathcal{I}$ contenant $\mathfrak{p}$, on a $(\mathfrak{p} \div \mathcal{I}).\mathcal{I} = \mathfrak{p}$. Comme $\mathfrak{p}$ est premier, il vient $(\mathfrak{p} \div \mathcal{I}) \subset \mathfrak{p}$ ou $\mathcal{I} \subset \mathfrak{p}$, c'est-à-dire respectivement $\mathfrak{p} = \mathcal{I}\mathfrak{p}$ ou $\mathfrak{p} = \mathcal{I}$. Mais $\mathfrak{p}$ étant inversible lui aussi, $\mathfrak{p} = \mathcal{I}\mathfrak{p}$ équivaut à $A = \mathcal{I}$, si bien que l'on a $A = \mathcal{I}$ ou $\mathfrak{p} = \mathcal{I}$. □

Exemple 11.129 *On note p un élément irréductible d'un anneau factoriel A. On sait que p est premier (voir théorème **??**), donc l'idéal premier pA est inversible, et ainsi pA est maximal parmi les idéaux propres inversibles. En conséquence, dans un anneau factoriel, tout idéal propre contenant strictement un idéal engendré par un élément irréductible ne peut être inversible.*

Lemme 11.130 *Dans un anneau commutatif, tout idéal non inversible est inclus dans un élément maximal (pour l'inclusion) parmi les idéaux non inversibles.*

Démonstration On note $\mathcal{I}$ un idéal non inversible. Montrons que l'ensemble des idéaux non inversibles contenant $\mathcal{I}$ est inductif pour l'inclusion : le lemme de Zorn (voir théorème **??**) permet alors de conclure. On note $(\mathcal{J}_i)_i$ une famille totalement ordonnée d'idéaux non inversibles contenant $\mathcal{I}$ et $\mathcal{J} = \cup_i \mathcal{J}_i$. Il est clair que $\mathcal{J}$ contient $\mathcal{I}$. Montrons que $\mathcal{J}$ n'est pas inversible : si $\mathcal{J}$ n'est pas de type fini, alors $\mathcal{J}$ n'est pas inversible (contraposée de la proposition 11.115), et si $\mathcal{J}$ est de type fini alors $\mathcal{J} = \langle j_1, \dots, j_d \rangle$. Or, tout élément j_i appartient à un certain $\mathcal{J}_{n_i}$. Ainsi, il existe un entier $k = \max\{n_1, \dots, n_d\}$ tel que $\mathcal{J} = \cup_{n \leqslant k} \mathcal{J}_n = \mathcal{J}_k$, et donc $\mathcal{J}$ n'est pas inversible. Conclusion : dans tous les cas, $\mathcal{J}$ est un majorant de la famille $(\mathcal{J}_i)_i$ dans l'ensemble des idéaux non inversibles contenant $\mathcal{I}$. On peut donc utiliser le lemme de Zorn. □

Proposition 11.131 *Dans un anneau commutatif, un élément maximal (pour l'inclusion) parmi les idéaux non inversibles est un idéal premier.*

Démonstration Dans un anneau commutatif A, on note $\mathcal{J}$ un élément maximal parmi les idéaux non inversibles et $a \in A \setminus \mathcal{J}$. Montrons que $ab \in \mathcal{J}$ implique $b \in \mathcal{J}$ ou encore $(\mathcal{J} : aA) = \mathcal{J}$. L'idéal $\mathcal{J} + aA$ contient strictement $\mathcal{J}$ donc $\mathcal{J} + aA$ est inversible : on peut donc écrire $\mathcal{J} = (\mathcal{J} \div (\mathcal{J} + aA))(\mathcal{J} + aA)$. Comme $\mathcal{J}$ n'est pas inversible, il en va de même pour $(\mathcal{J} \div (\mathcal{J} + aA))$. Or $\mathcal{J}$ est maximal pour cette propriété, donc $\mathcal{J} = (\mathcal{J} \div (\mathcal{J} + aA)) = (\mathcal{J} : aA)$. □

11.3 Factorisation des idéaux

11.3.1 Unicité d'une factorisation

Voici un résultat donnant une condition d'unicité (si prisée) d'une factorisation.

Théorème 11.132 *Un idéal inversible d'un anneau commutatif admet au plus une factorisation en produit d'idéaux premiers (à permutation près des facteurs).*

Démonstration On note $\mathcal{I}$ un idéal inversible. Considérons deux factorisations de $\mathcal{I}$ en produit d'idéaux premiers $\mathcal{I} = p_1 \cdots p_n = q_1 \cdots q_m$. Quitte à renuméroter les idéaux premiers p_i, on peut supposer p_n minimal (pour l'inclusion) parmi les p_i. Comme p_n est premier, quitte à renuméroter les q_j, on peut supposer que p_n contient l'idéal q_m. Mais q_m est lui-même premier, il contient donc l'un des p_i. Par minimalité de p_n, il vient l'égalité $q_m = p_n$! Enfin, $\mathcal{I}$ est inversible donc tous les idéaux p_i et q_j le sont aussi. Le lemme 11.117 de simplification (par p_n) implique alors $p_1 \cdots p_{n-1} = q_1 \cdots q_{m-1}$. Ainsi, une récurrence permet de prouver le résultat énoncé. □

Exemple 11.133 *Dans l'anneau $A = (\mathbb{Z}/6\mathbb{Z})[X] = \mathbb{Z}[X]/\langle 6 \rangle$, on considère l'élément $P = X^2 - X$. Cet élément P est régulier dans A car P est unitaire. Ce polynôme se factorise en produits d'irréductibles de deux manières :*

$$P = X(X-1) = (X+2)(X+3).$$

Malgré cela, l'idéal $\langle P\rangle$, inversible puisque P est régulier, se factorise en un produit d'idéaux premiers (maximaux) de manière unique :

$$\langle P\rangle = \langle 3, X\rangle \langle 2, X\rangle \langle 3, X-1\rangle \langle 2, X-1\rangle .$$

En effet, $\langle 3, X\rangle \langle 2, X\rangle = \langle X\rangle$ et $\langle 3, X-1\rangle \langle 2, X-1\rangle = \langle X-1\rangle$.
Remarquer que $\langle 3, X-1\rangle \langle 2, X\rangle = \langle X+2\rangle$ et $\langle 3, X\rangle \langle 2, X-1\rangle = \langle X+3\rangle$.

Dans la factorisation éventuelle d'un idéal inversible en produit d'idéaux premiers, tous ces idéaux premiers sont eux-mêmes inversibles (voir proposition 11.116). Par ailleurs, dans l'exemple 11.133, on s'aperçoit que les quatre idéaux premiers sont maximaux. Nous verrons qu'une clé de la construction des anneaux de Dedekind (qui sont des anneaux intègres) est de rendre inversible et maximal tout idéal premier non nul.

11.3.2 Existence d'une factorisation

Dans cette section, on présente quelques résultats d'existence de factorisation d'un idéal $\mathcal{I}$ en produit d'idéaux maximaux inversibles. Chacun de ces résultats est adapté à certaines circonstances que l'on rencontre ici ou là dans la littérature. Il s'agit de factorisations en produit d'idéaux maximaux inversibles : l'inversibilité permet d'assurer unicité des factorisations en vertu du théorème 11.132. Bien que l'on cherche *a priori* des factorisations en produit d'idéaux premiers, on pourrait croire que s'intéresser à des factorisations en produit d'idéaux maximaux est restrictif, mais ce n'est pas réellement le cas en raison de la proposition 11.140.

Lemme 11.134 *Dans un anneau commutatif, si un idéal premier $\mathfrak{p}$ contient un produit d'idéaux $\mathcal{I}_1 \cdots \mathcal{I}_n$, alors l'idéal $\mathfrak{p}$ contient l'un des idéaux $\mathcal{I}_1, \ldots, \mathcal{I}_n$.*

Démonstration Supposons que $\mathfrak{p}$ ne contienne aucun des idéaux $\mathcal{I}_2, \ldots, \mathcal{I}_n$. Montrons alors que $\mathfrak{p}$ contient $\mathcal{I}_1$. Pour tout $k \geqslant 2$, on considère $i_k \in \mathcal{I}_k \setminus \mathfrak{p}$. Alors, pour tout $i_1 \in \mathcal{I}_1$, le produit $i_1 i_2 \cdots i_n$ appartient à $\mathcal{I}_1 \cdots \mathcal{I}_n$ qui est inclus dans $\mathfrak{p}$, donc un élément parmi $i_1, i_2, \ldots, i_n$ appartient à $\mathfrak{p}$ (idéal premier). Cela ne peut être que i_1 par choix de $i_2, \ldots, i_n$. Ainsi tout élément de $\mathcal{I}_1$ appartient à $\mathfrak{p}$. □

Lemme 11.135 *Dans un anneau commutatif A, s'il existe un idéal $\mathcal{J}$ se factorisant en un produit d'idéaux maximaux inversibles $\mathcal{J} = M_1 \cdots M_n$ (certains M_i peuvent être égaux), alors*
- *les idéaux M_i sont exactement les idéaux premiers contenant $\mathcal{J}$;*
- *tout idéal $\mathcal{I}$ contenant $\mathcal{J}$ se factorise en un produit d'idéaux maximaux $\mathcal{I} = \prod_{j\in E} M_j$ où $E \subset \{1, \ldots, n\}$.*

Démonstration
- On note $\mathfrak{p}$ un idéal premier contenant $\mathcal{J} = M_1 \cdots M_n$. Alors $\mathfrak{p}$ contient l'un des facteurs M_i. Or, M_i est un idéal maximal donc $\mathfrak{p} = M_i$.
- Par récurrence sur n, si $n = 1$ alors $\mathcal{I} = A$ ou $\mathcal{I} = M_1$, et, dans ces deux cas, le résultat est évident. Supposons la propriété vraie au rang $n-1$. Supposons $M_1 \cdots M_n \subset \mathcal{I}$. Si $\mathcal{I} = A$, alors il n'y a rien à faire. Sinon, il existe un idéal maximal M contenant $\mathcal{I}$, donc contenant le produit $M_1 \cdots M_n$, donc contenant l'un des M_i (disons M_n quitte à renuméroter les M_i). Or, M_n est maximal donc $M = M_n$. De plus, M_n est inversible

donc $\mathcal{I} = M_n(\mathcal{I} \div M_n)$ et $M_1 \cdots M_{n-1} \subset (\mathcal{I} \div M_n)$ (voir lemme 11.117 de simplification par M_n). Par hypothèse de récurrence, on sait que $(\mathcal{I} \div M_n)$ se factorise en un produit $\prod_{j\in E} M_j$ où $E \subset \{1, \ldots, n-1\}$, donc $\mathcal{I} = \prod_{j\in E'} M_j$ où $E' = E \cup \{n\}$, et la propriété est vraie au rang n.

□

Proposition 11.136 *Dans un anneau commutatif A, on considère un idéal $\mathcal{I}$ ayant les propriétés suivantes :*

- *l'annulateur de $\mathcal{I}$ est nul ;*
- *tout idéal contenant $\mathcal{I}$ est de type fini ($\mathcal{I}$ en particulier) ;*
- *tout idéal maximal contenant $\mathcal{I}$ est inversible.*

Alors l'idéal $\mathcal{I}$ se factorise en un produit d'idéaux maximaux inversibles.

Démonstration Nous allons construire de manière récursive une suite croissante d'idéaux $(\mathcal{I}_n)_{n\in\mathbb{N}}$ telle que, pour tout $n \geqslant 0$, l'idéal $\mathcal{I}$ soit le produit de $\mathcal{I}_n$ et d'un certain nombre d'idéaux maximaux inversibles. La proposition est prouvée si l'un des $\mathcal{I}_n$ est égal à A. Posons $\mathcal{I}_0 = \mathcal{I}$ et considérons $n \geqslant 0$. Si $\mathcal{I}_n = A$, alors on pose $\mathcal{I}_{n+1} = \mathcal{I}_n = A$. Sinon $\mathcal{I}_n$ est inclus dans un idéal maximal M (qui est inversible). Alors on pose $\mathcal{I}_{n+1} = (\mathcal{I}_n \div M)$ de sorte que $\mathcal{I}_n = \mathcal{I}_{n+1}M$. Comme $\mathcal{I}_{n+1}$ contient $\mathcal{I}_n$, l'idéal $\mathcal{I}_{n+1}$ est de type fini et son annulateur est nul. Par ailleurs, le lemme de Nakayama (voir proposition **??**) montre que $\mathcal{I}_{n+1} \neq \mathcal{I}_n$: effectivement, si $\mathcal{I}_{n+1} = \mathcal{I}_n = M\mathcal{I}_{n+1}$ alors $A = M + \mathrm{Ann}(\mathcal{I}_{n+1}) = M$, ce qui est faux. Ainsi la (une) suite croissante $(\mathcal{I}_n)_{n\in\mathbb{N}}$ est construite. On considère l'idéal $\mathcal{J} = \cup_{n\in\mathbb{N}}\mathcal{I}_n$. Cet idéal $\mathcal{J}$ contient $\mathcal{I}$, donc, par hypothèse, $\mathcal{J}$ est de type fini : $\mathcal{J} = \langle j_1, \ldots, j_d\rangle$. Or, tout élément j_i appartient à un certain $\mathcal{I}_{n_i}$. Ainsi, il existe un entier $k = \max\{n_1, \ldots, n_d\}$ tel que $\mathcal{J} = \cup_{n\leqslant k}\mathcal{I}_n = \mathcal{I}_k$. Cela signifie que la suite croissante $(\mathcal{I}_n)_n$ stationne à partir du rang k. Or, $\mathcal{I}_k = \mathcal{I}_{k+1}$ si et seulement si $\mathcal{I}_k = A$. Par conséquent, au rang k, l'idéal $\mathcal{I}$ est le produit d'idéaux maximaux inversibles. □

Exemple 11.137 *Considérons l'anneau produit $\mathbb{Z}^2$. Il est noethérien et ses idéaux sont de la forme $\mathcal{I} \times \mathcal{J}$ où $\mathcal{I}$ et $\mathcal{J}$ sont des idéaux de $\mathbb{Z}$. Les idéaux maximaux de $\mathbb{Z}^2$ sont du type $p\mathbb{Z} \times \mathbb{Z}$ ou $\mathbb{Z} \times p\mathbb{Z}$ où p est un nombre premier. Or, $\langle(p,1)\rangle \cdot \langle(1,p)\rangle = \langle(p,p)\rangle$ et (p,p) est un élément régulier de $\mathbb{Z}^2$, si bien que tout idéal maximal de $\mathbb{Z}^2$ est inversible.*

Par ailleurs, l'annulateur d'un idéal $\mathcal{I} \times \mathcal{J}$ est $\mathrm{Ann}(\mathcal{I}) \times \mathrm{Ann}(\mathcal{J})$. Mais, comme $\mathcal{I}$ et $\mathcal{J}$ sont inclus dans $\mathbb{Z}$ qui est intègre, on a $\mathrm{Ann}(\mathcal{I}) = \langle 0\rangle$ si et seulement si $\mathcal{I} \neq \langle 0\rangle$; il en est bien sûr de même pour $\mathcal{J}$. Conclusion : les idéaux de $\mathbb{Z}^2$ d'annulateur nul sont les idéaux de la forme $\mathcal{I} \times \mathcal{J}$ où $\mathcal{I}$ et $\mathcal{J}$ sont des idéaux non nuls de $\mathbb{Z}$. Pour ces idéaux $\mathcal{I} \times \mathcal{J}$ d'annulateur nul, la proposition 11.136 s'applique : tout idéal de $\mathbb{Z}^2$ d'annulateur nul se factorise (de manière unique) en produit d'idéaux maximaux (inversibles).

D'autre part, un idéal d'annulateur non nul se factorise en produit d'idéaux premiers. En effet, $\mathcal{I}$ (inclus dans $\mathbb{Z}$) se factorise en produit d'idéaux premiers $\mathfrak{p}_i \subset \mathbb{Z}$, donc $\mathcal{I} \times \langle 0\rangle$ se factorise à l'aide des idéaux premiers $\mathfrak{p}_i \times \mathbb{Z}$ et $\mathbb{Z} \times \langle 0\rangle$ dans $\mathbb{Z}^2$. Il en est de même pour les idéaux du type $\langle 0\rangle \times \mathcal{J}$. Cela étant, cette factorisation n'est pas unique du fait que $(\mathbb{Z} \times \langle 0\rangle)^2 = \mathbb{Z} \times \langle 0\rangle$ ($\mathbb{Z} \times \langle 0\rangle$ est donc un idéal premier non inversible).

Proposition 11.138 *On considère un idéal $\mathcal{I}$ d'un anneau commutatif A. Si tous les idéaux premiers contenant $\mathcal{I}$ sont inversibles, alors tout idéal (premier ou pas) contenant $\mathcal{I}$ est inversible et $\mathcal{I}$ se factorise en produit d'idéaux maximaux inversibles.*

Démonstration En utilisant la proposition 11.131, il est clair que tout idéal contenant $\mathcal{I}$ est inversible (donc de type fini). Ainsi $\mathcal{I}$ contient un élément régulier, donc $\mathrm{Ann}(\mathcal{I}) = \langle 0 \rangle$. La proposition 11.136 montre que $\mathcal{I}$ se factorise en produit d'idéaux maximaux inversibles. □

11.3.3 Conséquences de la factorisation

Lemme 11.139 *Dans un anneau commutatif A, on considère deux idéaux $\mathcal{I}$ et $\mathfrak{p}$ et un élément $a \in A \setminus \mathfrak{p}$ tels que $\mathcal{I} \subset \mathfrak{p} \subset \mathcal{I} + aA$. Si $\mathfrak{p}$ est premier, alors $\mathfrak{p} = \mathcal{I} + a\mathfrak{p}$.*

Démonstration On considère $x \in \mathfrak{p}$. On écrit $x = i + ay$ avec $i \in \mathcal{I}$ et $y \in A$. Comme $\mathcal{I} \subset \mathfrak{p}$, il vient $ay = x - i \in \mathfrak{p}$. Or, $a \notin \mathfrak{p}$ donc $y \in \mathfrak{p}$, d'où $x \in \mathcal{I} + a\mathfrak{p}$. Conclusion : $\mathfrak{p} \subset \mathcal{I} + a\mathfrak{p}$ et l'inclusion inverse est évidente. □

> Rappel du théorème **??** Pour tout idéal $\mathcal{I}$ d'un anneau commutatif A, les idéaux contenant $\mathcal{I}$ sont en correspondance biunivoque avec les idéaux de $A/\mathcal{I}$.

Proposition 11.140 *On note A un anneau commutatif et un idéal inversible $\mathfrak{p} \subset A$ tels que tout idéal contenant $\mathfrak{p}$ se factorise en produit d'idéaux premiers de A. Si $\mathfrak{p}$ est un idéal premier, alors $\mathfrak{p}$ est maximal.*

Démonstration Prouver que $\mathfrak{p}$ est maximal revient à montrer que $\mathfrak{p} + aA = A$ pour tout $a \in A \setminus \mathfrak{p}$. On considère donc $a \in A \setminus \mathfrak{p}$. Par hypothèse, les idéaux $\mathfrak{p} + aA$ et $\mathfrak{p} + a^2A$ se factorisent en produits d'idéaux premiers : $\mathfrak{p} + aA = r_1 \cdots r_m$ et $\mathfrak{p} + a^2A = q_1 \cdots q_n$ où les idéaux premiers r_j et q_i contiennent $\mathfrak{p}$. On peut donc considérer les images de ces factorisations dans $A/\mathfrak{p}$:

$$\overline{q_1} \cdots \overline{q_n} = \left\langle \overline{a^2} \right\rangle = \langle \overline{a} \rangle^2 = \overline{r_1}^2 \cdots \overline{r_m}^2.$$

Or a est régulier modulo $\mathfrak{p}$, donc $\langle \overline{a} \rangle^2$ est un idéal inversible dans $A/\mathfrak{p}$. Par unicité de la factorisation en idéaux premiers des idéaux inversibles (voir théorème 11.132), les idéaux premiers q_i et r_j s'identifient ($n = 2m$), et on obtient $\mathfrak{p} + a^2A = (\mathfrak{p} + aA)^2$ dans A ! Ainsi $\mathfrak{p} \subset \mathfrak{p}^2 + a\mathfrak{p} + a^2A$ et, comme $\mathfrak{p}$ est premier et $a \notin \mathfrak{p}$, il vient $\mathfrak{p} = \mathfrak{p}^2 + a\mathfrak{p} + a^2\mathfrak{p}$ (voir lemme 11.139). On arrive à $\mathfrak{p} = \mathfrak{p}^2 + a\mathfrak{p}$, puis $A = \mathfrak{p} + aA$ car $\mathfrak{p}$ est inversible. Conclusion : $\mathfrak{p}$ est maximal. □

Nous donnons ci-après la définition d'un anneau de dimension de Krull inférieure ou égale à 1. On définit la dimension de Krull de manière plus générale pour tout anneau commutatif, mais nous nous contentons ici d'étudier certains anneaux de dimension inférieure ou égale à 1.

Définition 11.141 *Un anneau commutatif A est de* ***dimension de Krull inférieure ou égale à*** 1 *lorsque chacun de ses idéaux premiers est un élément minimal ou maximal (pour l'inclusion) parmi les idéaux premiers de A. En particulier, un anneau intègre (qui n'est pas un corps) est de* ***dimension de Krull égale à*** 1 *lorsque tous ses idéaux premiers non nuls sont maximaux.*

Par exemple, l'anneau $\mathbb{Z}$ des entiers relatifs est un anneau intègre de dimension 1.

Théorème 11.142 *Un anneau A intègre, dans lequel tout idéal se factorise en produit d'idéaux premiers, est de dimension de Krull inférieure ou égale à* 1.

Démonstration Tout idéal premier $\mathfrak{p}$ non minimal (c'est-à-dire non nul) contient un élément régulier a. Par hypothèse, l'idéal aA se factorise en produit d'idéaux premiers $\mathfrak{q}_1 \cdots \mathfrak{q}_r$, qui sont inversibles (car aA est inversible). Or, dans A, tous les idéaux premiers inversibles sont maximaux (voir proposition 11.140). Mais $\mathfrak{p}$ étant premier et contenant a, il contient l'un de ces idéaux maximaux $\mathfrak{q}_i$, ce qui prouve la maximalité de $\mathfrak{p}$. □

Ce résultat montre que vouloir construire un anneau intègre, dans lequel la généralisation du théorème 11.108 fondamental de l'arithmétique est vérifiée avec des idéaux, force les idéaux premiers non nuls de cet anneau à être maximaux. Cela est une contrainte importante et marque une différence claire avec les anneaux factoriels (comme dans l'anneau des polynômes $\mathbb{Z}[X_1, \ldots, X_n]$ par exemple) dans lesquels un élément premier (irréductible) n'est pas nécessairement extrémal (qui engendre un idéal maximal).

Lemme 11.143 *On considère deux éléments réguliers x, y d'un anneau commutatif A. On suppose que*

$$\langle x \rangle = \mathfrak{q}_1^{f_1} \cdots \mathfrak{q}_s^{f_s} \qquad et \qquad \langle y \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

où les idéaux $\mathfrak{p}_i$ et $\mathfrak{q}_j$ sont maximaux. Si x/y (appartenant à l'anneau total des fractions de A) est entier sur A, alors x/y appartient à A.

Démonstration Comme x/y est entier sur A (voir définition 11.110), on écrit $(x/y)^n + a_{n-1}(x/y)^{n-1} + \cdots + a_1(x/y) + a_0 = 0$. En multipliant par y^n, il vient

$$-x^n = a_{n-1}x^{n-1}y + \cdots + a_1 x y^{n-1} + a_0 y^n.$$

Comme $x^n \in yA$, il s'ensuit $x^n \in \mathfrak{p}_1$, donc $x \in \mathfrak{p}_1$. Or, $\langle x \rangle = \mathfrak{q}_1^{f_1} \cdots \mathfrak{q}_s^{f_s}$ donc $\mathfrak{p}_1$ contient l'un des $\mathfrak{q}_i$, disons $\mathfrak{q}_1$ quitte à renuméroter les $\mathfrak{q}_i$. Mais $\mathfrak{q}_1$ est maximal si bien que $\mathfrak{p}_1$ est égal à $\mathfrak{q}_1$. Par le même raisonnement, chaque idéal $\mathfrak{p}_i$ se retrouve parmi les idéaux q_j, et ainsi

$$\langle x \rangle = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_r^{f_r} \mathfrak{q}_{r+1}^{f_{r+1}} \cdots \mathfrak{q}_s^{f_s}.$$

Montrons que $e_i \leqslant f_i$ pour tout $i \leqslant r$: cela implique

$$\langle x \rangle = \langle y \rangle \, \mathfrak{p}_1^{f_1 - e_1} \cdots \mathfrak{p}_r^{f_r - e_r} \mathfrak{q}_{r+1}^{f_{r+1}} \cdots \mathfrak{q}_s^{f_s} \subset \langle y \rangle \,,$$

et donc $x/y \in A$ comme cela a été annoncé. Pour $0 \leqslant j \leqslant n-1$, on a $x^j y^{n-j} \in \mathfrak{p}_1^{jf_1 + (n-j)e_1}$. Lorsque j varie entre 0 et $n-1$, l'exposant $jf_1 + (n-j)e_1$ varie entre ne_1 et $(n-1)f_1 + e_1$. Posons $m = \min(ne_1, (n-1)f_1 + e_1)$. On a alors

$$-x^n = a_{n-1}x^{n-1}y + \cdots + a_1 x y^{n-1} + a_0 y^n \quad \in \mathfrak{p}_1^m.$$

Or, $\mathfrak{p}_1^{nf_1} \cdots \mathfrak{p}_r^{nf_r} \mathfrak{q}_{r+1}^{nf_{r+1}} \cdots \mathfrak{q}_s^{nf_s} = \langle x^n \rangle \subset \mathfrak{p}_1^m$ si bien que $m \leqslant nf_1$ (voir proposition 11.123 ; les idéaux $\mathfrak{p}_i$ et $\mathfrak{q}_j$ sont inversibles car x est régulier). Enfin, si $m = ne_1$ alors $e_1 \leqslant f_1$, et si $m = (n-1)f_1 + e_1$ alors $e_1 \leqslant f_1$ également ; donc, dans tous les cas, $e_1 \leqslant f_1$! Le même raisonnement montre que $e_i \leqslant f_i$ pour tous les indices $i \leqslant r$. □

Définition 11.144 *On note A un anneau intègre, de corps des fractions $\mathcal{K}$. On dit que A est* ***intégralement clos*** *lorsque tout élément de $\mathcal{K}$ entier sur A appartient à A.*

Théorème 11.145 *Un anneau A intègre, dans lequel tout idéal monogène non nul se factorise en produit d'idéaux maximaux, est intégralement clos.*

Démonstration C'est une conséquence directe du lemme 11.143. □

Ici, contrairement à la dimension de Krull (voir théorème 11.142), nous retrouvons un résultat vérifié également par les anneaux factoriels : un anneau factoriel est (intègre et) intégralement clos. En effet, si un élément du corps des fractions x/y (avec $\mathrm{pgcd}(x,y)=1$) est entier sur l'anneau factoriel, alors (en reprenant les notations du début de la preuve du lemme 11.143) il vient

$$-x^n = a_{n-1}x^{n-1}y + \cdots + a_1 x y^{n-1} + a_0 y^n \quad \in \langle y \rangle\,,$$

si bien que y divise $\mathrm{pgcd}(x^n, y^n) = \mathrm{pgcd}(x,y)^n = 1$; donc y est inversible et x/y appartient à l'anneau factoriel.

11.4 Anneaux de Dedekind

Définition 11.146 (due à Dedekind) *On note A un anneau commutatif. On dit que A est un **anneau de Dedekind** lorsque tout idéal de A est nul ou inversible.*

Par exemple, un anneau principal est un anneau de Dedekind, mais un anneau factoriel non principal ne l'est pas.

Proposition 11.147 *Un anneau de Dedekind est intègre et de dimension de Krull inférieure ou égale à 1.*

Démonstration Tout élément non nul engendre un idéal inversible, donc tout élément non nul est régulier : l'anneau est bien intègre. Enfin, tout idéal premier (en particulier tout idéal maximal) non nul est inversible, donc tout idéal premier non nul est maximal en raison de la proposition 11.128. C'est pourquoi la dimension de Krull est au plus 1. □

Théorème 11.148 (exerc.8 §2 ch.7 *Diviseurs* de [Bou]) *Un anneau commutatif A est un anneau de Dedekind si et seulement si tout idéal premier de A est nul ou inversible.*

Démonstration L'inversibilité des idéaux premiers non nuls est une condition évidemment nécessaire, mais elle est suffisante en raison de la proposition 11.131 : en effet, considérons un élément maximal parmi les idéaux non inversibles de A. Alors cet élément est un idéal premier, et par suite nul puisque non inversible. Conclusion : le seul idéal non inversible de A est $\langle 0 \rangle$ et l'anneau A est de Dedekind. □

Théorème 11.149 (dû à Matusita, cf. exerc.9 §2 ch.7 *Diviseurs* de [Bou]) *On note A un anneau intègre. Il y a équivalence entre les assertions suivantes.*

1. *L'anneau A est un anneau de Dedekind.*
2. *Tout idéal non nul de A se factorise en un produit unique (à l'ordre près) d'idéaux maximaux.*
3. *Tout idéal de A se factorise en produit d'idéaux premiers.*

Démonstration

- Montrons que l'assertion 1 implique l'assertion 2 : l'existence d'une factorisation vient de la proposition 11.136. L'unicité de la factorisation vient du théorème 11.132.
- Il est évident que l'assertion 2 implique l'assertion 3 (l'idéal nul est premier).

– Montrons que l'assertion 3 implique l'assertion 1 : si l'anneau est un corps, c'est évident. Sinon, comme l'anneau est intègre, le théorème 11.142 montre que la dimension de Krull est au plus 1, donc tout idéal premier non nul est maximal. Ainsi tout idéal $\mathcal{I}$ non nul se factorise en produit d'idéaux maximaux. Pour montrer que $\mathcal{I}$ est inversible, il suffit de prouver l'inversibilité des idéaux maximaux. On note M un idéal maximal : il contient un élément a non nul. Écrivons une factorisation $aA = M_1 \cdots M_n$ où les M_i sont maximaux. Comme l'idéal maximal M contient a (donc le produit $M_1 \cdots M_n$), par maximalité M est égal à l'un des M_i. Enfin, a est régulier (A est intègre) ; il s'ensuit que tous les M_i sont inversibles, M en particulier.

□

Remarque. Dans ce théorème, l'hypothèse d'intégrité est importante car on trouve facilement des anneaux commutatifs non intègres dans lesquels au moins l'une des deux assertions suivantes est juste.
– Tout idéal non nul se factorise de manière unique en produit d'idéaux maximaux.
– Tout idéal se factorise en produit d'idéaux premiers.
En effet, dans l'anneau $\mathbb{Z}/4\mathbb{Z}$ par exemple, les idéaux stricts sont $\langle 2\rangle$ (qui est maximal) et $\langle 0\rangle = \langle 2\rangle^2$.

Signalons rapidement le théorème amusant suivant. Nous l'admettons sans démonstration (il ne sera pas utilisé par la suite). Il montre que les idéaux d'un anneau de Dedekind ne sont pas principaux, certes, mais qu'ils sont engendrés par un couple d'éléments.

Théorème 11.150 ((« Un et demi »).) *On note $\mathcal{I}$ un idéal inversible d'un anneau commutatif de dimension de Krull inférieure ou égale 1. Alors, pour tout élément régulier $x \in \mathcal{I}$, il existe $y \in \mathcal{I}$ tel que $\mathcal{I} = \langle x, y\rangle$.*

Le nom de ce théorème provient probablement du fait que, pour construire un système générateur d'un idéal d'un anneau de Dedekind, un premier élément (non nul) peut être choisi aléatoirement : celui-ci compte « moralement pour un demi-générateur » puisqu'on a tout le loisir de le choisir comme on le souhaite ; puis un second élément complète le premier en un système générateur de l'idéal : ce second élément (dépendant du premier) compte « moralement pour une part entière ».

11.5 Caractères noethérien et intégralement clos des anneaux de Dedekind

11.5.1 Caractère noethérien

Proposition 11.151 *Un anneau de Dedekind est noethérien.*

Démonstration Dans un anneau de Dedekind, tout idéal est nul ou inversible, donc tout idéal est de type fini et l'anneau est noethérien. □

Tout comme le lemme de Nakayama (voir proposition **??**), le résultat suivant est un grand classique de l'algèbre commutative.

Théorème 11.152 *Pour tout idéal strict $\mathcal{J}$ d'un anneau noethérien, il existe un nombre fini d'idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ tels que $\prod_{i=1}^{s} \mathfrak{p}_i \subset \mathcal{J} \subset \bigcap_{i=1}^{s} \mathfrak{p}_i$. En particulier, il existe un nombre fini non nul d'éléments minimaux (pour l'inclusion) parmi les idéaux premiers contenant $\mathcal{J}$.*

Remarque. De manière générale, pour tout idéal $\mathcal{J}$ d'un anneau $\mathcal{A}$, on pose $\sqrt{\mathcal{J}} = \{x \in \mathcal{A} \mid \exists n \in \mathbb{N},\ x^n \in \mathcal{J}\}$. En reprenant les hypothèses et les notations du théorème 11.152, on obtient immédiatement que $\sqrt{\mathcal{J}} = \bigcap_{i=1}^{s} \mathfrak{p}_i$. En effet, si $x \in \sqrt{\mathcal{J}}$ alors il existe $n \in \mathbb{N}$ tel que $x^n \in \mathcal{J} \subset \bigcap_{i=1}^{s} \mathfrak{p}_i$, donc $x^n \in \mathfrak{p}_i$ pour tout i. Or $\mathfrak{p}_i$ est premier donc $x \in \mathfrak{p}_i$ pour tout i, ou encore $x \in \bigcap_{i=1}^{s} \mathfrak{p}_i$. Réciproquement, si $x \in \bigcap_{i=1}^{s} \mathfrak{p}_i$ alors $x^s \in \prod_{i=1}^{s} \mathfrak{p}_i \subset \mathcal{J}$, et donc $x \in \sqrt{\mathcal{J}}$.
De plus, en raison du lemme 11.134, la décomposition $\sqrt{\mathcal{J}} = \bigcap_{i=1}^{s} \mathfrak{p}_i$ est unique (à l'ordre près des idéaux $\mathfrak{p}_i$) lorsque les idéaux $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ sont les idéaux premiers minimaux contenant $\mathcal{J}$.

Démonstration On note $\mathcal{J}$ un idéal de l'anneau noethérien. Considérons des idéaux $\mathcal{I}_1, \ldots, \mathcal{I}_n$ contenant $\mathcal{J}$ tels que $\prod_{i=1}^{n} \mathcal{I}_i \subset \mathcal{J} \subset \bigcap_{i=1}^{n} \mathcal{I}_i$: cela est toujours possible en prenant $n = 1$ et $\mathcal{I}_1 = \mathcal{J}$. Si l'un des $\mathcal{I}_k$ n'est pas premier, alors il existe $x, y \notin \mathcal{I}_k$ tels que $xy \in \mathcal{I}_k$; autrement dit, $(\mathcal{I}_k + \langle x \rangle)(\mathcal{I}_k + \langle y \rangle) \subset \mathcal{I}_k$. Dans les inclusions $\prod_{i=1}^{n} \mathcal{I}_i \subset \mathcal{J} \subset \bigcap_{i=1}^{n} \mathcal{I}_i$, on remplace alors $\mathcal{I}_k$ par les idéaux $(\mathcal{I}_k + \langle x \rangle)$ et $(\mathcal{I}_k + \langle y \rangle)$, puis on itère le processus. Les nouveaux idéaux contiennent strictement $\mathcal{I}_k$, donc $\mathcal{J}$. L'anneau étant noethérien, le processus s'arrête forcément (attention tout de même : ici on ne construit pas une suite strictement croissante d'idéaux, mais un arbre binaire strictement croissant). La seule condition d'arrêt étant la primalité de tous les idéaux $\mathcal{I}_k$, nous obtenons la première partie du résultat annoncé. Par ailleurs, un idéal premier contenant $\mathcal{J}$ contient le produit des idéaux $\mathcal{I}_k$, donc contient l'un des $\mathcal{I}_k$. Comme les idéaux $\mathcal{I}_k$ sont eux-mêmes premiers et en nombre fini, on en déduit l'existence d'un nombre fini et non nul d'éléments minimaux dans l'ensemble des idéaux premiers contenant $\mathcal{J}$. □

Corollaire 11.153 *On note $\mathcal{J}$ un idéal strict d'un anneau noethérien et $\mathfrak{p}$ un élément minimal (pour l'inclusion) parmi les idéaux premiers contenant $\mathcal{J}$. Alors $\mathcal{J} \subsetneq (\mathcal{J} : \mathfrak{p})$.*

Démonstration D'après le théorème 11.152, l'idéal $\mathcal{J}$ contient un produit d'idéaux premiers, contenant eux-mêmes $\mathcal{J}$. Posons

$$n = \min\{k \in \mathbb{N}^* \mid \text{il existe des idéaux premiers } \mathfrak{p}_1, \ldots, \mathfrak{p}_k \text{ contenant } \mathcal{J} \text{ et } \mathfrak{p}_1 \cdots \mathfrak{p}_k \subset \mathcal{J}\}.$$

On a donc $p_1 \cdots p_n \subset \mathcal{J}$ où les idéaux p_i sont premiers et contiennent $\mathcal{J}$. Or, l'idéal premier $\mathfrak{p}$ contient aussi $\mathcal{J}$, donc contient l'un des p_i, disons p_n quitte à renuméroter les p_i. On a donc $\mathcal{J} \subset p_n \subset \mathfrak{p}$. Mais p_n est premier et $\mathfrak{p}$ est minimal parmi les idéaux premiers contenant $\mathcal{J}$, si bien que $p_n = \mathfrak{p}$ et ainsi $p_1 \cdots p_{n-1}\mathfrak{p} \subset \mathcal{J}$. On a donc $p_1 \cdots p_{n-1}$ inclus dans $(\mathcal{J} : \mathfrak{p})$, mais pas dans $\mathcal{J}$ par minimalité de n. □

Corollaire 11.154 *On note A un anneau noethérien, intègre, de corps des fractions $\mathcal{K} \neq A$ et de dimension de Krull égale à 1. Alors, pour tout idéal premier M non nul de A, le A-module $M' = \{x \in \mathcal{K} \mid xM \subset A\}$ contient strictement A.*

Démonstration Le fait que M' contient A est clair. Trouvons un élément de $M' \setminus A$. On note x un élément non nul de M. Alors M est un idéal minimal parmi les idéaux premiers contenant x car A est intègre et de dimension de Krull égale à 1. On applique alors le corollaire 11.153 à $\mathcal{J} = xA$ et $\mathfrak{p} = M$ pour obtenir $b \in (xA : M) \setminus xA$. On a alors $x^{-1}b \in M' \setminus A$. □

11.5.2 Caractère intégralement clos

Proposition 11.155 *Un anneau de Dedekind est intégralement clos.*

Démonstration Un anneau de Dedekind est intègre, et tous ses idéaux non nuls se factorisent en produit d'idéaux maximaux (voir théorème 11.149). Le théorème 11.145 permet de conclure. □

Lemme 11.156 *On note A un anneau intégralement clos, x un élément du corps des fractions de A. S'il existe un idéal non nul $\mathcal{I} \subset A$ de type fini tel que $x\mathcal{I} \subset \mathcal{I}$, alors x appartient à A.*

Démonstration Considérons un système générateur fini $\{v_1, \ldots, v_n\}$ de $\mathcal{I}$. Comme $x\mathcal{I} \subset \mathcal{I}$, il existe une matrice carrée $M = (m_{ij})_{1 \leqslant i,j \leqslant n}$ à coefficients dans A telle que $xv_i = \sum_{j=1}^{n} m_{ij} v_j$. Notons V le vecteur colonne $(v_1, \ldots, v_n)$, les égalités $xv_i = \sum_{j=1}^{n} m_{ij} v_j$ s'écrivent alors $(x \operatorname{Id}_n - M).V = 0$. En multipliant par ${}^{tc}(x \operatorname{Id}_n - M)$ la transposée de la comatrice de $x \operatorname{Id}_n - M$, il vient (*determinant trick*)

$$0 = {}^{tc}(x \operatorname{Id}_n - M).(x \operatorname{Id}_n - M).V = \det(x \operatorname{Id}_n - M).V.$$

Cela signifie que $\det(x \operatorname{Id}_n - M)$ annule tous les v_i. Or il existe au moins un v_i régulier ($\mathcal{I}$ n'est pas l'idéal nul), donc $\det(x \operatorname{Id}_n - M) = 0$, et x est racine du polynôme caractéristique de M (à coefficients dans A). Comme A est intégralement clos, x appartient à A. □

> Remarque. On pourra comparer cette preuve et celle du lemme de Nakayama (voir proposition **??**) pour voir qu'elles reposent toutes deux essentiellement sur ce fameux *determinant trick*.

Théorème 11.157 *On note A un anneau noethérien intègre (pas un corps). Les assertions suivantes sont équivalentes.*

1. *L'anneau A est un anneau de Dedekind.*
2. *(due à Noether). L'anneau A est intégralement clos et de dimension de Krull égale à 1.*
3. *Tous les idéaux maximaux de A sont inversibles.*

> Remarque. Souvent, les auteurs prennent l'assertion 2 pour définir les anneaux de Dedekind. Il est vrai que l'on peut construire des anneaux réalisant ces hypothèses (voir exemple 11.159), mais il est clair que ces hypothèses ne sont absolument pas intuitives face au problème initial de généralisation du théorème 11.108 fondamental de l'arithmétique, d'où, probablement, les difficultés rencontrées à ce sujet par de grands mathématiciens du XIX$^{\text{e}}$ siècle !
>
> L'assertion 3 est le cœur de certains algorithmes calculant des fermetures intégrales.

Démonstration

- L'assertion 1 implique l'assertion 2 : cela est déjà connu (voir propositions 11.147 et 11.155).

– Montrons que l'assertion 2 implique l'assertion 3 : on note M un idéal maximal (non nul) de A. Dans le corps des fractions de A, noté $\mathcal{K}$, considérons le A-module $M' = \{x \in \mathcal{K} \mid xM \subset A\}$. On a alors $M'M \subset A \subset M'$, et en particulier $M'M$ est un idéal de A. Mais, en multipliant par M, il vient $M'M^2 \subset M \subset M'M$, d'où finalement $M \subset M'M \subset A$. Par ailleurs, il existe $y \in M' \setminus A$ (voir corollaire 11.154). Comme y n'appartient pas à A, la contraposée du lemme 11.156 appliquée à l'idéal M (de type fini) montre que $yM \not\subset M$. *A fortiori*, on a $M'M \neq M$, si bien que $M'M = A$ et M est inversible (voir proposition 11.115).
– Montrons que l'assertion 3 implique l'assertion 1 : on note $\mathcal{I}$ un idéal non nul de A. La proposition 11.136 montre l'existence d'une factorisation de $\mathcal{I}$ en produit d'idéaux maximaux inversibles, donc $\mathcal{I}$ est inversible.

□

Exemple 11.158 *Les anneaux $\mathbb{Z}[i\sqrt{3}]$ et $\mathbb{Z}[\sqrt{5}]$ ne sont pas intégralement clos, donc ce ne sont pas des anneaux de Dedekind.*

Exemple 11.159 *On note $\mathcal{K}$ une extension algébrique finie de $\mathbb{Q}$ et A la fermeture intégrale de $\mathcal{K}$ sur $\mathbb{Z}$ (voir définition 11.111). Alors A est un anneau de Dedekind. Citons à titre d'exemples : $\mathbb{Z}[\xi]$ où ξ est une racine n-ième de l'unité, $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, etc.*

Utilisons le théorème 11.157. Par construction, A est intégralement clos et noethérien (admis). Montrons que tout idéal premier non nul $\mathfrak{p}$ de A est maximal (c'est-à-dire la dimension de Krull de A est égale à 1). On considère $x \in \mathfrak{p} \setminus \{0\}$. Il existe un polynôme P à coefficients dans $\mathbb{Z}$ s'annulant en x. Comme $x \neq 0$, on peut supposer $P(0) \neq 0$. Or $P(0)$ appartient à xA, donc $P(0) \in \mathfrak{p} \cap \mathbb{Z}$. Comme $\mathfrak{p}$ est un idéal premier et $P(0) \neq 0$, il s'ensuit que $\mathfrak{p} \cap \mathbb{Z}$ est un idéal non nul et premier (car $\mathfrak{p}$ premier dans A) : notons p le nombre premier engendrant $\mathfrak{p} \cap \mathbb{Z}$. Étant donné que tout élément de A est entier sur $\mathbb{Z}$, l'anneau intègre $A/\mathfrak{p}$ est algébrique sur le corps $\mathbb{Z}/p\mathbb{Z}$, donc $A/\mathfrak{p}$ est un corps et $\mathfrak{p}$ est maximal.

11.6 Critères « locaux » en terrain intègre noethérien

> Rappel de la proposition **??** Pour tout idéal premier $\mathfrak{p}$ d'un anneau commutatif A, on définit l'anneau local $A_\mathfrak{p}$ comme étant le localisé de A en la partie multiplicative $A \setminus \mathfrak{p}$. Si A est intègre alors A s'injecte canoniquement dans $A_\mathfrak{p}$, qui lui-même s'injecte canoniquement dans le corps des fractions de A.
>
> Rappel de la proposition **??**. Un anneau A intègre est l'intersection de tous ses localisés A_M (inclus dans le corps des fractions de A) en ses idéaux maximaux M.
>
> Rappel du théorème **??** Si l'anneau A est noethérien, alors $A_\mathfrak{p}$ l'est aussi.

Les résultats suivants sont généralisables aux anneaux commutatifs non intègres : la version générale du théorème 11.162 est un résultat important de l'algèbre commutative. Cela étant, le cadre des anneaux intègres, plus simple, nous sera suffisant.

Lemme 11.160 *On considère l'anneau localisé $A_\mathfrak{p}$ d'un anneau intègre A dont $\mathfrak{p}$ est un idéal premier. Pour tout idéal premier $\mathfrak{q}$ contenu dans $\mathfrak{p}$, l'idéal $\mathfrak{q}A_\mathfrak{p}$ est un idéal premier de $A_\mathfrak{p}$ et on a $(\mathfrak{q}A_\mathfrak{p}) \cap A = \mathfrak{q}$.*

Démonstration L'inclusion $\mathfrak{q} \subset (\mathfrak{q}A_\mathfrak{p}) \cap A$ est claire. Réciproquement, si $x \in (\mathfrak{q}A_\mathfrak{p}) \cap A$, alors $x = q/b \in \mathfrak{q}A_\mathfrak{p}$ avec $q \in \mathfrak{q}$ et $b \in A \setminus \mathfrak{p}$. Ainsi $bx \in \mathfrak{q}$ mais, comme $\mathfrak{q}$ est premier et

$b \notin \mathfrak{p} \supset \mathfrak{q}$, on a $x \in \mathfrak{q}$. Ainsi $(\mathfrak{q}A_\mathfrak{p}) \cap A = \mathfrak{q}$. Montrons maintenant que $\mathfrak{q}A_\mathfrak{p}$ est premier : on note $a/b, c/d \in A_\mathfrak{p}$ tels que $(a/b)(c/d) \in \mathfrak{q}A_\mathfrak{p}$. Alors $ac = bd(a/b)(c/d) \in \mathfrak{q}A_\mathfrak{p}$. Or, $ac \in A$ donc $ac \in (\mathfrak{q}A_\mathfrak{p}) \cap A = \mathfrak{q}$, donc $a \in \mathfrak{q}$ ou $c \in \mathfrak{q}$, donc $a/b \in \mathfrak{q}A_\mathfrak{p}$ ou $c/d \in \mathfrak{q}A_\mathfrak{p}$. □

Lemme 11.161 *On considère l'anneau localisé $A_\mathfrak{p}$ d'un anneau intègre A dont $\mathfrak{p}$ est un idéal premier. Pour tout idéal premier $\mathfrak{q}'$ de $A_\mathfrak{p}$, l'idéal $\mathfrak{q}' \cap A$ est un idéal premier de A et on a $(\mathfrak{q}' \cap A)A_\mathfrak{p} = \mathfrak{q}'$.*

Démonstration On considère $x, y \in A$ tels que $xy \in \mathfrak{q}' \cap A$. Comme $\mathfrak{q}'$ est premier, il vient $x \in \mathfrak{q}'$ ou $y \in \mathfrak{q}'$, et donc $x \in \mathfrak{q}' \cap A$ ou $y \in \mathfrak{q}' \cap A$. Ainsi l'idéal $\mathfrak{q}' \cap A$ est un idéal premier de A. Par ailleurs, l'inclusion $(\mathfrak{q}' \cap A)A_\mathfrak{p} \subset \mathfrak{q}'$ est claire. Réciproquement, on note $a/b \in \mathfrak{q}'$. Alors $a = b(a/b) \in \mathfrak{q}' \cap A$, donc $a/b \in (\mathfrak{q}' \cap A)A_\mathfrak{p}$. Cela montre l'inclusion $\mathfrak{q}' \subset (\mathfrak{q}' \cap A)A_\mathfrak{p}$. □

Théorème 11.162 *On considère l'anneau localisé $A_\mathfrak{p}$ d'un anneau intègre A dont $\mathfrak{p}$ est un idéal premier. Il existe une bijection (strictement croissante) entre les idéaux premiers de l'anneau localisé $A_\mathfrak{p}$ et les idéaux premiers de A contenus dans $\mathfrak{p}$.*

Démonstration Les deux lemmes précédents montrent que les applications $\mathfrak{q} \mapsto \mathfrak{q}A_\mathfrak{p}$ (définie pour tout idéal premier $\mathfrak{q}$ de A contenant $\mathfrak{p}$) et $\mathfrak{q}' \mapsto \mathfrak{q}' \cap A$ (définie pour tout idéal premier $\mathfrak{q}'$ de $A_\mathfrak{p}$) sont réciproques l'une de l'autre. De plus, elle sont évidemment croissantes, d'où le résultat. □

Lemme 11.163 ((Cas particulier du théorème d'intersection de Krull).) *On considère un élément non inversible x d'un anneau local noethérien A. Alors $\bigcap_{k\in\mathbb{N}} \langle x^k \rangle = \langle 0 \rangle$.*

Démonstration Posons $\mathcal{I} = \cap_{k\in N} \langle x \rangle^k$ et $y \in \mathcal{I}$. On écrit $y = a_k x^k$ pour tout $k \geqslant 1$ et on considère la suite croissante d'idéaux $\mathcal{I}_k = \langle a_1, \ldots, a_k \rangle$. Comme l'anneau est noethérien, cette suite stationne : il existe k tel que $a_{k+1} \in \langle a_1, \ldots, a_k \rangle$. Ainsi

$$y = a_{k+1}x^{k+1} \in \sum_{i=1}^{k} x^{k+1-i} \langle a_i x^i \rangle \subset x \langle y \rangle .$$

Ainsi il existe $a \in \mathcal{A}$ tel que $(1 - ax)y = 0$. Or, x appartient à l'idéal maximal (car A est un anneau local) donc $1 - ax$ est inversible, d'où $y = 0$. □

Théorème 11.164 *On note A un anneau noethérien intègre. Les assertions suivantes sont équivalentes.*

1. *L'anneau A est un anneau de Dedekind.*
2. *Pour tout couple $(a, b) \in A^2$, on a $1 \in (aA : bA) + (bA : aA)$.*
3. *Pour tout idéal premier $\mathfrak{p}$ non nul, l'anneau localisé $A_\mathfrak{p}$ est un anneau principal.*
4. *Pour tout idéal maximal M, il existe un élément $a \in M$ tel que $M = aA + M^2$.*
5. *(due à Krull ou Noether ?). Tout localisé A_M en un idéal M maximal est un anneau principal.*

Remarque. Les caractérisations 3, 4, 5 sont utiles en théorie des nombres bien sûr, mais aussi en géométrie algébrique. Un anneau local principal est un anneau *à valuation discrète.*

Démonstration

- Vérifions rapidement que l'assertion 1 implique l'assertion 2 : l'idéal $\langle a, b\rangle$ est inversible, donc $(aA : bA) + (bA : aA) = A$ (voir corollaire 11.126).
- Montrons que l'assertion 2 implique l'assertion 3 : on note $\mathfrak{p}$ un idéal premier non nul de A. On sait que $A_{\mathfrak{p}}$ est intègre et noethérien (comme A). Montrons que $A_{\mathfrak{p}}$ est un anneau de Bézout (voir définition **??**), ce qui implique que $A_{\mathfrak{p}}$ est principal. On considère $a, b \in A_{\mathfrak{p}}$. Montrons que a divise b ou b divise a. Sans perte de généralité, on peut supposer $a, b \in A$. Or, par hypothèse, il existe $i \in (aA : bA)$ et $j \in (bA : aA)$ tels que $i + j = 1$. L'idéal propre $\mathfrak{p}$ ne peut pas contenir simultanément i et j, donc, dans l'anneau local $A_{\mathfrak{p}}$, parmi i et j se trouve au moins un inversible. Cela signifie que $b \in aA_{\mathfrak{p}}$ (si i est inversible dans $A_{\mathfrak{p}}$) ou $a \in bA_{\mathfrak{p}}$ (si j est inversible dans $A_{\mathfrak{p}}$). Conclusion : $A_{\mathfrak{p}}$ est un anneau de Bézout noethérien intègre, donc $A_{\mathfrak{p}}$ est principal.
- Montrons que l'assertion 3 implique l'assertion 4 : si $M = \langle 0\rangle$, alors c'est évident. Si M n'est pas nul, alors l'idéal $M.A_M$ est principal : il existe $a \in A$ tel que $a.A_M = M.A_M$. Cela se traduit dans A par l'existence d'un élément $s \in A \setminus M$ tel que $sM \subset aA$. Or, M est maximal donc $A = M + sA$, puis $M = M^2 + sM \subset M^2 + aA$. L'inclusion réciproque $M \supset M^2 + aA$ est toujours vraie.
- Montrons que l'assertion 4 implique l'assertion 5 : dans l'anneau local A_M, posons $M' = M.A_M$ et écrivons $M' = M'^2 + \langle a\rangle$. Dans $A_M/\langle a\rangle$ (anneau local et noethérien), on a $\overline{M'} = \overline{M'}.\overline{M'}$: le lemme de Nakayama (voir proposition **??**) donne alors $A_M/\langle a\rangle = \overline{M'} + \mathrm{Ann}(\overline{M'})$. Or, $\overline{M'}$ est le seul idéal maximal de $A_M/\langle a\rangle$, donc $A_M/\langle a\rangle = \mathrm{Ann}(\overline{M'})$; autrement dit, $\overline{M'} = \langle 0\rangle$ ou encore $M' = \langle a\rangle$ dans A_M. L'idéal maximal de A_M est donc principal. Comme A_M est intègre et noethérien (comme A), il reste à montrer que tout idéal de type fini $\langle x_1, \ldots, x_n\rangle$ est principal. Il suffit pour cela de prouver que $x_i A_M = a^{k_i} A_M$ car ainsi on a $\langle x_1, \ldots, x_n\rangle = a^{\min(k_1,\ldots,k_n)} A_M$. On sait que $\cap_{k\in\mathbb{N}} a^k \mathcal{A}_M = \langle 0\rangle$ grâce au lemme 11.163. Ainsi, pour $x_i \neq 0$, on pose

$$k_i = \max\{k \in \mathbb{N} \mid x_i \in a^k \mathcal{A}_M\}.$$

  Alors on a $x_i \in a^{k_i} A_M \setminus a^{k_i+1} A_M$, donc $x_i = u a^{k_i}$ où u est un élément de A_M qui n'appartient pas à $aA_M = M'$. Conclusion : $x_i = u a^{k_i}$ avec u inversible de A_M et le résultat est prouvé.

  > Remarque. Dans ce passage, on touche réellement aux anneaux de valuation discrète : l'élément a engendrant l'idéal maximal $M.A_M$ est appelé *uniformisante* et l'exposant $k_i \in \mathbb{N}$ ($\mathbb{N}$ est un monoïde discret) tel que $\langle x_i\rangle = \langle a^{k_i}\rangle$ est la *valuation* de $x_i \neq 0$.

- Montrons que l'assertion 5 implique l'assertion 1 : pour tout idéal maximal M de A, le localisé A_M est un anneau principal, donc intégralement clos (comme tout anneau factoriel ou de Dedekind). Or, A est égal à l'intersection de tous ses localisés A_M en des idéaux maximaux, donc A est également intégralement clos. Par ailleurs, on note $\mathfrak{p}$ un idéal premier non nul de A et M un idéal maximal contenant $\mathfrak{p}$. L'idéal $\mathfrak{p}A_M$ en est un idéal premier non nul donc $\mathfrak{p}A_M$ est maximal (A_M est principal), donc $\mathfrak{p}A_M = MA_M$. Finalement, $\mathfrak{p} = M$ (voir théorème 11.162). Il en résulte que la dimension de Krull de A est égale 1. Enfin, comme l'anneau A est noethérien, on conclut la démonstration en utilisant le théorème 11.157.

□

Références

[Bou] N. Bourbaki. *Algèbre commutative,* ch. 5 à 7. Masson, 1985.

[Mal] M.P. Malliavin. *Algèbre commutative, applications en géométrie et théorie des nombres.* Masson, 1985.

[Mat] H. Matsumura. *Commutative Ring Theory.* Cambridge University Press, 1989. Cambridge studies in advanced mathematics 8.

[Sam] P. Samuel. *Théorie algébrique des nombres.* Hermann, 1967.

[Ser] J.P. Serre. *Corps locaux.* Hermann, 1962.

Index