LA NOTION D'ANNEAU DE DÉCOMPOSITION

C. CHEVALLEY

Introduction

Soit $\mathfrak{o}$ un domaine d'intégrité intégralement clos dans son corps des quotients, et soit $\mathfrak{m}$ un idéal premier de $\mathfrak{o}$. Soit $\mathfrak{J}$ un domaine d'intégrité intégralement clos dans son corps des quotients et dont $\mathfrak{o}$ est sous-anneau; soit $\mathfrak{M}$ un idéal premier de $\mathfrak{J}$ tel que $\mathfrak{m} = \mathfrak{M} \cap \mathfrak{o}$. M. Nagata ([4], I, §1) a posé la définition suivante: on dit que $\mathfrak{J}$ est anneau de décomposition pour $\mathfrak{M}$ s'il existe une extension normale séparable L'/K du corps des quotients K de $\mathfrak{o}$ et un idéal premier $\mathfrak{M}'$ de la clôture intégrale $\mathfrak{J}'$ de $\mathfrak{J}$ dans L' tel que $\mathfrak{M}' \cap \mathfrak{J} = \mathfrak{M}$ et que $\mathfrak{J}$ soit l'ensemble des éléments de $\mathfrak{J}'$ invariants par les automorphismes du groupe de Galois de L'/K qui conservent l'idéal $\mathfrak{M}'$. Appliquée au cas où $\mathfrak{o}$ est l'anneau des entiers rationnels et L/K une extension de degré fini, cette définition implique que L doit être le corps de décomposition tout entier d'un idéal premier contenant $\mathfrak{m}$ de la plus petite extension normale de K contenant L. Il convient donc de généraliser quelque peu cette définition: car, si $\mathfrak{M}$ est de degré relatif 1 et non ramifié par rapport au corps des rationnels, on désire évidemment pouvoir dire que $\mathfrak{J}$ est anneau de décomposition pour $\mathfrak{M}$. Dans le cas général, on est donc amené à demander non pas que $\mathfrak{J}$ soit l'ensemble de tous les éléments de $\mathfrak{J}'$ invariants par les opérations du groupe qui laisse $\mathfrak{M}'$ fixe, mais seulement que $\mathfrak{J}$ soit contenu dans cet ensemble. On arrive ainsi à ce qu'on peut appeler la définition *algébrique* des anneaux de décomposition. Mais on peut aussi chercher à généraliser la définition *arithmétique* ($\mathfrak{M}$ non ramifié et de degré relatif 1). Il est assez curieux que l'on arrive ainsi à une définition générale (sans faire aucune supposition sur les domaines d'intégrité $\mathfrak{o}$ et $\mathfrak{J}$ autre que celle que $\mathfrak{o}$ soit sous-anneau de $\mathfrak{J}$) de l'anneau de décomposition par rapport à $\mathfrak{o}$ d'un idéal premier $\mathfrak{M}$ de $\mathfrak{J}$: c'est le plus grand sous-anneau $\mathfrak{h}$ de $\mathfrak{J}$ qui possède les deux propriétés suivantes: tout élément de $\mathfrak{h}$ est congru modulo $\mathfrak{M}$ à un élément de $\mathfrak{o}$, et l'idéal maximal de l'anneau des quotients de $\mathfrak{M} \cap \mathfrak{h}$ est engendré par $\mathfrak{m} = \mathfrak{M} \cap \mathfrak{o}$ (condition qui généralise celle de non ramification).

Received April 26, 1954.

C'est cette définition que nous exposons ici ; nous montrons qu'elle conduit au même anneau que celui défini par M. Nagata dans le cas considéré par ce dernier, tout au moins si on suppose que $\mathfrak{o}$ est noethérien et est identique à l'anneau des quotients de $\mathfrak{m}$.

Nous obtenons également incidemment le résultat suivant. Supposons que $\mathfrak{o}$ soit un domaine d'intégrité noethérien qui ne possède qu'un seul idéal maximal $\mathfrak{m}$. Soit $\hat{\mathfrak{o}}$ la clôture intégrale de $\mathfrak{o}$ dans son corps des quotients, et soit $\hat{\mathfrak{m}}$ un idéal maximal de $\hat{\mathfrak{o}}$; il y a alors un anneau de valuation discrète non triviale du corps des quotients de $\mathfrak{o}$ dont l'idéal maximal contient $\hat{\mathfrak{m}}$, de sorte que la topologie $\hat{\mathfrak{m}}$-adique de l'anneau des quotients de $\hat{\mathfrak{m}}$ est séparée.

Terminologie

Nous appelons anneau local tout anneau qui ne possède qu'un seul idéal maximal. Si $\mathfrak{p}$ est un idéal premier d'un anneau $\mathfrak{o}$, nous dirons que son anneau des quotients est son anneau local. Nous appelons normal un domaine d'intégrité qui est intégralement clos dans son corps des quotients, et anneau dérivé normal d'un domaine d'intégrité $\mathfrak{o}$ la clôture intégrale de $\mathfrak{o}$ dans son corps des quotients. Tous les anneaux considérés sont commutatifs et pourvus d'un élément unité.

§ 1. Définition de l'anneau de décomposition

Nous désignerons dans ce § par $\mathfrak{J}$ un domaine d'intégrité, par $\mathfrak{o}$ un sous-anneau de $\mathfrak{J}$, par $\mathfrak{M}$ un idéal premier de $\mathfrak{J}$ et par $\mathfrak{m}$ l'idéal premier $\mathfrak{M} \cap \mathfrak{o}$ de $\mathfrak{o}$.

DÉFINITION 1. *Nous dirons que* $\mathfrak{M}$ *n'est pas ramifié par rapport* à $\mathfrak{o}$ *si l'idéal maximal de l'anneau local de* $\mathfrak{M}$ *est engendré par* $\mathfrak{m}$. *Nous dirons que* $\mathfrak{M}$ *est contrôlé par* $\mathfrak{o}$ *si les conditions suivantes sont satisfaites :* $\mathfrak{M}$ *n'est pas ramifié par rapport à* $\mathfrak{o}$ *et toute classe de restes de* $\mathfrak{J}$ *modulo* $\mathfrak{M}$ *contient un élément de* $\mathfrak{o}$.

La condition que $\mathfrak{M}$ ne soit pas ramifié par rapport à $\mathfrak{o}$ signifie que, pour tout $x \in \mathfrak{M}$, il existe un élément y de $\mathfrak{J}$ n'appartenant pas à $\mathfrak{M}$ tel que xy appartienne à l'idéal engendré par $\mathfrak{m}$ dans $\mathfrak{J}$. Si $\mathfrak{J}$ est noethérien, cette condition est équivalente à la suivante : l'idéal $(\mathfrak{m}\mathfrak{J}) : \mathfrak{M}$ n'est pas contenu dans $\mathfrak{M}$; en effet, $\mathfrak{M}$ a alors un ensemble fini de générateurs $x_1, \ldots, x_h$, et il existe un $y \in \mathfrak{J}$, $y \notin \mathfrak{M}$ tel que $x_i y \in \mathfrak{m}\mathfrak{J}$ $(1 \leqq i \leqq h)$, d'où $\mathfrak{M}y \subset \mathfrak{m}\mathfrak{J}$. La condition que toute classe de restes de $\mathfrak{J}$ modulo $\mathfrak{M}$ contienne un élément de $\mathfrak{o}$ est équivalente à l'égalité $\mathfrak{J} = \mathfrak{M} + \mathfrak{o}$.

THÉORÈME 1. *Soit F un ensemble de sous-anneaux de $\mathfrak{J}$ contenant $\mathfrak{o}$ tel que, pour tout anneau $\mathfrak{h}$ appartenant à F, l'idéal $\mathfrak{M} \cap \mathfrak{h}$ soit contrôlé par $\mathfrak{o}$. Si $\mathfrak{H}$ est le sous-anneau de $\mathfrak{J}$ engendré par tous les anneaux de l'ensemble F, l'idéal $\mathfrak{M} \cap \mathfrak{H}$ est contrôlé par $\mathfrak{o}$.*

Nous désignerons par $\mathfrak{N}$ l'idéal $\mathfrak{M} \cap \mathfrak{H}$ et par $\mathfrak{N}'$ l'ensemble des $x \in \mathfrak{H}$ pour lesquels il existe un $y \in \mathfrak{H}$ n'appartenant pas à $\mathfrak{N}$ tel que $xy \in \mathfrak{m}\mathfrak{H}$. Cet ensemble est un idéal, intersection de $\mathfrak{H}$ et de l'idéal engendré par $\mathfrak{m}$ dans l'anneau local de $\mathfrak{N}$. Tout anneau $\mathfrak{h} \in F$ est contenu dans $\mathfrak{o} + \mathfrak{N}'$. En effet, si $x \in \mathfrak{h}$, il y a un $a \in \mathfrak{o}$ tel que $x - a \in \mathfrak{M}$, d'où $x - a \in \mathfrak{M} \cap \mathfrak{h}$. Puisque $\mathfrak{M} \cap \mathfrak{h}$ n'est pas ramifié par rapport à $\mathfrak{o}$, il y a un $y \in \mathfrak{h}$ n'appartenant pas à $\mathfrak{M}$ tel que $y(x-a)$ appartienne à $\mathfrak{m}\mathfrak{h}$, donc, *a fortiori*, à $\mathfrak{m}\mathfrak{H}$. Il en résulte immédiatement que $x - a \in \mathfrak{N}'$, $x \in \mathfrak{o} + \mathfrak{N}'$. Or $\mathfrak{o} + \mathfrak{N}'$ est l'image inverse par rapport à l'homomorphisme canonique de $\mathfrak{H}$ sur $\mathfrak{H}/\mathfrak{N}'$ de l'image de l'anneau $\mathfrak{o}$; c'est donc un anneau, d'où $\mathfrak{H} = \mathfrak{o} + \mathfrak{N}'$. Si $u \in \mathfrak{N}$, il y a un $b \in \mathfrak{o}$ tel que $u - b \in \mathfrak{N}'$; on a $b = u - (u-b) \in \mathfrak{N} \cap \mathfrak{o} = \mathfrak{m} \subset \mathfrak{N}'$, d'où $u \in \mathfrak{N}'$, et $\mathfrak{N} = \mathfrak{N}'$; $\mathfrak{N}$ n'est donc pas ramifié par rapport à $\mathfrak{o}$. Puisque $\mathfrak{N} = \mathfrak{N}'$, on a $\mathfrak{H} = \mathfrak{o} + \mathfrak{N}$, et $\mathfrak{N}$ est contrôlé par $\mathfrak{o}$.

Le théorème 1 légitime la définition suivante :

DÉFINITION 2. *On appelle anneau de décomposition de $\mathfrak{M}$ par rapport à $\mathfrak{o}$ le plus grand sous-anneau $\mathfrak{h}$ de $\mathfrak{J}$ contenant $\mathfrak{o}$ tel que $\mathfrak{M} \cap \mathfrak{h}$ soit contrôlé par $\mathfrak{o}$.*

Il est clair que l'anneau de décomposition de $\mathfrak{M} \cap \mathfrak{h}$ par rapport à $\mathfrak{o}$ est alors $\mathfrak{h}$.

PROPOSITION 1. *Supposons que l'anneau de décomposition de $\mathfrak{M}$ par rapport à $\mathfrak{o}$ soit $\mathfrak{J}$ lui-même. Soit x un élément de l'anneau local $\mathfrak{J}_{\mathfrak{M}}$ de $\mathfrak{M}$. Pour tout entier $n > 0$, il y a un élément a_n de l'anneau local $\mathfrak{o}_{\mathfrak{m}}$ de $\mathfrak{m}$ tel que $x - a_n \in \mathfrak{m}^n \mathfrak{J}_{\mathfrak{M}}$.*

Considérons d'abord le cas où $n = 1$. On a $x = yz^{-1}$, où y, z sont dans $\mathfrak{J}$, $z \notin \mathfrak{M}$. Il y a des éléments b, c de $\mathfrak{o}$ tels que $y - b \in \mathfrak{m}\mathfrak{J}_{\mathfrak{M}}$, $z - c \in \mathfrak{m}\mathfrak{J}_{\mathfrak{M}}$, et, puisque $\mathfrak{m}\mathfrak{J}_{\mathfrak{M}} \cap \mathfrak{J}$ est contenu dans $\mathfrak{M}$, c n'est pas dans $\mathfrak{m}$, d'où $bc^{-1} \in \mathfrak{o}_{\mathfrak{m}}$. On a $x - bc^{-1} = (yc - zb)(cz)^{-1}$, d'où $x - bc^{-1} \in \mathfrak{m}\mathfrak{J}_{\mathfrak{M}}$. Supposons maintenant l'assertion vraie pour un $n > 0$. On a $x - a_n = \sum_{i=1}^{h} d_i u_i$, les d_i étant dans $\mathfrak{m}^n$ et les u_i dans $\mathfrak{J}_{\mathfrak{M}}$; il y a des $e_i \in \mathfrak{o}_{\mathfrak{m}}$ tels que $u_i - e_i \in \mathfrak{m}\mathfrak{J}_{\mathfrak{M}}$; si on pose $a_{n+1} = \sum_{i=1}^{h} d_i e_i + a_n$, $x - a_{n+1}$ est dans $\mathfrak{m}^{n+1}\mathfrak{J}_{\mathfrak{M}}$.

Soit $\mathfrak{h}$ l'anneau de décomposition de $\mathfrak{M}$ par rapport à $\mathfrak{o}$, et soit $\mathfrak{o}'$ un sous-anneau de $\mathfrak{h}$ contenant $\mathfrak{o}$. On peut se demander si l'idéal premier $\mathfrak{M} \cap \mathfrak{o}'$ de $\mathfrak{o}'$ est contrôlé par $\mathfrak{o}$. Il est évident que toute classe de résidus de $\mathfrak{o}'$ modulo $\mathfrak{M} \cap \mathfrak{o}'$ contient un élément de $\mathfrak{o}$. Mais il paraît peu probable que l'on puisse affirmer en général que $\mathfrak{M} \cap \mathfrak{o}'$ n'est pas ramifié par rapport à $\mathfrak{o}$.

PROPOSITION 2. *Soient $\mathfrak{h}$ l'anneau de décomposition de $\mathfrak{M}$ par rapport à $\mathfrak{o}$ et $\mathfrak{o}'$ un sous-anneau de $\mathfrak{h}$ contenant $\mathfrak{o}$ tel que $\mathfrak{M} \cap \mathfrak{o}'$ ne soit pas ramifié par rapport à $\mathfrak{o}$. L'anneau $\mathfrak{h}$ est alors l'anneau de décomposition de $\mathfrak{M}$ par rapport à $\mathfrak{o}'$.*

On a $\mathfrak{h} = \mathfrak{o} + (\mathfrak{M} \cap \mathfrak{h}) = \mathfrak{o}' + (\mathfrak{M} \cap \mathfrak{h})$. Si $x \in \mathfrak{M} \cap \mathfrak{h}$, il y a un $y \in \mathfrak{h}$ n'appartenant pas à $\mathfrak{M}$ tel que $xy \in \mathfrak{m}\mathfrak{h}$, et on a *a fortiori* $xy \in (\mathfrak{M} \cap \mathfrak{o}')\mathfrak{h}$, de sorte que $\mathfrak{M} \cap \mathfrak{h}$ n'est pas ramifié par rapport à $\mathfrak{o}'$ et que $\mathfrak{h}$ est contenu dans l'anneau de décomposition $\mathfrak{h}'$ de $\mathfrak{M}$ par rapport à $\mathfrak{o}'$. On a $\mathfrak{h}' = \mathfrak{o}' + (\mathfrak{M} \cap \mathfrak{h}')$, et, puisque $\mathfrak{o}' \subset \mathfrak{h}$, $\mathfrak{o}' \subset \mathfrak{o} + (\mathfrak{M} \cap \mathfrak{h})$; puisque $\mathfrak{h} \subset \mathfrak{h}'$, on a $\mathfrak{h}' = \mathfrak{o} + (\mathfrak{M} \cap \mathfrak{h}')$. Soit x' un élément de $\mathfrak{M} \cap \mathfrak{h}'$; il y a un élément y' de $\mathfrak{h}'$ n'appartenant pas à $\mathfrak{M}$ tel que $x'y' \in (\mathfrak{M} \cap \mathfrak{o}')\mathfrak{h}$. Écrivons $x'y' = \sum_{i=1}^{h} u'_i v'_i$, $u'_i \in \mathfrak{M} \cap \mathfrak{o}'$, $v'_i \in \mathfrak{h}'$; il résulte de l'hypothèse faite sur $\mathfrak{o}'$ qu'il y a des $w'_i \in \mathfrak{o}'$ n'appartenant pas à $\mathfrak{M}$ tels que $u'_i w'_i \in \mathfrak{m}\mathfrak{o}'$; soit w' leur produit. Alors $w'y'$ est un élément de $\mathfrak{h}'$ n'appartenant pas à $\mathfrak{M}$ et $x'w'$ est dans $\mathfrak{m}\mathfrak{h}'$, ce qui montre que $\mathfrak{M} \cap \mathfrak{h}'$ n'est pas ramifié par rapport à $\mathfrak{o}$, d'où $\mathfrak{h}' \subset \mathfrak{h}$ et $\mathfrak{h}' = \mathfrak{h}$.

§ 2. Extensions entières d'anneaux locaux noethériens

Nous utiliserons les mêmes notations qu'au § 1, mais nous supposerons de plus les conditions suivantes satisfaites : *l'anneau $\mathfrak{o}$ est un anneau local noethérien dont $\mathfrak{m}$ est l'idéal maximal, et $\mathfrak{J}$ est entier sur $\mathfrak{o}$.*

Lorsque $\mathfrak{J}$ est fini sur $\mathfrak{o}$, c'est-à-dire peut être obtenu par adjonction d'un nombre fini d'éléments à $\mathfrak{o}$, l'intersection des idéaux $\mathfrak{m}^n \mathfrak{J}_{\mathfrak{M}}$ se réduit à $\{0\}$. Nous nous proposons de montrer qu'il en est encore ainsi dans le cas général.

LEMME 1. *Soit $\mathfrak{o}^*$ l'anneau dérivé normal de $\mathfrak{o}$. Il n'y a alors qu'un nombre fini d'idéaux premiers de $\mathfrak{o}^*$ dont l'intersection avec $\mathfrak{o}$ soit $\mathfrak{m}$.*

Introduisons une complétion $\hat{\mathfrak{o}}$ de $\mathfrak{o}$, et désignons par A l'anneau des fractions de $\hat{\mathfrak{o}}$. L'anneau A est donc noethérien. Nous allons montrer qu'il en résulte que 1 s'y décompose en la somme d'un nombre fini d'idempotents orthogonaux primitifs (un idempotent e étant appelé primitif si $e \neq 0$ et s'il est impossible de représenter e comme somme de deux idempotents orthogonaux $\neq 0$). Supposons en effet le contraire, et soit E l'ensemble des idempotents $\neq 0$ qui ne peuvent pas se représenter comme sommes d'idempotents orthogonaux primitifs. Construisons inductivement une suite (e_n) d'éléments de E comme suit. On pose $e_0=1$. Si e_n est déjà déterminé, e_n n'est pas primitif et peut par suite se décomposer en la somme de deux idempotents orthogonaux $\neq 0$; l'un au moins de ces deux idempotents est dans E, et nous le désignerons alors par e_{n+1}. On a $A(1-e_n)\subset A(1-e_{n+1})$, car, si $e_n=e_{n+1}+f_{n+1}$, f_{n+1} étant un idempotent $\neq 0$ orthogonal à e_{n+1}, on a $1-e_n=(1-e_{n+1})(1-f_{n+1})$; de plus, $A(1-e_{n+1})\neq A(1-e_n)$, car $(1-e_n)e_n=0$, $(1-e_{n+1})e_n=f_{n+1}\neq 0$. On obtient donc une suite infinie strictement croissante d'idéaux de A, ce qui est impossible. Soit donc $1=e_1+\ldots+e_h$ une décomposition de 1 en somme d'idempotents orthogonaux primitifs. Tout idempotent e de A est alors la somme de certains des e_i; car $e=\sum_{i=1}^{h}ee_i$, et, si $ee_i\neq 0$, $ee_i=e_i$ comme il résulte tout de suite du caractère primitif de e_i. On en déduit tout de suite qu'il ne peut exister plus de h idempotents $\neq 0$ mutuellement orthogonaux dans A. Montrons alors que, si $\mathfrak{o}'$ est un anneau intermédiaire entre $\mathfrak{o}$ et $\mathfrak{o}^*$, fini sur $\mathfrak{o}$, il n'y a pas plus de h idéaux premiers de $\mathfrak{o}'$ dont les intersections avec $\mathfrak{o}$ soient $\mathfrak{m}$. L'anneau $\mathfrak{o}'$ est un $\mathfrak{o}$-module fini; c'est donc un anneau semi-local dont la complétion $\hat{\mathfrak{o}}'$ contient $\hat{\mathfrak{o}}$ comme sous-anneau, et on a $\hat{\mathfrak{o}}'=\hat{\mathfrak{o}}[\mathfrak{o}']$ (cf. [5], p. 17, *g.* et *h.*). Il résulte alors du fait que $\mathfrak{o}'$ est contenu dans le corps des quotients de $\mathfrak{o}$ et du fait qu'aucun élément $\neq 0$ de $\mathfrak{o}$ n'est diviseur de zéro dans $\hat{\mathfrak{o}}$ que $\hat{\mathfrak{o}}'$ est isomorphe à un sous-anneau de A. Mais, s'il y a h' idéaux premiers distincts de $\mathfrak{o}'$ dont les intersections avec $\mathfrak{o}$ soient $\mathfrak{m}$, $\hat{\mathfrak{o}}'$ est isomorphe au produit de h' anneaux ([5], p. 15, cor. 2) dont chacun a un élément unité, ce qui montre que $\hat{\mathfrak{o}}'$ contient h' idempotents $\neq 0$ orthogonaux. On a donc $h'\leqq h$. Il est alors facile de voir qu'il n'y a pas plus de h idéaux premiers de $\hat{\mathfrak{o}}$ dont les intersections avec $\mathfrak{o}$ soient $\mathfrak{m}$. En effet, si $\hat{\mathfrak{m}}_1,\ldots,\hat{\mathfrak{m}}_k$ sont des idéaux premiers distincts de $\hat{\mathfrak{o}}$ dont les intersections avec $\mathfrak{o}$ soient $\mathfrak{m}$, on peut trouver, pour chaque ensemble $\{i, j\}$ de deux indices distincts entre 1 et k, un élément x_{ij} de $\hat{\mathfrak{o}}$ qui soit dans l'un des idéaux $\hat{\mathfrak{m}}_i$, $\hat{\mathfrak{m}}_j$ sans être dans l'autre; si $\mathfrak{o}'=\mathfrak{o}[\ldots, x_{ij},\ldots]$, $\mathfrak{o}'$ est fini sur $\mathfrak{o}$, et les $\hat{\mathfrak{m}}_i\cap\mathfrak{o}'$ $(1\leqq i\leqq k)$ sont des idéaux premiers distincts de $\mathfrak{o}'$ dont les intersections avec $\mathfrak{o}$ sont égales à $\mathfrak{m}$.

De plus, la fin du raisonnement montre que l'on peut trouver un sous-anneau $\mathfrak{o}'$ de $\hat{\mathfrak{o}}$, contenant $\mathfrak{o}$ et fini sur $\mathfrak{o}$, tel que, pour tout idéal premier $\mathfrak{m}'$ de $\mathfrak{o}'$ dont l'intersection avec $\mathfrak{o}$ soit $\mathfrak{m}$, il n'y ait qu'un seul idéal premier de $\hat{\mathfrak{o}}$ dont l'intersection avec $\mathfrak{o}'$ soit $\mathfrak{m}'$ (il est bien connu qu'il existe au moins un pareil idéal ; cf. [2]).

LEMME 2. *Il existe un anneau de valuation discrète non triviale du corps des quotients de* $\mathfrak{o}$ *dont l'anneau contient* $\mathfrak{o}$ *et dont l'idéal maximal contient* $\mathfrak{m}$.

Soit en effet $(x_1, \ldots, x_d)$ un système de paramètres dans $\mathfrak{o}$; l'idéal $\mathfrak{a}$ engendré par $x_1, \ldots, x_d$ contient donc une puissance de $\mathfrak{m}$, mais il n'y a aucun idéal engendré par moins de d éléments ayant la même propriété. On a donc $x_d \neq 0$; posons $y_i = x_i/x_d$, $\mathfrak{o}' = \mathfrak{o}[y_1, \ldots, y_d]$. L'idéal engendré par x_d dans $\mathfrak{o}'$ ne contient pas 1. Supposons en effet le contraire ; on a alors $1 = x_d P(y_1, \ldots, y_{d-1})$, où P est un polynôme à coefficients dans $\mathfrak{o}$ dont nous désignerons le terme constant par a et le degré par s. Soit $\mathfrak{b}$ l'idéal engendré par $x_1, \ldots, x_{d-1}$ dans $\mathfrak{o}$; multipliant la relation précédente par x_d^s, on obtient une congruence $x_d^s \equiv a x_d^{s+1} \pmod{\mathfrak{b}}$. Il en résulte par recurrence sur n que $x_d^s \equiv a^n x_d^{s+n} \pmod{\mathfrak{b}}$. Or, x_d est évidemment dans $\mathfrak{m}$; il vient donc $x_d^s \in \mathfrak{m}^{s+n} + \mathfrak{b}$. L'idéal $\mathfrak{b}$ étant fermé dans la topologie $\mathfrak{m}$-adique de $\mathfrak{o}$, on a $x_d^s \in \mathfrak{b}$. Tout idéal premier $\mathfrak{p}$ de $\mathfrak{o}$ qui contient $\mathfrak{b}$ contient donc aussi x_d, donc $\mathfrak{a}$, et est par suite $\mathfrak{m}$; $\mathfrak{o}$ étant noethérien, il en résulte qu'il y a une puissance de $\mathfrak{m}$ contenue dans $\mathfrak{b}$, ce qui est impossible. Ceci dit, soit $\mathfrak{q}'$ un idéal premier minimal de l'idéal $\mathfrak{o}' x_d$ de $\mathfrak{o}'$; en vertu d'un théorème de Akizuki et Krull ([1] et [3] ; voir l'appendice pour une nouvelle démonstration), l'anneau local $\mathfrak{o}'_{\mathfrak{q}'}$ de $\mathfrak{q}'$ est contenu dans un anneau de valuation discrète $\mathfrak{v}$ du corps des quotients de $\mathfrak{o}$ dont l'idéal maximal $\mathfrak{w}$ contient $\mathfrak{q}'$. Il est clair que $\mathfrak{v}$ contient $\mathfrak{o}$ et que $x_d \in \mathfrak{w}$; comme $\mathfrak{o}' \subset \mathfrak{v}$, on a $x_i = x_d y_i \in \mathfrak{w}$ $(1 \leqq i \leqq d)$; l'idéal premier $\mathfrak{w} \cap \mathfrak{o}$ de $\mathfrak{o}$ contient donc $\mathfrak{a}$ et est par suite identique à $\mathfrak{m}$.

LEMME 3. *Il existe une valuation non triviale du corps des quotients* L *de* $\mathfrak{J}$ *dont le groupe des valeurs est archimédien, dont l'anneau contient* $\mathfrak{J}$ *et dont l'idéal contient* $\mathfrak{M}$.

Soit L'/K une extension normale de K contenant L/K, et soit $\mathfrak{J}'$ la clôture intégrale de $\mathfrak{J}$ dans L'. On sait qu'il y a au moins un idéal maximal $\mathfrak{M}'$ de $\mathfrak{J}'$ tel que $\mathfrak{M}' \cap \mathfrak{J} = \mathfrak{M}$. Il suffira évidemment de montrer qu'il y a une valuation non triviale de L' dont le groupe des valeurs est archimédien, dont l'anneau contient $\mathfrak{J}'$ et dont l'idéal contient $\mathfrak{M}'$. On peut donc supposer sans restriction de généralité que l'extension L/K est normale et que $\mathfrak{J}$ est intégralement clos dans L. Soit $\mathfrak{o}^*$ l'anneau dérivé normal de $\mathfrak{o}$; $\mathfrak{M} \cap \mathfrak{o}^*$ est un idéal maximal de $\mathfrak{o}^*$. Il y a un sous-anneau $\mathfrak{o}'$ de $\mathfrak{o}^*$, contenant $\mathfrak{o}$ et fini sur $\mathfrak{o}$, tel que $\mathfrak{M} \cap \mathfrak{o}^*$ soit le seul idéal premier de $\mathfrak{o}^*$ dont l'intersection avec $\mathfrak{o}'$ soit $\mathfrak{M} \cap \mathfrak{o}'$ (cf. les lignes qui précèdent l'énoncé du Lemme 2). Il résulte immédiatement du Lemme 2 qu'il y a une valuation discrète non triviale v de K dont l'anneau $\mathfrak{v}$ contient $\mathfrak{o}'$ et dont l'idéal maximal contient $\mathfrak{M} \cap \mathfrak{o}'$. L'intersection avec $\mathfrak{o}^*$ de l'idéal de valuation de v est alors $\mathfrak{M} \cap \mathfrak{o}^* = \mathfrak{M} \cap K$. Soit $\mathfrak{R}$ l'anneau engendré par $\mathfrak{v}$ et $\mathfrak{J}$; montrons que l'idéal engendré par $\mathfrak{M}$ dans $\mathfrak{R}$ ne contient pas 1. Supposons pour un moment qu'il n'en soit pas ainsi; il y a alors une relation de la forme $\sum_{i=1}^{h} u_i x_i = 1$ où les u_i sont dans $\mathfrak{v}$ et les x_i dans $\mathfrak{M}$. Soit L_0 le corps engendré par K, par $x_1, \ldots, x_h$ et par leurs conjugués par rapport à K; soit G le groupe de Galois de L_0/K; ses opérations transforment en lui-même l'anneau $\mathfrak{J} \cap L_0$. L'élément $1 = \prod_{s \in G} s(\sum_{i=1}^{h} u_i x_i)$ se met sous la forme $\sum_{j=1}^{k} u'_j y_j$ où les u'_j sont dans $\mathfrak{v}$ et où les y_j sont des sommes de produits de la forme $\prod_{s \in G} s x_{i(s)}$ $(1 \leqq i(s) \leqq h,$ $s \in G)$ et sont invariants par les opérations de G. On a donc $y_j \in \mathfrak{M}$ pour tout j; de plus, il y a une puissance q de l'exposant caractéristique de K telle que $y_j^q \in K$ pour tout j, d'où $v(y_j^q) > 0$; la relation $1 = \sum_{j=1}^{k} u_j'^q y_j^q$ conduit alors à une contradiction. On en déduit que $\mathfrak{M}$ est contenu dans au moins un idéal maximal $\mathfrak{N}$ de $\mathfrak{R}$. On sait qu'il y a un anneau de valuation $\mathfrak{B} \neq L$ de L qui contient $\mathfrak{R}$ et dont l'idéal maximal contient $\mathfrak{N}$. L'anneau $\mathfrak{B} \cap K$ contient $\mathfrak{v}$ mais est $\neq K$ (car, sinon, $\mathfrak{B}$ contiendrait L, qui est entier sur K); la valuation v étant discrète, on sait qu'il en résulte que $\mathfrak{B} \cap K = \mathfrak{v}$. Puisque L est algébrique sur K, la valuation d'anneau $\mathfrak{B}$, qui prolonge v, est à groupe de valeurs archimédien.

Lemme 4. *L'intersection des idéaux* $\mathfrak{m}^n \mathfrak{J}_{\mathfrak{M}}$ $(n = 1, 2, \ldots)$ *se réduit à* $\{0\}$.

Soit v une valuation possédant les propriétés énoncées au Lemme 3. Il est clair que $\mathfrak{M}$ est l'intersection de $\mathfrak{J}$ avec l'idéal maximal de v, donc que $\mathfrak{J}_{\mathfrak{M}}$ est contenu dans l'anneau de v. Soit $(c_1, \ldots, c_r)$ un système fini de générateurs de l'idéal $\mathfrak{m}$; soit α le plus petit des $v(c_k)$ $(1 \leqq k \leqq r)$; on a donc $\alpha > 0$. Il est clair que la condition $z \in \mathfrak{m}^n \mathfrak{J}_{\mathfrak{M}}$ entraîne $v(z) \geqq n\alpha$; le Lemme 4 résulte immédiatement de là.

Théorème 2. *Soient K et L les corps des quotients de $\mathfrak{o}$ et de $\mathfrak{J}$, et soit L'/K*

une extension algébrique normale de K contenant L/K. Soit $\mathfrak{J}'$ *la clôture intégrale de* $\mathfrak{J}$ *dans L', et soit* $\mathfrak{M}'$ *un idéal premier de* $\mathfrak{J}'$ *tel que* $\mathfrak{M}' \cap \mathfrak{J} = \mathfrak{M}$. *Les éléments de l'anneau de décomposition de* $\mathfrak{M}$ *par rapport à* $\mathfrak{o}$ *sont alors invariants par tout automorphisme de L'/K qui transforme* $\mathfrak{M}'$ *en lui-même.*

Soit x un élément de l'anneau de décomposition. $\mathfrak{h}$ de $\mathfrak{M}$ par rapport à $\mathfrak{o}$, et soit n un entier > 0 quelconque. Désignons par $\mathfrak{k}$ l'anneau local de l'idéal premier $\mathfrak{M} \cap \mathfrak{h}$ de $\mathfrak{h}$; il y a alors un élément $a \in \mathfrak{o}$ tel que $x - a \in \mathfrak{m}^n \mathfrak{k}$ (prop. 1). Il est clair que $\mathfrak{k}$ est contenu dans l'anneau local $\mathfrak{J}'_{\mathfrak{M}'}$ de $\mathfrak{M}'$; on a donc $x - a \in \mathfrak{m}^n \mathfrak{J}'_{\mathfrak{M}'}$. Soit s un automorphisme de L'/K qui transforme $\mathfrak{M}'$ en lui-même; s transforme alors $\mathfrak{J}'_{\mathfrak{M}'}$ en lui-même, et laisse fixes a et les éléments de $\mathfrak{m}^n$. On en conclut que $s \cdot x - x \in \mathfrak{m}^n \mathfrak{J}'_{\mathfrak{M}'}$. Ceci étant vrai quel que soit n, il résulte du Lemme 3 que $s \cdot x = x$, ce qui démontre le théorème.

Supposons à partir de maintenant les anneaux $\mathfrak{o}$ *et* $\mathfrak{J}$ *normaux, et supposons de plus que le corps des quotients L de* $\mathfrak{J}$ *soit séparable sur K.* Choisissons une extension séparable normale L'/K de K contenant L/K; désignons par $\mathfrak{J}'$ la clôture intégrale de $\mathfrak{J}$ (ou de $\mathfrak{o}$) dans L', et par $\mathfrak{M}'$ un idéal premier de $\mathfrak{J}'$ tel que $\mathfrak{M}' \cap \mathfrak{J} = \mathfrak{M}$. Soient H le groupe des automorphismes de L'/K qui transforment $\mathfrak{M}'$ en lui-même, et $\mathfrak{h}$ l'anneau des éléments de $\mathfrak{J}$ qui sont invariants par tous les automorphismes du groupe H. Il résulte du Théorème 2 que l'anneau de décomposition de $\mathfrak{M}$ par rapport à $\mathfrak{o}$ est contenu dans $\mathfrak{h}$. Par ailleurs, les résultats établis par M. Nagata montrent que $\mathfrak{h}$ est contenu dans l'anneau de décomposition de $\mathfrak{M}$. Nous allons démontrer ici qu'il en est bien ainsi, pour la commodité du lecteur; le raisonnement ne différera que par la forme de celui de M. Nagata.

Établissons d'abord que tous les idéaux premiers de $\mathfrak{J}'$ dont les intersections avec $\mathfrak{o}$ sont $\mathfrak{m}$ se déduisent les uns des autres par les automorphismes de L'/K. Il est bien connu qu'il en est ainsi pour les extensions finies; il ne s'agit que d'étendre le résultat aux extensions quelconques. Le groupe de Galois G de L'/K est muni d'une topologie qui en fait un groupe compact; on obtient un système fondamental de voisinages compacts de l'unité dans G en prenant les groupes de Galois des extensions L'/M, où M parcourt les extensions finies de K contenues dans L'. Le groupe H est fermé. En effet, soit s un élément de G adhérent à H, et soit u un élément de $\mathfrak{M}'$. Puisque s est adhérent à H, on peut écrire $s = s's''$, où $s' \in H$ tandis que s'' appartient au groupe de $L'/K(u)$.

On a donc $s \cdot u = s' \cdot u \in \mathfrak{M}'$, ce qui montre que $s \in H$. Soit $\mathfrak{M}_1'$ un idéal premier de $\mathfrak{J}'$ tel que $\mathfrak{M}_1' \cap \mathfrak{o} = \mathfrak{m}$. Si M/K est une extension normale finie de K contenue dans L'/K, $\mathfrak{J}' \cap M$ est la clôture intégrale de $\mathfrak{o}$ dans M, et $\mathfrak{M}' \cap M$, $\mathfrak{M}_1' \cap M$ sont des idéaux premiers de cet anneau dont les intersections avec $\mathfrak{o}$ sont $\mathfrak{m}$; il y a donc un antomorphisme de M/K qui transforme le premier de ces idéaux en le second. Cet automorphisme se prolonge en un automorphisme de L'/K; l'ensemble U_M des automorphismes de L'/K qui transforment $\mathfrak{M}' \cap M$ en $\mathfrak{M}_1' \cap M$ est donc non vide. Cet ensemble est la réunion d'un nombre fini de classes de G suivant le groupe de Galois de L'/M; il est donc compact. Il est clair que l'intersection d'un nombre fini d'ensembles de la forme U_M contient un ensemble de la même forme, et est par suite non vide. Le groupe G étant compact, l'intersection de tous les ensembles U_M est non vide; si t appartient à cette intersection, t transforme $\mathfrak{M}'$ en $\mathfrak{M}_1'$.

Soit x un élément de l'anneau $\mathfrak{h}$. Soit L''/K une extension normale finie de K contenant $K(x)/K$ et contenue dans L'/K; soient $\mathfrak{J}''$ l'anneau $\mathfrak{J}' \cap L''$ et $\mathfrak{M}''$ l'idéal $\mathfrak{M}' \cap \mathfrak{J}''$. Tout automorphisme s de L''/K qui laisse M'' invariant laisse alors x invariant. En effet, s se prolonge en un automorphisme s_1 de L'/K, et s_1^{-1} transforme $\mathfrak{M}'$ en un idéal $\mathfrak{M}_1'$ tel que $\mathfrak{M}_1' \cap \mathfrak{J}'' = \mathfrak{M}''$. Il résulte alors de ce que nous venons d'établir qu'il existe un automorphisme s_2 de L'/L'' qui transforme $\mathfrak{M}'$ en $\mathfrak{M}_1'$; $s_1 s_2$ appartient donc à H et laisse par suite x fixe. Mais on a aussi $s_2 \cdot x = x$ puisque $x \in L''$, d'où $s_1 \cdot x = x$, ce qui démontre notre assertion.

Les idéaux premiers de $\mathfrak{J}''$ dont les intersections avec $\mathfrak{o}$ sont $\mathfrak{m}$, étant conjugués par rapport à K, sont en nombre fini. Soient $\mathfrak{M}_1'', \ldots, \mathfrak{M}_h''$ ces idéaux (avec $\mathfrak{M}_i'' \neq \mathfrak{M}_j''$ si $i \neq j$); on peut supposer que les transformés de $\mathfrak{M}''$ par les opérations du groupe de Galois de $L''/K(x)$ sont $\mathfrak{M}_1'', \ldots, \mathfrak{M}_k''$. Les anneaux $\mathfrak{J}''/\mathfrak{M}_i''$ sont entiers sur le corps $\mathfrak{o}/\mathfrak{m}$; ce sont donc des corps, et les $\mathfrak{M}_i''$ sont des idéaux maximaux. Soit $\mathfrak{A}_i$ le produit des $\mathfrak{M}_j''$ pour $j \neq i$; cet idéal n'est pas contenu dans $\mathfrak{M}_i''$, d'où $\mathfrak{M}_i'' + \mathfrak{A}_i = \mathfrak{J}''$. Il y a donc un élément $y_i'' \in \mathfrak{A}_i$ tel que $1 - y_i'' \in \mathfrak{M}_i''$. Posons $y' = y_1'' + \ldots + y_k''$; $y' - 1$ est donc dans chacun des idéaux $\mathfrak{M}_1'', \ldots, \mathfrak{M}_k''$, tandis que $y' \in \mathfrak{M}_j''$ si $j > k$. Soit y la norme relative de y' par rapport à $K(x)$; cet élément est entier sur $\mathfrak{o}$, donc contenu dans $\mathfrak{h}$. Les automorphismes de $L''/K(x)$ permutant $\mathfrak{M}_1'', \ldots, \mathfrak{M}_k''$ entre eux, on a $y - 1 \in \mathfrak{M}_1'' \cap \mathfrak{h}$. Or, $\mathfrak{M}_1'' \cap \mathfrak{h}$ est aussi $\mathfrak{M}' \cap \mathfrak{h} = \mathfrak{M} \cap \mathfrak{h}$, d'où $y - 1 \in \mathfrak{M} \cap \mathfrak{h}$. Par contre, si t est un automorphisme de L''/K qui ne laisse pas x fixe, $t(\mathfrak{M}_1'')$ n'est pas parmi

$\mathfrak{M}_1'', \ldots, \mathfrak{M}_k''$. En effet, s'il en était ainsi, t pourrait se mettre sous la forme $t_1 t_2$ avec t_2 dans le groupe de $L''/K(x)$ et $t_1(\mathfrak{M}_1'') = \mathfrak{M}_1''$; mais nous avons vu que cela entraînerait que $t_1 \cdot x = x$, d'où $t \cdot x = x$. Si $t(\mathfrak{M}_1'')\mathfrak{M}_j''$, $j > K$, $t^{-1} \cdot y'$ est dans $\mathfrak{M}_1''$ puisque $y' \in \mathfrak{M}_1''$; $t^{-1} \cdot y$, qui est divisible par $t^{-1} \cdot y'$ dans $\mathfrak{Z}''$, est donc dans $\mathfrak{M}_1''$, d'où, en particulier, $t^{-1} \cdot y \neq y$. On en conclut que $K(x) = K(y)$; de plus, si $y_1 = y, \ldots, y_p$ sont les conjugués distincts de y par rapport à K, $y_2, \ldots, y_p$ sont dans $\mathfrak{M}_1''$. Les automorphismes de L''/K qui transforment y en $y_1, \ldots, y_p$ transforment x en $x_1 = x, x_2, \ldots, x_p$. La trace S de xy par rapport à K est donc $xy + x_2 y_2 + \ldots + x_p y_p$; puisque $\mathfrak{o}$ est normal, on a $S \in \mathfrak{o}$. Par ailleurs, $S - xy$ est dans $\mathfrak{h}$ et aussi dans $\mathfrak{M}_1'$; cet élément est donc dans $\mathfrak{M} \cap \mathfrak{h}$. Puisque $y - 1 \in \mathfrak{M} \cap \mathfrak{h}$, on a $x - S \in \mathfrak{M} \cap \mathfrak{h}$, et x est congru modulo $\mathfrak{M} \cap \mathfrak{h}$ à un élément de $\mathfrak{o}$. Soit $F(Y) = (Y - y_1) \ldots (Y - y_p)$ le polynôme minimal de y par rapport à K; la différente de y est donc $F'(y) = (y - y_2) \ldots (y - y_p)$; puisque $y \notin \mathfrak{M}_1'$, $y_j \in \mathfrak{M}_1'$ pour $j > 1$, $F'(y)$ n'est pas dans $\mathfrak{M}_1'$; puisque $F'(y) \in \mathfrak{h}$ cet élément n'est pas dans $\mathfrak{M} \cap \mathfrak{h}$. L'anneau $\mathfrak{h} \cap K(x)$ étant la clôture intégrale de $\mathfrak{o}[y]$ dans $K(x) = K(y)$, il est bien connu que $(F'(y))(\mathfrak{h} \cap K(x)) \subset \mathfrak{o}[y]$. Si on désigne par $\mathfrak{k}_x$ l'anneau local de l'idéal premier $\mathfrak{M} \cap \mathfrak{h} \cap K(x)$, $\mathfrak{k}_x$ est donc aussi l'anneau local de l'idéal premier $\mathfrak{M} \cap \mathfrak{o}[y]$ de $\mathfrak{o}[y]$. Cet idéal contient $\mathfrak{m}$ et $y - 1 = z$; or, tout élément de $\mathfrak{o}[y]$ peut évidemment se mettre sous la forme $b_0 + b_1 z + \ldots + b_{p-1} z^{p-1}$, les b_i étant dans $\mathfrak{o}$; si cet élément est dans $\mathfrak{M}$, il en est de même de b_0, d'où $b_0 \in \mathfrak{m}$, ce qui monter que $\mathfrak{M} \cap \mathfrak{o}[y]$ est engendré par $\mathfrak{m}$ et z. Posons $z_j = y_j - 1$ $(j = 1, \ldots, p)$, $P = z_1 \ldots z_p$, $P' = z_2 \ldots z_p$, d'où $z = P/P'$. On a $P \in K$, d'où $P \in \mathfrak{o}$, et, puisque $z \in M$, $P \in \mathfrak{m}$. On a $P' = P/z \in K(x)$, et, P' étant manifestement entier sur $\mathfrak{o}$, $P' \in \mathfrak{h} \cap K(x)$. Par ailleurs, si $j > 1$, on a $y_j \in \mathfrak{M}_1''$, d'où $z_j \notin \mathfrak{M}_1''$, $P' \notin \mathfrak{M}_1''$; P' n'appartient donc pas à $\mathfrak{M} \cap \mathfrak{h} \cap K(x)$, et la formule $z = P/P'$ montre que z appartient à l'idéal $\mathfrak{m}\mathfrak{k}_x$. Puisque $\mathfrak{M} \cap \mathfrak{o}[y]$ est engendré par $\mathfrak{m}$ et z, on voit que l'idéal maximal de $\mathfrak{k}_x$ est engendré par $\mathfrak{m}$. Ceci montre que $\mathfrak{M} \cap \mathfrak{h} \cap K(x)$ n'est pas ramifié par rapport à $\mathfrak{o}$. Comme nous avons déjà établi que tout élément de $\mathfrak{h}$ est congru (mod $\mathfrak{M} \cap \mathfrak{h}$) à un élément de $\mathfrak{o}$, on voit que $\mathfrak{M} \cap \mathfrak{h} \cap K(x)$ est contrôlé par $\mathfrak{o}$, donc que $\mathfrak{h} \cap K(x)$ est contenu dans l'anneau de décomposition de $\mathfrak{M}$ par rapport à $\mathfrak{o}$. Comme x était un élément quelconque de $\mathfrak{h}$, $\mathfrak{h}$ est contenu dans cet anneau de décomposition, et lui est par suite identique. Nous avons donc établi le

THÉORÈME 3. *Soient* $\mathfrak{o}$ *un domaine d'intégrité noethérien local et normal* *et* $\mathfrak{m}$ *son idéal maximal. Soit* L/K *une extension algébrique séparable du corps des quotients* K *de* $\mathfrak{o}$, *et soit* $\mathfrak{J}$ *la clôture intégrale de* $\mathfrak{o}$ *dans* L; *soit* $\mathfrak{M}$ *un idéal premier de* $\mathfrak{J}$ *tel que* $\mathfrak{M} \cap \mathfrak{o} = \mathfrak{m}$. *Soit* L'/K *une extension normale de* K *contenant* L/K, *et soit* $\mathfrak{M}'$ *un idéal premier de la clôture intégrale de* $\mathfrak{o}$ *dans* L' *tel que* $\mathfrak{M}' \cap \mathfrak{J} = \mathfrak{M}$. *L'anneau de décomposition de* $\mathfrak{M}$ *par rapport à* $\mathfrak{o}$ *est alors l'ensemble des éléments de* $\mathfrak{J}$ *qui sont invariants par tous les automorphismes de* L'/K *qui conservent* $\mathfrak{M}'$.

Soient $\mathfrak{h}$ cet anneau et $\mathfrak{k}$ l'anneau local de $\mathfrak{M} \cap \mathfrak{h}$. Montrons que l'on a

$$\mathfrak{m}^n \mathfrak{k} \cap \mathfrak{o} = \mathfrak{m}^n$$

Soit u un élément de $\mathfrak{m}^n \mathfrak{k} \cap \mathfrak{o}$. Cet élément peut s'écrire sous la forme $\sum_{i=1}^{q} u_i v_i w_i^{-1}$, où les u_i sont dans $\mathfrak{m}^n$, les v_i, w_i dans $\mathfrak{h}$ et où aucun w_i n'est dans $\mathfrak{M}$. Le corps $K(v_1, \ldots, v_q, w_1, \ldots, w_q)$ est engendré par un élément x, que l'on peut supposer appartenir à $\mathfrak{h}$. Utilisons alors, relativement à cet élément, les mêmes notations que plus haut. Il est clair que u appartient à $\mathfrak{m}^n \mathfrak{k}_x$. Il existe donc un élément $t \in \mathfrak{o}[y]$ n'appartenant pas à $\mathfrak{M}$ tel que $tu \in \mathfrak{M}^n \mathfrak{o}[y]$. Rappelons que p désignait le degré de y, donc aussi de z, par rapport à K; tout élément de $\mathfrak{o}[y] = \mathfrak{o}[z]$ se représente donc d'une manière et d'une seule sous forme d'un polynôme de degré $< p$ en z à coefficients dans $\mathfrak{o}$. Posons donc $t = t_0 + t_1 z + \ldots + t_{p-1} z^{p-1}$, avec $t_i \in \mathfrak{o}$ $(0 \leqq i \leqq p-1)$. Puisque $tu \in \mathfrak{m}^n \mathfrak{o}[y]$, les $t_i u$ sont dans $\mathfrak{m}^n$. Par ailleurs, puisque t n'est pas dans $\mathfrak{M}$ et $z \in \mathfrak{M}$, t_0 n'est pas dans $\mathfrak{m}$, d'où $t_0^{-1} \in \mathfrak{o}$ et $u = t_0^{-1}(t_0 u) \in \mathfrak{m}^n$.

On en conclut que la topologie $\mathfrak{m}$-adique de $\mathfrak{o}$ est celle induite par la topologie $\mathfrak{m}\mathfrak{k}$-adique de $\mathfrak{k}$. Comme $\mathfrak{o}$ est dense dans $\mathfrak{k}$ (prop. 1), on en conclut que l'application identique de $\mathfrak{o}$ dans son complété $\hat{\mathfrak{o}}$ se prolonge en un isomorphisme de $\mathfrak{k}$ dans $\hat{\mathfrak{o}}$ et que $\hat{\mathfrak{o}}$ peut s'identifier au complété de $\mathfrak{k}$ relativement à la topologie définie par $\mathfrak{m}\mathfrak{k}$.

M. Nagata a de plus démontré que l'anneau $\mathfrak{k}$ est noethérien. Rappelons ici sa démonstration. Identifions le complété de $\mathfrak{k}$ à l'anneau $\hat{\mathfrak{o}}$. L'anneau $\hat{\mathfrak{o}}$ étant noethérien, il suffira de montrer que, pour tout idéal $\mathfrak{a}$ de $\mathfrak{k}$, on a $\mathfrak{a} = \mathfrak{a}\hat{\mathfrak{o}} \cap \mathfrak{k}$. Soit u un élément de $\mathfrak{a}\hat{\mathfrak{o}} \cap \mathfrak{k}$. Cet élément appartient à l'idéal engendré dans $\hat{\mathfrak{o}}$ par un nombre fini d'éléments $x_1, \ldots, x_n$ de $\mathfrak{a}$. Il existe un élément $x \in \mathfrak{h}$ tel que $x_1, \ldots, x_n$, u appartiennent à l'anneau local $\mathfrak{k}_x$ de l'idéal $\mathfrak{M} \cap \mathfrak{h} \cap K(x)$. Or, nous avons vu que $\mathfrak{M} \cap \mathfrak{h} \cap K(x)$ est contrôlé par $\mathfrak{o}$; son anneau de décomposition par rapport à $\mathfrak{o}$ est donc $\mathfrak{h} \cap K(x)$ tout entier, et il résulte de ce que nous venons de voir que $\hat{\mathfrak{o}}$ s'identifie à la complétion de $\mathfrak{k}_x$. Si $\mathfrak{b}$ est l'idéal engendré par $x_1, \ldots, x_n$ dans $\mathfrak{k}_x$, l'élément u appartient à l'idéal engendré par $\mathfrak{b}$ dans la complétion de $\mathfrak{k}_x$. Or, $K(x)/K$ est une extension séparable finie; $\mathfrak{o}$ étant normal, $\mathfrak{h} \cap K(x)$, qui est entier sur $\mathfrak{o}$, est un $\mathfrak{o}$-module fini, donc un anneau noethérien. L'anneau $\mathfrak{k}_x$ est donc noethérien, et on en conclut que $u \in \mathfrak{b}$, d'où $u \in \mathfrak{a}$, ce qui achève la démonstration.

Appendice

Le théorème de Akizuki et Krull

Soit $\mathfrak{o}$ un domaine d'intégrité noethérien qui ne possède qu'un seul idéal premier $\mathfrak{m} \neq \{0\}$. Nous nous proposons de montrer que l'anneau dérivé normal $\hat{\mathfrak{o}}$ de $\mathfrak{o}$ est noethérien.

Soit $\mathfrak{o}'$ un sous-anneau de $\hat{\mathfrak{o}}$ contenant $\mathfrak{o}$ et fini sur $\mathfrak{o}$. Nous nous proposonos de montrer que, pour tout élément $x \neq 0$ de $\mathfrak{m}$, la longueur du $\mathfrak{o}'$-module $\mathfrak{o}'/\mathfrak{o}'x$ est au plus égale à celle du $\mathfrak{o}$-module $\mathfrak{o}/\mathfrak{o}x$. Pour ce faire, remarquons que, pour tout $n > 0$, la longueur de $\mathfrak{o}x^n/\mathfrak{o}x^{n+1}$ est égale à la longueur h de $\mathfrak{o}/\mathfrak{o}x$; car l'application $t \to tx^n$ est un isomorphisme de $\mathfrak{o}$ sur $\mathfrak{o}x^n$ qui applique $\mathfrak{o}x$ sur $\mathfrak{o}x^{n+1}$. On en conclut que, si $m > 0$, la longueur de $\mathfrak{o}x^n/\mathfrak{o}x^{n+m}$ est mh. Par ailleurs, puisque $\mathfrak{o}'$ est entier et fini sur $\mathfrak{o}$, il y a un élément $d \in \mathfrak{o}$, $d \neq 0$, tel que $\mathfrak{o}'d \subset \mathfrak{o}$. L'idéal $\mathfrak{o}d$ étant primaire pour l'unique idéal maximal $\mathfrak{m}$ de $\mathfrak{o}$ (si, comme on peut le supposer, $d \in \mathfrak{m}$), il y a une puissance de $\mathfrak{m}$ contenue dans $\mathfrak{o}d$, donc aussi un exposant $a > 0$ tel que $x^a \in \mathfrak{o}d$, d'où $\mathfrak{o}'x^a \subset \mathfrak{o}$. Tout idéal de $\mathfrak{o}'$ contenu dans $\mathfrak{o}'x^a$ est donc un idéal de $\mathfrak{o}$; de plus, si cet idéal contient $\mathfrak{o}'x^{a+n}$, il contient *a fortiori* $\mathfrak{o}x^{a+n}$. La longueur de $\mathfrak{o}'x^a/\mathfrak{o}'x^{a+n}$ est donc au plus égale à celle, $(a+n)h$, de $\mathfrak{o}/\mathfrak{o}x^{a+n}$. Par ailleurs, cette longueur est nh', si h' est la longueur de $\mathfrak{o}'/\mathfrak{o}'x$; on a donc $nh' \leqq h(a+n)$. La validité de cette formule pour tout $n > 0$ entraîne $h' \leqq h$. Ceci dit, supposons pour un moment qu'il existe une suite infinie strictement croissante $(\hat{\mathfrak{a}}_i)$ d'idéaux de $\hat{\mathfrak{o}}$. On peut supposer que $\hat{\mathfrak{a}}_1 \neq 0$; on peut alors trouver un élément $x \neq 0$ dans $\hat{\mathfrak{a}}_1 \cap 0$. Soit h la longueur de $\mathfrak{o}/\mathfrak{o}x$. Pour chaque i, soit y_i un élément de $\hat{\mathfrak{a}}_{i+1}$ non contenu dans $\hat{\mathfrak{a}}_i$, et soit $\mathfrak{o}' = \mathfrak{o}[y_1, \ldots, y_h]$. Les idéaux $\mathfrak{o}' \cap \hat{\mathfrak{a}}_1, \ldots, \mathfrak{o}' \cap \hat{\mathfrak{a}}_{h+1}$ de $\mathfrak{o}'$ sont alors tous distincts les uns des autres et de $\mathfrak{o}'$; de plus, ils contiennent tous $\mathfrak{o}'x$. L'anneau $\mathfrak{o}'$ est fini sur $\mathfrak{o}$, et la longueur de $\mathfrak{o}'/\mathfrak{o}'x$ est $\geqq h+1$, d'où contradiction.

Le même raisonnement prouve manifestement que tout anneau intermédiaire entre $\mathfrak{o}$ et $\hat{\mathfrak{o}}$ est noethérien (résultat dû à Akizuki).

Par ailleurs, il y a au moins un idéal premier $\hat{\mathfrak{m}}$ de $\hat{\mathfrak{o}}$ dont l'intersection avec $\mathfrak{o}$ est $\mathfrak{m}$, et il est bien connu que l'anneau local de $\hat{\mathfrak{m}}$ est un anneau de valuation discrète non triviale $\mathfrak{v}$; $\mathfrak{v}$ contient donc $\mathfrak{o}$, et son idéal maximal contient $\mathfrak{m}$: c'est le résultat utilisé dans le texte.

RÉFÉRENCES

[1] Y. Akizuki. Einige Bemerkungen über primäre Integritätsbereiche mit Teilerkettensatz, Proc. Phys. Math. Soc. Japan, **17**, 1935.

[2] Cohen and Seidenberg, Prime ideals and integral dependance, Bull. Amer. Math. Soc., **52**, 1946.

[3] W. Krull, Ein Satz über primäre Integritätsbereiche, Math. Ann., **103**, 1930.

[4] M. Nagata, On the theory of Henselian rings, Nagoya Math. Journ., **5**, 1953.

[5] P. Samuel, Algèbre locale, Mémorial des Sciences Mathématiques, fasc. 123, Paris, Gauthier-Villars, 1953.

Université du Nagoya