PUBLICATIONS

MATHEMATIQUES

D'ORSAY

André NÉRON

NOTIONS ÉLÉMENTAIRES DE GÉOMÉTRIE ALGÉBRIQUE

(cours 1964-65, retirage 1979)

Université de Paris-Sud

Département de Mathématique

Bât. 425

91405 ORSAY France

PUBLICATIONS

MATHEMATIQUES

D'ORSAY

André NÉRON

NOTIONS ÉLÉMENTAIRES DE GÉOMÉTRIE ALGÉBRIQUE

(cours 1964-65, retirage 1979)

Université de Paris-Sud

Département de Mathématique

Bât. 425

91405 **ORSAY** France

TABLE DES MATIERES

TABLE DES MATIERES (Suite).

CHAPITRE 0 : Préliminaires

A. Anneaux locaux, valuations et places.

1. Anneau local d'un idéal premier.

Soient A un anneau intègre unitaire, K son corps des fractions, P un idéal premier de A, et ϕ l'homomorphisme canonique $A \to A/P$.

L'ensemble des éléments de K qui sont de la forme $\frac{a}{b}$, avec $a, b \in A$, et $b \notin P$ est un sous-anneau de K, qu'on note A_P, et qu'on appelle anneau local de l'idéal P (une définition "intrinsèque" des anneaux locaux sera donnée au n° suivant).

Exemples : si $A = \mathbb{Z}$, et si $P = (p)$, où p est un nombre premier, $A_P = \mathbb{Z}_{(p)}$ est l'anneau composé des fractions à dénominateur premier à p.

Si $A = k[X]$ (polynômes à une variable), et si $P = (X-a)$, A_P est l'anneau des fractions rationnelles qui sont définies pour $x = a$.

L'anneau A_P a même corps des fractions K que A.

THEOREME 1.

Soit k le corps des fractions de l'anneau $B = A/P$. Il existe un et un seul homomorphisme $\psi : A_P \to k$ prolongeant $\phi : A \to B$. Cet homomorphisme est surjectif. Son noyau est PA_P (idéal de A_P engendré par P) ; il coïncide avec l'ensemble de tous les éléments inversibles de A_P, et contient tous les idéaux propres (i.e. $\neq A_P$) de A_P.

Démonstration. Soit $x \in A_P$, de la forme $\frac{a}{b}$ $(a, b \in A, b \notin P)$. On a $\phi(b) \neq 0$, d'où nécessairement

$$(1) \qquad \psi(x) = \frac{\phi(a)}{\phi(b)} .$$

Ceci prouve l'unicité de ψ. Inversement, $\frac{\phi(a)}{\phi(b)}$ ne dépend que de $x = \frac{a}{b}$, et l'application $\psi : A_P \to k$ définie par (1) est un homomorphisme prolongeant ϕ (vérifications triviales). Comme ϕ est surjectif, ψ l'est également.

Pour que x appartienne au noyau de ϕ, il faut et il suffit

.../...

qu'on ait $\varphi(a) = 0$, i.e. $a \in P$. On a alors $x = a \cdot \frac{1}{b} \in PA_P$.
Inversement, si $x \in PA_P$, on a $x = \sum_i \frac{a_i}{b_i}$ ($a_i \in P$, $b_i \notin P$), d'où $\psi(x) = 0$. On a donc bien $\ker \psi = PA_P$.

Si $y \in A_P$ est non inversible, de la forme $\frac{a}{b}$ ($b \notin P$), on a $\frac{b}{a} \notin A_P$, donc $a \in P$, donc $y \in PA_P$. D'autre part, l'idéal PA_P , de même que tout idéal propre de A_P est composé d'éléments non inversibles de A_P .

2. <u>Anneaux locaux</u>.

<u>THEOREME 2</u>

Soit A un anneau intègre unitaire. Les trois propriétés suivantes sont équivalentes.

(a) - L'ensemble des élements non inversibles de A est un idéal M de A ,

(b) - A possède un idéal maximal unique (ou, ce qui est équivalent, un idéal maximum) M'.

(c) - A possède un idéal premier M'' tel que $A = A_{M''}$. Si ces conditions sont satisfaites, on a de plus $M = M' = M''$.

<u>Démonstration</u>.

(a) $\Longrightarrow$ (b). En effet, M contient tout idéal propre de A , donc est maximum.

(b) $\Longrightarrow$ (a). En effet, tout élément de M' est non inversible, car $M' \neq A$. Réciproquement, si $y \in A$ est non inversible, on a $(y) \neq A$, donc $(y) \subset M'$, donc $y \in M'$.

(c) $\Longleftrightarrow$ (a). En effet, la relation $A = A_{M''}$ signifie que les inverses des éléments $x \in A$, tels que $x \notin M''$, sont dans A , ou encore que les éléments de A non inversibles sont dans M'' .

Un anneau A vérifiant l'une des conditions équivalentes (a), (b) ou (c) est dit <u>local</u>. Le quotient A/M est un corps, appelé <u>corps résiduel</u> de A .

.../...

L'anneau local A_p considéré au n° 1 est bien un anneau local, puisqu'il vérifie la condition (b), d'après le th. 1. D'autre part, tout anneau local est de la forme A_p, d'après (c) du th. 2.

Nouveaux exemples d'anneaux locaux.

Tout corps est un anneau local.

Si k est un corps, l'anneau de séries formelles $k[[X]]$ est local, et admet pour idéal maximal (X). Plus généralement, si A est local d'idéal maximal $\underline{m}$, $A[[X]]$ est local, et admet pour idéal maximal $\underline{m}$ $A[[X]]$.

3. Corps projectifs.

A tout corps K, on associe l'ensemble $K_\infty = K \cup \{\infty\}$ obtenu par adjonction à K d'un élément, noté ∞. On prolonge les opérations de K en posant $a + \infty = \infty$, et, pour $a \neq 0$, $a.\infty = \infty$; les symboles $\infty+\infty$ et $0.\infty$ ne sont pas définis. L'ensemble K_∞, muni de cette structure, est appelé corps projectif associé à K.

On convient de poser $0^{-1} = \infty$ et $\infty^{-1} = 0$, de sorte que l'application $x \mapsto x^{-1}$ de K_∞ dans lui-même est bijective.

4. Anneaux de valuation.

Soit A un anneau intègre unitaire, de corps des fractions K. On dit que A est un anneau de valuation si, pour tout $x \in K^*$, on a x ou $x^{-1} \in A$. On peut encore exprimer cette condition par la relation $K_\infty = A \cup A^{-1}$, en appelant A^{-1} l'ensemble des inverses des éléments de A

THEOREME 3.

Tout anneau de valuation est local.

Démonstration. Il suffit de montrer que l'ensemble des éléments non inversibles de A est un idéal, et, pour x, $y \in A$ non inversibles, $x+y$ est non inversible. On peut supposer x et y non tous les deux nuls. D'après l'hypothèse, on a $\frac{x}{y}$ ou $\frac{y}{x} \in A$. Si on a, par exemple $\frac{y}{x} \in A$, la somme $x+y = x(1+\frac{y}{x})$ est multiple de x dans A. Comme x est non inversible, il en est de même de $x + y$.

.../...

Exemples.

1. Si A est factoriel (par exemple, si $A = \mathbb{Z}$, ou si $A = k[X_1,\ldots, X_n]$, et si p est un élément extrémal (ou irréductible) de A , l'anneau local $A_{(p)}$ est un anneau de valuation.

2. L'anneau de séries formelles $k[[X]]$ est un anneau de valuation (l'ensemble des séries formelles non inversibles est en effet l'idéal principal (X)).

3. Pour $A = k[X,Y]$, et $P = (X,Y)$, l'anneau local A_P n'est pas un anneau de valuation, car on a $\frac{X}{Y} \notin A_P$, et $\frac{Y}{X} \notin A_P$.

5. Places.

Soient A un anneau de valuation, K son corps des fractions, M son idéal maximal, $k = A/M$ son corps résiduel, et soit ϕ l'homomorphisme canonique $\phi : A \to k$. Si x est un élément de K_∞ , n'appartenant pas à A , son inverse x^{-1} est un élément non inversible de A ; on a donc $x^{-1} \in M$, d'où $\phi(x^{-1}) = 0$. Il est donc naturel de prolonger ϕ à une application $\rho : K_\infty \to k_\infty$, en posant, pour un tel x , $\rho(x) = \infty$. L'application ρ est appelée place canonique associée à A du corps K . Le théorème suivant va permettre de donner une caractérisation intrinsèque de la notion de place.

THEOREME 4.

Soient K et k deux corps, et soit ρ une application $K_\infty \to k_\infty$. Les deux conditions suivantes sont équivalentes :

(a) - On a $\rho(1) = 1$, et

$$\rho(a+b) = \rho(a) + \rho(b)$$

$$\rho(a.b) = \rho(a) . \rho(b).$$

toutes les fois que les expressions figurant dans les deux membres ont un sens.

(b) - Il existe un anneau de valuation A de K (admettant K comme corps des fractions), dont le corps résiduel k' est isomorphe

.../...

à sous-corps de k, et tel que ρ soit le composé de cet isomorphisme avec la place canonique associée à A.

(La condition (b) peut encore s'énoncer comme suit : si $x \in K_\infty$, et $x \notin A$, on a $\rho(x) = \infty$ et, d'autre part, ρ induit sur A un homomorphisme dont le noyau est M).

<u>Démonstration</u>: (a) $\Rightarrow$ (b). Posons $A = \rho^{-1}(k)$. On a $\infty \notin A$; i.e. $\rho(\infty) = \infty$, car sinon, on aurait $\rho(1+\infty) = \rho(1) + \rho(\infty)$, d'où $\rho(1)=0$. D'après (a), A est un sous-anneau de K, et ρ induit un homomorphisme $A \to k$. Soit $x \in K$. Alors, pour que $x \notin A$, i.e. $\rho(x) = \infty$, il faut et il suffit qu'on ait $\rho(x^{-1}) = 0$. (car, pour $x \neq 0$ et ∞, on a $\rho(xx^{-1}) = \rho(1) = 1$). Donc $x \notin A$ implique $x^{-1} \in A$, et, par suite A est un anneau de valuation. De plus, l'idéal maximal de A est $M = \phi^{-1}(0) = \phi^{-1}(0)$.

(b) $\Rightarrow$ (a) : Vérification facile ; on examine successivement les différents cas dans lesquels l'élément ∞ intervient dans les formules à démontrer.

Une application $\rho : K_\infty \to k_\infty$ vérifiant les conditions équivalentes (a) ou (b) est appelée une <u>place</u> de K, à valeurs dans k. L'anneau de valuation A est dit <u>associé</u> à ρ.

Deux places $K_\infty \to k_\infty$ et $K_\infty \to k'_\infty$ sont dites <u>équivalentes</u> si on passe de l'une à l'autre au moyen d'un isomorphisme $k \to k'$. En particulier, d'après le théorème précédent, toute place surjective est équivalente à la place canonique de son anneau associé.

<u>Exemples</u>

1. <u>Place triviale</u> : On dit que ρ est triviale si elle est injective, i.e. si elle induit un monomorphisme de K dans k.

2. Soit $K = k(X)$ (corps des fractions rationnelles à une variable), et soit $a \in k$. A toute fractions $f \in K$, associons $f(a)$

.../...

en convenant que $f(a) = \infty$ si f n'est pas définie en a . L'application $f \mapsto f(a)$ est une place de K , à valeurs dans k .

3. La composée de deux places est une place (vérification facile, en utilisant (a)).

6. Valuations.

Soient A un anneau intègre, K son corps des fractions, U le sou sous-groupe de K^* composé des éléments inversibles de A , Considérons dans K^* , la relation de divisibilité $b \backslash a$ (b divise a), relative à A , définie par la condition $\frac{a}{b} \in A$. C'est une relation de préordre (i.e. réflexive et transitive), compatible avec la multiplication, qui fait donc de K^* un groupe préordonné. Pour qu'on ait $b \backslash a$ et $a \backslash b$, il faut et il suffit que $\frac{b}{a} \in U$. Par passage au quotient, on obtient donc sur le quotient K^*/U une structure de groupe ordonné.

Pour que A soit un anneau de valuation, il faut et il suffit que l'ordre du groupe $\Gamma = K^*/U$ soit total, comme il résulte des définitions. Le groupe Γ est alors totalement ordonné. D'autre part, l'homomorphisme canonique $\alpha : K \to \Gamma$ vérifie alors la condition

(*) $\alpha(x+y) \geq \inf (\alpha(x), \alpha(y))$

(car si on a, par exemple, $\alpha(x) \geq \alpha(y)$, on a $\frac{x}{y} \in A$, d'où $1+\frac{x}{y} = \frac{x+y}{y} \in A$, d'où $\alpha(x+y) \geq \alpha(y)$).

Γ étant un groupe commutatif totalement ordonné, quelconque, on convient

1. de noter additivement la loi de Γ .

2. d'adjoindre à Γ deux éléments $-\infty$, ∞ ; on convient de plus que, pour $a \in \Gamma$, on a $-\infty \leq a \leq \infty$; l'ensemble $\Gamma \cup \{\infty, -\infty\}$, noté également Γ_∞ , est ainsi muni d'une relation d'ordre total, prolongeant celle de Γ.

Si on prolonge α en posant $\alpha(0) = \infty$, $\alpha(\infty) = -\infty$, la relation (*) reste vraie quels que soient x et $y \in K_\infty$, non infinis tous les deux.

.../...

Définition. On appelle valuation d'un corps K une application $\omega : K_\infty \to \Gamma_\infty$ (où Γ est un groupe totalement ordonné) vérifiant les conditions suivantes

(1) $\omega(x.y) = \omega(x) + \omega(y)$

toutes les fois que les expressions figurant dans les deux membres ont un sens

(2) $\omega(x+y) \geq \inf(\omega(x), \omega(y))$.

Deux valuations sont dites équivalentes si on passe de l'une à l'autre par un isomorphisme $\Gamma \to \Gamma'$ de groupes totalement ordonnés.

D'après ce qui précède, à tout anneau de valuation de corps des fractions K, il correspond une valuation $K_\infty \to \Gamma_\infty$, où $\Gamma = K^*/U$, dite valuation canonique associée à A.

Réciproquement, soit ω une valuation de K. L'ensemble des $x \in K$ tels que $\omega(x) \geq 0$ est un anneau de valuation de K (en effet, les relations $\omega(x) \geq 0$ et $\omega(x) \leq 0$ se traduisent respectivement par $x \in A$ et $x^{-1} \in A$), et ω est équivalente à la valuation canonique associée à A (car le noyau de ω est $A-M = U$). On dit que A et M sont respectivement l'anneau et l'idéal de la valuation ω.

K étant un corps, la donnée d'un anneau de valuation A de K équivaut, d'après ce qui précède, à celle d'une classe de valuations équivalentes ω de K, ou encore à celle d'une classe de places équivalentes ρ de K.

L'anneau A, l'idéal maximal M, et le groupe $U = A-M$ des éléments inversibles de A sont caractérisés, à partir de la donnée de ω ou de ρ, par le tableau suivant :

x	$\omega(x)$	$\rho(x)$
$\in A$	≥ 0	$\neq \infty$
$\in M$	> 0	$= 0$
$\in U$	$= 0$	$\neq 0$ et ∞

.../...

Exemples de valuations.

1. Valuation triviale : $\omega(x) = 0$ pour tout $x \in K$ non nul. Pour que ω soit triviale, il faut et il suffit que $A = K$, ou encore que la place associée (unique à l'équivalence près) soit triviale.

2. Valuation p-adique. Soient A un anneau factoriel, de corps des fractions K, et soit p un élément extrémal de A, i.e. tel que (p) soit un idéal premier. Pour $x \in K^*$, il existe un et un seul entier $\alpha \in \mathbb{Z}$ tel qu'on ait $x = p^\alpha y$, y appartenant au groupe U des éléments inversibles de $A_{(p)}$. On définit une valuation ω de K, dite valuation p-adique de K, en posant $\omega(x) = \alpha$. L'anneau de valuation correspondant est $A_{(p)}$ (vérifications faciles).

3. On définit une valuation du corps de fractions rationnelles $k(X)$ à une variable en posant $\omega(\frac{f}{g}) = \deg g - \deg f$.

4. On définit une valuation du corps de séries formelles $k((X))$ en posant $\omega(s) = n$, pour $s = a_n X^n + a_{n+1} X^{n+1} + \ldots$, avec $a_n \neq 0$.

Exercice : déterminer dans les exemples ci-dessus l'anneau de valuation et la place canonique associés à ω.

THEOREME 5.

Soit A un anneau principal, et K son corps des fractions. Toute valuation ω de K qui est ≥ 0 sur A est la valuation triviale, ou bien est une valuation p-adique.

(Rappelons que tout anneau principal est factoriel).

Démonstration. L'ensemble P des $x \in A$ tels que $\omega(x) > 0$ est un idéal de A. On a $P = A \cap M_\omega$ où M_ω est l'idéal de ω ; donc P est premier. Si $P = (0)$, la valuation ω est nécessairement triviale. Sinon, P est un idéal de A, nécessairement propre (car $1 \notin P$), donc de la forme (p), où p est un élément extrémal de A. Montrons que l'anneau A_ω de ω coïncide avec $A_{(p)}$. En effet, soit $x \in A_\omega$;

.../...

comme A est factoriel, on peut écrire x sous forme de fraction irréductible $\frac{a}{b}$; on a alors a ou $b \notin (p)$; on ne peut avoir $a \notin (p)$, et $b \in (p)$; on a donc $b \notin (p)$, c'est à dire $x \in A_{(p)}$; inversement il est clair que $A_{(p)} \subset A_\omega$; on a donc bien $A_\omega = A_{(p)}$, ce qui montre bien que ω est équivalente à la valuation p-adique.

Corollaire 1. Les seules valuations de $\mathbb{Q}$ sont la valuation triviale et les valuations p-adiques. (Remarquer que toute valuation ω de $\mathbb{Q}$ est positive sur $\mathbb{Z}$, puisque $\omega(n) \geq \inf(\omega(1),\ldots,\omega(1)) = \omega(1) = 0$).

Corollaire 2. Les seules valuations du corps de fractions rationnelles $k(X)$ s'annulant sur k sont les valuations f-adiques, où f est un élément extrémal (i.e. un polynôme irréductible) de $k[X]$, et la valuation définie par le degré, introduite dans l'exemple 3 précédent.

En effet, si ω est positive sur $k[X]$, c'est une valuation f-adique. Sinon, on a nécessairement $\omega(X) < 0$, d'où $\omega(Y) > 0$, en posant $Y = X^{-1}$. Dans ce cas ω est positive sur $k[Y]$, donc ω est une valuation g-adique, avec $g \in k[Y]$, irréductible. La relation $\omega(Y) > 0$ entraine $Y \in (g)$, d'où $(Y) = (g)$, donc ω est la valuation Y-adique de $K = k(Y)$. Pour $f \in k(X)$, de la forme $\frac{F(X)}{G(X)}$, où F et G sont des polynômes de degrés respectifs m et n, on a $f(\frac{1}{Y}) = Y^{n-m} f_0(Y)$, où f_0 est une fraction rationnelle de valeur finie et $\neq 0$ pour $Y = 0$. On a donc $\omega(f) = n-m = \deg G - \deg F$.

7. Valuations discrètes.

Définition. On dit qu'une valuation ω non triviale est discrète si le groupe Γ de ses valeurs est cyclique. Le groupe Γ étant nécessairement infini (puisque totalement ordonné), il est isomorphe à $\mathbb{Z}$. Les valuations des exemples donnés ci-dessus sont toutes triviales ou discrètes.

THEOREME 6.

Soient A un anneau intègre, K son corps des fractions. Les pro-

.../...

priétés suivantes sont équivalentes :

(a) - A est un anneau de valuation discrète

(b) - A est principal et local

(c) - A est principal, et ne possède qu'une classe d'éléments extrémaux

(d) - A est local, noéthérien, et son idéal maximal est principal.

(e) - A est un anneau de valuation noéthérien.

<u>Démonstration</u>

(a) $\Longrightarrow$ (b) . Soit I un idéal propre de A . Si $x \in I$, x est non inversible, et on a donc $\omega(x) > 0$. Soit $a \in I$, tel que $\omega(a)$ soit minimum. Pour tout $x \in I$, on a $\omega(x) \geq \omega(a)$, donc $\omega(\frac{x}{a}) \geq 0$, d'où $\frac{x}{a} \in A$, i.e. $x \in (a)$. On a donc $I = (a)$.

(b) $\Longleftrightarrow$ (c) . En effet, dans un anneau principal, un élément u est irréductible si et seulement si (u) est maximal. L'existence d'un seul idéal maximal équivaut donc à celle d'une seule classe d'éléments irréductibles.

(b) $\Longrightarrow$ (d) et (e). Car A étant principal, est noéthérien.

(d) $\Longrightarrow$ (a). En effet, soit $M = (u)$ l'idéal maximal de A . Comme A est intègre noéthérien, l'intersection des puissances de M est réduite à (0) (théorème de Krull). Donc, pour $x \in A$, non nul, il existe un et un seul entier $\mu \geq 0$ tel qu'on ait $x \in (u^{\mu})$ et $x \notin (u^{\mu+1})$, i.e. tel que $x = u^{\mu} x_o$, avec $x_o \in A$ inversible. Plus généralement, on en déduit que, pour $y \in K$, non nul, il existe un et un seul entier $\nu \in \mathbf{Z}$ tel qu'on ait $y = u^{\nu} y_o$, où y_o est un élément inversible de A . En posant $\omega(y) = \nu$, on définit une valuation discrète de K , admettant A pour anneau associé.

(e) $\Longrightarrow$ (d) . En effet, soit M l'idéal maximal de A .

Il est engendré par un nombre fini d'éléments t_i $(1 \leq i \leq h)$. Si ω est la valuation associée à A , on a $\omega(t_i) > 0$ pour tout i . Choisissons parmi les t_i , un élément u de valuation minimum. On a ,

.../...

pour tout i , $\omega(t_i) \geq \omega(u)$, d'où $\omega(\frac{t_i}{u}) \geq 0$, i.e. $\frac{t_i}{u} \in A$, ou encore $t_i \in (u)$ pour tout i . On a donc $M = (u)$.

8. Le théorème de prolongement.

THEOREME 7

Soit A un sous-anneau d'un corps K . Tout homomorphisme φ de A dans un corps algébriquement clos k peut être prolongé à une place de K , à valeurs dans k .

LEMME. Pour tout idéal I de A , et pour $x \in K$, I engendre un idéal non trivial dans l'un des deux anneaux $A[x]$ ou $A[\frac{1}{x}]$.

En effet, dans le cas contraire, on aurait :

$$(1) \qquad 1 = \textstyle\sum_{i=0}^{p} a_i \, x^i$$
$$(2) \qquad 1 = \textstyle\sum_{j=0}^{q} b_j \, (\frac{1}{x})^j \qquad (a_i \, , \, b_j \in I)$$

Supposons que chacun des entiers p , q est le plus petit possible pour fixer les idées, supposons $p \geq q$. (1) et (2) s'écrivent encore

$$a_o - 1 + a_1 \, x + \ldots + a_p \, x^p = 0$$
$$b_q + b_{q-1} \, x + \ldots + (b_o - 1) \, x^q = 0 \, .$$

En multipliant respectivement les deux équations par $b_o - 1$ et $a_p \, x^{q-p}$, et en ajoutant, on trouve une relation de la forme

$$1 + c_o + c_1 \, x + \ldots + c_{p-1} \, x^{p-1} = 0$$

avec $c_i \in I$ pour tout $i \geq 0$. Ceci contredit le choix de p .

Démonstration du théorème.

On peut supposer A local, car $\varphi(A)$ étant intègre, le noyau de φ est un idéal premier p ; φ se prolonge à A_p de manière unique d'après le th. 1. Montrons que, pour $x \in K^*$, φ se prolonge à un homomorphisme de $A[x]$ ou de $A[\frac{1}{x}]$ dans k . Soit, en effet, M l'idéal maximal de A , noyau de φ . D'après le lemme, M engendre un idéal non trivial dans $A[x]$ ou $A[\frac{1}{x}]$. Supposons par exemple $M\,A[x]$ non trivial. Soit M_1 un idéal maximal de $A[x]$ contenant $M\,A[x]$. On a $M_1 \cap A = M$: en effet, on a $M \subset M_1 \cap A$, $M_1 \cap A \neq A$ (puisque $1 \notin M_1$), et M est maximal. Posons $k_1 = A[X]/M_1$. L'homomorphisme canonique .../...

$\phi_1 : A[x] \to k_1$ prolonge ϕ (le corps $k_o = \mathrm{Im}\,\phi$ étant identifié, par isomorphisme, à un sous-corps de k_1). De plus, si l'on pose $x_1 = \phi_1(x)$, on a $\mathrm{Im}\,\phi_1 = k_o[x_1] = k_o(x_1) = k_1$. Donc x_1 est algébrique sur k_o , et k_1 s'identifie, par isomorphisme, à un sous-corps de k , contenant k_o . On a donc bien prolongé ϕ à un homomorphisme $A[x] \to k$.

Considérons l'ensemble $\mathcal{E}$ des couples (B , ψ) composés d'un sous-anneau B de K contenant A , et d'un homomorphisme ψ de B sur un sous-corps de k , prolongeant ϕ . Dans cet ensemble $\mathcal{E}$, considérons la relation $(B , \psi) \leq (B' , \psi')$ définie par les conditions : $B \subset B'$, et ψ' prolonge ψ . On vérifie immédiatement que c'est une relation d'ordre, et que $\mathcal{E}$ est inductif pour cette relation. D'après le th. de Zorn, $\mathcal{E}$ possède un élément maximal $(\tilde{B} , \tilde{\psi})$. Comme on ne peut prolonger $\tilde{\psi}$, on a d'après ce qui précède, pour $x \in K^*$, l'une des deux relations $x \in \tilde{B}$ ou $\frac{1}{x} \in \tilde{B}$. Autrement dit, $\tilde{B}$ est un anneau de valuation de K . De plus $\tilde{k} = \mathrm{Im}\,\tilde{\psi}$ est un sous-corps de k . Donc $\mathrm{Ker}\,\tilde{\psi}$ est un idéal maximal de $\tilde{B}$. C'est donc l'unique idéal maximal $\tilde{M}$ de $\tilde{B}$ et $\tilde{\psi}$ s'identifie à l'homomorphisme canonique $\tilde{B} \to \tilde{B}/\tilde{M}$. Il suffit alors de prendre pour ρ la place canonique de K associé à $\tilde{B}$. En effet, ρ prolonge $\tilde{\psi}$, et est à valeurs dans k .

Corollaire. Soit K un corps, et soit L une extension de K . Toute valuation ω de K peut être prolongée à une valuation de L .

On se ramène en effet au théorème précédent, en utilisant la correspondance entre valuations et places.

B. Eléments entiers

1. Définition.

Soient A et B deux anneaux intègres unitaires, tels que $A \subset B$. Un élément x de B est dit entier sur A s'il existe un polynôme $P \in A[X]$ unitaire tel que $P(x) = 0$, i.e. si on a une relation de la forme

$$(1) \qquad x^n + a_1 x^{n-1} + \ldots + a_n = 0 ,$$

où $a_i \in A$ pour tout i. En particulier, x est algébrique sur le corps des fractions K de A. Si $A = K$ est un corps, les notions d'élément entier et d'élément algébrique sur K cïncident.

THEOREME 1

Pour $x \in B$, les propriétés suivantes sont équivalentes :

(a) - x est entier sur A

(b) - $x \in A[\frac{1}{x}]$

(c) - $A[x]$ est un A-module de type fini

(d) - $A[x]$ est contenu dans un sous-anneau A' de B qui est un A-module de type fini.

Démonstration

(a) $\Longleftrightarrow$ (b). En effet, en explicitant la relation $x \in A[\frac{1}{x}]$, on voit qu'elle se traduit par une relation de dépendance intégrale de la forme (1).

(a) $\Longrightarrow$ (c). En effet, supposons que x est solution de (1). Il suffit de montrer que $A[x]$ coïncide avec le A-module B engendré par $1, x, \ldots, x^{n-1}$, ou encore qu'on a $x^{n+p} \in B$ pour tout $p \geqslant 0$. Or ceci se voit, par récurrence sur p, en remarquant qu'on a $x^{n+p} + a_1 x^{n+p-1} + \ldots + a_n x^p = 0$.

(c) $\Longrightarrow$ (d) Trivial

(d) $\Longrightarrow$ (a). En effet, soit $A[x] \subset A' = Au_1 + \ldots + Au_n$

Pour tout j, on a $x u_j \in A'$, d'où

$$x u_j = \textstyle\sum_i a_{ij} u_i$$

.../...

avec $a_{ij} \in A$ $(1 \leq i \leq n, 1 \leq j \leq n)$. On a donc, pour tout j,

$$\sum_i (\delta_{ij}\, x - a_{ij})\, u_i = 0$$

où δ_{ij} est le symbole de Kronecker. Comme A' est intègre, et comme les u_i ne sont pas tous nuls, le déterminant de la matrice $(\delta_{ij}\, x - a_{ij})$ est nul. Ce déterminant est un polynôme unitaire en x. c.q.f.d

2. Fermeture et clôture intégrale.

Un anneau A' contenant A est dit entier sur A si tous ses éléments sont entiers sur A. En particulier, tout anneau A' de type f fini sur A (comme A-module) est entier sur A. Si M est un sous-ensemble de B composé d'éléments entiers sur A, l'anneau engendré $A[M]$ est entier sur A. Si $A \subset B \subset C$, si B est entier sur A et si C est entier sur B, C est entier sur A (toutes ces propriétés se démontrent facilement en utilisant (d) du th. 1, et les propriétés des modules de type fini).

L'ensemble des éléments de B qui sont entiers sur A est un sous-anneau $\bar{A}$ de B, appelé fermeture intégrale de A dans B. Si $A = \bar{A}$, A est dit intégralement fermé dans B. On a toujours $\bar{\bar{A}} = \bar{A}$.

Un anneau A intègre est dit intégralement clos s'il est intégralement fermé dans son corps des fractions K. La fermeture intégrale de A dans K est un sous-anneau de K, appelé clôture intégrale de A

Tout anneau factoriel A est intégralement clos.

En effet, pour $x \in K$, on a $x = \frac{p}{q}$, avec $p, q \in A$, premiers entre aux. Si x est entier sur A, on a $(\frac{p}{q})^n + a_1 (\frac{p}{q})^{n-1} + \dots + a_n = 0$, d'où l'on déduit, en chassant les dénominateurs $p^n + q\,(a_1 p^{n-1} + \dots) = 0$. Donc q divise p^n. Comme q est premier avec p, on a $q=1$, d'où $x \in A$.

Exemples.

1. $A = \mathbb{Z}[\sqrt{5}]$ n'est pas intégralement clos ; en effet le nombre $\frac{1+\sqrt{5}}{2}$ est entier sur $\mathbb{Z}$, donc aussi sur A, mais n'appartient pas à A.

.../...

2. (Exercice). Plus généralement, montrer que, pour $m \in Z$, non multiple d'un carré, l'anneau $Z[\sqrt{m}]$ est intégralement clos si et seulement si on a $m \not\equiv 1 \pmod 4$.

3. L'anneau $A = k[X,Y]/(Y^2 - X^3)$, ou anneau de coordonnée de la courbe d'équation $Y^2 - X^3 = 0$ (cf. plus loin, Chap I) n'est pas intégralement clos.

En effet, si x et y sont les éléments de A respectivement représentés par X et Y, on a $\frac{y}{x} \notin A$; ; cependant on a $\frac{y^2}{x^2} = x$, donc $\frac{y}{x}$ est entier sur A.

3. Eléments entiers et valuations

THEOREME 2 .

Soit A un sous-anneau d'un corps K, et soit $x \in K$. Les propriétés suivantes sont équivalentes

(a) - x est entier sur A

(b) - x appartient à tout anneau de valuation de K qui contient A.

(c) - Toute valuation de K positive sur A est positive en x.

(d) - Toute place de K finie sur A est finie en x.

Démonstration.

(b) $\Longleftrightarrow$ (c) $\Longleftrightarrow$ (d), d'après les propriétés des valuations et des places (paragraphe A, n° 6).

(a) $\Longrightarrow$ (c). En effet, si x est entier sur A, on a $x \in A[\frac{1}{x}]$. Soit ω une valuation de K, positive sur A. Si on avait $\omega(x) < 0$, on aurait $\omega(\frac{1}{x}) > 0$, et ω serait ≥ 0 sur $A[\frac{1}{x}]$, donc en x, d'où contradiction.

(d) $\Longrightarrow$ (a). Supposons en effet qu'il existe $x \in K$, non entier sur A, i.e. tel que $x \notin A' = A[\frac{1}{x}]$. L'élément $y = \frac{1}{x}$ de A' est non inversible. On peut donc trouver un idéal maximal M de A' contenant y, et prolonger l'homomorphisme canonique $A' \to A'/M$ à une place

.../...

ρ du corps des fractions de B . Cette place est finie sur A' , donc aussi sur A . D'autre part, on a $\rho(y) = 0$, d'où $\rho(x) = \infty$, ce qui contredit (d).

Corollaire 1. Tout anneau de valuation, ou toute intersection d'anneaux de valuation, est un anneau intégralement clos.

Corollaire 2. Si K est le corps des fractions de A , la clôture intégrale de A est l'intersection de tous les anneaux de valuation de K contenant A .

THEOREME 4.

Soient A un anneau intégralement clos, K son corps des fractions, L une extension algébrique séparable de degré fini de K . Alors la fermeture intégrale $\overline{A}$ de A dans L est contenue dans un sous-A-module B de L , de type fini, et de rang $n = [L : K]$.

Démonstration. On peut trouver $x \in L$, entier sur A , tel que $L = k(x)$. En effet, d'après le théorème de l'élément primitif, il existe $y \in L$, tel que $L = k(y)$. Comme y est algébrique sur K , on a $b_o y^n + \ldots + b_n = 0$, où les b_i appartiennent à A . On peut alors prendre $x = b_o y$, car on a $x^n + b_o b_1 x^{n-1} + \ldots + b_o^{n-1} b_n = 0$.

Pour $z \in L$, on a $z = \sum_{i=0}^{n-1} a_i x^i$, avec $a_i \in K$. Comme x est séparable sur K , il admet n conjugués distincts, qui sont de la forme x^{σ_j} $(1 \leq j \leq n)$, où les σ_j sont des K-automorphismes de la clôture algébrique $\overline{K}$ de K , et le déterminant D de la matrice $(x^{\sigma_j})^i$ est $\neq 0$. On a, pour tout j ,

(2) $$z^{\sigma_j} = \sum_i a_i (x^{\sigma_j})^i$$

Résolvons (2), regardé comme système linéaire aux inconnues $a_1, \ldots, a_n$ au moyen des formules de Cramer, soit $a_i = \frac{D_i}{D}$ $(1 \leq i \leq n)$. Les déterminants D , D_i appartiennent à l'anneau $A[x^{\sigma_1}, \ldots, x^{\sigma_n}]$, donc sont entiers sur A . En exprimant D comme déterminant de Vandermonde, on voit que D^2 est invariant par tout K-automorphisme de $\overline{K}$.

.../...

On a donc $D^2 \in K$. Puisque $a_i = \frac{DD_i}{D^2} \in K$, on a aussi $DD_i \in K$. Comme D^2 et $DD_i = b_i$ sont entiers sur A , et comme A est intégralement clos, on a $D^2 \in A$, et $b_i = DD_i \in A$. On a donc $z = \frac{1}{D^2} \sum_i b_i x^i \in \frac{1}{D^2} A[x]$. Or $\frac{1}{D^2} A[x]$ est bien un A-module de rang n .

<u>Corollaire 1.</u> Si, avec les mêmes hypothèses, on suppose de plus que A est <u>noethérien</u>, $\overline{A}$ est un A-module de type fini. (car tout sous-module d'un module de type fini sur un anneau noethérien est de type fini).

<u>Corollaire 2.</u> Si, avec les mêmes hypothèses, on suppose A <u>principal</u>, $\overline{A}$ est un A-module libre de rang $n = [L : K]$.

En effet, on a $A[x] \subset \overline{A} \subset \frac{A[x]}{D^2}$. Comme A est principal, le module $\overline{A}$, compris entre deux A-modules libres de rang n , est aussi un A-module libre de rang n .

C - Extensions transcendantes.

1. Dépendance algébrique.

Soit E une extension d'un corps k, et soient $x_1, \ldots, x_n$ des éléments de E. On dit que les x_i sont algébriquement dépendants sur k s'il existe un polynôme $P \in k[X_1, \ldots, X_n]$ non nul tel que $P(x_1, \ldots, x_n) = 0$, i.e. si le noyau de l'homomorphisme canonique $k[X_1, \ldots, X_n] \xrightarrow{\alpha} k[x_1, \ldots, x_n]$ (tel que $X_i \to x_i$) est $\neq 0$. Dans le cas contraire, on dit que les x_i sont algébriquement indépendants, ou qu'ils forment une famille algébriquement libre sur k. Dans ce dernier cas, α est un isomorphisme. Plus généralement une famille quelconque d'éléments de E (éventuellement infinie) est dite algébriquement libre si toutes ses sous-familles finies sont algébriquement libres. Si G est une famille d'éléments de E, on dit que G engendre E/k, ou que G est un système de générateurs de E/k, au sens de la dépendance algébrique si E est extension algébrique de $k(G)$.

La théorie de la dépendance algébrique est analogue à celle de la dépendance linéaire pour les espaces vectoriels. On peut du reste obtenir ces deux théories comme cas particuliers d'une théorie plus générale de la dépendance. On se borne, dans les deux n° qui suivent, à rappeler les énoncés de quelques résultats essentiels. Pour les démonstrations voir exemple Bourbaki, Algèbre, Chap. V.

2. Bases de transcendance.

THEOREME 1. Soit B une famille d'éléments d'une extension E d'un corps k. Les propriétés suivantes sont équivalentes :

a) - B est une famille algébriquement libre sur k maximale d'éléments de E.

b) - B est une famille algébriquement libre sur k, et B

.../...

est un système de générateurs de E/k (au sens de la dépendance algébrique).

c) - B est un système de générateurs minimal de E (au sens de la dépendance algébrique).

Toute famille B possèdant l'une et l'autre des propriétés équivalentes (a) (b) (c) du théorème est appelé une <u>base de transcendance</u> de E sur R.

Par exemple, le corps de fractions rationnelles $k(X_i)_{i \in I}$ admet pour base de transcendance la famille des indéterminées $(X_i)_{i \in I}$.

<u>THEOREME 2</u>. Toute extension E de k admet une base de transcendance.

(L'ensemble des familles libres sur k d'éléments de E est en effet inductif ; on applique le théorème de Zorn).

<u>THEOREME 3</u>. Deux bases quelconques de l'extension E/k sont équipotentes. En particulier, si E admet une base de transcendance composée de n éléments, toute autre base admet aussi n éléments.

Dans ce dernier cas, le nombre n est appelé <u>degré de transcendance</u> de l'extension. On le note deg.tr.(E/k). Notons que, pour qu'une extension soit algébrique, il faut et il suffit que son degré de transcendance soit 0.

3. <u>Extensions algébriquement disjointes</u>.

<u>THEOREME 4</u>. Soient E/k et F/k deux sous-extensions d'une même extension K/k. Les conditions suivantes sont équivalentes :

(a) - Toute famille d'éléments de E libre sur k est libre sur F.

(b) - La réunion d'une sous-famille libre de E/k et d'une sous-famille libre de F/k est une sous-famille libre de K/k.

.../...

(c) - $E \cap F$ est extension algébrique de k (i.e. deg.tr. $(E \cap F) = 0$).

Lorsque l'une ou l'autre de ces conditions est remplie on dit que les sous-extensions E/k et F/k sont <u>algébriquement disjointes</u>, ou que les corps E et F sont algébriquement disjoints sur k.

Autres caractérisations (on conserve les mêmes notations).

<u>THEOREME 5</u>. Soit B une base de transcendance de E/k. Pour que E/k et F/k soient algébriquement disjointes, il faut et il suffit que B soit une base de transcendance de EF/F.

<u>THEOREME 6</u>. Soient B une base de transcendance de E/k, et C une base de transcendance de F/k. Pour que E/k et F/k soient algébriquement disjointes, il faut et il suffit que $B \cup C$ soit une base de transcendance de EF/k.

D'autre part

<u>THEOREME 7</u>. L'extension EF/k est de degré de transcendance fini si et seulement si chacune des extensions E/k et F/k est de degré de transcendance fini. Pour que E/k et F/k soient algébriquement disjointes, il faut et il suffit qu'on ait

$$\text{deg. tr. } (EF/k) = \text{deg. tr. } (E/k) + \text{deg. tr. } (F/k) .$$

4. <u>Extensions linéairement disjointes</u>.

<u>THEOREME 8</u>. Soient E/k et F/k deux sous-extensions d'une extension K/k. Les conditions suivantes sont équivalentes.

(a) - Toute famille finie (x_i) d'éléments de E linéairement indépendante sur k est linéairement indépendante sur F.

(b) - Pour toute famille finie (x_i) d'éléments de E linéairement indépendants sur k, et pour toute famille finie (y_j) d'éléments de F linéairement indépendants sur k., la famille $(x_i\, y_j)$ est linéairement indépendante sur k.

.../...

Démonstration.

(a) $\Longrightarrow$ (b) - $\Sigma_{i,j}\ a_{ij}\ x_i\ y_j = 0 \Longrightarrow \Sigma_i\ a_{ij}\ x_i = 0\ \ \forall j \Longrightarrow$

$$\Longrightarrow a_{ij} = 0\ \forall i \text{ et } j .$$

(b) $\Longrightarrow$ (a) - Soit (u_j) une base de F/k . Soit $\Sigma\ b_i\ x_i = 0$, avec $b_i \in F$. On a, pour tout i, $b_i = \Sigma\ a_{ij}\ u_j$, avec $a_{ij} \in k$, d'où $\Sigma_{i,j}\ a_{ij}\ x_i\ u_j = 0$, d'où, compte tenu de (b), $a_{ij} = 0$ $\forall i$ et j , d'où $b_i = 0\ \forall i$.

Lorsque l'une ou l'autre des conditions (a) ou (b) du th. est remplie, on dit que les extensions E/k et F/k sont linéairement disjointes, ou que les corps E et F sont linéairement disjoints sur k .

Autre interprétation : la condition (b) signifie que l'application k-linéaire canonique $E \otimes_k F \to EF$ déduite de $(x,y) \mapsto xy$ est injective.

Remarques. 1 - Si E/k et F/k sont linéairement disjointes, on a $E \cap F = k$. Mais la réciproque est fausse (prendre $k = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt[3]{2})$, et $F = \mathbb{Q}(j\ \sqrt[3]{2})$.

2 - Pour que E/k et F/k soient linéairement disjointes, il faut et il suffit que, pour tout couple de sous-extensions E'/k , F'/k de type fini de E/k et F/k respectivement E'/k et F'/k soient linéairement disjointes.

Autres caractérisations (les notations sont celles du théorème 8; le mot base d'une extension signifie base de l'espace vectoriel sous-jacent).

THEOREME 9. Soit S une base de E/k . Pour que E/k et F/k soient linéairement disjointes, il faut et il suffit que S soit une base de EF/F .

THEOREME 10. Soient S une base de E/k, et T une base de

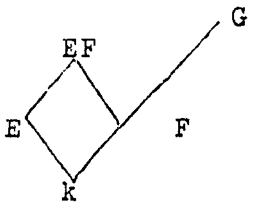
.../...

F/k. Pour que E/k et F/k soient linéairement disjointes, il faut et il suffit que ST (famille des produits d'un élément de S par un élément de T) soit une base de EF/k .

Ces théorèmes résultent trivialement de la définition; d'autre part

THEOREME 11. Pour que E/k et F/k soient de degré fini, il faut et il suffit que EF/k soit de degré fini. Dans ce cas, pour que E/k et F/k soient linéairement disjointes il faut et il suffit qu'on ait $[EF : k] = [E : k]\ [F : k]$.

THEOREME 12. Soient E/k et G/k deux sous-extensions d'une extension K/k , et soit F/k une sous-extension de G/k .



Les propriétés suivantes sont équivalentes

a) - E/k et G/k sont linéairement disjointes.

b) - E/k et F/k sont linéairement disjointes, et il en est de même de EF/F et G/F.

Démonstration.

Soit S une base de E/k

(a) $\Longrightarrow$ (b). En effet, d'après (a), et d'après le théorème 9 , S est une base de EG/G . C'est donc une famille linéairement indépendante sur F d'éléments de EF. Mais c'est aussi un système de générateurs de EF/F. C'est donc une base de EF/F. On en déduit (b), compte tenu du théorème 9 .

(b) $\Longrightarrow$ (a). On applique à nouveau le théorème 9. De (b) on déduit que S est une base de EF/F, puis que c'est une base de EG/G .

THEOREME 13. Soient E/k et F/k deux sous-extensions d'une extension K/k . Si elles sont linéairement disjointes, elles sont algébriquement disjointes.

Demonstration.

Soit (x_i) une famille algébriquement libre sur k d'éléments de E. Les monômes $M(x_i)$ sont alors linéairement indépendants sur k. Ils le sont donc aussi sur F.

5. Extensions régulières, séparables, primaires.

Soit K/k une extension), et considérons les corps $\bar{k}$ (clôture algébrique), $\bar{k}_r$ (clôture radicielle) et $\bar{k}_s$ (clôture séparable) de k, regardes comme sous-corps de $\bar{K}$.

Si les extensions

K/k et $\bar{k}/k$ sont linéairement disjointes, on dit que l'extension K/k est régulière

K/k et $\bar{k}_r/k$ " " " " " est séparable

K/k et $\bar{k}_s/k$ " " " " " est primaire.

Si k est algébriquement clos (resp. radiciellement clos, i.e. parfait, resp. séparablement clos), toute extension de k est regulière (resp. séparable, resp. primaire).

On déduit du th. précédent les conséquences suivantes :

THEOREME 14. Toute sous-extension d'une extension régulière (resp. séparable, resp.primaire) est regulière (resp. séparable, resp. primaire).

THEOREME 15. Si $F \supset E \supset k$, et si chacune des deux extensions, F/E et E/k est régulière (resp. séparable, resp. primaire), l'extension F/k est régulière (resp. séparable, resp. primaire).

THEOREME 16. Toute extension régulière est séparable et primaire.

Exemple d'extension régulière:

THEOREME 17. Pour toute famille d'indéterminées $(X_i)_{i \in I}$ (finie ou non), le corps de fractions rationnelles $K = k(X_i)_{i \in I}$

.../...

est extension régulière de k.

Démonstration.

Il suffit de montrer que toute extension algébrique k' de degré fini de k est linéairement disjointe de K sur k. Pour cela, on remarque que toute base de k'/k est aussi une base de K'/K, en posant $K' = k'(X_i)_{i \in I}$.

6. Caractérisation des extensions séparables.

Démontrons au préalable :

THEOREME 18. Soient E/k et F/k deux sous-extensions algébriques d'une extension K/k. Si l'une est séparable, et l'autre radicielle, elles sont linéairement disjointes.

D'après la remarque 2 du n° 4, on peut supposer que les extensions E/k et F/k sont de degré fini. Si l'extension E/k est séparable, elle est monogène, i. e. de la forme $k(x)$; si $n = [k(x) : k]$, elle admet pour base $B = \{1, x, \ldots, x^{n-1}\}$. Supposons F/k radicielle. Il suffit de montrer que B est une base i.e. que B est une famille linéairement indépendante, de l'extension $F(x)/F$: Supposons en effet qu'on ait $\sum_1^{n-1} a_i x^i = 0$, avec des $a_i \in F$ non nuls. Soit p la caractéristique. Il existe un entier $f \geq 0$ tel que $a_i^{p^f} \in k$ pour tout i. On a alors une relation $Q(x^{p^f}) = 0$, avec $Q \in k[X]$ non nul, de degré $\leq n-1$. Le polynôme $Q[X^{p^f}]$ est donc multiple du polynôme irréductible $P = \mathrm{Irr}_k\, x$ de x sur k. Or P admet exactement n racines distinctes dans $\bar{k}$, tandis que $Q[X^{p^f}]$ en admet $n-1$ au plus $\Longrightarrow$ contradiction.

On dit qu'une base de transcendance B d'une extension K/k est séparante si K est algébrique séparable sur $k(B)$.

.../...

THEOREME 13. Soit K/k une extension. Les trois propriétés suivantes sont équivalentes

(a) - K/k est séparable

(b) - K et $k^{\frac{1}{p}}$ sont linéairement disjoints sur k.

(c) - Toute sous-extension de type fini de K/k admet une base de transcendance séparante.

Démonstration.

(a) $\Longrightarrow$ (b) trivial

(b) $\Longrightarrow$ (c). On peut supposer K/k de type fini, soit $K = k(x_1, \ldots, x_n)$. Posons $r = \text{deg.tr.}\,(K/k)$, et raisonnons par récurrence sur l'entier positif $s = n-r$. Le résultat est trivial pour $s = 0$, i.e. $n = r$. Supposons $n > r$. Il existe $P \in k[X_1, \ldots, X_n]$ non nul tel que $P(x_1, \ldots, x_n) = 0$. Choisissons P de degré global d le plus petit possible. Montrons que P ne peut appartenir à l'anneau $k[X_1^p, \ldots, X_n^p]$. En effet, dans ce dernier cas, d serait multiple de p, soit $d = p\,d'$, et on aurait une relation de la forme $\sum_\alpha a_\alpha M_\alpha(x)^p = 0$, avec des $a_\alpha \in k$ non tous nuls, où les M_α sont des monômes de degré $\leq d'$. On en déduirait $\sum_\alpha a_\alpha^{\frac{1}{p}} M_\alpha(x) = 0$, autrement dit les $M_\alpha(x)$ seraient linéairement dépendants sur $k^{\frac{1}{p}}$. Ils le seraient donc aussi sur k, et on en déduirait une relation $Q(x) = 0$, avec $Q \in k[X_1, \ldots, X_n]$ de degré $\leq d'$. Comme on a $d' < d$, ceci contredirait le choix de P.

On a donc $P \notin k[X_1^p, \ldots, X_n^p]$. L'une des indéterminées, par exemple X_n, intervient dans P autrement que par sa puissance p-ième. Par suite, x_n est séparable sur $K' = k(x_1, \ldots, x_{n-1})$. D'après l'hypothèse de récurrence, l'extension K'/k admet une base de transcendance séparante, donc il en est de même de K/k.

(c) $\Longrightarrow$ (a). Soit $(u) = (u_1, \ldots, u_n)$ une base de transcendance séparante de K/k. Le corps $k(u) = k(u_1, \ldots, u_n)$ est

---/---

extension régulière, donc séparable de k, d'après le théorème 7 i.e. linéairement disjoint de $\bar{k}_r$ sur k. Le composé $\bar{k}_r k(u)$ est extension radicielle de $k(u)$. Comme K est extension algébrique separable de $k(u)$, les corps $\bar{k}_r\, k(u)$ et K sont linéairement disjoints sur k (th. 18). Il suffit alors d'appliquer le th. 12.

Complément.

La démonstration précédente prouve en outre que si K/k est de type fini, de la forme $k(M)$, avec $M = \{x_1, \dots, x_n\}$, on peut extraire de M une base de transcendance séparante.

7. Caractérisation des extensions régulières.

THEOREME 20. Pour qu'une extension K/k soit régulière, il faut et il suffit qu'elle soit séparable, et que k soit algébriquement fermé dans K.

Démonstration.

La condition est trivialement nécessaire. Pour montrer qu'elle est suffisante, considérons d'abord un $x \in \bar{k}$, et montrons que K et $k(x)$ sont linéairement disjoints sur k. En effet, posons $f = \mathrm{Irr}_k\, x$, et $n = \deg f = [k(x) : k]$. Les puissances $1, \dots, x^{n-1}$ forment une base de $k(x)/k$. Or f est irréductible dans $K[X]$: en effet, tout facteur de f dans $K[X]$ a ses coefficients dans $\bar{k} \cap K = k$, donc est constant ou égal à f. Donc $1, \dots, x^{n-1}$ forment une base de $K(x)/K$, ce qui prouve bien la disjonction linéaire de K et $k(x)$ sur k.

Soient maintenant x_i des éléments de K linéairement indépendants sur k, et supposons qu'ils soient liés par une relation de la forme $\sum_1^q a_i\, x_i = 0$, avec des $a_i \in \bar{k}$ non tous nuls. En appelant p la caractéristique, il existerait un entier m tel que $b_i = a_i^{p^m}$ soit algébrique séparable sur k pour tout i.

.../...

On aurait $\sum b_i x_i^{p^m} = 0$; Or, d'après le théorème de l'élément primitif, l'extension $k(b_1, \ldots, b_q)/k$, étant séparable, est monogène ; d'après ce qui précède, elle est donc disjointe de K sur k. Les $x_i^{p^m}$ seraient donc linéairement dépendants sur k, i.e. il existerait des $c_i \in k$ non tous nuls tels que $\sum_i c_i x_i^{p^m} = 0$. On en déduirait $\sum_i c_i^{p^{-m}} x_i = 0$, avec des coefficients $c_i \in \bar{k}_r = k^{p^{-\infty}}$ non tous nuls, ce qui contredirait la séparabilité de l'extension K/k.

<u>Lemme</u>. Soit K un corps, et soit $K \xrightarrow{\sigma} K'$ un isomorphisme. Soit L une extension algébrique de K. Alors toute place ρ de L prolongeant σ est triviale (i.e. est un isomorphisme de L sur une extension de K').

En effet, il suffit de montrer que, si $x \in L$, la relation $\rho(x) = 0$ implique $x = 0$. Or, si $f = \mathrm{Irr}_k\, x$, on a $f(x) = 0$, d'où $f(\rho(x)) = f(0) = 0$. Le terme constant de f est nul, donc f ne peut être que le polynôme X, et on a $x = 0$.

<u>THEOREME 20</u>. Soient K/k et L/k deux sous-extensions d'une même extension de k, et supposons K/k <u>régulière</u>. Alors, pour que K/k et L/k soient algébriquement disjointes, il faut et il suffit qu'elles soient linéairement disjointes.

<u>Démonstration</u>.

D'après le théorème de prolongement, il existe une place ρ_o de L, à valeurs dans $\bar{k}$, induisant l'identité sur k. Soit $u_1, \ldots, u_r$ une base de transcendance de K/k ; si K et L sont linéairement disjointes sur k les u_j sont linéairement indépendants sur L.

On peut prolonger ρ_o à une place ρ de KL, telle que les images $u_j' = \rho(u_j)$ soient des éléments algébriquement indépendants sur k. Alors ρ induit un isomorphisme $K \xrightarrow{\sigma} K'$,

.../...

où K' est une extension algébrique de $k(u'_1, \dots, u'_r)$ (d'après le lemme). Soient x_i des éléments de K linéairement indépendants sur k. Supposons qu'ils soient liés par une relation $\sum a_i x_i = 0$, avec des $a_i \in L$ non tous nuls. Notons ω la valuation associée à ρ, et choisissons l'indice i_o de façon que $\omega(a_{i_o})$ soit minimum. Alors, on a $\omega(a_i/a_{i_o}) \geq 0$, d'où $\rho(a_i/a_{i_o}) \neq \infty$ pour tout i. En appliquant ρ aux deux membres de la relation $\Sigma(a_i/a_{i_o})x_i = 0$ on trouve $\sum b_i x'_i = 0$, en posant $x'_i = \sigma(x_i)$, et $b_i = \rho(a_i/a_{i_o})$. Or on a $b_{i_o} = 1$. Donc les x'_i sont linéairement indépendants sur k. Par isomorphisme il en est de même des x_i c.q.f.d.

CHAPITRE I

ENSEMBLES et VARIETES AFFINES

1. Définitions.

On se donne un corps k, commutatif, et un corps algébriquement clos K contenant k.

Soit F une famille de polynômes appartenant à l'anneau $k[X_1,..X_n]$ (qu'on notera parfois $k[X]$, par abréviation).

Un point $x = (x_1,\dots, x_n)$ de K^n est appelé un zéro de F si on a $f_i(x_1,\dots, x_n) = 0$ pour tout i.

L'ensemble des zéros d'une telle famille F est appelé un ensemble algébrique affine, ou plus précisément, un k-ensemble algébrique affine. On le désigne par $\mathcal{Y}(F)$, ou $\mathcal{Y}_K(F)$.

Soit d'autre part E un sous-ensemble quelconque de K^n. L'ensemble des polynômes $f \in k[X] = k[X_1,\dots, X_n]$ s'annulant en tout point de E est un idéal de l'anneau $k[X]$, qu'on note $\mathfrak{I}(E)$, ou $\mathfrak{I}_k(E)$.

2. Propriétés des symbôles $\mathcal{Y}(F)$ et $\mathfrak{I}(E)$.

On a les implications évidentes

(1) $\quad F_1 \supset F_2 \quad \Longrightarrow \quad \mathcal{Y}(F_1) \subset \mathcal{Y}(F_2)$

(2) $\quad E_1 \supset E_2 \quad \Longrightarrow \quad \mathfrak{I}(E_1) \subset \mathfrak{I}(E_2)$

On a d'autre part

(3) $\quad \mathcal{Y}(\mathfrak{I}(E)) \supset E$

(4) $\quad \mathfrak{I}(\mathcal{Y}(F)) \supset F$

On en déduit

$$\mathfrak{I}(\mathcal{Y}(\mathfrak{I}(E))) = \mathfrak{I}(E)$$

(appliquer $\mathfrak{I}$ aux deux membres de (3), et faire $F = \mathfrak{I}(E)$ dans (4)).

On a de même

$$\mathcal{Y}(\mathfrak{I}(\mathcal{Y}(F))) = \mathcal{Y}(F)$$

Autrement dit, pour tout ensemble algébrique S, on a

(5) $\quad \mathcal{Y}(\mathfrak{I}(S)) = S \quad .$

.../...

L'application $S \mapsto \mathfrak{J}(S)$ de l'ensemble des k-ensembles algébriques affines sur celui des idéaux de $k[X]$ est donc injective, tandis que l'application $I \mapsto \mathcal{J}(I)$ du second ensemble sur le premier est surjective. On a pour tout I, la relation $\mathfrak{J}(\mathcal{J}(I)) \supset I$, d'après (4), mais non l'égalité, en général (on verra plus loin que $\mathfrak{J}(\mathcal{J}((I) = \text{rac } I)$, de sorte que les applications $\mathcal{J}$ et $\mathfrak{J}$ ne sont pas bijectives.

On a les relations suivantes (conséquences triviales des définitions)

(6) $\mathcal{J}(F_1 \cup F_2) = \mathcal{J}(F_1) \cap \mathcal{J}(F_2)$

(7) $\mathfrak{J}(E_1 \cup E_2) = \mathfrak{J}(E_1) \cap \mathfrak{J}(E_2)$

D'autre part, on a, quels que soient les idéaux I_1, I_2,

(8) $\mathcal{J}(I_1 \cap I_2) = \mathcal{J}(I_1) \cup \mathcal{J}(I_2)$

En effet, on a $\mathcal{J}(I_1 \cap I_2) \supset \mathcal{J}(I_1)$ et de même $\mathcal{J}(I_1 \cap I_2) \supset \mathcal{J}(I_2)$, d'où $\mathcal{J}(I_1 \cap I_2) \supset \mathcal{J}(I_1) \cup \mathcal{J}(I_2)$.

D'autre part, supposons qu'il existe $x \in K^n$ tel qu'on ait $x \notin \mathcal{J}(I_1)$, $x \notin \mathcal{J}(I_2)$, et $x \in \mathcal{J}(I_1) \cap \mathcal{J}(I_2)$. Soient $f_1 \in I_1$ et $f_2 \in I_2$, telles qu'on ait $f_1(x) \neq 0$, et $f_2(x) \neq 0$. On a $f_1 f_2 \in I_1 \cap I_2$, d'où $f_1(x)\, f_2(x) = 0$, d'où contradiction. On a bien démontré (8).

3. k-ensembles algébriques affines irréductibles (ou k-variétés affines)

On dit qu'un k-ensemble algébrique affine S est irréductible s'il n'est pas réunion non triviale de deux k-ensembles algébriques, i.e. si une relation de la forme $S = S_1 \cup S_2 \Longrightarrow S = S_1$ ou $S = S_2$. On dit aussi que S est une k-variété affine.

THEOREME 1.

Pour qu'un k-ensemble algébrique affine S soit irréductible, il faut et il suffit que son idéal associé $\mathfrak{J}(S)$ soit premier.

Démonstration. Supposons $\mathfrak{J}(S)$ premier. Si $S = S_1 \cup S_2$, on a $\mathfrak{J}(S) = \mathfrak{J}(S_1) \cap \mathfrak{J}(S_2) \supset \mathfrak{J}(S_1) . \mathfrak{J}(S_2)$, donc $\mathfrak{J}(S) \supset \mathfrak{J}(S_1)$ ou $\mathfrak{J}(S_2)$. Si,

.../...

par exemple, on a $\mathfrak{J}(S) \supset \mathfrak{J}(S_1)$, on en déduit $S \subset S_1$, d'où $S = S_1$. Donc S est irréductible.

Réciproquement, supposons S irréductible. Si $\mathfrak{J}(S)$ n'est pas premier, il existe f_1 et $f_2 \in k[X]$, tels qu'on ait $f_1 \notin \mathfrak{J}(S)$, $f_2 \notin \mathfrak{J}(S)$, et $f_1 f_2 \in \mathfrak{J}(S)$. Considérons les idéaux $I_1 = \mathfrak{J}(S) + (f_1)$, $I_2 = \mathfrak{J}(S) + (f_2)$, et posons $S_1 = \mathfrak{V}(I_1)$, $S_2 = \mathfrak{V}(I_2)$. Les k-ensembles algébriques S_1 et S_2 sont contenus dans S , et distincts de S Pour montrer, par exemple, qu'on a $S_1 \neq S$, on note que, puisque $f_1 \notin \mathfrak{J}(S)$, on peut trouver $x_1 \in S$ tel que $f_1(x_1) \neq 0$, d'où $x_1 \notin S_1$). D'autre part, on a $S = S_1 \cup S_2$. En effet, soit $x \in S$. Puisque $f_1 f_2 \in \mathfrak{J}(S)$, on a $f_1(x)\, f_2(x) = 0$, d'où $f_1(x) = 0$ ou $f_2(x) = 0$. Si par exemple, on a $f_1(x) = 0$, x est un zéro de $I_1 = (S) + (f_1)$, autrement dit $x \in S_1$. On a donc bien $S = S_1 \cup S_2$, et S est réductible, contrairement à l'hypothèse.

4. <u>Le théorème des zéros</u>

<u>Lemme de Normalisation</u> (E. Noether). Soit K un corps algébriquement clos, et soit L une extension de type fini de K , i.e. de la forme $L = K(x_1,\dots, x_n)$. Soit d le degré de transcendance de l'extension L/K . Il existe des éléments a_{ij} de K $(1 \leq i \leq n$, $1 \leq j \leq d)$ tels que, en posant $y_j = \sum_{i=1}^{n} a_{ij}\, x_i$ $(1 \leq j \leq d)$, les x_i soient entiers sur l'anneau $K[y_1,\dots, y_d]$.

<u>Démonstration</u>. On peut supposer $n > d$, sinon la solution est triviale (car il suffit de prendre $y_i = x_i$), et raisonner par récurrence sur $n-d$.

Puisque $n > d$, l'un des x_i est algébrique sur le corps engendré par les x_j d'indice $j \neq i$. Par exemple, x_n est algébrique sur $k(x_1,\dots, x_{n-1})$. D'après l'hypothèse de récurrence, il existe des $a'_{ij} \in K$ $(1 \leq i \leq n-1$, $1 \leq j \leq d)$ tels que, en posant

.../...

$y'_j = \sum_{i=1}^{n-1} a'_{ij}\, x_i$, les x_i $(1 \leq i \leq n-1)$ soient algébriques entiers sur $k[y'_1, \ldots, y'_d]$. Dans ces conditions, x_n est algébrique sur $k(y'_1, \ldots, y'_d)$, i.e. on a

$$F(y'_1, \ldots, y'_d , x_n) = 0 ,$$

où F est un polynôme à coefficients dans K . Posons

$$(9) \qquad y_j = y'_j + b_j\, x_n \qquad\qquad (1 \leq j \leq d)$$

où les b_j sont des éléments de K , provisoirement arbitraires. Les relations ci-dessus entraînent

$$(10) \qquad F(y_1 - b_1\, x_n , \ldots, y_d - b_d\, x_n , x_n) = 0 .$$

Notons F_o le polynôme homogène formé avec les termes de plus haut degré h (par rapport à l'ensemble des variables) du polynôme F . En développant le premier membre de (10), on trouve que le terme en x_n^h a pour coefficient $F_o(-b_1, \ldots, -b_d , 1)$. Comme K est infini, on peut choisir les b_j de façon que ce coefficient soit $\neq 0$. La relation (10) entraine alors que x_n est entier sur l'anneau $k[y_1, \ldots, y_d]$. D'après les relations (9), les y'_j sont également entiers sur cet anneau. D'après la transitivité de la dépendance intégrale, il en est de même des x_i $(1 \leq i \leq n-1)$.

<u>THEOREME 2</u> (Théorème des zéros de Hilbert)

Soit I un idéal propre de $A = k[X_1, \ldots, X_n]$. Alors on a $\mathcal{J}(I) \neq \emptyset$ (i.e. I possède au moins un zéro).

<u>Démonstration</u>. On se ramène immédiatement au cas où $I = P$ est premier (en remplaçant, s'il y a lieu, I par un idéal maximal le contenant). Considérons l'homomorphisme canonique $\phi : A \to A/P$, et posons $\phi(X_i) = x_i$ $(1 \leq i \leq n)$. Soit d le degré de transcendance du corps $k(x_1, \ldots, x_n)$ sur k . D'après le lemme de normalisation, il existe des éléments a_{ij} de k $(1 \leq i \leq n,\ 1 \leq j \leq d)$, tels que les x_i soient entiers sur $K[y] = K[y_1, \ldots, y_d]$. Soient $b_1, \ldots, b_d$ des éléments

.../...

quelconques de K .

Il existe un K-homomorphisme $\psi : K[y] \to K$ tel que $\psi(y_j) = b_j$ $(1 \leq j \leq d)$. On peut, d'après le th. de prolongement (Chap. 0, A, th. 7) construire une place ρ de $K(x)$ prolongeant ψ . Comme ρ est finie sur l'anneau $K[y]$, ρ est finie en x_i (Chap. 0, B, th.2) Comme le point $x = (x_1,\ldots, x_n)$ appartient à $\mathfrak{V}(I)$, il en est de même du point $a = (a_1,\ldots,a_n)$ (où $a_i = \rho(x_i)$) i.e. le point a est un zéro de I.

Corollaire 1. Pour tout idéal I de $k[X_1,\ldots, X_n]$, on a $\mathfrak{J}(\mathfrak{V}(I)) = \text{rad } I$.

Démonstration. On a évidemment $\text{rad } I \subset \mathfrak{J}(\mathfrak{V}(I))$. Il suffit donc de prouver l'inclusion opposée $\mathfrak{J}(\mathfrak{V}(I)) \subset \text{rad } I$.

Soit $f \in \mathfrak{J}(\mathfrak{V}(I))$. Soient $f_1,\ldots, f_m$ un système de générateurs de I . Considérons les polynômes $f_1(X),\ldots, f_n(X)$, $1 - Tf(X)$ de l'anneau $k[X,T] = k[X_1,\ldots, X_n, T]$ des polynômes à $n+1$ variables sur k ; ils n'admettent, dans K^{n+1} , aucun zéro commun : en effet si $z = (x_1,\ldots, x_n, t)$ est un tel zéro, le point $x = (x_1,\ldots, x_n)$ de K^n appartient à $\mathfrak{V}(I)$, donc est un zéro de f , et $1 - Tf(X)$ prend la valeur 1 en z , ce qui est contradictoire. D'après le théorème des zéros, les polynômes $f_1(X),\ldots, f_n(X)$, $1 - Tf(X)$ engendrent l'idéal trivial (1). Autrement dit, il existe des polynômes $g_1,\ldots, g_m$, $g \in k[X_1,\ldots, X_n , T]$ tels qu'on ait $g_1 f_1 + \ldots + g_m f_m + g\,(1-Tf) = 1$. En substituant $\frac{1}{f}$ à T dans cette relation, on obtient

$$\sum_{i=1}^{m} g_i(X_1,\ldots, X_m , \frac{1}{f(X_1,\ldots,X_m)})\, f_i(X_1,\ldots, X_m) = 1 .$$

En chassant les dénominateurs, on en déduit une relation de la forme

$$\sum_{i=1}^{m} h_i(X_1,\ldots, X_m)\, f_i(X_1,\ldots, X_m) = f(X_1,\ldots, X_m)^s ,$$

où les h_i sont des polynômes, et s un entier ≥ 1 . Autrement dit, on a $f \in \text{rad } I$. On a donc bien $\mathfrak{J}(\mathfrak{V}(I)) \subset \text{rad } I$.

.../...

<u>Corollaire 2</u>. Si P est un idéal premier, on a $\mathfrak{I}(\mathfrak{V}(P)) = P$. Donc le symbole $\mathfrak{V}$ induit une <u>application bijective de l'ensemble des idéaux premiers de $k[X]$ sur celui des k-ensembles algébriques irréductibles</u> ; l'application réciproque est induite par $\mathfrak{I}$.

<u>Corollaire 3</u>. Soit I un idéal de $k[X] = k[X_1, \ldots, X_n]$. Pour que I soit de la forme $\mathfrak{I}(E)$, avec $E \subset K^n$, il faut et il suffit que $I = \text{rad } I$.

En effet, si $I = \mathfrak{I}(E)$, on a aussi $I = \mathfrak{I}(\mathfrak{V}(\mathfrak{I}(E)) = \mathfrak{I}(\mathfrak{V}(I)) = \text{rad } I$

Réciproquement, la relation $I = \text{rad } I$, s'écrit $I = \mathfrak{I}(\mathfrak{V}(I))$, et on peut prendre $E = \mathfrak{V}(I)$.

<u>Corollaire 4</u>. Soient S_1 et S_2 deux k-ensembles algébriques, et soit T une k-variété. Si on a $T \subset S_1 \cup S_2$, on a $T \subset S_1$ ou $T \subset S_2$.

En effet, la relation $T \subset S_1 \cup S_2$ entraîne $\mathfrak{I}(T) \supset \mathfrak{I}(S_1) \cap \mathfrak{I}(S_2)$ d'où $\mathfrak{I}(T) \supset \mathfrak{I}(S_1) . \mathfrak{I}(S_2)$. Comme $\mathfrak{I}(T)$ est premier, il contient donc $\mathfrak{I}(S_1)$ ou $\mathfrak{I}(S_2)$. Si, par exemple, on a $\mathfrak{I}(T) \supset \mathfrak{I}(S_1)$, on a $T \subset S_1$.

<u>THEOREME 3.</u>

Tout k-ensemble algébrique S s'exprime d'une manière unique comme réunion finie non triviale de k-variétés (le terme "réunion non triviale" signifie qu'aucune de ces k-variétés n'est contenue dans la réunion des autres).

<u>Démonstration</u>.

<u>Première méthode</u> : on peut utiliser une décomposition primaire de $\mathfrak{I}(S)$

$$\mathfrak{I}(S) = Q_1 \cap \ldots \cap Q_r .$$

En appliquant $\mathfrak{V}$ aux deux membres, on obtient $S = S_1 \cup \ldots \cup S_r$, en posant $S_i = \mathfrak{V}(Q_i)$. Or l'idéal $\mathfrak{I}(S_i) = \mathfrak{I}(\mathfrak{V}(Q_i)) = \text{rad } Q_i$ est l'idéal premier P_i de Q_i. Donc S_i est irréductible, i.e. est une k-variété. L'unicité de la décomposition résulte de l'unicité des idéaux premiers P_i.

.../...

Deuxième méthode (n'utilisant pas la décomposition primaire). Soit $\mathcal{E}$ l'ensemble des sous-k-ensembles algébriques non vides S de K^n qui ne sont pas réunions finies de k-variétés. Supposons $\mathcal{E}$ non vide. Comme $k[X]$ est noëthérien, l'ensemble $\mathfrak{J}(\mathcal{E})$ des idéaux de la forme $\mathfrak{J}(S)$, avec $S \in \mathcal{E}$, admet un élément maximal I_o. Il existe $S_o \in \mathcal{E}$, tel que $I_o = \mathfrak{J}(S_o)$. Donc, si on pose $I_1 = \mathfrak{J}(S_1)$, et $I_2 = \mathfrak{J}(S_2)$ on a $I_o = I_1 \cap I_2$ et, de plus, I_o est distinct de I_1 et I_2. Comme on a $S \in \mathcal{E}$, on a aussi S_1 ou $S_2 \in \mathcal{E}$. Or, si, par exemple, on a $S_1 \in \mathcal{E}$, on a $I_1 \in \mathfrak{J}(\mathcal{E})$, ce qui contredit le choix de I_o. Donc $\mathcal{E}$ est vide, i.e. tout S est réunion finie de k-variétés. On peut, d'autre part, prouver la propriété d'unicité, au moyen d'un raisonnement par récurrence, en utilisant le coroll. 4 précédent.

5. k-variétés affines.

Soit $V \subset K^n$ une k-varieté, et posons $P = \mathfrak{J}_k(V)$. L'idéal P est premier (th. 1). On fait toujours la convention d'écriture $k[X] = k[X_1, \dots, X_n]$.

On appelle anneau de coordonnées de V, et on note $\mathcal{A}_k(V)$ l'anneau $\mathcal{A}_k(V) = k[X]/P$. On appelle corps des fractions sur V, et on note $\mathcal{F}_k(V)$, le corps des fractions de $\mathcal{A}_k(V)$. Le degré de transcendance de $\mathcal{F}_k(V)$ sur k est appelé dimension de V.

L'homomorphisme canonique $k[X] \to \mathcal{A}_k(V)$, de noyau $P = \mathfrak{J}_k(V)$, est noté α_V. Les images $u_i = \alpha_V(X_i)$ $(1 \leqslant i \leqslant n)$ sont appelées les fonctions coordonnées sur V. Elles engendrent $\mathcal{A}_k(V)$, i.e. on a $\mathcal{A}_k(V) = k[u_1, \dots, u_n]$. On a donc aussi $\mathcal{F}_k(V) = k(u_1, \dots, u_n)$.

Soient $x \in V$, et soit $f \in \mathcal{A}_k(V)$, image d'un élément $F \in k[X]$. L'élément $F(x)$ de K ne dépend que de f et de x, mais non de F. On le désigne aussi par $f(x)$. Si $\mathfrak{f}$ est une famille d'éléments de

.../...

$\mathcal{O}_k(V)$, et si $f(x) = 0$ pour tout $f \in F$, on dit que x est un zéro de Φ.

Soient V et W deux k-variétés, telles que $W \subset V$. On a $\mathfrak{I}_k(W) \supset \mathfrak{I}_k(V)$, et on peut donc compléter le diagramme

$$\begin{tikzcd} k[X] \arrow[r, "\alpha_V"] \arrow[dr, "\alpha_W"'] & \mathcal{O}_k(V) \arrow[d, dashed, "\beta"] \\ & \mathcal{O}_k(W) \end{tikzcd}$$

par un homomorphisme surjectif $\beta = \beta_{W/V} : \mathcal{O}_k(V) \to \mathcal{O}_k(W)$. Le noyau $\underline{p}$ de β est un idéal premier de $\mathcal{O}_k(V)$. On a $\mathfrak{I}_k(W) = \ker \alpha_W = \ker(\beta \circ \alpha_V) = \alpha_V^{-1}(\underline{p})$. On a donc $W = \mathfrak{V}_k(\alpha^{-1}(\underline{p}))$, de sorte que W est déterminée par $\underline{p}$. Il y a donc une correspondance bijective naturelle entre les idéaux premiers $\underline{p}$ de $\mathcal{O}_k(V)$ et les sous-k-variétés W de V. On peut encore caractériser W comme l'ensemble des zéros de $\underline{p}$, et $\underline{p}$ comme l'idéal composé des éléments de $\mathcal{O}_k(V)$ s'annulant sur W.

Pour que $\underline{p}$ soit un idéal maximal de $\mathcal{O}_k(V)$, il faut et il suffit que $\mathcal{O}_k(W)$ soit un corps, i.e. que les fonctions coordonnées sur W soient algébriques sur k, ou encore que $\dim W = 0$.

On appelle <u>anneau local de W sur V</u>, l'anneau local $(\mathcal{O}_k(V))_{\underline{p}}$ (Chap. 0, A, n°1), qu'on désignera aussi par la notation $\underline{o}_k(W,V)$. Par définition de l'anneau local d'un idéal, cet anneau est composé des éléments de $\mathcal{F}_k(V)$ qui sont de la forme $\frac{f}{g}$, avec f et $g \in \mathcal{O}_k(V)$, et $g \notin \underline{p}$. Comme on a $\mathcal{O}_k(W) \simeq \mathcal{O}_k(V)/\underline{p}$, le corps résiduel de l'anneau local $\underline{o}_k(W,V)$ est $\mathcal{F}_k(W)$. L'homomorphisme canonique

$$\underline{o}_k(W,V) \xrightarrow{\gamma} \mathcal{F}_k(W)$$

est obtenu par prolongement canonique de $\beta : \mathcal{O}_k(V) \to \mathcal{O}_k(W)$. Son noyau est l'idéal maximal de $\underline{o}_k(W,V)$, qu'on note $\underline{m}_k(W,V)$.

Dans le cas où W est un point de x rationnel sur k (c'est-à-dire à coordonnées dans k), on a $\mathcal{O}_k(x) \simeq k$, et $\mathcal{F}_k(x) \simeq k$.

.../...

L'homomorphisme $\beta = \beta_{x/V}$ fait alors correspondre à tout élément $f \in \mathfrak{A}_k(V)$ sa valeur $f(x)$ en x. L'anneau local $\underline{o}_k(x,V)$ est donc l'ensemble des fonctions sur V de la forme $h = \frac{f}{g}$, avec f, $g \in \mathfrak{A}_k(V)$, et $g(x) \neq 0$. Ces fonctions sont dites <u>morphiques</u> (ou régulières) en x. Si h est morphique en x, l'élément $\gamma(h) = \frac{\beta(f)}{\beta(g)} = \frac{f(x)}{g(x)}$ est appelé <u>valeur de h</u> en x, et noté $h(x)$. L'idéal maximal $\underline{m}(x,V)$ est l'ensemble des fonctions h qui s'annulent en x.

Revenons au cas où W est quelconque. On dit alors que les éléments de $\underline{o}_k(W,V)$ sont les fonctions sur V <u>morphiques sur W</u>. Pour $f \in \underline{o}_k(W,V)$, la fonction $\gamma(f) = g$ est appelée <u>fonction induite</u> par f sur W. L'idéal $\underline{m}_k(W,V)$ est composé des fonctions f sur V qui induisent 0 sur W.

Si $Z \subset W \subset V$, on voit facilement qu'on a des homomorphismes canoniques

$$\underline{o}_k(Z,V) \to \underline{o}_k(W,V) \qquad \text{(injectif)}$$

$$\underline{o}_k(Z,V) \to \underline{o}_k(Z,W) \qquad \text{(surjectif).}$$

6. <u>Points génériques et spécialisations</u>.

Soit $x \in K^n$, quelconque. On a un homomorphisme canonique

$$\alpha : k[X] \to k[x]$$

tel que $\alpha(X_i) = x_i$ pour tout i. Le noyau $P = \mathfrak{I}_k(x)$ de α est premier (puisque $k[x]$ est intègre). Posons $W = \mathfrak{V}(P) = \mathfrak{V}(\mathfrak{I}_k(x))$. On a $x \in W$, et <u>W est l'ensemble des zéros des polynômes à coefficients dans k qui s'annulent en x</u>.

On dit que W est le <u>lieu</u> de x sur k, ce qu'on écrit $W = \mathrm{loc}_k\, x$, ou encore que x est un <u>point générique</u> de W sur k. On a toujours $\mathfrak{A}_k(W) \simeq k[x]$, d'où $\mathfrak{F}_k(W) \simeq k(x)$.

<u>THEOREME 4</u>.

Soient x et y des points $\in K^n$. Les propriétés suivantes sont équivalentes.

.../...

(a) - $\mathfrak{J}_k(x) \subset \mathfrak{J}_k(y)$ (i.e. tout polynôme $\in k[X]$ qui s'annule en x s'annule aussi en y)

(b)- $y \in \mathrm{loc}_k\, x$

(c) - $\mathrm{loc}_k\, y \subset \mathrm{loc}_k(x)$

(d) - Il existe un k-homomorphisme $\psi : k[x] \to k[y]$ tel que $\psi(x_i) = y_i$ pour tout i .

<u>Démonstration.</u>

(a) $\Leftrightarrow$ (b) $\Leftrightarrow$ (c), comme on le voit en appliquant les propriétés des symboles $\mathfrak{J}$ et $\mathfrak{V}$.

(a) $\Leftrightarrow$ (d), car, pour qu'on puisse compléter le diagramme ci-dessous

$$\begin{tikzcd} k[X] \arrow[rr, "\alpha"] \arrow[dr, "\beta"'] & & k[x] \arrow[dl, dashed] \\ & k[y] & \end{tikzcd}$$

par un homomorphisme $k[x] \to k[y]$, il faut et il suffit qu'on ait $\ker \beta \subset \ker \alpha$, c'est à dire $\mathfrak{J}_k(x) \subset \mathfrak{J}_k(y)$.

Lorsque l'une quelconque de ces conditions est satisfaite, on dit que y est une <u>spécialisation</u> de x sur k , ou que x est une <u>généralisation</u> de y sur k .

Dans le cadre précédent, une variéte donnée n'admet pas nécessairement de point générique. Pour cette raison, nous allons adopter de nouvelles conventions.

7. <u>Domaine universel</u>.

Soit Ω une extension d'un corps k . On dit que Ω est un <u>domaine universel</u> pour k si

a) - Ω est algébriquement clos

b) - Ω est de degré de transcendance infini sur k .

Dans ces conditions, si k' est une extension de type fini quelconque de k , k' est k-isomorphe à un sous-corps de Ω .

.../...

En effet, soit $(u_1,\ldots, u_r)$ une base de transcendance de k' sur k ; on peut, d'autre part, trouver r éléments $v_1,\ldots, v_r$ de Ω algébriquement indépendants ; il existe un k-isomorphisme σ de $k(u_1,\ldots,u_r)$ sur $k(v_1,\ldots, v_r)$ tel que $\sigma(u_i) = v_i$, et on peut prolonger σ un k-isomorphisme de k' sur un sous-corps de Ω .

On se donne une fois pour toutes, dans la suite, un domaine universel Ω sur le corps premier. On prendra toujours $K = \Omega$ (i.e. les points de toutes les variétés considérées ont leurs coordonnées dans Ω); le corps k sera variable, mais toujours de degré de transcendance fini sur le corps premier. Ainsi, le degré de transcendance de Ω sur k est infini, de sorte que Ω est encore un domaine universel pour k .

Dans ces conditions, toute k-variété V admet un point générique. En effet, le corps $\mathcal{F}_k(V) = k(u_1,\ldots, u_n)$ est de type fini sur k (u_i = fonctions coordonnées). Il existe donc un k-isomorphisme ψ de $\mathcal{F}_k(V)$ sur un sous-corps de Ω . Si, pour tout i , on pose $\psi(u_i) = x_i$, on a $k[x_1,\ldots, x_n] \simeq \mathcal{A}_k(V)$, et x est un point générique de V sur k .

On dit que y est spécialisation générique de x sur k si y est spécialisation de x , et si x est spécialisation de y sur k . Il revient au même de dire qu'on a $I_k(x) = I_k(y)$, ou encore $\mathrm{loc}_k\, x = \mathrm{loc}_k\, y$, ou encore qu'il existe un k-isomorphisme $\sigma : k(x) \to k(y)$ tel que $\sigma(x_i) = y_i$ pour tout i . Il est clair que c'est là une relation d'équivalence sur l'ensemble Ω^n .

8. k-topologie de Zariski.

Soit V une k-variété affine. Une intersection quelconque, ou une réunion finie de sous-k-ensembles algébriques de V est encore un sous-k-ensemble algébrique de V . Ces ensembles sont donc les fermés

.../...

d'une topologie sur V ; les cuverts sont donc les complémentaires des sous-k-ensembles algébriques de V. Cette topologie est appelée k-topologie, ou k-topologie de Zariski sur V. Les ouverts (resp. les fermés) sont également appelés k-ouverts (resp. k-fermés). Cette topologie n'est pas séparée. Plus précisément, l'intersection de deux k-ouverts non vides n'est jamais vide. (car un point générique quelconque de V sur k appartient à tout k-ouvert de V). Si $x \in V$, l'adhérence (ou k-adhérence) de x coïncide avec le lieu $\mathrm{loc}_k\, x$.

9. Changement de corps de base. Variétés affines.

Lorsqu'on parlera d'un extension k' d'un corps $k \subset \Omega$, il sera entendu qu'il s'agit d'une extension de type fini de k contenue dans Ω (de sorte que Ω est encore un domaine universel pour k'.

Soit S un k-ensemble algébrique, et soit k' une extension de k. Alors S est aussi un k'-ensemble algébrique, et si on pose $I = \mathfrak{J}_k(S)$, et $I' = \mathfrak{J}_{k'}(S)$, on a $I' = I\, k'[X]$. Cependant, si $S=V$ est k-irréductible, i.e. est une k-variété, ce n'est pas nécessairement une k'-variété. Prenons par exemple $k = \mathbb{Q}$, et $k' = \mathbb{Q}(\sqrt{2})$. L'ensemble algébrique V défini par l'idéal principal $(X^2 - 2)$ est irréductible sur k, mais ne l'est pas sur k'.

THEOREME 5

Soit V une k-variété affine et posons $\mathfrak{J}_k(V) = P$; les deux propriétés suivantes sont équivalentes :

a) pour toute extension k' de k l'idéal $P\, k'[X]$ engendré par P est premier.

b) $\mathcal{F}_k(V)$ est extension régulière de k.

Chacune de ces deux conditions entraîne la suivante :

c) pour toute extension k' de k, V est k'-irréductible.

.../...

Démonstration

(b) $\Longrightarrow$ (a). La variété V admet un point générique x sur k. Montrons qu'on peut choisir x de façon que les extensions k' et $k(x)$ de k soient linéairement disjointes. En effet, soit $t_1,\ldots, t_s$ une base de transcendance de k' sur k. Soient $u_1,\ldots, u_n$ les fonctions coordonnées sur V, et soit $(z_1,\ldots, z_r)$ une base de transcendance de $\mathfrak{F}_k(V)$ sur k. Choisissons des éléments $v_1,\ldots, v_r$ de Ω, tels que $t_1,\ldots, t_s$, $v_1,\ldots, v_r$ forment une famille libre sur k. Il existe un k-isomorphisme σ de $\mathfrak{F}_k(V)$ sur un sous-corps de Ω, tel que $\sigma(z_j) = v_j$, pour $1 \leq j \leq r$. On peut alors prendre pour x le point ayant pour coordonnées les $x_i = \sigma(u_i)$. En effet, d'après le choix des v_j, les extensions k' et $k(x)$ de k sont algébriquement disjointes. Comme $k(x)$ est extension régulière de k, elles sont linéairement disjointes.

Posons $P' = \mathfrak{J}_{k'}(x) = \{f \mid f \in k'[X];\ f(x) = 0\}$. Cet idéal est premier, et il nous suffit de prouver qu'on a $Pk'[X] = P'$. En effet, il est clair que $Pk'[X] \subset P'$. Inversement, soit $f \in P'$; soit (u_j) une base (comme espace vectoriel) de l'extension k' de k ; on a une relation de la forme $f = \sum_j f_j u_j$ où les f_j sont des polynômes appartenant à l'anneau $k[X]$. On a donc $f(x) = \sum_j f_j(x)\, u_j = 0$. La disjonction linéaire de k' et $k(x)$ sur k entraine $f_j(x) = 0$ pour tout j, d'où $f_j \in P$, d'ou $f \in P\, k'[X]$.

(a) $\Longrightarrow$ (b). D'après (a), l'idéal $P' = P\, \overline{k}[X]$ engendré par P dans $\overline{k}[X]$ est premier. Donc, on a $\mathfrak{J}_{k'}(x) = \mathfrak{J}_{k'}(V) = \mathrm{rad}\, P' = P'$.

Soit x générique de V sur $\overline{k}$. Alors x est aussi générique de V sur k. Soit $\{u_j\}$ une base de $\overline{k}/k$. Supposons qu'on ait une relation de la forme $\sum_j u_j f_j(x) = 0$, avec $f_j\ k[X]$. Alors on a $\sum_j u_j f_j \in P'$, d'où, puisque $P' = P\, \overline{k}[X]$, $\sum_j u_j f_j = \sum_j u_j g_,$,

.../...

où les g_j appartiennent à P. On a donc $\sum_j u_j (f_j - g_j) = 0$.

Or $k(X)$ est extension régulière de k ; i.e. $\overline{k}$ et $k(X)$ sont linéairement indépendants. On a donc $f_j = g_j$, d'où $f_j(x) = 0$ pour tout j. On a donc bien montré la disjonction linéaire de $\overline{k}$ et $k(x)$ sur k, i.e. la régularité de l'extension $k(x)/k$.

Remarque 1. Comme k' est algébriquement disjoint de $k(x)$ sur k, on a deg. tr. $k'(x)/k'$ = deg. tr. $k(x)/k$. Donc la dimension de V n'est pas modifiée lorsqu'on remplace k par k'.

Remarque 2. La condition (c) de l'énoncé n'entraîne pas nécessairement (a). En effet, prenons pour k un corps non parfait de caractéristique $p \neq 0$, pour k' une extension purement inséparable de k, de la forme $k' = k(\alpha)$, avec $\alpha^p = a \in k$, et $\alpha \notin k$. La k-variété V définie par l'idéal premier $P = (X^p - a)$ de $k[X]$ est réduite à un point donc est irréductible sur k', et cependant l'idéal $Pk'[X]$, égal à la puissance p-ième de $(X-\alpha)$, n'est pas premier.

Soit V une k-variété affine. Supposons que son idéal reste premier par extension de k ou encore (théorème précédent), que $\mathfrak{F}_k(V)$ est une extension régulière de k. Cette propriété ne dépend pas alors de k. Lorsqu'elle est satisfaite, nous dirons que V est une variété affine, et que k est un corps de définition de V, ou que V est définie sur k. (N.B. On peut montrer que toute variété possède un plus petit corps de définition.) Si k est algébriquement clos, les notions de k-variété affine et de variété définie sur k, coïncident ; on a vu qu'il n'en est pas de même, en général, pour k quelconque.

THEOREME 5 bis.

Soient V une variété définie sur k, x un point de V, k' une extension de k. Pour que x soit générique de V sur k', il faut et il suffit qu'il soit générique de V sur k, et que k' soit linéairement disjoint de $k(x)$ sur k.

Démonstration. Notons d et d' les degrés de transcendance respectifs de $k(x)/k$ et de $k'(x)/k'$. On a toujours $d \geq d'$.

Supposons x générique de V sur k'. On a alors $d' = \dim V$, donc $d \geq \dim V$, donc nécessairement $d = \dim V$ et x est générique de V sur k. De plus, la relation $d = d'$ entraîne que k' et $k(x)$ sont algébriquement disjoints sur k. Ils sont donc linéairement disjoints sur k, compte tenu de chap. 0, C, 7, th. 20.

Réciproquement, supposons x générique de V sur k et k' linéairement disjoint de $k(x)$ sur k. Alors k' est algébriquement disjoint de $k(x)$ sur k, et on a $d = d' = \dim V$. La clôture algébrique $\bar{k}'$ est aussi algébriquement disjointe et, par suite, linéairement disjointe de $k(x)$ sur k. Donc (chap. 0, C, 4, th. 12), $\bar{k}'$ et $k'(x)$ sont linéairement disjoints sur k', i.e. l'extension $k'(x)/k'$ est régulière. Donc x est générique de V sur k'.

Tout sous-ensemble de $\Omega^n = \mathbb{S}_n$ (espace affine de dimension n) qui est un k-ensemble pour un $k \subset \Omega$ convenable est appelé un ensemble algébrique affine. Tout ensemble algébrique affine est une réunion finie de variétés affines. En effet, si S est un k-ensemble, c'est aussi un $\bar{k}$-ensemble ($\bar{k}$ = clôture algébrique de k), et les composantes de ce $\bar{k}$-ensemble sont des $\bar{k}$-variétés, donc des variétés, définies sur $\bar{k}$.

Si $V \subset \mathfrak{S}_n$ est une variété affine, on pose $\mathcal{J}(V) = \mathcal{J}_\Omega(V)$. L'anneau $\mathcal{A}_\Omega(V) = \Omega[X]/\mathcal{J}_\Omega(V)$, ou anneau de coordonnées de V , est encore noté $\mathcal{A}(V)$ (sans indice). De même, son corps des fractions, ou corps des fonctions sur V , est noté $\mathfrak{F}(V)$. Pour tout corps k de définitions de V , l'anneau $\mathcal{A}_k(V)$ s'identifie naturellement à un sous-anneau de $\mathcal{A}(V)$ et, de même $\mathfrak{F}_k(V)$ à un sous-corps de $\mathfrak{F}(V)$. Plus précisément $\mathcal{A}(V)$ (resp. $\mathfrak{F}(V)$) est la réunion des $\mathcal{A}_k(V)$ (resp. des $\mathfrak{F}_k(V)$).

<u>THEOREME 6</u>.

Soit $k' \supset k$. Soient V et W deux variétés définies sur k , telles que $W \subset V$. Alors, on a :

$$\underline{o}_k(W,V) = \underline{o}_{k'}(W,V) \cap \mathfrak{F}_k(V) .$$

Démonstration. Il est clair que le premier membre est inclus dans le second. Réciproquement, soit x générique de V sur k' (donc sur k). Identifions $\mathcal{F}_{k'}(V)$ à $k'(x)$. Soit $z \in \underline{o}_{k'}(W,V) \cap k(x)$.
On a $z = \frac{f(x)}{g(x)}$ $(f, g \in k'[X]$, $g \notin \mathfrak{J}_{k'}(W))$.

Si $\{u_\alpha\}$ est une base de k' sur k , on a $f = \Sigma_\alpha\, u_\alpha f_\alpha$, et $g = \Sigma_\alpha u_\alpha\, g_\alpha$, avec, pour tout α, f_α, $g_\alpha \in k[X]$; d'où

$$\Sigma_\alpha\, u_\alpha\, (g_\alpha(x)z - f_\alpha(x)) = 0 .$$

Or k' et $k(x)$ sont algébriquement disjoints, donc linéairement disjoints sur k . On a donc

$$g_\alpha(x)z - f_\alpha(x) = 0$$

pour tout α. Or il existe α tel que g_α ne s'annule pas sur W, i.e. tel que $g_\alpha \notin \mathfrak{J}_k(W)$. On a donc $z \in \underline{o}_k(W,V)$.

D'après le théorème ci-dessus, pour $f \in \mathcal{F}_k(V)$, la propriété pour f d'être morphique sur W ne dépend pas de k . L'ensemble des $f \in \mathcal{F}(V)$ qui sont morphiques sur W est un anneau local, qu'on note $\underline{o}(W,V)$; cet anneau est la réunion des $\underline{o}_k(W,V)$, pour k variable. Son idéal maximal $\underline{m}(W,V)$, composé des fonctions s'annulant sur W , est, de même, la réunion des $\underline{m}_k(W,V)$.

10. Produits de variétés affines.

THEOREME 7.

Le produit (au sens ensembliste) de deux k-ensembles algébriques affines est un k-ensemble algébrique affine.

En effet, soient $S \subset \mathbb{S}_m$, et $T \subset \mathbb{S}_n$, deux k-ensembles algébriques affines. Posons $I = \mathfrak{J}_k(S)$, et $J = \mathfrak{J}_k(T)$, ce qui implique $S = \mathcal{J}_k(I)$, et $T = \mathcal{J}_k(J)$. Pour qu'un point $z = (x,y)$ de $\mathbb{S}_{m+n} = \mathbb{S}_m \times \mathbb{S}_n$ soit $S \times T$, il faut et il suffit qu'on ait $f(x) = 0$ et $g(y) = 0$ quelles que soient $f \in I$ et $g \in I$. Autrement dit $S \times T$ est l'ensemble des zéros de l'ensemble $I \cup J$ de

.../...

$k[X,Y] = k[X_1,\ldots, X_m, Y_1,\ldots, Y_n]$, où I et J sont regardés comme sous-ensembles de $k[X] = k[X_1,\ldots, X_m]$ et $k[Y] = k[Y_1,\ldots,Y_n]$ respectivement. On a donc $S \times T = \mathcal{V}_k(I \cup J) = \mathcal{V}_k(I\,k[X,Y] + J\,k[X,Y])$, et $\mathfrak{J}_k(S \times T) = \mathrm{rad}\,(I\,k[X,Y] + J\,k[X,Y])$.

Corollaire : le produit de deux ensembles algébriques affines est un ensemble algébrique affine.

Cependant, le produit de deux k-variétés n'est pas toujours une k-variété.

Exemple : si $I = (X^2 - 2)$, et $J = (Y^2 - 2)$, $S \times T$ se compose des 4 points de coordonnées $x = \pm\sqrt{2}$, $y = \pm\sqrt{2}$. Si on a pris $k = \mathbb{Q}$, cet ensemble n'est pas irréductible, car il est l'union des deux Q-ensembles U_1, U_2, à deux composants, respectivement définis par les idéaux $(Y - X, X^2 - 2)$ et $(Y + X, X^2 + 2)$.

Complément : points génériques indépendants : Soient V et W deux k-variétés affines, et soient x,y génériques, l'un de V, l'autre de W, sur k. On dit qu'ils sont génériques indépendants si $k(x)$ et $k(y)$ sont algébriquement indépendants sur k. Dans le cas où V et W sont des variétés définies sur k, les extensions $k(x)$ et $k(y)$ sont régulières, donc linéairement disjointes. De plus, x est générique de V sur $k(y)$ et y de W sur $k(x)$.

THEOREME 8. Soient V et W deux variétés définies sur k. Alors $V \times W$ est une variété définie sur k, et on a

(1) $\mathfrak{J}_k(V \times W) = \mathfrak{J}_k(V)\,k[X,Y] + \mathfrak{J}_k(W)\,k[X,Y]$.

Soit de plus $(x,y) \in V \times W$. Pour que (x,y) soit générique de $V \times W$ sur k, il faut et il suffit que x et y soient génériques indépendants de V et W sur k.

Corollaire. $\dim(V \times W) = \dim V + \dim W$.

Démonstration. Posons $P = \mathfrak{J}_k(V)$, et $Q = \mathfrak{J}_k(W)$.

.../...

Pour $x \in V$ et $y \in W$ génériques indépendants sur k, on a évidemment

$$\mathfrak{I}_k(x \times y) \supset \mathfrak{I}_k(V \times W) \supset P\, k[X,Y] + Q\, k[X,Y].$$

Nous allons montrer qu'on a

$$(2) \quad \mathfrak{I}_k(x \times y) \subset P\, k[X,Y] + Q\, k[X,Y] .$$

Il en résultera que $\mathfrak{I}_k(V \times W)$ est premier, et que $V \times W$ est une variete definie sur k, de point générique $(x,y) = x \times y$; d'autre part, la relation (2) entrainera (1).

Pour démontrer (2), introduisons une base $\{u_i(x)\}$ de $k[x]$ (regarde comme espace vectoriel) sur k, et, de même, une base $\{v_j(y)\}$ de $k[y]$ sur k.

Tout polynôme $g \in k[X]$ (resp $h \in k[Y]$) est congru (mod P) (resp. (mod Q)) à une combinaison de la forme $\Sigma a_i\, u_i$ (resp $\Sigma b_j\, v_j$) où les a_i (resp. b_j) appartiennent à k.

Il en resulte que tout polynôme $f \in k[X,Y]$ est congru (mod $P\, k[X,Y] + Q\, k[X,Y]$), à une combinaison de la forme $\Sigma_{i,j}\, c_{ij}\, u_i\, v_j$, où les c_{ij} appartiennent à k (pour le montrer, ordonner d'abord en Y, décomposer les coefficients (mod P), puis grouper les termes de même indice i, et décomposer leurs coefficients (mod Q)).

Si $f \in \mathfrak{I}_k(x \times y)$, on a $f(x,y) = \Sigma_{i,j}\, c_{ij}\, u_i(x)\, v_j(y) = 0$. Or $k(x)$ et $k(y)$ sont linéairement disjoints sur k. Donc on a $c_{ij} = 0$ quels que soient i et j, ce qui demontre (2).

Il reste à montrer que si (x,y) est générique de $V \times W$ sur k, x et y sont génériques indépendants de V et W sur k. Or, d'après ce qui précède, on a $\dim(V \times W) = \dim V + \dim W$. Soient r, s, t les degrés de transcendance respectifs de $k(x,y)$, $k(x)$ et $k(y)$ sur k. On a $r = \dim(V \times W)$, $s \leq \dim V$, $t \leq \dim W$, et

.../...

$r \leqslant s + t$. On a donc nécessairement $s = \dim V$ et $t = \dim W$, ce qui prouve l'assertion. (cf. plus loin, n° 12, coroll. du th. 13).

11. Applications rationnelles et morphismes.

Soient V et W deux variétés affines $(V \subset S_m, W \subset S_n)$, définies sur k . Soit x un point générique de V sur k . Soit $\Phi = (\Phi_1, \dots, \Phi_n)$ une famille de n fonctions sur V , définies sur k , telles que le point $y = \Phi(x) = (\Phi_1(x), \dots, \Phi_n(x))$ appartienne à W . La famille Φ des Φ_j est appelée une application rationnelle de V dans W définie sur k . Les fonctions Φ_j sont dites coordonnées de Φ . Si $\Phi(x)$ est générique de W sur k , on dit que Φ est génériquement surjective, ou dominante ; dans ce cas, $\mathcal{F}_k(W) \simeq k(y)$ est isomorphe à un sous-corps de $\mathcal{F}_k(V) \simeq k(x)$. Si, de plus, on a $k(x) = k(y)$ (d'où $\mathcal{F}_k(V) \simeq \mathcal{F}_k(W)$), on dit que V est birationnelle. On a alors $x = \psi(y)$, où ψ est une application rationnelle $W \to V$, définie sur k , qu'on note Φ^{-1} .

Soit $a \in V$. Si chacune des Φ_j est morphique en a , on dit que Φ est morphique en a ; le point b de coordonnées des $b_j = \Phi_j(a)$ est alors un point de W , appelé image de a par Φ , et noté $\Phi(a)$. Soit V' une sous-variété de V , définie sur k . On dit que Φ est morphique sur V' si elle est morphique en un point générique (donc en tout point générique) x' de V' sur k . Le lieu W' du point $y' = \Phi(x')$ sur k est alors une sous-variété de W , définie sur k , qu'on note $\Phi_g(V')$, et appelée image ou transformée générique de V' par Φ .

Soit g une fonction sur W , morphique sur $\Phi_g(V)$, i.e. morphique en y . On a $g(y) \in k(x)$, i.e. $g(y) = g(\Phi(x))$ est de la forme $f(x)$, avec $f \in \mathcal{F}_k(V)$. La fonction f est notée $g \circ \Phi$. On dit que c'est la fonction sur V obtenue en relevant g au moyen de Φ . Soit $a \in V$, et supposons Φ morphique en a , de valeur b . Si on a $g \in \underline{o}(b,W)$, on a fortiori $g \in \underline{o}(\Phi_g(V), W)$, i.e. le symbole $f = g \circ \Phi$ est défini, et on a $f \in \underline{o}(a,V)$. L'application $\underline{o}(b,W) \xrightarrow{\Phi^*} \underline{o}(a,V)$ obtenue en prenant $\Phi^*(g) = f$ est un homomorphisme, qui, de plus, est local, i.e. envoie $\underline{m}(b,W)$ dans $\underline{m}(a,V)$; cet homomorphisme est dit local canonique. Plus

.../...

généralement si Φ est morphique sur V' , et si $W' = \Phi_g(V')$, on a un homomorphisme local canonique $\underline{o}(W',W) \to \underline{o}(V',V)$. On a aussi des homomorphismes locaux analogues lorsqu'on remplace le symbole $\underline{o}$ par $\underline{o}_k$.

On peut composer de façon évidente deux applications rationnelles $\Phi : U \to V$ et $\psi : V \to W$ à la condition que Φ soit morphique sur l'image $\Phi_g(V)$; on obtient une application rationnelle $\theta : U \to W$, qu'on note $\psi \circ \Phi$. Si Φ et ψ sont définies sur k , il en est de même de θ .

Si Φ est morphique en $a \in V$, et si ψ est morphique en $b = \Phi(a)$, $\theta = \psi \circ \Phi$ est morphique en a , et on a $\theta(a) = \psi(\Phi(a))$.

On dit qu'une application rationnelle $\Phi : V \to W$ est un <u>morphisme</u> si elle est morphique en tout point de V . Le composé de deux morphismes est encore un morphisme.

Si Φ est un morphisme, l'image ensembliste $\Phi(V)$ est toujours contenue dans l'image générique $\Phi_g(V)$, mais on n'a pas en général $\Phi(V) = \Phi_g(V)$. (Exemple : prendre pour V , l'hyperbole $XY = 1$ dans le plan affine $\mathcal{S}_2$, et pour Φ l'application $V \to \mathcal{S}_1$ induite par la projection sur Ox) . Cependant, tout point générique de $\Phi_g(V)$ sur k appartient à $\Phi(V)$, et, par suite $\Phi_g(V)$ coïncide avec la k-adhérence de $\Phi(V)$. (<u>Remarque</u> : on peut montrer que $\Phi(V)$ est un sous-ensemble <u>constructible</u> de W , i.e. est la réunion d'un nombre fini d'ouverts de sous-variétés de W).

<u>THEOREME 9</u>.

Soient V et W deux variétés définies sur k , et soit $\Phi : V \to W$ une application rationnelle définie sur k . Alors, l'ensemble U des points de V où f est morphique est un k-ouvert non vide de V . Plus précisément, cet ouvert est le complémentaire du fermé $F = \mathcal{J}(I)$ déterminé par l'idéal :

$$I = \{ g \mid g \in k[X] \ , \ \Phi_j(x)\, g(x) \in k[x] \text{ pour tout } j \} \ .$$

<u>Démonstration</u>. En effet, posons $y_j = \Phi_j(x)$.

f morphique en $x \iff \exists\, k[X]$ tel que $y_j\, g(x) \in k[x]$ pour tout j, et que $g(x) \neq 0$.

Donc,

f non morphique en $x \iff \forall g \in k[X]$, tel que $y_j g(x) \in k[x]$ pour tout j, on a $g(x) = 0$.

Autrement dit : f non morphique en $x \iff x \in \mathcal{J}(I)$.

Enfin, U est non vide, car U contient tout point générique de V sur k.

Corollaire 1. Si Φ est un morphisme, on a $\Phi_j \in k[x]$ pour tout j , i.e. les Φ_j sont induites par des polynômes.

En effet, la condition pour ϕ d'être un morphisme équivaut à $\mathcal{Y}(I) = \emptyset$, où encore à $1 \in I$, d'après le théorème des zéros.

Corollaire 2. Tout morphisme est continu pour la topologie de Zariski.

Exemple de morphisme : Si V et W sont deux variétés définies sur k , les applications rationnelles définies par les projections $V \times W \to V$, et $V \times W \to W$ (notées pr_1 et pr_2) sont des morphismes.

Graphe d'une application rationnelle ou d'un morphisme.

Soit $\phi : V \to W$ une application rationnelle, définie sur k . On appelle graphe de ϕ la sous-variété Γ_ϕ de $V \times W$ lieu du point $(x, \phi(x))$ sur k . Si ϕ est définie en a , de valeur b , le couple (a,b) est un point du graphe Γ_ϕ .

12. Hypersurfaces.

a) THEOREME 13.

Soient $x, y \in \Omega^n$; supposons que y est spécialisation de x sur k . Alors

$$\deg.\, tr(k(x)|k) = \deg tr(k(y)|k) \iff k(x) = k(y).$$

Dem. En effet, il existe, par hypothèse, un k-homomorphisme $\psi : k[x] \to k[y]$. Supposons $\deg.\, tr(k(x)|k) = \deg tr(k(y)|k) = r$, et soit $v_1, \ldots, v_r$ une base de transcendance de $k(y)$, contenue dans $k|y|$. Soient $u_1, \ldots, u_r$ des éléments de $k[x]$ tels que $v_i = \psi(u_i)$ pour tout i . Les u_i sont nécessairement algébriquement independants sur k . Donc ψ induit un isomorphisme $k[u_1, \ldots, u_n] \to k[v_1, \ldots, v_n]$ et toute place de $k(x)$, à valeur dans $k(y)$ prolongeant ψ est un isomorphisme.

Corollaire. Soit W une sous-variété d'une variété V . Pour que $W = V$, il faut et il suffit que $\dim W = \dim V$.

.../...

b) THEOREME 14.

Soit V une variété affine ($V \subset \mathcal{E}_n$) définie sur k. Pour qu'on ait $\dim V = n-1$, il faut et il suffit que $\mathfrak{J}_k(V)$ soit principal.

On dit alors que V est une hypersurface de $\mathcal{S}_n$.

Démonstration. Supposons $\dim V = n-1$.

Soit $f \in \mathfrak{J}(V)$, et considérons l'ensemble $H = \mathcal{J}(f)$ des zéros de f. Soit $f = \prod_i f_i$, où les f_i sont irréductibles, et, pour tout i, posons $H_i = \mathcal{J}(f_i)$. On a $V \subset H$, et $H = \bigcup_i H_i$, d'où $V = \bigcup_i V_i$, en posant $V_i = V \cap H_i$. Comme V est irréductible, il existe un i tel que $V = V_i$, d'où $V \subset H_i$. Comme $\dim H_i \leq n-1$, ceci implique $\dim V = \dim H_i$, et, par suite, $V = H_i$.

Reciproquement, soit $\mathfrak{J}_k(V) = (f)$, avec $f \in k[X] = k[X_1, \dots, X_n]$ non constant. Supposons que l'indéterminée X_n intervient dans f. Soient $x_1, \dots, x_{n-1}$ des éléments de Ω algébriquement indépendants sur k. On peut trouver dans Ω une solution x_n de l'équation $f(x_1, \dots, x_{n-1}, x_n) = 0$. Le point $x = (x_1, \dots, x_n)$ ainsi construit appartient à V, et le degre de transcendance de $k(x)|k$ est $n-1$. On a donc $\dim V \geq n-1$. Or on a $V \neq \mathcal{S}_n$, donc $\dim V \leq n-1$. Donc $\dim V = n-1$.

CHAPITRE II

Variétés (ou variétés abstraites)

1. Définition.

Soient V un ensemble, $\{U_\alpha\}_{\alpha \in A}$ un recouvrement fini de V, $\{\psi_\alpha\}_{\alpha \in A}$ une famille de bijections $U_\alpha \to V_\alpha$, où, pour tout α, V_α est une variété affine, $\{t_{\beta\alpha}\}_{\beta,\alpha \in A \times A}$ une famille d'applications birationnelles, $t_{\beta\alpha} : V_\alpha \to V_\beta$, ces données étant astreintes à vérifier les conditions :

a) $\forall\, (\alpha,\beta) \in A\times A$, $\psi_\alpha(U_\alpha \cap U_\beta)$ est un ouvert dans V_α et si $x \in U_\alpha \cap U_\beta$, $x_\alpha = \psi_\alpha(x)$, $x_\beta = \psi_\beta(x)$, alors $t_{\beta\alpha}$ est bimorphique en x_α de valeur x_β.

b) L'ensemble $E_{\beta\alpha}$ des couples $(x_\alpha, x_\beta) \in V_\alpha \times V_\beta$ de la forme $(\psi_\alpha(x), \psi_\beta(x))$ est fermé dans $V_\alpha \times V_\beta$, autrement dit il coïncide avec $\Gamma_{\beta\alpha}$, le graphe $t_{\beta\alpha}$.

On dit que V est une variété. (V ne vérifiant que (a) est dite une prévariété).

Une forme équivalente au couple (a) et (b) est :

(c) $t_{\beta\alpha}$ est bimorphique en tout couple $(x_\alpha, x_\beta) \in \Gamma_{\beta\alpha}$ et $E_{\beta\alpha} = \Gamma_{\beta\alpha}$.

Le fait que (a) et (b) entraînent (c) est évident ; dans l'autre sens, on voit que $\Phi_\alpha(U_\alpha \cap U_\beta)$ est domaine de définition de $t_{\beta\alpha}$, qui est morphique, donc est ouvert de V_α.

Exemple. Considérons l'ensemble $\mathbb{S}^*_{n+1}$ complémentaire de l'origine dans l'espace affine $\mathbb{S}_{n+1}$. L'espace projectif $\mathbb{P}_n$ est défini comme le quotient de $\mathbb{S}_{n+1}$ par la relation définie par la proportionalité des coordonnées. Si $(x_0, x_1, \dots, x_n) \in \mathbb{S}^*_{n+1}$ représente $x \in \mathbb{P}_n$, on dit que les x_i forment un système de coordonnées homogènes de x. On prend pour U_α $(0 \leq \alpha \leq n)$ l'ensemble des $x \in \mathbb{P}_n$ tels que $x_\alpha \neq 0$, pour V_α l'espace $\mathbb{S}_n$, et pour ψ_α l'application bijective $U_\alpha \to \mathbb{S}_n$ qui, à x, fait correspondre le point ayant pour coordonnées les $\frac{x_\lambda}{x_\alpha}$, avec $\lambda \neq \alpha$ (rangées, par exemple, dans l'ordre des λ croissants). Comme on le vérifie immédiatement, ces données définissent sur $\mathbb{P}_n$ une structure de variété abstraite.

2. Autres définitions et remarques.

Dans les n° 2,3 4 ci-dessous, on se borne à indiquer les principales définitions généralisant pour les variétés abstraites celles déjà données dans le cas affine, laissant au lecteur le soin de reformuler les propriétés correspondantes.

K est dit corps de définition de V s'il est corps de définition de V_α et de $t_{\beta\alpha}$ quels que soient α et $\beta \in A$.

Un élément de V est appelé point.

$x \in V$, on parlera de $k(x) = k(x_\alpha)$ en effet $t_{\beta\alpha}$ étant un morphisme, $k(x_\alpha)$ ne dépend pas de $\alpha \in A$.

Un <u>sous-k-ensemble algébrique de V</u> : est un sous ensemble de V tel que, $\forall \alpha \in A$, $\psi_\alpha(S \cap U_\alpha)$ soit un sous-k-ensemble algébrique de V_α.

On étend aux variétés abstraites la <u>k-topologie</u> de <u>Zariski</u>, dont les fermés sont les sous-k-ensembles algébriques de V.

Une sous-k-variété de V est un sous-k-ensemble algébrique qui n'est pas réunion non triviale de sous-k-ensembles plus petits.

Soit V définie sur k, et soit $x \in V$. Pour $x \in U_\alpha$, représenté par x_α dans V_α, notons W_α la sous-variété de V_α lieu de x_α sur k. Le sous-ensemble W de V composé des spécialisations de x sur k coïncide avec l'ensemble des points de V qui sont représentés dans l'une des V_α par un point de W_α. On dit que W est la <u>sous-k-variété</u> de V <u>lieu de x</u> sur k, ce qu'on écrit $W = \mathrm{loc}_k\, y$. On dit aussi que y est un <u>point générique</u> de W sur k.

Dans le cas où $\mathcal{F}_k(x)$ est extension régulière de k, les W_α sont des variétés définies sur k. Posons alors $U'_\alpha = \psi_\alpha^{-1}(W_\alpha)$, et soit $\psi'_\alpha : U'_\alpha \to W_\alpha$ induite par ψ_α. Les U'_α forment un recouvrement de W, et la famille des $(U'_\alpha, \psi'_\alpha)$ définit sur W une structure de variété, définie sur k. On dit alors que W est une <u>sous-variété</u> de V, définie sur k.

Toute variété V admet un point générique sur k. Il suffit en effet, de prendre pour x le point représenté par un point générique x_α de l'une des V_α. Le point x est alors représenté dans V_β quel que soit β (i.e. on a $x \in \bigcap_\beta U_\beta$) : en effet, $t_{\beta\alpha}$ est bimorphique en x_α, et x est représenté dans V_β par $x_\beta = t_{\beta\alpha}(x_\alpha)$, qui est générique de V_β sur k.

.../...

Considérons $\mathcal{F}_k(V_\alpha)$ le corps des fonctions de V_α. Si x_α est un point générique de V_α, $\mathcal{F}_k(V_\alpha)$ est isomorphe à $k(x_\alpha)$, qui est lui-même isomorphe à $k(x_\beta)$, $\forall \beta \in A$.

On peut donc définir le corps des fonctions de V sur k :

$$\mathcal{F}_k(V) \simeq k(x) .$$

Soit $x \in U_\alpha$, représenté par x_α dans V_α. Supposons f_α morphique en x_α. Alors, pour tout β tel que $x \in U_\beta$, f_β est morphique en x_β. On dit que f est <u>morphique en x</u>. L'élément $f_\alpha(x_\alpha)$ de $k(x)$ ne dépend pas de α ; il ne dépend pas non plus de k.
On le désigne par $f(x)$, et on l'appelle <u>valeur de f en x</u>.
L'ensemble des $f \in \mathcal{F}_k(V)$ (resp $\mathcal{F}(V)$) qui sont morphiques en x est un anneau local, appelé <u>anneau local de V en x</u>, et noté $\underline{o}_k(x,V)$ (resp $\underline{o}(x,V)$. On définit de même la notion de fonction morphique sur une sous-variété W, et l'anneau local $\underline{o}_k(W,V)$ (resp $\underline{o}(W,V)$).

3. <u>Application rationnelle</u>.

V et V' étant deux variétés abstraites, on définit une application rationnelle $\phi : V \to V'$ par la donnée pour tout couple (α,α') d'une application rationnelle $\phi_{\alpha\alpha'} : V_\alpha \to V'_{\alpha'}$, avec la condition suivante : si x est un point générique de V sur k représenté pour tout α, par x_α dans V_α, les points $x'_{\alpha'} = \phi_{\alpha'\alpha}(x_\alpha)$ représentent un même point x' de V'.

- Une application $\phi : V \to V'$ rationnelle est dite <u>morphique</u> en $y \in V$ si $\exists\, \alpha$ et α' tels que $y \in U_\alpha$ et $\phi_{\alpha\alpha'}$ soit morphique en y_α ; dans ce cas $\forall \beta$ et β' vérifiant la même condition, $\phi_{\beta'\beta}$ est morphique en y_β. De plus le point y' de V' représenté par $y'_\beta = \phi_{\beta'\beta}(y_\beta)$ ne dépend pas de β et β'. On le note $y' = \phi(y)$.

4. <u>Produit de deux variétés abstraites</u>.

Soient V et V' deux variétés abstraites, et $\{U_\alpha\}_{\alpha' \in A}$,

.../...

$\{U'_{\alpha'}\}_{\alpha'\in A'}$ leurs recouvrements.

On définit le produit $V \times V'$ comme le produit ensembliste ayant pour recouvrement $\{U_\alpha \times U_{\alpha'}\}_{(\alpha;\alpha')\in A\times A'}$;

les bijections étant $\psi_\alpha \times \psi_{\alpha'} : x, x' \to (\psi_\alpha(x), \psi'_{\alpha'}(x'))$.

On définit ainsi sur $V \times V'$ une structure de variété.

5. Notion d'ouvert affine.

Définition.

On appelle immersion de V dans V' un morphisme birationnel qui est bimorphique en tout point de V , et donc injectif.

- ϕ étant une immersion, $\phi(V)$ est un ouvert de V' car $\phi(V)$ est l'ensemble des points où le morphisme ϕ^{-1} est défini lorsque V est une variété affine, $\phi(V)$ est appelé ouvert affine.

THEOREME.

Tout ouvert de V contient un ouvert affine.

On va en fait prouver que pour $x \in U$ ouvert de V , il existe un ouvert affine contenant x et contenu dans U .

Preuve :

(On va résoudre le problème pour une variété affine, les ouverts "abstraits" se définissant par recollement d'ouverts affines, le problème sera résolu dans tous les cas) on rappelle que $S_n = \Omega^n$.

Soit $V \subset S_n$; soient $u_1, \dots, u_n$ les fonctions coordonnées sur V ; soit f une fonction sur V qui s'annule sur le complémentaire de U et qui n'est pas nulle en x .

Considérons l'application birationnelle ayant pour fonctions coordonnées, $u_1, \dots, u_n$, $\frac{1}{f} = \psi$; si $V = \mathrm{loc}_k\, x$, on a $V' = \mathrm{loc}_k\, y$ où $y = \psi(x)$. De plus, ϕ^{-1} est un morphisme car ϕ^{-1} est induit par une projection.

Alors si U' est l'ensemble des points où ϕ est morphique,

.../...

U' est bien un ouvert affine (chap. I, th. 9) contenant x et contenu dans U.

Remarque 1. Du fait que la topologie de Zariski est quasi-compacte (d'après le théorème de la base finie de Hilbert), on déduit que tout ouvert peut être recouvert par un nombre fini d'ouverts affines.

Remarque 2. On déduit de la remarque 1 que tout ouvert U de V peut être muni d'une structure de variété, et ceci canoniquement, la structure étant déterminée à un isomorphisme près par la condition que l'injection $U \to V$ soit une immersion.

Remarque 3. Les notations étant celles de la définition du n° 1, la variété abstraite V est uniquement déterminée, à un isomorphisme près, par la connaissance des V_α et des $t_{\beta\alpha}$.

Réciproquement, à toute famille $\{V_\alpha, t_{\beta\alpha}\}$ composée d'un nombre fini de variétés V_α et de transformations birationnelles $t_{\beta\alpha}$ vérifiant la condition (c) du n° 1, on peut faire correspondre une variété abstraite : considérons en effet l'ensemble des couples (α, x_α) tels que $x_\alpha \in V_\alpha$ pour tout α, et, dans cet ensemble, la relation définie par $(x_\alpha, x_\beta) \in \Gamma_{\beta\alpha}$; c'est là une relation d'équivalence; si V est l'ensemble quotient correspondant, on a des injections évidentes $V_\alpha \to V$ dont les images U_α recouvrent V ; ceci permet de reconstituer la situation du n° 1 et de munir V d'une structure de variété abstraite. On dira que V est la variété abstraite canoniquement associée à la famille $\{V_\alpha, T_{\beta\alpha}\}$.

6. Variétés complètes.

Définition 1. (place finie en un point d'une variété).

Soit V une variété définie sur k. Soit x un point de V et soit ρ une place de $k(x)$, induisant l'identité sur k, à valeurs dans Ω. S'il existe un α tel que $\rho(x_\alpha)$ soit fini, le point y de V représenté par $y_\alpha = \rho(x_\alpha)$ dans V_α ne dépend pas de α ; ce point est spécialisation de x sur k. On dit que ρ est finie en x, de valeur y, et on écrit $y = \rho(x)$.

Inversement, si x et $y \in V$, et si y est une spécialisation de x sur k, il existe une place ρ de $k(x)$, à valeurs dans $k(y)$, telle que $y = \rho(x)$ (on le voit en appliquant le théorème de prolongement à l'un quelconque des k-homomorphismes $k[x_\alpha] \to k[y_\alpha]$.

Définition 2.

On dit qu'une variété V est complète si pour tout point x de V et pour toute place ρ de $k(x)$, ρ est finie en x. Il suffit d'ailleurs que, pour x générique de V sur k, toute place ρ de Ω soit finie en x.

On démontre facilement que :

- Toute sous-variété d'une variété complète est complète,
- Tout produit de variétés complètes est une variété complète,
- L'espace projectif $\mathbb{P}_n$ est une variété complète.

CHAPITRE III

Points simples

1. Différentielles.

THEOREME 1

Soit K une extension d'un corps k. Il existe un K-espace vectoriel D, et une application $d = d_{K/k}$, s'annulant sur k, telle que $\operatorname{Im} d$ engendre D, vérifiant les conditions

(a) $d(f + g) = df + dg$

(b) $d(f\, g) = f\, dg + g\, df$,

et telle que, pour tout autre couple (D',d') vérifiant les mêmes conditions, il existe un K-homomorphisme $\phi : D \to D'$ rendant commutatif le diagramme

$$\begin{tikzcd} K \arrow[rr, "d"] \arrow[dr, "d'"'] & & D \arrow[dl, "\phi"] \\ & D' & \end{tikzcd}$$

Le couple (D,d) est unique à un K-isomorphisme près.

On dit que l'espace D, également noté $D(K/k)$, est l'espace des <u>k-différentielles de K</u>, ou l'espace des différentielles de l'extension K/k. L'image df est appelée <u>différentielle</u> de f.

La propriété d'unicité du couple (D,d) est triviale. Pour l'existence, on renvoie à la littérature (par exemple Bourbaki, Algèbre). De (a) et (b) résultent les règles de calcul habituelles sur les différentielles.

THEOREME 2

Soit $x \in K$. Alors

$dx = 0 \iff x$ algébrique séparable sur k.

Démonstration.

$\Longleftarrow$

Il existe $f \in k[X]$ tel que $f(x) = 0$ et $f'(x) \neq 0$. On en tire $f'(x)dx = 0$, d'où $dx = 0$.

.../...

$\Longrightarrow$

Pour x transcendant ou inséparable sur k, on définit une application $K \xrightarrow{d_1} K$, s'annulant sur k, surjective, et vérifiant (a) et (b), en posant $d_1(f(x)) = f'(x)$ (dans les deux cas, en effet $f'(x)$ est déterminé par $f(x)$). D'après la condition d'application universelle du th. 1, il existe une application $\alpha : D \to K$, K-linéaire telle que $\alpha \circ d = d_1$, d'où $\alpha(dx) = 1$. On a donc $dx \neq 0$.

2. <u>Différentielles sur un sous-corps.</u>

Pour $k \subset K \subset L$, on a un L-homomorphisme surjectif canonique $\beta : D(L/k) \to D(L/K)$, obtenue en complètant le diagramme

$$\begin{tikzcd} L \arrow[r, "d_{L/k}"] \arrow[dr, "d_{L/K}"'] & D(L/k) \arrow[d, dashed, "\beta"] \\ & D(L/K) \end{tikzcd}$$

D'autre part, on a une application K-linéaire canonique $\alpha_0 : D(K/k) \to D(L/k)$ déduite de l'injection $K \to L$.

On en déduit une application K-bilinéaire $D(K/k) \times L \to D(L/k)$, d'où un L-homomorphisme $\alpha : D(K/k) \otimes_K L \to D(L/k)$.

<u>THEOREME 3</u>. Supposons que l'extension L/K est séparable (non nécessairement algébrique). On a la suite exacte suivante de L-espaces vectoriels

$$0 \longrightarrow D(K/k) \otimes_K L \xrightarrow{\alpha} D(L/K) \xrightarrow{\beta} D(L/K) \to 0 .$$

<u>Démonstration.</u>

On a déjà remarqué que β est <u>surjectif</u>.

<u>$\mathrm{Im}\,\alpha \subset \mathrm{Ker}\,\beta$</u>. En effet, pour $f \in K$, et $a \in L$, on a

$\beta(\alpha(df \otimes a)) = \beta(a\, \alpha_0(d_{K/k}\, f)) = \beta(a\, d_{L/k}\, f) = a\, \beta(d_{L/k}\, f) = a\, d_{L/K}\, f = 0.$

<u>$\mathrm{Ker}\,\beta \subset \mathrm{Im}\,\alpha$</u>. En effet, on a le diagramme

$$\begin{tikzcd} L \arrow[r, "d_{K/k}"] \arrow[dr, "d_{L/K}"'] & D(L/k) \arrow[r, "\mu"] \arrow[d, "\beta"] & D(L/k)/\mathrm{Im}\,\alpha \\ & D(L/K) \arrow[ur, dashed, "\lambda"'] & \end{tikzcd}$$

qu'on peut complèter par un L-homomorphisme $\lambda : D(L/K) \to D(L/k)/\mathrm{Im}\,\alpha$.

.../...

On a donc $\operatorname{Ker} \beta \subset \operatorname{Ker} \mu = \operatorname{Im} \alpha$.

<u>α injectif.</u> Posons $\alpha = \alpha_{KL}$. Commençons par la remarque suivante : si on a une chaîne d'extensions $k \subset K \subset L \subset L'$, et si les homomorphismes α_{KL} et $\alpha_{LL'}$ sont injectifs, il en est de même de $\alpha_{LL'}$; en effet, compte tenu de l'isomorphisme $(D(K/k) \otimes_K L) \otimes_L L' = D(K/k) \otimes_K L'$, on peut prolonger $\alpha_{KL} : D(K/k) \otimes_K L \to D(L/k)$ à un L-homomorphisme $\overline{\alpha}_{KL} : D(K/k) \otimes_K L' \to D(L/k) \otimes_K L'$; on vérifie sans difficulté que $\alpha_{KL} = \alpha_{LL'} \circ \overline{\alpha}_{KL}$, et notre assertion résulte du fait que l'injectivité de α_{KL} entraîne celle de $\overline{\alpha}_{KL}$.

Par récurrence transfinie, on se ramène donc au cas où L est une extension monogène de K , i.e. où $L = K(u)$, $u \in L$.

Pour tout polynôme $f = \Sigma a_i U^i$, posons $\delta_u^* f = \Sigma\, d_{K/k} a_i \otimes u^i$. L'application $\delta_u^* : k[U] \to D(K/k) \otimes_K L$ ainsi définie vérifie les conditions (a) et (b), et se prolonge d'une manière unique à une application $\delta_u : k(U) \to D(K/k) \otimes_K L$ vérifiant aussi ces deux conditions

Considérons l'élément ω de $D(K/k) \otimes_K L$ défini comme suit : si u est transcendant sur K , on prend $\omega = 0$; si u est algébrique, donc séparable sur K , et si $f \in K[U]$ est son polynôme irréductible, on prend pour ω l'unique solution de l'équation $\delta_u(f) + f'(u)\omega = 0$.

Pour $y \in L$, de la forme $g(u)$ (avec $g \in K(U)$), l'élément $\theta = \delta_u(g) + g'(u)\omega$ ne dépend que de y , et l'application

$$d' : L \longrightarrow D(K/k) \otimes_K L$$

obtenue en prenant $d'y = \theta$ vérifie encore les conditions (a) et (b). On peut donc compléter le diagramme

$$\begin{tikzcd} L \arrow[rr, "d_{L/k}"] \arrow[dr, "d'"'] & & D(L/k) \arrow[dl, dashed, "\alpha'"] \\ & D(K/k) \otimes_K L & \end{tikzcd}$$

.../...

par un L-homomorphisme $\alpha' : D(L/k) \to D(K/k) \otimes_K L$; on vérifie immédiatement que $\alpha' \circ \alpha$ est l'identité, ce qui entraîne bien que α est injectif.

Corollaire 1. On a $\dim D(L/k) = \dim D(K/k) + \operatorname{Dim} D(L/K)$ cela résulte en effet de la suite exacte, et du fait que $\dim(D(K/k) \otimes_K L) = \dim D(K/k)$.

Corollaire 2. Soit K/k une extension séparable. Pour que $D(K/k)$ soit de dimension finie, il faut et il suffit que K/k soit de degré de transcendance fini, et on a alors

$$\dim D(K/k) = \text{deg. tr. } (K/k).$$

En effet, d'après le th. 2, la propriété a lieu si l'extension est algébrique, car alors les deux membres sont nuls, ou si l'extension est transcendante pure, de la forme $k(u)$, car alors les deux membres sont égaux à 1 . Le corollaire 2 résulte du corollaire 1, par récurrence sur deg. tr. (K/k)

Corollaire 3. Soit K/k une extension séparable. Pour que des éléments $x_1, \dots, x_n$ de K soient algébriquement indépendants sur k, il faut et il suffit que $dx_1, \dots, dx_n$ soient linéairement indépendants sur K .

En effet, si on pose $K' = K(x_1, \dots, x_n)$, ces deux conditions se traduisent respectivement par deg. tr. $(K'/k) = n$, et par $\dim D(K'/k) = n$.

3. Espace tangent de Zariski.

Soit $\underline{o}$ un anneau local ; soit $\underline{m}$ son idéal maximal, et notons $k = \underline{o}/\underline{m}$ son corps résiduel. Considérons le quotient $\underline{m}/\underline{m}^2$ (pour la structure de $\underline{o}$-module). Soit $\bar{x} \in \underline{m}/\underline{m}^2$, représenté par $x \in \underline{m}$, et soit $\bar{a} \in k$, représenté par $a \in \underline{o}$. Alors on a $y = a\,x \in \underline{m}$, et la classe $\bar{y}$ de $y (\text{mod } \underline{m}^2)$ ne dépend que de $\bar{a}$ et de $\bar{x}$.

.../...

La loi $(\bar{a}, \bar{x}) \longmapsto \bar{a}\,\bar{x} = \bar{y}$ définit sur $\underline{m}/\underline{m}^2$ une structure d'espace vectoriel sur le corps résiduel k.

Dans le cas particulier où $\underline{o} = \underline{o}(a,V)$ est l'anneau local d'un point a d'une variété V, $\underline{m}/\underline{m}^2$ est un espace vectoriel sur le domaine universel Ω, appelé espace tangent de Zariski à V en a, qu'on note $Z(a,V)$. Plus généralement, si W est une sous-variété de V, on définit, en prenant $\underline{o} = \underline{o}(W,V)$, l'espace tangent de Zariski à V en W (ou le long de W), qui est un espace vectoriel sur le corps des fonctions $\mathcal{F}(W)$, noté $Z(W,V)$. Si k est un corps de définition de V, a, W, on définit de même $Z_k(a,V)$ (resp $Z_k(W,V)$), qui est un espace vectoriel sur k (resp $\mathcal{F}_k(W)$).

Lemme. Soient $\underline{o}$ un anneau local, $\underline{m}$ son idéal maximal, et $a_1, \dots, a_m$ des éléments de $\underline{m}$. Pour que les a_i forment un système de générateurs de $\underline{m}$, il faut et il suffit qu'ils représentent un système de générateurs de l'espace $\underline{m}/\underline{m}^2$.

Démonstration. La condition est évidemment nécessaire. Inversement, supposons que les a_i représentent un système de générateurs de $\underline{m}/\underline{m}^2$. Si on pose $\underline{a} = \Sigma_i\, a_i\, \underline{o}$, on a $\underline{m} = \underline{a} + \underline{m}^2$, d'où, puisque $\underline{a} \subset \underline{m}$, et $\underline{m}^2 \subset \underline{m}$, $\underline{m} = \underline{a} + \underline{m}^2$. Par récurrence, on en déduit $\underline{m} = \underline{a} + \underline{m}^n$ pour tout n. En effet, si on suppose $\underline{m} = \underline{a} + \underline{m}^{n-1}$, on a $\underline{m}^2 = \underline{a}\,\underline{m} + \underline{m}^n$, d'où $\underline{m} = \underline{a} + \underline{a}\,\underline{m} + \underline{m}^n$, i.e. $\underline{m} = \underline{a} + \underline{m}^n$. Or, d'après le théorème de Krull, on a $\bigcap_n (\underline{a} + \underline{m}^n) = \underline{a}$. On a donc $\underline{m} = \underline{a}$ c.q.f.d.

Si V est une variété, nous notons Δ_V la diagonale du produit $V \times V$, i.e. l'ensemble des points de $V \times V$ de la forme (x,x), avec $x \in V$; c'est une sous-variété de $V \times V$; plus précisément, si V est définie sur k, et si $\bar{x}$ est un point générique de V sur k, on a $\Delta_V = \mathrm{loc}_k\,(\bar{x},\bar{x})$.

L'espace des différentielles $D(\mathcal{F}(V)/\Omega)$ (resp. $D(\mathcal{F}_k(V)/k)$

.../...

sur le corps $\mathfrak{F}(V)$ (resp $\mathfrak{F}_k(V)$) est noté $D(V)$ (resp $D_k(V)$).

THEOREME 4.

Soit V une variété définie sur k. On a un isomorphisme canonique

$$Z_k(\Delta_V , V \times V) \simeq D_k(V).$$

Démonstration. Posons, pour simplifier, $Z = Z_k(\Delta_V , V \times V)$, et $D = D_k(V)$. Soient x et y deux points génériques indépendants de V sur k. A toute fonction $f \in \mathfrak{F}_k(V)$, associons la fonction $g(x,y) = f(x)-f(y)$ sur $V \times V$. Il est clair que $g(x,y) \in \underline{m}(\Delta_V , V \times V)$. Notons δf l'élément de Z représenté par $g(x,y)$. On voit immédiatement que l'application $\delta : \mathfrak{F}_k(V) \to Z$, ainsi définie vérifie les conditions (a) et (b) du th.1. On a donc un $\mathfrak{F}_k(V)$-homomorphisme surjectif $\alpha : D \to Z$ tel que le diagramme

$$\begin{tikzcd} \mathfrak{F}_k(V) \arrow[rr, "d"] \arrow[dr, "\delta"'] & & D \arrow[dl, "\alpha"] \\ & Z & \end{tikzcd}$$

soit commutatif. Il suffit de montrer que $\dim D = \dim Z$. Or on a $\dim D = \dim V$, et, plus précisément, si $(u_1,\dots, u_r)$ est une base de transcendance séparable de $\mathfrak{F}_k(V)$, les du_i forment une base de D. Les δu_i forment donc un système de générateurs de Z. Il suffit de montrer qu'ils sont indépendants. Or supposons-les dépendants. Dans ce cas, on peut engendrer Z par $n-1$ des éléments δu_i, par exemple par $\delta u_2,\dots, \delta u_n$. D'après le lemme précédent, l'idéal $\underline{m} = \underline{m}(\Delta_V, V \times V)$ admet pour générateurs les fonctions $u_2(x) - u_1(y),\dots, u_n(x)-u_n(y)$. On a donc une relation de la forme

$$(1)\quad u_1(x) - u_1(y) = \sum_{i\geq 2} g_i(x,y)\,(u_i(x) - u_i(y))$$

avec $g_i \in \underline{o}_k(\Delta_V , V \times V)$.

Soit w_1 un élément de Ω transcendant sur $k(x)$. Comme les $u_i(y)$ sont algébriques indépendants sur $k(x)$, on peut trouver une

.../...

place ρ_1 de Ω, à valeurs dans Ω, induisant l'identité sur $k(x)$, telle qu'on ait $\rho_1(u_1(y)) = w_1$, et $\rho_1(u_i(y)) = u_i(x)$ pour tout $i \geq 2$. On peut aussi trouver une place ρ_2 de Ω, à valeurs dans Ω, induisant l'identité sur $k(x)$, et telle que $\rho_2(w_1) = u_1(x)$. Posons $\rho = \rho_2 \circ \rho_1$. Puisque ρ prolonge l'isomorphisme $k(u(y)) \to k(u(x))$ et puisque y est algébrique sur $k(u(y))$, ρ induit un isomorphisme sur le corps $k(y)$ (cf. Chapitre 0, C, n° 7 lemme), et applique donc bijectivement les conjugués de y par rapport à $k(u(y))$ sur ceux de x par rapport à $k(u(x))$. On a donc $\rho(\overline{y}) = x$, où $\overline{y}$ est l'un des conjugués de y. Si on pose $\overline{y}_1 = \rho_1(\overline{y})$, on a $\rho_2(\overline{y}_1) = \rho_2(x) = x$. Comme les g_i sont morphiques en (x,x), ils le sont en $(x,\overline{y}_1)$. En remplaçant y par $\overline{y}$ dans (1), et en appliquant ρ_1 aux deux membres on obtient $u_1(x) - w_1 = 0$, ce qui contredit le choix de w_1.

<u>Remarque</u> : On a aussi l'isomorphisme analogue $Z(\Delta_V, V\times V) = D(V)$ (sans indices k).

4. <u>Relèvement de l'espace tangent de Zariski par un morphisme.</u>

Soit $\phi : W \to V$ une application rationnelle. Soit $b \in W$, tel que ϕ soit morphique en b, et posons $a = \phi(b)$. On a, comme on a vu (Chapitre I, n° 11), un homomorphisme canonique $\underline{o}(a,V) \to \underline{o}(b,W)$ qui est local, i.e. tel que l'image de $\underline{m}(a,V)$ soit contenue dans $\underline{m}(b,W)$. Par passage au quotient, on en déduit un homomorphisme canonique

$$Z(a,V) \xrightarrow{\mu} Z(b,W)$$

sur le domaine universel Ω. Nous dirons que μ est <u>canoniquement associé</u> à ϕ.

Plus généralement, si X est une sous-variété de W, telle que ϕ soit morphique en X et si on pose $Y = \phi_g(X)$, on a une application

$$Z(Y,V) \xrightarrow{\mu} Z(X,W)$$

canoniquement associée à ϕ, qui est un di-homomorphisme relativement à l'injection canonique $\mathcal{F}(Y) \to \mathcal{F}(X)$.

Si ϕ induit un isomorphisme $X \to Y$ (par exemple si ϕ est une injection) μ est toujours surjectif.

Si k est un corps de définition de V, W, X, Y, a, b, on a des homomorphismes canoniques analogues aux précédents, dans lesquels le symbole Z est remplacé par Z_k.

5. <u>Espace tangent de Zariski dans un produit</u>.

Soient V et W deux variétés, et soient $a \in V$, $b \in W$. On a des homomorphismes locaux $\underline{o}(a,V) \to \underline{o}(a\times b, V\times W)$, et $\underline{o}(b,W) \to \underline{o}(a\times b, V\times W)$ respectivement associés aux deux projections $pr_1 : V\times W \to V$ et $pr_2 : V\times W \to W$. Il résulte du théorème

.../...

du chapitre I que $\underline{m} = \underline{m}(a \times b,\ V \times W)$ est engendré par la réunion des images respectives de $\underline{m}(a,V)$ et $\underline{m}(b,W)$ par ces homomorphismes. On en déduit que les images par relèvement de $Z(a,V)$ et $Z(b,W)$ engendrent l'espace $Z(a \times b,\ V \times W)$. On voit facilement d'autre part que ces images sont supplémentaires dans cet espace. On a donc l'isomorphisme

$$Z(a \times b,\ V \times W) = Z(a,V) \times Z(b,W).$$

De même, si X et Y sont des sous-variétés de V et W respectivement, l'espace $Z(X \times Y,\ V \times W)$ est isomorphe à la somme directe des sous-espaces (supplémentaires) de cet espace respectivement engendrés par les images par relèvement de $Z(X,V)$ et $Z(Y,W)$.

6. Lemme de relèvement des spécialisations.

LEMME 2. Soit ϕ un morphisme $S_n \to S_r$. Soient k un corps, et x un point de S_n, posons $u = \phi(x)$. Supposons que les coordonnees x_i de x sont algébriques entières sur $k[u] = k[u_1,\dots,u_r]$. Soit a un point de S_n qui est spécialisation de x sur k. Posons $b = \phi(a)$. Soit ρ une place de Ω telle que $\rho(u) = b$. Alors on a $\rho(\overline{x}) = a$, où $\overline{x}$ est l'un des conjugués de x sur $k(u)$.

Démonstration : En effet, en utilisant les équations de dépendance intégrale vérifiées par les x_i, on voit qu'il n'existe qu'un nombre fini de points $a_\alpha \in \mathrm{loc}_k\, x$ tels que $\phi(a_\alpha) = b$. Choisissons $g \in k[X] = k[X_1,\dots,X_n]$ tel que $g(a) = 0$, et que $g(a_\alpha) \neq 0$ pour les a_α distincts de a. L'élément $y = g(x)$ de $k[x]$ est entier sur $k[u]$. Soit

$$(1) \qquad y^n + h_1(u)\, y^{n-1} + \dots + h_n(u) = 0$$

où les h_i sont des polynômes à coefficients dans k, une équation

.../...

de dépendance intégrable vérifiée par y. Notons $y^{(\nu)}$ les conjugués de y sur $k(u)$. On a donc :

$$(2) \qquad h_n(u) = \pm \prod_\nu (y^{(\nu)}) .$$

Puisque a est spécialisation de x sur k, on a un k-homomorphisme $k[x] \xrightarrow{\theta} k[a]$. On a nécessairement $\theta(y) = 0$, et $\theta(u) = b$. En appliquant θ aux deux membres de (1), on obtient $h_n(b) = 0$. D'autre part, les $y^{(\nu)}$ sont entiers sur $k[u]$, donc on a $\rho(y^{(\nu)}) \neq \infty$ pour tout ν. En appliquant ρ aux deux membres de (2), on obtient $\rho(\prod_\nu y^{(\nu)}) = 0$, d'où $\rho(\bar{y}) = 0$, où $\bar{y}$ est l'un des $y^{(\nu)}$.

On peut prolonger le $k(u)$-isomorphisme $k(u,y) \to k(u,\bar{y})$ à un homomorphisme $k(u,x) \to k(u,\bar{x})$. On a $\bar{y} = g(\bar{x})$, d'où $g(\rho(\bar{x})) = \rho(\bar{y}) = 0$. D'autre part, on a $\Phi(\bar{x}) = u$, d'où $\Phi(\rho(\bar{x})) = b$. On a donc : $\rho(\bar{x}) = a$.

7. <u>L'espace vectoriel</u> $D(V)_W$.

<u>THEOREME 5</u>.

Soient V une variété et W une sous-variété de V. Soit k un corps de définition de V et W. On a une suite exacte :

$$0 \to Z_k(W,V) \xrightarrow{\alpha} Z_k(\Delta_W, V \times W) \xrightarrow{\beta} Z_k(\Delta_W, W \times W) \to 0$$

d'espaces vectoriels sur $\mathfrak{F}_k(W)$, où α et β sont les homomorphismes canoniques respectivement associés à la projection $pr_1 : V \times W \to V$ et à l'injection $i : W \times W \to V \times W$.

<u>Démonstration</u>. On peut supposer V affine ($V \subset \mathfrak{S}_n$).

β est <u>surjectif</u>, comme associé à l'injection i.

<u>Im α $\subset$ ker β</u>, car si $f \in \underline{m}_k(W,V)$, f se relève sur $V \times W$ à une fonction qui s'annule sur Δ_W.

<u>ker β $\subset$ Im α</u>. Posons $r = \dim W$. Soient x, x' deux points génériques de V, et y, y' deux

....../...

points génériques de W, tous les quatre indépendants sur k.
Soit (u_i) $(1 \leq i \leq r)$ une famille de polynômes $\in k[X] = k[X_1,\ldots,X_n]$ induisant sur W des fonctions algebriquement indépendantes sur k et telles que les coordonnées de y soient entières sur $k[u(y)] = k[u_1(y),\ldots, u_r(y)]$.

Soit (v_j) une famille de polynômes tels que les $v_j(x)$ forment un système de générateurs de $\underline{m}_k(W,V)$.

Considérons un élement θ de $Z_k(\Delta_W, V \times W)$. Il est représenté par une fonction $f(x,y)$ sur $V \times W$, où f est une fraction rationnelle qui est morphique sur Δ_W, et telle que $f(y,y) = 0$. Pour qu'on ait $\theta \in \ker \beta$, il faut et il suffit qu'on ait $f(y,y') \in \underline{m}_k^2(\Delta_W, W \times W)$. D'après la démonstration du théorème 4, l'idéal $\underline{m}_k(\Delta_W, W \times W)$ est engendré par les $u_i(y) - u_i(y')$; on a donc alors une relation de la forme

$$f(y',y) = \sum_{h,i} (u_h(y') - u_h(y))\,(u_i(y') - u_i(y))f_{hi}(y',y),$$

où les f_{hi} sont des fractions rationnelles définies sur k, morphiques sur Δ_W. On en déduit

$$f(x,y) = \sum_{h,i} (u_h(x) - u_h(y))\,(u_i(x) - u_i(y))\, f_{hi}(x,y)+f^*(x,y),$$

où f^* est morphique sur Δ_W, et s'annule sur $W \times W$. On a donc

$$f^*(x,y) = \sum_j v_j(x) \quad b_j(x,y),$$

où les $b_j(x,y)$ sont morphiques sur Δ_W. On en déduit

$$f^*(x,y) \equiv h(x) \quad \bmod \quad \underline{m}_k(\Delta_W, V \times W)^2$$

en posant $h(x) = \sum_j v_j(x) \; b_j(x,x)$, donc θ est l'image par α de l'élément de $\underline{m}(W,V)$ représenté par h.

Pour achever de montrer l'exactitude de la suite, il suffit d'établir la relation

$$\dim Z_k(\Delta_W, V \times W) = \dim Z_k(W,V) + r \; ;$$

on sait en effet, d'après le th. 4, que

.../...

$\dim Z_k(\Delta_W, W \times W) = \dim D_k(W) = \dim W = r$.

Pour cela, considérons à nouveau les polynômes u_i , v_j introduits plus haut ; on peut supposer les u_i choisis de façon que $k[x]$ soit entier sur $k[u(x)] = k[u_1(x),\ldots, u_r(x)]$ (par exemple en prenant les u_i linéaires et homogènes, compte tenu du lemme de normalisation, chapitre I , n° 4) ; on peut en outre supposer que les v_j représentent une base de $Z_k(W,V)$. Il nous suffit de prouver que les fonctions $u_i(x) - u_i(y)$ et $v_j(x)$ représentent une base de $Z_k(\Delta_W, V \times W)$.

Montrons d'abord que ces fonctions représentent un système de générateurs de cet espace, i.e. qu'elles engendrent $\underline{m}_k(\Delta_W, V \times W)$. En effet, si $f(x,y) \in \underline{m}_k(\Delta_W, V \times W)$, la fonction induite $f(y',y)$ sur $W \times W$ est définie et, compte tenu de la démonstration du th. 4 de la forme

$$f(y',y) = \textstyle\sum_i (u_i(y') - u_i(y))\, g_i(y',y), \text{ avec}$$

$g_i(y',y) \in \underline{o}_k(\Delta_W, W \times W)$. On en déduit

$$f(x,y) - \textstyle\sum_i (u_i(x) - u_i(y))\, g_i(x,y) \in \underline{m}_k(W \times W\ ,\ V \times W),$$

et on conclut en remarquant que ce dernier idéal est engendré par les $v_j(x)$.

Compte tenu du lemme du n° 3, il suffit de montrer maintenant que toute relation de la forme

$$(3) \quad \sum_i (u_i(x) - u_i(y))\, a_i(x,y) + \sum_j v_j(x)\, b_j(x,y) = 0\ ,$$

avec $a_i(x,y)$ et $b_j(x,y) \in \underline{o}_k(\Delta_W, V \times W)$, entraine $a_i(x,y)$ et $b_j(x,y) \in \underline{m}_k(\Delta_W\ , W \times W)$ quels que soient i et j.

En chassant les dénominatuurs, on peut supposer que les a_i b_j sont des polynômes. Considérons une place ρ de Ω induisant l'identité sur k , et telle que $\rho(x) = y$. On peut trouver un point $\bar{y} \in W$ (necessairement générique de W sur k) tel que

.../...

$u_i(\bar{y}) = u_i(x)$ pour tout i ; les coordonnées de ce point sont entières sur l'anneau $k[u(x)]$. D'après le lemme 2 du n° 6 (relèvement des spécialisations), on peut en outre choisir $\bar{y}$ de façon que $\rho(\bar{y}) = y$.

Comme les fonctions a_{ij} , b_{ij} sont morphiques en (y,y), elles le sont aussi en $(x,\bar{y})$. Si l'on spécialise (x,y) en $(x,\bar{y})$ dans (3), on obtient

$$\sum_j v_j(x)\, b_j(x,\bar{y}) = 0 .$$

Or $k[x,\bar{y}]$, regardé comme $k[x]$-module, admet une base finie $t_1,\dots, t_m$. En décomposant les $b_j(x,\bar{y})$ suivant cette base, sous la forme $b_j(x,\bar{y}) = \sum_h c_{jh}(x)\, t_h$, on obtient $\sum_{j,h} v_j(x)\, c_{jh}(x) t_h = 0$. On a donc, pour tout h , $\sum_j v_j(x)\, c_{jh}(x) = 0$, d'où, compte tenu du choix des v_j , $c_{jh}(x) \in \underline{m}(W,V)$ quels que soient j et h . On en déduit $c_{jh}(\bar{y}) = 0$, d'où $b_j(\bar{y},\bar{y}) = 0$, i.e. $b_j(x,y) \in \underline{m}(\Delta_W, V \times W)$ Par suite, on a $\sum_i (u_i(x) - u_i(y))\, a_i(x,y) \in \underline{m}(\Delta_W, V \times W)^2$. Donc $\sum_i (u_i(y') - u_i(y))\, a_i(y',y) \in \underline{m}(\Delta_W, W \times W)^2$. D'après la démonstration du th. 4, ceci entraine $a_i(y,y) = 0$, i.e. $a_i(x,y) \in \underline{m}(\Delta_W, V \times W)$

c.q.f.d.

<u>Remarque</u> : On a aussi une suite exacte analogue

$$0 \to Z(W,V) \to Z(\Delta_W, V \times W) \to Z(\Delta_W, W \times W) \to 0$$

sans indices k .

W étant toujours une sous-variété de V , considérons une différentielle $\omega \in D(V)$. Compte tenu de l'isomorphisme $D(V) \simeq Z(\Delta_V, V \times V)$, on peut représenter ω par une fonction

$f(x,x') \in \underline{m}(\Delta_V, V \times V)$. Si on peut choisir pour f une fonction morphique sur Δ_W , nous dirons que <u>ω est morphique sur W</u>. La fonction f est alors de la forme $\dfrac{p(x,x')}{q(x,x')}$, où p et q

.../...

sont des polynômes, avec $q(y,y) \neq 0$, et $p(x,x) = 0$. Si (x_i) sont les coordonnées de x, et (x'_i) celles de x', on a une relation de la forme $p(x,x') = \sum(x_i - x'_i)\, p_i(x,x')$, où les p_i sont des polynômes. En posant $f_i = p_i/q$, on a donc

$f(x,x') = \sum\limits_i (x_i - x'_i)\, f_i(x,x')$, d'où

$f(x,x') \equiv \sum\limits_i (x'_i - x_i)\, g_i(x) \pmod{\underline{m}(\Delta_V, V \times V)^2}$, avec

$g_i(x) = f_i(x,x)$. Donc ω est de la forme $\omega = \sum_i g_i(x) dx_i$, où les $g_i(x)$ sont morphiques sur W. Inversement, toute différentielle $\omega \in D(V)$ de cette forme est morphique sur W.

L'ensemble des $\omega \in D(V)$ qui sont morphiques sur W est un $\underline{o}(W,V)$-module, qu'on note $D(W,V)$. De même, si k est un corps de definition de V et W, on définit $D_k(W,V)$, comme le $\underline{o}_k(W,V)$-module composé des différentielles sur V, définies sur k, et qui sont morphiques sur W.

On a une application $D(W,V) \xrightarrow{\lambda} Z(\Delta_W, V \times W)$ déduite de l'homomorphisme local canonique $\underline{o}(\Delta_W, V \times W) \xrightarrow{\mu} \underline{o}(\Delta_W, W \times W)$ associé à l'injection $W \times W \to V \times W$. Comme μ est surjectif, il en est de même de λ. L'application λ possède les propriétés suivantes :

$$\lambda\,(\omega_1 + \omega_2) = \lambda\,\omega_1 + \lambda\,\omega_2$$

et, pour $a \in \underline{o}(W,V)$,

$$\lambda(a\,\omega) = \bar{a}\,\lambda(\omega)$$

en appelant $\bar{a}$ l'image de a par l'homomorphisme canonique $\underline{o}(W,V) \xrightarrow{\nu} \mathcal{F}(W)$. Autrement dit, λ est un di-homomorphisme compatible avec ν.

L'image $\lambda(\omega)$ est encore appelée valeur de la différentielle ω en W, et notée ω_W. L'espace $Z(\Delta_W, V \times W)$, image de λ est encore noté $D(V)_W$. L'espace $Z_k(\Delta_W, V \times W)$ est, de même, noté

.../...

$D_k(V)_W$.

La suite exacte du théorème 5 peut s'écrire, avec ces nouvelles notations :

$$0 \to Z_k(W,V) \xrightarrow{\alpha} D_k(V)_W \xrightarrow{\beta} D_k(W) \to 0 .$$

On identifiera d'autre part tout élément de l'espace de Zariski $Z_k(W,V)$ avec son image par α, ce qui nous permettra de désigner l'élément de $Z_k(W,V)$ représenté par f par $(df)_W$.

8. Dimension de l'espace $D(V)_W$.

Examinons d'abord le cas où $V = S_n$.

THEOREME 6.

On a $\dim D(S_n)_W = n$, pour toute sous-variété W de S_n .

Démonstration. En effet, soit k un corps de définition de W , et soient x,y des points génériques indépendants de S_n et W respectivement sur k . L'espace $D(S_n)_W$ est engendré par les $(dx_i)_W$ $(1 \leq i \leq n)$, i.e. par les classes (mod $\underline{m}(\Delta_W, S_n \times W)^2$ des $x_i - y_i$. Il suffit de montrer que ces éléments sont linéairement indépendants. Supposons qu'ils sont dépendants, et, par exemple, que $D(S_n)_W$ est engendré par $(dx_2)_W ,\ldots, (dx_n)_W$. Alors (lemme, n° 3), l'idéal $\underline{m}(\Delta_W , S_n \times W)$ est engendré par $x_2-y_2,\ldots, x_n-y_n$. On a donc

(1) $x_1-y_1 = \sum_{j\geq 2} (x_j-y_j)\, g_j(x,y)$, avec $g_j \in \underline{o}(\Delta_W, S_n \times W)$.

Soit $\bar{y}_1$ un élement de Ω algébrique indépendant de $y_1,\ldots, y_n$ sur k . Comme les fonctions g_j sont morphiques en (y,y), elles le sont à fortiori en $(\bar{y},y)$, où $\bar{y}$ est le point de coordonnées $\bar{y}_1, y_2,\ldots, y_n$. Or on peut spécialiser x en $\bar{y}$ sur le corps $k(y)$; cette spécialisation appliquée à chacun des deux membres de (1), donne $\bar{y}_1 - y_1 = 0$, ce qui contredit le choix de $\bar{y}_1$. c.q.f.d.

Supposons maintenant que V est une variété affine quelconque

.../...

($V \subset \mathbb{S}_n$). Posons $q = \dim V$, et $r = \dim W$. On a un homomorphisme canonique

$$D(\mathbb{S}_n)_W \xrightarrow{\gamma} D(V)_W$$

déduit de l'homomorphisme local canonique $\underline{o}(\Delta_W, \mathbb{S}_n \times W) \xrightarrow{\mu} \underline{o}(\Delta_W, V\times W)$ associé à l'injection $V \times W \to \mathbb{S}_n \times W$. Comme μ est surjectif, γ est <u>surjectif</u>.

Nous allons montrer que <u>le noyau de γ est l'ensemble des $(dh)_W$, où h parcourt l'ensemble des éléments de $\underline{o}(W, \mathbb{S}_n)$ qui s'annulent sur V</u>.

En effet, notons x, y, z trois points génériques indépendants de $\mathbb{S}_n$, V, W respectivement sur k. Soit $\theta \in \ker \gamma$, représenté par $f(x,z)$, où f est une fraction ratinnnelle morphique et de valeur nulle sur Δ_W. On a $f(y,z) \in \underline{m}(\Delta_W, V \times W)^2$, c'est à dire $f(y,z) = \sum_i g_i(y,z)\, h_i(y,z)$, avec g_i, h_i, morphiques et de valeur nulle sur Δ_W. Donc la fonction $f^*(x,z) = f(x,z) - \sum_i g_i(x,z)$ $h_i(x,z)$ sur $\mathbb{S}_n \times W$ s'annule sur $V \times W$. Donc, si $\{h_j\}$ est un système de générateurs de l'idéal $\mathfrak{J}(V)$, on a $f^*(x,z) = \sum_i h_j(x)$ $b_j(x,z)$, où les b_j sont morphiques sur Δ_W. Donc, si on pose $c_j(x) = b_j(x,x)$, et $h(x) = \sum_j h_j(x)\, c_j(x)$, on a $f(x,z) \equiv h(x)$ (mod $\underline{m}(\Delta_W, \mathbb{S}_n \times W)^2$). On a donc $\theta = (dh)_W$. Réciproquement, si $h \in \underline{o}(W, \mathbb{S}_n)$ s'annule sur V, il est clair qu'on a $(dh)_W \in \ker \gamma$.

L'assertion est donc demontrée. En outre, le calcul précédent donne la relation $(dh)_W = \sum_j c_j(y)\, (dh_j)_W$. Donc si les h_j engendrent $\mathfrak{J}(V)$ les $(dh_j)_W$ engendrent $D(V)_W$. Comme les $(dx_i)_W$ sont linéairement indépendantes, et comme on a $(dh_j)_W = \sum_i \frac{\partial h_j}{\partial X_i}(y)\, (dx_i)_W$, <u>la dimension s de $\ker \gamma$ est égale au rang de la matrice</u> $\left(\frac{\partial h_j}{\partial X_i}(y)\right)$.

Notons d'autre part, que si W et W' sont deux sous-variétés

.../...

de V telles que $W \subset W' \subset V$, si on note γ' l'homomorphisme $D(S_n)_{W'} \xrightarrow{\gamma'} D(V)_{W'}$ analogue à γ, et si on pose $s' = \dim(\ker \gamma')$ on a $s \leq s'$. En effet, il suffit de remarquer que tout déterminant extrait de la matrice $\frac{\partial h_j}{\partial X_i}$ qui s'annule sur W' s'annule aussi sur W.

En particulier, prenons $W' = V$. Comme on a $(D(V))_V \simeq$ $\simeq Z(\Delta_V, V \times V) \simeq D(V)$, on a, dans ce cas particulier, $s' = n-q$

On en déduit l'inégalité $s \leq n-q$. On a d'autre part $\dim D(V)_W = n-s$ et $\dim D(W) = \dim W = r$. Compte tenu de la suite exacte du th. on a donc $\dim Z(W,V) = n-r-s$ et, par conséquent $\dim Z(W,V) \geq q-r =$ $=$ codimension de W relativement à V. On a donc démontré :

THEOREME 7

Soient $W \subset V \subset S_n$, et posons $q = \dim V$, $r = \dim W$. Soit k un corps de définition de V et W, et soit y un point générique de W sur k. Soit h_j un système de générateurs de l'idéal $\mathfrak{J}_k(V)$.

Alors, on a $\dim Z(W,V) = n-r-s$, et $\dim D(V)_W = n-s$, où s est le rang de la matrice $(\frac{\partial h_j}{\partial X_i}(y))$.

On a l'inégalité $s \leq n-q$ d'où $\dim D(V)_W \geq q$, et $\dim Z(W,V) \geq q-r$.

Corollaire. Soient V et W deux variétés (abstraites) telles que $W \subset V$, de dimensions respectives q et r. Alors on a $\dim D(V)_W \geq q$, et $\dim Z(W,V) \geq q-r$.

(On remplace en effet V par un ouvert affine de V contenant W

9. Point ou sous-variété simple.

Définition : Soient V et W deux variétés telles que $W \subset V$, et de dimensions respectives q et r. On dit que W est simple sur V si on a l'une des égalités équivalentes $\dim D(V)_W = q$, ou $\dim Z(W,V) = q-r$.

Il revient au même de dire que l'idéal $\underline{m}(W,V)$ peut être engendré par $q-r$ éléments.

La définition s'applique en particulier au cas où $W = a$ est un point. La condition s'écrit alors $\dim Z(a,V) = q$.

Un point (ou une sous-variété) non simple est dit multiple.

.../...

Dans le cas ou V est affine, on peut encore caractériser une sous-variété simple W par la relation <u>$s = n-q$</u> , où s est le rang de la matrice $\frac{\partial h_j}{\partial X_i}(y)$ intervenant dans le th. précédent. C'est le <u>critère jacobien</u> de simplicité.

Notons que, si k est un corps de définition de V et W, et si y est un point générique de W sur k, pour que W soit simple sur V, il faut et il suffit qu'il en soit de même de y. D'autre part, la propriété pour W d'être simple sur V n'est pas modifiée par toute transformation birationnelle définie sur k, qui est bimorphique en y.

<u>Remarque</u> : On définit la notion de sous-variété <u>k-simple</u> par la condition $\dim Z_k(W,V) = q-r$. Si V et W sont définies sur k, et si W est simple sur V, alors W est k-simple sur V. La réciproque est vraie en caractéristique nulle, mais fausse en caractéristique $p \neq 0$. On ne considérera dans la suite que la notion "absolue" de simplicité.

10. <u>Propriétés des points simples.</u>

Remarquons d'abord que tout point, ou toute sous-variété de $\mathbb{S}_n$ est simple sur $\mathbb{S}_n$ (th.6). Il en est de même de tout point ou sous-variété de $\mathbb{P}_n$.

<u>THEOREME 8</u>

Soit V une variété. L'ensemble des points simples de V est un ouvert non vide U de V.

<u>Démonstration</u>. il suffit en effet de considérer le cas où V est affine. Or dans ce cas l'ensemble des points multiples de V est l'ensemble des zéros de tous les déterminants d'ordre $\geqslant n-r$ extraits de la matrice $\frac{\partial h_j}{\partial X_i}$ (cf. th. 7) ; c'est donc un sous-ensemble fermé de V.

.../...

THEOREME 9

Soient V et W deux variétés, et soient $a \in V$, $b \in W$. Pour que $a \times b$ soit simple sur $V \times W$, il faut et il suffit que a soit simple sur V, et que b soit simple sur W.

Démonstration. Il suffit d'utiliser l'isomorphisme $Z(a \times b , V \times W) = Z(a,V) \times Z(b,V)$ introduit au n° 5.

THEOREME 10

Soit V une variété, et soit W une sous-variété de codimension 1 de V. Pour que W soit simple sur V, il faut et il suffit que $\underline{m}(W,V)$ soit principal, et $\underline{o}(W,V)$ est alors un anneau de valuation discrète.

Démonstration. La première assertion résulte trivialement de la définition d'une sous-variété simple. D'autre part, si $\underline{m}(W,V)$ est principal, l'anneau $\underline{o}(W,V)$, étant noethérien, est de valuation discrète.

La valuation de $\mathcal{F}(V)$, associée à l'anneau $\underline{o}(W,V)$, et normée de façon que l'ensemble de ses valeurs soit Z, est notée ω_W.

11. Diviseurs.

Soit V une variété définie sur un corps k. On considère les couples (U,f) composés d'un ouvert U de V, et d'une fonction $f \neq 0$ sur V. Deux tels couples (U,f) et (U',f') sont dits compatibles si f/f' est inversible (i.e. si f/f' et f'/f sont morphiques) en tout point de $U \cap U'$; c'est là une relation d'équivalence. On considère d'autre part les systèmes $\{U_\alpha , f_\alpha\}$ composés de tels couples deux à deux compatibles, et tels que les U_α recouvrent V. On dira que deux tels systèmes sont compatibles si les couples du premier sont compatibles avec ceux du second. C'est encore une relation d'équivalence.

.../...

Les classes pour cette relation sont appelées les diviseurs sur V. On dira qu'un diviseur D est rationnel sur k si on peut le représenter par un système $\{U_\alpha , f_\alpha\}$ tel que les U_α soient des k-ouverts, et les f_α des fonctions définies sur k.

On peut aussi, pour définir les diviseurs, utiliser la théorie des faisceaux : on définit un faisceau de groupes en prenant en chaque point a de V le groupe multiplicatif des fonctions $\neq 0$ sur V, modulo le sous-groupe des fonctions inversibles en a. Les diviseurs s'identifient aux sections de ce faisceau.

Cas particulier : si f est une fonction sur V, l'unique couple (V,f) définit un diviseur sur V, appelé diviseur de f, et noté $\mathrm{div}(f)$.

Si D et D' sont deux diviseurs sur V, respectivement représentés par $\{U_\alpha , f_\alpha\}$ et $\{U'_\beta , f'_\beta\}$, le diviseur représenté par $\{U_\alpha \cap U'_\beta , f_\alpha f'_\beta\}$ ne dépend que de D et D'. On le désigne par $D + D'$. Muni de cette loi, l'ensemble des diviseurs sur V est un groupe commutatif, qu'on note $\mathcal{D}(V)$.
(remarque : Cette loi est notée additivement, bien qu'elle se déduise de la multiplication des fonctions). On a, en particulier $\mathrm{div}(ff') = \mathrm{div}(f) + \mathrm{div}(f')$. Si k est un corps de définition de V, les diviseurs sur V qui sont rationnels sur k forment un sous-groupe de $\mathcal{D}(V)$, qu'on note $\mathcal{D}_k(V)$.

Si, pour tout α, la fonction f_α est morphique en tout point U_α, le diviseur D est dit positif. Il est clair que cette propriété ne dépend que de D, mais non du choix des (U_α, f_α) La relation $D-D'$ positif, notée également $D \geq D'$ est une relation d'ordre, compatible avec la structure de groupe de $\mathcal{D}(V)$, et qui fait donc de $\mathcal{D}(V)$ un groupe ordonné.

.../...

Soit $\Phi : V' \to V$ un morphisme, et soit D un diviseur sur V, défini par une famille $\{U_\alpha, f_\alpha\}$. Supposons que, pour tout α, la fonction f_α soit morphique sur l'image $\Phi_g(V')$. Alors on peut définir un diviseur D' sur V', au moyen des couples (U'_α, f'_α) obtenus en prenant $U'_\alpha = \phi^{-1}(U_\alpha)$, et $f'_\alpha = f_\alpha \circ \phi$ (fonction obtenue en relevant f_α). Le diviseur D' ainsi construit est noté $\phi^{-1}(D)$. L'application $D \mapsto \phi^{-1}(D)$ est un homomorphisme de $\mathcal{D}(V)$ dans $\mathcal{D}(V')$.

Cas particulier : si V' est une sous-variété de V, et si i est l'injection $V' \to V$, le diviseur $D' = i^{-1}(D)$ sur V' est appelé diviseur <u>induit</u> par D sur V'.

12. <u>Cycle associé à un diviseur.</u>

<u>THEOREME 11.</u>

Soit f une fonction $\neq 0$ sur une variété V. Il n'existe qu'un nombre fini de sous-variétés W de V, simples et de codimension 1, telles qu'on ait $\omega_W(f) \neq 0$.

<u>Démonstration.</u> On peut supposer que V est affine $(V \subset \mathbb{S}_n)$, et que f est induite par un polynôme p (car si $f = \frac{g}{h}$, et si le théorème est vrai pour g et h, il l'est pour f).
Soit alors $H = \mathcal{Y}(p)$ l'ensemble des zéros de p. Comme on a $f \neq 0$, on a $V \not\subset H$. Toute composante de $V \cap H$ est donc de dimension $\leq q-1$, en posant $q = \dim V$. Soit W une sous-variété simple et de codimension 1 de V, telle que $\omega_W(f) \neq 0$. Puisque f est induite par un polynôme, on a $\omega_W(f) \geq 0$. On a donc $\omega_W(f) > 0$, donc $f \in \underline{m}(W,V)$, donc $f \in \mathfrak{J}(W)$, donc $W \subset H$, donc $W \subset V \cap H$. Puisque $\dim W = q-1$, W cïncide avec l'un des composants (en nombre fini) de $V \cap H$.

Soit V une variété de dimension n. Soit r un entier, tel que $0 \leq r \leq n$. On appelle <u>cycle de dimension r</u> sur V toute combinaison linéaire formelle $X = \sum_i m_i W_i$, à coefficients m_i

.../...

entiers (nuls, sauf un nombre fini) de sous-variétés simples de dimension r de V.

Le nombre $n-r$ est appelé codimension de X.

L'ensemble des cycles de dimension r sur V est un groupe commutatif. On a de plus sur cet ensemble une structure de groupe ordonné, un cycle positif étant caractérisé par la condition $m_i \geq 0$ pour tout i. Les cycles

$\sum_i m_i^+ \; W_i$, et $\sum_i m_i^- W_i$ (où l'on pose $m_i^+ = \sup(m_i, 0)$, et $m_i^- = \mathrm{Sup}(-m_i, 0)$) sont respectivement notés X^+ et X^-. Ils sont caractérisés par la propriété d'être positifs, sans composante commune, et tels que $X = X^+ - X^-$.

Les W_i ayant des coefficients $m_i \neq 0$ sont appelées les composantes de X. La réunion des composantes de X est appelée le support de X, et notée supp X.

Si W est une sous-variété, on confondra souvent W avec le cycle admettant comme unique composante W, de coefficient $+1$.

Soit f une fonction $\neq 0$ sur V. On appelle cycle associé à f, et on note $\mathfrak{X}(f)$, le cycle $\mathfrak{X}(f) = \sum_W \omega_W(f)W$, où W parcourt l'ensemble des sous-variétés simples et de codimension 1 de V. Ce symbole a un sens, compte tenu du th. 11. On a d'autre part $\mathfrak{X}(f_1 f_2) = \mathfrak{X}(f_1) + \mathfrak{X}(f_2)$.

Plus généralement, soit D un diviseur sur V, défini par une famille $\{U_\alpha, f_\alpha\}$. Considérons une sous-variété W de V simple et de codimension 1 sur V, choisissons α tel que W rencontre U_α. L'entier $\omega_W(f_\alpha)$ ne dépend pas alors de α (car si W rencontre U_α et U_β, la fonction f_α/f_β est inversible sur W, i.e. on a $\omega_W(f_\alpha/f_\beta) = 0$). Nous désignerons cet entier par $\omega_W(D)$. On déduit du th. 11 que, pour D donné cet entier n'est $\neq 0$ que pour un nombre fini de valeurs

.../...

de W. On note $\mathfrak{X}(D)$, et on appelle <u>cycle associé à D</u>, le cycle de codimension 1 $\mathfrak{X}(D) = \sum_W \omega_W(D)\, W$. Il est clair qu'on a $\mathfrak{X}(\mathrm{div}(f)) = \mathfrak{X}(f)$, et que l'application $D \mapsto \mathfrak{X}(D)$ est un homomorphisme de groupes ordonnés.

13. <u>Paramètres uniformisants.</u>

Soit W une sous-variété de V. On appelle <u>système de paramètres uniformisants</u> de V en W un système de générateurs minimal $\{u_j\}$ de l'idéal $\underline{m}(W,V)$, i.e. tel que les $(du_j)_W$ forment une base de l'espace $Z(W,V)$. Si W est simple sur V, le nombre de ces éléments est égal à la codimension $q-r$ de W relativement à V.

<u>Remarques.</u>

1. Tout système de paramètres uniformisants $\{u_j\}$ de V en W est composé d'éléments algébriquement indépendants de $\mathfrak{F}(V)$. En effet, puisque les $(du_j)_W$ sont linéairement indépendantes, il en est de même à fortiori des du_i, et il suffit d'appliquer le coroll. 3 du th. 3 de ce chapitre.

2. Si $W \subset V \subset \mathbb{S}_n$, on peut trouver un système de paramètres uniformisants de V en W composé d'éléments $u_j \in \mathfrak{A}(V)$, i.e. induits par des polynômes ; on peut plus précisément, extraire ces polynômes d'une famille quelconque de générateurs de $\mathfrak{J}(V)$.

3. Si, de plus, $W = a$ est un point, on peut extraire les u_j de la famille des fonctions $x_i - a_i$. On remarque également que, si c_{ij} $(1 \leq i \leq n,\ 1 \leq j \leq q = \dim V)$ sont des éléments de Ω, les fonctions $t_j = \sum_i c_{ij}(x_i - a_i)$ induisent encore un système de paramètres uniformisants $\{u_j\}$ de V en a, pourvu que les c_{ij} ne vérifient pas certaines relations algébriques non triviales en nombre fini : en effet, si lon note h_α $(1 \leq \alpha \leq n-q)$ un système de générateurs de l'idéal de $\mathfrak{J}(V)$, tels que les $(dh_\alpha)_a$ soient

.../...

linéairement indépendantes, les relations en question s'obtiennent en écrivant que les éléments $(dh)_a$, $(dt_j)_a$ de l'espace $(D(S_n))_a$ sont dépendants, et se traduisent par la nullité d'un nombre fini de déterminants (faciles à expliciter).

En combinant cette remarque avec le lemme de normalisation (chap. I n° 4) on voit qu'on peut trouver un système de paramètres uniformisants $\{u_j\}$ de V en a tels que, pour x générique de V sur k , les coordonnées x_i de x soient <u>algébriques entières</u> sur l'anneau $k[u_1(x),\dots, u_r(x)]$.

14. <u>Etude locale des cycles de codimension 1</u>.

<u>THEOREME 12</u>

Soient V une variété, et a un point <u>simple</u> sur V . Tout cycle X sur V de codimension 1 "est localement en a le diviseur d'une fonction".

(On veut dire par là qu'il existe une fonction f sur V telle que $a \notin \mathrm{supp}\,(\mathfrak{X}(f)-X)$ ou encore que les composantes de $\mathfrak{X}(f)$ et de X qui passent par a ont les mêmes coefficients).

<u>Démonstration</u>. On peut supposer V affine $(V\subset S_n)$, et $X = W$ (composante unique, de coefficient $+1$).

Posons $r = \dim V$. Soient $t_1,\dots, t_r$ des polynômes induisant un système de paramètres uniformisants $u_1,\dots, u_r$ de V en a . Soit k un corps de définition de V , a , $t_1,\dots, t_r$. Soient x et y des points génériques indépendants de V et W respectivement sur k . Soit ϕ le morphisme $V \to S_r$ défini par $\phi(x) = x'$, où x' a pour coordonnées les $x'_j = t_j(x) = u_j(x)$ $(1 \leq j \leq r)$. D'après la remarque 3 précédente, on peut supposer $t_1,\dots, t_r$ choisis de façon que les coordonnées x_i de x $(1 \leq i \leq n)$ soient entières sur l'anneau $k[x'] = k[x'_1,\dots, x'_r]$.

.../...

Posons d'autre part $a' = \phi(a)$, $y' = \phi(y)$, et $W' = \mathrm{loc}_k\, y' = \phi_g(y)$.

Les $(du_j)_a$ sont des éléments linéairement indépendants de $D(V)_a$. A fortiori, les $(du_j)_y$ sont des éléments linéairement de $D(V)_y$, et forment donc une base de $D(V)_y$. L'homomorphisme canonique $D(S_r)_{y'} \xrightarrow{\mu} D(V)_y$ associé à ϕ applique la base de $D(S_r)_{y'}$ composée des $(d\,x'_i)_y$ sur celle de $D(V)_y$ composée des $(d\,u_j)_y$. Donc μ est un isomorphisme.

Nous allons montrer que codim $W' = 1$ i.e. que W' est une hypersurface de S_r . En effet, posons codim $W' = s$, et soit $\{v'_h\}$ $(1 \leq h \leq s)$ un système de paramètres uniformisants, définis sur k , de S_r en W' . Considérons les fonctions $v_h = v'_h \circ \phi$ sur V obtenues en relevant les v'_h . Comme les $(du'_h)_{W'}$ sont linéairement indépendantes, il en est de même des $(du'_h)_{y'}$, donc aussi, par isomorphisme, des $(dv_h)_y$. Comme les v_h sont définies sur k , ceci signifie que les $(dv_h)_W$ $(1 \leq h \leq s)$ sont linéairement indépendantes. Or, puisque a est simple sur V , W est simple sur V , i.e. l'espace $Z(W,V)$ est de dimension 1 . On a donc $s \leqslant 1$; comme on ne peut avoir $s = 0$, on a bien $s = 1$.

Soit $f'(X) = 0$ l'équation de l'hypersurface W' $(f' \in k[X_1,\ldots,X_r])$. Soit $f = f' \circ \phi$ la fonction obtenue en relevant f' . Montrons qu'il n'existe pas de composante de $\mathfrak{X}(f)$ passant par a autre que W .

En effet, le raisonnement précédent montre que l'image $Z' = \phi_g(Z)$ est de codimension 1 dans S_r . Comme f s'annule sur Z , f' s'annule sur Z' , ce qui implique $Z' \subset W'$, d'où $Z' = W'$. Soit $k_1 \supset k$ un corps de définition de z . Il existe un point générique z_1 de Z sur k_1

.../...

tel que $\phi(z_1) = y'$, et les coordonnées de z_1 sont entières sur l'anneau $k_1[y']$. Soit ρ une place de Ω, induisant l'identité sur k , et telle qu'on ait $\rho(y) = a$; on a aussi $\rho(y') = a'$. Puisqu'on a $a \in Z$, et d'après le lemme de relèvement des spécialisations (n°6 , lemme 2) il existe $z \in Z$, conjugué de z_1 sur $k_1(y)$ (donc aussi générique de Z sur k_1 , et tel que $\phi(z) = y'$), tel qu'on ait $\rho(z) = a$

Soient $\{h_\alpha\}$ $(1 \leq \alpha \leq n-r)$ des éléments de l'idéal $\mathfrak{J}_{k_1}(V)$, tels que les $(dh_\alpha)_a$ soient linéairement indépendantes, et constituent donc une base du noyau de l'homomorphisme canonique $\gamma : D(\mathbb{S}_n)_a \to D(V)_a$. Comme γ est surjectif, et comme les $(du_j)_a$ forment une base de $D(V)_a$, la réunion des $(dh_\alpha)_a$ et des $(du_j)_a$ est une base de $D(\mathbb{S}_n)_a$. Pour x , $\overline{x}$ génériques indépendants de V sur k_1 , on a, $h_\alpha(x) - h_\alpha(\overline{x}) = 0$, d'où l'on déduit, en appliquant la formule de Taylor, une relation de la forme

$$\sum_i \left(\frac{\partial h_\alpha}{\partial X_i}(x) + \varepsilon_\alpha(x,\overline{x})\right)(x_i - \overline{x}_i) = 0 \quad ,$$

où les ε_α sont des polynômes qui s'annulent en (a,a). De même, on a

$$t_j(x) - t_j(\overline{x}) = \sum_i \left(\frac{\partial t_j}{\partial X_i}(x) + \eta_j(x,\overline{x})\right)(x_i - \overline{x_i})),$$

où les η_j sont des polynômes qui s'annulent en (a,a). Par spécialisation de $(x,\overline{x})$ en (y,z), on en déduit les relations

$$\sum_i \left(\frac{\partial h_\alpha}{\partial X_i}(y) + \varepsilon_\alpha(y,z)\right) \quad (y_i - z_i) = 0 \ (1 \leq \alpha \leq n-r)$$

$$\sum_i \left(\frac{\partial t_j}{\partial X_i}(y) + \eta_j(y,z)\right) \quad (y_i - z_i) = 0 \ (1 \leq j \leq r).$$

Le déterminant de ce système linéaire aux inconnues $y_i - z_i$ est de la forme $D(y,z)$, où D est un polynôme, tel qu'on ait $\rho(D(y,z)) = D(a,a) \neq 0$; donc on a $D(y,z) \neq 0$. Il en résulte $y_i = z_i$ pour tout i , c'est à dire $y = z$, d'où $Z = W$.

Il reste seulement à montrer qu'on a $\omega_W(f) = 1$, c'est à dire $f \notin \underline{m}(W,V)^2$, ou encore $(df)_y \neq 0$; or on a $f' \notin \underline{m}(W',\mathbb{S}_r)^2$, d'où

.../...

$(df')_{y'} \neq 0$. Par application de l'isomorphisme μ introduit plus haut, on en déduit bien $(df)_y \neq 0$ c.q.f.d.

15. Le théorème de la dimension.

THEOREME 13

Soit V une variété. Soient W, Z des sous-variétés de V. Posons $n = \dim V$, $q = \dim W$, et $r = \dim Z$.
Soit C une composante de $W \cap Z$, simple sur V . Alors on a $\dim C \geq q+r-n$.

Démonstration. Le problème étant local, on peut supposer V affine. On peut se ramener au cas où C est l'unique composante de $W \cap Z$: pour cela, on remplace, s'il y a lieu, V par un ouvert affine de V contenant C , et ne contenant pas les autres composantes de $W \cap Z$. On examine successivement les cas suivants :

a) $V = S_n$, et codim $Z = 1$. Alors Z est une hypersurface de S_n , d'équation $f(X) = 0$. Soit k un corps de définition de V , W , Z , C et f , et soit x un point générique de W sur k . D'après le lemme de normalisation (chap. I, n°4), on peut trouver des fonctions linéaires $u_1, \dots, u_q$ sur S_n telles que les x_i soient algébriques entiers sur $k[u(x)]$. Notons ϕ le morphisme ayant pour coordonnées les u_j , i.e. tel que $\phi(x) = x'$, où $x' \in S_q$ est le point ayant pour coordonnées les $x'_j = u_j(x)$. Soit y un point générique de C sur k ; posons $y' = \phi(y)$, et $C' = \phi_g(C) = \mathrm{loc}_k\, y'$. Notons z la norme de $f(x)$ relativement à l'extension algébrique $k(x)/k(x')$. Cette norme appartient à $k(x')$, et est entière sur $k[x']$. Comme $k[x']$ est intégralement clos (comme isomorphe à un anneau des polynômes), on a $z \in k[x']$, c'est à dire $z = f'(x')$, où $f' \in k[X_1, \dots, X_q]$.
On va montrer que C' coïncide avec l'ensemble S' des zéros de f' .

.../...

En effet, on peut prolonger l'homomorphisme $k[x] \to k[y]$ à une place ρ de Ω. Notons $x^{(\nu)}$ les conjugués de x sur $k(x')$. Comme ils sont entiers sur $k[x']$, on a pour tout ν, $y^{(\nu)} \neq \infty$, en posant $y^{(\nu)} = \rho(x^{(\nu)})$. Comme on a $f'(x') = \prod\limits_{\nu} f(x^{(\nu)})$, on a aussi $f'(y') = \prod\limits_{\nu} f(y^{(\nu)})$. Comme y figure parmi les $y^{(\nu)}$, on a donc $f'(y') = 0$, d'où $C' \subset S'$.

Inversement, soit $g' \in \mathfrak{J}_k(C')$, et soit g le polynôme sur S_n obtenu en relevant g', i.e. défini par $g(x) = g'(x')$. On a $g(y) = g'(y') = 0$, d'où $g \in \mathfrak{J}(C) = \mathfrak{J}(W \cap Z) = \mathrm{rad}(\mathfrak{J}(W) + \mathfrak{J}(Z)) = \mathrm{rad}(\mathfrak{J}(W) + (f))$. On a donc $g^{\mu} \equiv f\ h \pmod{\mathfrak{J}(W)}$, avec $h \in k[X_1, \ldots, X_n]$, d'où $g(x)^{\mu} = f(x)\ h(x)$, d'où en posant $m = [k(x) : k(x')]$, et en prenant la norme, $g'(x')^{m\nu} = f(x')\ h'(x')$, avec $h' \in k[X_1, \ldots, X_q]$. On a donc $S' = \mathcal{V}(f') \subset \mathcal{V}(g')$ quel que soit g'. Donc $S' \subset \mathcal{V}(\mathfrak{J}(C')) = C'$, d'où $C' = S'$. On a donc bien $\dim C \geq \dim C' = q-1$.

(b) - <u>V quelconque, C simple sur Z</u>.

Raisonnons par récurrence sur $\dim V$. Remarquons que le résultat est trivial pour $\dim V = 1$. Supposons $V \subset S_m$. Puisque C est simple sur V, on peut trouver des polynômes $f_1, \ldots, f_{m-n} \in \mathfrak{J}_k(V)$, tels que les $(df_j)_C$ soient linéairement indépendants (critère jacobien). Puisque C est simple sur Z, on peut en outre trouver un $g \in \mathfrak{J}_k(Z)$ tel que $(dg)_C$ soit linéairement indépendant des $(df_j)_C$. Notons H l'ensemble $\mathcal{V}(g)$ des zéros de g dans S_n. Soit V_1 une composante de $V \cap H$ contenant C, et soit Z_1 une composante de $V \cap H$ contenant W_1. Puisque les $(df_j)_C$ et $(dg)_C$ sont linéairement indépendants, C est simple sur V_1 (critère jacobien). De plus, on a $C = W \cap Z_1$.
D'après (a), on a $\dim Z_1 \geqslant q-1$, et $\dim V_1 \geqslant n-1$. D'autre part, g ne s'annule pas sur V, donc on a $V \not\subset H$, d'où $V_1 \neq V$.

.../...

On a donc dim $V_1 = n-1$. D'après l'hypothèse de récurrence, on a $\dim C \geq \dim W_1 + \dim Z - \dim V_1$. On en deduit
$\dim C \geq (q-1) + r - (n-1) = q + r - n$.

c) Cas général. On remplace l'intersection considérée par celle de Δ_V avec $W \times Z$ dans le produit $V \times V$ .Il est clair que cette intersection est Δ_C . Comme C est simple sur V , Δ_C est simple sur Δ_V , et on est ramené au cas (b).

CHAPITRE IV

Points simples et points normaux.

1. Points normaux, sous-variétés normales.

THEOREME 1.

Soit V une variété, et soit W une sous-variété simple de V. L'anneau local $\underline{o}(W,V)$ est intégralement clos.

Démonstration. Posons $\underline{o} = \underline{o}(W,V)$ et $\underline{m} = \underline{m}(W,V)$. On a vu que l'espace tangent de Zariski $\underline{m}/\underline{m}^2$ est un espace vectoriel sur $\mathfrak{F}(W)$, de dimension egale à la codimension r de W dans V. De même, pour tout entier $\nu \geq 0$, le quotient $\underline{m}^\nu/\underline{m}^{\nu+1}$ est canoniquement muni d'une structure d'espace vectoriel sur $\mathfrak{F}(W)$. Soient $t_1,\dots, t_r \in \mathfrak{J}(W)$ induisant un système de paramètres uniformisants $u_1,\dots, u_r$ de V en W. Alors les monômes de degré ν en $u_1,\dots, u_r$ représentent un système de générateurs de l'espace $\underline{m}^\nu/\underline{m}^{\nu+1}$. Nous allons montrer que ces générateurs sont indépendants, i.e. forment une base de cet espace. Il revient au même de prouver que, pour $h \in \underline{o}[X] = \underline{o}[X_1,\dots,X_r]$ homogène et de degré ν, tel qu'on ait

$$(1) \quad h(u_1,\dots, u_r) \in \underline{m}^{\nu+1} ,$$

les coefficients de h appartiennent à $\underline{m}$. Par un changement de variable linéaire sur les u_i, on se ramène au cas où le coefficient de u_1^ν au premier membre de (1) est $\neq 0$. La relation (1) entraine alors

$$(2) \quad u_1^\nu \in \sum_{j\geq 2} \underline{o}\, u_j .$$

Soit Z une composante de l'intersection de V avec les variétés $t_2(X) = 0,\dots, t_r(X) = 0$. Soit k un corps de définition de V, W, et Z, et soit z un point générique de Z sur k. On a, pour $j \geq 2$, $t_j(z) = u_j(z) = 0$. Compte tenu de (2), on a donc aussi $t_1(z) = u_1(z) = 0$. Or tout polynôme de l'anneau $\mathfrak{J}(W)$ induit sur V un élément de $\underline{m} = \underline{o}\, u_1 +\dots+ \underline{o}\, u_n$, donc s'annule sur Z.

.../...

On a donc $\mathfrak{I}(W) \subset \mathfrak{I}(Z)$, donc $W \supset Z$. D'autre part, d'après le théorème de la dimension, on a $\dim Z \geq n-r+1 > n-1 = \dim W$, d'ou contradiction, et l'assertion est démontrée.

Pour $x \in \underline{o}$ non nul, il existe, d'après le th. de Krull, un (et un seul) entier $\nu = \nu_x$ tel qu'on ait $x \in \underline{m}^{\nu}$, et $x \notin \underline{m}^{\nu+1}$. On a alors $x \equiv F(u_1, \dots, u_r) \pmod{\underline{m}^{\nu+1}}$, où $F \in \underline{o}[X]$ est homogène et de degré ν_x. De plus le polynôme $f \in \mathcal{F}(W)[X]$, également homogène et de degré ν_x, obtenu par réduction de $F \pmod{\underline{m}}$ est parfaitement déterminé par x. Nous le désignerons dans la suite par f_x. Si x, y, z sont trois éléments de $\underline{o}$, tels que $z = xy$, on voit en outre que $\nu_z = \nu_x + \nu_y$, et que $f_z = f_x f_y$, (ces propriétés permettent de munir canoniquement la somme des $\underline{m}^{\nu}/\underline{m}^{\nu+1}$ d'une structure d'algèbre graduée, qui est isomorphe à une algèbre de polynômes).

Soit $x \in \mathcal{F}(V)$, entier sur $\underline{o}$. On veut prouver que $x \in \underline{o}$. Or on a $x = \frac{a}{b}$, avec $a, b \in \underline{o}$, et $b \neq 0$. Par récurrence sur ν, on va d'abord montrer qu'il existe, pour tout ν, un $x_\nu \in \underline{o}$ tel que $a \equiv b\, x_\nu \pmod{\underline{m}^{\nu+1}}$.

Admettant l'existence d'un $y \in \underline{o}$ tel que $a \equiv b\, y \pmod{\underline{m}^{\nu}}$, il suffit de trouver $y' \in \underline{o}$ tel que $a \equiv b\, y' \pmod{\underline{m}^{\nu+1}}$. Pour cela posons $z = a-by$. Comme $\frac{a}{b}$ est entier sur $\underline{o}$, il en est de même de $\frac{z}{b} = t$. Il existe donc un entier m tel qu'on ait $\underline{o}[t] = \underline{o} + \underline{o}\, t + \dots + \underline{o}\, t^{m-1}$. On a alors $b^{m-1}\, \underline{o}[t] \subset \underline{o}$. En particulier, pour tout entier $s \geq 0$, on a $b^{m-1} t^s = b^{m-s-1} z^s \in \underline{o}$, donc f_b^{s+1-m} divise f_z^s. Ceci implique que f_b divise f_z, soit $f_z = f_b\, g$. On peut trouver $w \in \underline{o}$ tel que $f_w = g$ (prendre $w = G(u)$, où $G \in \underline{o}[X]$ admet g comme polynôme réduit). On a alors $z \equiv b\, w \pmod{\underline{m}^{\nu+1}}$ (puisque $\nu_z \geq \nu$), d'où $a \equiv b(y+w) \pmod{\underline{m}^{\nu+1}}$, et on peut prendre $y' = y + w$.

.../...

On a donc montré que $a \in b\,\underline{o} + \underline{m}^{\nu}$ pour tout ν. D'après le théorème de Krull, il en résulte $a \in b\,\underline{o}$, i.e. $x \in \underline{o}$, c.q.f.d.

On dit qu'une sous-variété W de V est <u>normale</u> (ou que V est <u>normale en W</u>) si l'anneau local $\underline{o}(W,V)$ est intégralement clos. Cette définition s'applique en particulier au cas où W est un <u>point</u>. Une variété dont tous les points sont normaux (ce qui implique que toutes ses sous-variétés sont normales) est dite <u>normale</u>. Si V et W sont définies sur k, et si y est générique de W sur k, il faut et il suffit, pour que W soit normale, que y le soit.

Le théorème précédent s'interprète comme suit : <u>toute sous-variété simple de V est une sous-variété normale de V</u>.

<u>Remarque 1</u>. La réciproque n'a pas lieu ; par exemple, sur un cône du second degré non dégénéré de S_3, le sommet est un point multiple, et cependant normal.

<u>THEOREME 2</u>.

Pour qu'une variété V soit normale, il faut et il suffit que son anneau de coordonnées $\mathfrak{A}(V)$ soit intégralement clos.

<u>Démonstration</u>. Supposons V normale, et soit $f \in \mathfrak{F}(V)$ entière sur $\mathfrak{A}(V)$, pour $a \in V$, on a $\mathfrak{A}(V) \subset \underline{o}(a,V)$, donc f est entière sur $\underline{o}(a,V)$, donc puisque a est normal, $f \in \underline{o}(a,V)$. Donc f est morphique en tout point de V. Donc (chap. I, th. 9, coroll. 1), on a $f \in \mathfrak{A}(V)$.

Réciproquement, supposons $\mathfrak{A}(V)$ intégralement clos. Soit $a \in V$, et soit $f \in \mathfrak{F}(V)$ entière sur $\underline{o}(a,V)$. On a $u_o f^n + u_1 f^{n-1} + \ldots + u_n = 0$, avec $u_i \in \mathfrak{A}(V)$, pour $0 \leq i \leq n$, et $u_o(a) \neq 0$. Il en résulte $(u_o f)^n + u_1(u_o f)^{n-1} + \ldots + u_o^{n-1} u_n = 0$, donc la fonction $u_o f$ est entière sur $\mathfrak{A}(V)$. On a donc $u_o f \in \mathfrak{A}(V)$, d'où $f \in \underline{o}(a,V)$.

<u>Remarque 2</u>. Soit $W \subset V$, et soit k un corps de définition de V et W ; on dit que W est <u>k-normale</u> si l'anneau $\underline{o}_k(W,V)$ est

.../...

intégralement clos. Si W est normale, W est aussi k-normale, mais la réciproque est inexacte.

Pour qu'une variété soit k-normale, il faut et il suffit que l'anneau $\mathcal{O}_k(V)$ soit intégralement clos (demonstration comme ci-dessus).

2. Fonction définie en un point.

Soit $f \in \mathcal{F}(V)$, et soit $a \in V$. On dit que f est définie en a si f ou f^{-1} est morphique en a. Si f est définie, et non morphique en a, on a $f^{-1}(a) = 0$. On pose alors $f(a) = \infty$.

Autre interprétation : on peut adjoindre à f l'application rationnelle $f^* : V \to \mathbb{P}_1$ de V dans la droite projective $\mathbb{P}_1$, définie par $f^*(x)=((f(x),1)$, pour x générique de V sur k. Pour que f soit définie en a, il faut et il suffit que f^* soit morphique en a.

3. Ensemble des valeurs d'une fonction en un point.

Soit V une variété ; soient $f \in \mathcal{F}(V)$, et $a \in V$. L'ensemble des points $b \in \mathbb{P}_1$ tels qu'on ait $(a,b) \in \Gamma_{f^*}$(où Γ_{f^*} = graphe de f^*) est appelé ensemble des valeurs de f en a, et noté $f_e(a)$. Cet ensemble peut encore être défini par la formule $f_e(a) = pr_2 (\Gamma_{f^*} \cap (a \times \mathbb{P}_1))$, où pr_2 est la projection sur le second facteur, dans $V \times \mathbb{P}_1$.

Plus généralement, soient V et W deux variétés ; soit $\phi : V \to W$ une application rationnelle, et soit E un sous-ensemble de V. Le sous-ensemble $pr_2 \ (\Gamma_\phi \cap (E \times W))$ de W est noté $\phi_e(E)$, et est appelé ensemble des valeurs de ϕ sur E, ou image ensembliste de E par ϕ. De même, si F' est un sous-ensemble de W, le sous-ensemble $E'=pr_1(\Gamma_\Phi \cap (V \times F'))$ est noté $(\Phi^{-1})_e(F')$ et est appelé image inverse ensembliste de F' par Φ. Revenons au cas d'une fonction f. Soit k un corps de définition de V et f, et soit x un point générique de V sur k. D'après le théorème de prolongement d'un homomorphisme à une place (chap. 0, A, th. 7), l'ensemble $f_e(a)$ coïncide avec celui des éléments

.../...

de Ω qui sont de la forme $\rho(f(x))$, où ρ est une place de Ω prolongeant l'homomorphisme canonique $k[x] \to k[a]$. L'ensemble $f_e(a)$ n'est donc jamais vide (puisque $\mathbb{P}_1$ est complète). C'est de plus un sous-ensemble fermé de $\mathbb{P}_1$ (car Γ_{f^*} est un sous-ensemble fermé de $V \times \mathbb{P}_1$). Autrement dit, ou bien on a $f_e(a) = \mathbb{P}_1$, ou bien $f_e(a)$ est un sous-ensemble fini de $\mathbb{P}_1$.

Une définition analogue est valable également pour le symbole $\phi_e(a)$ lorsque $\phi : V \to W$ est à valeurs dans une variété W complète On trouve encore dans ce cas que $\phi_e(a)$ est un sous-ensemble fermé non vide de W .

Lemme. Soit $a \in V$, soit k un corps de définition de a et V et soit x un point générique de V sur k . Soit ρ une place de $K(x)$ induisant l'identité sur k . Pour qu'on ait $\rho(x) = a$, il faut et il suffit que ρ soit finie sur l'anneau $\underline{o}(a,V)$.

Démonstration.

Si $f \in \underline{o}(a,V)$, on a $f(a) = \frac{p(a)}{q(a)}$, avec $q(a) \neq 0$. Donc si $\rho(x) = a$, on a $\rho(f(x)) = \frac{p(a)}{q(a)} \neq \infty$.

Réciproquement, supposons ρ finie sur $\underline{o}(a,V)$. Soient x_i (resp a_i) les coordonnées de x (resp. a).
L'hypothèse implique $\rho(x_i) = b_i \neq \infty$ pour tout i . S'il existe un i tel que $b_i \neq a_i$, la fonction $g(x) = \frac{1}{x_i - b_i}$ est morphique en a , mais cependant on a $\rho(g(x)) = \infty$. Ceci est contradictoire. On a donc $b_i = a_i$ pour tout i , d'où $\rho(x) = a$.

THEOREME 3.

Soit V une variété. Soient $f \in \mathcal{F}(V)$, et $a \in V$, normal sur V . Pour que f soit définie en a , il faut et il suffit que l'ensemble $f_e(a)$ soit fini, et on a alors $f_e(a) = \{f(a)\}$.

En effet, il est clair que la condition est nécessaire.

.../...

Supposons donc $f_e(a)$ fini soit k un corps de définition de V, f et a, et soit x un point générique de V sur k. Soit $b \in \mathbb{P}_1$, non contenu dans $f_e(a)$, et posons $g(x) = \frac{1}{f(x)-b}$.
Pour toute place ρ de $k(x)$ induisant l'identité sur k, et finie sur l'anneau local $\underline{o}(a,V)$, on a $\rho(x) = a$, d'après le lemme précédent, d'où $\rho(f(x)) \in f_e(a)$. On a donc $\rho(g(x)) \neq \infty$. Donc $g(x)$ est entier sur $\underline{o}(a,V)$ (chap. 0, B, th. 2). Puisque a est normal sur V, on a donc $g(x) \in \underline{o}(a,V)$. Or on a $f(x) = b + \frac{1}{g(x)}$. Si $g(a) \neq 0$, f est morphique en a ;si $g(a) = 0$, f^{-1} est morphique en a

c.q.f.d.

THEOREME 4

Soit V une variété, et soit W une sous-variété de codimension 1 de V. Pour que W soit normale sur V, il faut et il suffit que W soit simple sur V.

Démonstration.

La condition est suffisante, d'après le th. 1.

Supposons donc que W est normale sur V. Nous allons montrer que $\underline{o}(W,V)$ est un anneau de valuation. En effet, soit k un corps de définition de V et W, et soit y un point générique de W sur k. Montrons que l'ensemble $f_e(y)$ est fini. Sinon, en effet, il coïnciderait avec $\mathbb{P}_1$. En appelant u un point générique de $\mathbb{P}_1$ sur $k(y)$, on aurait $(u,y) \in \Gamma_f$. Le lieu $\Gamma' = loc_k(y \times u)$ serait donc une sous-variété de Γ_f. Le degré de transcendance de $k(u,y)$ sur k étant n, on aurait $\dim \Gamma' = \dim \Gamma_f = n$, d'où $\Gamma' = \Gamma_f$. Or ceci est absurde, car Γ', contenue dans $W \times \mathbb{P}_1$, ne peut contenir Γ_f.

On a donc bien montré que $f_e(y)$ est fini. D'après le théorème 3, f est définie en y, i.e. on a f ou $\frac{1}{f} \in \underline{o}(W,V)$. En d'autres

.../...

termes, $\underline{o}(W,V)$ est un anneau de valuation. Or il est noethérien. C'est donc un anneau de valuation discrète. En particulier, il est principal, donc W est simple sur V c.q.f.d.

Corollaire. Sur une courbe algébrique, les notions de point simple et de point normal coïncident.

4. Normalisation des variétés.

Complément : On peut apporter à l'énoncé du lemme de normalisation de E . Noether donné au Chap. I (n°4 , p. 4) la précision suivante : dans le cas où l'extension $k(x_1,\dots, x_n)/k$ est séparable, les coefficients a_{ij} peuvent être choisis tels que chacun des x_i soit algébrique séparable sur $k(y)$. En effet, il suffit de montrer qu'on peut, dans la construction récurrente utilisée, imposer aux coefficients b_j choisis, outre la condition

$$(3) \quad F_o(-b_1 ,\dots, -b_d , 1) \neq 0$$

(Cf. Chap. I , n° 4 , p. 5), la condition suivante

$$(4) \quad -\sum_j b_j \frac{\partial F}{\partial Y_j} (y'_1 ,\dots, y'_d , x_n) + \frac{\partial F}{\partial X} (y'_1 ,\dots, y'_d , x_n) \neq 0 .$$

Or on peut supposer que x_n est algébrique séparable sur $k(x_1,\dots, x_{n-1})$; compte tenu de l'hypothèse de récurrence, x_n est alors algébrique séparable sur $k(y'_1,\dots, y'_d)$, et on a donc $\frac{\partial F}{\partial X}(y'_1 ,\dots, y'_d , x_n) \neq 0$. Le premier membre de (4) n'est donc pas identiquement nul ; comme le corps Ω est infini, il est possible de choisir $b_1,\dots, b_n$ de façon que (3) et (4) soient vérifiées simultanément.

Lemme. Soient k un corps, et soit k' une extension séparable de k . Soit V une variété définie sur k . Si V est k-normale, V est k'-normale.

Démonstration. Notons x un point générique de V sur k' . Les extensions k' et $k(x)$ de k sont alors algébriquement disjointes, donc linéairement disjointes. Par récurrence transfinie, il suffit d'examiner les deux cas suivants :

a) - $k' = k(u)$, où u est transcendant sur k . Soit $y \in k'(x)$, entier sur l'anneau $A' = k'[x]$. On a $y = f(u)/g(u)$, où f et g sont des polynômes à coefficients dans K ; on peut supposer que f , g sont premiers entre eux, et que g est unitaire. Montrons d'abord

.../...

que g est à coefficients dans k. En effet, k est algébriquement fermé dans $k(x)$ (Chap. 0, C, n° 7, th. 19). Donc si certains des coefficients de g n'appartiennent pas à k, l'une des racines t de g est transcendante sur k. On peut alors trouver une place ρ de $K' = k'(x)$, induisant l'identité sur $K = k(x)$, et telle que $\rho(u) = t$. Comme t n'est pas racine de f, on a $\rho(f(u)) \neq 0$, d'où $\rho(y) = \infty$, ce qui est contradictoire. Donc on a bien $g(u) \in k[u]$ Montrons maintenant que les coefficients de f sont dans l'anneau $A = k[x]$. En effet, posons $f(u) = a_o u^n + \ldots + a_n$, et supposons qu'il existe un i tel que $a_i \notin A$. Comme A est intégralement clos, on peut trouver une place ρ_o de K finie sur A, telle que $\rho_o(a_i) = \infty$; plus précisément, il existe un i_o tel qu'on ait $\rho_o(a_{i_o}) = \infty$, et $\rho_o(a_i/a_{i_o}) \neq \infty$ pour tout i. Supposons que ρ_o prend ses valeurs dans un corps k_o. Comme u est transcendant sur K, on peut prolonger ρ_o à une place ρ_1 de $K(u) = k'(x)$, telle que $u_1 = \rho_1(u)$ soit transcendant sur k_o. Cette place ρ_1 est alors finie sur l'anneau A', mais on a $\rho_1(y) = \infty$, d'où contradiction. On a donc $f \in A[u]$, d'où $y \in A'$.

b) - k' est algébrique séparable de degré fini sur k. Introduisons une base $w_1, \ldots, w_n$ de l'extension k'/k. L'extension $k'(x)/k(x)$ admet alors également pour base $w_1, \ldots, w_n$ (Chap. 0, C, n° 4, th. 9). Soit $y \in k'(x)$, entier sur l'anneau $A' = k'[x]$. On a $y = \sum_{i=1}^n a_i w_i$, avec $a_i \in k(x)$ pour tout i. Pour tout $k(x)$-isomorphisme σ de $k'(x)$ sur l'un de ses conjugués, on a aussi $y^\sigma = \sum_i a_i w_i^\sigma$. Comme l'extension k'/k est séparable, le déterminant de la matrice w_i^σ est un élément non nul de k'. Comme les conjugués y^σ de y sont tous entiers sur l'anneau $\bar{k}[x]$, il en est de même de chacun des coefficients a_i. Or ceux-ci appartiennent

.../...

à $k(x)$; ils sont donc entiers sur A ; comme A est intégralement clos, ils appartiennent à A, et on a donc $y \in A'$, c.q.f.d.

Corollaire. Soit V une variété définie sur un corps parfait k. Pour que V soit normale, il faut et il suffit qu'elle soit k-normale.

THEOREME 5. (Normalisation des variétés affines).

Soit V une variété affine définie sur un corps k. Il existe une variété affine V^* k-normale et un k-morphisme birationnel $\lambda : V^* \to V$ tel que l'anneau de coordonnées $\mathcal{A}_k(V^*)$ soit entier sur $\mathcal{A}_k(V)$.

Remarque 1. Comme $\mathcal{A}_k(V^*)$ a même corps des fractions que $\mathcal{A}_k(V)$, l'énoncé précédent implique que $\mathcal{A}_k(V^*)$ est la clôture intégrale de $\mathcal{A}_k(V)$; en particulier, $\mathcal{A}_k(V^*)$ est déterminé, à un k-isomorphisme près, par la donnée de V. Le couple (V^*, λ) est donc uniquement déterminé, à un k-isomorphisme près, par la donnée de V. En d'autres termes, pour tout autre couple $(\overline{V}^*, \overline{\lambda})$ vérifiant les conditions du théorème, on peut compléter le diagramme

$$\begin{tikzcd} V^* \arrow[rr, "\lambda"] \arrow[dr, dashed, "\alpha"'] & & V \\ & \overline{V}^* \arrow[ur, "\overline{\lambda}"'] & \end{tikzcd}$$

par un k-isomorphisme $\alpha : V^* \to \overline{V}^*$. Nous dirons que le couple (V^*, λ) est un modèle k-normal canonique de V.

Remarque 2. Une variété V étant donnée, on peut trouver un corps k parfait sur lequel elle est définie. La variété V^* correspondante, étant k-normale, est normale, en vertu du corollaire du lemme précédent. Donc toute variété affine V admet un modèle normal (V^*, λ), uniquement déterminé à un isomorphisme près par la donnée de V. Nous dirons que c'est un modèle normal canonique de V.

Démonstration du th. 5. Soit x un point générique de V sur k, de coordonnées $(x_1, \ldots, x_n)$. Posons $r = \dim V$. D'après le lemme de

.../...

normalisation, complèté par la remarque précédente (début de ce n°), il existe des éléments $y_1, \dots, y_r$ de $k[x_1, \dots, x_n]$ tels que les x_i soient entiers séparables sur $k[y_1, \dots, y_r]$. L'anneau $k[y_1, \dots, y_r]$ étant isomorphe à un anneau de polynômes (donc factoriel) est intégralement clos. Donc (Chap. 0, B, th. 3), sa fermeture intégrale B dans $k(x_1, \dots, x_n)$ est un A-module de type fini, i.e. de la forme $B = Az_1 + \dots + Az_s$, avec $z_1, \dots, z_s \in B$. Notons x^* le point de l'espace affine S_{n+s} ayant pour coordonnées $x_1, \dots, x_n$, $z_1, \dots, z_s$, et V^* le lieu de ce point sur k . Il est clair qu'on a $k(x^*) = k(x)$ et que l'application $\lambda : V^* \to V$ définie en posant $\lambda(x^*) = x$ est un k-morphisme. D'autre part, l'anneau de coordonnées $\mathcal{O}_k(V^*) = k[x_1, \dots, x_n, z_1, \dots, z_s]$ contient B , et est entier sur B , donc est égal à B .

<u>THEOREME 6</u>.

Soient V et W deux variétés affines, et soit $\phi : V \to W$ une application rationnelle. Soit k un corps de définition de V , W et ϕ . Soient (V^*, λ) et (W^*, μ) des modèles k-normaux canoniques de V et W respectivement. Soit $\phi^* : V^* \to W^*$ l'application rationnelle transposée de ϕ , i.e. définie par $\phi^* = \mu^{-1} \circ \phi \circ \lambda$. Soit a^* un point de V^*, et soit $a = \lambda(a^*)$ son image dans V . Alors, si ϕ est morphique en a , ϕ^* est morphique en a^* .

<u>Démonstration</u>. Soit x un point générique de V sur k . Posons $y = \phi(x)$, $x^* = \lambda^{-1}(x)$, et $y^* = \mu^{-1}(y) = \phi^*(x^*)$. On a $k(x) = k(x^*) \supset k(y) = k(y^*)$. On a d'autre part avec $b = \Phi(a)$ $\mathcal{O}_k(W) \subset \underline{o}_k(b, W) \subset \underline{o}(a, V) \subset \underline{o}(a^*, V^*)$. Les coordonnées de y^* sont entières sur $\mathcal{O}_k(W)$, donc aussi sur $\underline{o}_k(a^*, V^*)$; donc elles appartiennent à ce dernier anneau, qui est intégralement clos.

<u>THEOREME 7</u>. (Normalisation des variétés quelconques).

Soit V une variété (abstraite) définie sur un corps k . Il

.../...

existe une variété V^* k-normale, définie sur k, et un morphisme birationnel $\lambda : V^* \to V$ vérifiant la condition suivante :

(*) - Pour tout k-ouvert affine U de V, l'image inverse $U^* = \lambda^{-1}(U)$ est un ouvert affine de V^*, et l'anneau de coordonnées $\mathcal{O}_k(U^*)$ est la clôture intégrale de $\mathcal{O}_k(U)$ (i.e. U^* est un modèle k-normal canonique de U).

Remarque 3. L'unicité du modèle k-normal canonique d'une variété affine implique encore l'unicité du couple (V^*,λ) à un k-isomorphisme près. Nous dirons encore que (V^*,λ) est un modèle k-normal canonique de V. Si, pour V donnée, on choisit k parfait, la variété V^*, étant k-normale, est normale. Donc toute variété abstraite V admet un modèle normal (V^*,λ) unique à un isomorphisme près, et que nous appellerons encore modèle normal canonique de V.

Démonstration du th. 6. En effet, soit $\{U_\alpha\}$ un recouvrement de V par des k-ouverts affines et, pour tout α, soit $(U^*_\alpha, \lambda_\alpha)$ un modèle k-normal canonique de U_α. Pour tout couple (α,β) d'après le th. 6, l'application birationnelle $t^*_{\beta\alpha} = \lambda_\beta^{-1} \circ \lambda_\alpha : U^*_\alpha \to U^*_\beta$ est bimorphique en tout couple (x^*_α, x^*_β) appartenant à son graphe. En recollant les variétés affines U^*_α, et les morphismes λ_α au moyen des $t^*_{\beta\alpha}$, on définit un modèle (V^*,λ) de V vérifiant les conditions voulues.

THEOREME 7.

Soit V une variété définie sur un corps k, et soit (V^*, λ) un modèle k-normal canonique de V. Pour tout $a \in V$, l'ensemble des valeurs $(\lambda^{-1})_e(a)$ de λ^{-1} en a est un sous-ensemble fini non vide de V. Pour que λ^{-1} soit morphique en a, il faut et il suffit que a soit normal sur V.

Démonstration. On se ramène au cas où V est une variété affine.

.../...

Reprenons alors les notations de la démonstration du th. 5 . Soit ρ une place du corps $k(x) = k(x^*)$, induisant l'identité sur k ,et telle que $\rho(x) = a$. Alors ρ est finie sur l'anneau local $\underline{o}_k(a,V)$, donc sur l'anneau $\mathfrak{O}_k(V)$, donc aussi sur $\mathfrak{O}_k(V^*)$, puisque ce dernier anneau est entier sur $\mathfrak{O}_k(V)$. Donc le symbole $\rho(x^*)$ a un sens, et $a^* = \rho(x^*)$ est un point de V^*. Comme on a $x = \lambda(x^*)$, on a aussi $a = \lambda(a^*)$, d'où $a^* \in (\lambda^{-1})_e(a)$. De plus, tout élément $u^* = f(x^*)$ $\in k[x^*] = k[x_1^*,\ldots, x_n^*]$ est entier sur l'anneau $\underline{o}_k(a,V)$, autrement dit vérifie une équation $(u^*)^m + (u^*)^{m-1} g_1(x) +\ldots+ g_n(x) = 0$, où les g_i sont des polynômes à coefficients dans k . Par application de ρ , on en déduit

$$(5) \quad z^m + z^{m-1} g_1(a) +\ldots+ g_n(a) = 0 ,$$

en posant $z = \rho(u^*) = f(a^*)$. Donc, pour a et f donnés, $z = f(a^*)$ ne peut prendre qu'un nombre fini de valeurs, à savoir les racines de (5), regardée comme équation en z . On peut, en particulier, prendre pour f l'une quelconque des fonctions coordonnées ; on voit ainsi que, pour a donné, le point a^* ne peut occuper qu'un nombre fini de positions. Autrement dit, $(\lambda^{-1})_e(a)$ est fini.

Si λ^{-1} est morphique en a , on a $\underline{o}_k(a,V) = \underline{o}_k(a^*,V^*)$, donc a est normal sur V . Réciproquement, supposons a normal sur V , et soit $a^* \in (\lambda^{-1})_e(a)$. Les coordonnées de x^* sont entières sur $\mathfrak{O}(V)$, donc sur $\underline{o}(a,V)$. Donc elles appartiennent à $\underline{o}(a,V)$, i.e. λ^{-1} est morphique en a c.q.f.d.

<u>Remarque</u>. Le raisonnement précédent montre que toute place ρ de Ω finie en x est finie en x^*. Ceci entraîne en particulier que, si V est <u>complète</u>, V^* est également <u>complète</u>.

<u>Corollaire</u>. Soit V une variété définie sur un corps k . L'ensemble des points k-normaux (resp. normaux) de V est un k-ouvert (resp. un ouvert) de V .

En effet, si (V^*,λ) est un modèle k-normal de V , l'ensemble des points k-normaux de V coïncide avec l'ensemble des points

.../...

en lesquels λ^{-1} est morphique. Il suffit alors d'appliquer le th. 9 du n° 11 du Chap. I . L'assertion concernant les points normaux se ramène à celle concernant les points k-normaux, en choisissant pour k un corps de définition parfait de V .

5. Critère pour qu'une fonction soit morphique en un point.

THEOREME 8.

Soit V une variété. Soient f une fonction sur V , et a un point normal de V . Alors les propriétés suivantes sont équivalentes

(a) - f est morphique en a

(b) - $\infty \notin f_e(a)$

(c) - $a \notin \mathrm{supp}(\mathfrak{X}(f)^-)$

Démonstration.

(a) $\Longrightarrow$ (b). En effet, il est clair que

(b) $\Longrightarrow$ (a). Inversement, si $\infty \notin f_e(a)$, on a $f_e(a) \neq \mathbb{P}_1$. Donc l'ensemble $f_e(a)$ est fini. Donc (chap. IV, n° 2, th. 3) f est définie en a , et nécessairement de valeur $\neq \infty$. Donc f est morphique en a .

(b) $\Longrightarrow$ (c). Supposons $a \in \mathrm{supp}(\mathfrak{X}(f)^-)$. Alors il existe une composante W de $\mathfrak{X}(f)^-$ contenant a . On a $\omega_W(f^{-1}) > 0$, d'où $f^{-1} \in \underline{m}(W,V)$. Donc, si k est un corps de définition de V et W , et si y est un point générique de W sur k , f est définie en y , de valeur ∞ . On a donc $(y,\infty) \in \Gamma_{f^*}$ (où f^* a la signification introduite au n° 2 de ce chapitre). On a donc aussi $(a,\infty) \in \Gamma_{f^*}$, i.e. $\infty \in f_e(a)$.

(c) $\Longrightarrow$ (b). On peut supposer V affine ($V \subset \mathbb{S}_n$). Soit $a \in V$, tel q ait $\infty \in f_e(a)$, i.e. $(a,\infty) \in \Gamma_{f^*}$. Soit C une composante, contenant $a \times \infty$, de l'intersection $\Gamma_{f^*} \cap (\mathbb{S}_n \times \infty)$, dans le produit $\mathbb{S}_n \times \mathbb{P}_1$. D'après le théorème de la dimension (chap. III, n° 15, th. 13), on a $\dim C \geq 2n - (n+1) = n-1$. Comme on a $\Gamma_{f^*} \subset V \times \mathbb{P}_1$, la variété C est contenue dans $V \times \infty$, i.e. est de la forme $W \times \infty$, où W

.../...

est une sous-variété de V contenant a. La fonction f^* étant distincte de la constante ∞, on ne peut avoir $W = V$. Donc W est une sous-variété de codimension 1 de V. Comme a est normal sur V, W est normale sur V, compte tenu du coroll. du th. 7 du n° précédent. Donc, compte tenu du th. 4 du n° 3, W est simple sur V. Donc f est définie sur W, nécessairement de valeur ∞. Donc on a $f^{-1} \in \underline{m}(W,V)$, i.e. $\omega_W(f) < 0$. Donc W est une composante de $\mathfrak{X}(f)^-$ contenant a

c.q.f.d.

Corollaire 1. Soient V une variété, f une fonction sur V, et a un point normal de V. Pour que f soit définie en a, il faut et il suffit qu'on ait

$$a \notin \operatorname{supp}(\mathfrak{X}(f)^-) \cap \operatorname{supp}(\mathfrak{X}(f)^+)$$

Pour que f soit inversible (morphique et non nulle) en a, il faut et il suffit qu'on ait

$$a \notin \operatorname{supp}(\mathfrak{X}(f)).$$

Corollaire 2. Soit V une variété normale complète. Toute fonction f sur V telle que $\mathfrak{X}(f) \geq 0$ est constante.

En effet, supposons f non constante. Alors, si k est un corps de définition de V et f, et si x est un point générique de V sur k, $u = f^{-1}(x)$ est transcendant sur k. Il existe un k-homomorphisme $k[u] \xrightarrow{\alpha} k$ tel que $\alpha(u) = 0$. On peut prolonger α à une place ρ de $k(x)$. Comme V est complète, le symbole $\rho(x)$ est défini, et on a $\rho(x) = a$, avec $a \in V$. Comme $\rho(f(x)) = \rho(u)^{-1} = \infty$, on a $(a,\infty) \in \Gamma_{f^*}$, donc $a \in \operatorname{supp}(\mathfrak{X}(f)^-)$, d'où $\mathfrak{X}(f^-) \neq 0$, contrairement à l'hypothèse.

THEOREME 9.

Si V est une variété sans point multiple, l'homomorphisme $D \to \mathfrak{X}(D)$ du groupe des diviseurs sur V, dans le groupe des cycles

.../...

de codimension 1 sur V est <u>bijectif</u>. Si V est <u>normale</u> il est injectif.

<u>Démonstration</u> : Supposons V sans point multiple, et soit X un cycle de codimension 1 sur V. A tout point $a \in V$, on peut (chap. III n° 14, th. 12) faire correspondre un ouvert U contenant a, et une fonction f sur V, tels qu'on ait $U \cap \mathrm{supp}(X - \mathrm{div}(f)) = \emptyset$. Considérons la famille des couples (U, f) obtenue en faisant varier a ; on peut en extraire une famille finie (U_α, f_α), telle que les U_α recouvrent V. Pour tout point $y \in U_\alpha \cap U_\beta$, on a alors $y \notin \mathrm{supp}\, \mathcal{Z}(f_\alpha/f_\beta)$, donc f_α/f_β est inversible en y (th. 8, coroll. 1). La famille (U_α, f_α) définit donc un diviseur D sur V, tel qu'on ait $\mathcal{Z}(D) = X$. Donc l'application $\mathcal{Z}$ est surjective.

Soit maintenant V normale, et supposons $\mathcal{Z}(D) = 0$. Alors, si (U,f) est l'un quelconque des couples définissant D, le diviseur $\mathcal{Z}(f)$ induit sur U le diviseur nul; donc (th. 8) f est inversible en tout point de U. On a donc $D = 0$.

<u>THEOREME 10</u>.

Soient V une variété, et Z une sous-variété <u>simple</u> (de dimension arbitraire) de V. Alors l'anneau local $\underline{o}(Z,V)$ est factoriel.

<u>Démonstration</u> : Notons $\underline{o}(Z,V)^*$ le semi-groupe multiplicatif préordonné des éléments non nuls de l'anneau $\underline{o}(Z,V)$, la relation de préor-
e étant la divisibilité. A toute fonction $f \in \underline{o}(Z,V)$, associons la contribution, dans le cycle $\mathcal{Z}(f)$, des sous-variétés de V qui contiennent Z. On définit ainsi un homomorphisme $\psi : \underline{o}(Z,V)^* \to \mathcal{G}(Z)$ (pour la structure de semi-groupe préordonné) de $\underline{o}(Z,V)^*$ dans le semi-groupe $\mathcal{G}(Z)$ composé des cycles positifs de codimension 1 de V dont toutes les composantes contiennent Z. D'après le th. 12 au Chap. III, ψ est surjectif. D'autre part, pour qu'on ait $f \in \ker \psi$, il faut

.../...

et il suffit qu'on ait $a \notin \mathrm{supp}(\mathfrak{X}(f))$, i.e. d'après le coroll. 2 du th. 8, que f soit inversible sur Z. Donc le semi-groupe ordonné $\mathfrak{U}$ des classes d'éléments de $\underline{o}(Z,V)^*$, modulo les éléments inversibles est isomorphe à $\mathcal{G}(Z)$. Or les éléments extrémaux de $\mathcal{G}(Z)$ sont les variétés W de codimension 1 de V contenant Z, et il est clair que tout élément de $\mathcal{G}(Z)$ s'exprime de façon unique comme combinaison d'éléments extrémaux. On a donc la propriété analogue pour $\mathfrak{U}$, i.e. $\underline{o}(Z,V)$ est factoriel c.q.f.d.

6. L'espace vectoriel $L(D)$. Corps de définition d'un diviseur.

Soit V une variété, et soit D un diviseur sur V. On note $L(D)$ l'ensemble des fonctions sur V telles que $\mathrm{div}(f) \geq -D$. Il est clair que $L(D)$ est un espace vectoriel sur le domaine universel. D'autre part, si V est une variété normale, et si X est un cycle de codimension 1 sur V, l'ensemble des fonctions f sur V telles qu'on ait $\mathfrak{X}(f) \geq -X$ est encore un espace vectoriel sur le domaine universel, qu'on note $L(X)$. En particulier, V étant supposée normale, si X est de la forme $\mathfrak{X}(D)$, où D est un diviseur sur V, on a $L(X) = L(D)$.

Si la variété V et le diviseur D sur V sont définis sur k, l'ensemble des fonctions f sur V, définies sur k, et appartenant à $L(D)$ est un espace vectoriel sur k, qu'on note $L_k(D)$.

Pour tout corps K contenant k, on a un homomorphisme canonique

$$\sigma : L_k(D) \otimes_k K \longrightarrow L_K(D)$$

d'espaces vectoriels sur K.

THEOREME 11.

Soient V une variété, D un diviseur sur V, k un corps de définition de V et de D. Pour tout corps K contenant k, on a l'isomorphisme

$$L_k(D) \otimes_k K = L_K(D).$$

Plus précisément, l'homomorphisme σ défini ci-dessus est un

.../...

isomorphisme.

<u>Démonstration</u>. Soit (U_α, f_α) une famille représentant D, où les U_α sont des k-ouverts de V, et les f_α des fonctions sur V, définies sur k. On peut supposer que les U_α sont affines (quitte à introduire un recouvrement ouvert affine de chacun d'eux). Pour tout α, on a alors un k-isomorphisme $\psi_\alpha : U_\alpha \to V_\alpha$, avec $V_\alpha \subset S_{n_\alpha}$.

Soit $f \in L_K(D)$. Pour tout α, la fonction sur V_α, transposée par ψ_α de $f.f_\alpha$, est morphique sur V_α, donc induite par un polynôme. Autrement dit, si x est générique de V sur K, on a

$$f(x).f_\alpha(x) = g_\alpha(x_\alpha)$$

où l'on pose $x_\alpha = \psi_\alpha(x)$, et où g_α est un polynôme. Introduisons une base $\{u_\tau\}$ de l'extension K/k. En décomposant les coefficients des g_α suivant cette base, et en regroupant les termes de même indice τ, on obtient

$$f(x). f_\alpha(x) = \sum_\tau u_\tau \, g_{\alpha\tau} \, (x_\alpha) ,$$

où les $g_{\alpha\tau}$ sont des polynômes à coefficients dans K. On a donc

$$f(x) = \sum_\tau \, u_\tau \, h_{\alpha\tau} \, (x) ,$$

en posant

$$(6) \quad h_{\alpha\tau}(x) = f_\alpha^{-1}(x) \, g_{\alpha\tau}(\psi_\alpha(x)).$$

Quels que soient α et τ, on a $h_{\alpha\tau}(x) \in k(x)$.
D'autre part, $k(x)$ et K sont algébriquement indépendants, donc linéairement indépendants sur k. Donc (Chap. O, C, n° 4, th. 9), les u_τ forment une base de $K(x)$ sur $k(x)$. Ceci implique que les $h_{\alpha\tau}$ ne dépendent pas de α, mais seulement de τ. On peut donc les désigner par h_τ. La relation (6) entraine que $g_{\alpha\tau} = h_\tau f_\alpha$ est morphique sur U_α quels que soient τ et α. Donc on a $\operatorname{div}(h_\tau) \geq -D$ i.e. $h_\tau \in L_k(D)$. Donc f appartient à l'image de σ. On a donc montré

.../...

que σ est surjectif. D'autre part, si $f = 0$, on a nécessairement $h_\tau = 0$ pour tout τ, d'où $g_{\alpha\tau} = 0$ pour tout α et tout τ, ce qui prouve que σ est injectif. Donc σ est bien un isomorphisme.

Corollaire. Soit V une variété complète, définie sur k, et soit D un diviseur sur V, défini sur k. Supposons qu'il existe une fonction f sur V, non nulle, telle que $\mathrm{div}(f) = D$. Alors, il existe une fonction f_o sur V, définie sur k, telle que $\mathrm{div}(f_o) = D$.

En effet, supposons f définie sur une extension K de k. D'après le théorème précédent, on a $L_K(-D) = L_k(D) \otimes_k K$. Comme on a $f \neq 0$, on a nécessairement $L_k(-D) \neq 0$. Soit $f_o \neq 0$, appartenant à $L_k(-D)$. Alors on a $\mathrm{div}(f_o/f) \geq 0$, donc (n° 5, th. 8), f_o/f est morphique sur V. Comme V est complète, f_o/f est constante (n° 5, th. 8, coroll. 2), et on a donc $\mathrm{div}(f_o) = \mathrm{div}(f) = D$.

Remarque : le raisonnement montre en outre que $L_k(-D)$ est de dimension 1, et admet pour générateur f_o.

THEOREME 12.

Soit V une variété complète, et soit D un diviseur sur V. Alors l'espace vectoriel $L(D)$ est de dimension finie.

Démonstration. On procède par récurrence sur $n = \dim V$. On remarque d'abord que, si (V^*, λ) est un modèle normal canonique de V, on a un homomorphisme injectif $L(D) \to L(D^*)$ obtenu par relèvement avec $D^* = \lambda^{-1}(D)$. Donc, si $L(D^*)$ est de dimension finie, il en est de même de $L(D)$. Donc si le théorème est vérifié par les variétés normales de dimension n, il l'est par toutes les variétés de dimension n. On note d'autre part que la propriété est triviale pour $n = 0$.

On peut donc supposer que V est normale, de dimension $n > 0$, et que le théorème est démontré pour une variété quelconque de dimen-

.../...

sion $\leq n-1$. On peut en outre supposer qu'on a $D \geq 0$ (sinon, on se ramène à ce cas en remarquant qu'il existe $D' \geq 0$, tel que $D' \geq D$, et qu'on a alors $L(D) \subset L(D')$). Si $X = \chi(D)$ est le cycle correspondant on a aussi $X \geq 0$. Posons $X = \sum_i m_i W_i$ $(m_i \geq 0)$, où les W_i sont des sous-variétés de codimension 1 de V . La variété V étant fixée nous allons utiliser une seconde récurrence sur l'entier $m = m(X) = \sup_i m_i$.

La propriété à démontrer ($L(D) = L(X)$ est de dimension finie) est triviale pour $m = 0$. Il suffit donc de prouver que, si X est un cycle de codimension 1 sur V , et si W est une sous-variété de codimension 1 sur V , tels qu'on ait $L(X+W) \subset L(D)$, et tels que l'espace $L(X)$ soit de dimension finie, l'espace $L(X+W)$ est aussi de dimension finie.

Or on a $L(X) \subset L(X+W)$. On peut supposer $L(X) \neq L(X+W)$ (sinon il n'y a rien à démontrer). Soit alors f_o une fonction sur V , telle qu'on ait $f_o \in L(X+W)$ et $f_o \notin L(X)$, c'est à dire $\chi(f_o) \geq -(X+W)$, et $\chi(f_o) \not\geq -X$. Alors le coefficient $\nu_o = \omega_W(f_o)$ de W dans $\chi(f_o)$ est égal au coefficient de W dans $-(X+W)$. La fonction f_o étant fixée, soit maintenant $f \in L(X+W)$ quelconque. Alors, on a $\omega_W(f/f_o) \geq 0$. Donc f est morphique sur W , et induit sur W une fonction g . Comme on a $f/f_o \in L(D+\mathrm{div}(f_o))$, on a $g \in L(E)$, où E est le diviseur sur W induit par $D + \mathrm{div}(f_o)$. Pour $f \in L(X)$, la fonction f/f_o s'annule sur W , et on a donc $g = 0$. Reciproquement, la relation $g = 0$ entraîne $\omega_W(f/f_o) > 0$, d'où $\omega_W(f) > \nu_o$ et, par suite $f \in L(X)$. On a donc une suite exacte

$$0 \longrightarrow L(X) \xrightarrow{i} L(X+W) \xrightarrow{\alpha} L(E)$$

où i est l'injection naturelle $L(X) \longrightarrow L(X+W)$, et où α est l'homomorphisme défini en posant $\alpha(f) = g$. Or on a supposé $L(X)$ de dimen-

.../...

sion finie. D'autre part, d'après l'hypothèse de récurrence sur n, $L(E)$ est aussi de dimension finie. Il en est donc de même de $L(X+W)$ c.q.f.d.

N° d'impression 361

2ème trimestre 1979