PUBLICATIONS

MATHEMATIQUES

D'ORSAY

GEOMETRIE DIOPHANTIENNE

(cours 1966-67, retirage 1981)

André NÉRON

Université de Paris-Sud

Département de Mathématique

Bât. 425

91405 ORSAY France

PUBLICATIONS

MATHEMATIQUES

D'ORSAY

GEOMETRIE DIOPHANTIENNE

(cours 1966-67, retirage 1981)

André NÉRON

Université de Paris-Sud

Département de Mathématique

Bât. 425

91405 ORSAY France

TABLE DES MATIERES

.....

CHAPITRE I

VALEURS ABSOLUES

Le cours de l'année 1964-65 : "Notions élémentaires de Géométrie algébrique" est cité E ; le cours de l'année 1965-66 "Variétés abéliennes" est cité VA .

1. Définitions, exemples.

Définition 1.1. Soit K_∞ le corps projectif associé à un corps K . On appelle valeur absolue de K toute application v de K_∞ dans $\bar{\mathbb{R}}$ vérifiant les axiomes suivants :

VA1 $v(x) = -\infty$ équivaut à $x = 0$

VA1' $v(x) = +\infty$ équivaut à $x = \infty$

VA2 $v(xy) = v(x) + v(y)$ quels que soient x , y dans K

VA3 il existe α dans $\mathbb{R}$ tel que quels que soient x , y dans K : $v(x+y) \leq \sup(v(x),v(y)) + \alpha$.

N.B. Les conventions faites ci-dessus diffèrent des conventions usuelles, d'une part par le fait qu'on choisit la notation additive, et d'autre part par la forme attribuée à l'axiome VA3 (appelé condition U_A dans Bourbaki, Algèbre, VI, § 6.1). Une valeur absolue au sens ci-dessus est le produit par une constante réelle >0 arbitraire du logarithme d'une valeur absolue au sens classique.

On posera $|x|_v = \exp v(x)$ (notation multiplicative habituelle).

Conséquences

1. Chaque fois que l'on peut donner un sens aux deux membres de VA2 (resp. VA3) avec x , y dans K_∞ compte tenu de VA1 et VA1' on a encore VA2 (resp. VA3)

.../...

2. Si ζ est racine de l'unité $v(\zeta) = 0$. En particulier $v(1) = v(-1) = 0$, d'où $v(-x) = v(x)$.

3. $\alpha \geq 0$ car $0 = v(1) \leq \sup(v(1), v(0)) + \alpha = \alpha$ si $\alpha = 0$ on dira que v est <u>ultramétrique</u>. Une valeur absolue non ultramétrique est également dite <u>archimédienne</u>.

4. v induit un homomorphisme de K^* dans $\mathbb{R}$.

<u>Exemples</u> :

1. $v(x) = 0$ pour tout x dans K^* est dite valeur absolue <u>impropre</u> ou <u>triviale</u>.

2. A toute <u>valuation</u> réelle ω de K_ω est associée une valeur absolue ultramétrique $v = -\omega$. En particulier si A est un anneau factoriel à une valuation p-adique ω_p du corps des fractions, il correspond $v_p = -\omega_p$. Inversement, toute valeur absolue ultramétrique provient d'une valuation.

3. Dans $\mathbb{R}$ ou $\mathbb{C}$, on définit une valeur absolue, notée v_∞ , en posant $v_\infty(x) = \log |x|$ (de sorte que $|x|_\infty = |x|_{v_\infty}$ est la valeur absolue usuelle $|x|$).

2. <u>Corps valués.</u>

Soit K un corps muni d'une valeur absolue v . On peut définir une topologie sur K par le système fondamental $\{V_a\}$ de voisinages de 0 $V_a = \{x \in K \ ; \ v(x) \leq a\}$.

K est alors un <u>corps topologique</u> ; on le dira <u>corps valué</u>.

<u>Définition 2.1.</u> Deux valeurs absolues sont dites <u>équivalentes</u> si elles définissent la même topologie.

En particulier, deux valeurs absolues ultramétriques sont équivalentes si les valuations correspondantes sont équivalentes (E, 0, A, 6).

.../...

THEOREME 2.1.

Soit K un corps muni de deux valeurs absolues v_1 et v_2 non impropres, les propriétés suivantes sont équivalentes :

a) v_1 et v_2 sont équivalentes

b) $v_1(x) < 0 \implies v_2(x) < 0$

c) il existe un réel $\mu > 0$ tel que $v_1 = \mu . v_2$.

$x \xrightarrow{i} a$ signifiera x tend vers a au sens de la topologie définie par v_i .

a) $\implies$ b) car $v_i(x) < 0 \iff x^n \xrightarrow{i} 0$ quand $n \to +\infty$

b) $\implies$ c) Notons v_1^* (resp. v_2^*) la restriction de v_1 (resp. v_2) à K^* ; c'est un homomorphisme de K^* sur $v_1(K^*)$ (resp. $v_2(K^*)$), sous-groupe du groupe additif $\mathbb{R}$. Or b) donne $v_2(x) = 0 \Rightarrow v_1(x) = 0$; donc $\ker v_2 \subset \ker v_1$; on peut factoriser $v_1^* = \gamma \circ v_2^*$, où γ est un homomorphisme de sous-groupe additif ordonné de $\mathbb{R}$, donc une homothétie de rapport $\mu \geq 0$; or $\mu \neq 0$ sinon v_1 serait impropre.

c) $\implies$ a) Les voisinages sont les mêmes.

LEMME 2.1. Soient a_i dans K_∞ $i = 1,2,\ldots,m$; alors

$$v(a_1+a_2+\ldots+a_m) \leq \sup_i v(a_i) + \alpha \left(\frac{\log m}{\log 2} + 1\right) .$$

Par récurrence sur r on déduit de VA3 lorsque $m = 2^r$ pour tout r $v(a_1+a_2+\ldots+a_{2^r}) \leq \sup_i v(a_i) + r\alpha$.

Si $m \neq 2^r$ pour tout r , il existe r tel que $2^{r-1} < m < 2^r$ et $r < \frac{\log m}{\log 2} + 1$; posons $a_j = 0$ pour $j = m+1 , m+2,\ldots,2^r$ on a :

$$v(a_1+a_2+\ldots+a_m) = v(a_1+a_2+\ldots+a_{2^r}) \leq \sup v(a_i) + \alpha r$$

et a fortiori l'inégalité du lemme.

.../...

THEOREME 2.2.

Soient K un corps et v une valeur absolue de K ; alors v ultramétrique équivaut à v majorée sur le sous-anneau premier de K .

Si v est ultramétrique, $\alpha = 0$ et $v(n.1) = v(1+1+\ldots+1) \leq 0$.

Réciproquement, si v est majorée par C sur $\mathbb{Z}.1$ soit

$$(a+b)^m = \sum_{i=0}^{m} \binom{m}{i} a^i b^{m-i}$$ alors, par le lemme 1,

$$m\, v(a+b) \leq \sup_i (C + iv(a) + (m-i)\, v(b)) + \alpha \left(\frac{\log(m+1)}{\log 2} + 1\right) ;$$

posant $s = \sup(v(a), v(b))$. On a

$$v(a+b) \leq s + \frac{C}{m} + \alpha \left(\frac{\log(m+1)}{m \log 2} + 1\right) .$$

En faisant tendre m vers $+\infty$, $v(a+b) \leq s$.

COROLLAIRE 1. Sur un corps de caractéristique $p > 0$ toute valeur absolue est ultramétrique

car l'anneau premier est $\mathbb{F}_p$ et n'a qu'un nombre fini d'éléments.

COROLLAIRE 2. La possibilité de prendre $\alpha \leq \log 2$ dans VA3 équivaut à $|\ |_v$ satisfait l'inégalité triangulaire.

$v(n.1) \leq \alpha\left(\frac{\log n}{\log 2} + 1\right)$, d'après le lemme 1 .

$$m\, v(a+b) \leq \sup_i \left(\alpha\left(\frac{\log \binom{m}{i}}{\log 2} + 1\right) + iv(a) + (m-i)v(b)\right) + u_m$$

avec $u_m = \alpha\left(\frac{\log m+1}{\log 2} + 1\right)$

$$|a+b|_v^m \leq \sup_i \binom{m}{i} |a|_v^i\, |b|_v^{m-i}\, e^{u_m+\alpha} \qquad \text{si} \quad \alpha < \log 2$$

et a fortiori $|a+b|_v \leq (|a|_v + |b|_v)\, e^{\frac{u_m+\alpha}{m}}$;

faisant tendre m vers $+\infty$ $|a+b|_v \leq |a|_v + |b|_v$.

Inversement $|a+b|_v \leq |a|_v + |b|_v \leq 2 \sup(|a|_v , |b|_v)$

et $v(a+b) \leq \sup(v(a), v(b)) + \text{Log } 2$.

.../...

COROLLAIRE 3. Tout corps valué est un espace métrisable avec pour distance $d(x,y) = |x-y|_v^{\mu}$, où $\mu = \frac{\log 2}{\alpha}$

ceci résulte du théorème 1 et du corollaire 2.

3. Valeurs absolues de $\mathbf{Q}$.

THEOREME 3.1.

Soit v une valeur absolue de $\mathbf{Q}$ alors :

a) ou bien v est la valeur absolue impropre de $\mathbf{Q}$

b) ou bien v est équivalente à une valeur absolue p-adique

c) ou bien v est équivalente à v_∞.

Si v est ultramétrique $\omega = -v$ est une valuation, et on a a) ou b) d'après l'étude des valuations de $\mathbf{Q}$ (E, O, A, 6, th. 5, coroll. 1).

Si v n'est pas ultramétrique soient m, n deux entiers > 1 écrivons m^s en base n.

$$m^s = a_o + a_1 n + \ldots + a_q n^q \qquad 0 \leq a_i \leq n \quad i = 1,2,\ldots q$$

$$n^q \leq m^s < n^{q+1}$$

$$v(m^s) \leq \sup(v(a_i) + iv(n)) + \alpha\left(\frac{\log(q+1)}{\log 2} + 1\right) \text{ d'après le lemme 1.}$$

Si $S = \sup(0, v(n))$, et $C = \sup_i v(a_i)$, on a

$$s\, v(m) \leq C + qS + \alpha\left(\frac{\log(q+1)}{\log 2} + 1\right).$$

Or $q < \frac{\log m}{\log n} s$ donc $v(m) \leq \frac{C}{s} + \frac{\log m}{\log n} S + \alpha\left(\frac{\log\left(s\frac{\log m}{\log n}+1\right)}{s \log 2} + \frac{1}{s}\right)$.

Faisons tendre s vers $+\infty$

$$v(m) \leq \frac{\log m}{\log n} S$$

si $v(n) < 0 \Longrightarrow v(m) \leq 0$ donc v serait ultramétrique (Th.2.2.)

d'où $S = v(n)$, échangeant n et m on déduit

$$\frac{v(m)}{\log m} = \frac{v(n)}{\log n} \quad \text{donc } v \text{ est équivalente à } v_\infty .$$

.../...

4. Théorème d'approximation.

(p,q) désigne l'ensemble des entiers $n : p \leq n \leq q$

THEOREME D'APPROXIMATION.

Soient v_i , $i \in (1,m)$ des valeurs absolues non impropres et deux à deux non équivalentes sur un même corps K . Soient a_i , $i \in (1,m)$ des éléments de K et α réel. Il existe alors $x \in K$ tel que

$$v_i(x-a_i) < \alpha \quad \text{pour tout} \quad i \in (1,m)$$

Il suffit de trouver une suite $x_n = x_{1,n}\, a_1 + x_{2,n}\, a_2 + \ldots + \ldots + x_{m,n}\, a_m$, avec $x_{i,n} \xrightarrow{j} \delta_{i,j}$ quand $n \to +\infty$; alors, pour n assez grand, prenant $x = x_n \Longrightarrow v_i(x-a_i) < \alpha$.

Pour construire $(x_{1,n})$ nous allons prouver par récurrence sur m qu'il existe $y \in K$ tel que $v_1(y) > 0$, $v_j(y) < 0$ pour $j \in (2,m)$.

a) $m = 2$ v_1 , v_m sont non équivalentes ; or d'après le th.21. b) il existe y', y'' tels que $v_1(y') \geq 0$, $v_2(y') < 0$, $v_1(y'') > 0$ et $v_2(y'') \leq 0$ il suffit alors de prendre $y = y'.y''$.

b) Il existe t tel que $v_1(t) > 0$ $v_j(t) < 0$ pour $j \in (2,m-1)$ mais aussi u tel que $v_1(u) > 0$, $v_m(u) < 0$

α) si $v_m(t) \leq 0$ posons $y_n = t^n u$ quand $n \to +\infty$ $y_n \xrightarrow{1} \infty$, $y_n \xrightarrow{j} 0$ si $j \in (2,m-1)$ et $v_m(y_n) < 0$ donc pour n assez grand $y = y_n$ convient.

β) si $v_m(t) > 0$ posons $y_n = u \dfrac{t^n}{1+t^n} = \dfrac{u}{1+t^{-n}}$ quand $n \to +\infty$ $y_n \xrightarrow{1} u$, $y_n \xrightarrow{m} u$, $y_n \xrightarrow{j} 0$ si $j \in (2,m-1)$ donc pour n assez grand $y = y_n$ convient.

c) Il suffit de prendre $x_{1,n} = \dfrac{y^n}{1+y^n}$.

.../...

En recommençant cette construction pour chaque indice $i \in (1,m)$ on obtient la suite x_n convenable.

COROLLAIRE. Dans les hypothèses du théorème précédent, si l'on suppose que v_j , $j \in (1,q)$ $q \leq m$ sont ultramétriques, et si l'on se donne $\gamma_j \in v_j(K^*)$ $j \in (1,q)$, alors il existe $x \in K$ tel que

$$v(x-a_j) = \gamma_j \quad \text{pour} \quad j \in (1,q)$$

et $$v(x-a_i) < \alpha \quad \text{pour} \quad i \in (q+1,m).$$

Soient u_j tels que $\gamma_j = v(u_j)$ $j \in (1,q)$ posons

$$b_j = a_j + u_j \qquad j \in (1,q)$$

$$b_i = a_i \qquad i \in (q+1,m).$$

Appliquons le théorème d'approximation avec (b_j) $j \in (1,m)$ et $\beta < \mathrm{Inf}(\alpha,\gamma_1,\gamma_2,\ldots,\gamma_q)$ il existe x tel que : $v(x-b_j) < \beta < \alpha$ or $v(x-b_j) = v(x-a_j-u_j) = v(u_j) = \gamma_j$, si $j \in (1,q)$, puisque :

$$v(x-b_j) < \beta < \gamma_j = v(u_j) \quad \text{et que} \quad -v \quad \text{est une valuation.}$$

4. Complétion d'un corps valué.

THEOREME 4.1.

Soit K un corps valué. Il existe un couple $(\hat{K},\varphi)$, où $\hat{K}$ est un corps topologique complet et φ un monomorphisme de K dans $\hat{K}$ pour la structure de corps topologique, tel que pour tout autre couple $(\hat{K}',\varphi')$ analogue, φ' se factorise à travers φ par un monomorphisme $\alpha : \hat{K} \longrightarrow \hat{K}'$ pour la même structure. L'image $\varphi(K)$ est alors partout dense dans $\hat{K}$. En prolongeant par continuité la valeur absolue v de K , on obtient une valeur absolue $\hat{v}$ de $\hat{K}$ compatible avec sa topologie (de sorte que $\hat{K}$ est un corps valué complet pour $\hat{v}$).

Pour construire $(\hat{K},\varphi)$, il suffit de compléter K comme

.../...

espace métrique.

Le théorème entraîne l'unicité de $(\hat{K},\hat{v})$ à un isomorphisme près pour la structure de corps valué.

Définition 4.1. Le corps valué $(\hat{K},\hat{v})$ du théorème précédent est appelé le complété de K relativement à v.

Dans la suite, on regardera K comme un sous-corps de $\hat{K}$, en l'identifiant canoniquement à son image par φ.

Remarque : On obtient une définition équivalente à la précédente en remplaçant, dans l'énoncé du th. 4.1. l'exigence de la condition d'application universelle pour les couples $(\hat{K},\varphi)$ par celle de la propriété pour $\varphi(K)$ d'être partout dense dans $\hat{K}$

Propriétés : Si v est ultramétrique soit $\omega = -v$ la valuation réelle associée à v alors :

a) $\hat{v}$ est ultramétrique, i.e. $\hat{\omega} = -\hat{v}$ est une valuation réelle de K.

b) L'anneau de valuation $\hat{A}$ de $\hat{\omega}$ s'identifie au complété de l'anneau de valuation A de ω, en tant que sous-anneau topologique de K. Son idéal maximal $\hat{\underline{m}}$ est engendré par l'idéal maximal $\underline{m}$ de A. On a : $A = \hat{A} \cap K$ et $\underline{m} = \hat{\underline{m}} \cap A = \hat{\underline{m}} \cap K$.

c) Introduisons les corps résiduels $A/\underline{m} = K^o$ et $\hat{A}/\hat{\underline{m}} = \hat{K}^o$ alors K^o s'identifie canoniquement à $\hat{K}^o$.

d) $\hat{A} = A + \hat{\underline{m}}$

e) Si $\Gamma = \Gamma_\omega = \omega(K^*)$ est le groupe de la valuation ω et $\hat{\Gamma} = \Gamma_{\hat{\omega}}$ alors $\Gamma = \hat{\Gamma}$.

Démonstrations.

a) $\hat{v}$ coïncide avec v sur l'anneau premier ; on applique le th. 2.2.

b) $\hat{\omega}$ prolonge ω

.../...

c) le diagramme $\begin{array}{ccc} A & \longrightarrow & K^o \\ \downarrow & & \vdots \\ \hat{A} & \longrightarrow & \hat{K}^o \end{array}$ se complète en une injection de K^o dans $\hat{K}^o$ car $\hat{\underline{m}} \cap A = \underline{m}$. Cette injection est une bijection car $\hat{A} = A + \hat{\underline{m}}$ d'après :

d) A est dense dans $\hat{A}$ donc : pour tout $x \in \hat{A}$, il existe $a \in A$ tel que $\hat{v}(x-a) < 0$ ce qui équivaut à $x-a \in \hat{\underline{m}}$.

e) si $\gamma = \hat{\omega}(x)$ d'après la densité, il existe $y \in K^*$ tel que $\omega(x-y) > \gamma$ donc $\omega(y) = \gamma$.

Propriétés : Si ω est discrète, toute uniformisante t de ω est uniformisante de $\hat{\omega}$; et si R est un système de représentants de $A/\underline{m}$ dans A, alors tout x dans $\hat{K}$ s'écrira $\sum_{n \geq s} a_n t^n$ où $s \in \mathbb{Z}$ et $a_n \in R$. Si les éléments de R sont distincts modulo $\underline{m}$ cette écriture est unique.

Soit d'abord $x \in \hat{A}$; comme $\hat{A} = A + t\hat{A}$, on a :

$$x = a_o + x_1 t$$
$$x_1 = a_1 + x_2 t$$
$$\cdots\cdots\cdots\cdots$$
$$x_{n-1} = a_{n-1} + x_n t$$

avec $a_i \in R$ et $x_i \in \hat{A}$, d'où : $x = a_o + a_1 t + \ldots + a_{n-1} t^{n-1} + x_n t^n$. Il suffit alors de faire tendre n vers $+\infty$. Si maintenant $x \in \hat{K}$, on remarque qu'il existe s tel que $t^s . x \in \hat{A}$.

Exemples :

a) Soient A un anneau factoriel, K son corps des fractions, p un élément extrémal de A. Les complétés respectifs $\hat{K}_p$ et $\hat{A}_p$ de K et A relativement à la valuation p-adique ω_p sont appelés complétés p-adiques de K et A.

En particulier, en prenant $A = \mathbb{Z}$, d'où $K = \mathbb{Q}$, et $p \in \mathbb{Z}$ premier, on obtient le corps $\mathbb{Q}_p$ des nombres p-adiques, et l'anneau $\mathbb{Z}_p$ des entiers p-adiques. On peut alors prendre

.../...

$t = p$, et $R = \{0,1,\ldots,p-1\}$.

b) Soient V une courbe algébrique définie sur un corps k , et soit a un point de V rationnel sur k . On a vu (VA, II, 5) que l'anneau local $\underline{o} = \underline{o}_k(a,V)$ du point a est un anneau de valuation discrète admettant pour corps résiduel k . On peut, dans ce cas, prendre $R = k$, et le complété $\hat{\underline{o}}$ de $\underline{o}$ est isomorphe (non canoniquement) à l'anneau des séries formelles à coefficients dans k .

Plus généralement, si W est une sous-variété de codimension 1 de V , définie sur k , simple sur V , l'anneau local $\underline{o} = \underline{o}_k(W,V)$ est un anneau de valuation discrète (E, III, 10, th. 10) admettant pour corps résiduel le corps $\mathcal{F}_k(W)$ des fonctions sur W définies sur k . Le complété $\hat{\underline{o}}$ de $\underline{o}$ est isomorphe à l'anneau de séries formelles à coefficients dans $\mathcal{F}_k(W)$.

5. Extensions des valuations réelles et des valeurs absolues.

Dans ce qui suit K' désigne une extension d'un corps K , ω' une valuation réelle de K' dont la restriction à K est ω . $A = A_\omega$; $A' = A_{\omega'}$, $\underline{m} = \underline{m}_\omega$; $\underline{m}' = \underline{m}'_\omega$;

$K^o = A/\underline{m}$; $K'^o = A'/\underline{m}'$; $\Gamma = \omega(K^*)$; $\Gamma' = \omega'(K'^*)$

$v = -\omega$; $v' = -\omega'$.

Le diagramme $\begin{array}{ccc} A & \longrightarrow & K^o \\ \downarrow & & \downarrow \\ A' & \longrightarrow & K'^o \end{array}$ se complète en une injection $K^o \longrightarrow K'^o$ car $A = A' \cap K$ et $\underline{m} = \underline{m}' \cap K$

donc K'^o peut être considéré comme une extension de K^o .

Définition 5.1. On appelle indice de ramification de l'extension (K',ω') de (K,ω) l'indice $(\Gamma' : \Gamma) = e$.

Définition 5.2. On appelle degré résiduel de l'extension (K',ω') de (K,ω) le degré $[K'^o : K^o] = f$.

.../...

Propriétés : Soit (K'',ω'') une extension de (K',ω') ; désignons par e' et f', l'indice de ramification et le degré résiduel de cette extension, par e'' et f'' le degré résiduel et l'indice de ramification de l'extension (K'',v'') de (K,v) ; alors $e'' = e'e$ et $f'' = f'f$.

THEOREME 5.1.

Si $[K' : K] = n < +\infty$ alors e, f sont finis et $ef \leq n$

Soient $r \leq e$ et $s \leq f$; il existe des éléments (x_i), $i \in (1,r)$, dans K'^* tels que $(\omega(x_i))$ soient distincts mod Γ et des (y_j), $j \in (1,s)$ dans A' tels que leurs images (y_j°) dans K'° soient linéairement indépendantes sur K° ; donc les $y_j \in A' - \underline{m}$ et sont inversibles. Il suffit de prouver $rs \leq n$ et, pour cela, que les $x_i y_j$ sont linéairement indépendants sur K. Soient (b_j), $j \in (1,s)$ dans A non tous nuls alors : $\omega'(\sum_j b_j y_j) = \inf_j(\omega(b_j)) \in \Gamma$; en effet après multiplication par un élément de K^* on se ramène au cas où $\inf(\omega(b_j)) = 0$, c'est-à-dire b_j entier pour tout j et l'un deux inversible dans A ; comme les y_j sont indépendants, on a : $\sum_j b_j^\circ y_j^\circ \neq 0$ et par conséquent $\omega'(\sum_j b_j y_j) = 0$. Supposons $\sum_{i,j} a_{i,j} x_i y_j = 0$, avec $a_{i,j} \in K$ non tous nuls ; posons $u_i = \sum_j a_{i,j} y_j$. D'après ce qui précède les u_i sont non tous nuls et pour $u_i \neq 0$, on a $\omega'(u_i) \in \Gamma$. Or les $\omega'(x_i)$ sont distincts mod Γ. Donc il en est de même des $\omega'(u_i x_i)$ pour les $u_i \neq 0$. Ceci est contradictoire, compte tenu de la relation $\sum_i u_i x_i = 0$.

Remarque : On peut montrer que, pour plusieurs valuations $(\omega_i)_{i \in I}$ deux à deux indépendantes de K' prolongeant ω, on a : $\sum_i e_i f_i \leq n$.

.../...

THEOREME 5.2.

Si $[K' : K] = n < +\infty$ alors ω impropre (resp. de rang 1, resp. discrète) équivaut à ω' impropre (resp. de rang 1, resp. discrète).

$(\Gamma' : \Gamma) = e < +\infty$; donc l'homomorphisme $\alpha : x \longmapsto ex$ de Γ' dans Γ est surjectif ; de plus, $\ker \alpha = \{0\}$, car Γ' est un groupe ordonné ; donc α est un isomorphisme de groupe ordonné.

THEOREME 5.3.

Soient (K,v) un corps valué et L une extension de K ; on peut prolonger v à une valeur absolue de L.

Si v est archimédienne, on peut, d'après le théorème d'Ostrowski, identifier par isomorphisme K à un sous corps de $\mathbb{C}$, de façon que v soit (à l'équivalence près) induite par la valeur absolue ordinaire de $\mathbb{C}$. Comme $\mathbb{C}$ est algébriquement clos, on peut supposer $L \subset \mathbb{C}$.

Si v est ultramétrique, la valuation réelle associée $\omega = -v$ est de rang 1, elle se prolonge à une valuation de L (E, O, A, 8, th. 7, coroll.) qui est de rang 1, donc que l'on peut supposer réelle ; son opposée est une valeur absolue sur L prolongeant v.

THEOREME 5.4.

Soient (K,v) un corps valué complet, et L une extension algébrique de K. Il existe une et une seule valeur absolue de L prolongeant v. De plus, si $[L : K] = n < +\infty$, alors L muni de cette valeur absolue est un corps valué complet.

.../...

On peut supposer $[L : K] = n < +\infty$.

Si K est muni de la topologie discrète, sa valeur absolue est triviale, auquel cas L est lui-même valué trivialement (th. 5.2.) muni de la topologie discrète, il est complet.

Si K est muni d'une topologie non discrète, L, étant un espace vectoriel de dimension finie sur ce corps valué complet, est isomorphe à K^n comme espace vectoriel topologique. Donc L est complet et deux valeurs absolues quelconques w , w' de L prolongeant v sont équivalentes, d'où $w = \mu w'$ d'après c) du th. 2.1. ; comme v n'est pas triviale, on peut prendre $x \in K^*$ tel que $v(x) \neq 0$, d'où $\mu = 1$.

COROLLAIRE 1. Soient (K,v) un corps valué complet, L et L' deux extensions conjuguées de K , i.e. telles qu'il existe un K-isomorphisme σ de L sur L' . Soient w et w' les prolongements (uniques) de v à L et L' respectivement. Alors $w = w' \circ \sigma$.

COROLLAIRE 2. Les hypothèses étant celles du th. 5.4., si $[L : K] = n < +\infty$, pour tout $y \in L$, $w(y) = \frac{1}{n} v(N_{L/K}(y))$.

On a $N_{L/K}(y) = \prod_{i=1}^{n} y_i$, où les y_i sont les conjugués de y répétés un nombre de fois égal au degré d'inséparabilité de L sur K . Quitte à agrandir L on peut la supposer quasi-galoisienne alors :

$$v(N_{L/K}(y)) = \sum_{i=1}^{n} w'(y_i) = n\, w(y).$$

Définition 5.3. Soient (K,v) un corps valué, L une extension finie de K , w une valeur absolue de L prolongeant v , $\hat{K}$ et $\hat{L}$ leurs complétés respectifs. L étant identifié à un sous-corps de $\hat{L}$, le corps $\hat{K}$ s'identifie à l'adhérence de K dans $\hat{L}$, et on a $\hat{L} = \hat{K}.L$. On appelle degré local de

.../...

L sur K par rapport à w : $n_w = [\hat{L} : \hat{K}]$.

THEOREME 5.5.

Soit K un corps muni d'une valeur absolue v , L une extension de K , $[L : K] = n < +\infty$; alors il existe seulement un nombre fini de valeurs absolues $(v_i)_{i\in I}$ prolongements à L de v , et $\sum_{i\in I} n_i \leq n$, avec $n_i = n_{v_i}$. Si l'extension est séparable on a l'égalité.

On peut supposer $L = K(z)$ car dans la situation :

$K \subset K' \subset K''$
$v \quad v_i \quad v_{ij}$

$n(v_{ij}/v) = n(v_{ij}/v_i).n(v_i/v)$ si $\sum_i n(v_i/v) \leq n(K'/K)$ et $\sum_j n(v_{ij}/v_i) \leq n(K''/K')$ alors :

$$\sum_{ij} n(v_{ij}/v) = \sum_i n(v_i/v) \sum_j n(v_{ij}/v_i) \leq n(K'/K).n(K''/K) = n(K''/K).$$

Soit P le polynôme irréductible de z sur K ; il se factorise sur $\hat{K}$ en $P = P_1 P_2 \ldots P_r$. Introduisons $\hat{K}_a$ la clôture algébrique de $\hat{K}$ et z_j une racine de P_j ; $\hat{L}_j' = \hat{K}(z_j)$ est un corps valué complet pour une valeur absolue unique w_j prolongeant celle de $\hat{K}$; soit σ la restriction à $K(z)$ du $\hat{K}$-isomorphisme $\hat{K}(z) \longrightarrow \hat{K}(z_j)$; $w_j \circ \sigma$ est une valeur absolue v_i de L indépendante de la racine de P_j choisie, d'où une application $\varphi : j \longmapsto i$ de $(1,r)$ dans I .

Inversement, soit w une valeur absolue quelconque de L prolongeant v , et soit $\hat{L}$ le complété correspondant. Alors $\hat{K}$ est isomorphe à un sous-corps de $\hat{L}$, et on a $\hat{L} = \hat{K}(z)$. Il existe donc un $\hat{K}$-isomorphisme ρ de $\hat{L}$ sur un sous-corps $\hat{L}'$ de $\hat{K}_a$. L'image $\sigma(z)$ est une racine z_j de P , donc de

.../...

l'un des facteurs P_j . On a nécessairement $\hat{L}' = \hat{K}(z_j) = \hat{L}'_j$, et $w = v_{\varphi(j)}$. Donc φ est surjective.

Comme $\deg P_j = n_{\varphi(j)}$, on a $n = \sum_{j=1}^{r} n_{\varphi(j)} \geq \sum_{i\in I} n_i$; donc I est fini, et l'égalité a lieu si et seulement si φ est bijective. Il en est bien ainsi dans le cas séparable car, pour v_i donné $\hat{L}_i \longrightarrow \hat{K}(z_j)$ est déterminé à un $\hat{K}$-isomorphisme près, donc z_j est racine d'un et un seul des facteurs de P .

Autre méthode :

Pour tout i , on a une application $\hat{K}$-linéaire canonique $\beta_i : \hat{K} \otimes_K L \longrightarrow \hat{L}_i$ déduite de l'injection $\varphi_i : L \longrightarrow \hat{L}_i$. On en déduit une application canonique $\beta : \hat{K} \otimes_K L \longrightarrow \prod_{i\in I} \hat{L}_i$. Montrons que β est surjective. Soient en effet $y_i \in \hat{L}_i$, $i\in I$; d'après le théorème d'approximation, on peut trouver une suite $(x_j)_{j\in\mathbb{N}}$ d'éléments de L telle que, pour tout i , $\varphi_i(x_j)$ tende vers y_i au sens de la topologie définie par v_i , lorsque $j \longrightarrow +\infty$. Soit (a_h), $h \in (1,n)$ une base de L sur K , et posons $x_j = \sum_{h=1}^{n} u_{jh} a_h$. Pour tout h , la suite $(u_{jh})_{j\in\mathbb{N}}$ converge nécessairement vers un élément $u_h \in \hat{K}$. On a $\varphi_i(x_j) = \sum_{h=1}^{n} \beta_i(u_{jh} \otimes a_h)$; la suite $(\beta_i(u_{jh} \otimes a_h))_{j\in\mathbb{N}}$ converge vers $\beta_i(v_h \otimes a_h)$, et pour tout i , on a $\beta_i(\sum_{h=1}^{n} v_h \otimes a_h) = y_i$, ce qui prouve bien que β est surjective.

Il suffit alors de remarquer que les dimensions de $\hat{K} \otimes_K L$ et $\prod_i \hat{L}_i$, comme espaces vectoriels sur $\hat{K}$, sont respectivement n et $\sum_i n_i$.

6. La relation : $n = \sum_{i\in I} e_i f_i$.

Remarque : Une valuation discrète ω sur K est toujours équivalente à une valuation ω_K dont le groupe des valeurs est

.../...

$\mathbb{Z}$, on dira ω_K <u>valuation normée</u>.

Si ω' est une valuation de L , extension de (K,ω), et si ω_L est la valuation normée associée à ω' , on a alors : pour tout $x \in K$ $\boxed{\omega_L(x) = e\,\omega(x)}$

<u>THEOREME 6.1.</u>

Soient K un corps, ω une valuation discrète de K , A son anneau, $\underline{m}$ son idéal, L une extension de degré fini n de K , B la fermeture intégrale de A dans L , et $(\omega_i)_{i\in I}$ l'ensemble des prolongements réels de ω à L . On a alors

$$[B/\underline{m}B : A/\underline{m}] = \sum_{i\in I} e_i f_i$$

(Pour une forme plus générale de cet énoncé, avec ω non nécessairement discrète, voir Bourbaki, Alg. comm. 6, § 8, n°5).

<u>LEMME 6.1.</u> Soit $(\underline{q}_i)_{i\in I}$ une famille finie d'idéaux étrangers deux à deux de B . Alors $\bigcap_{i\in I} \underline{q}_i = \prod_{i\in I} \underline{q}_i$ et l'homomorphisme canonique $\beta : \underline{m}/\bigcap_{i\in I} \underline{q}_i \longrightarrow \prod_{i\in I} B/\underline{q}_i$ est bijectif.

$\underline{q}_i + \underline{q}_j = B$ pour $i \neq j \Rightarrow \underline{q}_i$ est étranger à $\prod_{i\neq j} \underline{q}_j$ car tout idéal premier $\underline{p}$ contenant $\underline{q}_i$ et $\prod_{i\neq j} \underline{q}_j$ contiendra un $\underline{q}_j$ avec $j \neq i$, sinon ils existeraient $(s_j)_{j\neq i}$ tels que $s_j \in \underline{q}_j$, mais $s_j \notin \underline{p}$ et $\prod_{j\neq i} s_j \in \underline{p}$, ce qui est absurde.

Pour démontrer que $\bigcap_{i\in I} \underline{q}_i = \prod_{i\in I} \underline{q}_i$, raisonnons par récurrence sur le nombre d'idéaux étrangers $\underline{q}_i$. Considérons le cas $n=2$.

Il existe $x_1 \in \underline{q}_1$ et $x_2 \in \underline{q}_2$ tels que $1 = x_1 + x_2$; pour tout $x \in \underline{q}_1 \cap \underline{q}_2$, on a : $x = xx_1 + xx_2 \in \underline{q}_1\underline{q}_2$, d'où $\underline{q}_1\underline{q}_2 \supset \underline{q}_1 \cap \underline{q}_2$ comme $\underline{q}_1\underline{q}_2 \subset \underline{q}_1 \cap \underline{q}_2$ on a l'égalité.

Admettant $\bigcap_{i=1}^{n} \underline{q}_i = \prod_{i=1}^{n} \underline{q}_i$, alors $\underline{q}_{n+1}$ est étranger à $\prod_{i=1}^{n} \underline{q}_i$, et on a :

$$\bigcap_{i=1}^{n+1} \underline{q}_i = (\prod_{i=1}^{n} \underline{q}_i) \cap \underline{q}_{n+1} = (\prod_{i=1}^{n} \underline{q}_i)\underline{q}_{n+1} = \prod_{i=1}^{n+1} \underline{q}_i ,$$

.../...

β est injectif puisque $\ker \beta = \bigcap_{i\in I} \underline{q}_i / \prod_{i\in I} \underline{q}_i = \{0\}$;

β est surjectif car $I = z_i + t_i$, avec $z_i \in \underline{q}_i$ et $t_i \in \underline{q}_j$;

donc $t_i \equiv \begin{cases} 1 \mod \underline{q}_i \\ 0 \mod \underline{q}_j \end{cases}$, et $(\bar{x}_i)_{i\in I}$, où $\bar{x}_i$ est réduit mod $\underline{q}_i$ de x_i , est l'image de $\sum_{i\in I} x_i t_i$, réduit mod $\bigcap_{i\in I} \underline{q}_i$, par β .

Démonstration du théorème 6.1.

$B = \bigcap B_j$ où B_j parcourt la famille des anneaux de valuations de L contenant A . (E, Chap. 0, § B, n° 3, th. 2). Les B_j sont les B_{ω_i} .

Soient $\underline{n}_i$ l'idéal maximal de ω_i et $\underline{m}_i = B \cap \underline{n}_i$; prouvons que $B_i = B_{\underline{m}_i}$, avec $B_{\underline{m}_i} = B[S_i^{-1}]$, pour $S_i = B - \underline{m}_i$; c'est-à-dire $B_{\underline{m}_i}$ est l'ensemble des fractions $\frac{a}{b}$ avec $a,b \in B$ et $b \notin \underline{m}_i$.

$B_{\underline{m}_i} \subset B_i$, car $b \in B$ et $b \notin \underline{m}_i$ entraînent $b \in B_i - \underline{n}_i$, puisque $\underline{m}_i = \underline{n}_i \cap B$. Or $B_i \subset B_{\underline{m}_i}$, car appliquant le théorème d'approximation : pour $x \in B_i$, il existe $z \in L^*$ tel que :

$\omega_j(z) = (\omega_j(x))^- \geq 0$, pour tout j . On a :

$\omega_j(xz) = (\omega_j(x))^+ \geq 0$, donc $xz \in B$ et $z \in B$, or $z \notin \underline{m}_i$, puisque $\omega_i(x) \geq 0$, d'où $\omega_i(z) = 0$; or $x = \frac{xz}{z}$, donc $x \in B_{\underline{m}_i}$.

Les idéaux maximaux de B sont les $\underline{m}_i$. En effet, soit $\underline{n}$ un idéal maximal de B ; d'après le théorème de prolongement, l'homomorphisme canonique $B \longrightarrow B/\underline{n}$ se prolonge à une place non triviale sur K de L , il existe donc un anneau de valuation B' de L , contenant B , d'idéal maximal $\underline{m}'$ contenant $\underline{n}$. Or $A \subset B' \cap K \subset K$; comme A est un anneau de valuation discrète et $\underline{n} \neq B$, on a : $B' \cap K = A$. Alors B' est un B_i et $\underline{m}' = \underline{n}_i$, d'où : $\underline{n} \subset \underline{n}_i \cap B = \underline{m}_i \subset B$; comme $\underline{n}$ est maximal, $\underline{n} = \underline{m}_i$.

.../...

Inversement, pour prouver que $\underline{m}_i$ est maximal, nous utiliserons : <u>les idéaux premiers de</u> B <u>contenant</u> $\underline{m}B$ <u>sont les</u> $\underline{m}_i$. En effet, prenant $\underline{p}$, idéal premier de B contenant $\underline{m}B$, $B/\underline{p}$ est intègre et entier sur le corps $K^\circ = A/\underline{m}$, car B est entier sur A . Si $y \in B/\underline{p}$ alors $K^\circ[y]$ est intègre et de type fini, puisque y est entier d'où $K^\circ[y] = K^\circ(y)$, donc pour $y \neq 0$, y est inversible, $B/\underline{p}$ est un corps et $\underline{p}$ est maximal. Comme les $\underline{m}_i$ sont premiers et contiennent $\underline{m}B$, ce sont des idéaux maximaux de B . Il résulte également que, si rac $\underline{a}$ désigne la racine de $\underline{a}$, i.e. l'intersection des idéaux premiers de B contenant l'idéal $\underline{a}$, ou ensemble des $x \in B$ tels que $x^n \in \underline{a}$.

$$\text{rac } \underline{m}B = \bigcap_{i \in I} \underline{m}_i \ .$$

<u>Si $\underline{q}_i = \underline{m}B_i \cap B$, alors : rac $\underline{q}_i = \underline{m}_i$</u> . En effet $\underline{q}_i \subset \underline{m}_i$, car $\underline{m}B_i \subset \underline{n}_i$, donc rac $\underline{q}_i \subset \underline{m}_i$. Inversement, soit $x \in \underline{m}_i$, d'après le théorème d'approximation il existe $y \notin \underline{m}_i$ et $y \in \underline{m}_j$ pour $j \neq i$. Alors $xy \in \underline{m}_j$ pour tout j , donc $xy \in$ rac $\underline{m}B$ et il existe n tel que $x^n y^n \in \underline{m}B$. Comme $y \notin \underline{m}_i$, on a $y^n \notin \underline{m}_i$ et par conséquent $x^n \in \underline{m}B_i$. Or $x^n \in B$, d'où $x^n \in \underline{q}_i$ et donc $x \in$ rac $\underline{q}_i$.

<u>$\underline{q}_i$ est primaire</u>, c'est-à-dire si $xy \in \underline{q}_i$ et $x \notin \underline{q}_i$, alors $y \in$ rac $\underline{q}_i$. Puisque rac $\underline{q}_i = \underline{m}_i$, si $y \notin \underline{m}_i$, avec $xy = \frac{m}{z}$ et $z \notin \underline{m}_i$, alors $yz \notin \underline{m}_i$ et $x \in \underline{m}B_i$.

<u>$\underline{m}B = \bigcap_{i \in I} \underline{q}_i$</u> , puisque $\underline{m}B \subset \underline{m}B_i \cap B = \underline{q}_i$. Inversement, soit $x \in \bigcap_{i \in I} \underline{q}_i$; si $x \notin \underline{m}B$, l'idéal $\underline{x} = (\underline{m}B : (x)) = \{y \in B \ ; \ xy \in \underline{m}B\}$ n'est pas B car $1 \in \underline{x} \iff x \in \underline{m}B$. Donc il existe $i \in I$ tel que $\underline{x} \subset \underline{m}_i$ or $(\underline{m}B : (x)) \subset \underline{m}_i \iff (yx \in \underline{m}B \Rightarrow y \in \underline{m}_i) \iff x \notin \underline{m}B_i$ d'où $x \notin \underline{q}_i = \underline{m}B_i \cap B$.

<u>$\underline{q}_i$ et $\underline{q}_j$ sont étrangers pour $i \neq j$, c'est-à-dire $\underline{q}_i + \underline{q}_j = B$,</u>

.../...

car tout idéal premier contenant $\underline{q}_i$ et $\underline{q}_j$ contiendra $\underline{m}_i$ et $\underline{m}_j$. D'après le lemme, les espaces vectoriels $B/\underline{m}B$ et $\prod_{i\in I} B/\underline{q}_i$ sur $K^o = A/\underline{m}$ ont même dimension d'où

$$\dim B/\underline{m}B = \sum_{i\in I} \dim B/\underline{q}_i$$

$\underline{B_i = B + \underline{m}B_i}$. Il suffit de prouver $B_i \subset B + \underline{m}B_i$.

Si $x \in B_i$ alors $x = ab^{-1}$ avec $b \notin \underline{m}_i$, et $1 \in bB + \underline{q}_i$, sinon $bB = \underline{q}_i \subset \underline{m}_i$ (car $\underline{m}_i$ est le seul idéal maximal de B contenant $\underline{q}_i$), donc $b \in \underline{m}_i$ ce qui est absurde. D'où $b^{-1} \in B + \underline{m}B_i$ et $x \in B = \underline{m}B_i$.

D'après le deuxième théorème d'isomorphisme $B/_{B \cap \underline{m}B_i} = B/\underline{q}_i$ est isomorphe à $B_i/\underline{m}B_i$ alors : $\underline{\dim B/\underline{q}_i = \dim B_i/\underline{m}B_i}$

$B_i/\underline{m}B_i$ est un espace vectoriel sur $B_i/\underline{m}_i B_i$ extension de K^o or $\underline{[B_i/\underline{m}_i B_i : A/\underline{m}] = f_i}$, puisque $\underline{n}_i = \underline{m}_i B_i$ car $B_i = B_{\underline{m}_i}$.

Comme ω_i est discrète, soit u une uniformisante de ω_i , alors d'après la remarque : $\underline{m}_i B_i = (u)$ et $\underline{m}B_i = (u^{e_i})$. De plus les $u^j B_i/u^{j-1}B_i$ sont des espaces vectoriels de dimension 1 sur K^o car il n'y a pas d'idéaux entre (u^j) et (u^{j-1}) . D'où

$$\dim B_i/\underline{m}B_i = \sum_{j=1}^{e_i} \dim u^j B_i/u^{j-1}B_i = e_i$$

THEOREME 6.2.

Avec les notations et les hypothèses du théorème précédent, les conditions suivantes sont équivalentes :

a) B est un A-module de <u>type fini</u> ;

b) B est un A-module <u>libre</u> ;

c) on a $[B/\underline{m}B : A/\underline{m}] = n$;

d) On a $\sum_{i\in I} e_i f_i = n$, et $n_i = e_i f_i$

.../...

LEMME de NAKAYAMA. Soient M un A-module de type fini, $\underline{a}$ un idéal de A contenu dans le radical de A alors :

$$M = \underline{a}M \Longrightarrow M = \{0\}$$

Si $M \neq \{0\}$ il existe un sous-module maximal M' de M, puisque M est de type fini. Prenons $u \in M-M'$, considérons $U : A \longrightarrow M$ telle que $U(a) = au$ et i l'application canonique $M \longrightarrow M/M'$.

Posons $V = i \circ U$.

M' étant maximal M/M' est simple (n'a pas de sous-module $\neq 0$) or $U(1) = u \notin M'$ donc $V(A) \neq \{0\}$ et par conséquent V est surjective, mais alors $\ker V = \underline{b}$ est maximal puisque M/M' est simple. On a : $M = \underline{a}M \subset \underline{b}M \subset M$ et donc $M = \underline{b}M$, puisque $\underline{a} \subset \text{rad } A$ = intersection des idéaux maximaux $\subset \underline{b}$. En particulier $u \in \underline{b}M$; or $M = Au + M'$, donc $u \in \underline{b}u + M' \subset M'$ ce qui est absurde.

Démonstration du théorème 6.2.

a) $\Longrightarrow$ b) Soit $(x_i)_{i\in(1,n)}$ un système de générateurs minimal de B. Alors : $B = \coprod_{i=1}^{n} Ax_i$. En effet $B \subset \sum_{i=1}^{n} Ax_i$ et les x_i sont indépendants, car si $\sum_{i=1}^{n} a_i x_i = 0$, avec a_i non tous nuls, on peut supposer $a_1 \neq 0$ et $\omega(a_1) \leq \omega(a_i)$ pour tout i, mais alors $\omega(\frac{a_i}{a_1}) \geq 0$ et $\frac{a_i}{a_1} \in A$, donc $x_1 \in \sum_{i=2}^{n} Ax_i$ ce qui est absurde car $(x_i)_{i\in(1,n)}$ est minimal.

b) $\Longrightarrow$ c) et a). Soit $\mathcal{B}$ une base de B sur A, alors $\mathcal{B}$ est base de L sur K, car $y \in L$ s'écrit $y = \frac{z}{x}$, avec $z \in B$ et $x \in A$; d'où a), et le A-module B est de rang n. Donc B est isomorphe à A^n, alors $\underline{m}B$ est isomorphe à $\underline{m}^n$, et $B/\underline{m}B$ est isomorphe à $(A/\underline{m})^n$ d'où c).

c) $\Longrightarrow$ a) Soit $(x_i)_{i\in(1,n)}$ une base de $B/\underline{m}B$ sur $A/\underline{m}$.

.../...

Soit $B' = Ax_1 + Ax_2 + \ldots + Ax_n$, pour $y \in B$ considérons $B'' = Ay + B'$. Alors $B' \subset B'' \subset B$ et donc $\underline{m}B' \subset \underline{m}B'' \subset \underline{m}B$. Introduisons les homomorphismes canoniques $B'/_{\underline{m}B'} \xrightarrow{\lambda} B''/_{\underline{m}B''} \xrightarrow{\beta} \xrightarrow{\beta} B/_{\underline{m}B}$. Comme les rangs de B' et B'' sont $\leq n$, il en est de même des dimensions de $B'/\underline{m}B'$ et $B''/\underline{m}B''$. Or, $\beta \circ \lambda$ est surjectif par choix des x_i , et $B/\underline{m}B$ est de dimension n , donc $B'/_{\underline{m}B'}$ et $B''/_{\underline{m}B''}$ sont de dimension n , et λ est surjectif. Ou encore $B'' = B' + \underline{m}B''$ donc $B''/_{B'} = \underline{m}B''/_{B'}$, d'après le lemme de Nakayama, puisque $\underline{m} = \operatorname{rad} A$ on a : $B''/_{B'} = \{0\}$, d'où $B'' = B'$, donc $y \in B'$, et B est de type fini puisque $B = B'$.

c) $\Longleftrightarrow$ d) D'après le théorème 6.1., on a $[B/\underline{m}B : A/\underline{m}] = \sum_{i \in I} e_i f_i$. Quant à $e_i f_i = n_i$, cela résulte de $\sum_{i \in I} n_i \leq n$ d'après le théorème 5.4., et $e_i f_i \leq n_i$ d'après le théorème 5.1.

<u>COROLLAIRE 1</u>. Si L <u>est séparable</u> : $n = \sum_{i \in I} e_i f_i$ et $n_i = e_i f_i$.

A est de valuation discrète, donc noethérien (E, Chap. O, § A, n° 7, th. 6) alors B est un A-module de type fini (E, chap. O, § B, n° 3, cor. 1 du th. 4).

<u>COROLLAIRE 2</u>. Si K <u>est complet</u> : $n = ef$.

En effet $[B/\underline{m}B : A/\underline{m}] = ef \leq n < +\infty$, soit (y_j) avec $j \in (1, ef)$ les représentants d'une base de $B/\underline{m}B$ sur K° , alors $B = \sum_j A\, y_j + \underline{m}B$ et plus généralement $\underline{m}^n B = \sum_j \underline{m}^n y_j + \underline{m}^{n+1} B$, d'où $B = \sum_j A\, y_j$, puisque A , étant fermé dans K , est complet.

Si <u>$e = 1$ et L° séparable sur K°</u> , on dit que <u>ω' est non ramifiée sur ω</u> .

Si <u>$f = n$ et L° séparable sur K°</u> , on dit que <u>L est non ramifiée sur K</u> .

.../...

Si K est complet et L non ramifiée alors L est monogène.

D'après le théorème de l'élément primitif $L^\circ = K^\circ(\eta)$.

Soit y un représentant de η dans L, alors les (y^i) avec $i \in (0,f-1)$ sont indépendants d'après la démonstration du théorème 4.1., et forment une base de L, car $f = n$ d'après le cor. 2 donc $L = K(y)$.

Si <u>e=n et f=1</u> l'extension sera dite <u>totalement ramifiée</u>.

Si u est solution d'un polynôme d'Eisenstein de degré n, L=K(u) est une extension totalement ramifiée de K de degré n. Inversement si L est totalement ramifiée sur K complet, alors L = K(u), avec u solution d'un polynôme d'Eisenstein de degré $[L : K]$.

Si $u^n + a_1 u^{n-1} + \ldots + a_n = 0$, avec $\omega_K(a_n) = 1$ et $\omega_K(a_j) \geq 1$, soit $\omega_L(a_i u^{n-i})$ le minimum des $\omega_L(a_j u^{n-j})$, avec $j \in (1,n)$.

$\omega_L(u^n) \geq \omega(a_i u^{n-i})$ donc $i\omega_L(u) \geq \omega_L(a_i) = e$ et donc $\omega_L(a_i u^{n-i}) = e$ avec $\omega_L(u) > 0$, ce qui entraîne : $i = 0$, ou $i = n$. Comme deux termes de la somme doivent avoir la valuation minimale : $\omega_L(u^n) = \omega_L(a_n) = e$.

Alors $n\,\omega_L(u) = e$, or $e \leq [L : K] \leq n$ et $\omega_L(u) \geq 1$ d'où $n = e = [L : K]$, et $\omega_L(u) = 1 = f$.

Inversement, soit u une uniformisante de ω_L ; les (u^i) avec $i \in (0,e-1)$ sont indépendants d'après la démonstration du th. 4.1., comme K est complet $e = n$, d'après le cor. 2 ; donc les (u^i) forment une base, L = K(u) et u est racine d'un polynôme irréductible $F = X^e + a_1 X^{e-1} + \ldots + a_e$. En se plongeant dans une extension quasi-galoisienne, $\omega_K(a_i) \geq 1$ et $\omega_L(a_e) = e\,\omega_L(u) = e$, donc $\omega_K(a_e) = 1$, par conséquent F est

.../...

un polynôme d'Eisenstein.

7. Valeurs absolues "well behaved".

Définition 7.1. On appelle valeur absolue "well behaved" d'un corps K (terminologie de S. Lang, Dioph. Geometry, I, § 4) toute valeur absolue v de K vérifiant la condition suivante : (W.B.) pour toute extension algébrique L de K de degré fini n on a : $\sum_{w/v} n_w = n$; la somme est étendue à toutes les valuations w de L prolongeant v .

Exemples :

a) Si v est archimédienne sur K elle est well behaved, car (K,v) est isomorphe en tant que corps valué à un sous-corps de $\mathbb{C}$, donc K est de caractéristique 0 , par conséquent L est séparable, il suffit alors d'appliquer le c) du théorème 6.2.

b) Démontrons d'abord le théorème :

THEOREME 7.1.

Soient A une algèbre intègre de type fini sur un corps k , K son corps des fractions, B la fermeture intégrale de A dans une extension algébrique L de degré fini de K . Alors B est un A-module de type fini.

Autrement dit : toute algèbre intègre de type fini sur un corps k , est un anneau japonais (E. G. A. Grothendieck n° 20, Chap. 0, § 23).

Démonstration.

Il suffit de prouver que B est un sous-module d'un A-module de type fini et que A est noethérien, puisque tout sous-

.../...

module d'un A-module de type fini, lorsque A est noethérien, est un A-module de type fini.

Or d'après le lemme de normalisation (E, Chap. 1, § 4), la k-algèbre de type fini A est entière sur une algèbre C , isomorphe à une algèbre de polynômes $k[X_1 , \ldots , X_n]$. Par conséquent A est une C-algèbre de type fini (E, Chap. 0, § 3, th. 4) puisque C est noethérien, comme anneau de polynômes, d'après le théorème de Hilbert ; et même A est noethérien comme C-algèbre de type fini sur un anneau noethérien. B est la fermeture intégrale de C dans L , il suffit donc de faire la démonstration dans le cas $A = k[X_1,\ldots,X_n]$; en effet, si B est un C-module de type fini, il est contenu dans un A-module de type fini.

Soit $K' = L \cap K^{p^{-\infty}}$, alors L est séparable sur K' et B est un sous-module d'un module de type fini sur A' , clôture algébrique de A dans K' (E. Chap. 0, § 3, th. 4). Ainsi il suffit de démontrer que lorsque L est une extension radicielle de $k(X_1,\ldots,X_n)$, la clôture intégrale B de $A = k[X_1,\ldots,X_n]$ dans L est un sous-module d'un A-module de type fini. Or il existe une puissance q de la caractéristique telle que : $L \subset L' = k'(X_1^{\frac{1}{q}},\ldots, X_n^{\frac{1}{q}})$ où k' est une extension finie et radicielle de k Or B est un sous-module de la fermeture intégrale B' de A dans L' , et $B' = k'[X_1^{\frac{1}{q}},\ldots, X_n^{\frac{1}{q}}]$ car l'anneau de polynômes $k'[X_1^{\frac{1}{q}},\ldots,X_n^{\frac{1}{q}}]$ est factoriel, donc intégralement clos et entier sur A . Or B' est un A-module de type fini car si S est une base de l'extension k'/k , B' est engendré comme A-module par les produits de la forme $\gamma \prod_i X_i^{\frac{m_i}{q}}$ où $\gamma \in S$, et où les m_i sont des entiers positifs $\leq q$.

.../...

THEOREME 7.2.

Soient A une algèbre intègre de type fini sur un corps k, et K son corps des fractions. Toute valuation discrète de K dont l'anneau est de la forme $A_{\underline{p}}$, où $\underline{p}$ est un idéal premier de A est well-behaved.

Soit B la fermeture de A dans une extension L de degré fini de K, alors B est un A-module de type fini (th. 7.1). Considérons la clôture intégrale A' de $A_{\underline{p}} = A[S^{-1}]$ avec $S = A-\underline{p}$. La fermeture intégrale B' de A' dans L est $B[S^{-1}]$; d'où B' est de type fini sur A' et le th. 6.2. a) implique le th. 7.2..

8. Norme et trace locales.

Définition 8.1. Soient L une extension algébrique de degré fini d'un corps K, w une valeur absolue de L et v sa restriction à K. On appelle norme locale N_w ou $N_{w/v}$, (resp. : trace locale Tr_w ou $Tr_{w/v}$), la norme $N_{\hat{L}_w/\hat{K}_v}$, (resp. la trace $Tr_{\hat{L}_w/\hat{K}_v}$), de l'extension $\hat{L}_w$, complété de L pour la valeur absolue w, sur $\hat{K}_v$, complété de K pour la valeur absolue v.

THEOREME 8.1.

Soient K un corps, v une valeur absolue de K well-behaved, L une extension de degré fini n de K, si l'on pose $N = N_{L/K}$ et $Tr = Tr_{L/K}$, alors pour tout $x \in L$:

$$N(x) = \prod_{w/v} N_w(x)$$

$$Tr(x) = \sum_{w/v} Tr_w(x)$$

$$v(N(x)) = \sum_{w/v} n_w \cdot w(x)$$

.../...

v est archimédienne, ou bien -v est une valuation ω, dont l'anneau A_ω est japonais, d'après le a) du th. 6.2.. Ainsi il faut et il suffit que : $n = \sum_{w/v} n_w$.

La dernière formule du théorème est conséquence de la première formule et du coroll. 2 du th. 5.4.

1ère démonstration.

Cas 1 : Si $L = K(y)$ et si P est le polynôme minimal de y sur K, factorisant P en polynômes irréductibles dans $\hat{K}[X]$, $P = P_1 \cdots P_r$ et les valeurs absolues de L correspondent bijectivement aux P_j (th. 5.5.) ; la norme de y (resp. la trace de y) se déduit au signe près du terme constant (resp. : du coefficient de degré juste inférieur au degré du polynôme).

Cas 2 : Si $y \in K$: $N(y) = y^n$ (resp. : $Tr(y) = ny$) et $n = \sum_{w/v} n_w$.

Cas général : Si $x \in L$, il suffit d'utiliser la transitivité de la norme (resp. : de la trace), puisque pour tout $x \in L$ on a $K \subset K(x) \subset L$.

2ème démonstration.

Reprenons l'homomorphisme canonique $\beta : \hat{K} \otimes_K L \longrightarrow \prod_{w/v} \hat{L}_w$ de la démonstration du th. 5.5.. Comme v est well-behaved, β est un isomorphisme puisque les deux espaces vectoriels sont de dimension n sur $\hat{K}$. Soit $x \in L$, considérons le K-endomorphisme $u \longmapsto ux$ de L ; alors, par définition $N(x)$ est son déterminant et $Tr(x)$ sa trace. Si (e_i) est une base de L sur K, les $1 \otimes e_i$ forment une base du $\hat{K}$-espace vectoriel $\hat{K} \otimes_K L$; donc $N(x)$ (resp. : $Tr(x)$) est le déterminant (resp. : la trace) du $\hat{K}$-endomorphisme $z \longmapsto z.(1 \otimes x)$

.../...

de $\hat{K} \otimes_K L$, qui se transporte par l'isomorphisme canonique en l'endomorphisme de $\prod_{w/v} \hat{L}_w$ laissant stable chacun des facteurs et se réduisant dans chaque facteur $\hat{L}_w$ à la multiplication par $\varphi_w(x)$. Dans la base $(\beta(1 \otimes e_i))$ la matrice de cet endomorphisme s'écrit comme une matrice diagonale de matrices carrées relatives aux multiplications par $\varphi_w(x)$ dans chaque L_w ; d'où les deux premières formules, puisque φ_w permet d'identifier L à un sous-corps de $\hat{L}_w$.

9. Anneaux de Dedekind.

Définition 9.1. Soient A un anneau intègre, K son corps des fractions. On appelle idéal fractionnaire de A tout sous-A-module $\underline{a}$ de K tel qu'il existe un élément $d \neq 0$ de A pour lequel $d\,\underline{a} \subset A$.

Tout idéal fractionnaire s'écrit $\underline{a} = d^{-1}\underline{b}$ où $\underline{b}$ est un idéal de A .

Tout sous-A-module $\underline{a}$ de type fini de K est un idéal fractionnaire, car il suffit de prendre pour d un dénominateur commun des générateurs. En particulier les sous-A-modules monogènes Ax de K sont des idéaux fractionnaires que l'on appelle idéaux principaux fractionnaires. Inversement, si A est noethérien, tout idéal fractionnaire $\underline{a}$ est un sous-A-module de type fini de K , puisque $\underline{a}$ est contenu dans le sous-A-module de type fini $d^{-1}A$ de K .

Opérations sur les idéaux fractionnaires.

Si $\underline{a}$ et $\underline{b}$ sont deux idéaux fractionnaires de A , les sous-A-modules de K : $\underline{a} + \underline{b}$, $\underline{a} \cap \underline{b}$ et $\underline{a}.\underline{b}$ sont des idéaux fractionnaires de A . Le transporteur de $\underline{b}$ dans $\underline{a}$, à savoir $(\underline{a} : \underline{b}) = \{x \in K \ ; \ x\underline{b} \subset \underline{a}\}$ est un sous-A-module de K , mais

.../...

pour $\underline{b} = \{0\}$, c'est le corps K tout entier, qui n'est pas, en général, un idéal fractionnaire. Par contre, pour $\underline{b} \neq \{0\}$, alors il existe un élément $b \neq 0$ de $A \cap \underline{b}$; pour $x \in (\underline{a} : \underline{b})$ on a $bx \in \underline{a}$; or il existe $d \neq 0$ de A pour lequel $d\,\underline{a} \subset A$ et par conséquent $dbx \in A$, donc $(\underline{a} : \underline{b})$ est un idéal fractionnaire, de plus si $\underline{a} \neq \{0\}$, il existe $a \neq 0$ dans $\underline{a}$ et $c \neq 0$ dans A tel que $c\,\underline{b} \subset A$ et $c\,a\,\underline{b} \subset \underline{a}$ donc $(\underline{a} : \underline{b}) \neq \{0\}$. L'application $\varphi : x \longmapsto (x) = Ax$ est un homomorphisme surjectif du groupe multiplicatif K^* sur l'ensemble $\mathcal{P}$ des idéaux fractionnaires principaux de K muni de la multiplication ; donc $\mathcal{P}$ est un groupe pour la multiplication ; le noyau de φ est l'ensemble des x tels que $Ax = A$, c'est-à-dire le groupe U de unités de A ; donc $\mathcal{P}$ est isomorphe à K^*/U . Si A est principal, tous les idéaux fractionnaires sont principaux car $\underline{a} = d^{-1}\underline{b}$ où $\underline{b}$ est un idéal de A de la forme $b\,A = (b)$, d'où $\underline{a} = (d^{-1}b)$. Pour les idéaux principaux fractionnaires on a : $((a) : (b)) = (ab^{-1})$.

Localisation.

Soient A un anneau intègre, $\underline{p}$ un idéal premier de A et $A_{\underline{p}}$ le localisé de A en $\underline{p}$. Le sous-$A_{\underline{p}}$-module $\underline{a}\,A_{\underline{p}}$ de K est un idéal fractionnaire de $A_{\underline{p}}$ que l'on notera $\underline{a}_{\underline{p}}$.
On a alors :

$$(\underline{a}.\underline{b})_{\underline{p}} = \underline{a}_{\underline{p}}.\underline{b}_{\underline{p}} \; ; \; (\underline{a}+\underline{b})_{\underline{p}} = \underline{a}_{\underline{p}} + \underline{b}_{\underline{p}} \; ; \; (\underline{a} \cap \underline{b})_{\underline{p}} = \underline{a}_{\underline{p}} \cap \underline{b}_{\underline{p}}$$

$(\underline{a} : \underline{b})_{\underline{p}} \subset (\underline{a}_{\underline{p}} : \underline{b}_{\underline{p}})$ et l'on a l'égalité si $\underline{b}$ est un A-module de type fini, en particulier si A est noethérien.

Les premières propositions résultent des définitions ; quant à la dernière relation, on remarque que si $x \in (\underline{a} : \underline{b})$ alors $x\,\underline{b} \subset \underline{a}$, donc $x\,\underline{b}_{\underline{p}} \subset \underline{a}_{\underline{p}}$ et par conséquent $x \in (\underline{a}_{\underline{p}} : \underline{b}_{\underline{p}})$.

.../...

Inversement, si $\underline{b}$ est de type fini, $\underline{b} = b_1A + b_2A + \ldots + b_nA$ et si $x \in (\underline{a}_{\underline{p}} : \underline{b}_{\underline{p}})$, on a $x\,\underline{b}_{\underline{p}} \subset \underline{a}_{\underline{p}}$ et donc $x\,b_i \in \underline{a}_{\underline{p}}$ pour tout $i \in (1,n)$; alors $x\,b_i = \frac{c_i}{d_i}$, avec $c_i \in \underline{a}$ et $d_i \in A-\underline{p}$; posons $d = d_1d_2\ldots d_n$; puisque $\underline{p}$ est premier, $d \in A-\underline{p}$, et $x\,d\,\underline{b} \subset \underline{a}$; donc $x\,d \in (\underline{a} : \underline{b})$, par conséquent $x \in (\underline{a} : \underline{b})A_{\underline{p}}$.

Définition 9.2. Soient A un anneau intègre, on dira que A est un anneau de Dedekind si

a) A est noethérien

b) Pour tout idéal maximal $\underline{m}$ non nul de A, le localisé $A_{\underline{m}}$ est un anneau de valuation discrète.

En particulier l'anneau $\mathbb{Z}$ ou, plus généralement, tout anneau principal, est un anneau de Dedekind.

THEOREME 9.1.

Si un anneau intègre est de Dedekind, ses idéaux fractionnaires non nuls, forment un groupe pour la multiplication.

Soit $\underline{a}$ un idéal fractionnaire non nul, alors $(A : \underline{a}).\underline{a} = A$. En effet pour tout $\underline{m}$ maximal $(A : \underline{a})_{\underline{m}} = (A_{\underline{m}} : \underline{a}_{\underline{m}})$ puisque A es noethérien, et $(A : \underline{a})_{\underline{m}}.\underline{a}_{\underline{m}} = A_{\underline{m}}$ puisque $A_{\underline{m}}$ est principal, comme anneau de valuation discrète. Ainsi pour tout idéal maximal $\underline{m} \neq (0)$ on a $((A : \underline{a}).\underline{a})_{\underline{m}} = A_{\underline{m}}$; or $(A : \underline{a}).\underline{a}$ est un idéal $\underline{b}$ de A. On a $\underline{b} = A$, sinon il existerait un idéal maximal $\underline{m} \supset \underline{b}$ de A et on aurait $A_{\underline{m}} = \underline{b}\,A_{\underline{m}} \subset \underline{m}\,A_{\underline{m}}$, ce qui est absurde.

THEOREME 9.2.

Si A est un anneau de Dedekind tout idéal premier non nul de A est maximal.

.../...

Autrement dit : dim A $\leq$ 1 c'est-à-dire toutes les chaînes d'idéaux premiers sont réduites à deux idéaux au plus : si $\underline{p} \subset \underline{q}$, avec $\underline{p}$ et $\underline{q}$ idéaux premiers de A , on a $\underline{p} = 0$ ou $\underline{p} = \underline{q}$.

Démonstration.

Si $\underline{p}$ est un idéal premier non nul de A , et si $\underline{m}$ est un idéal maximal de A contenant $\underline{p}$, l'anneau $A_{\underline{m}}$ est principal comme anneau de valuation discrète ; or $\underline{p}\, A_{\underline{m}}$ est un idéal premier non nul de $A_{\underline{m}}$, on a donc nécessairement $\underline{p}\, A_{\underline{m}} = \underline{m}\, A_{\underline{m}}$. Or $A_{\underline{m}} \subset A_{\underline{p}}$ et $\underline{p}\, A_{\underline{m}} \cap A \subset \underline{p}\, A_{\underline{p}} \cap A = \underline{p}$, comme $\underline{m}\, A_{\underline{m}} \cap A = \underline{m}$, on trouve $\underline{m} \subset \underline{p}$, donc $\underline{m} = \underline{p}$.

THEOREME 9.3.

Soient A un anneau de Dedekind et x non nul dans A ; alors il n'y a qu'un nombre fini d'idéaux premiers de A contenant x .

Si $(\underline{p}_n)$ est une suite d'idéaux premiers contenant x , la suite $(\underline{q}_n)$ avec $\underline{q}_n = \bigcap_{i=1}^{n} \underline{p}_i$ est décroissante pour l'inclusion et minorée par (x). Donc la suite $(A : \underline{q}_n)$, croissante et majorée par $(A : (x)) = A\, x^{-1}$, est formée d'idéaux fractionnaires de A , donc de sous-A-modules du sous-module noethérien Ax^{-1} du corps K des fractions de A ; par conséquent la suite $(A : \underline{q}_n)$ est stationnaire. Or d'après le th. 9.1. on a $(A : (A : \underline{q}_n)) = \underline{q}_n$, donc la suite $\underline{q}_n$ est stationnaire. Or $\underline{q}_{n+j} = \underline{q}_n$ entraîne $\underline{p}_{n+j} \supset \bigcap_{i=1}^{n} \underline{p}_i \supset \prod_{i=1}^{n} \underline{p}_i$, comme $\underline{p}_{n+j}$ est premier, il contient l'un des $\underline{p}_i$ pour $i \in (1,n)$; avec le th. 9.2. on en déduit que $\underline{p}_{n+j}$ est égal à l'un des $\underline{p}_i$ pour $i \in (1,n)$. Il n'y a donc qu'un nombre fini de $\underline{p}_n$ distincts.

.../...

COROLLAIRE. Notant $\omega_{\mathfrak{p}}$ la valuation normée de K d'anneau $A_{\mathfrak{p}}$, pour tout $x \in K^*$, les entiers rationnels $\omega_{\mathfrak{p}}(x)$ sont nuls sauf un nombre fini d'entre eux, lorsque $\mathfrak{p}$ parcourt les idéaux premiers non nuls de A.

En effet, il suffit de le prouver pour $x \in A$; or $\omega_{\mathfrak{p}}(x) > 0$ équivaut à $x \in \mathfrak{p}\, A_{\mathfrak{p}} \cap A = \mathfrak{p}$.

Convenons de poser $\omega_{\mathfrak{p}}(E) = \inf_{x \in E} \omega_{\mathfrak{p}}(x)$ pour tout sous-ensemble E de K. Si $\underline{a}$ est un idéal fractionnaire de A, anneau noethérien, $\underline{a} = a_1 A + a_2 A + \ldots + a_n A$, et $\omega_{\mathfrak{p}}(\underline{a}) = \inf_{i \in (1,n)} \omega_{\mathfrak{p}}(a_i)$ est fini. D'après le corollaire précédent $\omega_{\mathfrak{p}}(a)$ est nul sauf pour un nombre fini de $\mathfrak{p}$, et $A_{\mathfrak{p}}$ étant un anneau de valuation discrète $\underline{a}_{\mathfrak{p}} = (\mathfrak{p}\, A_{\mathfrak{p}})^{\omega_{\mathfrak{p}}(\underline{a})}$.

THEOREME 9.4.

Soit A un anneau de Dedekind. Alors A est intégralement clos, et on a $A = \bigcap_{\mathfrak{p}} A_{\mathfrak{p}}$, où l'intersection est étendue à tous les idéaux premiers de A.

Comme toute intersection d'anneaux de valuation est un anneau intégralement clos, il suffit de prouver la seconde assertion, c'est-à-dire de prouver que $x \in A_{\mathfrak{p}}$ pour tout $\mathfrak{p}$ entraîne $x \in A$. Or supposons $x \notin A$. Alors $1 \notin (A : (x))$; l'idéal $\underline{a} = A \cap (A:(x))$ de A est distinct de A, donc contenu dans un idéal maximal $\underline{m}$ de A. On a $x \in A_{\underline{m}}$, donc il existe $y \in A - \underline{m}$ tel que $xy \in A$; ceci implique $y \in \underline{a} \subset \underline{m}$, donc conduit à une contradiction.

Les théorèmes 9.2. et 9.4. entraînent que tout anneau de Dedekind est

a) - noethérien

b) - de dimension ≤ 1

.../...

c) - intégralement clos.

Il est bien connu que ces trois propriétés sont caractéristiques, i.e. que tout anneau intègre vérifiant a) b) et c) est de Dedekind. Nous n'aurons pas dans la suite à utiliser cette dernière propriété.

THEOREME 9.5. (décomposition en facteurs premiers).

Soit A un anneau de Dedekind. Tout idéal fractionnaire $\underline{a}$ non nul de A admet une décomposition et une seule de la forme : $\underline{a} = \prod_{\underline{p}} \underline{p}^{n(\underline{p})}$ où le produit est étendu aux idéaux premiers $\underline{p}$ non nuls de A et les exposants entiers rationnels $n(\underline{p})$ nuls à l'exception d'un nombre fini d'entre eux. De plus, on a $n(\underline{p}) = \omega_{\underline{p}}(\underline{a})$.

LEMME. Si $\underline{p}$ et $\underline{q}$ sont deux idéaux premiers de A :

$$\underline{p} \neq \underline{q} \iff \underline{p} A_{\underline{q}} = A_{\underline{q}} .$$

En effet il suffit de prouver que $\underline{p} A_{\underline{q}} \subset \underline{q} A_{\underline{q}}$ entraîne $\underline{p} = \underline{q}$, car $\underline{q} A_{\underline{q}}$ est un idéal maximum dans l'anneau de valuation discrète $A_{\underline{q}}$. Or $\underline{p} A_{\underline{q}} \supset \underline{p}$ et $\underline{q} A_{\underline{q}} \cap A = \underline{q}$ donc $\underline{p} \subset \underline{q}$, et $\underline{p} = \underline{q}$ d'après le th. 9.2.

Démonstration du th. 9.5.

Unicité : par localisation $a_{\underline{p}} = \prod_{\underline{p}} (\underline{p} A_{\underline{p}})^{n(\underline{p})}$ et d'après le lemme $\underline{a}_{\underline{q}} = (\underline{q} A_{\underline{q}})^{n(\underline{q})}$; d'où $n(\underline{q}) = \omega_{\underline{q}}(\underline{a})$.

Existence : $a_{\underline{p}} = (\underline{p} A_{\underline{p}})^{\omega_{\underline{p}}(\underline{a})}$. Considérons l'idéal fractionnaire $\underline{b} = \prod_{\underline{p}} \underline{p}^{\omega_{\underline{p}}(\underline{a})}$ alors $\underline{a}$ et $\underline{b}$ sont localement égaux puisque :

$$(\underline{a} : \underline{b})_{\underline{q}} = (\underline{a}_{\underline{q}} : \underline{b}_{\underline{q}}) = ((\underline{q} A_{\underline{q}})^{\omega_{\underline{q}}(\underline{a})} : \prod_{\underline{p}} (\underline{p} A_{\underline{q}})^{\omega_{\underline{p}}(\underline{a})}) = A_{\underline{q}}$$

.../...

car d'après le lemme :

$$\prod_{\underline{p}} (\underline{p}\, A_{\underline{q}})^{\omega_{\underline{p}}(\underline{a})} = (\underline{q}\, A_{\underline{q}})^{\omega_{\underline{q}}(\underline{a})} \quad .$$

En particulier, on a $(\underline{a} : \underline{b}) \subset A_{\underline{q}}$ pour tout $\underline{q}$, donc, compte tenu du th. 9.4.

$(\underline{a} : \underline{b}) \subset A$

Si $(\underline{a} : \underline{b}) \neq A$ il existerait $\underline{m} \supset (\underline{a} : \underline{b})$ maximal, et $(\underline{a} : \underline{b})_{\underline{m}} \subset \underline{m}\, A_{\underline{m}} \neq A_{\underline{m}}$, ce qui est contradictoire.

D'où l'égalité "globale" $\underline{a} = \underline{b}$.

COROLLAIRE 1. Soient $\underline{a}$ et $\underline{b}$ deux idéaux fractionnaires d'un idéal A de Dedekind. Les propriétés suivantes sont équivalentes

1) $\underline{a}$ divise $\underline{b}$ i.e. $\underline{a} : \underline{b}$ est un idéal entier de A.

2) $\underline{a} \supset \underline{b}$

3) $\omega_{\underline{p}}(\underline{a}) \leqslant \omega_{\underline{p}}(\underline{b})$ pour tout idéal premier $\underline{p}$ non nul de A.

1) $\Longrightarrow$ 2) car $(\underline{b} : \underline{a}) \subset A$ entraîne $\underline{b} \subset \underline{a}$.

2) $\Longrightarrow$ 3) par définition de $\omega_{\underline{p}}(\underline{a})$.

3) $\Longrightarrow$ 1) on utilise le théorème après avoir remarqué que $\omega_{\underline{p}}(\underline{a}) \geqslant 0$ pour tout $\underline{p}$ équivaut à $\underline{a}$ entier $(\underline{a} \subset A)$.

THEOREME 9.6.

L'anneau des entiers d'un corps de nombres algébriques est un anneau de Dedekind.

Ce théorème est conséquence du

THEOREME 9.7.

Soient A un anneau de Dedekind, K son corps des fractions, L une extension de K de degré fini séparable, alors la fermeture intégrale B de A dans L est un anneau de Dedekind.

.../...

L/K étant une extension séparable, B est une A-algèbre de type fini (E, O, 3, coroll. 1 du th. 4). Comme A est un anneau noethérien B est aussi un anneau noethérien.

Il reste à prouver que pour tout idéal $\underline{q}$ premier non nul de B, l'anneau $B_{\underline{q}}$ est un anneau de valuation discrète. L'idéal $\underline{p} = \underline{q} \cap A$ de A n'est pas nul, en effet, il existe $x \in \underline{q}$ non nul ; comme x est entier sur A, on a une relation $x^n + a_1 x^{n-1} + \ldots + a_n = 0$, avec $a_i \in A$ pour tout i, et où l'on peut supposer $a_n \neq 0$; la relation montre que a_n est multiple de x, donc que $a_n \in \underline{q}$, d'où $a_n \in \underline{p}$ et $\underline{p} \neq (0)$.

L'anneau $A_{\underline{p}}$ est un anneau de valuation discrète puisque A est un anneau de Dedekind La fermeture intégrale B' de $A_{\underline{p}}$ dans L est égale à $B[S^{-1}]$ avec $S = A - \underline{p}$. Comme $\underline{q} \cap S = \emptyset$, l'idéal $\underline{q}' = \underline{q}B'$ de B' est premier. Comme de plus cet idéal contient $\underline{p}B'$, il est maximal, d'après la démonstration du th. 6.1. ; donc l'anneau $B'_{\underline{q}'}$ est un anneau de valuation de L contenant $A_{\underline{p}}$, et même il est de valuation discrète puisque la valuation de L d'anneau $B'_{\underline{q}'}$ prolonge la valuation discrète de K d'anneau $A_{\underline{p}}$ (th. 5.2.).

Il suffit de montrer que $B_{\underline{q}} = B'_{\underline{q}'}$. Or $\underline{q} \cap S = \emptyset$ entraîne $\underline{q} = \underline{q}' \cap B$ et donc $B_{\underline{q}} \subset B'_{\underline{q}'}$. Mais $B' \subset B_{\underline{q}}$, car $B' = B[S^{-1}]$ et $B - \underline{q} \supset S$, donc $B'_{\underline{q}'} \subset B_{\underline{q}}[S'^{-1}]$ avec $S' = B' - \underline{q}'$. Si $y \in B'$, on a $y = \frac{a}{b}$ avec $a \in B$ et $b \in A - \underline{p}$; si $y \notin \underline{q}'$, on a : $a \notin \underline{q}$, sinon $\frac{1}{b} \in B' = B[S^{-1}]$, et $a \in \underline{q}$ entraîne $y \in \underline{q}'$; donc $y \in S'$ entraîne $y^{-1} \in B_{\underline{q}}$ et par conséquent $B'_{\underline{q}'} \subset B_{\underline{q}}$.

.../...

THEOREME 9.8.

Soient A un anneau de Dedekind, K son corps des fractions, L une extension de K séparable et de degré fini, B la fermeture intégrale de A dans L. Soient $\mathfrak{p}$ un idéal premier non nul de A, $\omega_{\mathfrak{p}}$ la valuation de K d'anneau $A_{\mathfrak{p}}$ et $\mathfrak{p}B = \prod_{\mathfrak{q}} \mathfrak{q}^{n(\mathfrak{q})}$ la décomposition de l'idéal $\mathfrak{p}B$ en facteurs premiers. Alors

a) $n(\mathfrak{q}) > 0$ équivaut à $\mathfrak{q} \supset \mathfrak{p}$;

b) les valuations $\omega_{\mathfrak{q}}$ de L, correspondant aux idéaux $\mathfrak{q} \supset \mathfrak{p}$, sont, a une équivalence près, les valuations de L prolongeant $\omega_{\mathfrak{p}}$;

c) on a $n(\mathfrak{q}) = e(\omega_{\mathfrak{q}}/\omega_{\mathfrak{p}})$, indice de ramification de $\omega_{\mathfrak{q}}$ sur $\omega_{\mathfrak{p}}$

a) $\mathfrak{q} \supset \mathfrak{p} \iff \mathfrak{q} \supset \mathfrak{p}B \iff \mathfrak{q}$ divise $\mathfrak{p}B \iff n(\mathfrak{q}) > 0$

b) $\mathfrak{p} A_{\mathfrak{p}} \subset \mathfrak{q}$ d'où b) d'après la démonstration du th. 5.2..

c) Pour $x \in A_{\mathfrak{p}}$ on a : $\omega_{\mathfrak{q}}(x) = e(\omega_{\mathfrak{q}}/\omega_{\mathfrak{p}})\omega_{\mathfrak{p}}(x)$ donc

$n(\mathfrak{q}) = \omega_{\mathfrak{q}}(\mathfrak{p}B) = \omega_{\mathfrak{q}}(\mathfrak{p}) = e(\omega_{\mathfrak{q}}/\omega_{\mathfrak{p}})$.

COROLLAIRE. $\mathfrak{p}B = \prod_{\mathfrak{q}\backslash\mathfrak{p}} \mathfrak{q}^{e_{\mathfrak{q}}}$ avec $e_{\mathfrak{q}} = e(\omega_{\mathfrak{q}}/\omega_{\mathfrak{p}})$.

En effet $\mathfrak{p}B$ est un idéal entier de B donc $n(\mathfrak{q}) \geqslant 0$; or $n(\mathfrak{q}) > 0$ équivaut à $\mathfrak{q} \supset \mathfrak{p}$, donc $\mathfrak{q}$ divise $\mathfrak{p}$.

10 - La formule du produit

Définition 10.1. Nous appellerons ensemble propre de valeurs absolues d'un corps K tout ensemble M de valeurs absolues de K, well-behaved, deux à deux non équivalentes, et telles que pour tout $x \in K$ on ait $v(x)=o$ pour presque toute $v \in M$ (i.e. pour toute valeur absolue v qui n'appartient pas à un sous-ensemble fini de M).

Remarques : M ne peut contenir qu'un nombre fini de valeurs absolues archimédiennes.

Pour toute extension L de K, nous noterons M_L l'ensemble de toutes les valeurs absolues de L obtenues en prolongeant à L les éléments de M. Si le degré $[L:K]$ est fini, M_L est aussi un ensemble propre de valeurs absolues.

En effet les valeurs absolues de M_L sont : inéquivalentes, well-behaved car si E est une extension finie de L, on a :

$$[E:K] = \sum_{u/v} n_{u/v} = \sum_{u/w} n_{u/w} \sum_{w/v} n_{w/v} \leqslant [E:L]\,[L:K]$$

d'où l'égalité $[E:L] = \sum_{u/w} n_{u/w}$; enfin pour tout $x \in L$, on a $w(x) = o$ pour presque toute $w \in M_L$. En effet, soit $y \in L$, vérifiant la relation de dépendance algébrique

$$y^n + a_1 y^{n-1} + \ldots + a_n = o \quad (a_i \in K,\ a_n \neq o) ;$$

pour presque toute v ultramétrique $\in M$, on a $v(a_i) = o$ quel que soit i tel que $a_i \neq o$, de sorte que y et $\frac{1}{y}$

.....

sont entiers sur l'anneau de valuation correspondant; or ceci implique $w(y) = o$ pour toute $w \in M_L$ prolongeant v .

Définition IO.2. Soit M un ensemble propre de valeurs absolues de K ; donnons-nous pour toute $v \in M$, un nombre réel $\lambda_v \geq o$. Nous dirons que M vérifie la formule du produit avec les coefficients λ_v si on a : $\sum_{v \in M} \lambda_v v(x) = o$ pour tout $x \in K$. Nous dirons que M satisfait la formule du produit s'il satisfait la formule du produit avec les coefficients $\lambda_v = 1$ pour tout $v \in M$.

N.B. - La somme $\sum_{v \in M} \lambda_v \, v(x)$ ne fait intervenir qu'un nombre fini de termes non nuls puisque M est propre.

On a conservé la terminologie classique "formule du produit" bien qu'en notation additive il s'agit en fait d'une formule de la somme.

Remarque : Si M satisfait la formule du produit avec les coefficients λ_v alors M_L satisfait la formule du produit avec les coefficients $n_{w/v} \, \lambda_v$ d'après le th.8.1 .

11. Exemple des corps de nombres

1) Si $K = \mathbb{Q}$, $|x| = \prod_p p^{\omega_2(x)}$, où p parcourt les nombres premiers donc : $\log |x| = - \sum_p \log p \; v_p(x)$, et en considérant

.....

l'ensemble propre M^* des valeurs absolues v_i^* définies par $v_\infty^* = v_\infty$ et $v_p^* = v_p \log p = -\omega_p \log p$, on a : $\sum_{v^* \in M^*}{}' v(x) = 0$ pour tout $x \in \mathbb{Q}$ donc M^*, satisfait la formule du produit.

2) Si K est un corps de nombres algébriques avec $[K : \mathbb{Q}] = n < +\infty$ les valeurs absolues w de K prolongeant les valeurs absolues de M^* satisfont une formule du produit avec les coefficients n_{w/v^*} d'après le §.10. L'ensemble des valeurs absolues équivalentes $w^* = n_{w/v^*} \cdot w$ satisfait la formule du produit.

Définition 11.3 Soient K un corps de nombres algébriques avec $[K : \mathbb{Q}] = m < +\infty$ et A les entiers de K. Pour tout idéal $\underline{a}$ de A, on appelle norme de $\underline{a}$; $N(\underline{a})$, le cardinal de $A/\underline{a}$.

Reprenons la factorisation de $\underline{a}$ dans l'anneau de Dedekind A: $\underline{a} = \prod_{\underline{p}} \underline{p}^{\omega_{\underline{p}}(\underline{a})}$ alors $\underline{a} \subset \underline{p}^{\omega_{\underline{p}}(\underline{a})}$ et les homomorphismes canoniques $A/\underline{a} \longrightarrow A/\underline{p}^{\omega_{\underline{p}}(\underline{a})}$ induisent un isomorphisme $A/\underline{a} \longrightarrow \prod_{\underline{p}} A/\underline{p}^{\omega_{\underline{p}}(a)}$, cet homomorphisme est injectif puisque $\underline{a} = \bigcap_{\underline{p}} \underline{p}^{\omega_{\underline{p}}(\underline{a})}$ et surjectif d'après le théorème d'approximation; d'où $N(\underline{a}) = \prod_{\underline{p}} N(\underline{p}^{\omega_{\underline{p}}(a)})$.

Nous avons $A \supset \underline{p} \supset \underline{p}^2 \supset \ldots\ldots \supset \underline{p}^{\omega_{\underline{p}}(a)}$ et les $\underline{p}^i/\underline{p}^{i+i}$ sont des $A/\underline{p}$ espaces vectoriels de dimension 1 car il n'y a

.....

aucun idéal entre $\underline{p}^i$ et $\underline{p}^{i+1}$; donc $A/\underline{p}^{\omega_{\underline{p}}(\underline{a})}$ est isomorphe à $(A/\underline{p})^{\omega_{\underline{p}}(\underline{a})}$ et $N(\underline{p}^{\omega_{\underline{p}}(\underline{a})}) = N(\underline{p})^{\omega_{\underline{p}}(\underline{a})}$. Le diagramme

$$\begin{array}{ccc} A & \longrightarrow & A/\underline{p} \\ \downarrow & & \vdots \\ A_{\underline{p}} & \longrightarrow & A/_{\underline{p}}/\underline{p}A_{\underline{p}} \end{array}$$

se complète en un isomorphisme

$$A/\underline{p} \longrightarrow A_{\underline{p}}/\underline{p}A_{\underline{p}}$$

ainsi

$$\boxed{\begin{array}{l} N(\underline{a}.\underline{b}) = N(\underline{a})\ N(\underline{b}) \\ N(\underline{p}) = p^{f\underline{p}} \quad \text{où} \quad (p) = \underline{p} \cap \mathbb{Z} \end{array}} \quad (p \text{ nombre premier de } \mathbb{Z})$$

En particulier $N(\underline{a}) = \prod_{\underline{p}} p^{f_{\underline{p}}\,\omega_{\underline{p}}(\underline{a})}$ et donc <u>$N(\underline{a})$ est fini</u> puisque $\omega_{\underline{p}}(\underline{a})$ est nul pour presque tout $\underline{p}$.

Revenons alors à l'ensemble M_K^* des w^* de l'exemple 2. Si w^* est archimédienne les complétés sont isomorphes à $\mathbb{R}$ pour $\mathbb{Q}$ et à $\mathbb{R}$ ou $\mathbb{C}$ pour K ; donc n_{w^*} sera égal à 1 ou 2. Si w^* est archimédienne, soit $\underline{p}$ l'idéal de la valuation $\omega^* = -w^*$, alors ω^* prolonge $-n_{\underline{p}}(\log p)v_p$, où $(p) = \underline{p} \cap \mathbb{Z}$ et $n_{\underline{p}} = n_{w^*}$. Soient $\omega'_{\underline{p}}$ le prolongement de ωp d'idéal $\underline{p}$, et $\omega_{\underline{p}}$ la valuation normée d'idéal $\underline{p}$; on a : $e_{\underline{p}}\,\omega'_{\underline{p}} = \omega_{\underline{p}}$, avec $e_{\underline{p}} = e_{w/v}$,

et $\omega^* = -n_{\underline{p}}(\log p)\omega'_{\underline{p}} = -f_{\underline{p}}(\log p)\omega_{\underline{p}}$

ainsi $|\ |_{w^*} = (p^{f\underline{p}})^{-\omega_{\underline{p}}} = (N(\underline{p}))^{-\omega_{\underline{p}}}$.

<u>Remarque</u> : Si un idéal $\underline{a}$ est <u>principal</u> avec pour générateur α alors $N(\underline{a}) = |N_{K/\mathbb{Q}}(\alpha)|$. Il en résulte que α est inversible dans A si et seulement si $|N(\alpha)| = 1$.

.....

En effet, pour tout nombre premier p dans $\mathbb{Z}$ on a $\omega_p(N(\alpha)) = \sum_{\underline{p}\setminus p} n_{\underline{p}}\,\omega'_{\underline{p}}(\alpha)$ d'après le th.8.1 ; or,

$$\omega_p(N(\underline{a})) = \sum_{\underline{p}\setminus p} f_{\underline{p}}\,\omega_{\underline{p}}(\underline{a}) \quad \text{et} \quad \omega_{\underline{p}}(\underline{a}) = e_{\underline{p}}\,\omega'_{\underline{p}}(\alpha) .$$

THEOREME 11.1 (Finitude du groupe des classes d'idéaux)

Soient K un corps de nombres algébriques avec $[K : \mathbb{Q}] = n < +\infty$, A la fermeture intégrale de $\mathbb{Z}$ dans K, I le groupe des idéaux fractionnaires non nulles de A, P le sous-groupe des idéaux fractionnaires principaux. Alors I/P (qu'on appelle groupe des classes d'idéaux de A) est un groupe fini.

Nous allons montrer qu'il existe un ensemble S fini d'idéaux fractionnaires de A tel que tout idéal soit de la forme $\underline{a} = \underline{a}_o\,.(x)$ où $\underline{a}_o \in S$. Il suffit de le prouver pour les idéaux entiers puisque tout idéal fractionnaire est de la forme $(d^{-1})\,\underline{b}$ où $\underline{b}$ est un idéal entier. Or A étant un module libre de rang n sur $\mathbb{Z}$ (E, chap 0, § 3 coroll.2 du th. 4) soit (ω_i), $i \in (1,n)$, une base de A sur $\mathbb{Z}$. Nous désignerons par $S(b)$ l'ensemble des éléments de A de la forme $a_1\omega_1+\ldots+a_n\omega_n$ les $a_i \in (o, [b])$ où $[b]$ est la partie entière de b, alors card $S(b) > b^n$. Soit $\underline{a}$ un idéal entier de A prenons b tel que $b^n = N(a) + 1$. Parmi les éléments de $S(b)$ il y en a deux y et z au moins dans la même classe modulo $\underline{a}$, et $x = y-z \in \underline{a}$ donc $(x) \subset \underline{a}$; ainsi (x) est multiple de $\underline{a}$, de la forme $(x) = \underline{a}.\underline{b}$ où $\underline{b}$ est idéal entier $\neq 0$. Or $|N(x)| = N(\underline{a}.\underline{b}) = N(a).\ N(b)$ et $|N(x)| = (b^n-1)N(\underline{b})$ comme $|N(x)| = \prod_\sigma |a_1\,\omega_1^\sigma+\ldots+a_n\,\omega_n^\sigma|$ on a

.....

$N(x) \leq C\, b^n$ avec $C = b^n \sup_i |\omega_i|$ donc $N(\underline{b})$ est majoré par $2C$ car $\frac{b^n}{b^n-1} = 1 + \frac{1}{N(\underline{a})} \leq 2$.

Comme $N(\underline{b}) = \prod_{\underline{p}} p^{f_{\underline{p}} \omega_{\underline{p}}(\underline{b})}$ il n'y a qu'un nombre fini de nombres premiers p tels que $\omega_{\underline{p}}(\underline{b}) \neq o$ et un nombre fini de possibilités pour chaque exposant; ainsi le nombre de possibilités pour $\underline{b}$, donc pour $\underline{b}^{-1}$, est fini.

THEOREME 11.2 (Dirichlet)

Soient K un corps de nombres, A l'anneau des entiers de K, U le groupe des unités de A (i.e des éléments inversibles de A, μ le sous-groupe de U des racines de l'unité dans A. Alors μ est fini et le groupe U/μ est libre à $s-1$ générateurs où s est le nombre des valeurs absolues archimédiennes non équivalentes de K .

Remarques: On obtient les valeurs absolues archimédiennes de K en le plongeant dans $\mathbb{C}$ par les $\mathbb{Q}$ isomorphismes σ .
On a $v_\sigma(x) = \log |x^\sigma|$.

s est le nombre des isomorphismes distincts modulo le R automorphisme de $\mathbb{C}$. Si tous les conjugés sont réels $s = [K : \mathbb{Q}]$; autrement, s'il y a des conjugés imaginaires, seulement la moitié d'entre eux donneront des v_σ distinctes.

Le théorème des unités assure que U/μ est un groupe libre de rang $s-1$ et ainsi il existe des unités (u_i); $i \in (1, s-1)$ telles que tout $u \in U$ s'écrit de manière unique $u = \xi\, u_1^{m_1} \ldots u_{s-1}^{m_{s-1}}$ où ξ est racine de l'unité. Nous prouverons uniquement que U/μ est un groupe libre de rang au

....

plus s-1 .Nous ne donnons pas la démonstration (plus difficile) de l'égalité dont nous n'aurons pas besoin par la suite.

LEMME : Le nombre des x dans A tels que $v_\sigma(x) \leqslant C$ pour tout σ est fini.

En effet les coefficients du polynôme minimal de x sont bornés en valeur absolue, comme fonctions symétriques des racines, et le degré de ce polynôme est borné par $[K : \mathbb{Q}]$; donc il n'y a qu'un nombre fini de polynômes possibles pour x.

COROLLAIRE : $v_\sigma(x) = o$ pour tout σ équivaut à x est racine de l'unité.

D'après le lemme, le sous-groupe $\bigcap_\sigma \operatorname{Ker} v_\sigma$ est fini, donc de rang fini; il est donc formé de racines de l'unité et elles sont en nombre fini.

Maintenant à tout $u \in U$, faisons correspondre le point de $\mathbb{R}^s$ de coordonnées les $v_\sigma(u)$; comme $\bigcap_\sigma \ker v_\sigma = \mu$ on en déduit un isomorphisme du groupe multiplicatif U/μ dans un sous-groupe additif Δ de $\mathbb{R}^s$. Or Δ n'a qu'un nombre fini de points communs avec tout domaine borné de $\mathbb{R}^s$, d'après le lemme; donc Δ est un sous groupe discret de $\mathbb{R}^s$; c'est donc un groupe libre de rang au plus s . Mais u étant inversible $|N(u)| = 1$ et par conséquent $\sum_\sigma n_\sigma v_\sigma(u) = o$ avec $n_\sigma = 1$ ou 2 . Δ est donc dans un hyperplan de $\mathbb{R}^s$ déterminé par cette relation de dépendance et peut être engendré par s-1 générateurs.

I2 - Formule du produit (cas des corps de fonctions) .

Définition - I2.1 Diviseurs premiers rationnels . Soient T une variété, et W une sous-variété de codimension 1 de T, simple sur T . L'anneau local $\underline{o}$ (W,T) est un anneau de valuation discrète; on note ω_W la valuation normée correspondante (cf. E,III,10,th 10) . Si T est non singulière en codimension 1, et si f est une fonction sur T, le diviseur de f s'écrit sous la forme

$$(1) \quad \mathrm{div}\,(f) = \sum_W \omega_W(f)\, W$$

où W parcourt l'ensemble des sous-variété de codimension 1 de T (rappelons que l'hypothèse "T non singulière en codimension 1" entraîne l'existence d'un isomorphisme canonique $D \longrightarrow \mathfrak{X}(D)$ du groupe $\mathcal{D}(T)$ des diviseurs sur T sur celui des cycles de codimension 1 (diviseurs "à la Weil") sur T; On convient d'identifier canoniquement D et son image $\mathfrak{X}(D)$.

Si k est un corps de définition de T, on a, pour f définie sur k , une décomposition de div (f) analogue à (1), formée de termes rationnels sur k , à la condition d'introduire la notion de diviseur premier rationnel sur k .On note $\mathcal{D}(T)_k$ le groupe des diviseurs sur T, rationnels sur k ; c'est un sous-groupe du groupe des diviseurs $\mathcal{D}(T)$. Le groupe $\mathcal{D}(T)_k$ est ordonné et, de plus, réticulé; si D_1 et D_2 appartiennent à $\mathcal{D}(T)_k$, il en est de même de sup (D_1, D_2) : en effet, si W est une sous-variété de T, et si f_1 et f_2 sont des fonctions définies sur k représentant respectivement D_1 et D_2 dans un même ouvert rencontrant W , le diviseur

...

sup (D_1, D_2) est représenté par f_1 ou par f_2 suivant que $\omega_W(f_1) > \omega_W(f_2)$ ou que $\omega_W(f_2) \leq \omega_W(f_1)$. Donc $\mathcal{D}(T)_k$ est un <u>sous-groupe réticulé</u> de $\mathcal{D}(T)$.

On appelle <u>diviseur premier rationnel de T sur k</u> un élément <u>extrémal</u> du groupe réticulé $\mathcal{D}(T)_k$, c'est-à-dire un diviseur $P > 0$ sur T, rationnel sur k, et tel que $P = P_1 + P_2$ avec P_1 et $P_2 \geqslant 0$, rationnels sur k, entraîne $P_1 = 0$ ou $P_2 = 0$. Comme tout ensemble non vide d'éléments positifs de $\mathcal{D}(T)_k$ possède un élément minimal (condition MIN de Bourbaki, Alg. VI, 1, I3), tout diviseur $D \in \mathcal{D}(T)_R$ s'écrit d'une et d'une seule manière sous la forme $D = \sum_P \nu_P(D)\, P$ où la somme est étendue à tous les diviseurs premiers rationnels sur k, où les $\nu_P(D) \in \mathbb{Z}$ et sont presque tous nuls. Il résulte aussitôt des définitions que l'application $\omega_P : \mathcal{F}_k(T)^* \longrightarrow \mathbb{Z}$ obtenue en posant $\omega_P(f) = \nu_P(\mathrm{div}(f))$ est une <u>valuation</u> du corps $\mathcal{F}_k(T)$ des fonctions sur T, définies sur k; on a en outre, avec cette notation : $\mathrm{div}(f) = \sum_P \omega_P(f)\, P$. Remarquons que si k est algébriquement clos, les diviseurs premiers rationnels sur k s'identifient aux sous-variétés de codimension 1 définies sur k.

Si P est un diviseur premier rationnel de T sur k, son support S est nécessairement k irréductible, donc si W est l'une des composantes irréductibles (au sens absolu) de S, l'ensemble S est la réunion des variétés W^σ

.....

conjuguées de W sur k. Or P est invariant par tout k automorphisme σ de $\bar{k}$, donc chacune des W^σ a le même coefficient dans P, donc P est de la forme $P = \nu \sum_\sigma W^\sigma$.

Le coefficient ν est en outre une puissance de l'exposant caractéristique p. En effet, soit k' le sous-corps de $\bar{k}$ formé des éléments invariants par les k - automorphismes laissant fixes chacun des W^σ ; pour tout σ, W^σ est une k'- variété, donc est une variété (au sens absolu) définie sur une extension radicielle k'' de k'. Si $p^{h'} = [k'':k']$, le diviseur $p^{h'} \sum_\sigma W^\sigma$ est rationnel sur k. On a donc bien nécessairement $P = p^h \sum_\sigma W^\sigma$ où h est un entier ($\leq h'$).

Remarquons que la valuation ω_P est équivalente à la valuation induite sur $\mathcal{F}_k(T)^*$ par ω_W. Plus précisément, on a, pour $f \in \mathcal{F}_k(T)^*$, la relation $\omega_P(f) = p^h \omega_W(f)$, de sorte que p^h s'interprète comme l'indice de ramification relatif à ω_W/ω_P

Cet entier p^h est appelé <u>l'ordre d'inséparabilité de W</u> (pour une autre définition, voir Weil, Foundations, V, 1). Bien entendu, toute sous-variété de codimension 1 de T définie sur k est un diviseur premier rationnel P particulier, et on a alors $\omega_P = \omega_W$. Il résulte du théorème 7.2 que toutes les valuations de la forme ω_P ou ω_W sont well-behaved, donc la famille des valeurs absolues $v_P = e^{-\omega_P}$ est propre.

.....

Formule du produit pour le corps des fonctions sur une courbe :

Prenons pour T une courbe complète et sans point multiple. Le degré de tout diviseur d'une fonction f sur T est nul (V A, II, 7, th.5, coroll.), et on a donc

$$\sum_a v_a(f) = 0$$

où a parcourt l'ensemble de tous les points de T, et où l'on note v_a la valeur absolue $-\omega_a$. Autrement dit, la famille $\{v_a\}$ vérifie la formule du produit.

Si k est un corps de définition de T, on a de même pour $f \in \mathcal{F}_k(T)^*$,

$$\sum_P v_P(f) \deg P = 0$$

où P parcourt l'ensemble des diviseurs premiers de T rationnels sur k, et où $v_p = -\omega_p$. Autrement dit, la famille $\{v_P\}$ vérifie la formule du produit avec les coefficients $\deg P$.

DEFINITION I2 - Degré projectif. Soit d'abord T une variété affine $(T \subset \mathfrak{S}_n)$, de dimension r, définie sur un corps k. On appelle sous-variété linéaire générique de $\mathfrak{S}_n$ sur k toute variété linéaire $L = L_{u,v}$ définie par un système d'équations de la forme

$$(2) \quad \sum_{i=1}^{n} u_{ij} X_i = v_j \qquad (1 \leqslant j \leqslant n-s)$$

où les u_{ij}, v_j sont algébriquement indépendants sur k.

On a nécessairement $\dim L = s$; si $s = n-r$, l'intersection $T \cap L$ est nécessairement de dimension 0,

.....

i.e. composée de points. Si x est un tel point, les v_j appartiennent à $k(u,x)$, donc le degré de transcendance de $k(u,x)/k(u)$ est $\geqslant r$ et par suite x est générique de T sur $k(u)$. Les autres points de $T \cap L$ sont les conjugués de x sur $k(u,v)$. En effet, un tel conjugué appartient à l'intersection, et inversement, si x' appartient à celle-ci, x' est conjugué de x sur $k(u)$, donc on peut trouver une place ρ du domaine universel Ω, triviale sur k, telle que $\rho(u_{ij}) = u_{ij}$ et $\rho(x) = x'$; les relations exprimant l'appartenance de x et x' à L entraînent alors $\rho(v) = v$, donc x' est bien conjugué de x sur $k(u,v)$.

D'après la démonstration du lemme de normalisation (E,I,4) et (E,IV.4), l'extension $k(u,v,x)/k(u,v)$ est algébrique séparable; son degré d est donc égal au nombre des points de $T \cap L$. Ce nombre ne dépend pas du choix de la famille de coefficients (u,v), car toute famille (u',v') analogue s'en déduit par application d'un k-automorphisme de Ω. Le nombre d est appelé <u>degré</u> de T ; il est > 0, car on peut réaliser la construction en partant de x générique de T sur k, puis en prenant arbitrairement des u_{ij} algébriquement indépendants sur $k(x)$, et en posant : $\sum u_{ij} x_i = v_j$; On a ainsi $x \in T \cap L$, ce qui entraîne bien $d > 0$.

Supposons maintenant que T est une variété <u>projective</u> $(T \subset \mathbb{P}_n)$ de dimension r. On appelle <u>sous-variété linéaire générique</u> de $\mathbb{P}_n$ toute sous-variété linéaire $L = L_u$ de de $\mathbb{P}_n$ définie par un système d'équations de la forme

.....

$$(2)\quad \sum_{i=0}^{n} u_{ij} X_i = 0 \qquad (1 \leqslant j \leqslant n-s)$$

On a dim L = s . Si s = n-r, l'intersection $T \cap L$ est encore de dimension 0. Il résulte de l'étude faite ci-dessus dans le cas affine que chacun des composants x de cette intersection est générique de T sur k, que le nombre d de ces points ne dépend pas du choix de u, et qu'on a $d = \left[k(x,u) : k(u)\right]$. Le nombre d est appelé <u>degré</u>, ou <u>degré projectif</u> de T .

Si T (affine ou projective) est non singulière en codimension 1, et si $D = \sum_W \nu_W (D)\, W$ est un diviseur sur T , on définit le degré de D en prolongeant par linéarité la définition précédente, i.e. en posant

$$\deg D = \sum_W \nu_W (D) \deg W .$$

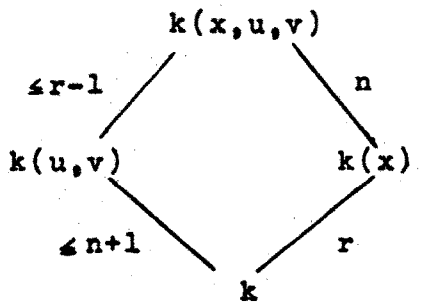
<u>THEOREME I2. 1</u> (irréductibilité d'une section hyperplane générique) . Soit T une varieté affine (resp.projective) définie sur k, de dimension $\geqslant 2$. L'intersection de V avec un hyperplan générique $H = H_{uv}$ (resp. $H = H_u$) sur k d'équation $\sum u_{ij} X_i = v_j$ (resp. $\sum u_i X_i = 0$) est une sous-variété T' de codimension 1 de T , définie sur k(u,v) (resp : k(u)) .

<u>Démonstration</u> - Il suffit de traiter le cas où T est affine. D'autre part, la propriété de l'énoncé est indépendante du choix de la famille de coefficients (u,v), car pour toute famille analogue (u',v'), il existe un k - isomorphisme de Ω appliquant (u,v) sur (u',v') . Partons de x générique de T sur k, et prenons H "générique passant par x", i.e.

.....

prenons les u_i génériques indépendants sur $k(x)$ et définissons v par $v = \sum u_i x_i$. Alors on a $x \in T \cap H$. Comme T n'est pas réduite à un point, et d'après le choix de H, on a $T \not\subset H$.

La comparaison des degrés de transcendance des extensions intervenant dans le diagramme

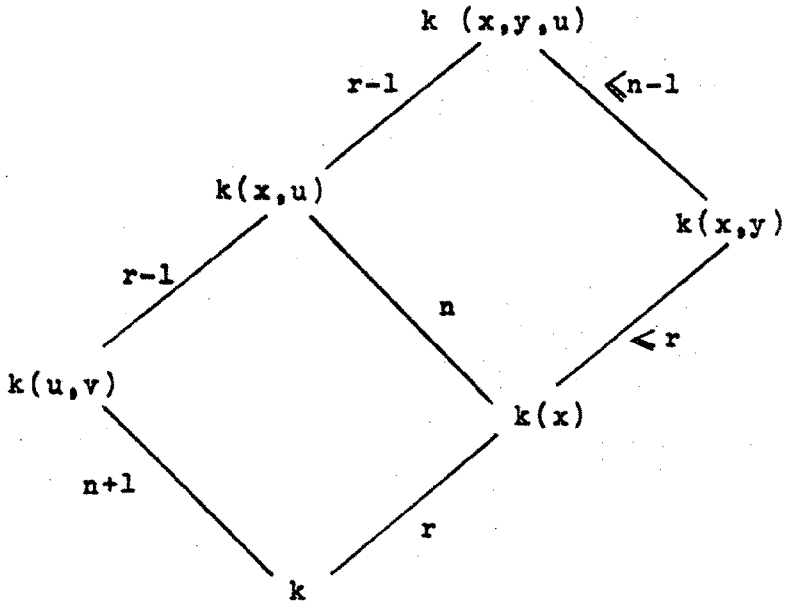


montre qu'on a nécessairement les égalités
deg. tr. $(k(u,v)/k) = n+1$ (de sorte que H est bien générique sur k) et deg.tr. $(k(x,u,v) / k(u,v)) = r - 1$; donc le lieu Z de x sur $k(u,v)$ est une sous-$k(u,v)$-variété de codimension 1 de T , contenue dans $T \cap H$. Pour $z \in T \cap H$, on peut spécialiser x en z sur $k(u)$ (puisque x est générique de T sur $k(u)$); en écrivant que $z \in H$, on voit que v est invariant par cette spécialisation, donc que $z \in Z$. On a donc $T \cap H = Z$.

Nous allons montrer que Z est une variété (i.e. est irréductible au sens absolu) . Pour cela, considérons un point y générique sur $\overline{k(u,v)}(x)$ de l'une des composantes de Z .

La comparaison des degrés de transcendance des extensions intervenant dans le diagramme

.....



montre qu'on a nécessairement les égalités

deg.tr. $(k(x,y) / k(x))$ = r et

deg.tr. $(k(x,y,u) / k(x,y))$ = n-1

Cette dernière égalité entraîne que x et y sont génériques indépendants de T sur k .

Supposons que Z ait plusieurs composantes distinctes. Soit Y la composante de Z contenant x, et soit $Y' \neq Y$ une autre composante. Soit y (resp. y') un point générique de Y (resp.Y') sur k (u,x) . On peut spécialiser y en y' sur k (u,x), et comme : $\sum u_i x_i = \sum u_i y_i = \sum u_i y'_i = v$, cette spécialisation laisse v invariant; on peut la prolonger à un automorphisme σ de Ω . Comme on a $x \in Y$, on a $x^\sigma = x \in Y^\sigma$, d'où $Y^\sigma = Y$; Comme $y \in Y$, on a $y^\sigma = y' \in Y^\sigma$ d'où $Y^\sigma = Y' = Y$, ce qui est contradictoire.

Donc, Z est l'unique composante de $T \cap H$. Pour voir

.....

que Z est une variété définie sur k(u,v) il suffit de prouver que l'extension transcendante $k(x,u,v)/k(u,v)$ est séparable. Or on a vu plus haut, dans la définition du degré, que si $L' = L_{u',v'}$ est la variété linéaire intersection de r hyperplans génériques H_j indépendants, l'extension k(x,u'v') / k(u'v') est algébrique séparable. On peut supposer que H figure parmi les H_j . L'extension k(u',v') /k(u,v) est alors transcendante pure, donc séparable. Donc l'extension k(x,u',v') /k(u,v) est séparable, et il en est de même de k(x,u,v) / k(u,v), c.q.f.d.

COROLLAIRE - Avec les notations du théorème, on a

$$\deg T' = \deg T$$

En effet, si L' est une sous-variété linéaire générique de H sur k(u), c'est aussi une sous-variété linéaire générique de $\mathbb{S}_n$ (resp $\mathbb{P}_n$) sur k. Il suffit de prendre

$$\dim L' = n-r, \text{ et de remarquer que}$$

$$L' \cap T' = L' \cap T$$

Formule du produit pour le corps des fonctions sur une variété de dimension quelconque:

THEOREME I2, 2 - Soit T une variété projective non singulière en codimension 1 . Pour toute fonction f sur T , on a deg div (f) = 0 .

DEMONSTRATION - On raisonne par récurrence sur r = dim T; le résultat est déjà démontré pour r = 1 . Soit k un

.....

corps de définition algébriquement clos pour T et f. Introduisons un hyperplan générique $H = H_u$ sur k. La fonction f' induite par f sur la variété $T' = T \cap H$ est définie. Si W est une sous-variété de codimension 1 de V, définie sur k, l'intersection $W \cap H$ est une sous-variété de codimension 1 de W. Montrons, plus précisément que W' s'identifie au diviseur induit par W, regardé comme diviseur sur T. En effet, soit g (resp. h) un paramètre uniformisant, défini sur k (resp. sur $k(u)$) de T en W (resp. en T'). Le fait que H est générique entraîne que les différentielles $(dg)_{W'}$ et $(dh)_{W'}$ sont linéairement indépendantes; il en résulte $(dg')_{W'} \neq 0$, où g' est la fonction induite par g sur T', de sorte que W' regardé comme diviseur sur T', est représenté par g' en W', donc est bien induit par W. Puisqu'on a $\operatorname{div}(f) = \sum_W \omega_W(f)\, W$, on a aussi $\operatorname{div}(f') = \sum_W \omega_W(f) W'$ (d'où $\omega_{W'}(f') = \omega_W(f)$ quelle que soit W); comme $\deg W' = \deg W$, d'après le coroll. du th. précédent, on a $\deg \operatorname{div}(f) = \deg \operatorname{div}(f')$, et il suffit d'appliquer l'hypothèse de récurrence.

D'après de théorème, on a, pour toute fonction $f \in \mathcal{F}_k(T)$, la formule

$$\sum_P v_P(f) \deg P = 0,$$

où la somme est étendue à tous les diviseurs premiers rationnels de T sur k. Autrement dit, la famille des valeurs absolues v_P vérifie la <u>formule du produit</u> avec

.....

pour coefficients les entiers deg P .

Remarque - Si T est une courbe, la famille $\{v_p\}$ est déterminée par la connaissance du corps de fonctions $K = \mathcal{F}_k(T)$: elle se compose de toutes les valeurs absolues de K triviales sur k . Il n'en est plus de même si dim $T \geqslant 2$; dans ce cas, la famille $\{v_p\}$ et la formule du produit, qui lui correspond, dépendent du modèle projectif choisi.

CHAPITRE II

HAUTEURS

1 - Définitions

Soit K_o un corps muni d'un ensemble propre de valeurs absolues M_o vérifiant la formule du produit, (chap. I § IO), soit x un point de l'espace projectif P_m, rationnel sur la clôture algébrique $\overline{K}_o$ de K_o, et soit $(x_o, \ldots, x_m)$ un système de coordonnées homogènes de x, appartenant à une même extension algébrique k de K_o, de degré fini n. Le nombre réel :

$$h(x) = \frac{1}{n} \sum_{w \in M_k} n_w \sup_{i \in (o,m)} w(x_i)$$

ne dépend que de x, mais non du choix des coordonnées x_i, ni de celui du corps K.

En effet, si l'on choisit un autre système de coordonnées homogènes pour x, h(x) est invariant car M_K satisfait la formule du produit avec les coefficients n_w ; si l'on change de corps, on peut supposer que $K' \supset K$, or avec

$$h'(x) = \frac{1}{n'} \sum_{w' \in M_{K'}} n_{w'} \sup_{i \in (o,m)} w'(x_i) \qquad \text{où} \quad n' = \left[K' : K_o \right]$$

et $x_i \in K$, si w' prolonge w on a : $w'(x_i) = w(x_i)$ donc:

$$h'(x) = \frac{1}{n'} \sum_{w \in M_k} n_w \sum_{w'/w} n_{w'/w} \sup_i w(x_i)$$

.....

ainsi

$$h'(x) = \frac{1}{n'} \sum_{w \in M_K} n_w \sup_i w(x_i) \sum_{w'/w} n_{w'/w}$$

$\sum_{w'/w} n_{w'/w} = \left[K':K\right]$ puisque M_K étant propre les $w \in M_K$ sont "well behaved" ; d'où $h'(x) = h(x)$.

N.B. - La définition précédente n'est pas conforme à la terminologie habituelle, où intervient la notation multiplicative.

Remarque :

$h(x) \geqslant o$ car x peut toujours être représenté par des coordonnées x_i dont l'une au moins est égale à 1, alors

$$h(x) = \frac{1}{n} \sum_{w \in M_K} n_w \sup w^+(x_i) \quad \text{où } w^+ = \sup(v,o)$$

Si $x \in \mathbb{S}_m$ avec pour coordonnées $x = (x_1,\ldots,x_m)$ on définit $h(x)$ par : $h(x) = h(x')$ où x' est le point de $\mathbb{P}_m$ de coordonnées $(1,x_1,\ldots,x_m)$ donc :

$$h(x) = \frac{1}{n} \sum_{w \in M_K} n_w \sup_{i \in (1,m)} w^+(x_i) .$$

En particulier , on définit la hauteur d'un élément de K en l'identifiant à un point de $\mathbb{S}_1$ et si $x \in K$ on a :

$$h(x) = \frac{1}{n} \sum_{w \in M_K} n_w \, w^+(x)$$

.....

Si x est rationnel sur K_o alors :

$$h(x) = \sum_{v \in M_o}{}' \sup_i v^+(x_i)$$

Soit $x \in \mathbb{P}_m$ avec pour coordonnées $(x_o, \ldots, x_m)$; soit σ un K_o - automorphisme de $\overline{K}_o$; désignant par x^σ le point de $\mathbb{P}_m$ de coordonnées $(x_o^\sigma, \ldots, x_m^\sigma)$ on a $\underline{h(x^\sigma) = h(x)}$. En effet, si l'on pose $w^\sigma(x) = w(x^\sigma)$, l'application $w \longmapsto w^\sigma$ est une bijection de $M_K\sigma$ sur M_K, et on a $n_w\sigma = n_w$.

Exemple

Prenons $K_o = \mathbb{Q}$; si x est un point de $\mathbb{P}_m$ rationnel sur $\mathbb{Q}$, on peut choisir ses coordonnées dans $\mathbb{Z}$ et supposer les x_i premiers entre eux, donc $\sup_i v_p(x_i) = o$ et

$$h(x) = \sup_i v_\infty(x_i) = \sup_i \log|x_i| ;$$

en conséquence, il n'y a qu'un nombre fini de points rationnels sur $\mathbb{Q}$ de hauteur bornée dans $\mathbb{P}_m$.

Si x est un point de $\mathbb{P}_m$ rationnel sur un corps de nombres algébriques K, avec $\left[K : \mathbb{Q}\right] = n$, on trouve :

$$h(x) = \frac{1}{n} \sum_\sigma{}' \sup_i \log \left| x_i^\sigma \right| - \log N(\underline{d})$$

où σ parcourt les $\mathbb{Q}$ - isomorphismes de K dans $\mathbb{C}$, et où $\underline{d}$ est le p.g.c.d. des x_i dans l'anneau des entiers de K ; si $\underline{d}$ est <u>principal</u> on peut choisir les x_i de telle façon

.....

que $N(d) = 1$.

2. - Hauteur d'un polynôme

Soit (K,v) un corps valué; si $f = \sum_{\nu} a_\nu M_\nu$

où $f \in K\left[X_1,\ldots,X_n\right]$, $a_\nu \in K$ et

$$M_\nu = X_1^{\nu_1} \ldots X_n^{\nu_n}$$

nous posons :

$$\boxed{v(f) = \sup_{\nu} v(a_\nu)}$$

Si v est une valeur absolue ultramétrique de K , $fg^{-1} \longmapsto v(f) - v(g)$ est une valeur absolue ultramétrique de $K(X_1,\ldots,X_n)$; il suffit pour cela de prouver que

$$v(fg) = v(f) + v(g) .$$

LEMME 1 (Gauss)

Soit K un corps muni d'une valuation ω ; posons $\omega(f) = \inf_{\nu} \omega(a_\nu)$ (avec les notations précédentes) alors pour tout $f,g \in K\left[X_1,\ldots,X_n\right]$ on a :

$$\omega(fg) = \omega(f) + \omega(g) .$$

Démonstration :

Le cas $fg = o$ résulte de $\omega(o) = +\infty$; autrement on peut supposer $\omega(f) = \omega(g) = o$ après une multiplication convenable. Considérons l'homomorphisme $f \longmapsto f^\circ$ réduisant les coefficients de $f \in A_\omega\left[X_1,\ldots, X_n\right]$ modulo l'idéal $\underline{m}_\omega$;

on a : $(fg)^\circ = f^\circ g^\circ \neq o$ donc $\omega(fg) = o$.

LEMME 2

Soit (K,v) un corps valué; soit f un polynôme unitaire de $K[X]$ de degré n et soit

$$f(X) = \prod_{i=1}^{n} (X - \lambda i)$$

sa factorisation dans $\overline{K}$, clôture algébrique de K . Supposons v prolongée à $\overline{K}$. Alors

$$\left| v(f) - \sum_i v^+(\lambda_i) \right| \leqslant n \alpha$$

où α est la constante de l'axiome VA.III, à savoir :

$$v(x+y) \leqslant \sup (v(x), v(y)) + \alpha$$

Démonstration:

Si $n = 1$, $f = X - \lambda$ donc $v(f) = v^+(\lambda)$;

Raisonnons par récurrence sur n en décomposant l'inégalité en deux :

$$\sum_i v^+(\lambda_i) - \alpha \leqslant v(f) \leqslant \sum_i v^+(\lambda_i) + n \alpha$$

Soient $f = (X-\lambda_1)\, g = X^n + \sum_{i=1}^{n} a_i X^{n-i}$, $g = X^{n-1} + \sum_{j=1}^{n-1} b_j X^{n-1-j}$

on a : $a_i = b_i - \lambda_1 b_{i-1}$ avec la convention $b_o = 1$, $b_n = o$

D'après le théorème 5.2 du Chap.1 et le théorème d'Ostrowski, le prolongement de v satisfait VA III avec le même α .

Ainsi

$$v(a_i) \leqslant \sup(v(b_i) , v(\lambda_1) + v(b_{i-1})) + \alpha$$

.....

a fortiori

$$v(a_i) \leqslant \sup_i (v(b_i)) + v^+(\lambda_1) + \alpha$$

et avec l'hypothèse de récurrence :

$$v(f) \leqslant \sum_{i=2}^{n} v^+(\lambda_i) + (n-1)\alpha + v^+(\lambda_1) + \alpha .$$

Pour démontrer l'autre inégalité, on peut exclure le cas

$v(\lambda_i) \leqslant \alpha$ pour tout i, car $v(f) > o$ puisque f est unitaire. Supposons $v(\lambda_1) > \alpha$, et choisissons s tel que $v(b_s)$ soit maximum.

$$\lambda_1 b_s = b_{s+1} - a_{s+1}$$

$$v(\lambda_1) + v(b_s) \leqslant \sup (v(b_{s+1}), v(a_{s+1})) + \alpha$$

or

$$v(\lambda_1) + v(b_s) > \alpha + v(b_{s+1})$$

donc

$$v(\lambda_1) + v(b_s) \leqslant v(a_{s+1}) + \alpha$$

d'où

$$v(\lambda_1) + \sup_j v(b_j) \leqslant \sup_i v(a_i) + \alpha$$

avec l'hypothèse de récurrence

$$v(\lambda_1) + \sum_{i=2}^{n} v^+(\lambda_i) - (n-1)\alpha \leqslant v(f) + \alpha$$

or $v(\lambda_1) = v^+(\lambda_1)$; il suffit alors d'ajouter $-\alpha$ aux deux membres de cette inégalité.

.....

THEOREME 2.1

Soient (K,v) un corps valué, f et g deux polynômes non nuls de $K\left[X_1,\ldots, X_n\right]$ si deg f + deg g = deg fg < d alors

$$\left| v(fg) - v(f) - v(g) \right| \leqslant 2\, d^n \alpha$$

Remarque - Si v est ultramétrique $\alpha = o$ et l'on retrouve le lemme de Gauss pour les valuations réelles.

Démonstration -

Cas $n = 1$: Soient (λ_i) les racines de f et (μ_j) celles de g ; on peut supposer f et g unitaire, et d'après le lemme 1

$$| v(f) - \sum_i v^+(\lambda_i) | \leqslant \alpha \deg f$$

$$| v(g) - \sum_j v^+(\mu_j) | \leqslant \alpha \deg g$$

$$| v(fg) - \sum_i v^+(\lambda_i) - \sum_j v^+(\mu_j) | \leqslant \alpha(\deg f + \deg g)$$

d'où

$$| v(fg) - v(f) - v(g) | \leqslant 2\alpha d$$

Cas n quelconque : On considère le K - homomorphisme d'algèbre défini par $X_i \longmapsto Y^{d^{i-1}}$. Lorsque deg $f < d$, f et son image f^* ont les mêmes coefficients car le degré

.....

de M_ν^* image du monôme $X_1^{\nu_1} \ldots X_n^{\nu_n}$ est

$\nu_1 + \nu_2\, d + \ldots + \nu_n\, d^{n-1}$ avec $\nu_n < d$ où l'on reconnait un entier $< d^n$ écrit en base d

$(fg)^* = f^* g^*$ nous ramène au cas $n = 1$.

mais avec un degré $< d^n$.

Définition 2.1

Soit K_o un corps muni d'un ensemble propre de valeurs absolues satisfaisant la formule du produit. Considérons un polynôme $f = \sum_j a_j M_j$ à plusieurs variables,

$M_j = X_1^{j_1} \ldots X_m^{j_m}$, et à coefficients dans la clôture algébrique $\overline{K}_o$ de K_o , donc dans une extension K de degré fini. On appelle hauteur, $h(f)$, de f , la hauteur du point a de coordonnées (a_j) (dans n'importe quel ordre)

Remarque : $h(f)$ ne dépend que de la classe de f pour la relation de divisibilité.

THEOREME 2.2

Avec les notations précédentes, soit d un réel $\geqslant o$, il existe un réel C , tel que pour tout f et $g \in K_o\left[X_1,\ldots,X_m\right]$, satisfaisant deg f + deg $g < d$, on ait : $\left| h(fg) - h(f) - h(g) \right| \leqslant C$

.....

En effet $h(fg)-h(f)-h(g) = \frac{1}{n}\sum_{v} n_v(v(fg)-v(f)-v(g))$

où v parcourt les valeurs absolues archimédiennes de M_K, où K est une extension de degré n fini de K_o contenant les coefficients de f et g ; or il n'y a qu'un nombre fini de valeurs absolues archimédiennes dans l'ensemble propre M_K et $v(fg) - v(f) - v(g)$ est borné d'après le th.2.1.

COROLLAIRE - Soit f_x le polynôme irréductible sur K_o de $x \in \overline{K}_o$, soit d un réel $> o$, il existe un réel C tel que

$| h(f_x) - d\, h(x) | \leqslant C$ pour tous les $x \in \overline{K}_o$ tels que deg $f_x \leqslant d$.

Il suffit de factoriser : $f = \prod (X-x_i)$

THEOREME 2.3

Soient n et d deux entiers, α un nombre réel $> o$. Le nombre des points x de $\mathbb{P}_n$ algébriques sur $\mathbb{Q}$ tels que

$$\left[\mathbb{Q}(x) : \mathbb{Q} \right] \leqslant d \quad \text{et} \quad h(x) \leqslant \alpha$$

est fini.

Remarque: On a démontré ce théorème dans l'exemple du § 1 pour le cas $d = 1$.

.....

Démonstration : Soit $(x_o, \ldots, x_n)$ un système de coordonnées de x, posons $F = x_o X_o + \ldots + x_n X_n$; alors $h(f) = h(x)$, si $F^\sigma = x_o^\sigma X_o + \ldots + x_n^\sigma X_n$; où σ désigne un $\mathbb{Q}$ isomorphisme $h(F^\sigma) = h(F)$

or d'après le th 2.2.

$$h(\prod_\sigma F^\sigma) \leqslant d\, h(F) + C \leqslant d\, \alpha + C$$

or $G = \prod_\sigma F^\sigma \in \mathbb{Q}\left[X_o, \ldots, X_n \right]$ comme $h(G)$ est bornée

G ne peut appartenir qu'à un nombre fini de classes pour la relation de divisibilité, d'après la remarque ci-dessus; F doit être un diviseur de G dans l'anneau factoriel $\bar{\mathbb{Q}}\left[X_o, \ldots, X_n \right]$, donc à un facteur dans $\bar{\mathbb{Q}}$ près, il ne peut prendre qu'un nombre fini de valeurs.

3. Hauteurs sur les corps de fonctions

Soit T une variété projective $(T \subset \mathbb{P}_n)$ définie sur un corps k, non singulière en codimension 1, et soit K le corps des fonctions $\mathcal{F}_k(V)$. Ce corps K est aussi isomorphe à $k(t)$, t étant un point générique de T sur k. Soit M la famille des valeurs absolues v_P respectivement associées aux diviseurs premiers rationnels P de T sur k. On a vu que cette famille est propre et vérifie la formule du produit avec les coefficients deg P. Si x est un point de $\mathbb{P}_n$ rationnel sur K, il admet un

.....

système de coordonnées $(x_o,\ldots, x_m)$ où les $x_i \in K$,et on a :

$$h(x) = \sum_P{}' \deg P \sup_i v_P(x_i)$$

La donnée du point x est équivalente à la donnée d'une application φ rationnelle de T dans $\mathbb{P}_n$, à savoir celle qui au point générique t de T associe le point w de $\mathbb{P}_n$ dont un système de coordonnées est $(x_o(t),\ldots,x_n(t))$.

On peut en outre choisir les x_i de façon que les $\operatorname{div}(x_i)_o$ n'aient pas de composante commune. On a, dans ces conditions

THEOREME 3.1

$$h(x) = \deg \sup_i \operatorname{div}(x_i)_\infty$$

On peut supposer $x_o = 1$. Il suffit de montrer que le coefficient de P dans $\sup_i \operatorname{div}(x_1)_\infty$ est égal à $\sup_i v_P(x_i)$. Or le coefficient de P dans $\operatorname{div}(x_i)_\infty$ est $\sup(o, v_P(x_1)) = v_P^+(x_i)$. Donc son coefficient dans $\sup_i(\operatorname{div}(x_i)_\infty)$ est $\sup_i v_P^+(x_i) = \sup_i v_P(x_i)$, puisque $v_P(x_o) = 0$

THEOREME 3.2

Avec les notations précédentes on a $h(x) = \deg \varphi^{-1}(H)$ où H est un hyperplan de $\mathbb{P}_n$ tel que $\varphi^{-1}(H)$ ait un sens (i.e $w \notin H$) .

....

On peut supposer $x_o = 1$. Notons H_i l'hyperplan de $\mathbb{P}_n$ d'équation $X_i = 0$ et si $X = (X_o,\dots,X_n)$ soit

$$F(X) = \sum_{i=o}^{n} a_i X_i = o \quad \text{l'équation de } H .$$

Posons $X_i / F(X) = g_i(X)$; g_i est une fonction sur $\mathbb{P}_n$ qui induit par φ sur T la fonction $g_i \circ \varphi$ que nous noterons y_i . On a $\operatorname{div}(g_i) = H_i - H$. Or il existe i tel que $\varphi^{-1}(H_i)$ soit défini (choisir i tel que $w \notin H_i$) , d'où $\operatorname{div}(y_i) = \varphi^{-1}(H_i) - \varphi^{-1}(H)$. Comme les y_i forment un système de coordonnées homogènes de x , on a d'après le th. 3.1 $h(x) = \deg \sup_i \operatorname{div}(y_i)_\infty$ où l'on ne prend que les $y_i \neq o$, pour lesquels on a

$$\operatorname{div}(y_i)_\infty = \varphi^{-1}(H) - \inf(\varphi^{-1}(H_i), \varphi^{-1}(H)),$$

d'où $\sup_i \operatorname{div}(y_i)_\infty = \varphi^{-1}(H) - \inf(\varphi^{-1}(H), \inf_i \varphi^{-1}(H_i))$.

Or les $\varphi^{-1}(H_i)$ n'ont pas de composante commune Z car si z était un point générique de Z , φ serait morphique en z, et on aurait $\varphi(z) \in H_j$ pour tout $j \in (o,n)$ ce qui est absurde car l'intersection des H_j est vide. On a donc

$\inf_i \varphi^{-1}(H_i) = o$, d'où

.....

$$\sup_i \operatorname{div}(y_i)_\infty = \varphi^{-1}(H) \quad \text{et} \quad R(x) = \deg \varphi^{-1}(H)$$

4 - Propriété des hauteurs

Définition 4.1

Soient K un corps, M un ensemble propre de valeurs absolues de K. On suppose donnée une clôture algébrique $\overline{K}$ de K. On appelle M-diviseur toute application

$$\gamma : M_{\overline{K}} \longrightarrow \mathbb{R}$$

vérifiant les conditions suivantes

(i) pour $v \in M_{\overline{K}}$, $\gamma(v)$ ne dépend que de la valeur absolue v_K induite par v sur K (i.e il existe une application $\gamma_K : M_K \longrightarrow \mathbb{R}$ telle que $\gamma(v) = \gamma_K(v_K)$).

(ii) γ_K s'annule pour presque toute $v \in M_K$.

Remarque : Si L est une extension algébrique de degré fini de K, tout M_K diviseur est un M_L diviseur.

Exemples :

Pour x donné rationnel sur K $\quad x \mapsto v(x)$ est un M-diviseur.

L'application $v \to \alpha(v)$, où $\alpha(v)$ est la constante de l'axiome VA3, est un M_K-diviseur, (puisque $\alpha(v) = 0$ pour les valeurs absolues ultramétriques).

.....

Définition 4.2

Soit E un ensemble. Dans l'ensemble des applications $E \to \mathbb{R}$ la relation d'équivalence "f-g est bornée" est notée $f \asymp g$.

Pour toute variété V définie sur un corps K, on notera V_K l'ensemble des points de V rationnels sur K.

Dans ce qui suit, on se donne un ensemble propre M_o de valeurs absolues vérifiant la formule du produit sur un corps K_o et une clôture algébrique $\overline{K}_o$ de K_o. On désigne par K un sous corps arbitraire de $\overline{K}_o$, et on prend $\overline{K} = \overline{K}_o$.

Soit V une variété définie sur K, et soit φ une application rationnelle $V \to \mathbb{P}_n$. Notons $U = U_\varphi$ l'ouvert de morphicité de φ, i.e l'ouvert composé des points en lesquels φ est morphique. On désigne par h_φ l'application

$$U_{\overline{K}} \to \mathbb{R}$$

définie par $h_\varphi(x) = h(\varphi(x))$.

Rappelons qu'à toute application rationnelle $\varphi: V \to \mathbb{P}_n$, il correspond canoniquement un système linéaire $\mathfrak{L} = \mathfrak{L}\varphi$ sur V, composé de tous les diviseurs de la forme $D = \varphi^{-1}(H)$, où H est un hyperplan de $\mathbb{P}_n$ tel que ce dernier symbole ait un sens, i.e un hyperplan ne contenant pas l'image $W = \varphi_g(V)$. Soit $D_o = \varphi^{-1}(L_o)$ un élément particulier de $\mathfrak{L}\varphi$. Soient respectivement $F_o(X) = o$ et $F(X) = o$ les équations des hyperplans L_o et L

.....

Pour F_o fixée, et F variable, l'ensemble des fonctions $f = (F/F_o) \circ \varphi$ (complété par l'adjonction de la fonction nulle) est un espace vectoriel L sur K, et comme $\mathrm{div}(f) = D - D_o$, $\mathcal{L}$ est le système linéaire associé à L (VA,IV,3). Le système $\mathcal{L} = \mathcal{L}_\varphi$ est défini sur K et de dimension $< n$. Sa classe pour l'équivalence linéaire sera désignée par $\mathcal{C}_\varphi$.

Rappelons que, pour que φ soit un morphisme il faut et il suffit que $\mathcal{L} = \mathcal{L}_\varphi$ soit sans point fixe.

THEOREME 4.1

Soit V une variété complète, normale, définie sur K; soient $\varphi : V \to \mathbb{P}_m$ et $\Psi : V \to \mathbb{P}_n$ deux applications rationnelles. Supposons qu'on ait $\mathcal{C}_\varphi = \mathcal{C}_\Psi$, et que φ soit un morphisme. Alors, pour $x \in (U_\Psi)_{\overline{K}}$, on a :

$h_\Psi(x) \leqslant h_\varphi(x) + C$

où C est une constance indépendante de x.

Lemme 4.1 - Soit V une variété normale et complète définie sur K et soient $f_1, \ldots, f_n$ des fonctions sur V telles que les supports des $\mathrm{div}(f_i)_o$ soient sans point commun. Alors il existe un M - diviseur γ_o tel que, pour toute place $\mathfrak{p}$ du corps de fonctions $\mathcal{F}_K(V)$, à valeurs dans $\overline{K}$,

...

triviale sur K, on ait $\sup_i v(\rho(f_i)) \geqslant \gamma_o(v)$.

En effet, notons x un point générique de V sur K, de sorte que $\mathcal{F}_K(V)$ est isomorphe à $K(x)$. Posons $f_i(x)=u_i$. dans l'anneau $A = K\left[u_1,\ldots,u_n\right]$, l'idéal $I = (u_1,\ldots,u_n)$ est l'idéal trivial ($I = A$). Sinon l'homomorphisme $A \longrightarrow A/I$ serait trivial sur K et s'annulerait en $u_1,\ldots,u_n$. On aurait donc $A/I \simeq K$. On aurait ainsi un homomorphisme $A \longrightarrow K$, trivial sur K, qu'on pourrait prolonger à une place ρ_o de $K(x)$, à valeurs dans le domaine universel. Comme V est complète, ρ_o serait finie en x. Le point $\rho_o(x) = a$ appartiendrait à $\mathrm{div}(f_i)_o$ pour tout i, d'après VA, IV, 5, th 8, équiv. de (b) et (c) .

On a donc $1 \in I$, d'où $1 = \sum a_\nu M_\nu (u_1,\ldots,u_n)$ ou encore $1 = \sum a_\nu M_\nu (f_1,\ldots f_n)$, où les M_ν sont des monômes de degré $\geqslant 1$ et où $a_\nu \in K$. On en déduit, pour toute place ρ de $\mathcal{F}_K(V)$, à valeurs dans $\overline{K}$, triviale sur K

$$1 = \sum a_\nu M_\nu (\rho(f_1),\ldots, \rho(f_n)) .$$

D'où pour $v \in M_K$: $o \leqslant \sup_\nu v(a_\nu) + d \sup_i v(\rho(f_i)) + C_o(v)$

où l'on pose $d = \sup_\nu \deg M_\nu$, et où $C_o(v)$ est un nombre réel qui s'annule pour v archimédienne. D'où le lemme .

.....

Démonstration du th. 4.1 :

Soit H_o un hyperplan de $\mathbb{P}_m$, d'équation $F_o(X) = o$, tel que $D_o = \varphi^{-1}(H_o)$ soit défini. Soit L l'espace vectoriel sur K composé des fonctions f sur V obtenues en relevant les fonctions de la forme F/F_o sur $\mathbb{P}_m$, où F est une forme linéaire arbitraire à coefficients dans K. Le système $\mathcal{L}_\varphi$ est, comme on a vu, associé à L, i.e composé des diviseurs de la forme $D = D_o + \mathrm{div}(f)$ avec $f \in L$. Soit $f_o, \ldots, f_r$ une base de L. On peut supposer $f_o = 1$. On a, pour $i \in (o,r)$

$$\mathrm{div}(f_i) = D_i - D_o$$

avec $D_i \in \mathcal{L}_\varphi$. Puisque φ est un morphisme, $\mathcal{L}_\varphi$ est sans point fixe, donc les D_i, $i \in (o,r)$ sont sans point commun.

Soit de même H'_o un hyperplan de $\mathbb{P}_n$ d'équation $G_o(X) = o$, tel que $E_o = \psi^{-1}(H_o)$ soit défini. Soit M l'espace des fonctions g sur V, définies sur K, obtenues en relevant les fonctions G/G_o sur $\mathbb{P}_n$ (G forme linéaire à coefficients dans K). Le système $\mathcal{L}_\psi$ est composé des diviseurs $E = E_o + \mathrm{div}(g)$, avec $g \in M$. Soit $g_o, \ldots g_s$ une base de M. On peut supposer $g_o = 1$. On a pour $j \in (o,s)$

$$\mathrm{div}(g_j) = E_j - E_o$$

avec $E_j \in \mathcal{L}_\psi$.

.....

Puisque $\mathcal{C}_\varphi = \mathcal{C}_\psi$, il existe une fonction h sur V, définie sur K, telle que

$$\operatorname{div}(h) = E_o - D_o$$

Posant $g'_j = hg_j$

on a $\operatorname{div}(g'_j) = E_j - D_o$

d'où $\operatorname{div}(f_i / g'_j) = D_i - E_j$

Pour j fixé, les $(f_i / g'_j)(x)$ forment un système de coordonnées homogènes du point $\varphi(x)$, pour $x \in$ l'ouvert U_j complémentaire de supp E_j. On a, d'après le lemme 4.1, pour $x \in (U_j)_{\overline{K}}$

$$\sup_i \; v\left((f_i / g'_j)(x) \right) \geqslant c_{oj}(v)$$

où c_{oj} est un M-diviseur indépendant de x.

Si de plus x appartient à l'ouvert T_o complémentaire de supp D_o, les fonctions f_i et g'_j sont définies en x, et on a

$$\sup_i \; v(f_i(x) / g'_j(x)) \geqslant c_{oj}(v)$$

Puisque les U_j recouvrent V, on en déduit, pour tout $x \in (T_o)_{\overline{K}}$,

$$\sup_i \; v(f_i(x)) \geqslant \sup_j \; v(g'_j(x)) + c_o(v),$$

en posant $c_o(v) = \inf_j c_{oj}(v)$.

Par sommation sur v, on en déduit pour tout $x \in (T_o)_{\overline{K}}$, la formule $h_\psi(x) \leqslant h_\varphi(x) + C_o$,

.....

en posant $C_o = -\sum_v c_o(v)$. En supposant au départ $f_i = 1$ et $g_i = 1$, on aurait obtenu de même une inégalité de la forme $h_{\psi}(x) \leqslant h_{\varphi}(x) + C_i$, valable pour tout $x \in (T_i)_{\overline{K}}$, où T_i est l'ouvert complémentaire de supp D_i . Comme les T_i recouvrent V , on en déduit l'inégalité de l'énoncé, avec $C = \sup_i C_i$.

THEOREME 4.2

Soit V une variété définie sur K , et soient $\varphi : V \to \mathbb{P}_m$, $\psi : V \to \mathbb{P}_n$, $\theta : v \to \mathbb{P}_q$ trois morphismes, tels que $\mathcal{C}_\theta = \mathcal{C}_\varphi + \mathcal{C}_\psi$ alors on a :

$h_\theta \approx h_\varphi + h_\psi$

Démonstration : Comme dans la démonstration du th. 4.1 , définissons $\mathcal{L}_\varphi$ et $\mathcal{L}_\psi$ comme associés aux espaces vectoriels L , M sur K , admettant respectivement pour bases $(f_o,\ldots,f_r)$ et $(g_o,\ldots,g_s)$. Posons à nouveau :

$$\mathrm{div}(f_i) = D_i - D_o$$

$$\mathrm{div}(g_j) = E_j - E_o$$

Considérons l'espace vectoriel N sur k engendré par les $f_i\, g_j$. Pour $h \in N$, on a

.....

$$\mathrm{div}(h) = H - D_o - E_o$$

où H est un diviseur positif rationnel sur K, et H décrit un système linéaire $\mathcal{L}'$ (c'est le système linéaire somme de $\mathcal{L}_\varphi$ et $\mathcal{L}_\psi$, i.e. le plus petit système linéaire contenant tous les diviseurs de la forme $D + E$, avec $D \in \mathcal{L}_\varphi$ et $E \in \mathcal{L}_\psi$). Il est clair que $\mathcal{L}'$ est sans point fixe, donc que toute application rationnelle θ' associée à $\mathcal{L}'$ est un morphisme ; par exemple prenons pour θ' l'application qui, au point x fait correspondre le point de $\mathbb{P}_{mn-1}$ ayant pour coordonnées les $f_i\, g_j$. On a, d'après l'hypothèse :

$\mathcal{C}_\theta = \mathcal{C}_{\theta'}$, donc $h_\theta \asymp h_{\theta'}$. D'autre part, pour $x \in V_{\overline{K}}$, rationnel sur $L \subset \overline{K}$ de degré fini n sur K, on a

$$h_{\theta'}(x) = \frac{1}{n} \sum_{v \in M_L} n_v \sup_{i,j} \left(v(f_i(x)) + v(g_j(x))\right)$$

$$= \frac{1}{n} \sum_{v} n_v \left(\sup_i v(f_i(x)) + \sup_j v(g_j(x))\right)$$

$$= h_\varphi(x) + h_\psi(x)$$

CHAPITRE III

LE THEOREME DE MORDELL-WEIL

1 - Descente du corps de base

THEOREME 1.1 - Toute variété V admet un plus petit corps de définition .

Démonstration : Remarquons que V est définie sur un corps de type fini, et que toute suite décroissante de corps de type fini est stationnaire. Il suffit donc de prouver que si V est définie sur deux corps K et K' , elle l'est sur $k = K \cap K'$.

La propriété est vraie lorsque V est une hypersurface de $\mathbb{S}_n$. En effet, V est alors définie par une équation $F(x) = o$. On peut supposer que l'un des coefficients de F est 1 . Tous les coefficients de F appartiennent alors à K et à K' , donc à k .

Supposons V affine quelconque, de dimension r , dans $\mathbb{S}_n$, et soit x un point générique de V sur $L = KK'$. Soient u_{ij} $(1 \leqslant i \leqslant n , \quad 1 \leqslant j \leqslant r + 1)$ des éléments de Ω algébriquement indépendants sur $L(x)$.

.....

Notons y le point de $\mathbb{S}_{r+1}$ de coordonnées

$$y_j = \sum_{i=1}^{n} u_{ij} x_i \qquad (1 \leqslant j \leqslant r+1)$$

Le point x est algébrique séparable sur K (u,y) (cf. démonstration du lemme de normalisation, E I 4 et E IV 4) . Donc le lieu $\tilde{V} = \mathrm{loc}_{k(u)} y$ est de dimension r , i.e. est une hypersurface de $\mathbb{S}_{r+1}$ (dite "projection générique" de V sur $\mathbb{S}_{r+1}$) . Montrons que x est en fait rationnel sur K (u,y) . Sinon en effet il existerait un conjugué x' de x sur K (u,y), distinct de x . On aurait

$$\sum_i u_{ij} (x_i - x'_i) = 0 \qquad (1 \leqslant j \leqslant r+1)$$

Comme $x' \in V$, le degré de transcendance de $K(x',x)/K(x)$ serait $< r$, ce qui est incompatible avec l'indépendance algébrique des u_{ij} sur K .

On a donc prouvé que $K(u,x) = K(u,y)$, i.e. que l'application rationnelle $V \longrightarrow \tilde{V}$ induite par la projection générique est birationnelle, définie sur K (u) . Elle l'est de même sur K'(u) . Donc l'hypersurface $\tilde{V}$ est définie sur $K(u) \cap K'(u)$. Comme k(u,y) est linéairement disjoint de K et de K' sur k , on a $K(u) \cap K'(u) = k(u)$, et $K(u,y) \cap K'(u,y) = k(u,y)$, d'où $k(u,x) = k(u,y)$. Donc V et φ sont définies sur k(u), et on a $V = \mathrm{loc}_{k(u)} x$.

.....

Le corps $k(u,x)$ est extension régulière de $k(u)$, donc de k ; donc $k(x)$ est extension régulière de k. Comme $k(u)$ est linéairement disjoint de $k(x)$ sur k, on a $V = \mathrm{loc}_k x$, donc V est définie sur k.

THEOREME 1.2 (descente du corps de base, d'après A.WEIL). Soient k un corps, K une extension séparable (algébrique ou transcendante) de k, et soit V une variété définie sur K.

Pour tout couple de k-monomorphismes (σ, τ) de K dans le domaine universel Ω, supposons donnée une application birationnelle $\varphi_{\tau\sigma} = V^\sigma \to V^\tau$, de façon que

(a) $-\varphi_{\tau\rho} = \varphi_{\tau\sigma} \circ \varphi_{\sigma\rho}$

(b) - Pour tout k-automorphisme ω de Ω on a $\varphi_{\omega\tau,\,\omega\sigma} = \varphi^{\omega}_{\tau\sigma}$

(où $\omega\tau$, $\omega\sigma$ signifient $\omega\circ\tau$, $\omega\circ\sigma$). Alors

(i) - Il existe une variété W, définie sur k, et une application birationnelle $\psi : W \to V$, définie sur K, telles qu'on ait

(1) $\varphi_{\tau\sigma} = \psi^\tau \circ (\psi^\sigma)^{-1}$

quels que soient σ et τ.

(ii) - Si les $\varphi_{\tau,\sigma}$ sont des isomorphismes, on peut choisir (W, ψ) de façon que ψ soit un isomorphisme.

.....

Remarque 1.1 - Le théorème admet une réciproque évidente : si V est une variété birationnellement équivalente (resp. isomorphe) sur K à une variété W définie sur k, la formule (1) permet de définir une famille de transformations birationnelles (resp. d'isomorphismes) $\varphi_{\tau\sigma}$ vérifiant (a) et (b).

Démonstration : Il suffit d'examiner le cas où V est affine ($V \subset \$_m$) (puisqu'on peut recouvrir V par un nombre fini de K - ouverts affines).

Appelons S l'ensemble des k-monomorphismes $\sigma : K \to \Omega$.

Il résulte de (a) que $\varphi_{\sigma\sigma}$ est l'identité, et que $\varphi_{\sigma\tau} = \varphi_{\tau\sigma}^{-1}$. Soit x un point générique de V sur K. Pour $\sigma \in S$, posons $x_\sigma = \varphi_{\sigma\varepsilon}(x)$, où ε est l'identité. Le point x_σ est générique de V^σ sur K^σ. D'après (a) on a, quels que soient $\sigma, \tau \in S$, la relation $x_\tau = \varphi_{\tau\sigma}(x_\sigma)$.

Il existe, pour tout σ, un et un seul k-isomorphisme $\sigma^* : K(x) \to K^\sigma(x_\sigma)$ prolongeant σ, et tel que $x \mapsto x^\sigma$. Si $\tau \in S$, et si $\overline{\tau}$ est un k-automorphisme de Ω prolongeant τ^*, on a, d'après (a) et (b),

$$x_\sigma^{\overline{\tau}} = \varphi_{\sigma\varepsilon}^{\overline{\tau}}(x^{\overline{\tau}}) = \varphi_{\overline{\tau\sigma},\tau}(x_\tau) = \varphi_{\overline{\tau\sigma},\tau}(\varphi_{\tau\varepsilon}(x)) = \varphi_{\overline{\tau\sigma},\varepsilon}(x)$$

d'où

$$x_\sigma^{\overline{\tau}} = x_{\overline{\tau\sigma}} \qquad (2)$$

Notons L le sous-corps de $K(x)$ formé des éléments invariants par les isomorphismes σ^*, pour $\sigma \in S$. L'extension

L/k est régulière. En effet elle est séparable : les extensions $K(x)/K$ et K/k étant séparables, il en est de même de $K(x)/k$, donc de L/k. De plus, k est algébriquement fermé dans L : en effet, soit $z \in L$, algébrique sur k ; on a aussi $z \in K(x)$, algébrique sur K ; comme l'extension $K(x)/K$ est régulière, on a $z \in k$; pour $\sigma \in S$, on a de plus $z^{\sigma} = z^{\sigma^*} = z$; on a donc $z \in k$.

L'extension L/k est donc de la forme $k(y)/k$, où y est un point générique d'une variété W définie sur k. Notons ψ l'application rationnelle $W \to V$, définie sur k, telle que $\psi(y) = x$.

En utilisant cette construction, nous allons commencer par démontrer le théorème dans les deux cas particuliers suivants

a) - <u>L'extension K/k est algébrique de degré fini séparable</u>. Notons $\tilde{K}$ le composé des corps K^{σ} ; ce composé est une extension galoisienne de k ; désignons par Γ son groupe de Galois. Pour $\tilde{\sigma} \in \Gamma$, induisant σ sur K, il existe un et un seul automorphisme $\tilde{\sigma}^* = \varphi(\tilde{\sigma})$ du corps $\tilde{K}(x)$ prolongeant $\tilde{\sigma}$ tel $x^{\tilde{\sigma}^*} = x_{\sigma}$ (de sorte que $\tilde{\sigma}^*$ est l'unique automorphisme de $\tilde{K}(x)$ prolongeant à la fois σ et σ^*). Pour $\tilde{\sigma}, \tilde{\tau} \in \Gamma$, prolongeant respectivement $\sigma, \tau \in S$, on a, compte tenu de (2),

$$x^{\tilde{\tau}^* \tilde{\sigma}^*} = x_{\sigma}^{\tilde{\tau}^*} = x_{\tilde{\tau}^* \sigma} = x^{(\tilde{\tau}\tilde{\sigma})^*},$$

d'où $(\tilde{\tau}\tilde{\sigma})^* = \tilde{\tau}^* \tilde{\sigma}^*$. Donc l'application $\varphi : \tilde{\sigma} \to \tilde{\sigma}^*$

.....

est un monomorphisme de Γ dans le groupe Γ^* des $k(y)$ - automorphismes de $\tilde{K}(x)$.

Montrons que φ est surjectif. En effet, soit $z \in \tilde{K}(x)$, c'est-à-dire $z = f(x)$, où f est une fonction sur V, définie sur $\tilde{K}$. Supposons z invariant par $\varphi(\Gamma)$. Alors, pour $\tilde{\sigma} \in \Gamma$, induisant l'identité ε sur K, on a $\tilde{\sigma}^*(x) = x^{\varepsilon^*} = x$, d'où $z^{\tilde{\sigma}^*} = f^{\tilde{\sigma}}(x) = f(x)$, ce qui implique $f^{\partial} = f$. Donc f est définie sur K, et on a $z \in K(x)$; de plus, pour $\sigma \in S$, z est invariant par σ^* ; on a donc $z \in k(y)$. On a ainsi montré que le sous-corps de $\tilde{K}(x)$ formé des invariants par $\varphi(\Gamma)$ est contenu dans $k(y)$, donc coïncide avec $k(y)$. L'extension $\tilde{K}(x)/k(y)$ est donc galoisienne et, d'après la théorie de Galois, on a $\varphi(\Gamma) = \Gamma^*$. Donc φ est surjectif, donc φ est un <u>isomorphisme</u> $\Gamma \longrightarrow \Gamma^*$.

En outre, si $\tilde{\sigma} \in \Gamma$ induit l'identité sur $K(y)$, $\tilde{\sigma}$ induit l'identité sur K, et on a, comme on a vu, $x^{\tilde{\sigma}^*} = x$, donc $\tilde{\sigma}^*$ induit l'identité sur $K(x)$. D'après la théorie de Galois, on a $K(x) \subset K(y)$. On a donc $K(x) = K(y)$, i.e. ψ est birationnelle, ce qui démontre(i) dans le cas considéré.

Pour démontrer (ii), posons $\left[\tilde{K} : k\right] = n$, et introduisons une base $\alpha_1, \ldots, \alpha_n$ de l'extension $\tilde{K}/k$. C'est aussi une base de $\tilde{K}(y)/k(y)$, i.e. de $\tilde{K}(x)/k(y)$, de sorte que

.....

les coordonnées du point $x = \psi(y)$ peuvent s'écrire sous la forme

$$x_i = \sum_j \alpha_j \, f_{ij}(y) \qquad (1 \leqslant i \leqslant m) \ ,$$

où les f_{ij} sont des fonctions sur W, définies sur k. En appliquant σ^* aux deux membres, on obtient

$$(x_i)^{\sigma^*} = \sum_j \alpha_j^{\sigma} \, f_{ij}(y) \ .$$

Or les $(x_i)^{\sigma^*}$ sont aussi les coordonnées du point x_σ, donc s'expriment par des polynômes à coefficients dans $\tilde{K}$ en fonction des coordonnées x_i de x. Notons z le point de $\$_{mn}$ ayant pour coordonnées les $f_{ij}(y)$, et posons $W_o = \mathrm{loc}_k z$. L'extension K/k étant séparable, le déterminant de la matrice (α_j^{σ}) est $\neq o$. Donc les $f_{ij}(y)$ s'expriment par des polynômes à coefficients dans $\tilde{K}$ en fonction des x_i, et par suite l'application $\psi_o : W_o \longrightarrow V$ telle que $\psi_o(z) = x$ est un isomorphisme. De plus, l'application rationnelle $\theta : W \longrightarrow W_o$ telle que $\theta(y) = z$ est birationnelle; puisqu'elle est définie sur k, W_o est définie sur k, et ψ_o est définie sur K, ce qui démontre (ii).

b) - <u>L'extension K/k est régulière de type fini</u>.

On a alors $K = k(t)$, où t est un point générique sur k d'une variété $\top$ définie sur k. Pour $\sigma \in S$, le point

.....

$u = t^\sigma$ est générique de $\top$ sur k, et inversement tout point générique de $\top$ sur k est de cette forme, i.e l'application $\sigma \longmapsto u$ est bijective. La variété V^σ, l'application birationnelle $\varphi_{\sigma,\sigma}$, le point x_σ seront encore désignés respectivement par V_u, $\varphi_{u'u}$ et x_u. On a ainsi, en particulier, $V_t = V$, et $x_t = x$. Pour tout couple u, u' de points génériques de $\top$ sur k, on a $x_{u'} = \varphi_{u'u}(x_u)$.

Comme φ_{ut} est définie sur $k(t,u)$, on a $k(t,u,x_u) = k(t,u,x_t) = k(t,u,x)$. Prenons u générique de $\top$ sur $k(t,x_t)$; l'extension $k(t,u,x_u)/k(t,x)$ est régulière; considérons la sous-variété

$$Z = \mathrm{loc}_{k(t,x)}(u,x_u)$$

du produit $\top \times \mathfrak{S}_m$. Montrons que, pour tout point générique v de $\top$ sur k, la variété Z est définie sur $k(v,x_v)$. Prenant u générique de $\top$ sur k $(t,v,x) = k(t,v,x_v)$, il suffit pour cela de montrer que la variété

$$Z' = \mathrm{loc}_{k(v,x_v)}(u,x_u)$$

coïncide avec Z. Or soit $z'_o = (u_o,x_o) \in Z'$. On peut spécialiser (u, x_u, v, x_v) en (u_o, x_o, v, x_v) sur k. En composant cette spécialisation avec un k-automorphisme convenable de Ω, on voit qu'on peut spécialiser (t,x_t,v,x_v) en (u_o, x_o, v, x_v) sur k. On a donc $z'_o \in Z$, et on a montré que $Z' \subset Z$. On a de même $Z \subset Z'$.

.....

D'où $Z' = Z$.

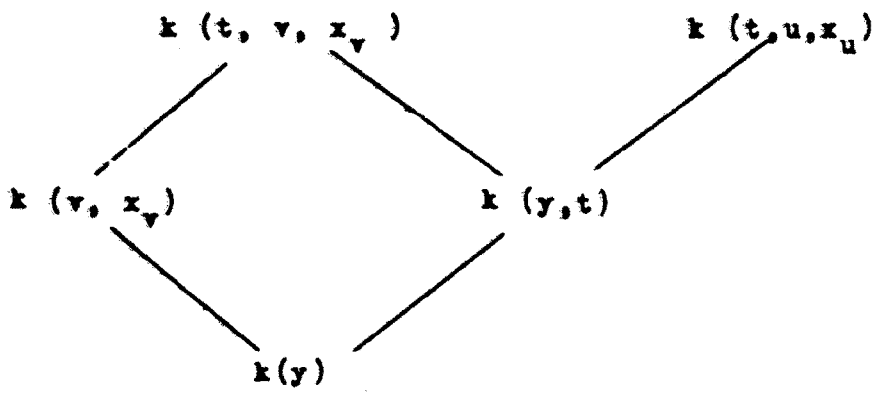
En conservant les mêmes notations, montrons qu'on a

$$k(y) = k(t,x_t) \cap k(u,x_u) .$$

En effet, $k(y)$ est contenu dans le second membre. Inversement, tout élément $z \in k(t,x_t) \cap k(u,x_u)$ est de la forme $z = f(t,x_t) = g(u,x_u)$, où f et g sont des fonctions sur $T \times V_t$ et $T \times V_u$ respectivement, définies sur k . Pour t, u, v comme ci-dessus, on peut spécialiser (t, x_t, u, x_v) en (v, x_v, u, x_u) sur k . On obtient $f(t,x_t) = f(v,x_v) = g(u,x_u)$, donc $z = f(t,x_t) = f(v,x_v)$, ce qui implique $z \in k(y)$.

Donc Z est définie sur $k(y)$, d'après le théorème 1.1 et chacun des points (u,x_u), (v, x_v), (t, x_t) est générique de Z sur $k(y)$. Si de plus on a pris u et v génériques indépendants sur $k(t, x_t)$, les trois points (t,x_t) , (u, x_u) , (v, x_v) sont génériques indépendants de Z sur $k(y)$. Dans cette dernière situation chacune des extensions $k(u, x_u) / k(y)$ et $k(t,y) / k(y)$ est linéairement disjointe de $k(v,x_v) / k(y)$; il en est donc de même de l'extension composée $k(t,u,x_u) / k(y)$. L'examen du diagramme

.....



montre, compte tenu de E, O., C, § 4, th. I2, que les extensions $k(t, u, x_u) / k(y,t)$ et $k(t, v, x_v)/k(y,t)$ sont linéairement disjointes. On a donc $k(y,t) = k(t,v,x_v) \cap k(t,v,x_v)$, d'où $k(x,t) \subset k(y,t)$, et par suite $k(x,t) = k(y,t)$, i.e. $K(x) = K(y)$, donc ψ est birationnelle, et on a prouvé (i).

Pour prouver (ii), introduisons la sous-variété $Y = \mathrm{loc}_k (u, x_u)$ de $T \times \mathbf{P}_n$, et l'application birationnelle $\alpha : T \times W \longrightarrow Y$, définie sur k, telle que $\alpha (u,y) = (u,x_u)$. Soient encore u,v, deux points génériques indépendants de T sur $k(t,x)$. Désignant par y_o un point quelconque de W, montrons que α est bimorphique en (v,y_o) si et si seulement α est bimorphique en (u,y_o). En effet, notons β l'application rationnelle $T \times Y \longrightarrow Y$, définie sur k, telle que $\beta (u,(v,x_v)) = (u, x_u)$. On a

(3) $\quad \alpha (u,y) = (u, \beta(u,v, \alpha(v,y)))$.

Supposons α morphique en (v,y_o), et posons

.....

$\alpha(v, y_o) = (v, z_o)$. Par hypothèse φ_{uv} est morphique en z_o . Compte tenu du fait que u et v sont génériques indépendants sur k , il en résulte que β est morphique en (u,v,z_o) . La relation (3) entraîne donc que α est morphique en (u, y_o) . De même l'application rationnelle α^{-1} étant supposée morphique en (v, z_o) , elle l'est aussi en (u,z_o) . L'assertion précédente est donc démontrée.

On peut trouver un ouvert U_1 de W tel que α soit bimorphique en tout point de $u \times U_1$. D'après ce qui précède, α est bimorphique également en tout point de $v \times U_1$. Par suite, il existe un k-ouvert U de W contenant U_1 et un k-ouvert U_o de T tels que α soit bimorphique en tout point de $U_o \times U$.

Notons t_h les coordonnées de t rapportées à U_o , et y_j celles de y rapportées à U .

Les coordonnées de $x = x_t$ s'expriment en fonction des t_h et des y_j par des polynômes P_i à coefficients dans k

$$x_i = P_i(t,y)$$

Le second membre s'écrit encore

$$P_i(t,y) = \sum_{\mu=1}^{\mu_o} Q_{i\mu}(t) \; R_{i\mu}(y)$$

où les $Q_{i\mu}$, $R_{i\mu}$ sont des polynômes à coefficients dans k,

.....

et où de plus on peut supposer que les $Q_{i\mu}(t)$ sont, pour i fixé, linéairement indépendants sur k. Pour tout point u générique de V sur k, on a

$$(4)\quad (x_u)_i = \sum_{\mu} Q_{i\mu}(u)\ R_{i\mu}(y)$$

Soient $t = u_1, \ldots, u_{\mu_o}$ des points génériques indépendants de T sur k. Alors la matrice M formée (pour i fixé) avec les $Q_{i\mu}(u_\nu)$ est inversible, i.e. de rang $r = \mu_o$: supposons en effet qu'on ait $r < \mu_o$ et, par exemple, que les r premières lignes de M soient indépendantes; il existerait des éléments a_μ $(1 \leqslant \mu \leqslant \mu_o)$ non tous nuls du corps $L_o = k(u_1,\ldots,u_r)$ tels qu'on ait

$$\sum_{\mu} a_\mu\ Q_{i\mu}(u_\nu) = 0 \qquad (1 \leqslant \nu \leqslant \mu_o).$$

Pour $\nu > r$, les $Q_{i\mu}(u_\nu)$ seraient donc linéairement dépendants sur L_o; comme $k(u_\nu)$ et L_o sont linéairement disjoints sur k, ils seraient linéairement dépendants sur k, ce qui est contradictoire.

Soit maintenant z le point ayant pour coordonnées les $R_{i\mu}(y)$, et posons $W_o = \mathrm{loc}_k z$. Les $(x_{u_\nu})_i$ s'expriment, d'après l'hypothèse, par des polynômes en fonction des x_i, à coefficients dans $L = k(u_1,\ldots,u_{\mu_o})$. Puisque M est inversible, on en déduit que l'application rationnelle

.....

$\psi_o : W_o \longrightarrow V$, définie sur L, telle que $\psi_o(z) = x$, est un isomorphisme. Comme plus haut, l'application $\theta : W \longrightarrow W_o$ telle que $\theta(y) = z$ est birationnelle, et définie sur k , donc W_o est définie sur k , et ψ_o est définie sur K , ce qui démontre (ii) dans le cas (b) .

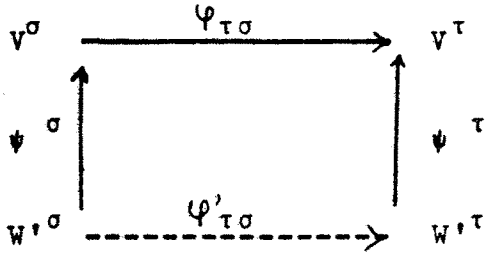
Pour achever la démonstration du théorème 1.2, remarquons qu'on peut supposer l'extension K/k de type fini (puisque toute variété est définie sur une telle extension) . Comme toute extension séparable de type fini est extension algébrique séparable d'une extension régulière (E,chap.0, C, , 6, th.18), il nous suffit de prouver l'assertion suivante : si k' est un corps intermédiaire ($k \subset k' \subset K$) tel que K/k' soit séparable, et si le théorème est vrai pour les extensions K/k' et k'/k, il l'est aussi pour K/k .

En effet, notons S_o le sous-ensemble de S formé des éléments induisant l'identité sur k' . Puisque les conditions (a) et (b) sont satisfaites pour $\rho, \sigma, \tau \in S_o$, et puisque le théorème est supposé vrai pour K/k', il existe une variété W' , définie sur k', et une transfortion birationnelle $\psi' : W' \longrightarrow V$, définie sur K, telles qu'on ait

$$(5) \qquad \varphi_{\tau_o \sigma_o} = \psi'^{\tau_o} \circ \left(\psi'^{\sigma_o}\right)^{-1}$$

quels que soient $\sigma_o, \tau_o \in S_o$. Pour $\sigma, \tau \in S$ quelconques, on peut compléter le diagramme

.....



par une transformation birationnelle $\varphi'_{\tau\sigma} : W'^{\sigma} \longrightarrow W'^{\tau}$.

Pour $\sigma \in S$, notons σ' la restriction de σ au corps k'. La variété W'^{σ} ne dépend que de σ', et on peut donc la noter $W'^{\sigma'}$. De plus, pour $\sigma, \tau \in S$, tels que $\sigma' = \tau'$, il existe un k-automorphisme ω de Ω, et des éléments $\sigma_o, \tau_o \in S_o$, tels que $\tau = \omega \circ \tau_o$ et $\sigma = \omega \circ \sigma_o$. En transformant (5) par ω, on obtient, compte tenu de (b), $\varphi_{\tau o} = \psi'^{\tau} \circ (\psi'^{\sigma})^{-1}$, donc $\varphi'_{\tau\,\sigma}$ est l'identité. Tenant compte de (a), on en déduit que la transformation $\varphi'_{\tau\sigma}$ ne dépend que de τ' et de σ' ; on peut donc la désigner par $\varphi'_{\tau',\sigma'}$. On voit alors que la famille des variétés $W'^{\sigma'}$ et des transformations birationnelles $\varphi'_{\tau',\sigma'}$ vérifie les conditions (a) et (b). On utilise alors le fait que le théorème est supposé vrai pour l'extension k'/k, c.q.f.d.

Remarque 1.2 - Dans le cas où $K = k(t)$ est une extension régulière de k (où t est générique d'une variété définie sur k), on peut modifier l'énoncé du théorème 1.2 en ne considérant que les φ_{ut} relatifs aux couples

.....

de points génériques <u>indépendants</u> de T sur k , et en se restreignant dans (a) aux triplets (u,v,w) formés de 3 points génériques indépendants sur k .

En effet, la signification du symbole $\varphi_{u,t}$ peut alors être prolongée à tous les couples (u,t) de points génériques non nécessairement indépendants : il suffit de prendre v générique de T sur $k(t,u)$ et de poser $\varphi_{ut} = \varphi_{uv} \circ \varphi_{vt}$. On voit trivialement que le symbole φ_{ut} ainsi prolongé vérifie les conditions du théorème initial .

2 - <u>Le théorème de CHOW (complément)</u>

<u>THEOREME 2.1</u> (CHOW) Soit A une variété abélienne, définie sur un corps K . Toute sous-variété abélienne B de A est définie sur une extension algébrique <u>séparable</u> de K .

Le résultat ci-dessus est énoncé dans V A , IV , 8 , remarque 2, mais on a seulement prouvé (th.9) que B est définie sur une extension algébrique de K . Il nous suffit donc de prouver que si B est définie sur une extension radicielle (i.e. purement inséparable) de K , B est définie sur K . Nous utiliserons pour cela le lemme suivant :

.....

Lemme 2.1 - Soient K un corps A et B deux variétés abéliennes, et φ: A $\longrightarrow$ B un homomorphisme bijectif (i.e. une isogénie radicielle) défini sur K . On peut trouver un morphisme surjectif (i.e. une isogénie) ψ : B $\longrightarrow$ A, défini sur K, et une puissance p^μ de l'exposant caractéristique, tels que

$\psi \circ \varphi = p^\mu \delta$ (i.e $\psi(\varphi(x)) = p^\mu x$, pour $x \in A$)

Démonstration : On peut trouver une extension régulière L de K , une courbe V sur A, définie sur L , et un point $x \in V$ qui soit générique de A sur K et de V sur L (il suffit pour cela, de couper A par une variété linéaire générique de dimension convenable) . Considérons la courbe $W = \varphi(V)$ et le L-morphisme $\alpha : V \longrightarrow W$ induit par φ . Le point $y = \psi(x)$ étant regardé comme un diviseur sur W, le diviseur $\alpha^{-1}(y)$ est rationnel sur L(y). D'après VA III 5, lemme 11, ce diviseur est de la forme $\alpha^{-1}(y) = p^\mu x$, où p^μ est le degré de l'extension radicielle L(x)/L(y) . D'après le théorème des fonctions symétriques (VA III 5, th.4) , le point $z = (p^\mu \delta)(x)$ de A (p^μ-ième multiple de x, au sens de la loi de groupe) est rationnel sur L(y) . Mais comme l'extension L/K est régulière, il en est de même de L(y)/K(y) , donc K(x) et L(y) sont linéairement disjoints sur K(y), et par suite z est rationnel sur K(y) . Il existe une application rationnelle ψ : B $\longrightarrow$ A, définie sur K, telle

.....

que $\psi(y) = z$. D'après VA I 6, th.8, ψ est un homomorphisme. Comme on a $\psi \circ \varphi = p^{\mu} \delta$, et comme $p^{\mu} \delta$ est surjectif (VA IV 6 , th. 7, coroll.) , ψ est surjectif, ce qui démontre le lemme.

Revenons à la démonstration du théorème de Chow. D'après notre hypothèse, il existe un entier m tel que B soit définie sur le corps $K^{p^{-m}}$. Considérons le K-morphisme $\varphi : A \longrightarrow A' = A^{p^m}$ induit par F^m , où F est l'automorphisme de Frobenius de Ω . L'image $B' = \varphi(B)$ est définie sur K . D'après le lemme ci-dessus, il existe un homomorphisme $\psi : A' \longrightarrow A$, défini sur K , et une puissance p^{μ} de l'exposant caractéristique, tels que $\psi \circ \varphi = p^{\mu} \delta$. On a $(p^{\mu}\delta)(B) = B$, d'où $\psi(B') = B$, donc B est définie sur K, c.q.f.d.

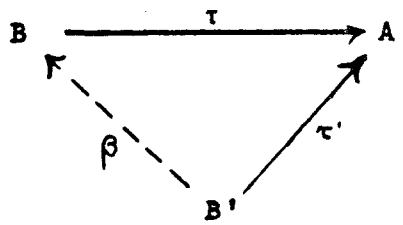
COROLLAIRE - Si A est une variété abélienne définie sur K , et si B est une sous-variété abélienne de A définie sur une extension primaire de K, B est définie sur K .

En effet, une extension primaire est, par définition, disjointe de la clôture séparable K_s de K . Donc B est définie sur $K_s \cap K' = K$.

.....

3 - La (K/k)-trace d'une variété abélienne

THEOREME 3.1 - Soit K une extension régulière d'un corps k , et soit A une variété abélienne définie sur K . Il existe un couple (B,τ) composé d'une variété abélienne B définie sur k, et d'un K-homomorphisme $\tau = B \longrightarrow A$ tel que, pour tout couple (B', τ') analogue, on puisse compléter le diagramme



par un k-homomorphisme $\beta : B' \longrightarrow B$.
L'homomorphisme τ est nécessairement injectif, et le couple (B, τ) est unique à un k-isomorphisme près .

Remarque 3.1 - Le théorème implique que τ induit une isogénie radicielle de B sur $\tau(B)$; on peut montrer que celle-ci n'est pas en général un isomorphisme, i.e. que τ n'est pas en général une immersion.

Démonstration - Considérons d'abord, parmi les couples (B', τ'), l'un de ceux (B_o, τ_o) pour lesquels dim $\tau_o(B_o)$=d

.....

est minimum.

Posons $\tau_o(B_o) = A_o$; et montrons qu'on a $\tau'(B') \subset A_o$ pour tout couple (B', τ') . En effet, considérons le K-homomorphisme $\tau_* : B' \times B_o \longrightarrow A$, obtenu en posant $\tau_*(x,y) = \tau'(x) + \tau_o(y)$. Son image est la variété abélienne $\tau'(B') + \tau_o(B_o)$: donc cette image contient A_o. Sa dimension étant $\leq d$, elle coïncide avec A_o. On a donc bien $\tau'(B') \subset A_o$.

Montrons maintenant qu'on peut, parmi les couples (B', τ'), trouver un couple (C, φ) tel que φ soit une <u>isogénie</u> $C \longrightarrow A_o$. En effet, notons H la composante neutre de $\ker \tau_o$. C'est une sous-variété abélienne de B_o , invariante par tout K-automorphisme de Ω , donc définie sur une extension radicielle de K , donc définie sur k d'après le théorème de Chow . D'après VA,I,7 ,th.9 (théorème d'irréductibilité de Poincaré), il existe une sous-variété C de B_o , définie sur k , telle que $C + H = B_o$ et que $C \cap H$ soit un sous-groupe fini de B_o. Il suffit de prendre pour φ la restriction de τ_o à C .

L'extension K/k étant régulière, K est de la forme $k(t)$, où t est un point générique d'une variété T .

.....

définie sur k . Pour tout point u générique de T sur k , notons A_u, φ_u les transformés respectifs de A, φ par le k-isomorphisme $k(t) \xrightarrow{\sim} k(u)$ appliquant t sur u . Considérons une suite $u_1 = t$, $u_2, \ldots, u_m, \ldots$ de points génériques indépendants de T sur k ; pour tout m , considérons le morphisme $\theta_m = \varphi_{u_1} \times \ldots \times \varphi_{u_m} : C \longrightarrow A_{u_1} \times \ldots \times A_{u_m}$, et désignons son image par D_m . Pour $m \geqslant n$, on a $\theta_n = \pi_{mn} \circ \theta_m$, où π_{mn} est l'homorphisme $D_m \longrightarrow D_n$ induit par la projection sur le produit des n premiers facteurs. Pour tout m , θ_m est une isogénie $C_m \longrightarrow D_m$, et on a $\deg \theta_m \leqslant \deg \theta_n$. La suite $(\deg \theta_m)$ est décroissante, donc stationnaire. Il existe donc m_o tel que, pour m et $n \geqslant m_o$, π_{mn} soit un isomorphisme puisque $\deg \pi_{mn} = \deg \theta_n - \deg \theta_m$. En particulier, prenons $n \geqslant m_o$, et $m = 2n$. Posons $L = k(u_1, \ldots, u_{2n})$; soit x un point générique de C sur L et, pour $1 \leqslant i \leqslant 2n$, posons $\varphi_{u_i}(x) = y_i$. D'après le choix de m et n , on a

$L(y_1, \ldots, y_n) = L(y_1, \ldots, y_{2n})$ i.e.

$y_{n+1}, \ldots, y_{2n} \in L(y_1, \ldots, y_n)$. En échangeant les rôles des points, on en déduit

.....

$L(u_1,\dots,u_n) = L(y_{n+1},\dots,y_{2n})$. Désignons par $\bar{u}$ le point $(u_1,\dots,u_n)$ de $\bar{T} = T \times \dots \times T$, par $\bar{A} = \bar{A}_{\bar{u}}$ la variété $A_{u_1} \times \dots \times A_{u_n}$, par $\varphi_{\bar{u}}$ l'application rationnelle $\varphi_{u_1} \times \dots \times \varphi_{u_n} : C \longrightarrow A$, définie sur $L = k(\bar{u})$, et par $D_{\bar{u}}$ l'image de $\varphi_{\bar{u}}$ (précédemment notée D_n) . Nous venons de montrer que, pour $\bar{u}$ et $\bar{u}'$ génériques indépendants de $\bar{T}$ sur k, il existe un isomorphisme $\alpha_{\bar{u}',\bar{u}} : D_{\bar{u}} \longrightarrow D_{\bar{u}'}$, tel que $\varphi_{\bar{u}'} = \alpha_{\bar{u}',\bar{u}} \circ \varphi_{\bar{u}}$ Il en résulte que la famille constituée par les variétés $D_{\bar{u}}$ et par les isomorphismes $\alpha_{\bar{u}',\bar{u}}$ vérifie les conditions du théorème de descente, relativement à l'extension L/k . Par suite, il existe une variété B définie sur k, et un L-isomorphisme (pour la structure de variété algébrique) $\beta_{\bar{u}} : B \longrightarrow D_{\bar{u}}$, tel qu'on ait $\alpha_{\bar{u}',\bar{u}} = \beta_{\bar{u}'} \circ \beta_{\bar{u}}^{-1}$ .En transportant par $\beta_{\bar{u}}$ la structure de $D_{\bar{u}}$, on définit sur B une structure de variété abélienne dont la loi $\gamma = \gamma_{\bar{u}}$ est définie sur $k(\bar{u})$. On a nécessairement $\gamma_{\bar{u}} = \gamma_{\bar{u}'}$, donc, d'après le th. 1.1, γ est définie sur k , i.e. B est une variété abélienne définie sur k . Pour $1 \leqslant i \leqslant n$, notons τ_i le L - homomorphisme $B \longrightarrow A_{u_i}$ obtenu en composant $\beta_{\bar{u}}^{-1}$ avec la projection sur le i-ème facteur. Posons en

.....

particulier $\tau = \tau_1$. Appliquant le théorème de Chow au graphe de τ_i , on voit que τ_i est défini sur $k(u_i)$. En particulier, τ est un K-homomorphisme $B \longrightarrow A$.

La composante de l'origine de $\ker \tau_i$ est une sous-variété abélienne de B définie sur une extension radicielle de k , donc sur k , d'après le théorème de Chow. Donc, $\ker \tau_i$ est un $\overline{k}$-ensemble algébrique. Indroduisant, pour tout couple (i,j) , un $\overline{k}$-automorphisme de Ω tel que $u_i \longmapsto u_j$, on voit que $\ker \tau_i$ ne dépend pas de i . On a donc $\ker \tau_{\underline{u}} = \ker \tau_i = o$ pour tout i et, en particulier, $\ker \tau = o$.

Soient maintenant B', τ' comme dans l'énoncé. L'application (ensembliste) $\beta : \tau_{u_i}^{-1} \circ \tau'_{u_i} : B' \longrightarrow B$ est un homomorphisme de groupes. Son graphe Γ est donc une sous-variété de groupe de B(VA I 2, th.2) , donc une sous-variété abélienne de B, nécessairement définie sur une extension radicielle de $k(u_i)$. D'après le théorème de Chow, Γ est définie sur k , donc ne dépend pas de i . Donc, pour $z' \in B'$, et en posant $z = \beta(B)$, le point $\beta_{\underline{u}}(z)$ coïncide avec $(\tau'_{u_1}(z), \ldots, \tau'_{u_n}(z))$, donc est rationnel sur $L(z')$. Comme $\beta_{\underline{u}}$ est birationnelle et définie sur L, z est rationnel sur $L(z')$. Donc β est un L-homomorphisme; comme son graphe Γ est défini sur k, c'est un k-homomorphisme. La relation $\tau'_{u_i} = \tau_{u_i} \circ \beta$

.....

donne en outre, pour $i = 1$, $\tau' \circ \beta = \tau$.

Enfin, l'unicité du couple (B,τ') est triviale, compte tenu de l'injectivité de τ , et de la propriété universelle.

Le couple (B, τ) est appelé une <u>(K/k) - trace</u> de A. L'image $\tau(B)$ sera également notée $A^{K/k}$.

Le théorème suivant sera utilisé, à plusieurs reprises, dans la suite, pour remédier aux difficultés dues au fait que τ n'est pas une immersion (remarque 3.1 précédente) .

<u>THEOREME 3.2</u> - Soit K une extension régulière d'un corps k. Posons $K = k(t)$, où t est un point générique d'une variété T définie sur k . Soit A une variété abélienne définie sur K , et soit (B,τ') une (K/k) - trace de A. Soient $u_1 = t$, $u_2,\ldots,u_n$ des points génériques indépendants de T sur k . Pour $1 \leqslant i \leqslant n$, soient A_{u_i} , τ_{u_i} les conjugués respectifs correspondants de A et τ . Pour n assez grand, le morphisme $\overline{\tau} = \tau_{u_1} \times \ldots \times \tau_{u_n} : B \longrightarrow A = A_{u_1} \times \ldots \times A_{u_n}$ est une immersion.

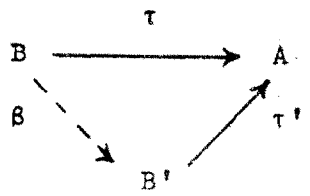
Ce théorème résulte immédiatement de la dernière partie de la démonstration précédente.

On a de plus le théorème suivant, exprimant l'invariance de la trace par extension du corps de base.

.....

THEOREME 3.3 - Soit K une extension régulière d'un corps k , et soit k' une extension de k linéairement disjointe de K . Posons K' = Kk' . Si A est une variété abélienne définie sur K , toute (K/k) - trace de A est aussi une (K'/k')-trace de A .

Démonstration - Soient (B, τ) une (K/k)-trace et (B', τ') une (K'/k')-trace de A. D'après la propriété universelle de (B,τ), on peut compléter le diagramme

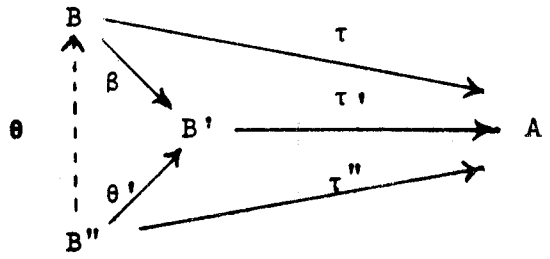


par un k'-morphisme $\beta : B \longrightarrow B'$. Il s'agit de montrer que β est un isomorphisme.

On peut supposer que k'/k est de type fini : en effet, d'après la propriété universelle, le théorème est vrai pour l'extension k'/k s'il l'est pour toute sous-extension de type fini. Remarquons aussi que si $k \subset k'' \subset k'$ et si le théorème est vrai pour les extensions k"/k et k'/k" , il l'est pour k'/k : pour le voir, il suffit de remarquer que K" = Kk" est une extension régulière de k" , linéairement disjointe de k'/k" . Comme toute extension de type fini est extension algébrique d'une extension régulière,

il suffit de traiter séparément chacun des trois cas suivants:

a) - <u>k'/k radicielle</u> - Supposons $k'=k^{p^{-m}}$. La variété abélienne $B'' = (B')^{p^m}$ est définie sur k . D'après le lemme 2.1 , il existe une isogénie radicielle $\theta : B'' \longrightarrow B'$, définie sur k' . Comme B" et A sont définies sur K , l'application rationnelle $\tau'' = \tau' \circ \theta' : B'' \longrightarrow A$ est définie sur K, d'après le théorème de Chow. En vertu de la propriété universelle de (B, τ) , il existe un k-homomorphisme $\theta : B'' \longrightarrow B$ tel que le diagramme



soit commutatif. Ceci entraîne que β est bijectif , i.e. est une isogénie radicielle, et que $\tau(B) = \tau'(B')$. Posant $K = k(t)$, où t est générique d'une variété T définie sur k , il résulte du théorème 3.2 que, pour n assez grand, les homomorphismes

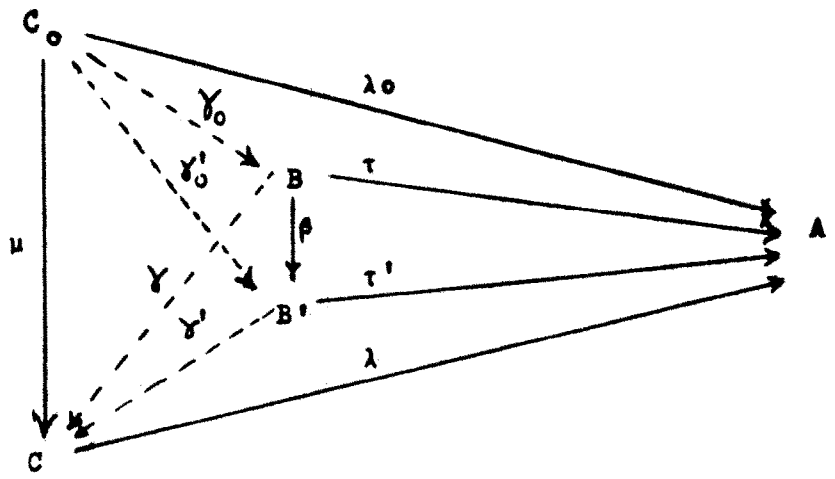
$\overline{\tau} = \tau_{u_1} \times \ldots \times \tau_{u_n} : B \longrightarrow A_{u_1} \times \ldots \times A_{u_n}$ et

$\overline{\tau}' = \tau'_{u_1} \times \ldots \times \tau'_{u_n} : B' \longrightarrow A_{u_1} \times \ldots \times A_{u_n}$ sont des immersions. D'après ce qui précède, ils ont même image. Comme $\overline{\tau} = \overline{\tau}' \circ \beta$, β est un isomorphisme.

.....

b)- <u>k'/k algébrique séparable.</u> Notons k^* la clôture séparable de k. Comme K est linéairement disjoint de k^* sur k, tout k-automorphisme de k^* se prolonge à un et un seul K-automorphisme de $K^* = Kk^*$, et ceci définit un isomorphisme du groupe de Galois de k^*/k sur celui Γ de K^*/K. Soit (C,λ) une (K^*/k^*) - trace de A. Il existe un sous-corps E de k^* contenant k, de type fini sur k, tel que C soit définie sur E, et que λ soit défini sur KE. En transformant par un élément arbitraire $\sigma \in \Gamma$ la propriété universelle de (C,λ), on voit que $(C^\sigma, \lambda^\sigma)$ est encore une (K^*/k^*)-trace de A. On en déduit que, pour $\sigma, \tau \in \Gamma$, il existe un k^*-isomorphisme $\varphi_{\tau\sigma} : C^\sigma \longrightarrow C^\tau$, tel que $\lambda^\sigma = \lambda^\tau \circ \varphi_{\tau\sigma}$. Les $\varphi_{\tau\sigma}$ vérifient en outre les conditions du théorème de descente (th.1.2.). Il existe donc une variété C_o définie sur k, et un E-isomorphisme $\mu : C_o \longrightarrow C$, tels qu'on ait $\varphi_{\tau\sigma} = \mu^\tau \circ (\mu^\sigma)^{-1}$ pour tout couple (σ,τ). En transportant par μ^{-1} la structure de variété abélienne de C, on définit sur C_o une structure de variété abélienne invariante par σ, donc définie sur k. De même, l'homomorphisme $\lambda_o = \lambda \circ \mu : C_o \longrightarrow A$ est invariant par σ, donc défini sur k. D'après la propriété universelle de chacun des couples (B,τ), (B',τ'), (C,λ); il existe des morphismes $\gamma_o : C_o \longrightarrow B$, $\gamma'_o : C_o \longrightarrow B'$ $\gamma : B \longrightarrow C$ $\gamma' : B' \longrightarrow C$, tels que le diagramme

.....

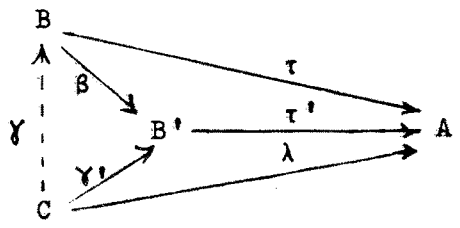


soit commutatif; comme $\mu = \gamma \circ \gamma_0 = \gamma' \circ \gamma'_0$ est un isomorphisme, tous ces morphismes sont des isomorphismes. Donc $\beta = \gamma_0 \circ \gamma'^{-1}_0 = \gamma \circ \gamma'^{-1}$ est un isomorphisme.

c)- <u>k'/k régulière</u> - Soit $K=k(t)$, où t est un point générique d'une variété T définie sur k. Soient $u_1,\dots,u_n$ des points génériques indépendants de T sur k'. Pour n assez grand, d'après le th. 3.2, l'homomorphisme $\overline{\tau}' = \tau'_{u_1} \times \dots \times \tau'_{u_n} : B' \longrightarrow \overline{A} = A_{u_1} \times \dots \times A_{u_n}$ est une immersion, définie sur $L = k(u_1,\dots,u_n)$. On a en outre $k' = k(v)$, où v est un point générique sur L d'une variété V définie sur k. Pour tout point générique w de V sur L, il existe un L-automorphisme σ de Ω tel que $w = v^\sigma$. Notons B'_w, $\overline{\tau}'_w$ les transformés respectifs de B' et $\overline{\tau}'$ par σ ; en particulier,

.....

$B' = B'_v$, et $\bar{\tau}' = \bar{\tau}'_v$. L'image $\bar{\tau}'_v(B'_v)$ est une sous-variété de $\bar{A}$ définie sur $L(v)$. L'extension $L(v)/L$ étant régulière, $\bar{\tau}'_v(B'_v)$ est définie sur L, d'après le théorème de Chow, donc invariante par σ, de sorte que $\bar{\tau}'_v(B'_v) = \bar{\tau}'_w(B'_w)$. Comme $\bar{\tau}'_v$ et $\bar{\tau}'_w$ sont des immersions, il existe, quels que soient v et w, un isomorphisme $\varphi_{wv} : B'_v \longrightarrow B'_w$ tel que $\varphi_{wv} = \bar{\tau}'^{-1}_w \circ \bar{\tau}'_v$. Les φ_{wv} vérifient en outre les conditions du théorème de descente. Donc il existe une variété C définie sur k et un k'-isomorphisme $\gamma' = \gamma'_v : C \longrightarrow B'$ tel que $\varphi_{wv} = \gamma'_v \circ \gamma'^{-1}_w$. En transformant par γ'^{-1} la structure de variété abélienne de B', on définit sur C une structure de variété abélienne invariante par σ, donc définie sur k. De même, l'homomorphisme $\lambda = \tau' \circ \gamma'$ est invariant par σ, donc défini sur k. D'après la propriété universelle de (B, τ), il existe un homomorphisme $\beta : C \longrightarrow B$ tel que le diagramme



.....

soit commutatif. Comme γ' est un isomorphisme, γ et β sont des isomorphismes c.q.f.d.

4 - Enoncé du théorème de Mordell-Weill et de ses variantes:

V étant une variété définie sur un corps k (ou, plus généralement, un k-ensemble algébrique) , l'ensemble des points de V rationnels sur k est noté V_k. Si V est un groupe algébrique défini sur k , V_k est un groupe pour la structure induite.

THEOREME 4.I (Mordell-Weil) . Soit K un corps de nombres algébriques (de degré fini sur $\mathbb{Q}$) , et soit A une variété abélienne définie sur K . Alors le groupe A_K est de type fini.

K étant maintenant une extension régulière d'un corps k , et A une variété abélienne définie sur k , on note $A^{K/k}$ l'image τ (B) d'une (K/k)-trace de A , et $A_{(k)}^{K}$ l'image τ (B_k) du groupe B_k des points de B rationnels sur k

THEOREME 4.2 (ou "théorème de Mordell-Weil relatif") Soit K une extension régulière d'un corps k , et soit A une variété abélienne définie sur k . Alors le groupe $A_K/A_{(k)}^{K}$ est de type fini.

.....

THEOREME 4.3 (généralisant le th.4.1) .
Soit K un corps de type fini (extension de type fini du corps premier) , et soit A une variété abélienne définie sur K . Alors le groupe A_K est de type fini.

5 - Réduction du problème

Montrons d'abord que le théorème 4.3 résulte des théorèmes 4.1 et 4.2 . En effet, soit K un corps de type fini. On peut trouver une extension algébrique de degré fini k' du corps premier telle que, en posant Kk' = K' , l'extension K'/k' soit régulière : on a en effet K = k(t) où t est un point d'un espace affine $\mathbb{A}_n$; il suffit de prendre pour k' le plus petit corps de définition de l'une des composantes de l'ensemble algébrique $\mathrm{loc}_k\, t$.

D'une part le théorème 4.2 implique que le groupe $A_{K'}/A^{K'}_{(k')}$ est de type fini, d'autre part, si (B, τ) est une (K'/k')-trace de A, le groupe $A^{K'}_{(k')}$ est isomorphe à $B_{k'}$. Or ce dernier groupe est de type fini : en effet, si la caractéristique p est nulle, k' est un corps de nombres algébriques, et la propriété résulte du théorème 4.1 ; si p =o , la propriété est triviale, car $B_{k'}$ est un groupe fini. D'où le th. 4.3.

.....

On va maintenant démontrer certains résultats auxiliaires, permettant en particulier de réduire le th. 4.2 au cas où k est algébriquement clos, et où K est de degré de transcendance 1 sur k, i.e. est un <u>corps de fonctions sur une courbe</u> définie sur k.

<u>THEOREME 5.1</u> - Soit K une extension régulière d'un corps k, et soit k' une extension de k linéairement disjointe de K. Posant $K' = Kk'$, on a

$$A_K \cap A_{(k')}^{K'} = A_{(k)}^{K}$$

<u>Démonstration</u> - On a vu (th.3.3) que toute (K/k)-trace (B, τ) de A est aussi une (K'/k')-trace de A. On a donc $A_{(k)}^{K} = \tau(B_k) \subset A_{(k')}^{K'} = \tau(B_{k'})$, d'où $A_{(k)}^{K} \subset A_K \cap A_{(k')}^{K'}$.

Pour prouver l'inclusion opposée, considérons un point $b \in B_{k'}$ tel que $\tau(b) \in A_K$. Il s'agit de montrer que $b \in B_k$. Posons $K = k(t)$, où t est un point générique d'une variété T définie sur k. D'après le théorème 3.2, il existe un entier n tel que, pour $(u_1,\dots,u_n)$ génériques indépendants de T sur k, l'homomorphisme $\overline{\tau} : \tau_{u_1} \times \dots \times \tau_{u_n} : B \longrightarrow A_{u_1} \times \dots \times A_{u_n}$ soit une immersion. Pour tout i $(1 \leqslant i \leqslant n)$, le point $\tau_{u_i}(b)$ est

.....

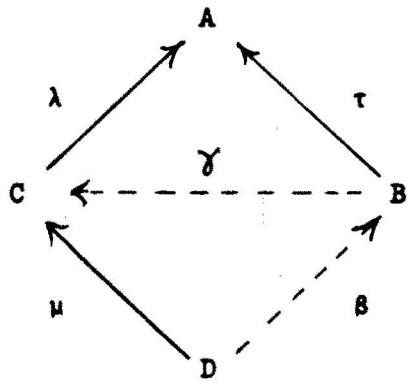
rationnel sur $k(u_i)$. Comme $\bar{\tau}$ est défini sur $L = k(u_1,\ldots,u_n)$, b est rationnel sur L . Or L et k' sont linéairement disjoints sur k (E,0,C,7, th.20) , donc on a $L \cap k' = k$, donc b est rationnel sur k, c.q.f.d.

Corollaire : Les hypothèses étant celles du th.5.1, le groupe $A_K/A^K_{(k)}$ est isomorphe à un sous-groupe du groupe $A_{K'}/A^{K'}_{(k')}$.

THEOREME 5.2 Soient k, K, L trois corps tels que $k \subset K \subset L$, et que les extensions K/k et L/K soient régulières. Si le th. 4.2 est vrai pour L/k, il l'est pour L/K . S'il l'est pour L/K et K/k, il l'est pour L/k.

Démonstration - Soit A une variété abélienne définie sur L . Soient (B,τ) une (L/k) - trace de A, et (C, λ) une (L/K)- trace de A . Soit , en outre , (D, μ) une (K/k)-trace de C . D'après la propriété universelle de (C, λ), et d'après celle de (B, τ), on peut trouver un k-homomorphisme $\beta : D \longrightarrow B$ et un K-homomorphisme $\gamma : B \longrightarrow C$ tels que le diagramme

.....

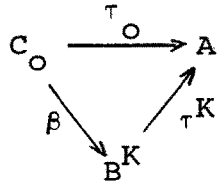


soit commutatif. On a donc $\lambda(C_K) \supset \tau(B_k)$. Par suite, si $A_L/\tau(B_k)$ est de type fini, il en est de même de $A_K/\lambda(C_K)$. Inversement, supposons que $A_K/\lambda(C_K)$ et $C_K/\mu(D_k)$ soient de type fini. Alors $\lambda(C_K)/\lambda(\mu(D_k))$ est de type fini, et il en est de même de $A_K/\lambda(\mu(D_k)) = A_K/\tau(\beta(D_k))$. A fortiori, puisque $\tau(\beta(D_k)) \subset \tau(B_k)$, le groupe $A_L/\tau(B_k)$ est de type fini, c.q.f.d.

THEOREME 5.3 - Soient K et L deux extensions régulières d'un corps k, telles que $K \subset L$ et que L/K soit algébrique de degré fini séparable. Soit A une variété abélienne définie sur K. Alors le groupe $A^L_{(k)} \cap A_K / A^K_{(k)}$ est fini.

.....

Démonstration : Soient respectivement (B^K , τ^K) et (B^L , τ^L) une (K/k)-trace et une (L/k)-trace de A. Soit $\Gamma = \Gamma^L$ le graphe de τ^L. Notons Δ l'intersection $\bigcap_\sigma \Gamma^\sigma$ des conjugués de Γ sur K, et C la projection de Γ sur B^L. Nécessairement Δ et C sont des groupes algébriques. La composante neutre C_o de C est une variété abélienne invariante par σ, donc définie sur une extension radicielle de K. Comme B^L est définie sur K, C_o est définie sur k par le théorème de Chow. Toujours par le théorème de Chow, l'homomorphisme $\tau_o : C_o \longrightarrow A$ induit par τ^L est défini sur k. D'après la propriété universelle de (B^K , τ^K), il existe un k-homomorphisme $\beta : C_o \longrightarrow B^K$ tel que le diagramme



soit commutatif. On a, d'une part :

$$\tau_o(C_o)_k = \tau^L(C_o) \subset A^K_{(k)} .$$

On a d'autre part

$$\tau^L(C_k) = A^L_{(k)} \cap A_K .$$

En effet, il est clair que $\tau^L(C_k)$ est contenu dans le

second membre. Inversement, pour $y \in A_K$, de la forme $\tau^L(x)$, avec $x \in B_k^L$, le point (x,y) de Γ est invariant par σ ; on a donc $(x,y) \in \Delta$, d'où $x \in C$, d'où $x \in C_k$.

Comme C/C_o est un groupe fini, il en est de même de $C_k/(C_o)_k$, donc de $\tau^L(C_k)/\tau^L(C_o)_k$, et a fortiori de $\tau^L(C_k)/A^K_{(k)}$ c.q.f.d.

<u>Corollaire</u> - Soient L , K , k comme dans le théorème 5.3. Si le théorème 4.2 est vrai pour l'extension L/k , il l'est pour K/k .

En effet, l'homomorphisme de groupes $\alpha : A_K \longrightarrow A_L / A^L_{(k)}$ déduit de l'injection $A_K \longrightarrow A_L$ a pour noyau $N = A_K \cap A^L_{(k)}$. D'après le théorème 5.3 le groupe $N/A^K_{(k)}$ est fini. L'hypothèse entraîne que le groupe $A_K/N = \mathrm{Im}\ \alpha$ est de type fini. Donc $A_K / A^K_{(k)}$ est de type fini.

On peut maintenant démontrer la réduction annoncée concernant le théorème 4.2. Supposons en effet que ce dernier soit vrai pour k algébriquement clos, et pour K/k régulière, de degré de transcendance 1 . Compte

tenu du coroll. du th 5.1 et de la disjonction linéaire de K et $\bar{k}$ sur k, le théorème 4.2 est vrai aussi pour k quelconque, et pour K/k régulière de degré de transcendance 1. Passons au cas d'une extension régulière K/k de degré de transcendance r quelconque. On a alors $K = k(t)$, où t est un point générique d'une variété T, de dimension r, définie sur k. On peut supposer T affine ($T \subset \mathbb{S}_n$). Considérons dans $\mathbb{S}_n$ la variété linéaire générique $L = L_{u,v}$, de dimension $n - r + 1$, définie par les équations

$$\sum_i u_{ij} X_i = v_j \qquad (1 \leqslant j \leqslant r-1),$$

où les u_{ij}, v_j sont algébriquement indépendants sur k.

Posons $F = k(u,v)$. D'après I, th. I2.1, l'intersection $L \cap T = Z$ est une courbe définie sur F ; la démonstration de ce th. montre en outre qu'on peut choisir les u_{ij}, v_j de façon que $t \in Z$, et que t soit générique de Z sur F. L'extension $F(t)/F$ est régulière de degré de transcendance 1. L'extension F/k est transcendante pure, donc obtenue par une succession d'extensions régulières de degré de transcendance 1. Le théorème 4.2 étant supposé vrai pour les extensions de degré de transcendance 1 est vrai pour $F(t)/k$, et aussi pour $F(t)/F$

.....

compte tenu du th. 5.2 . Comme t est générique de T sur F , le corps $K = k(t)$ est linéairement disjoint de F sur k , donc le th. 4.2 est vrai aussi pour K/k, compte tenu du coroll. du th. 5.1 .

6 - Enoncé du "théorème de Mordell-Weil" faible

THEOREME 6.1 - (Théorème de Mordell-Weil faible) . Soit A une variété abélienne définie sur un corps K , et soit m un entier naturel premier avec la caractéristique p de K . Si K est un corps "global" , c'est-à-dire ou bien (a) un corps de nombres algébriques (de degré fini sur $\mathbb{Q}$) , ou bien (b) une extension régulière de type fini d'un corps algébriquement clos k (i.e. un corps de fonctions sur une variété T définie sur k) , le groupe $A_K/m\,A_K$ est fini.

Justifions d'abord le nom attribué à ce théorème. Dans le cas (a) , il résulte trivialement du théorème de Mordell-Weil (th. 4.1) . Dans le cas (b) , on le déduit comme suit du th. 4.2 ; posons $G = A_K / A_{(k)}^K$; le th. 4.2 implique que G/mG est fini ; la multiplication par m dans A_K induit un homomorphisme $A_K \longrightarrow G/mG$, de noyau $N = mA_K + A_{(k)}^K$; désignons par (B, τ) une (K/k)-trace de A; comme k est algébriquement clos, tout élément de $A_{(k)}^K = \tau(B_k)$ est divisible par m ; on a donc $A_{(k)}^K \subset mA_K$,

.....

d'où $N = m A_K$; donc $A_K/m A_K$ est fini.

7 - La descente infinie

Nous allons, inversement, utiliser le théorème de Mordell-Weil faible comme étape intermédiaire de la démonstration des théorèmes 4.1 et 4.2 . Plus précisément, nous allons, par la méthode de "descente infinie" , commencer par démontrer le th.suivant :

THEOREME 7.1 - Soient A, K et m comme dans le théorème 6.1 . Supposons de plus qu'on a $m \geqslant 2$ et que, dans le cas (b) , l'extension K/k est de degré de transcendance 1 , i.e. que la variété T est une courbe.

Supposons que le groupe $A_K /m A_K$ est fini. Alors, dans le cas (a) (resp.(b)) , le groupe A_K (resp. $A_K/A^K_{(k)}$) est de type fini.

Démonstration : Comme on a vu dans I , I2, le corps global K est canoniquement muni d'une famille M de valeurs absolues vérifiant la formule du produit. En outre on peut (VA IV, th.5) supposer A projective ($A \subset P_r$) . A tout $x \in A_K$, regardé comme point de P_r , on peut associer sa hauteur h (x) . Notons R un système de

.....

de représentants des classes (mod $m A_k$) dans A_K. Par hypothèse, R est fini. Partant d'un point $x \in A_K$ quelconque, on peut former une suite $x_o = x$, $x_1, \ldots, x_n, \ldots$ d'éléments de A_K tels que

$$(1) \quad \begin{cases} x_o = b_o + m\, x_1 \\ \text{----------} \\ x_{n-1} = b_{n-1} + m\, x_n \\ \text{----------} \end{cases}$$

où les b_i appartiennent à R. On va démontrer

(*) Il existe une constante réelle h_o qui ne dépend pas de x , ni de la manière dont on a construit la suite (x_n) , telle que, pour n assez grand, on ait $h(x_n) < h_o$.

Dans le cas (a) , le théorème en résultera aussitôt. En effet, d'après II, th. 2.3, l'ensemble R_o des points $x \in A_K$ tels que $h(x) \leqslant h_o$ est fini. D'après les relations (1) , x s'exprime comme combinaison linéaire à coefficients entiers d'éléments de R et de R_o . Donc A_K est engendré par l'ensemble fini $R \cup R_o$.

Dans le cas (b), on obtiendra de même le théorème à partir de la propriété (*) à condition de prouver la propriété supplémentaire suivante.

(**) - L'ensemble des classes mod. $A^K_{(k)}$ des points

.....

$x \in A_K$ tels que $h(x) \leqslant h_o$ est fini.

Démonstration de (*)

D'une part on désignera par $\sim$ l'équivalence linéaire pour les diviseurs, d'autre part, on utilisera l'équivalence représentée par le signe $\equiv$ (VA , 9) . Rappelons que, pour qu'un diviseur X sur A soit $\equiv 0$, il faut et il suffit que $X_a \sim X$ pour tout $a \in A$, où l'on note X_a le translaté de X par la translation $\tau_a : x \longmapsto x + a$. Démontrons préalablement deux lemmes.

LEMME 1 - Soit A une variété abélienne et soit m un entier $\neq o$. Si X est un diviseur $\equiv o$ sur A , on a

$$(m\,\delta)^{-1}\,(X) \sim m\,X$$

Posons en effet $B = A \times \ldots \times A$ (m facteurs) . On a $m\delta = \lambda_m \circ \mu$, où μ est le morphisme diagonal $A \longrightarrow B$; et où λ_m est le morphisme $B \longrightarrow A$ défini par $\lambda_m\,(x_1,\ldots,x_m) = x_1 + \ldots + x_m$. On en déduit

$$(m\,\delta)^{-1}\,(X) = \mu^{-1}\,(\lambda_m^{-1}\,(X))$$

Or, d'après VA IV 9 , lemme 2, coroll. , on a

$$\lambda_m^{-1}\,(X) \sim \sum_i \pi_i^{-1}\,(X) ,$$

où π_i est la projection de $B = A \times \ldots \times A$ sur le i-ème facteur . On a donc

.....

$$(m\,\delta)^{-1}(X) \sim \sum_i \mu^{-1}\left(\pi_i^{-1}(X)\right)$$

$$\sim \sum_i (\pi_i \circ \mu)^{-1}(X)$$

Or $\pi_i \circ \mu$ est l'application identique, donc

$$(m\,\delta)^{-1}(X) \sim m\,X$$

LEMME 2 - Soient A et m comme dans le lemme 1 . Pour tout diviseur X sur A , on a

$$(m\,\delta)^{-1}(X) \equiv m^2 X$$

En effet, soit $a \in A$. Désignant toujours par τ_a la translation $x \longmapsto x + a$, on a le diagramme commutatif

$$\begin{array}{ccc} A & \xrightarrow{\tau_a} & A \\ {\scriptstyle m\,\delta}\downarrow & & \downarrow{\scriptstyle m\,\delta} \\ A & \xrightarrow{\tau_{ma}} & A \end{array}$$

d'où l'on déduit

$$\left((m\,\delta)^{-1}(X)\right)_a = (m\,\delta)^{-1}(X_{ma}) .$$

Donc on a

$$(2) \quad \left((m\,\delta)^{-1}(X)\right)_a - (m\delta)^{-1}(X) = (m\delta)^{-1}(X_{ma} - X) .$$

Or, d'après le théorème du carré,

$$X_{ma} - X \sim m\,(X_a - X) .$$

On a aussi $X_a - X \equiv o$, donc, d'après le lemme 1 ,

.....

$$(m\delta)^{-1}\,(X_a - X) \sim m\,(X_a - X)\ ,$$

d'où

$$(m\delta)^{-1}\,(X_{ma} - X) \sim m^2\,(X_a - X)$$

Posant $Y = (m\delta)^{-1}\,(X) - m^2\,X$, on en déduit, compte tenu de (2) , $Y_a \sim Y$. Comme a est arbitraire, ceci implique $Y \equiv o$, d'où le lemme.

Revenons à la démonstration de (*) .
Notons X une section hyperplane de A , rationnelle sur K . Nécessairement, X est un diviseur ample, donc non dégénéré sur A (VA IV 7, th. 8) . Rappelons que, pour qu'un diviseur Z sur A soit $\equiv o$, il faut et il suffit qu'il existe $q \in \mathbb{Z}$ non nul et $b \in A$ tel que $q\,Z \sim X_b - X$. Si Z est rationnel sur un corps de définition K de A , on peut en outre choisir q et b de façon que b soit rationnel sur K (démonstration : partons de $c \in A$, vérifiant $rZ \sim X_c - X$; si c' est conjugué de c sur $\overline{K}$, on a encore, par isomorphisme $rZ \sim X_{c'} - X$, d'où $X_{c'} \sim X_c$; posant $V = \mathrm{loc}_{\overline{K}}\, c$, on en déduit, compte tenu de VA III,6 , th. 7, qu'on a encore $X_{b_1} \sim X_c$ pour tout point $b_1 \in V$; on peut, en particulier prendre $b_1 \in V$ algébrique sur K ; on a alors aussi $rZ \sim X_{b_1} - X$ pour tout conjugué b_i de b_1 sur K ; la somme $\sum_{i=1}^{m} b_i$ de tous ces conjugués est un point purement inséparable sur K ;

.....

D'après le lemme 2.1 , il existe une puissance p^μ de l'exposant caractéristique telle que le point $b = p^\mu \sum_i b_i$ soit rationnel sur K , et on a $q\,Z \sim X_b - X$, en posant $q = p^\mu\ m\ r$) .

Compte tenu du lemme 2 , il existe donc $q \in \mathbb{Z}$ non nul et $b_o \in A_K$ tels que

$$q\,((m\delta)^{-1}(X) - m^2 X) \sim X_{b_o} - X$$

Pour $b \in A$, on a, d'après le lemme 1 ,

$$(m\delta)^{-1}(X_{-b} - X) \sim m\,(X_{-b} - X)$$

On en déduit

$$q(m\delta)^{-1}(X_{-b}) \sim q\,m^2 X + qm\,(X_{-b} - X) + X_{b_o} - X$$

d'où, en vertu du théorème du carré

$$q\,(m\delta)^{-1}(X_{-b}) \sim (qm^2 - 1)\,X + X_{b'} \ ,$$

en posant $b' = b_o - qmb$. Prenons $b \in A_K$. Désignons par φ_b le morphisme $x \longmapsto mx + b$ de A dans A , par $\mathcal{C}$ la classe du diviseur X pour l'équivalence linéaire et, conformément aux notations de II, 4 , par $\mathcal{C}_{\varphi_b}$ celle du diviseur $\varphi_b^{-1}(X)$. On a $\varphi_b = \tau_b \circ (m\delta)$, d'où $\varphi_b^{-1}(X) \sim (m\delta)^{-1}(X_{-b})$. On a donc

$$q\,\mathcal{C}_{\varphi_b} = (qm^2 - 1)\,\mathcal{C} + \mathcal{C}'$$

où $\mathcal{C}'$ est positive (i.e. est la classe d'un diviseur

.....

positif, à savoir $X_{b,}$). D'après les propriétés des hauteurs (II, 4, th.4.2), on a

$$q\,h(\varphi_b(x)) = q\,h(mx+b) \geqslant (qm^2-1)\,h(x) + c(b)$$

d'où, à fortiori,

$$h(mx+b) \geqslant (m^2-1)\,h(x) + \frac{1}{q}\,c(b)$$

Posant $c_o = -\frac{1}{q}\inf_{b\in R} c(b)$, on a, pour tout n,

$$(m^2-1)\,h(x_n) \leqslant h(x_{n-1}) + c_o$$

Ceci donne, par récurrence sur n

$$h(x_n) \leqslant \frac{1}{(m^2-1)^n}\,h(x) + c_o \sum_{i=1}^{n} \frac{1}{(m^2-1)^i}$$

Donc, pour n assez grand, on a $h(x_n) \leqslant h_o$, en posant $h_o = \varepsilon + \frac{c_o}{m^2-2}$, où ε est un nombre réel $> o$ arbitraire.

<u>Démonstration de (**)</u>. Désignant par s un entier naturel $\geqslant$ ho, introduisons, sur la courbe T, supposée projective sans point multiple, le système linéaire $\mathcal{L}_s$ des sections de T par les hypersurfaces de degré s, et le système linéaire complet $\mathcal{L}$ contenant $\mathcal{L}_s$. Le système linéaire $\mathcal{L}_s$ est ample, donc à fortiori $\mathcal{L}$ est ample. Donc il existe un k-isomorphisme $\psi : T \to T'$, ayant pour image une variété projective T', et associé à $\mathcal{L}$ au sens de VA IV 3.

.....

Tout diviseur D de degré $s' \leqslant s$ sur T est majoré par un élément de $\mathfrak{L}_s$, . C'est en effet évident lorsque $s' = 1$, et le cas s' quelconque s'en déduit par linéarité. Considérons un point $x = (x_0, \ldots, x_n) \in A_K$, avec $x_i \in K$ pour tout i, les x_i étant en outre choisis de façon que les $\mathrm{div}.(x_i)_o$ n'aient pas de composante commune. D'après II, 3, th. 3.1, on a $h(x) = \deg \sup_i \mathrm{div}(x_i)_\infty$. Si l'on suppose $h(x) \leqslant h_o$, on a $h(x) \leqslant s$, et le diviseur positif $\sup_i \mathrm{div}(x_i)_\infty$ est majoré par un élément $D_o \in \mathfrak{L}$, qu'on peut peut choisir en outre rationnel sur k. On en déduit, pour tout i, $\mathrm{div}(x_i) = D_i - D_o$ avec $D_i \in \mathfrak{L}$ rationnel sur k. Si, pour tout i $(o \leqslant i \leqslant r)$, on note x_i, la fonction sur T' transposée de x_i, on a $\mathrm{div}(x'_i) = D'_i - D'_o$ où $D'_i = \psi(D_i)$ est une section hyperplane de T'

Désignant par $t'_o, \ldots, t'_r$, un système de coordonnées homogènes du point générique $t' = \psi(t)$ de T', on a donc, pour le point x, un système de coordonnées homogènes de la forme

$$(3) \qquad x'_i = \sum_{j=1}^{r'} a_{ij} \, t'_j \qquad (1 \leqslant i \leqslant r)$$

avec $a_{ij} \in k$

Posons $l = (r + 1)(r' + 1) - 1$. Le point a de l'espace projectif $\mathbb{P}_l$ de coordonnées homogènes les a_{ij}

.....

(écrits dans un ordre arbitraire) ne dépend que du point x, non du choix des coordonnées x_i. Les formules (3) (où l'on regarde maintenant les a_{ij} comme des "variables" et les t_{ij} comme des "coefficients") s'interprètent par l'existence d'une application linéaire projective $\lambda : \mathbb{P}_l \dashrightarrow \mathbb{P}_r$, définie sur $K = k(t) = k(t')$, telle que $x = \lambda(a)$. Notons U l'ouvert de morphicité de λ (complémentaire d'une certaine sous-variété linéaire de $\mathbb{P}_l$. Pour $a \in U$, rationnel sur k, la propriété $\lambda(a) \in A$ se traduit par un nombre fini de relations algébriques entre les a_{ij} à coefficients dans k. En effet, on peut définir A par un système d'équations de la forme

$$(4) \qquad F_\alpha (t'_0, \ldots, t'_r, X_0, \ldots, X_r) = 0$$

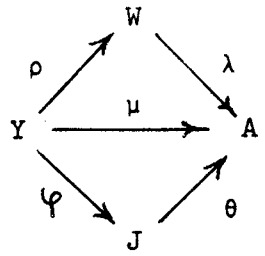
où, pour tout α, F_α est un polynôme à coefficients dans k, homogène séparément par rapport aux X_i et par rapport aux t'_j ; la condition $\lambda(a) \in A$ se traduit en remplaçant dans (4) les X_i par les x_i tirés de (3) ; désignant, pour tout α, par d_α le degré global de F_α, et par $B_\alpha = \{ f_{\alpha\beta}(t') \}$ une base de l'espace vectoriel formé des polynômes homogènes en t' de degré d_α à coefficients dans k, on peut écrire les relations obtenues sous la forme : $\sum_\beta g_{\alpha\beta}(a) \; f_{\alpha\beta}(t') = 0$, où les $g_{\alpha\beta}$ sont des

∘∘∘∘∘

polynômes homogènes à coefficients dans k ; ces relations sont donc équivalentes à $g_{\alpha\beta}(a) = o$ pour tout couple (α,β).

On a donc montré que l'ensemble $\{ a \mid a \in U_k , \lambda(a) \in A \}$ est de la forme E_k, où E est un sous-ensemble k-fermé de U. Désignons par W l'une quelconque des composantes (en nombre fini) de E. Il suffit de prouver que, pour $a \in W_k$, le point $x = \lambda(a)$ appartient à une classe déterminée (mod $A^K_{(k)}$).

D'après VA III 4, lemme 9, et remarque 4, on peut trouver une extension L de k, une courbe Y complète sans point multiple définie sur L, une application rationnelle $\rho : Y \to W$ définie sur L et un point $y \in Y$ tels que ρ soit morphique en y, de valeur a et que, pour $\overline{y}$ générique de Y sur $L(y)$, le point $\overline{a} = \varphi(y)$ soit un point générique donné de W sur k. L'application rationnelle $\mu = \lambda \circ \rho$ est un morphisme (VA I 5, th 6) défini sur KL. Soient J la jacobienne de Y, et φ un morphisme canonique $Y \to J$. D'après la propriété universelle du couple (J, φ) (VA III 7, th 6), il existe un morphisme $\theta : J \to A$ tel que le diagramme



soit commutatif.

∘∘∘∘∘

Ce morphisme θ est le composé d'un homomorphisme θ_o et d'une translation sur A. Soit L' un corps de définition de J et φ contenant $L(y, \bar{y})$. Quitte à remplacer t par un conjugué convenable sur k, on peut supposer que $K = k(t)$ est algébriquement indépendant, donc linéairement disjoint, de L' sur k. Dans ces conditions, θ et θ_o sont définis sur $L'K$. Posant $\bar{z} = \varphi(\bar{y})$, $z = \varphi(y)$, puis $\bar{x} = \theta(\bar{z}) = \lambda(\bar{a})$ et $x = \theta(z) = \lambda(a)$, on a $\bar{x} - x = \theta(\bar{z}) - \theta(z) = \theta_o(\bar{z}) - \theta_o(z) = \theta_o(\bar{z} - z)$.

Comme le point $\bar{z} - z$ est rationnel sur L', on a $\bar{x} - x \in A_{L'}^{L'K}$. Donc si x_1 et $x_2 \in A_K$ sont respectivement de la forme $x_1 = \lambda(a_1)$, $x_2 = \lambda(a_2)$, avec a_1 et $a_2 \in W_k$, on a $x_1 - x_2 \in A_{L'}^{L'K} \cap A_K$, d'où $x_1 - x_2 \in A_{(k)}^{K}$, compte tenu du théorème 5.1. Autrement dit, la classe de x (mod. $A_{(k)}^{K}$) ne dépend que de la composante W, c.q.f.d.

8 - Théorie de Kummer

THEOREME 8.1 - Soit G une variété de groupe définie sur un corps K, et soit m un entier premier à la caractéristique de K. L'homomorphisme $m\delta : G \longrightarrow G$ est de degré fini (donc surjectif) et séparable.

.....

Démonstration - Posons $r = \dim G$. Désignons par $\underline{o}$ (resp. $\underline{o}'$) l'anneau local de G (resp. de $G \times G$) à l'origine 0, et par $\underline{m}$ (resp. $\underline{m}'$) son idéal maximal. Soit $(u_1, \ldots, u_r)$ un système de paramètres uniformisants de G en 0 (i.e. un système minimal de générateurs de $\underline{m}$). Désignant par (x,y) un point générique de $G \times G$ sur k, les fonctions $u_1(x), \ldots, u_r(x)$, $u_1(y), \ldots, u_r(y)$ forment un système de paramètres uniformisants de $G \times G$ à l'origine (cf. E III 5).

Montrons que si $f \in \underline{m}$, la fonction g sur $G \times G$ définie par $g(x,y) = f(x+y) - f(x) - f(y)$ appartient à l'idéal $\underline{m}'^2$. En effet, on a $f(x+y) \in \underline{m}'$, donc il existe des constantes a_i, b_j telles que

$$f(x+y) \equiv \sum_i a_i u_i(x) + \sum_j b_j u_j(y) \pmod{\underline{m}'^2},$$

En faisant $y = o$, puis $x = o$, on en déduit

$$f(x) \equiv \sum_i a_i u_i(x) \pmod{\underline{m}'^2}$$

puis

$$f(y) \equiv \sum_j b_j u_j(y) \pmod{\underline{m}'^2}$$

ce qui donne bien $f(x+y) - f(x) - f(y) \in \underline{m}'^2$

On en déduit, pour toute fonction $f \in \underline{m}$,

$$f(mx) - mf(x) \in \underline{m}^2$$

Comme m est premier à la caractéristique de K,

.....

il en résulte que les $v_i(x) = u_i(mx)$ engendrent l'idéal $\underline{m}$, i.e. forment un système de paramètres uniformisants de G en O, i.e. sont tels que les différentielles $(dv_i)_0$ à l'origine soient linéairement indépendantes ; a fortiori les dv_i sont linéairement indépendantes, donc les v_i forment une base de transcendance séparante du corps de fonctions $\mathcal{F}_K(V)$ (d'après E III 2, th. 3). Donc x est algébrique séparable sur k(mx), c.q.f.d.

G étant un groupe algébrique, on désignera par $\Delta_m(G)$, ou simplement par Δ_m, le groupe $\ker(m\delta)$ des points d'ordre m de G.

Corollaire - Avec les hypothèses du th. précédent, le groupe $\Delta_m = \ker(m\delta)$ est fini. Pour $a \in G$ tout point $b \in G$ tel que $mb = a$ est algébrique séparable sur k(a).

La première assertion résulte du fait que, pour x générique de G sur K, l'ensemble $(m\delta)^{-1}(x)$ est fini. D'autre part, tout conjugué de b sur k(a) appartient à l'ensemble fini $(m\delta)^{-1}(a)$. Donc b est algébrique sur k(a). Soit $y \in G$; si y est générique de G sur k(b), il en est de même de $x = my$ et de $x' = a-x = m(b-y)$. D'après le th. 8.1, les points y et b-y sont algébriques séparables sur $k(x,x') = k(a,x)$. Donc b est algébrique séparable sur k(a,x). Or k(a,x) est extension régulière,

.....

donc séparable de $k(a)$. Donc b est algébrique séparable sur $k(a)$.

Dans toute la suite de ce n° , on considère un corps K et un groupe algébrique G défini sur K tel que $\Delta_m(G) \subset G_K$, i.e. que tous les points de $\Delta_m = \Delta_m(G)$ soient rationnels sur K .

On considère tous les sous-groupes H de G_K tels que $m\,G_K \subset H \subset G_K$. Le groupe $(m\delta)^{-1}(H)$ est noté $\frac{1}{m}H$. Le corps $K(\frac{1}{m}H)$ engendré par tous les éléments de ce groupe est encore noté L_H . En particulier, on pose

$$L = L_{G_K} = K(\tfrac{1}{m}G_K) .$$

Si $b \in \frac{1}{m}H$, on a $mb = a \in G_K$, donc $mb^\sigma = a$ pour tout conjugué b^σ de b sur K , d'où $b^\sigma \in \frac{1}{m}H$. Donc l'extension L_H/K est galoisienne. On désignera par Γ_H (resp. Γ) le groupe de Galois de L_H/K (resp. L/K) . L'extension L_H/K est de plus abélienne (i.e. Γ_H est abélien) . En effet, soient $\sigma, \tau \in \Gamma_H$, et soit $b \in \frac{1}{m}H$; on a $b^\sigma - b = c_\sigma \in \Delta_m$; comme on suppose $\Delta_m \in G_K$, on a $c_\sigma^\tau = c_\sigma$, d'où

$b^{\tau\sigma} - b^\tau = c_\sigma$, d'où

$$(5) \qquad b^{\tau\sigma} - b = c_\sigma + c_\tau$$

et par suite $b^{\tau\sigma} = b^{\sigma\tau}$; on a donc $\tau\sigma = \sigma\tau$. En outre, l'extension abélienne L_H/K est d'exposant m , i.e. tous les éléments de Γ_H sont d'ordre m. En effet, on a .

.....

d'après (5), pour $\sigma \in \Gamma_H$ et $b \in \frac{1}{m} H$, $b^{\sigma^m} - b = m\, c_\sigma = 0$.

Remarquons en outre que, si $b \in \frac{1}{m} H$, le point $c_\sigma = b^\sigma - b$ de Δ_m ne dépend que du point $mb = a$ de H. Plus précisément, l'application

$$\varphi : \Gamma_H \times H \longrightarrow \Delta_m$$

obtenue en posant $\varphi(\sigma, a) = c_\sigma$ est bilinéaire. Son noyau à gauche est l'identité, car $\varphi(\sigma, a) = o$ pour tout $a \in H$ signifie $b^\sigma = b$ pour tout b, donc $\sigma = \varepsilon$; son noyau à droite se compose des $a \in H$ tels que $b^\sigma = b$ pour tout $\sigma \in \Gamma_H$, donc tels que $b \in G_K$; autrement dit, ce noyau est $m\, G_K$. On en déduit, par passage au quotient, une application bilinéaire

$$\psi : \Gamma_H \times (H/m\, G_K) \longrightarrow \Delta_m$$

dont les noyaux à droite et à gauche sont nuls.

THEOREME 8.2 - Pour que le groupe H/mG_K soit fini, il faut et il suffit que l'extension L_H/K soit de degré fini. En particulier, pour que $G_K/m\, G_K$ soit fini, il faut et il suffit que L/K soit de degré fini.

En effet, Γ_H et $H/m\, G_K$ sont respectivement isomorphes, d'après ce qui précède, à des sous-groupes de $\mathrm{Hom}(H/mG_K, \Delta_m)$ et de $\mathrm{Hom}(\Gamma_H, \Delta_m)$; d'où le théorème puisque Δ_m est

.....

un groupe fini.

Remarque- Si on abandonne l'hypothèse $\Delta_m \subset G_K$, l'extension L/K est encore galoisienne, mais non, en général, abélienne. Pour $b \in \frac{1}{m} G_K$, l'application $\sigma \longrightarrow b^\sigma - b = c_\sigma$ est alors un cocycle du groupe de Galois Γ de L/K, à valeurs dans Δ_m, et la classe de cohomologie correspondante ne dépend que du point $mb = a \in G_K$. Utilisant la suite de cohomologie associée à la suite exacte

$$0 \longrightarrow \Delta_m \longrightarrow G \xrightarrow{m\delta} G \longrightarrow 0$$

on voit que $G_K/m\,G_K$ est isomorphe à un sous-groupe du groupe de cohomologie $H^1(\Gamma, \Delta_m)$. On en déduit encore que $G_K/m\,G_K$ est de degré fini si et si seulement L/K est de degré fini.

La théorie de Kummer proprement dite concerne le cas où G est le groupe multiplicatif. On a alors $G_K = K^*$; On adopte la notation multiplicative et on écrit, par exemple, K^{*m} au lieu de $m\,G_K$. Dans ce cas, Δ_m est le groupe des racines m-ièmes de l'unité, donc est cyclique. Donc l'application bilinéaire ψ précédente met en dualité les deux groupes Γ et H/K^{*m}. En particulier, ces deux groupes ont toujours le même nombre d'éléments.

.....

THEOREME 8.3 (th. fondamental de la théorie de Kummer). Soient K un corps, et m un entier premier à la caractéristique de K. Supposons que K contient les racines m-ièmes de l'unité. Alors $H \xmapsto{\lambda} L_H = K(H^{\frac{1}{m}})$ est une application bijective de l'ensemble des sous-groupes H de K^* tels que $K^{*m} \subset H \subset K^*$ sur l'ensemble des extensions abéliennes d'exposant m de K. Pour que le groupe H/K^{*m} soit fini, il faut et il suffit que L_H/K soit de degré fini, et on a alors, quel que soit H, $(H:K^{*m}) = \left[L_H : K\right]$.

Conséquence : Le corps $L = K(K^{*\frac{1}{m}})$ est l'extension abélienne maximum d'exposant m de K.

Démonstration : D'une part, la dernière assertion résulte du th. 8.2, et de la remarque précédant l'énoncé. D'autre part :

λ est surjective. En effet, toute extension abélienne de K d'exposant m s'obtient comme composée d'extensions cycliques d'exposant m, et on sait que toute extension cyclique d'exposant m de K est obtenue par l'adjonction de la racine m-ième d'un élément de K^*.

λ est injective. En effet, soient H et H' tels que $L_H = L_{H'}$. On a alors $\Gamma_H = \Gamma_{H'}$. Compte tenu de la

.....

dualité précédente, chacun des groupes H/K^{*m} , H'/K^{*} est isomorphe à $\mathrm{Hom}(\Gamma_H , \Delta_m) = \tilde{\Gamma}$ et pour que $a \in H$ et $a' \in H'$ aient même image dans $\tilde{\Gamma}$, il faut et il suffit que $a \equiv a' \bmod K^{*m}$. Ceci entraîne $H' \subset H K^{*m} = H$. On a de même $H \subset H'$, d'où $H = H'$, c.q.f.d.

9 - Ramification d'une extension de Kummer

ω étant une valuation discrète d'un corps K , et L une extension algébrique de K , on dit que ω est non ramifiée dans L , ou que l'extension L/K est non ramifiée pour ω si toute valuation ω' de L prolongeant ω est non ramifiée sur ω ce qui signifie (I, 6) que l'indice de ramification $e_{\omega'/\omega}$ est 1 , et que l'extension résiduelle correspondante est séparable (ceci entraîne en particulier que L/K est séparable). On remplacera parfois, dans la terminologie précédente, la valuation ω par la valeur absolue ultramétrique $v = e^{-\omega}$.

LEMME 9.1 Soit K un corps muni d'une valuation discrète ω d'anneau A et de corps résiduel K° . Soit L une extension de K de la forme $K(u)$, où u est racine d'un polynôme unitaire $F \in A[X]$. Si le polynôme $F^{\circ} \in K^{\circ}[X]$, réduit de F mod A , a ses racines distinctes, ω est non ramifiée dans L .

Démonstration - On peut supposer K complet et F irréductible. Introduisons une clôture algébrique $\overline{K}^{\circ}$ de K° .

.....

Soit $u^\circ \in \overline{K}^\circ$ l'une des racines de F°, et posons $L^\circ = K^\circ(u^\circ)$. On peut prolonger l'homomorphisme canonique $\lambda : A \longrightarrow K^\circ$ à une place ρ de L, à valeurs dans L°, telle que $\rho(u) = u^\circ$. Comme on a supposé K complet, cette place ρ est unique à l'équivalence près. Autrement dit, si u°_1 et u°_2 sont deux racines de F°, et si on leur a fait correspondre respectivement ρ_1 et ρ_2, il existe un automorphisme σ de $\overline{K}^\circ$ tel que $\rho_2 = \sigma \circ \rho_1$. Comme ρ_1 et ρ_2 prolongent λ, σ induit l'identité sur K°. On a $u^\circ_2 = \sigma(u^\circ_1)$, donc u°_1 et u°_2 sont conjugués sur K°. Comme les u°_i sont distinctes, F° est irréductible et L°/K° séparable. Posant $n = [L : K] = \deg F$, et $f = [L^\circ : K^\circ]$, on a de plus $f = \deg F^\circ = n$, d'où $e = 1$, c.q.f.d.

Lemme 9.2 : Soit K un corps muni d'une valuation discrète ω.

(a) - Soient K' et K'' deux extensions algébriques de degré fini de K telles que $K \subset K' \subset K''$. Pour que ω soit non ramifiée dans K'', il faut et il suffit que ω soit non ramifiée dans K' et que toute valuation ω' de K' prolongeant ω soit non ramifiée dans K''.

(b) - Soient K' et L deux extensions algébriques de degré fini de K, et soit ω' une valuation de K' prolongeant ω. Si ω est non ramifiée dans L, ω' est non ramifiée dans $K'L$.

.....

(c) - Si L et L' sont deux extensions algébriques de degré fini de K non ramifiées pour ω , l'extension composée LL' est non ramifiée pour ω .

Démonstration - On peut supposer K complet dans chacune des assertions (I, 4, propriétés c) et e))

(a) - Désignant par K° , K'° , K''° les corps résiduels respectifs de K , K' , K" , l'extension K''°/K'° est séparable si et seulement si K'°/K° et K''°/K'° le sont. Les égalités $[K':K]=[K'^\circ : K^\circ]$ et $[K'' : K'] = [K''^\circ : K'^\circ]$ entraînent $[K'':K]=[K''^\circ : K^\circ]$; inversement, cette dernière entraînent les deux précédentes, car on sait que $[K' : K] \geq [K'^\circ : K^\circ]$ et $[K'' : K'] \geq [K''^\circ : K'^\circ]$.

(b) - K étant complet, l'extension non ramifiée K' de K est de la forme K(u) , où u est racine d'un polynôme $F \in K[X]$ unitaire irréductible à coefficients entiers , tel que le polynôme réduit F° ait ses racines distinctes (I,6) . Il suffit d'appliquer le lemme 9.1 .

(c) - Résulte trivialement de (a) et (b)

THEOREME 9.1 Soient K un corps muni d'une valuation discrète ω normée, m un entier premier à la caractéristique du corps résiduel, et a un élément de K^*. Pour que ω soit non ramifiée dans $L = K(\alpha)$ où α est une racine m-mième de a , il faut et il suffit que m divise $\omega(a)$

.....

Démonstration : Notons A l'anneau de ω et t une uniformisante ($\omega(t) = 1$) .

Si m divise $\omega(a)$, on a : $a = t^{rm} u$, où r est un entier et où u est un élément inversible de A. On a $L = K(\nu)$, L est obtenu par adjonction d'une racine ν de $F = X^m - u$. D'après l'hypothèse sur m , le polynôme réduit $F^\circ = X^m - u^\circ$ a ses racines distinctes. D'après le lemme 9.1 , ω est non ramifiée dans L .

Inversement, si ω est non ramifiée dans L , et si ω' est une valuation de L prolongeant ω , les groupes des valeurs de ω et de ω' coïncident; ils coïncident avec $\mathbb{Z}$, puisque ω est normée. On a donc $\omega'(\alpha) \in \mathbb{Z}$, donc $\omega'(a) = \omega(a) \in m\mathbb{Z}$, c.q.f.d.

THEOREME 9.2- Soit K un corps de nombres, ou bien un corps de fonctions sur une courbe T définie sur un corps k algébriquement clos, et soit m un entier premier à la caractéristique de K . Soit M la famille propre canonique de valeurs absolues de K, et soit S un sous-ensemble fini de m ; notons $\overline{M}$ le sous-ensemble de M formé des $v \in M-S$ ultramétriques. Il existe un élément maximum $\overline{L}$ dans l'ensemble des extensions abéliennes d'exposant m de K non ramifiées pour toute $v \in \overline{M}$ et cette extension $\overline{L}/K$ est de degré fini.

.....

Démonstration : L'existence de $\overline{L}$ résulte du fait que la composée de deux extensions abéliennes d'exposant m et non ramifiées pour v est encore une extension abélienne d'exposant m et (d'après le lemme 9.2, (c)) non ramifiée pour v. D'après le th. 8.3, $\overline{L}$ est de la forme $K(\overline{H}^{\frac{1}{m}})$, où $\overline{H}$ est un sous-groupe de K^* tel que : $K^{*m} \subset \overline{H} \subset K^*$. Compte tenu de la théorie de Kummer (th.8.3), il suffit de prouver que le groupe $\overline{H}/K^{*m}$ est fini .

(a) - Cas des corps de nombres : Désignons par R l'anneau des entiers de K, par U le groupe des unités de K, par J le groupe des idéaux fractionnaires de K, par J_o le sous-groupe de J formé des idéaux principaux, par $\overline{J}$ le sous-groupe de J engendré par les idéaux premiers $\underline{p}$ de R tels que $v_{\underline{p}} \in \overline{M}$. Le théorème 9.1 entraîne que, pour $a \in \overline{H}$, l'idéal principal (a) est de la forme $(a) = \underline{\overline{b}}\ \underline{b}^m$, avec $\underline{\overline{b}} \in \overline{J}$ et $\underline{b} \in J$. L'application $a \longmapsto (a)$ est un homomorphisme de groupes $\overline{H} \longrightarrow \overline{J}\, J^m$. Par passage au quotient, on en déduit un homomorphisme $\lambda : \overline{H} \to \overline{J}\ J^m/J_o^m$. Or on a $\overline{J} \cap J^m = \overline{J}^m$, donc $\overline{J}J^m/J^m \simeq \overline{J}/\overline{J}^m$. Comme $\overline{J}$ est de type fini, $\overline{J}/\overline{J}^m$ est fini. D'autre part J^m/J_o^m est isomorphe au groupe des classes d'idéaux J/J_o, donc est un groupe fini (I. th.11.1) . L'image de λ est donc un groupe fini. Par ailleurs on a $\ker \lambda = UK^{*m}$. Donc $\overline{H}/UK^{*m}$ est fini.

.....

Or $U \cap K^{*m} = U^m$, donc $UK^{*m}/K^{*m} \simeq U/U^m$. Puisque U est de type fini, d'après le théorème de Dirichlet (I,th.11.2), U/U^m est fini. Donc $\overline{H}/K^{*m}$ est fini.

(b) - <u>Cas des corps de fonctions</u> : Désignons par $\mathfrak{D}_0$ le groupe des diviseurs de degré 0 sur T , par $\mathfrak{D}_1$ le sous-groupe de $\mathfrak{D}_0$ formé des diviseurs linéairement équivalents à zéro, par $\bar{\mathfrak{D}}_0$ le sous-groupe de $\mathfrak{D}_0$ formé des diviseurs dont chacun des composants est un point associé à l'une des valeurs absolues $v \in \overline{M}$. Pour $x \in \overline{H}$, on a, d'après le th. 9.1 , $\operatorname{div}(x) \in \bar{\mathfrak{D}}_0 + m\mathfrak{D}_0$. L'application $x \mapsto \operatorname{div}(x)$ est un homomorphisme de groupes $\overline{H} \to (\bar{\mathfrak{D}}_0 + m\mathfrak{D}_0) \cap \mathfrak{D}_1$, et on en déduit, par passage au quotient, un homomorphisme $\lambda : \overline{H} \to ((\bar{\mathfrak{D}}_0 + m\mathfrak{D}_0) \cap \mathfrak{D}_1)/m\mathfrak{D}_1$. On a $\bar{\mathfrak{D}}_0 \cap m\mathfrak{D}_0 = m\bar{\mathfrak{D}}_0$, donc $\bar{\mathfrak{D}}_0 + m\mathfrak{D}_0/m\mathfrak{D}_0 \simeq \bar{\mathfrak{D}}_0/m\bar{\mathfrak{D}}_0$, et ce dernier groupe est fini, puisque $\bar{\mathfrak{D}}_0$ est de type fini. Donc $((\bar{\mathfrak{D}}_0 + m\mathfrak{D}_0) \cap \mathfrak{D}_1) / (m\mathfrak{D}_0 \cap \mathfrak{D}_1)$ est fini. Désignons par J la jacobienne de T . D'après VA,III 8, th. 7, on a un homomorphisme canonique $\alpha : \mathfrak{D}_0 \to J$ de noyau $\mathfrak{D}_1$. Désignant par μ la multiplication par m $\mu : \mathfrak{D}_0 \to m\mathfrak{D}_0$, on voit que le groupe $\mu^{-1}(m\mathfrak{D}_0 \cap \mathfrak{D}_1)$ coïncide avec $\alpha^{-1}(\Delta_m(J))$; comme $\mu^{-1}(m\mathfrak{D}_1) = \mathfrak{D}_1$ est

.....

le noyau de α, le groupe $m\mathfrak{D}_0 \cap \mathfrak{D}_1 / m\mathfrak{D}_1$ est isomorphe au groupe $\Delta_m(J)$ des points d'ordre m de J. Or ce dernier est fini (VA,IV,6, th. 7 coroll.). Donc $m\mathfrak{D}_0 \cap \mathfrak{D}_1 / m\mathfrak{D}_1$ est fini. Donc $\mathrm{Im}\lambda$ est un groupe fini. De plus, le noyau $\ker \lambda$ se compose des $x \in \overline{H}$ tels que $\mathrm{div}(x)$ soit de la forme $m\,\mathrm{div}(y)$, avec $y \in K = \mathcal{F}_k(T)$, autrement dit des $x \in \overline{H}$ de la forme $u\,y^m$, avec $u \in k$ et $y \in K$. Comme k est algébriquement clos, on a $\ker \lambda = K^{*m}$. Donc $\overline{H}/K^{*m}$ est fini.

IO. Réduction modulo $\underline{p}$

On considère un corps K muni d'une valuation discrète ω. On désigne par A l'anneau et par $\underline{p}$ l'idéal de valuation correspondants, par t une uniformisante, par K° le corps résiduel, par λ l'homomorphisme canonique $A \longrightarrow K^\circ$. Outre le domaine universel Ω pour K, on introduit un domaine universel Ω° pour K°. On distinguera entre l'espace affine $\$_n = \Omega^n$ et l'espace affine $\$^\circ_n = (\Omega^\circ)^n$, et de même entre les espaces projectifs correspondants $\mathbb{P}_n$ et $\mathbb{P}^\circ_n$. On se bornera à l'étude de la réduction des variétés affines ou projectives, définies sur K.

Pour tout polynôme $F \in A[X] = A[X_1, \ldots, X_n]$, on note $\rho(F)$, ou $\rho_\omega(F)$, le polynôme F° réduit de

$F \pmod{\underline{p}}$. Si I est un idéal de $A[X]$, l'image $I^\circ = \rho(I) = \rho_\omega(I)$ est un idéal de $K^\circ[X]$ qu'on appelle <u>idéal réduit de $I \pmod{p}$ ($\pmod{\omega}$)</u>. On dira qu'un point $x^\circ \in \mathbb{S}^\circ_n$ est un <u>zéro</u> de I si c'est un <u>zéro de</u> I°, i.e. Si, pour tout $F \in I$, et en posant $F^\circ = \rho(F)$, on a $F^\circ(x^\circ) = 0$. Si S est un sous-K-ensemble algébrique de $\mathbb{S}_n$, on note $\mathcal{J}_\omega(S)$ l'idéal formé des polynômes de $A[X]$ qui s'annulent sur S ; l'ensemble des zéros de $I = \mathcal{J}_\omega(S)$ dans $\mathbb{S}^\circ_n$ est un sous-K°-ensemble algébrique de $\mathbb{S}^\circ_n$ qu'on note $\rho_e(S)$, ou S°_e, et qu'on appelle <u>ensemble réduit de $S \pmod{p}$ ($\pmod{\omega}$)</u> .

De même, si I est un idéal homogène de $A[X_o,\ldots,X_n]$ on dira qu'un point $x^\circ = (x^\circ_o, \ldots, x^\circ_n)$ de $\mathbb{P}^\circ_n$ est un zéro de I si c'est un zéro de l'idéal réduit $\rho(I)$. Si S est un sous-K-ensemble algébrique de $\mathbb{P}_n$, on note $\mathcal{J}_\omega(S)$ l'idéal engendré par les polynômes homogènes de $A[X]$ qui s'annulent sur S ; l'ensemble des zéros dans $\mathbb{P}^\circ_n$ de $I = \mathcal{J}_\omega(S)$ est un sous-K°-ensemble algébrique de $\mathbb{P}^\circ_n$, qu'on note $\rho_e(S)$, ou S°_e, et qu'on appelle encore ensemble réduit de S. On peut aussi définir $\rho_e(S)$ en recollant les ensembles $\rho_e(S_i)$, où S_i est l'intersection de S avec l'ouvert affine $X_i \neq 0$.

.....

Soient x un point de $\$_n$ (resp. de $\mathbb{P}_n$), et x° un point de $\$_n^\circ$ (resp.de $\mathbb{P}_n^\circ$) . S'il existe une place $\Pi : \Omega \to \Omega^\circ$ prolongeant $\lambda : A \to K^\circ$, telle que $x^\circ = \Pi(x)$, on dit que x° est une <u>p - spécialisation</u> , ou une <u>ω - spécialisation</u> de x .

Soit V une sous-K-variété de $\$_n$ (resp. de $\mathbb{P}_n$) , et soit x un point générique de V sur K . L'ensemble V_e° réduit de V coïncide avec l'ensemble des ω -spécialisations de x : pour le montrer, il suffit d'examiner le cas $V \subset \$_n$. Si $x^\circ \in V_e^\circ$, on a un diagramme commutatif

$$\begin{array}{ccc} A[X] & \xrightarrow{\mu} & K^\circ[X] \\ \alpha \downarrow & & \downarrow \alpha^\circ \\ A[x] & \xrightarrow{\nu} & K^\circ[x^\circ] \end{array}$$

Comme $\ker \alpha = I = \mathfrak{J}_\omega(V)$, et comme $\ker \alpha^\circ \supset I^\circ = \rho(I)$, on peut compléter ce diagramme par un homomorphisme $\nu : A[x] \to K^\circ[x^\circ]$, i.e. x° est une ω -spécialisation de x . Inversement, s'il existe un tel ν prolongeant λ , l'homomorphisme $\nu \circ \alpha$ s'annule sur $\ker \mu$; il existe donc un homomorphisme $\alpha^\circ : K^\circ[X] \to K^\circ[x^\circ]$ permettant de reconstituer le diagramme ci-dessus, donc x° est un zéro de $I^\circ = \rho(I)$, i.e. on a $\in x^\circ \in S_e^\circ$.

Si W° est une sous-K°variété de l'ensemble réduit V_e° d'une variété affine V définie sur K , et si x° est un

.....

point générique de W° sur K°, l'ensemble des fonctions sur V, définies sur K, et qui sont de la forme $F(x) / G(x)$, avec $F, G \in A[X]$, et $G^\circ(x^\circ) \neq 0$ est un anneau local : il s'agit en effet de l'anneau $A[x]_Q$, où Q est l'idéal premier $\ker v$. Cet anneau local est appelé <u>l'anneau local de W° sur V</u> (où de V en W°), et noté $\underline{o}(W^\circ, V)$, ou $\underline{o}_\omega(W^\circ, V)$; son idéal maximal est noté $\underline{m}(W^\circ, V)$, ou $\underline{m}_\omega(W^\circ, V)$. Une fonction f induite par F/G sur V, définie sur K, est dite <u>morphique sur W°</u> si elle appartient à $\underline{o} = \underline{o}(W^\circ, V)$. La fonction f° sur W° induite par F°/G° ne dépend que de f ; on l'appelle <u>fonction induite</u> par f sur W°. L'application $f \longmapsto f^\circ$ donne un homomorphisme surjectif $\underline{o} \longrightarrow K^\circ(x^\circ)$ de noyau $\underline{m} = \underline{m}(W^\circ, V)$, de sorte que $\underline{o}$ a pour corps résiduel $K^\circ(x^\circ)$. On dira qu'une application rationnelle $\varphi : V \longrightarrow V'$ est <u>morphique sur W°</u> si les coordonnées φ_i de φ sont morphiques sur W°. Ceci s'applique en particulier au cas où W° est un point $x^\circ \in V_e^\circ$. Une fonction $f \in \underline{o}(x^\circ, V)$ est dite <u>morphique en x°</u>, et l'élément $F^\circ(x^\circ) / G^\circ(x^\circ)$ de Ω°, qui ne dépend que de f et de x°, est noté $f^\circ(x^\circ)$, et appelé <u>valeur de f en x°</u>. De même, si une application $\varphi : V \longrightarrow W$ est morphique en x°, le point y° de coordonnées les $\varphi_i^\circ(x^\circ)$, qui appartient nécessairement à $\rho_e(W)$ est appelé valeur de φ en x°, et noté $\varphi^\circ(x^\circ)$. Si φ est birationnelle, et si φ^{-1} est morphique en y°, on a

.....

$x^\circ = (\varphi^{-1})^\circ (y^\circ)$. On dit alors que φ est bimorphique en x° . On a bien entendu des définitions analogues dans le cas où V est projective, par restriction à un ouvert affine ; on emploie les mêmes notations et la même terminologie que ci-dessus.

Dans le cas où V est une hypersurface de $\$_n$ (resp. de $\mathbb{P}_n$), l'idéal $\mathfrak{J}_\omega(V)$ est principal et engendré par un polynôme (resp. par un polynôme homogène) F irréductible de $A[X]$, i.e. irréductible dans $K[X]$ et à coefficients premiers entre eux. L'ensemble $V_e^\circ = \rho_e(V)$ est alors composé des zéros du polynôme réduit $F^\circ = \rho(F)$; ses composantes sont les hypersurfaces d'équations $G_i^\circ(X) = o$, où les G_i° sont les facteurs irréductibles de F° sur $\overline{K}^\circ$.

La variété V étant maintenant quelconque dans $\$_n$, (resp. dans $\mathbb{P}_n$) , on va ramener l'étude de la réduction de V à celle d'une hypersurface, au moyen d'une projection générique. Soient :

u_{ij} $(1 \leqslant i \leqslant n \ , \ 1 \leqslant j \leqslant r+1)$ (resp. $o \leqslant i \leqslant n \ , \ o \leqslant j \leqslant r+1$)

des éléments de Ω algébriquement indépendants sur K .

Notons $\gamma = \gamma_u$ l'application linéaire $\$_n \longrightarrow \$_{r+1}$

(resp. l'application linéaire projective $\mathbb{P}_n \longrightarrow \mathbb{P}_{r+1}$)

qui, au point x de coordonnées $(x_1, \ldots, x_n)$ (resp. $(x_o, \ldots, x_n)$) , fait correspondre le point y de coordonnées les $y_j = \sum_i u_{ij} x_i$. Soient de même u_{ij}°

.....

(les indices prenant les mêmes valeurs que ci-dessus) des éléments de Ω° algébriquement indépendants sur K°. Notons γ° l'application linéaire $\mathfrak{S}^\circ_n \to \mathfrak{S}^\circ_{r+1}$ (resp. l'application linéaire projective $\mathfrak{P}^\circ_n \to \mathfrak{P}^\circ_{r+1}$) qui, au point x°, fait correspondre le point y° de coordonnées les $y^\circ_j = \sum_i u^\circ_{ij} x^\circ_i$. Posons $A_u = A[u]$, $K_u = K(u)$ et, de même $A^\circ_u = K^\circ[u^\circ]$, et $K^\circ_u = K^\circ(u^\circ)$. La place canonique $K \to K^\circ$ se prolonge à une place canonique $K_u \to K^\circ_u$, telle que $u \mapsto u^\circ$. La valuation correspondante ω_u de K_u est celle qui, à tout $f \in A[u]$, fait correspondre la valuation du p.g.c.d. de ses coefficients. L'application γ est morphique en tout point de V et, comme on l'a déjà remarqué (démonstration du théorème 1.1), l'application $\beta : V \to \tilde{V}$ induite par γ de V sur son image $\tilde{V}$ est birationnelle. De même, si W° est une sous-variété de $V^\circ_e = \rho_e(V)$, γ° est morphique en tout point de W°, et si $\dim W^\circ \leqslant r = \dim V$, l'application $\beta^\circ : W^\circ \to \tilde{W}^\circ$ induite par γ° de W° sur son image $\tilde{W}^\circ$ est birationnelle. Il est clair qu'on a $\tilde{W}^\circ \subset \tilde{V}^\circ_e$, où $\tilde{V}^\circ_e$ est l'ensemble réduit (mod. ω_u) de $\tilde{V}$. Le théorème de prolongement E,O,I,8,th.7, permet en outre de vérifier qu'on a l'égalité $\gamma^\circ(V^\circ_e) = \tilde{V}^\circ_e$ dans le cas projectif.

.....

THEOREME 10.1 . Soit V une variété (affine ou projective) définie sur K , de dimension r . L'ensemble réduit $V_e^\circ = \rho_e(V)$ est purement de dimension r (i.e. toutes ses composantes sont de dimension r) .

Démonstration : Soit W° une composante de V_e° , et posons $s = \dim W^\circ$.

a) $s \leq r$: en effet, soient x un point générique de V sur K, et x° un point générique de W° sur K° ; parmi les coordonnées x_i° de x° , on peut trouver s éléments algébriquement indépendants sur K° ; comme x° est une ω-spécialisation de x, les x_i correspondants sont algébriquement indépendants sur K ; d'où $s \leq r$.

b) $s \geq r$: Il suffit de considérer le cas projectif $(V \subset \mathbb{P}_n)$. Compte tenu de (a) , l'application $\delta^\circ : W^\circ \longrightarrow \tilde{W}^\circ$ est birationnelle, donc on a $\dim \tilde{W}^\circ = s$. Tout revient donc à montrer que $\tilde{W}^\circ$ est l'une des composantes de $\tilde{V}_e^\circ$. Posons $y = \gamma(x)$, et $y^\circ = \gamma^\circ(x^\circ)$. Le point x° est l'unique composant de l'intersection de V_e° avec la variété linéaire $L^\circ = (\gamma^\circ)^{-1}(y^\circ)$. En effet, puisque δ° est birationnelle, on a $W^\circ \cap L^\circ = \{ x^\circ \}$, et d'autre part L° est une variété linéaire "générique parmi celles de dimension n-r-1 passant par x° " , donc ne rencontre aucune

.....

composante W'° de V_e° distincte de W° . Donc, pour toute place $\Pi : \Omega \longrightarrow \Omega^{\circ}$ prolongeant λ , telle que $\Pi(u) = u^{\circ}$ et $\Pi(y) = y^{\circ}$, on a $\Pi(x) = x^{\circ}$. Soit y° un point générique sur $\overline{K}^{\circ}$ de l'une des composantes W° de $\tilde{V}_e^{\circ}$ contenant $\tilde{W}^{\circ}$. D'une part ce point y_*° est une ω_u-spécialisation de y°, i.e. il existe une place $\Pi_* : \Omega \longrightarrow \Omega^{\circ}$ prolongeant λ telle que $\Pi_*(u) = u^{\circ}$ et $\Pi_*(y) = y_*^{\circ}$. D'autre part, y° est une spécialisation de y_*° sur $K^{\circ}{}_u$, donc il existe une place $\Pi^{\circ} : \Omega^{\circ} \longrightarrow \Omega^{\circ}$, triviale sur K° telle que $\Pi^{\circ}(y_*^{\circ}) = y^{\circ}$. D'après ce qui précède, x a pour image x° par la place composée $\Pi^{\circ} \circ \Pi_*$; autrement dit, on a $\Pi^{\circ}(x_*^{\circ}) = x^{\circ}$, en posant $x_*^{\circ} = \Pi_*(x)$. Comme l'espace projectif $\mathbb{P}_n^{\circ}$ est complet, x_*° est un point de $\mathbb{P}_n^{\circ}$; d'une part ce point x_*° appartient à V_e° et d'autre part x° est une spécialisation de x_*° sur K° . On a donc $x_*^{\circ} \in W^{\circ}$, d'où $y_*^{\circ} = \gamma^{\circ}(x_*^{\circ}) \in \tilde{W}^{\circ}$, et par suite $\tilde{W}^{\circ} = W_*^{\circ}$. Donc $\tilde{W}_o$ est bien une composante de $\tilde{V}_e^{\circ}$, c.q.f.d.

Avec les notations introduites ci-dessus, la variété $\tilde{V} = \gamma(V)$ est une hypersurface de $\mathbb{S}_{r+1}$ (resp. $\mathbb{P}_{r+1}$). Donc l'idéal $\mathfrak{J}_{\omega_u}(\tilde{V})$ est principal et engendré par un polynôme irréductible $F_u \in A_u[X]$. De même $\tilde{W}^{\circ} = \gamma^{\circ}(W^{\circ})$ est une hypersurface de $\mathbb{S}^{\circ}{}_{r+1}$ (resp. $\mathbb{P}^{\circ}{}_{r+1}$) , donc

.....

l'idéal $\mathfrak{J}(\tilde{W}^\circ)$ est principal et engendré par un polynôme irréductible $G_u^\circ \in K_u^\circ[X]$. L'ensemble réduit $\tilde{V}_e^\circ$ se compose des zéros du polynôme F_u° réduit de F_u . Comme cet ensemble contient $\tilde{W}^\circ$, le polynôme G_u° est l'un des facteurs irréductibles de F_u° . On désignera par $\nu(W^\circ)$, et on appellera <u>ω-multiplicité</u> de W° l'exposant de ce facteur dans F_u° . On appelle <u>cycle réduit</u> de V (mod.<u>p</u>) (ou mod (ω)) le cycle $\sum_{W^\circ} \nu(W^\circ)\, W^\circ$, où la somme est étendue à toutes les composantes W° de V° .

<u>Remarque 10.1</u> - On a, par la projection générique, une application injective de l'ensemble des composantes de V_e° dans celui des composantes de $\tilde{V}_e^\circ$ (ou, ce qui revient au même, dans l'ensemble des facteurs irréductibles de F_u°) . Dans le cas où V est projective, cette application est <u>bijective</u> . Il n'en est pas nécessairement de même si V est affine.

On dira que V est <u>non dégénérée</u> (<u>mod.p</u>) (ou mod.(ω)) si le cycle réduit $\rho(V)$ admet une composante unique V° de multiplicité $\nu(V^\circ) = 1$. On conviendra alors d'identifier le cycle $\rho(V)$ et la variété V° .

Si le polynôme F_u° est irréductible, V est non dégénérée (mod. <u>p</u>) , et ces deux propriétés sont équivalentes dans le cas projectif, en vertu de la remarque 10.1 .

.....

Si V et W sont deux variétés affines définies sur K, on a trivialement $\rho_e(V \times W) = \rho_e(V) \times \rho_e(W)$. Si V et et W sont non dégénérées (mod $\underline{p}$), on trouve qu'il en est de même de $V \times W$, et qu'on a $\rho(V \times W) = \rho(V) \times \rho(W)$. Supposons maintenant $V(\subset \mathbb{P}_m)$ et $W(\subset \mathbb{P}_n)$ projectives. On peut identifier $\mathbb{P}_m \times \mathbb{P}_n$ à une sous-variété de $\mathbb{P}_{mn+m+n}$ par le morphisme qui, au point $(x_o, \ldots, x_m) \times (y_o, \ldots, y_n)$, fait correspondre le point de coordonnées homogènes les $x_i y_j$. On peut donc parler de l'ensemble réduit de $V \times W$. Les formules $\rho_e(V \times W) = \rho_e(V) \times \rho_e(W)$ et $\rho(V \times W) = \rho(V) \times \rho(W)$ sont encore valables dans ces conditions.

THEOREME I0.2 - Soit V une variété (affine ou projective) définie sur K, et soit W° une composante de l'ensemble réduit $\rho_e(V)$. Les deux propriétés suivantes sont équivalentes

(a) - $\nu(W^\circ) = 1$

(b) - L'idéal $\underline{m}(W^\circ, V)$ est principal et engendré par t.

Commençons par démontrer.

.....

Lemme 10.1 - Soient $u_1 = \{u_{1ij}\}, \ldots, u_m = \{u_{mij}\}$, des spécialisations génériques indépendantes de $u = \{u_{ij}\}$. Si m est assez grand, l'idéal $\mathcal{J}(V)$ de $\Omega[X]$ est engendré par les polynômes $\overline{F}_{u_\alpha} = F_{u_\alpha} \circ \gamma_{u_\alpha}$.

(Remarque : L'équation $\overline{F}_{u_\alpha}(X) = 0$ représente le "cône générique" de base V et de "sommet" la variété linéaire définie par les équations $\sum_i u_{\alpha ij} X_i = 0$).

Il suffit d'examiner le cas affine ($V \subset \mathbb{S}_n$). Posons $P = \mathcal{J}(V)$, et soit Q l'idéal de $\Omega[X]$ engendré par les $\overline{F}_{u_\alpha}$. Il est clair qu'on a $Q \subset P$. On a d'autre part $\mathcal{J}(P) = \mathcal{J}(Q)$, i.e. P et Q ont mêmes zéros. En effet, il suffit de vérifier que $\mathcal{J}(P) \supset \mathcal{J}(Q)$ Soit, dans $\mathbb{S}_n$, $a \notin \mathcal{J}(P)$. Si m a été pris assez grand, on peut, quel que soit a, trouver un α tel que les $u_{\alpha ij}$ soient génériques indépendants sur $K(a)$. La variété linéaire L_α d'équations $\sum_i u_{\alpha ij}(X_i - a_i) = 0$ ne rencontre pas V, donc on a $\overline{F}_{u_\alpha}(a) \neq 0$, d'où $a \notin \mathcal{J}(Q)$. On a donc bien $\mathcal{J}(P) = \mathcal{J}(Q)$. Comme P est premier, Q est primaire de racine P. La différentielle $(d\,\overline{F}_{u_\alpha})_V$ appartient, pour tout α, à l'espace engendré par les

.....

$\sum_i u_{\alpha ij} (d X_i)_V$, et par suite les $(d \overline{F}_{u_\alpha})_V$ engendrent l'espace tangent de Zariski $Z(V, \$_n)$, donc (E,III,3) , les F_{u_α} forment un système de générateurs de l'anneau local $\underline{m}(V, \$_n)$. Ce dernier contient P , donc pour $f \in P$, il existe $g \notin P$ tel que $fg \in Q$. Comme Q est primaire de racine P , ceci implique $f \in Q$. On a donc $P \subset Q$, d'où $P = Q$.

Démonstration du théorème 10.2 On peut supposer V affine . Posons $\underline{o} = \underline{o}(W^\circ, V)$ et $\underline{m} = \underline{m}(W^\circ V)$. Introduisons un entier m vérifiant la condition du lemme 10.1 pour W° Soient $u_1 = u, \ldots, u_m$ des spécialisations génériques indépendantes de u sur K et, de même $u_1^\circ = u^\circ, \ldots, u^\circ_m$ des spécialisations génériques indépendantes de u° sur K° . Posons $A' = A[u_1, \ldots, u_m]$, $K' = K(u_1, \ldots, u_m)$ et $K'^\circ = K^\circ(u_1^\circ, \ldots, u_m^\circ)$. Notons ω' la valuation de A' associée à la place $K' \longrightarrow K'^\circ$ prolongeant la place canonique $K \to K^\circ$ telle que $u_\alpha \longmapsto u^\circ_\alpha$ pour tout α . Posons $\underline{o}' = \underline{o}_{\omega'}(W^\circ, V)$ et $\underline{m}' = \underline{m}_{\omega'}(W^\circ, V)$. Par un raisonnement calqué sur celui utilisé dans E,I, 9 , th. 6 on voit qu'on a $\underline{o}' \cap \mathcal{F}_K(V) = \underline{o}$ et $\underline{m}' \cap \mathcal{F}_K(V) = \underline{m}$

(a) $\Rightarrow$ (b) . On a, par hypothèse, $F^\circ_u = G^\circ_u Q^\circ$, avec $Q^\circ \in K^\circ_u[X]$ ne s'annulant pas sur W° . On a aussi

.....

$\overline{F}^{\circ}_{u} = \overline{G}^{\circ}_{u}\ \overline{Q}^{\circ}$, en posant $\overline{F}_{u} = F_{u} \circ \gamma$, $\overline{G}_{u} = G_{u} \circ \gamma$, $\overline{Q} = Q \circ \gamma$. On a donc $\overline{F}_{u} = \overline{G}_{u}\ \overline{Q} + t\ H$ avec $\overline{G}_{u}$, $\overline{Q}$ et $H \in A_{u}[X]$, admettant respectivement comme polynômes réduits $\overline{G}^{\circ}_{u}$, $\overline{Q}^{\circ}$ et H° . Désignant par $\overline{g}_{u}$, $\overline{q}$, h les fonctions de V respectivement induites par $\overline{G}_{u}$, $\overline{Q}$, H , on en déduit $\overline{g}_{u}\ \overline{q} + t\ h = 0$, d'où $\overline{g}_{u} \in t\ \underline{o}'$. On a de même $\overline{g}_{u_{\alpha}} \in t\ \underline{o}'$ pour tout α Or pour $g \in \underline{o}'$ induite par $G \in A'[X]$, la relation $g \in \underline{m}'$ équivaut à $\rho(G) \in \mathfrak{J}(W^{\circ})$. D'après le lemme IO.1 , l'idéal $\mathfrak{J}(W^{\circ})$ est engendré par les $\overline{G}^{\circ}_{u_{\alpha}}$. Donc $\underline{m}'$ est engendré par les $\overline{g}_{u_{\alpha}}$ et par t . On a donc $\underline{m}' \subset t\ \underline{o}'$, d'où $\underline{m} \subset t\ \underline{o}$ d'où $\underline{m} = t\ \underline{o}$.

(b) $\Longrightarrow$ (a) . Désignons par x un point générique de V sur K' , par x° un point générique de W° sur K'° ; soient $y = \gamma(x)$ et $y^{\circ} = \gamma^{\circ}(x^{\circ})$ les points génériques respectifs correspondants de $\tilde{V}$ sur K' et de $\tilde{W}^{\circ}$ sur K'° . Posons $\underline{\tilde{o}} = \underline{o}_{\omega'}(\tilde{W}^{\circ}, \tilde{V})$ et $\underline{\tilde{m}} = \underline{m}_{\omega'}(\tilde{W}^{\circ}, \tilde{V})$. Commençons par montrer que $\underline{o}'$ est entier sur $\underline{\tilde{o}}$. En effet, pour toute place Π de K'(y) prolongeant la place canonique $K' \longrightarrow K'^{\circ}$ et finie sur $\tilde{o}$, le point $y'^{\circ} = \Pi(\tilde{x})$ est générique de $\tilde{W}^{\circ}$ sur K° (sinon il existerait $G^{\circ} \in K'^{\circ}[X]$ tel que $G^{\circ}(y^{\circ}) \neq 0$ et $G^{\circ}(y'^{\circ}) = 0$; désignant par G un polynôme $\in A'[X]$ relevant G° , et par g la fonction induite par G sur V,

on aurait $g^{-1} \in \tilde{\underline{o}}$, et cependant $\Pi(g^{-1}) = \infty$). Or on a vu (partie (b) de la démonstration du th.10.1) que, pour une telle place Π , on a nécessairement $\Pi(x) = x'^{\circ}$, en posant $x'^{\circ} = (\beta^{\circ})^{-1}(x^{\circ})$. Comme x'° est générique de W° sur K'° , Π est finie sur $\underline{o}'$. Donc (E , O , B , 3 , th 2) , $\underline{o}'$ est bien entier sur $\tilde{\underline{o}}$.

Comme on a vu, $\beta^{\circ} : W^{\circ} \longrightarrow \tilde{W}^{\circ}$ est birationnelle, autrement dit, le monomorphisme de $\tilde{\underline{o}} / \tilde{\underline{m}} \simeq K'^{\circ}(y^{\circ})$ dans $\underline{o}' / \underline{m}' \simeq K'^{\circ}(x^{\circ})$ déduit du monomorphisme canonique $\alpha : \tilde{\underline{o}} \longrightarrow \underline{o}'$ est un isomorphisme. Donc on a (en identifiant $\tilde{\underline{o}}$ avec son image par α ,

$$(6) \qquad \underline{o}' = \tilde{\underline{o}} + \underline{m}'$$

On a d'autre part, par hypothèse, $\underline{m} = t\,\underline{o}$, d'où $\underline{m}' = t\,\underline{o}'$. Montrons qu'on a aussi $\tilde{\underline{m}} = t\,\tilde{\underline{o}}$. En effet, on a $t\,\tilde{\underline{o}} \subset \tilde{\underline{m}}$. D'autre part, compte tenu de (6), on a $\tilde{\underline{m}} \subset \underline{m}' = t\,\underline{o}' \subset t\,\tilde{\underline{o}} + t\,\underline{m}' \subset t\,\tilde{\underline{o}} + \underline{m}'^2$. Or on a $\tilde{\underline{m}} = \underline{m}' \cap \tilde{\underline{o}}$, d'où $\underline{m}'^2 \cap \tilde{\underline{o}} = t^2\underline{o}' \cap \tilde{\underline{o}} = \tilde{\underline{m}}^2$. On a donc $\tilde{\underline{m}} \subset t\,\tilde{\underline{o}} + \tilde{\underline{m}}^2$, d'où , par itération, $\tilde{\underline{m}} \subset t\,\tilde{\underline{o}} + \tilde{\underline{m}}^{\mu}$ pour tout entier $\mu \geqslant o$, d'où $\tilde{\underline{m}} \subset t\,\tilde{\underline{o}}$ par le théorème de Krull, d'où $\tilde{\underline{m}} = t\,\tilde{\underline{o}}$. L'anneau local $\tilde{\underline{o}}$ étant noétherien, et $\tilde{\underline{m}}$ étant principal , $\tilde{\underline{o}}$ est un anneau de valuation discrète (E, O, A , 7, th. 6) donc est intégralement clos. Puisque $\underline{o}'$ est entier sur $\tilde{\underline{o}}$, on a donc $\underline{o}' \subset \tilde{\underline{o}}$, d'où

.....

$\underline{o}' = \tilde{\underline{o}}$, i.e. β est bimorphique en x° , de valeur y° Supposons qu'on ait $\nu(W^\circ) > 1$. On a alors $F_u^\circ = G_u^{\circ 2} Q_1^\circ$, avec $Q_1^\circ \in K_u^\circ [X]$. On a donc $F_u = G_u^2 Q_1 + t H_1$, avec G_u , Q_1 et $H \in A_u [X]$, et $\rho(Q_1) = Q_1^\circ$. Désignant par g_u la fonction sur $\tilde{V}$ induite par G_u , on a $G_u \in \tilde{\underline{m}}$, donc $g_u \in t\,\tilde{\underline{o}}$. Posant $\underline{o}^* = \underline{o}_{\omega'}(\tilde{W}^\circ, \$_n)$, et $\underline{i} = \mathfrak{J}_{\omega'}(\tilde{V})\ \underline{o}^*$, on a donc $G_u \in t\,\underline{o}^* + \underline{i}$, d'où $F_u \in t\,\underline{o}^* + \underline{i}^2$. Comme $\underline{i} = F_u\ \underline{o}^*$, on a $\underline{i} \subset t\,\underline{o}^* + \underline{i}^2$, d'où, par itération, $\underline{i} \subset t\,\underline{o}^* + \underline{i}^n$, d'où, par le théorème de Krull, $\underline{i} = t\,\underline{o}^*$, c'est-à-dire $F_u \subset t\,\underline{o}^*$, ce qui implique $F_u \in A'[X]$, contrairement au fait que F_u est irréductible, c.q.f.d.

Dans toute la suite de ce n°, on considère un corps K muni d'un ensemble M de valeurs absolues ultramétriques discrètes telles que, quel que soit $a \in K$, on ait $v(a) = 0$ pour presque toute $v \in M$ (l'expression "pour presque toute $v \in M$" signifie : pour v appartenant au complémentaire d'un sous-ensemble fini de M) . Il en est ainsi en particulier, si M est un ensemble propre (I,10). Pour $v = -\omega \in M$, on remplacera ω par v dans la terminologie et les notations introduites ci-dessus.

* * * * *

LEMME 10.2 - Soient $F_1, \ldots, F_r$ des polynômes de $K[X] = K[X_1, \ldots, X_n]$ sans zéro commun dans $\$_n$. Alors, pour presque toute $v \in M$, les polynômes réduits $(F_i)_v^\circ = \rho_v(F_i)$ sont définis et sont sans zéro commun.

Démonstration - En effet, d'après le théorème des zéros de Hilbert, l'idéal de $K[X]$ engendré par les F_i est trivial, i.e. il existe des $G_i \in K[X]$ tels que $\sum_i G_i F_i = 1$. Dans ces conditions, pour presque toute $v \in M$,

(a) - les coefficients des F_i sont entiers (appartiennent à l'anneau A_v de v), donc les $(F_i)_v^\circ$ sont définis.

(b) - les coefficients des G_i sont entiers, et on a : $\sum_i (F_i)_v^\circ (G_i)_v^\circ = 1$, donc les $(F_i)_v^\circ$ sont sans zéro commun.

LEMME 10.3 - Si $P \in K[X] = K[X_1, \ldots, X_n]$ est absolument irréductible (i.e. irréductible sur $\overline{K}$), le polynôme réduit $P_v^\circ = \rho_v(P)$ est absolument irréductible pour presque toute $v \in M$.

Démonstration - Posons $d = \deg P$, et soient r, s deux entiers $\geqslant 0$ tels que $d = r + s$. Soient F, G, H trois polynômes de $\Omega[X]$, de degrés respectifs d, r, s.

.....

Soient a_λ $(1 \leqslant \lambda \leqslant l)$ les coefficients de F (de sorte que $F = \sum_\lambda a_\lambda M_\lambda$, où les M_λ sont tous les monômes de degré $\leqslant d$) ; soient de même b_μ $(1 \leqslant \mu \leqslant m)$ les coefficients de G et c_ν $(1 \leqslant \nu \leqslant n)$ ceux de H. La relation $F = G\,H$ se traduit par des relations de la forme $a_\lambda = U_\lambda (b_1, \ldots, b_m, c_1, \ldots, c_n)$, où les U_λ sont des polynômes universels. Soient a'_λ $(1 \leqslant \lambda \leqslant l)$ les coefficients de P. Puisque P est absolument irréductible, les polynômes $U_\lambda (X_1, \ldots, X_m, Y_1, \ldots, Y_n) - a'_\lambda$ n'ont aucun zéro commun. La propriété se conserve par réduction (mod v) pour presque toute $v \in M$, i.e. P°_v n'est pas le produit de deux polynômes de degrés respectifs r et s. D'où le lemme.

THEOREME 10.3 - Soit V une variété (affine ou projective) définie sur K. Alors

(a) - V est non dégénérée (mod v) pour presque toute $v \in M$

(b) - Si de plus V est sans point multiple, la variété réduite V°_v est aussi sans point multiple pour presque toute $v \in M$.

(c) - Soit f une fonction sur V, définie sur K, et soit $U = V - S$ l'ouvert de morphicité de f. Pour presque toute $v \in M$, la fonction f°_v induite par f sur V°_v est définie, et admet pour ouvert de morphicité $U^\circ_v = V^\circ_v - (\rho_v)^\circ_e (S)$.

....

Démonstration : Introduisons $u = (u_{ij})$ comme plus haut, et posons $v_u = -\omega_u$ Si $a \in K(u)^*$, on a encore $v_u(a) = o$ pour presque toute $v \in M$. Pour que V soit non dégénérée (mod v), il suffit que le polynôme $(F_u)^\circ_v$ réduit (mod v_u) soit irréductible. Donc (a) s'obtient par application du lemme 10.3 au polynôme F_u.

Pour démontrer (b) et (c), on peut supposer V affine ($V \subset \$_n$). Soit $\{ F_\alpha \}$ $(1 \leqslant \alpha \leqslant q)$ un système de générateurs de l'idéal $\mathcal{J}(V)$. Posons dim V = r. La propriété "V est sans point multiple" équivaut, d'après le critère jacobien (E,III,9) à celle, pour la matrice des $\left(\frac{\partial F_\alpha}{\partial X_i} \right)$, d'être de rang n-r en tout point de V. Désignant par $\{ D_\beta \}$ la famille des déterminants d'ordre n-r de cette matrice, la condition équivaut encore à la propriété pour les F_α et les D_β d'être sans zéro commun. Donc (b) s'obtient par application du lemme 10.2.

Pour prouver (c), remarquons que S se compose des zéros de l'idéal I composé des polynômes $G \in K[X]$ tels que, en désignant par g la fonction induite par G sur V, on ait $gf \in \mathcal{O}_K(V)$, où $\mathcal{O}_K(V)$ est l'anneau de coordonnées de V. Notons $\{ G_\mu \}$ un système de générateurs de l'idéal I. Pour presque toute $v \in M$, les coefficients des G_μ sont entiers, i.e. appartiennent à l'anneau A_v ; supposons en outre V non dégénérée (mod v),

.....

et soit V° la variété réduite correspondante. Dans ces conditions soit $a^\circ \in V^\circ$. Pour que $a^\circ \notin (\rho_V)^\circ_e(S)$, il faut et il suffit qu'il existe $G \in A_v[X]$ telle que l'une des $g_\alpha f$ appartienne à $\mathcal{A}_K(V)$, i.e. soit induite par un $H_\alpha \in K[X]$; nécessairement, H_α est alors à coefficients dans A_v, donc la condition ci-dessus équivaut à la propriété pour f d'être morphique en a°, c.q.f.d.

Soient maintenant V et W deux variétés (affines ou projectives) définies sur K, et soit φ un K-morphisme $V \longrightarrow W$. Il résulte du théorème précédent que, pour presque toute $v \in M$, les variétés V et W sont non dégénérées (mod v) et que, si V° et W° sont les variétés réduites correspondantes, φ induit un morphisme $\varphi^\circ : V^\circ \longrightarrow W^\circ$. Le symbole φ° possède de bonnes propriétés fonctorielles, dont la vérification est triviale à partir des définitions. En particulier, on a $(\varphi \circ \psi)^\circ = \varphi^\circ \circ \psi^\circ$, et $(\varphi \times \psi)^\circ = \varphi^\circ \times \psi^\circ$

Compte tenu de ces propriétés, on déduit du th.10.3 :

.....

THEOREME IO.4 - Soit A une variété abélienne définie sur K . Pour presque toute $v \in M$, on a les propriétés suivantes:

(a) - A est non dégénérée (mod v)

(b) - La variété réduite $A^\circ = A_v^\circ$ correspondante est sans point multiple.

(c) - La loi $\gamma^\circ : A^\circ \times A^\circ \longrightarrow A^\circ$ réduite de la loi de groupe γ de A est définie, et A°, munie de cette loi, est une variété abélienne.

Lorsque les conditions (a) , (b) et (c) sont vérifiées, on dit que A admet une bonne réduction (mod v) .

Remarque IO.2 : on peut en fait démontrer que (a) et (b) entraînent (c) .

11. - Fin de la démonstration des théorèmes 4.1 et 4.2

Compte tenu des théorèmes 7.1 , 5.3 , 8.2 et 9.2, il nous reste à démontrer que, si K est un corps de nombres, ou un corps de fonctions sur une courbe à corps des constantes algébriquement clos, si M est l'ensemble propre habituel de valeurs absolues de K , si m est un entier premier à la caractéristique de K , et si A est une variété abélienne définie sur K , telle que $\Delta_m = \Delta_m(A) \subset A_K$,

.....

l'extension $L = K\left(\frac{1}{m} A_K\right)$ de K est non ramifiée pour presque toute $v \in M$.

Or, pour presque toute $v \in M$, les points réduits c_j° des éléments $c_j \in \Delta_m$ sont distincts. Il nous suffit de prouver que lorsqu'il en est ainsi, et lorsque A admet une bonne réduction (mod v), l'extension L/K est non ramifiée pour v.

Compte tenu du lemme 9.2, il suffit de montrer que, pour $a \in A_K$, et pour $b \in A$ tel que $m\,b = a$, l'extension $K(b) / K$ est non ramifiée pour v. Or soit w l'une des valeurs absolues de $K(b)$ prolongeant v. Comme on a vu, les conjugués de b sur K sont les points $b_j = b + c_j$. Leurs points réduits respectifs b_j° (mod w) sont distincts, car on a $b_j^\circ = b^\circ + c_j^\circ$ au sens de la loi de groupe de A°, réduite de celle de A. On peut trouver une fonction f sur A, définie sur K, telle que la fonction réduite de f° sur A° soit définie, et prenne des valeurs distinctes en les b_j°. Posons $u = f(b)$; les conjugués de u sur K sont les $u_j = f(b_j)$. Les u_j° sont respectivement égaux aux $f^\circ(b_j^\circ)$, donc distincts. A fortiori, les u_j sont distincts. Comme l'extension $K(b) / K$ est séparable, on a $\left[K(u) : K\right] = \left[K(b) : K\right]$, d'où $K(b) = K(u)$, et l'extension $K(b) / K$ est bien non ramifiée, d'après le lemme 9.1.

.....

I2 - Complément : hauteur invariante sur une variété abélienne

Soit G un groupe commutatif. Une fonction sur G, à valeurs réelles $l : G \longrightarrow \mathbb{R}$ est dite <u>linéaire</u> si c'est un homomorphisme de G sur le groupe additif de $\mathbb{R}$. Une fonction $q : G \longrightarrow \mathbb{R}$ est dite <u>quadratique</u> si elle est de la forme $q(x) = F(x,x)$, où $F : G \times G \longrightarrow \mathbb{R}$ est bilinéaire symétrique. Pour toute fonction $f : G \longrightarrow \mathbb{R}$, on pose $\Delta_1 f(x,y) = f(x+y) - f(x) - f(y)$, et

$$\Delta_2 f(x,y,z) = f(x+y+z)-f(y+z)-f(z+x)-f(x+y)+f(x)+f(y)+f(z)$$

Pour que f soit linéaire, il faut et il suffit qu $\Delta_1 f = o$. Pour que f soit de la forme $f(x) = q(x)+l(x)$, avec q quadratique et l linéaire, il faut et il suffit que $\Delta_2 f = o$. Dans ce dernier cas, $\Delta_1 f$ est bilinéaire symétrique, et on a $q(x) = \frac{1}{2} \Delta_1 f(x,x)$. Comme dans II, 4, la relation "f-g est bornée" est notée $f \approx g$; en particulier "f est bornée" se traduit par $f \approx 0$.

<u>LEMME I2.1</u> - Soit $f : G \longrightarrow \mathbb{R}$ une fonction telle que $\Delta_1 f \approx 0$. Alors il existe une et une seule fonction linéaire $l : G \longrightarrow \mathbb{R}$ telle que $f \approx l$.

<u>Démonstration</u> :

<u>Unicité:</u> Soit l linéaire telle que $f \approx l$, i.e. $|f(x) - l(x)| \leqslant c_1$ pour tout $x \in G$.
Comme l est linéaire, on a, pour tout entier $n \geqslant o$,

.....

$$l(2^n x) = 2^n l(x)$$

on a d'autre part

$$| f(2^n x) - l(2^n x) | \leqslant c_1$$

On a donc

$$| l(x) - \frac{1}{2^n} f(2^n x) | \leqslant \frac{c_1}{2^n}$$

d'où

$$(7) \quad l(x) = \lim_{n \to \infty} \frac{1}{2^n} f(2^n x)$$

Existence Montrons que si $\Delta_1 f \gtrsim o$, i.e. si $|\Delta_1 f(x,y)| = |f(x+y)-f(x)-f(y)| \leqslant c$, la limite (7) existe. En effet, on a :

$$|\Delta_1 f(x,x)| = |f(2x) - 2f(x)| \leqslant c \text{ , d'où}$$

$$|\frac{1}{2} f(2x) - f(x)| \leqslant \frac{c}{2}$$

et de même

$$(8) \quad |\frac{1}{2^n} f(2^n x) - \frac{1}{2^{n-1}} f(2^{n-1} x)| \leqslant \frac{c}{2^n}$$

Comme la série de terme général $\frac{c}{2^n}$ converge, la limite (7) existe. De plus, la fonction l définie par (7) est linéaire : on le voit en écrivant que $\Delta_1 f(2^n x, 2^n y) \leqslant c$, et, en faisant tendre n vers l'infini après division des deux membres par 2^n. Enfin $f \gtrsim l$, car on déduit de (8) , par sommation,

$$|\frac{1}{2^n} f(2^n x) - f(x)| \leqslant c(\frac{1}{2} + \ldots + \frac{1}{2^n}) ,$$

.....

d'où en passant à la limite

$$|f(x) - l(x)| \leqslant c$$

LEMME I2.2 - Soit $f : G \longrightarrow \mathbb{R}$ une fonction telle que $\Delta_2 f \approx 0$. Alors il existe un et un seul couple (q,l) de fonctions $G \longrightarrow \mathbb{R}$, avec q quadratique et l linéaire , tel que $f \approx q + l$.

Démonstration : Compte tenu du lemme I2.1 , il suffit de démontrer l'existence d'une et une seule fonction quadratique q telle que $\Delta_1 (f - q) \approx 0$.

Unicité - Soit q quadratique telle que, en posant $F = \Delta_1 f$, et $G = \Delta_1 q$, on ait $F \approx Q$,
i.e. $| F(x,y) - Q(x,y) | \leqslant c_1$ quels que soient $x,y \in G$.

Comme Q est bilinéaire, on a, pour tout entier $n \geqslant 0$,

$$Q(2^n x , 2^n y) = 4^n Q(x,y)$$

On a d'autre part

$$| F(2^n x , 2^n y) - Q(2^n x, 2^n y) | \leqslant c_1$$

On a donc

$$| Q(x,y) - \frac{1}{4^n} F(2^n x, 2^n y) | \leqslant \frac{c_1}{4^n}$$

d'où

$$(9) \qquad Q(x,y) = \lim_{n \to \infty} \frac{1}{4^n} F(2^n x, 2^n y)$$

ce qui montre l'unicité de Q, d'où celle de q, puisque $q(x) = \frac{1}{2} Q(x,x)$.

.....

Existence : Montrons que si $\Delta_2 f \overset{\sim}{\leq} 0$, i.e. si $| F(x, y + z) - F(x,y) - F(x,z) | \leqslant c$, en posant à nouveau $\Delta_1 f = F$, la limite (9) existe . En effet, l'inégalité ci-dessus entraîne

$$| F (2x, 2y) - 4 F (x, y) | \leqslant 3 c$$

ou encore

$$| \tfrac{1}{4} F (2x, 2y) - F (x,y) | \leqslant \tfrac{3}{4} c$$

et de même

$$(10) \qquad | \tfrac{1}{4^n} F (2^n x , 2^n y) - \tfrac{1}{4^{n-1}} F(2^{n-1}x,2^{n-1}y)| \leqslant \tfrac{3}{4^n} c$$

Comme la série de terme général $\frac{3}{4^n} c$ converge, la limite (9) existe. De plus, la fonction Q définie par (9) est bilinéaire. On le voit en remarquant que

$$| F (2^n x, 2^n y + 2^n z) - F (2^n x, 2^n y) - F (2^n x, 2^n z)| \leqslant c$$

et en faisant tendre n vers l'infini, après division des deux membres par 4^n . Enfin, en posant $Q = \Delta_1 q$, on a bien $\Delta_1 (f-g) = F - Q \overset{\sim}{\leq} 0$, car on déduit de (10) , par sommation,

$$| \tfrac{1}{4^n} F (2^n x, 2^n y) - F(x,y)| \leqslant 3 c (\tfrac{1}{4} + \ldots + \tfrac{1}{4^n})$$

d'où, en passant à la limite

$$| F (x,y) - Q (x,y) | \leqslant c ,$$

c.q.f.d.

Soit maintenant K un corps muni d'un ensemble propre M de valeurs absolues vérifiant la formule du produit (cf. I , 11, 12 et I3) et soit A une variété

.....

abélienne définie sur K. Considérons une application rationnelle $\varphi : A \to \mathbb{P}_n$, à valeurs dans l'espace projectif $\mathbb{P}_n$, définie sur K. Cette application est un morphisme (VA,I,5, th 6). Pour $x \in A_K$, posons, comme dans II, 4, $h_\varphi(x) = h(\varphi(x))$; regardons h_φ comme une fonction $A_K \longrightarrow \mathbb{R}$.

THEOREME I2.1 On a $\Delta_2\ h_\varphi \approx 0$.

Démonstration - Posons $B = A \times A \times A$. Notons π_1, π_2, π_3 les projections respectives $B \to A$ sur les trois facteurs. Pour $1 \leqslant i \leqslant j \leqslant 3$, posons $\pi_{ij} = \pi_i + \pi_j$ (de sorte qu'on a, par exemple, $\pi_{23}(x, y, z) = y + z$) ; posons de même $\pi_{123} = \pi_1 + \pi_2 + \pi_3$. La relation à démontrer s'écrit

$$h_{\pi_{123}\circ\varphi} - \sum_{i<j} h_{\pi_{ij}\circ\varphi} + \sum_i h_{\pi_i\circ\varphi} \approx 0$$

Désignons par H un hyperplan de $\mathbb{P}_n$ tel que le symbole $X = \varphi^{-1}(H)$ soit défini (de sorte que $X \in \mathcal{L}_\varphi$, avec les notations de II, 4). D'après II, th. 4.1 et 4.2, il suffit de prouver que le diviseur

$$Y = \pi_{123}^{-1}(X) - \sum_{i<j} \pi_{ij}^{-1}(X) + \sum_i \pi_i^{1}(X)$$

.....

est linéairement équivalent à zéro.

Or, quels que soient a et $b \in A$, on trouve par application répétée de VA,III,3, lemme 5,

$$\pi_3 (Y . (a \times b \times A)) = X_{-a-b} - X_{-a} - X_{-b} + X$$

Donc le premier membre est ~ 0, en vertu du théorème du carré. D'après VA,III,3, lemme 6, il existe un diviseur Z sur $A \times A$ tel que

$$Y \sim Z \times A$$

On a de même, quels que soient a et $c \in A$,

$$\pi_2 (Y . (a \times A \times c)) \sim 0$$

On a donc

$$\pi_2 (Z . (b \times A)) \sim 0$$

Donc il existe un diviseur T sur A tel que

$$Z \sim T \times A$$

Enfin, quels que soient b et $c \in A$, on a

$$\pi_1 (Y . (A \times b \times c)) \sim 0$$

ce qui donne $T \sim 0$, d'où $Y \sim 0$, c.q.f.d.

THEOREME I2.2 - Soit A une variété abélienne définie sur K, et soit φ un K-morphisme $A \to \mathbb{P}_n$. Il existe un et un seul couple (q_φ, l_φ) de fonctions $A_K \to \mathbb{R}$, avec q_φ quadratique et l_φ linéaire, telles qu'on ait

.....

$h_\varphi \overset{\sim}{\sim} g_\varphi$, en posant $g_\varphi = q_\varphi + l_\varphi$. De plus, les fonctions q_φ, l_φ et g_φ ne dépendent que de la classe $\mathcal{C}_\varphi$ (pour l'équivalence linéaire) du système linéaire $\mathcal{L}_\varphi$ associé à φ .

Démonstration - D'une part, la première assertion résulte du lemme I2.2 et du th. I2.1 .

D'autre part, si φ' : $A \longrightarrow \mathbb{P}_n$, est un K-morphisme tel que $\mathcal{C}_{\varphi'} = \mathcal{C}_\varphi$, on a $h_{\varphi'} \overset{\sim}{\sim} h_\varphi$ (II , th. 4.1) . La propriété d'unicité du lemme I2.2 entraîne donc $g_{\varphi'} = g_\varphi$, c.q.f.d.

Le symbole g_φ pourra encore être désigné par $g_{\mathcal{C}}$, en posant $\mathcal{C} = \mathcal{C}_\varphi$, ou encore par g_X , Si X est un diviseur appartenant à $\mathcal{C}$. Si $X \sim X_1 + X_2$, on a $g_X = g_{X_1} + g_{X_2}$ (d'après II , th. 4.2) . Ceci permet de prolonger, par linéarité, la définition du symbole $g_X = g_{\mathcal{C}}$ au cas où X est un diviseur quelconque sur A , défini sur K .

THEOREME I2.3 - Soient A et B deux variétés abéliennes définies sur K , et soit α : $B \longrightarrow A$ un K-morphisme. Soit X un diviseur sur A , rationnel sur K , et posons $Y = \alpha^{-1}(X)$. Soient b, b', $\in B_K$, et posons

.....

$a = \alpha(b)$, $a' = \alpha(b')$. Alors on a

$$g_Y(b') - g_Y(b) = g_X(a') - g_X(a) \quad .$$

En particulier, si α est un k-homomorphisme, on a $g_Y(b) = g_X(a)$.

Démonstration- : Il suffit de considérer le cas où X appartient au système linéaire $\mathcal{L}_\varphi$ associé à un K-morphisme $\varphi : A \longrightarrow \mathbb{P}_n$. Posant $\psi = \varphi \circ \alpha$, on a $h_\psi = h_\varphi \circ \alpha$. Pour $x \in A_K$, posons $g'_X = g_X(x+a) - g_X(a)$, et $h'_\varphi(x) = h_\varphi(x+a) - h_\varphi(a)$; de même, pour $y \in B_K$, posons $g'_Y(y) = g_Y(y+b) - g_Y(b)$, et $h'_\psi(y) = h_\psi(y+b) - h_\psi(b)$. On a $g'_X \tilde{\sim} h'_\varphi$, et $g'_Y \tilde{\sim} h'_\psi$, d'où $g'_Y - g'_X \circ \alpha \tilde{\sim} h'_\psi - h'_\varphi \circ \alpha = 0$. Compte tenu du fait que α est le composé d'un homomorphisme et d'une translation (VA,I,6 , th. 8) la fonction $g'_Y - g'_X \circ \alpha$ est linéaire. Donc elle est nulle, c.q.f.d.

D'après ce théorème, le symbole $g_X(x)$, qu'on peut appeler hauteur invariante de x relativement à X , est invariant par tout K-isomorphisme $A \longrightarrow B$ (pour la structure de variété abélienne) .

Remarque - Supposons $X \equiv 0$. On a alors $X_b \sim X$ pour tout $b \in A_K$, d'où $g_{X_b} = g_X$. En appliquant le th. I2.3

.....

à la translation $\tau_{-b} : x \to x-b$, on obtient

$g_{X_b}(a+b) - g_{X_b}(b) = g_X(a) - g_X(0)$, d'où

$g_X(a+b) = g_X(a) + g_X(b)$, i.e. g_X est <u>linéaire</u>,

i.e. on a $q_X = 0$. Dans ce cas, $G_X(x) = g_{\mathscr{C}}(x)$

<u>est une fonction bilinéaire de $\mathscr{C}$ et de x</u> .

On en déduit en outre que, pour X arbitraire, q_X ne dépend que de la classe de X modulo l'équivalence $\equiv$; il n'en est pas de même, en général, de l_X .

2ème trimestre 1981

N° d'impression 492