BULLETIN DE LA S. M. F.

JEAN DIEUDONNÉ

Sur la théorie de la divisibilité

Bulletin de la S. M. F., tome 69 (1941), p. 133-144

<http://www.numdam.org/item?id=BSMF_1941__69__133_0>

SUR LA THÉORIE DE LA DIVISIBILITÉ;

PAR M. JEAN DIEUDONNÉ.

Introduction.

Comme l'a clairement reconnu le premier Dedekind [1], la théorie de la *divisibilité* dans un anneau d'intégrité commutatif, est essentiellement l'étude d'un *groupe ordonné*. On appelle ainsi un groupe abélien, dans lequel est définie une relation d'ordre [2] *invariante par translation* : si le groupe G est noté multiplicativement, par exemple, et la relation d'ordre notée $a\mathrm{R}b$, cela signifie que $x\mathrm{R}y$ entraîne $(xz)\mathrm{R}(yz)$ quel que soit z. Si A est un anneau d'intégrité, K son corps des quotients, K^* l'ensemble des éléments $\neq 0$ de K, la relation « a divise b » (c'est-à-dire $b = ca$, où $c \in \mathrm{A}$) devient une relation d'ordre dans le groupe multiplicatif K^*, après qu'on a identifié les éléments de K^* qui ne diffèrent que par un facteur de A *diviseur de l'unité*; autrement dit, c'est une relation d'ordre dans le groupe multiplicatif K^*/E, où E est le groupe des diviseurs de l'unité dans A; et cette relation fait de K^*/E un *groupe ordonné*, dont l'étude constitue la théorie de la *divisibilité* dans A. Ce groupe est d'ailleurs isomorphe au groupe multiplicatif des *idéaux principaux* non nuls de K, ordonné par la relation $(a) \supset (b)$.

Les groupes ordonnés les plus intéressants sont les groupes *réticulés*, c'est-à-dire les groupes dans lesquels deux éléments quelconques ont une *borne supérieure* (et par suite une *borne inférieure*); dans la théorie de la divisibilité « borne inférieure »

---

[1] DEDEKIND, *Werke*, t. II, p. 126-135.

[2] Pour la terminologie relative aux *ensembles ordonnés* (borne supérieure, ensemble totalement ordonné, théorème de Zorn, etc.), voir N. BOURBAKI, *Éléments de Mathématique*, Livre I (fasc. de résultats), § 6 (*Actual. Scient. et Ind.*, n° 846).

se traduit par « plus grand commun diviseur », « borne supérieure » par « plus petit commun multiple ».

On sait qu'en général, le groupe ordonné K^*/E n'est pas réticulé; il en est ainsi, en particulier, dans la plupart des corps de nombres algébriques K, et c'est pour tourner cet obstacle que Dedekind créa la théorie des *idéaux*, dont le principe consiste essentiellement à *plonger* le groupe des idéaux principaux non nuls de K dans le groupe de tous les idéaux non nuls de K, qui, lui, est réticulé, dans le cas envisagé par Dedekind.

On peut se demander à quelle condition un groupe ordonné peut ainsi être plongé dans un groupe réticulé; cette question a été résolue tout récemment par M. Lorenzen (3), comme cas particulier de résultats plus généraux, découlant de la théorie des « *r*-systèmes d'idéaux » de cet auteur. Dans le paragraphe 1 de ce travail, je donne une démonstration directe de ce théorème (4). Les anneaux d'intégrité A tels que la condition de Lorenzen s'applique au groupe K^*/E peuvent être appelés anneaux *semi-clos*; en effet, tout anneau *clos* (= « ganz-abgeschlossen ») satisfait à cette condition, mais la réciproque n'est pas vraie, comme je le montre par la formation d'un exemple.

Il est bien connu que la théorie de Dedekind n'est pas applicable à un anneau clos quelconque : dans un tel anneau, les idéaux de Dedekind ne forment pas un groupe multiplicatif, en général. Les travaux de Van der Waerden (5) et Prüfer (6) ont conduit à distinguer plusieurs catégories d'anneaux clos, suivant les propriétés de certains sous-ensembles de l'ensemble des idéaux de Dedekind (v-idéaux, a-idéaux). Dans le paragraphe 2, je résous une question laissée ouverte par Prüfer (*loc. cit.*) : parmi les anneaux clos qu'il considère figurent en particulier ceux qui satisfont à l'une des trois propriétés qu'il désigne

(3) Lorenzen, *Math. Zeit.*, t. 45, 1939, p. 533-553.

(4) Cette démonstration, comme celle de Lorenzen lui-même, s'apparente à une démonstration d'un théorème analogue de Krull, *Idealtheorie* (*Erg. der Math.*, t. 4, fasc. 3, p. 111).

(5) Van der Waerden, *Math. Ann.*, t. 101, 1929, p. 293-308, et *Moderne Algebra*, t. 2 (1re éd.), p. 106.

(6) Prüfer, *Journ. de Crelle*, t. 168, 1932, p. 1-36. *Voir* aussi A. H. Clifford, *Ann. of Math.*, t. 39, 1938, p. 594-610.

par (V_β), (V_γ) et (V_δ) ; (V_β) entraîne (V_γ) et (V_γ) entraîne (V_δ), mais la question de savoir si ces propriétés sont ou non équivalentes n'est pas tranchée. Il résulte aisément d'un théorème de Lorenzen (*loc. cit.*) que (V_γ) et (V_δ) sont *équivalentes*; par contre, je donne un exemple d'anneau prouvant que (V_δ) *n'entraîne pas* (V_β). M. Lorenzen a donné un exemple prouvant ce même fait pour un groupe ordonné (*loc. cit.*, p. 551) ; mais cet exemple ne résout pas entièrement la question initiale de Prüfer, car il n'est nullement prouvé qu'étant donné un groupe ordonné G (et en particulier le groupe donné en exemple par Lorenzen), il existe un anneau d'intégrité dont le groupe des idéaux principaux soit isomorphe à G.

1.

Les groupes ordonnés que nous considérerons seront notés *multiplicativement*, et la relation d'ordre, dans ces groupes, écrite $a \leqq b$; 1 désigne l'élément unité d'un tel groupe.

Théorème (Lorenzen). — *Pour qu'un groupe ordonné* G *soit isomorphe à un sous-groupe d'un groupe réticulé, il faut et il suffit que, dans* G, *la condition* $x^n \geqq 1$ (n *entier* > 0) *entraîne* $x \geqq 1$. D'après un théorème de Dedekind [7], la condition est satisfaite par tout groupe réticulé, et par suite aussi par tout sous-groupe d'un groupe réticulé.

Pour voir que la condition est *suffisante*, nous allons montrer que, si elle est remplie, G est isomorphe à un sous-groupe d'un *produit direct* de groupes *totalement ordonnés* [8] ; il est immédiat qu'un tel produit est réticulé.

Désignons par G_+ l'ensemble des éléments $x \geqq 1$ de G, et soit a un élément *n'appartenant pas à* G_+. Soit $\mathfrak{M}_a$ l'ensemble des parties P de G satisfaisant aux quatre conditions suivantes :

1° $a \notin P$; 2° $G_+ \subset P$ et $a^{-1} \in P$; 3° $P.P \subset P$; 4° si $x^n \in P$ pour n entier > 0, $x \in P$.

(7) *Loc. cit.*, p. 128.

(8) Si (G_α) est une famille quelconque de groupes ordonnés (finie ou non), le produit direct G de ces groupes est ordonné par la relation suivante : on pose $(x_\alpha) \leqq (y_\alpha)$ si $x_\alpha \leqq y_\alpha$ *quel que soit* α.

Montrons d'abord que $\mathcal{M}_a$ *n'est pas vide*. A cet effet, considérons l'ensemble P_0 des $x \in G$ ayant la propriété suivante : il existe deux entiers $m > 0$, $n \geqq 0$, et un élément $y \geqq 1$ de G tels que $x^m = a^{-n}y$. Il est immédiat que P_0 satisfait aux trois dernières conditions imposées aux ensembles de $\mathcal{M}_a$; il satisfait aussi à la première, car si l'on avait $a^m = a^{-n}y$, avec $y \geqq 1$, on en conclurait $a^{m+n} = y \geqq 1$, d'où $a \geqq 1$ d'après l'hypothèse sur G, ce qui contredirait le choix de a.

En second lieu, $\mathcal{M}_a$ est un ensemble *inductif* quand on l'ordonne par inclusion : si $\mathcal{G}$ est une partie totalement ordonnée de $\mathcal{M}_a$, et Q la réunion des $P \in \mathcal{G}$, il est clair que Q satisfait aux conditions 1°, 2° et 4° des ensembles de $\mathcal{M}_a$; d'autre part, si $x \in Q$ et $y \in Q$, il existe un $P \in \mathcal{G}$ tel que $x \in P$ et $y \in P$ (puisque $\mathcal{G}$ est totalement ordonnée), donc $xy \in P.P \subset P \subset Q$.

D'après le théorème de Zorn, $\mathcal{M}_a$ possède donc un élément *maximal* P_a. Nous allons voir que, si b est un élément quelconque de G, on a, ou bien $b \in P_a$, ou bien $b^{-1} \in P_a$. En effet supposons qu'on ait $b \notin P_a$; considérons l'ensemble P' des $x \in G$ ayant la propriété suivante : il existe deux entiers $m > 0$, $n \geqq 0$ et un élément $y \in P_a$ tels que $x^m = b^{-n}y$. P' appartient à $\mathcal{M}_a$: il suffit pour le voir de vérifier la condition $a \notin P'$; or, si l'on avait $a^m = b^{-n}y$, on en tirerait d'abord $n > 0$ (sans quoi on aurait $a^m \in P_a$, donc $a \in P_a$ contrairement au fait que $P_a \in \mathcal{M}_a$), puis $b^n = a^{-m}y$, donc $b^n \in P_a$, et par suite $b \in P_a$, contrairement à l'hypothèse. Comme P_a est maximal, et $P_a \subset P'$, on a nécessairement $P_a = P'$, donc $b^{-1} \in P_a$.

Soit H_a l'intersection de P_a et de P_a^{-1} (ensemble des x^{-1} lorsque x parcourt P_a); il est immédiat que H_a est un *sous-groupe* de G; en outre, le groupe quotient $G_a = G/H_a$ est *totalement ordonné* si l'on définit la relation $\dot{x} \leqq \dot{y}$ entre deux classes (mod. H_a) comme équivalente à la relation : il existe $x \in \dot{x}$ et $y \in \dot{y}$ tels que $yx^{-1} \in P_a$. Soit f_a l'application canonique de G sur G_a; la relation $x \geqq 1$ entraîne $f_a(x) \geqq 1$ (puisque $G_+ \subset P_a$), et l'on a $f_a(a) < 1$.

Considérons alors le *produit direct* G' de tous les groupes G_a, lorsque a parcourt le complémentaire de G_+ dans G; et soit f l'application $x \to (f_a(x))$ de G dans G'; f est évidemment une *représentation croissante* de G dans G'; montrons que c'est un *isomorphisme* du groupe ordonné G sur le sous-groupe ordonné $f(G)$ de G'. En effet, on ne peut avoir $f(a) = 1$ que si $a = 1$; car si $a \notin G_+$ on a $f_a(a) < 1$, et si $a > 1$, $a^{-1} \notin G_+$ donc $f(a^{-1}) = [f(a)]^{-1} \neq 1$, d'où $f(a) \neq 1$. En second lieu, la condition $f(x) \geqq 1$ entraîne $x \geqq 1$, puisque si $x \notin G_+$, $f_x(x) < 1$.

C. Q. F. D.

Appliqué au groupe multiplicatif K^*/E correspondant à un anneau d'intégrité A, le théorème de Lorenzen donne le résultat suivant : pour que le groupe K^*/E soit isomorphe à un sous-groupe d'un groupe réticulé, il faut et il suffit que tout élément x de K tel que $x^n \in A$ pour un entier $n > 0$, appartienne lui-même à A. Autrement dit, si $x \in K$ satisfait à une *équation binome* $x^n = a$, où $a \in A$, on doit avoir nécessairement $x \in A$. Tout anneau *clos* A satisfait évidemment à cette condition, puisque, plus généralement, tout $x \in K$ satisfaisant à une équation $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ à coefficients dans A, est alors un élément de A. Nous appellerons *semi-clos* les anneaux d'intégrité pour lesquels le groupe K^*/E peut être plongé dans un groupe réticulé.

Exemple d'un anneau semi-clos et non clos. — Soit Ω le corps de *tous* les nombres algébriques, Ω_0 le sous-ensemble de Ω formé des nombres algébriques θ « exprimables par radicaux » (c'est-à-dire tels que le groupe de Galois de l'équation irréductible à laquelle satisfait θ soit *résoluble*); il est immédiat que Ω_0 est un *sous-corps* de Ω. Considérons l'anneau A formé des *polynomes* $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, dont le premier coefficient a_0 appartient à Ω_0, et les autres à Ω. Le corps des quotients K de A contient évidemment Ω (puisque la fraction rationnelle $\frac{a_1 x}{x}$ appartient à K, quel que soit $a_1 \in \Omega$); il en résulte que A *n'est pas clos*, car il existe des nombres algébriques θ non exprimables par radicaux, satisfaisant par suite à une équation

$$x^n + r_1 x^{n-1} + \ldots + r_n = 0$$

à coefficients rationnels (donc dans A), bien que n'appartenant pas à A. Par contre A est *semi-clos*; supposons en effet que g soit un polynome de A, f une fraction rationnelle de K, telle que $f^n = g$ (n entier > 0); A est contenu dans l'anneau $\Omega[x]$ des polynomes sur Ω, et K dans le corps des quotients $\Omega(x)$ de $\Omega[x]$; comme

$\Omega[x]$ est *clos*, f appartient nécessairement à $\Omega[x]$; en outre, si l'on pose

$$f(x) = a_0 + a_1 x + \ldots + a_p x^p, \qquad g(x) = b_0 + b_1 x + \ldots + b_q x^q,$$

on a $a_0^n = b_0$, et comme b_0 appartient à Ω_0, il en est de même de a_0, d'après la définition du corps Ω_0; donc f appartient à A.

2.

Rappelons brièvement les définitions et résultats principaux de la théorie des *v-idéaux* de Van der Waerden et Prüfer (*loc. cit.*). Soit A un anneau d'intégrité, H une partie quelconque de K^*; on désignera par $d(H)$ l'ensemble des éléments de K^* qui divisent *tous* les éléments de H, par $m(H)$ l'ensemble des éléments de K^* qui sont multiples de *tous* les éléments de H. Il est immédiat que $H \subset H'$ entraîne $d(H) \supset d(H')$ et $m(H) \supset m(H')$; d'autre part, on a $H \subset m[d(H)]$, et $H \subset d[m(H)]$. L'ensemble $m[d(H)]$ est appelé le *v-idéal* (9) *engendré par* H et se note $[H]$; on vérifie aisément que $\big[[H]\big] = [H]$; $[H]$ n'est vide que si H est vide; $[H]$ n'est égal à K^* que si $d(H)$ est vide. Si H est l'ensemble des éléments d'une suite finie $a_1, a_2, \ldots, a_n$, on écrit $[a_1, \ldots, a_n]$ au lieu de $[H]$; en particulier $[a]$ n'est autre que l'idéal principal (a) $\big(= m(a)\big)$; un v-idéal engendré par un nombre fini d'éléments est dit *de type fini*. La relation $H \subset H'$ entraîne $[H] \subset [H']$.

Nous ne considérerons plus désormais que des parties H de K^* non vides, et telles que $d(H)$ soit non vide; soit $\mathfrak{M}$ l'ensemble des v-idéaux correspondants. Si B et C sont deux parties de K^*, on montre sans peine que $[B.C] = \big[[B].C\big] = \big[[B].[C]\big]$ (B.C désignant, comme d'ordinaire, l'ensemble des produits xy, où x parcourt B et y parcourt C). Ceci conduit à définir le *produit* $\mathfrak{ab}$ de deux v-idéaux $\mathfrak{a}$, $\mathfrak{b}$ de $\mathfrak{M}$ comme égal au v-idéal $[\mathfrak{a}.\mathfrak{b}]$ (10). Cette loi de composition, ainsi définie dans $\mathfrak{M}$, est

(9) Cette dénomination provient du fait que la réunion de $m[d(H)]$ et de l'élément zéro, lorsque H et $d(H)$ ne sont pas vides, est un *idéal* (fractionnaire) au sens de Dedekind; mais la réciproque n'est pas vraie en général.

(10) On aura soin de ne pas confondre cette opération avec le produit de deux idéaux, au sens de Dedekind; le produit de $\mathfrak{a}$ et $\mathfrak{b}$, au sens de Dedekind, est contenu dans $[\mathfrak{a}.\mathfrak{b}]$, mais en est en général distinct.

associative et commutative; elle a pour élément unité $A = [1]$; la relation $\mathfrak{a} \subset \mathfrak{b}$ entraîne $\mathfrak{ac} \subset \mathfrak{bc}$; comme $[a][b] = [ab]$, on voit que la loi de composition et la relation d'ordre dans $\mathcal{M}$ *prolongent* respectivement la multiplication et la relation d'ordre dans le groupe ordonné G des idéaux principaux de K^*. Il s'en suit immédiatement que, si $\mathcal{M}$ est un *groupe*, c'est un *groupe réticulé* (car le v-idéal engendré par la *réunion* $\mathfrak{a} \cup \mathfrak{b}$ est le plus petit v-idéal contenant à la fois $\mathfrak{a}$ et $\mathfrak{b}$) dont G est un sous-groupe; on comprend donc l'intérêt que présentent les v-idéaux dans la théorie de la divisibilité.

En général $\mathcal{M}$ n'est pas un groupe; pour qu'il le soit, il faut et il suffit, d'après un théorème de Van der Waerden ([11]), que l'anneau A soit *complètement clos*, c'est-à-dire possède la propriété suivante : si x est un élément de K^* tel qu'il existe un élément $c \in A$ tel que $cx^n \in A$ pour *tout* entier $n > 0$, x appartient nécessairement à A.

Au lieu de considérer l'ensemble $\mathcal{M}$, on peut seulement, avec Prüfer, prendre l'ensemble $\mathcal{M}_f$ des v-idéaux *de type fini*; le produit de deux v-idéaux de $\mathcal{M}_f$ appartient encore à $\mathcal{M}_f$; lorsque $\mathcal{M}_f$ est un *groupe*, c'est encore un groupe *réticulé* dont G est un sous-groupe. Prüfer désigne par (V_β) la propriété « $\mathcal{M}_f$ est un groupe », ou, ce qui revient au même : « tout élément de $\mathcal{M}_f$ a un inverse appartenant à $\mathcal{M}_f$ »; il considère en outre les deux propriétés suivantes de $\mathcal{M}_f$:

(V_γ) Si trois v-idéaux $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ de $\mathcal{M}_f$ sont tels que $\mathfrak{ab} = \mathfrak{ac}$, on a $\mathfrak{b} = \mathfrak{c}$ (autrement dit, tout élément de $\mathcal{M}_f$ est *régulier* pour la multiplication).

(V_δ) Tout v-idéal $\mathfrak{a}$ de $\mathcal{M}_f$ possède la propriété suivante : si x est un élément de K tel que $x.\mathfrak{a} \subset \mathfrak{a}$, on a $x \in A$.

On voit aisément ([12]) que (V_β) entraîne (V_γ), et que (V_γ) entraîne (V_δ). En outre, (V_δ) *entraîne* (V_γ), et lui est donc *équivalente*, en vertu du théorème suivant de Lorenzen ([13]) : *pour que le v-idéal $\mathfrak{a}$ soit inversible dans $\mathcal{M}$, il faut et il suffit que la*

([11]) *Moderne Algebra*, t. 2 (2ᵉ éd.), p. 94.
([12]) PRÜFER, *loc. cit.*
([13]) *Loc. cit.*, p. 538.

relation $x.\mathfrak{a} \subset \mathfrak{a}$ *entraîne* $x \in A$. D'après ce théorème, (V_δ) signifie que tout v-idéal de type fini est *inversible dans* $\mathfrak{M}$, et *a fortiori, régulier dans* $\mathfrak{M}$, donc aussi *régulier dans* $\mathfrak{M}_f$.

Nous utiliserons encore le résultat suivant ([14]) : si, pour une partie H de K^*, on désigne par $i(H)$ l'ensemble des inverses x^{-1} des éléments x de H ([15]), l'inverse d'un v-idéal inversible $\mathfrak{a}$ est identique à $m[i(\mathfrak{a})] = i[d(\mathfrak{a})]$.

3.

Nous allons maintenant montrer que (V_δ) [équivalente à (V_γ)] *n'entraîne pas* (V_β), en construisant un exemple d'anneau A dans lequel (V_δ) est vérifiée, mais non (V_β).

La condition (V_δ) est certainement vérifiée si A est *complètement clos*, puisqu'alors $\mathfrak{M}$ est un groupe, et par suite tout v-idéal est inversible. Pour que $\mathfrak{M}_f$ soit un *sous-groupe* de $\mathfrak{M}$, il faut et il suffit alors que l'*inverse d'un v-idéal de type fini soit de type fini*. Dans l'anneau A que nous allons construire cette condition *ne sera pas vérifiée*, ce qui établira notre assertion.

K désignant un corps commutatif quelconque, nous désignerons par K_x le système hypercomplexe ayant pour base les éléments x^α, où α parcourt l'ensemble des nombres réels $\geqq 0$, et où la table de multiplication est donnée par les relations $x^\alpha . x^\beta = x^{\alpha+\beta}$. Les éléments de l'anneau K_x sont donc les sommes de la forme $\sum\limits_\alpha a_\alpha x^\alpha$, où l'indice α parcourt l'ensemble des nombres réels $\geqq 0$, mais de sorte que l'élément a_α de K ne soit $\neq 0$ que pour un nombre *fini* de valeurs de α; pour abréger, nous appellerons encore *polynomes en* x ces éléments; la plus grande (resp. la plus petite) valeur de α telle que $a_\alpha \neq 0$ sera dite le *degré maximum* (resp. *degré minimum*) ou simplement *degré* du polynome. On vérifie aussitôt que le terme de degré maximum (resp. minimum) d'un produit de deux polynomes est égal au produit des termes de degré maximum

---

([14]) LORENZEN, *loc. cit.*

([15]) Nous utilisons cette notation afin de réserver la notation $\mathfrak{a}^{-1}$ à l'*inverse* d'un v-idéal $\mathfrak{a}$ dans $\mathfrak{M}$ (lorsqu'il existe), ensemble qu'il faut bien se garder de confondre avec $i(\mathfrak{a})$.

(resp. minimum) des deux facteurs, ce qui entraîne que K_x est un *anneau d'intégrité*. Cette même remarque prouve qu'un polynome f ne peut diviser un monome $ax^\alpha (a \neq 0)$ que s'il est lui-même un monome bx^β, avec $\beta \leqq \alpha$.

Faisons encore la remarque suivante : si $f = gh$ est un produit de deux polynomes tels que les exposants des termes de f et g appartiennent tous à un même sous-groupe Γ du groupe additif des nombres réels, alors les exposants de h appartiennent aussi à Γ; sinon, dans le produit gh, le terme provenant du produit du terme de degré maximum de g par le terme de h dont l'exposant est le plus grand de ceux n'appartenant pas à Γ, ne pourrait se réduire avec aucun autre, et ne pourrait être égal à aucun terme de f.

On peut généraliser dans K_x le processus de la *division euclidienne* :

Lemme 1. — *Soient f et g deux polynomes de K_x de degrés maxima α et β; il existe deux polynomes q et r, tels que $f = qg + r$, et que le degré maximum de r soit $< \beta$.*

Il suffit de considérer le cas où $\alpha > \beta$. Soit μ la plus petite valeur de la différence de deux exposants consécutifs de g (rangés par ordre croissant); nous allons montrer qu'on peut trouver un polynome h tel que le degré maximum de $f - gh$ soit $\leqq \gamma = \mathrm{Max}(\beta, \alpha - \mu)$; un raisonnement de récurrence évident démontrera alors le lemme. Or, si $a_\alpha x^\alpha + a_{\alpha_1} x^{\alpha_1} + \ldots + a_{\alpha_p} x^{\alpha_p}$ est la somme des termes de f dont l'exposant est $> \gamma$ et $b_\beta x^\beta$ le terme de plus haut degré de g, il suffit de prendre

$$h = \frac{a_\alpha}{b_\beta} x^{\alpha-\beta} + \frac{a_{\alpha_1}}{b_\beta} x^{\alpha_1-\beta} + \ldots + \frac{a_{\alpha_p}}{b_\beta} x^{\alpha_p-\beta}.$$

Ce lemme va nous permettre de démontrer la propriété suivante :

Lemme 2. — *K_x est complètement clos.*

En effet, supposons qu'il existe trois polynomes $\neq 0$, f, g, h, tels que g^n divise hf^n quel que soit n; nous allons en conclure que g divise f. En effet, on peut écrire $f = qg + r$, où le degré γ de r

est strictement inférieur au degré β de g; g divise $hf = hqg + hr$, donc il divise hr; nous allons voir par récurrence que g^n divise hr^n. En effet, g^n divise

$$hf^n = h \sum_{p=0}^{n} \binom{n}{p} q^{n-p} g^{n-p} r^p$$

et l'on voit, d'après l'hypothèse, que g^n divise tous les termes de la somme du second membre, à l'exception éventuelle du dernier hr^n; donc g^n divise aussi hr^n. Or, cette conclusion est absurde si $r \neq 0$, car si μ est le degré de h, on en déduit $n\beta \leqq \mu + n\gamma$ quel que soit n, ce qui contredit l'inégalité $\gamma < \beta$.

Nous désignerons par $\overline{K}_x$ le corps des quotients de K_x, formé des « fractions rationnelles » $\frac{f}{g}$, où f et g sont deux éléments quelconques de $K_x (g \neq 0)$.

Soit maintenant $K_{x,y}$ l'ensemble des polynomes (au sens ci-dessus) en y, dont les coefficients sont des polynomes de K_x (ou encore le système hypercomplexe sur K dont une base est formée des éléments $x^\alpha y^\beta$, avec $(x^\alpha y^\beta)(x^\gamma y^\delta) = x^{\alpha+\gamma} y^{\beta+\delta}$). $K_{x,y}$ est contenu dans l'anneau $(\overline{K}_x)_y$ des polynomes en y à coefficients dans le corps $\overline{K}_x$; c'est donc un anneau d'intégrité. En outre :

Lemme 3. — $K_{x,y}$ *est complètement clos.*

En effet, soient f, g, h trois polynomes $\neq 0$ de $K_{x,y}$ tels que g^n divise hf^n quel que soit n; g^n divise *a fortiori* hf^n dans l'anneau $(\overline{K}_x)_y$, qui est complètement clos d'après le lemme 2; donc g divise f *dans cet anneau*, c'est-à-dire qu'il existe un polynome $q \in K_{x,y}$ et un polynome $u \in K_x$ tels que $uf = gq$. On en tire que u^n divise hq^n, c'est-à-dire divise tous les coefficients de ce dernier polynome, considéré comme polynome en y. Si β est le degré de u, on peut, en faisant la division euclidienne de chacun des coefficients de q par u, mettre q sous la forme $q = uq_1 + r$, où r est un polynome en y dont les coefficients sont des polynomes en x de degré $< \beta$. Par le même raisonnement que dans le lemme 2, on voit que u^n divise hr^n, c'est-à-dire tous les coefficients de ce polynome en y. Or, si $\gamma < \beta$ est le plus grand des degrés des coefficients de r, μ le plus grand des degrés des coefficients de h, les coefficients de hr^n qui ne sont pas nuls ont un degré $\leqq \mu + n\gamma$, quantité qui est $< n\beta$ pour n assez grand; ces coefficients sont donc tous nuls pour n assez grand; mais comme $K_{x,y}$ est un anneau d'intégrité, cela entraîne $r = 0$, donc u divise tous les coefficients de q, ce qui achève la démonstration.

Soit maintenant θ un nombre réel > 0 quelconque, et soit G_θ le sous-anneau de $K_{x,y}$ engendré par les monomes $x^\alpha y^\beta$ tels que $\beta \geqq \theta\alpha$. G_θ est un anneau *isomorphe* à $K_{x,y}$, car l'application $(x, y) \rightarrow (xy^\theta, y)$ fait correspondre biunivoquement aux monomes $x^\alpha y^\beta$ engendrant $K_{x,y}$, les monomes $x^\alpha y^\beta$ tels que $\beta \geqq \theta\alpha$, et de sorte qu'au produit de deux monomes corresponde le produit des deux monomes correspondants. Donc G_θ est *complètement clos* d'après le lemme 3.

Supposons maintenant que θ soit un nombre *irrationnel* et < 1; nous définirons l'anneau A comme le sous-anneau de G_θ engendré par les monomes $x^\alpha y^\beta$ tels que α et β soient *rationnels* (et satisfassent à l'inégalité $\beta > \theta\alpha$). Si f et g sont deux polynomes de A tels que g divise f dans G_θ, g divise aussi f *dans* A; en effet, si $h = \frac{f}{g}$, les exposants de h, considéré comme polynome en x, sont rationnels d'après une remarque antérieure, et il en est de même des exposants de h, considéré comme polynome en y.

Comme G_θ est complètement clos, il résulte aussitôt de cette remarque que A est, lui aussi, *complètement clos*.

Considérons maintenant, dans le corps des quotients (privé du zéro) de A, que nous désignerons par H, le v-idéal $\mathfrak{a}$ engendré par les deux éléments y et xy de A. Nous allons examiner ce que sont les éléments de son inverse $\mathfrak{a}^{-1}$ dans le groupe $\mathcal{M}$ des v-idéaux.

Tout diviseur de y dans A est de la forme $\frac{y}{h}$, où h est un polynome de A; pour que ce soit aussi un diviseur de xy, il faut et il suffit que xh soit un polynome de A. L'inverse $\mathfrak{a}^{-1}$ étant égal à $m(i(\mathfrak{a})) = i(d(\mathfrak{a}))$, est donc l'ensemble des $\frac{h}{y}$, où h est un polynome de A tel que $xh \in$ A : autrement dit, les monomes $x^\alpha y^\beta$ qui figurent dans h doivent être tels que $\beta > \theta(\alpha + 1)$. En particulier pour que y^β appartienne à $\mathfrak{a}^{-1}$, il faut et il suffit que $\beta > \theta - 1$.

Nous allons en déduire que $\mathfrak{a}^{-1}$ *n'est pas de type fini.* Supposons-le en effet engendré par un nombre fini d'éléments $\frac{h_i}{y}$; pour tous les monomes $x^\alpha y^\beta$ qui figurent dans les h_i, on a $\beta - \theta\alpha > \theta$; comme ces monomes sont en nombre fini, et que α et β sont *rationnels*, le minimum ρ des expressions $\beta - \theta\alpha$ est $> \theta$. Soient alors λ et μ deux nombres rationnels tels que $\rho - 1 > \lambda > \mu > \theta - 1$: y^λ et y^μ appartiennent à $\mathfrak{a}^{-1}$; d'autre part, y^λ divise tous les $\frac{h_i}{y}$, donc serait un diviseur commun de tous les éléments de $\mathfrak{a}^{-1}$, et en particulier de y^μ, ce qui est absurde.