CHAPITRE II

ANNEAU DE POLYNÔMES SUR UN ANNEAU FACTORIEL

THÉORÈME 1 - *Si A est un anneau noethérien, alors l'anneau $A[X]$ est aussi noethérien* (Théorème de la base finie de Hilbert; cf. D. Hilbert, Ueber die Theorie der algebraischen Formen, Math. Ann. 36 (1890), 473).

Étant donné un idéal $\mathfrak{a}$ de $A[X]$, on notera par $d_n(\mathfrak{a})$ l'ensemble formé par les coefficients dominants des polynômes de degré n appartenant à l'idéal $\mathfrak{a}$ et par l'élément 0. Les propriétés suivantes sont vérifiées:

(1) *pour tout entier $n \geq 0$, $d_n(\mathfrak{a})$ est un idéal de A.* En effet, soient a et b deux éléments de $d_n(\mathfrak{a})$; ou bien $a+b=0 \in d_n(\mathfrak{a})$, ou bien $a+b \neq 0$. Dans ce dernier cas, soient $f(X)=aX^n+a_1X^{n-1}+\ldots$ et $g(X)=bX^n+b_1X^{n-1}+\ldots$ des polynômes de $\mathfrak{a}$ dont les coefficients dominants sont a et b respectivement. Alors $f(X)+g(X)$ est un polynôme de $\mathfrak{a}$ et son coefficient dominant est $a+b$. Ceci nous montre que

$a+b\in d_n(\mathfrak{a})$. Si $c\in A$, alors le coefficient dominant de $cf(X)\in\mathfrak{a}$ est ca, d'où, $ca\in d_n(\mathfrak{a})$.

(2) $d_n(\mathfrak{a})$ *est une fonction croissante de* n *pour un idéal* $\mathfrak{a}$ *fixé.* En effet si $a\in d_n(\mathfrak{a})$, alors $f(X)=aX^n+a_1X^{n-1}+\ldots$ est un élément de $\mathfrak{a}$ et il en resulte que a est le coefficient de X^{n+1} dans le polynôme $Xf(X)\in\mathfrak{a}$ (on remarque que $Xf(X)=aX^{n+1}+a_1X^n+\ldots$). Ceci nous montre que $a\in d_{n+1}(\mathfrak{a})$.

(3) *pour un entier* n *fixé,* $d_n(\mathfrak{a})$ *est une fonction croissante de* $\mathfrak{a}$, c'est à dire, si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux de $A[X]$ tels que $\mathfrak{a}\subset\mathfrak{b}$, alors $d_n(\mathfrak{a})\subset d_n(\mathfrak{b})$. Ceci est bien clair.

(4) *si* $\mathfrak{a}\subset\mathfrak{b}$ *et si* $d_n(\mathfrak{a})=d_n(\mathfrak{b})$ *pour tout entier* $n\geq 0$, *alors* $\mathfrak{a}=\mathfrak{b}$. Soit $f(X)\in\mathfrak{b}$. On va démontrer que $f(X)\in\mathfrak{a}$, par récurrence sur $d^0(f)$. Si $d^0(f)=0$, alors $f\in\mathfrak{b}\cap A=d_0(\mathfrak{b})=d_0(\mathfrak{a})=\mathfrak{a}\cap A$ et donc, $f\in\mathfrak{a}$. Soit maintenant $n=d^0(f)>0$. On peut écrire $f(X)=aX^n+a_1X^{n-1}+\ldots$ avec $a\in d_n(\mathfrak{b})=d_n(\mathfrak{a})$ et ceci nous montre qu'il existe un $g(X)\in\mathfrak{a}$ tel que $g(X)=aX^n+b_1X^{n-1}+\ldots$. Sur le polynôme $f-g$ on peut dire que $d^0(f-g)<n$ et comme $f\in\mathfrak{b}$ et $g\in\mathfrak{a}\subset\mathfrak{b}$, alors $f-g\in\mathfrak{b}$. Par l'hypothèse de récurrence, on a $f-g\in\mathfrak{a}$ et donc, $f=(f-g)+g\in\mathfrak{a}$.

Soit $\mathfrak{a}_1\subset\ldots\subset\mathfrak{a}_n\subset\ldots$ une suite croissante d'idéaux de $A[X]$. Celle-ci nous donne le diagramme que voici (où $\rightarrow$ indique l'inclusion):

$$\begin{array}{ccccccc}
d_0(\mathfrak{a}_1) & \rightarrow & d_0(\mathfrak{a}_2) & \rightarrow\cdots\rightarrow & d_0(\mathfrak{a}_n) & \rightarrow\cdots \\
\downarrow & & \downarrow & & \downarrow & \\
d_1(\mathfrak{a}_1) & \rightarrow & d_1(\mathfrak{a}_2) & \rightarrow\cdots\rightarrow & d_1(\mathfrak{a}_n) & \rightarrow\cdots \\
\downarrow & & \downarrow & & \downarrow & \\
\cdots\cdots & & \cdots\cdots & & \cdots\cdots & \\
\downarrow & & \downarrow & & \downarrow & \\
d_p(\mathfrak{a}_1) & \rightarrow & d_p(\mathfrak{a}_2) & \rightarrow\cdots\rightarrow & d_p(\mathfrak{a}_n) & \rightarrow\cdots \\
\downarrow & & \downarrow & & \downarrow & \\
\vdots & & \vdots & & \vdots &
\end{array}$$

D'après la condition maximale sur A, si l'on considère la famille des $d_p(\mathfrak{a}_n)$, il existe un élément maximal $d_{p_0}(\mathfrak{a}_{n_0})$. Or, on voit que la première ligne s'arrête à un indice j_0, la deuxième à un indice j_1, et ainsi

de suite, la p_0-ième s'arrête en un indice j_{p_0-1}. Soit maintenant $q=max(j_0,j_1,\ldots,j_{p_0-1},n_0)$. Ceci étant, on voit que pour tout indice p, la ligne formé par les $d_p(\mathfrak{a}_n)$ $(n=1,2,\ldots)$ stationne pour $n\geq q$, c'est à dire, $d_p(\mathfrak{a}_n)=d_p(\mathfrak{a}_q)$ pour tout $n\geq q$ et ceci, quel que soit $p\geq 0$. En vertue de (4), ceci nous donne $\mathfrak{a}_n=\mathfrak{a}_q$ pour tout $n\geq q$.

COROLLAIRE 1 - *Si* A *est un anneau noethérien, alors* $A[X_1,\ldots,X_n]$ *l'est aussi.*

On démontre le corollaire par récurrence sur n.

COROLLAIRE 2 - *Si* K *est un corps, alors* $K[X_1,\ldots,X_n]$ *est un anneau noethérien.*

Il suffit de remarquer qu'un corps est un anneau noethérien.

COROLLAIRE 3 - *Soit* $\mathbf{Z}$ *l'anneau des entiers. Alors* $\mathbf{Z}[X_1,\ldots,X_n]$ *est un anneau noethérien.*

On a déjà vu que $\mathbf{Z}$ est principal, donc noethérien.

COROLLAIRE 4 - *Soient* A' *un anneau,* A *un sous-anneau de* A' *et* $x_1,\ldots,x_n$ *des éléments de* A'. *Si* A *est noethérien, alors le sous-anneau de* A' *engendré par* A *et les* x_i, *c'est à dire,* $A[x_1,\ldots,x_n]$, *est aussi noethérien.*

En effet, on considère l'homomorphisme surjectif $\varphi:A[X_1,\ldots,X_n]\longrightarrow A[x_1,\ldots,x_n]$ défini par $\varphi(f(X_1,\ldots,X_n))=f(x_1,\ldots,x_n)$ pour tout $f\in A[X_1,\ldots,X_n]$. Alors $A[x_1,\ldots,x_n]=A[X_1,\ldots,X_n]/Ker(\varphi)$ et il suffit de connaître le lemme suivant:

LEMME 1 - *Si* B *est un anneau noethérien et* $\mathfrak{b}$ *est un idéal de* B, *alors* $B/\mathfrak{b}$ *est aussi un anneau noethérien.*

En effet, les idéaux de $B/\mathfrak{b}$ sont de la forme $\mathfrak{a}/\mathfrak{b}$, où $\mathfrak{a}$ est un idéal de B contenant $\mathfrak{b}$. Donc, la condition maximale pour les idéaux de B entraîne la condition maximale pour les idéaux de $B/\mathfrak{b}$.

Soit A un anneau factoriel et $f\in A[X_1,\ldots,X_n]$. On

appele *contenu de* f un *pgcd* des coefficients de f. On notera le contenu de f par $c(f)$. On dira que un polynôme $f \in A[X_1,\ldots,X_n]$ est *primitif* si $c(f)=1$. Ceci équivaut à dire que les coefficients de f sont tous étrangers.

LEMME 2 - (*Lemme de Gauss*). *Le produit de deux polynômes primitifs est un polynôme primitif.*

Soient $f,g \in A[X_1,\ldots,X_n]$ (on remarque que A est factoriel) deux polynômes primitifs et supposons que $f.g$ ne soit pas primitif. Alors il existe un élément extremal $p \in A$ qui divise tous les coefficients de $f.g$. Étant donné un polynôme $h \in A[X_1,\ldots,X_n]$, on peut considerer le polynôme $\bar{h} \in (A/pA)[X_1,\ldots,X_n]$ obtenu de h en réduisant tous les coefficients de h modulo p. On remarque que ceci nous donne un homomorphisme d'anneaux $A[X_1,\ldots,X_n] \longrightarrow (A/pA)[X_1,\ldots,X_n]$. Comme A est factoriel, alors pA est un idéal premier de A et donc, A/pA est intègre. Pour cela, il suffit de se souvenir qu'un élément extremal qui divise un produit, divise un des facteurs. Il en resulte alors que $(A/pA)[X_1,\ldots,X_n]$ est aussi intègre et comme $\bar{f}.\bar{g}=0$, alors on a, par exemple, $\bar{f}=0$. Ceci nous montre que p divise tous les coefficients de f, c'est à dire, $c(f) \neq 1$.

LEMME 3 - *Soient A un anneau factoriel et $f,g \in A[X_1,\ldots,X_n]$. Alors $c(fg)$ est associé à $c(f)c(g)$.*

En effet, étant donné $f \in A[X_1,\ldots,X_n]$, on peut écrire $f=c(f).f'$, où $f' \in A[X_1,\ldots,X_n]$ est un polynôme primitif (la formule $f=c(f).f'$ caractérise le contenu de f). De même, on peut écrire $g=c(g).g'$ où g' est un polynôme primitif et d'après le lemme de Gauss, $f'.g'$ est un polynôme primitif. La formule $f.g=c(f)c(g)f'g'$ nous donne le lemme.

THÉORÈME 2 - (*Théorème de Gauss*) - *Soient A un anneau factoriel K son corps de fractions et P un système representatif d'éléments extremaux de A. Si P' est un système (répresentatif) de polynômes primitifs de $A[X]$ et irreductibles sur K (c'est à dire, irreductibles dans $K[X]$), alors $P \cup P'$ est un système répresentatif d'éléments extremaux de $A[X]$.*

Soit $f \in A[X]$ tel que $d^0(f)>0$ (si $d^0(f)=0$, alors $f \in A$ et il n'y a rien à démontrer). Dans $K[X]$, on peut décomposer f en facteurs irreductibles $f=a\prod_{g\in P'} g^{n(g)}$ (produit fini), où $a \in K^*$ et les $n(g) \geq 0$ sont des entiers (cf. N. Bourbaki, Algèbre, Chap. IV, parag. 1, n. 5, Corollaire de la Proposition 8). Dans K^*, on peut écrire $a=u\prod_{p\in P} p^{m(p)}$, où $u \in U$ (= groupe des unités de l'anneau A) et où les $m(p)$ sont des entiers tous nuls, sauf un nombre fini d'entr'eux. Comme $c(g)=1$ pour tout $g \in P'$ (car, les g sont tous primitifs), il en resulte que $a=c(f)$ et donc, $a \in A$. Ceci nous montre que $m(p) \geq 0$ pour tout $p \in P$. Ainsi, on a démontré l'existence de la décomposition $f=u\prod_{p\in P} p^{m(p)}\prod_{g\in P'} g^{n(g)}$. Quant à l'unicité, puisque on a $f=a\prod_{g\in P'} g^{n(g)}$ dans $K[X]$, l'unique factorisation dans $K[X]$ nous donne l'unicité des $n(g)$. D'autre part, comme $c(f)=u\prod_{p\in P} p^{m(p)}$ dans A et A est factoriel, on a l'unicité des $m(p)$.

REMARQUE - On peut traduire l'ennoncé du théorème ci-dessus d'une façon beaucoup plus simple (mais aussi beaucoup moins précise) en disant que *si A est un anneau factoriel, alors l'anneau des polynômes $A[X]$ est aussi factoriel.*

COROLLAIRE 1 - a) *Si A est un anneau factoriel, alors $A[X_1,\ldots,X_n]$ l'est aussi.* b) *Si K est un corps, l'anneau $K[X_1,\ldots,X_n]$ est factoriel.* c) *Soit $\mathbf{Z}$ l'anneau des entiers. L'anneau $\mathbf{Z}[X_1,\ldots,X_n]$ est factoriel.*

Soit K un corps. Un élément extremal de l'anneau $K[X_1,\ldots,X_n]$ s'appele un *polynôme irreductible sur K* (par exemple, le polynôme X^2+1 est irreductible sur $\mathbf{R}$, mais pas irreductible sur le corps $\mathbf{C}$ des complexes).

COROLLAIRE 2 - (*complement au Corollaire 1*). *Soient A un anneau factoriel et K son corps de fractions. Les éléments extremaux de $A[X_1,\ldots,X_n]$ sont des deux types suivants:* (1) *les constantes extremales;* (2) *les polynômes*

irreductibles sur K et primitifs sur A.

En effet, si P est un système répresentatif d'éléments extremaux de A et P' est un système (répresentatif) de pòlynômes irreductibles sur K et primitifs sur A, on montrera que $P \cup P'$ jouit des propriétés qu'il faut. Si $f \in A[X_1, \ldots, X_n]$, $f \neq 0$, alors on peut écrire $f = a \prod_{g \in P'} g^{n(g)}$ (produit fini), où $a \in K^*$ et où $n(g) \geqq 0$ sont des entiers. La factorialité de $K[X_1, \ldots, X_n]$ nous donne l'unicité des entiers $n(g)$. L'unicité de l'élément a vient du fait que $a = c(f)$. Étant donné que $a \in K^*$, alors on peut écrire que $a = u \prod_{p \in P} p^{m(p)}$ (produit fini), où les $m(p)$ sont des entiers et où $u \in U$ (= groupe des unités de A). Puisque $a = c(f)$, alors $a \in A$ et donc $m(p) \geqq 0$ pour tout $p \in P$. Étant donné que A est factoriel, on a l'unicité des $m(p)$. On a ainsi démontré l'existence et l'unicité de la décomposition $f = u \prod_{p \in P} p^{m(p)} \prod_{g \in P'} g^{n(g)}$.

THÉORÈME 3 - *(Théorème de van der Waerden). Soient k un corps, $T_1, \ldots, T_n$ des indeterminées et $K = k(T_1, \ldots, T_n)$ le corps de fractions de l'anneau intègre $k[T_1, \ldots, T_n]$. On considère des polynômes non constants $f_i(X) \in k[X_1, \ldots, X_q]$ $(i = 1, \ldots, n)$, étrangers dans leur ensemble. Alors le polynôme $f = \sum_{i=1}^{n} T_i f_i(X)$ est irreductible sur K.*

Soient $A = k[T_1, \ldots, T_n]$, $B = K[X_1, \ldots, X_q]$, $A' = k[X_1, \ldots, X_q]$ et K' le corps de fractions de A'. Le polynôme f est un élément extremal de l'anneau $A'[T_1, \ldots, T_n] = A[X_1, \ldots, X_q]$. En effet, comme les f_i sont étrangers dans leur ensemble, alors $c_{A'}(f) = 1$ et ceci nous montre que f est primitif sur A'. D'autre part, comme f est homogène de degré 1 en les T_i, il en resulte que f est irreductible sur K' (c'est à dire, irreductible dans l'anneau $K'[T_1, \ldots, T_n]$) et donc, par le corollaire 2 du Théorème de Gauss, f est un élément extremal de l'anneau $A'[T_1, \ldots, T_n]$. Comme f n'est pas constant par rapport aux X_j (car, les f_i ne le sont pas), et qu'il est un élément extremal de l'anneau $A[X_1, \ldots, X_n]$, par le corollaire 2 du Théorème de Gauss il en resulte que f est irreductible sur K, ou encore, irreductible dans l'anneau B.

CHAPITRE III

ANNEAUX DE FRACTIONS D'UN ANNEAU FACTORIEL

Soit A un anneau commutatif à élément unité. Une partie S de A s'appele une *partie multiplicative de A* si l'élément unité de A est dans S et si $SS \subset S$, c'est à dire, S est stable par la multiplication. Si M est un A-module unitaire, on définit dans $M \times S$ une relation d'équivalence (qu'on la note par le symbole $\equiv$), en posant $(x,s) \equiv (x',s')$ si et seulement si, il existe un $t \in S$ tel que $t(s'x - sx') = 0$. On vérifie aisement qu'il s'agit bien d'une relation d'équivalence dans $M \times S$ et le quotient de $M \times S$ par cette relation sera noté $S^{-1}M$ ou M_S. La classe d'un élément (x,s) modulo cette relation sera notée x/s. Si l'on considère le A-module libre A, on peut fabriquer $S^{-1}A$. On définit une loi de groupe additif dans $S^{-1}M$, une loi multiplicative dans $S^{-1}A$ et une loi externe sur $S^{-1}M$ ayant $S^{-1}A$ comme ensemble d'opérateurs, respectivement par $(x/s) + (x'/s') = (s'x + sx')/ss'$, $(a/s).(a'/s') = aa'/ss'$ et $(a/s).(x/t) = ax/st$ pour tous x/s et x'/s' dans $S^{-1}M$ et a/s et a'/s' dans $S^{-1}A$. On vérifie que ces définitions sont indépendantes des répresentants qu'on prend dans