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 $n(g) \geq 0$ 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 $m(p) \geq 0$ 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

les classes d'équivalence et que ainsi $S^{-1}A$ est muni d'une structure d'anneau appelé *anneau de fractions de A à dénominateurs dans S*. De plus, $S^{-1}M$ est muni d'une structure de $S^{-1}A$-module appelé *module de fractions de M à dénominateurs dans S*. On remarque que $S^{-1}M$ est aussi muni d'une structure de A-module en posant pour tout $a\in A$ et pour tout x/s dans $S^{-1}M$, $a.(x/s)=ax/s$.

EXEMPLES

(1) Soient A un anneau intègre, $S=A-(0)$ et K son corps de fractions. On vérifie immediatement que $S^{-1}A=K$.

(2) Soient U le groupe multiplicatif des éléments inversibles de A et $S=U$. Alors $S^{-1}A=A$.

(3) Dans un anneau commutatif à élément unité, un idéal $\mathfrak{p}$ de A, $\mathfrak{p}\neq A$, est dit un *idéal premier de A* si $A/\mathfrak{p}$ est un anneau intègre. Ceci équivaut à dire que étant donnés deux éléments $a,b\in A$ tels que $ab\in\mathfrak{p}$, alors $a\in\mathfrak{p}$ ou $b\in\mathfrak{p}$, ou encore, que $A-\mathfrak{p}$ est une partie multiplicative de A. Soient alors $\mathfrak{p}$ un idéal premier de A et $S=A-\mathfrak{p}$ (partie multiplicative de A). On notera $S^{-1}A=A_{\mathfrak{p}}$ et $A_{\mathfrak{p}}$ est appelé *anneau localisé de A en $\mathfrak{p}$* ou *anneau local de A en $\mathfrak{p}$*. Les anneaux locaux ont une grande importance dans differentes branches des mathématiques et en particulier en Géométrie Algèbrique. Leur nom est, d'ailleurs, d'origine géométrique, car on les emploient pour étudier des propriétés locales dans les variétés algèbriques.

§1. RELATIONS ENTRE IDÉAUX DE A ET DE $S^{-1}A$.

Soient A un anneau intègre (on remarque que l'hypothèse que A soit intègre n'est pas essentielle), S une partie multiplicative de A ne contenant pas le zero ($0\notin S$) et $A'=S^{-1}A$. Soient I l'ensemble des idéaux de A et I' celui des idéaux de A'. Étant donné un idéal $\mathfrak{a}$ de A, on notera $\mathfrak{a}A'$ le plus petit idéal de A' contenant $\mathfrak{a}$ (*) et si $\mathfrak{a}'$ est un idéal de

(*) Soient B un anneau et G et H deux sous-groupe additifs de B. On peut définir GH comme étant l'ensemble des sommes finies $\sum_i a_i b_i$ telles que les a_i sont dans G et les b_i sont dans H. On voit que GH est un sous-groupe additif de B. De même, on définit le sous-groupe somme $G+H$ et pour ces opérations on a le formulaire suivant: $(GH)K=G(HK)$, $GH=HG$, $(G+G')H=GH+G'H$, quelques soient les sous-groupes G,H,K,G' additifs de l'anneau B.

A', alors $\mathfrak{a}'\cap A$ est un idéal de A (on sait que $A\subset A'$). On ordonne I et I' par inclusion et ce qu'on vient de dire ci-dessus nous montre que, on a définit deux applications $e:I\to I'$ *(operation d'extension)* et $r:I'\to I$ *(opération de restriction)*. Il s'agit de deux applications croissantes mais, en général, non réciproques.

THÉORÈME 1 - *Pour tout idéal $\mathfrak{a}'$ de A', on a $(\mathfrak{a}'\cap A)A'=\mathfrak{a}'$, ou encore, $e\circ r=1_{I'}$ (on note $1_{I'}$ l'application identique dans I').*

En effet, il est évident que $(\mathfrak{a}'\cap A)A'\subset\mathfrak{a}'$ et soit $x\in\mathfrak{a}'$. On peut écrire $x=a/s$ avec $a\in A$ et $s\in S$ et donc, $a=sx\in\mathfrak{a}'\cap A$, d'où, $x=(1/s).a\in(\mathfrak{a}'\cap A)A'$.

THÉORÈME 2 - *Pour tout idéal $\mathfrak{a}$ de A, on a $\mathfrak{a}A'\cap A=\{a\in A\mid\exists s\in S,\ sa\in\mathfrak{a}\}$* (cet idéal s'appele le *saturé de $\mathfrak{a}$ par rapport à S*).

Si x est dans le second membre, alors il existe un $s\in S$ tel que $sx\in\mathfrak{a}$ et donc, $x=(1/s)(sx)\in\mathfrak{a}A'$ et comme $x\in A$, alors $x\in\mathfrak{a}A'\cap A$. Soit maintenant $x\in\mathfrak{a}A'\cap A$. Alors $x\in A$ et l'on peut écrire $x=\sum_i a_i c_i'$ (somme finie) avec a_i dans $\mathfrak{a}$ et les c_i' dans A'. Il existe alors un $s\in S$ tel que $c_i'=b_i/s$ avec les b_i dans A. Donc, $sx=\sum_i a_i b_i\in\mathfrak{a}$.

COROLLAIRE - *(du théorème 1) - L'opération d'extension $e:I\to I'$ est surjective et celle de restriction $r:I'\to I$ est injective.*

Maintenant on va noter I_0 l'ensemble des saturés des idéaux de A (il s'agit d'un sous-ensemble ordonné de I) et considérons les opérations d'extension $e:I_0\to I'$ et de restriction $r:I'\to I_0$ avec les saturés. Il est clair que encore ici, $e\circ r=1_{I'}$ et on va donner le corollaire suivant:

COROLLAIRE 1 - *Les applications $e:I_0\to I'$ et $r:I'\to I_0$ sont des bijections réciproques entre I' et I_0 et en particulier, I_0 et I' sont isomorphes en tant qu'ensembles ordonnés. De plus,*

e et r sont des bijections croissantes.

Il suffit de voir que pour tout idéal $\mathfrak{a} \in I_0$, on a $r(e(\mathfrak{a})) = r(\mathfrak{a}A') = \mathfrak{a}A' \cap A = \mathfrak{a}$ et ceci nous montre que $r \circ e = 1_{I_0}$.

COROLLAIRE 2 - *Si A est un anneau noethérien, il en est de même de $S^{-1}A$.*

Ceci resulte du Corollaire 1.

UN EXEMPLE - Soient $\mathfrak{p}$ un idéal premier de A et $S = A - \mathfrak{p}$. Alors, le saturé de $\mathfrak{p}$ par rapport à S est $\mathfrak{p}$.

THÉORÈME 3 - *Les applications e et r définissent un isomorphisme d'ensembles ordonnés entre l'ensemble de tous les idéaux premiers de $A' = S^{-1}A$ et l'ensemble des idéaux premiers $\mathfrak{p}$ de A tels que $\mathfrak{p} \cap S = \emptyset$.*

Soit $\mathfrak{p}'$ un idéal premier de A'. Alors $\mathfrak{p}' \cap A$ est un idéal premier de A et, de plus, $\mathfrak{p}' \cap A \cap S = \emptyset$, car sinon il existe un $s \in \mathfrak{p}' \cap A \cap S$ et comme $s \in S$, alors $1/s$ est dans A' et ceci nous montre que $1 = (1/s)s \in \mathfrak{p}'$, c'est à dire, $\mathfrak{p}' = A'$. On remarque que $(\mathfrak{p}' \cap A)A' = \mathfrak{p}'$. Soit maintenant $\mathfrak{p}$ un idéal premier de A tel que $\mathfrak{p} \cap S = \emptyset$. Alors, $1 \notin \mathfrak{p}A'$, car sinon $1 = \sum_i a_i c_i'$ (somme finie) avec les a_i dans $\mathfrak{p}$ et les c_i' dans A'. On peut écrire que $c_i' = b_i/s$ avec les b_i dans A et $s \in S$ et donc, $s = \sum_i a_i b_i \in \mathfrak{p}$. Ceci contredit le fait que $\mathfrak{p} \cap S = \emptyset$. Montrons que $\mathfrak{p}A'$ est un idéal premier de A'. En effet, si a', b' sont dans A' et sont tels que $a'b' \in \mathfrak{p}A'$, alors on peut écrire que $a' = a/s$ et $b' = b/s$ avec $a, b \in A$ et $s \in S$. Il existe alors un $t \in S$ tel que $tab \in \mathfrak{p}$ et comme $\mathfrak{p} \cap S = \emptyset$, alors $t \notin \mathfrak{p}$ et ceci nous montre que $ab \in \mathfrak{p}$. Il en resulte alors que $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$ et donc, $a' \in \mathfrak{p}A'$ ou $b' \in \mathfrak{p}A'$. Donc, $\mathfrak{p}A'$ est un idéal premier de A'. Comme $\mathfrak{p}$ est saturé, alors on a $\mathfrak{p}A' \cap A = \mathfrak{p}$.

Pour "voir plus clair", on peut proceder de la façon suivante: soient I_1' l'ensemble des idéaux premiers de A' et I_1 l'ensemble des idéaux premiers de A tels que si $\mathfrak{p} \in I_1$, alors $\mathfrak{p} \cap S = \emptyset$. On considère maintenant les opérations d'extension

et de restriction, $I_1' \xrightarrow{r} I_1 \xrightarrow{e} I_1'$, et il est facile de voir que $(e \circ r)(\mathfrak{p}') = e(\mathfrak{p}' \cap A) = (\mathfrak{p}' \cap A)A' = \mathfrak{p}'$ pour tout idéal premier $\mathfrak{p}'$ de A' et $(r \circ e)(\mathfrak{p}) = r(\mathfrak{p}A') = \mathfrak{p}A' \cap A = \mathfrak{p}$ pour tout $\mathfrak{p}$ dans I_1. Donc, I_1' et I_1 sont des ensembles ordonnés isomorphes.

COROLLAIRE - *Soient A un anneau (intègre) et $\mathfrak{p}$ un ideal premier de A. Alors l'application $\mathfrak{m} \to \mathfrak{m}A_{\mathfrak{p}}$ est une bijection de l'ensemble des ideaux premiers de A contenus dans $\mathfrak{p}$ sur l'ensemble de tous les idéaux premiers de $A_{\mathfrak{p}}$, la bijection reciproque etant $\mathfrak{m}' \to \mathfrak{m}' \cap A$.*

Soient $S = A - \mathfrak{p}$ et $A' = S^{-1}A$. On voit immediatement que la relation $\mathfrak{m} \cap S = \emptyset$ équivaut à $\mathfrak{m} \subset \mathfrak{p}$ et donc, d'après le théorème 3 on a le corollaire.

EXERCICE - Soient A un anneau (intègre), S une partie multiplicative de A, $S^{-1}A = A'$ et $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux de A. Alors on a la formule $\mathfrak{a}A' \cap \mathfrak{b}A' = (\mathfrak{a} \cap \mathfrak{b})A'$.

§2. FACTORIALITÉ DES ANNEAUX DE FRACTIONS

THÉORÈME 4 - *Soient A un anneau factoriel et S une partie multiplicative de A telle que $0 \notin S$. Alors $S^{-1}A$ est aussi un anneau factoriel. Plus précisement, soient P un système répresentatif d'éléments extremaux de A, $P' = \{p \in P \mid \exists s \in S$ tel que $p \mid s\}$ et $P'' = P - P'$. Alors P'' est un système répresentatif d'éléments extremaux de $S^{-1}A$.*

EXISTENCE - Tout d'abord on remarque que tout élément de P' est inversible dans $S^{-1}A$. En effet, si $p \in P'$, alors il existe un $s \in S$ tel que $s = ap$ avec $a \in A$ et ceci entraîne que $1/p = a/s \in S^{-1}A$. Si $x \in S^{-1}A$, alors on peut écrire que $x = u \prod_{p \in P} p^{n(p)}$ et comme $P = P' \cup P''$, alors on peut écrire $x = u \prod_{p \in P'} p^{n(p)} \prod_{q \in P''} q^{n(q)}$. Comme u est un élément inversible dans A et les éléments de P' sont inversibles dans $S^{-1}A$, il en resulte que l'élément $v = u \prod_{p \in P'} p^{n(p)}$ est inversible dans $S^{-1}A$. Il

faut maintenant démontrer que $n(q) \geq 0$ pour tout $q \in P''$. En effet, on voit tout d'abord que si $x \in S$, alors $n(q) = 0$ pour tout $q \in P''$, car s'il existe un $q \in P''$ tel que $n(q) > 0$, alors $q | x$ et comme $x \in S$ il en resulte que $q \in P'$. Ceci contredit le fait que $P' \cap P'' = \emptyset$. Soit maintenant $x \in S^{-1}A$. Alors $x = a/s$ avec $a \in A$ et $s \in S$. Si l'on designe par v_q la valuation q-adique, alors $v_q(a) \geq 0$ pour tout $q \in P''$ et $v_q(s) = 0$ pour tout $q \in P''$. Donc, $v_q(x) \geq 0$ pour tout $q \in P''$.

UNICITÉ - Soit $x \in S^{-1}A$ et supposons que $x = u \prod_{q \in P''} q^{n(q)}$ avec u inversible dans $S^{-1}A$. Il en resulte immediatement que $v_q(x) = v_q(u) + \sum_{q' \in P''} n(q') v_q(q')$ et comme $v_q(q') = 0$ ou 1 selon que $q' \neq q$ ou $q' = q$, alors on a $v_q(x) = v_q(u) + n(q)$. Puisque u est dans $S^{-1}A$, alors on peut écrire que $u = a/s$ avec $a \in A$ et $s \in S$ et donc, $v_q(u) = v_q(a) \geq 0$. D'autre part, u est inversible dans $S^{-1}A$ et l'on peut donc écrire $1/u = b/t$ avec $b \in A$ et $s \in S$ et donc, $v_q(1/u) = v_q(b) \geq 0$. Ceci nous donne $v_q(u) = 0$ et il en resulte que $v_q(x) = n(q)$, d'où l'unicité.

EXEMPLES

1. Soient k un corps et $B = k[x,y]$ avec $xy = 1$. On remarque que l'anneau B est le quotient $B = k[X,Y]/(XY-1)$ et x et y sont les classes de X et Y respectivement, modulo l'idéal $(XY-1)$. On va montrer que B est un anneau factoriel. En effet, on peut écrire $B = k[x][1/x]$ et si l'on considère la partie multiplicative de $k[x]$, $S = \{1, x, \ldots, x^n, \ldots\}$ alors on voit immediatement que $B = S^{-1}(k[x])$. Comme $k[x]$ est un anneau principal, donc factoriel, le théorème 4 nous montre que B *est aussi factoriel*.

2. Soient $\mathbf{C}$ le corps des complexes et $B' = \mathbf{C}[x,y]$ avec $x^2 + y^2 = 1$. On va montrer que B' est factoriel. En effet, si l'on pose $u = x + iy$ et $v = x - iy$, alors on a d'un côté $uv = x^2 + y^2 = 1$ et d'autre part, $x = (u+v)/2$ et $y = (u-v)/2i$ nous donne $B' = \mathbf{C}[u,v]$. Par exemple précedent on a que B' *est factoriel*.

3. On considère l'anneau $B = \mathbf{R}[x,y]$ avec $x^2 + y^2 = 1$, où $\mathbf{R}$ est le corps des réels. On va montrer que B *n'est pas factoriel*. En effet, on considère l'anneau B' de l'exercice précedent, où $k = \mathbf{C}$ est le

corps des complexes. On voit que les éléments inversibles de $B' = \mathbf{C}[u,v]$ sont les éléments de la forme cu^n avec $c \in \mathbf{C}$ et $n \in \mathbf{Z}$ (on remarque que $uv = 1$). Puisque $x = (u+v)/2 = (1/2)(u + (1/u)) = (u^2+1)/2u$, on voit que le seul moyen de décomposer x (dans B') est $x = (u+i)(u-i)/2u$ et donc, x est extremal dans B. De plus, on voit que $x^2 = 1 - y^2 = (1-y)(1+y)$ entraîne $x | (1-y)(1+y)$, mais x ne divise pas $1-y$, ni $1+y$ (dans B). En effet, montrons, par exemple, que $x \nmid (1-y)$ dans B. Pour cela on écrit $y = (u^2-1)/2ui$ et ceci nous donne $1 - y = -(u-i)^2/2ui$. Puisque $x = (u+i)(u-i)/2u$, il en resulte alors que $(1-y)/x = i(u-i)/(u+i) = i(x+iy-i)/(x+iy+i)$ et donc, $(1-y)/x$ n'est pas dans B. Ceci nous montre que $x \nmid (1-y)$ dans B. De même, on peut démontrer que $x \nmid (1+y)$ dans B et donc, B n'est pas factoriel.

§3. THÉORÈME DE NAGATA

THÉORÈME 5 - *(Théorème de Nagata) - Soient A un anneau intègre noethérien et S une partie multiplicative de A engendrée par des éléments premiers p_i pour $i \in I$ (ceci veut dire que les éléments de S sont des produits des puissances des p_i). Si $S^{-1}A$ est factoriel, alors A est aussi factoriel. Précisement, supposons que les p_i sont deux à deux non associés et soient P' l'ensemble des p_i et P'' un système répresentatif d'éléments extremaux de $S^{-1}A$. Alors $P = P' \cup P''$ est un système répresentatif d'éléments extremaux de A.*

LEMME 1 - *Soient A un anneau noethérien intègre* (*) *et p un élément premier de A. Alors il existe une valuation v_p du corps de fractions K de A telle que l'anneau de fractions $A_{(p)}$ soit l'ensemble des éléments $x \in K$ tels que $v_p(x) \geq 0$ et $v_p(p) = 1$* (**).

On sait que $A_{(p)}$ est un anneau noethérien (si l'on prend sur A la condition (M), il faut vérifier que $A_{(p)}$ obéit aussi à la condition (M)), intègre, local d'idéal maximal $(p)A_{(p)}$. Pour tout $x \neq 0$ dans $A_{(p)}$ on peut écrire $x = p^n z$, où $n \geq 0$ est

(*) Il suffit de prendre A intègre obéissant à la condition (M).

(**) Si v est une valuation d'un corps K, alors $A = \{x \in K | v(x) \geq 0\}$ est *l'anneau de v* et $\mathfrak{p} = \{x \in K | v(x) > 0\}$ est *l'idéal de v*.

un entier et z est inversible dans $A_{(p)}$. On va montrer qu'il existe un plus grand entier n tel que $p^n|x$ et $p^{n+1}\nmid x$. En effet, si $p^n|x$ pour tout entier $n\geq 0$, alors on peut écrire que $x=p^n a_n=p^{n+1}a_{n+1}$ et ceci nous montre que $a_n=pa_{n+1}$, c'est à dire, $a_nA_{(p)}\subset a_{n+1}A_{(p)}$. Comme p n'est pas inversible dans $A_{(p)}$, il en resulte que $a_nA_{(p)}\neq a_{n+1}A_{(p)}$ et donc, on a une suite strictement croissante d'idéaux $a_0A_{(p)}\subsetneq a_1A_{(p)}\subsetneq\ldots\subsetneq a_nA_{(p)}\subsetneq\ldots$, ce qui contredit le fait que $A_{(p)}$ soit noethérien. On posera alors pour tout $x\neq 0$ dans $A_{(p)}$, $v_p(x)$ comme étant le plus grand entier ≥ 0 tel que l'on a les relations $p^{v_p(x)}|x$ et $p^{v_p(x)+1}\nmid x$. De plus, pour le zero, on posera $v_p(0)=+\infty$. Montrons que si x et y sont deux éléments de $A_{(p)}$, alors on a les formules $v_p(xy)=v_p(x)+v_p(y)$ et $v_p(x+y)\geq$ $\geq min\,(v_p(x),v_p(y))$. En effet, on peut écrire que $x=p^{v_p(x)}x'$ et $y=p^{v_p(y)}y'$ avec x' et y' dans $A_{(p)}-(p)A_{(p)}$ et donc, $xy=$ $=p^{v_p(x)+v_p(y)}x'y'$ avec $x'y'$ dans $A_{(p)}-(p)A_{(p)}$. Ceci nous montre que $v_p(xy)=v_p(x)+v_p(y)$. D'autre part, si $n=$ $=min(v_p(x),v_p(y))$, alors on peut écrire $x\in p^nA_{(p)}$ et $y\in p^nA_{(p)}$. Donc, $x+y\in p^nA_{(p)}$ et ceci nous montre que $v_p(x+y)\geq$ $\geq min(v_p(x),v_p(y))$. Maintenant on étend v_p au corps de fractions K de A et v_p dévient ainsi une valuation de K qu'on la note encore v_p. Il est évident que $v_p(p)=1$. Montrons maintenant que $A_{(p)}=\{x\in K\,|\,v_p(x)\geq 0\}$ c'est à dire, que $A_{(p)}$ est l'anneau de la valuation v_p. Il est immediat que si $x\in A_{(p)}$, alors $v_p(x)\geq 0$. Supposons que $z\in K$ est tel que $v_p(z)\geq 0$. On peut écrire $z=x/y$ avec $x,y\in A_{(p)}$ et donc, $0\leq v_p(z)=v_p(x)-v_p(y)$. Ceci nous dit que $y|x$ dans $A_{(p)}$ et donc, $z\in A_{(p)}$.

On remarque que l'idéal maximal de $A_{(p)}$ est $(p)A_{(p)}=\{x\in K\,|\,v_p(x)>0\}$ et que $(p)A_{(p)}\cap A=(p)$ (!).

LEMME 2 - *Les hypothèses et notations sont celles du théorème 5 - Pour tout $a\in A$, $a\neq 0$ on a $v_p(a)=0$ sauf pour un nombre fini de $p\in P'$ et, de plus, on peut écrire $a=a'\prod_{p\in P'}p^{v_p(a)}$ avec $a'\in A$ et $v_p(a')=0$ pour tout $p\in P'$.*

Si $v_p(a)=0$ pour tout $p\in P'$, il suffit de prendre $a'=a$. Sinon, il existe un $p_1\in P'$ tel que $v_{p_1}(a)>0$ et d'après la (!) on peut écrire $a=p_1a_1$ avec $a_1\in A$. Si $v_p(a_1)=0$ pour tout $p\in P'$, on s'arrête; sinon il existe un $p_2\in P'$ tel que $a_1=p_2a_2$ et ainsi de suite. On a une suite croissante d'idéaux $Aa\subset Aa_1\subset Aa_2\subset$ $\subset\ldots\subset Aa_n\subset\ldots$ et comme A est noethérien, il existe un indice n tel que $v_p(a_n)=0$ pour tout $p\in P'$ et $a=a_np_1\ldots p_n$. Ainsi, on peut écrire ceci sous la forme suivante: $a=a'\prod_{p\in P'}p^{j(p)}$ avec $v_p(a')=0$ pour tout $p\in P'$ et où les $j(p)$ sont presque tous nuls. On sait que $v_p(q)=0$ ou 1 selon que $q\neq p$ ou $q=p$, car $q\notin(p)$ si $q\neq p$. Donc, on peut écrire que $v_p(a)=v_p(a')+$ $+\sum_{q\in P'}j(q)v_p(q)=j(p)$ et le lemme est démontré.

LEMME 3 - *Les éléments inversibles de $S^{-1}A$ sont ceux de la forme $u\prod_{p\in P'}p^{j(p)}$ avec u inversible dans A et $j(p)\in\mathbf{Z}$ et presque tous nuls.*

Il est clair que tout élément de la forme ci-dessus est inversible dans $S^{-1}A$. Réciproquement, soit $x\in S^{-1}A$ un élément inversible dans $S^{-1}A$. Alors on peut écrire que $x=$ $=a/s$ et $1/x=b/t$ avec $a,b\in A$ et $s,t\in S$ et donc, $ab=st=\prod_{p\in P'}p^{n(p)}$ avec les $n(p)\in\mathbf{N}$ et presque tous nuls (on rappele que tout élément de S est un produit d'éléments de P'). Par le lemme 2, on peut écrire $a=a'\prod_{p\in P'}p^{v_p(a)}$ et $b=b'\prod_{p\in P'}p^{v_p(b)}$ où, $a',b'\in A$, $v_p(a')=v_p(b')=0$ pour tout $p\in P'$. Donc, $a'b'\prod_{p\in P'}p^{v_p(a)+v_p(b)}=$ $=\prod_{p\in P'}p^{n(p)}$ et si l'on prend la valuation p-adique des deux membres, on a $v_p(a)+v_p(b)=n(p)$. Ceci nous montre que $a'b'=1$ et donc, a' est inversible dans A. On peut alors écrire que $x=a/s=a'\prod_{p\in P'}p^{v_p(a)}/\prod_{p\in P'}p^{m(p)}=a'\prod_{p\in P'}p^{v_p(a)-m(p)}$ et le lemme est démontré.

DÉMONSTRATION DU THÉORÈME 5

EXISTENCE - Soit $a\in A$. Dans $S^{-1}A$ on peut écrire $a=u\prod_{p\in P'}p^{m(p)}$ avec u inversible dans $S^{-1}A$ et $m(p)\geq 0$ pour

tout $p \in P''$. Par le lemme 3 on peut écrire $u = v \prod_{p \in P'} p^{n(p)}$ avec v inversible dans A et $n(p) \in \mathbf{Z}$ pour tout $p \in P'$. Si l'on prend la valuation p-adique (avec $p \in P'$) il en resulte que $v_p(u) = n(p)$ et $v_p(a) = v_p(u)$ (on remarque que $v_p(v) = 0$, $v_p(p) = 1$ pour tout $p \in P'$ et que $v_p(q) = 0$ pour tout $q \in P''$) et donc, $v_p(a) = n(p)$. Ceci nous montre que $n(p) \geq 0$ pour tout $p \in P'$.

UNICITÉ - Maintenant il faut démontrer que la décomposition ci-dessus est unique. En effet, supposons que $a = v \prod_{p \in P'} p^{m(p)} \prod_{q \in P''} q^{n(q)}$ avec v inversible dans A. Il en resulte que $v_p(a) = m(p)$ pour tout $p \in P'$ et donc, les $m(p)$ sont uniques. Si l'on pose $u = v \prod_{p \in P'} p^{m(p)}$, comme u est inversible dans $S^{-1}A$, grâce à la factorialité de $S^{-1}A$ il en resulte que u et les $n(q)$ sont uniques.

REMARQUE - On peut supposer que les éléments de P' sont deux à deux non associés, car dans une partie multiplicative on peut enlever les éléments inversibles sans modifier $S^{-1}A$.

COROLLAIRE - *(Théorème de Klein) - Soient K un corps algébriquement clos de caractéristique $\neq 2$ et $g(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ avec $n \geq 5$ une forme quadratique non-dégénerée. Alors l'anneau quotient $A = K[X_1, \ldots, X_n]/(g) = K[x_1, \ldots, x_n]$ est factoriel* (cf. M. Nagata, A remark on unique factorization domain 9 (1957), 143-145).

Puisque K est un corps algébriquement clos de caractéristique $\neq 2$ et $g(X_1, \ldots, X_n)$ est non-dégénerée ayant au moins trois variables, alors on peut écrire que $g(X_1, \ldots, X_n) = X_1X_2 + f(X_3, \ldots, X_n)$, après un changement convenable de variables. On voit maintenant que f est non-dégénerée et a au moins trois variables (car $n \geq 5$) et donc, f est un polynôme irreductible. En effet, sinon f serait un produit de deux formes linéaires et n'aurait donc plus que deux variables; f serait donc dégénerée. Dans l'anneau A, l'élément x_1 est premier. En effet, $A/x_1A = K[X_2, \ldots, X_n]/(f)$ et ceci est intègre

car f est un polynôme irreductible. Maintenant on considère la partie multiplicative de A, $S = \{1, x_1, \ldots, x_1^n, \ldots\}$ et l'on a $S^{-1}A = A[x_1^{-1}]$. Puisque $0 = g(x_1, \ldots, x_n) = x_1x_2 + f(x_3, \ldots, x_n)$, alors $x_2 = -f(x_3, \ldots, x_n)/x_1 \in K[x_3, \ldots, x_n, x_1^{-1}]$ donc,

$$A[x_1^{-1}] = K[x_1, \ldots, x_n, x_1^{-1}] =$$
$$= K[x_1, x_3, \ldots, x_n, x_1^{-1}] = K[x_1, x_3, \ldots, x_n][x_1^{-1}].$$

Il n'y a pas de relations algébriques entre $x_1, x_3, \ldots, x_n$ et donc, $K[x_1, x_3, \ldots, x_n]$ est isomorphe à un anneau de polynômes à $n-1$ indéterminées sur un corps. D'après le théorème de Gauss, $K[x_1, x_3, \ldots, x_n]$ est un anneau factoriel et par le théorème 4, $A[x_1^{-1}] = S^{-1}(K[x_1, x_3, \ldots, x_n])$ est aussi factoriel. D'après le théorème de Nagata on en déduit que A est factoriel.

REMARQUE - Le théorème de Klein s'étend au cas d'un corps K quelconque de caracteristique $\neq 2$ (cf. Nagata, loc. cit.).

EXEMPLES

1. Soit k un corps de caractéristique $\neq 2$ et tel que $i \notin k$ (ceci équivaut à dire que le polynôme $X^2 + 1$ est irreductible sur k). Alors l'anneau $A = k[x,y,z]$ avec $x^2 + y^2 + z^2 = 1$ est *factoriel*. En effet, comme $A/(z-1) = k[X,Y]/(X^2+Y^2)$ et $X^2 + Y^2$ est un polynôme irreductible sur k, alors $A/(z-1)$ est intègre et donc, $z-1$ est un élément premier de A. Considerons la partie multiplicative de A, $S = \{(z-1)^n\}_{n \geq 0}$. Si l'on pose $t = 1/(z-1)$, alors $x^2 + y^2 = -(z^2-1) = -(z-1)(z+1)$ nous donne $z + 1 = -t(x^2+y^2)$ et donc, $z \in k[x,y,t]$. Ceci nous montre que $A[t] = k[x,y,z,t] = k[x,y,t]$. Montrons que $k[x,y,t] = k[tx,ty,1/t]$. En effet, comme $tx, ty \in k[x,y,t]$ et aussi $1/t \in k[x,y,t]$, car $1/t = z-1$, alors $k[tx,ty,1/t] \subset k[x,y,t]$. D'autre part, étant donné que $x = (tx)(1/t)$ et $y = (ty)(1/t)$ et $t = t^2(1/t)$, il en resulte que $k[x,y,t] \subset k[tx,ty,1/t]$. On considère maintenant la partie multiplicative $T = \{1, t, t^2, \ldots, t^n, \ldots\}$ et il est clair qu'on a $A[t] = T^{-1}(k[tx,ty])$. Puisque $k[tx,ty]$ est isomorphe à un anneau de polynômes, il est factoriel et donc, $A[t]$ est aussi factoriel. Comme $A[t] = S^{-1}A$, par le théorème de Nagata il en resulte que A est aussi factoriel. On remarque finalement que T est une partie multiplicative de $k[tx,ty]$. En effet, $(tx)^2 + (ty)^2 = t^2(x^2+y^2) = t^2(1-z^2)$ et comme $z = (t+1)/t$, alors il en resulte que $(tx)^2 + (ty)^2 = -(2t+1)$ et ceci nous montre que $t \in k[tx,ty]$.

2. Soient k un corps et $T_1,\dots,T_n$ des indéterminées, avec $n\geq 3$. On considère l'anneau $A=k(T_1,\dots,T_n)[x_1,\dots,x_n]$ avec $\sum_{i=1}^{n}T_i x_i^{j(i)}=0$. Alors A est un *anneau factoriel*. En effet, x_n est un élément premier de l'anneau A, car $A/x_nA=k(T_1,\dots,T_n)[\bar{x}_1,\dots\ \bar{x}_{n-1}]$ où $\bar{x}_i$ est la classe de x_i modulo l'idéal x_nA. Par le théorème de van der Waerden, l'anneau A est intègre et comme on a la relation $\sum_{i=1}^{n-1}T_i\bar{x}_i^{j(i)}=0$ et le polynôme $\sum_{i=1}^{n-1}T_iX_i^{j(i)}$ est irreductible sur le corps $k(T_1,\dots,T_n)$, alors A/x_nA est intègre. Il en resulte que x_n est un élément premier de A et soit $S=\{1,x_n,\dots,x_n^s,\dots\}$ la partie multiplicative de A engendré par l'élément x_n. Considérons l'anneau

$$B=k[T_1,\dots,T_n;x_1,\dots,x_n,\ 1/x_n].$$

Comme $T_n=-\big(\sum_{i=1}^{n-1}T_ix_i^{j(i)}\big)/x_n^{j(n)}$, il en resulte que

$$B=k[T_1,\dots,T_{n-1};x_1,\dots,x_n,1/x_n]=S^{-1}(k[T_1,\dots,T_{n-1};x_1,\dots,x_n])$$

et comme $k[T_1,\dots,T_{n-1};x_1,\dots,x_n]$ est un anneau de polynômes il est factoriel et donc, par le théorème 4, B est aussi factoriel. On considère maintenant la partie multiplicative de $k[T_1,\dots,T_n]$, $R=k[T_1,\dots,T_n]-(0)$. On voit que

$$R^{-1}B=R^{-1}(S^{-1}(k[T_1,\dots,T_{n-1};x_1,\dots,x_n]))=$$
$$=S^{-1}(R^{-1}(k[T_1,\dots,T_{n-1};x_1,\dots,x_n]))=S^{-1}(A)=A[1/x_n];$$

comme B est factoriel, alors $R^{-1}B$ est factoriel et il en est de même pour $S^{-1}A$. Par le théorème de Nagata, A est factoriel.

REMARQUE - Dans l'exercice précedent on a employé le fait suivant: si R et S sont deux parties multiplicatives d'un anneau commutatif à élément unité A et M est un A-module unitaire, alors $R^{-1}(S^{-1}M)=S^{-1}(R^{-1}M)$. "Il s'agit... là d'un cas particulier d'un principe de commutativité des problèmes universels qu'il est difficile d'enoncer avec précision" (cf. P. Samuel, Lettres). La démonstration directe ne présente pas de difficultés.

3. Soient $\mathbf{R}$ le corps des réels et $A=\mathbf{R}[x,y]$ avec $x^2+y^2+1=0$. On va montrer que A est un *anneau factoriel*. Pour cela on va établir tout d'abord que:

(a) soit $\mathfrak{p}$ un idéal premier de A et $\varphi:A\to A/\mathfrak{p}$ l'homomorphisme canonique. Si $\varphi(x)$ est transcendant sur $\mathbf{R}$ alors φ est un isomorphisme et $\mathfrak{p}=(0)$. En effet, si $\mathfrak{p}\neq(0)$, alors il existe un $f(x,y)\in\mathfrak{p}$ tel que $f(x,y)\neq 0$ et $f(\varphi(x),\varphi(y))=0$. D'autre part, $x^2+y^2+1=0$ nous donne $\varphi(x)^2+\varphi(y)^2+1=0$ et si l'on prend le resultant des équations $f(\varphi(x),\varphi(y))=0$ et $\varphi(x)^2+\varphi(y)^2+1=0$ on voit que $\varphi(x)$ et $\varphi(y)$ sont

algébriques sur $\mathbf{R}$. Ainsi, on voit que si $\mathfrak{p}\neq(0)$ alors $\varphi(x)$ et $\varphi(y)$ sont dans le corps $\mathbf{C}$ des complexes et on va démontrer qu'il existe $a,b,c\in\mathbf{R}$ non tous nuls tels que $ax+by+c\in\mathfrak{p}$. En effet, si l'on considère la droite réelle joignant le point $(\varphi(x),\varphi(y))$ à son complexe conjugué, on voit qu'il existent des nombres réels a,b,c non tous nuls tels que $a\varphi(x)+b\varphi(y)+c=0$ et donc, $ax+by+c\in Ker(\varphi)=\mathfrak{p}$;

(b) On va montrer qu'un tel élément $ax+by+c\in\mathfrak{p}$ est premier. En effet, $A/(ax+by+c)A=\mathbf{R}[X,Y]/(X^2+Y^2+1,aX+bY+c)$ et si l'on suppose, par exemple, que $b\neq 0$, alors $(aX+bY+c)=(Y-(a'X+b'))$ (ce sont des idéaux). Ceci nous donne

$$\mathbf{R}[X,Y]/(aX+bY+c)=\mathbf{R}[X,Y]/(Y-(a'X+b'))=\mathbf{R}[X]$$

et donc,

$$A/(ax+by+c)A=\mathbf{R}[X]/(X^2+Y^2+1)=\mathbf{R}[X]/(X^2+(a'X+b')^2+1)=\mathbf{C},$$

car $X^2+(a'X+b')^2+1$ est un polynôme irreductible dans $\mathbf{R}[X]$. Ceci nous montre que $(ax+by+c)A$ est un idéal maximal de A;

(c) On va déduire de (a) et (b) que l'anneau A est factoriel, au moyen du théorème de Nagata. En effet, soit S la partie multiplicative de A engendrée par les $ax+by+c$ tels que $(a,b)\neq(0,0)$. D'après ce qu'on vient de voir (partie (a)), tous les idéaux premiers de A qui sont $\neq(0)$ rencontrent S et comme les idéaux premiers de $S^{-1}A$ sont en correspondance biunivoque avec les idéaux premiers de A qui ne rencontrent pas S (cf. théorème 3), il en resulte que le seul idéal premier de $S^{-1}A$ est (0). Ceci nous montre que $S^{-1}A$ est un corps, donc factoriel. Par le théorème de Nagata, A est aussi factoriel.

§4. LIEN AVEC LA GÉOMÉTRIE ALGÉBRIQUE

Soit A un anneau commutatif à élément unité. On dit qu'un idéal premier $\mathfrak{p}$ est de *hauteur zero* (notation: $h(\mathfrak{p})=0$) s'il est minimal parmi tous les idéaux premiers de A. Par exemple, si A est intègre, le seul idéal premier de A de hauteur zero est $\mathfrak{p}=(0)$. On dira qu'un idéal premier $\mathfrak{p}$ de A est de *hauteur un* ($h(\mathfrak{p})=1$) s'il est minimal parmi les idéaux premiers de A qui ne sont pas de hauteur zero. Si A est intègre, un idéal premier de hauteur un est un idéal minimal parmi les idéaux premiers $\neq(0)$. En général, on dit qu'un idéal premier $\mathfrak{p}$ de A est de *hauteur* n (notation: $h(\mathfrak{p})=n$) s'il est minimal parmi les idéaux premiers de A qui ne sont pas de hauteur $0,1,\dots,n-1$.

LEMME - *(Théorème de Krull) - Soit A noethérien. Alors tout élément non inversible de A est contenu dans au moins un idéal premier de hauteur* 1 (cf. D. G. Northcott, Ideal Theory, Cambridge University Press 1953; Chap. III, §3.5, Th. 6).

THÉORÈME 6 - *Soit A un anneau noethérien intègre. Pour que A soit factoriel il faut et il suffit que tout idéal premier de A de hauteur* 1 *soit principal.*

En effet, supposons que A soit factoriel et soit $\mathfrak{p}$ un idéal premier de A tel que $h(\mathfrak{p})=1$. Puisque $\mathfrak{p}\neq(0)$, alors il existe un $a\in\mathfrak{p}$ tel que $a\neq 0$ et comme A est factoriel on peut écrire $a=up_1\dots p_n$, où u est inversible dans A et les p_i sont extremaux. Comme $a\in\mathfrak{p}$ et $u\notin\mathfrak{p}$, alors $p_1\dots p_n\in\mathfrak{p}$ et donc, il existe un indice i tel que $p_i\in\mathfrak{p}$. On va montrer que $\mathfrak{p}=Ap_i$. En effet, comme A est factoriel, alors Ap_i est un idéal premier de A; d'autre part, on a $Ap_i\subset\mathfrak{p}$ et $h(\mathfrak{p})=1$ et ceci nous montre que $\mathfrak{p}=Ap_i$.

Réciproquement, il suffit de démontrer que tout élément extremal de A est premier. En effet soit $q\in A$ un élément extremal. Comme q n'est pas inversible par définition, il existe, d'après le lemme précedent, un idéal premier $\mathfrak{p}$ de A tel que $q\in\mathfrak{p}$ et $h(\mathfrak{p})=1$. Par hypothèse, $\mathfrak{p}$ est principal et donc, on peut écrire $\mathfrak{p}=Ap$ avec p premier. On peut alors écrire que $q=cp$ avec $c\in A$ et comme q est extremal, alors c est inversible dans A. Ceci nous montre que q et p sont associés et donc, q est premier.

Soient maintenant k un corps, V une k-variété affine, $I_k(V)$ l'idéal de V et $A=k[X_1,\dots,X_n]/I_k(V)=k[x_1,\dots,x_n]$ l'anneau de coordonnées affines de V sur k. On sait que A est noethérien intègre. Les idéaux premiers de A définissent les sous-k-variétés de V et aux idéaux premiers de hauteur 1 de A correspondent les sous-k-variétés de codimension 1. Le théorème 6 nous montre alors que si *A est factoriel, toute sous-k-variété de V de codimension* 1 *est une intersection complète, c'est à dire, qu'elle est définie par une seule équation.*

CHAPITRE IV

COMPLÉTÉS DE CERTAINS ANNEAUX

§1. IDÉAUX MAXIMAUX

Soient A un anneau commutatif à élément unité et $\mathfrak{m}$ un idéal de A. On dira que $\mathfrak{m}$ est un *idéal maximal de A*, s'il est maximal parmi les idéaux de A qui sont $\neq A$. On voit facilement que $\mathfrak{m}$ est un idéal maximal de A si et seulement si $A/\mathfrak{m}$ est un corps et en particulier, tout idéal maximal est premier, car un corps est un anneau intègre. On va démontrer trois propriétés qui nous seront essentielles par la suite:

THÉORÈME 1 - *(Théorème de Krull-Zorn sur l'existence d'idéaux maximaux) - Dans un anneau commutatif à élément unité A, tout idéal de A qui est $\neq A$ est contenu dans un idéal maximal de A.*

En effet, soit $\mathfrak{a}\neq A$ un idéal de A (ceci équivaut à $1\notin\mathfrak{a}$) et considérons la famille $\mathcal{F}$ d'idéaux de A telle que si $\mathfrak{b}\in\mathcal{F}$, alors $\mathfrak{b}\neq A$ ($\Leftrightarrow 1\notin\mathfrak{b}$) et $\mathfrak{a}\subset\mathfrak{b}$. La famille $\mathcal{F}$ est $\neq\emptyset$ et si l'on met sur $\mathcal{F}$ l'ordre partiel donné par l'inclusion, alors $\mathcal{F}$ est inductive. En effet, il suffit de voir que l'unité n'appar-