PUBLICATIONS

MATHEMATIQUES

D'ORSAY

André NÉRON

VARIÉTÉS ABÉLIENNES

(cours 1965-66, retirage 1979)

Université de Paris-Sud

Département de Mathématique

Bât. 425

91405 ORSAY France

PUBLICATIONS

MATHEMATIQUES

D'ORSAY

André NÉRON

VARIÉTÉS ABÉLIENNES

(cours 1965-66, retirage 1979)

Université de Paris-Sud

Département de Mathématique

Bât. 425

91405 ORSAY France

TABLE DES MATIERES

CHAPITRE III

La Jacobienne d'une courbe algébrique.

CHAPITRE IV

Diviseurs sur les variétés abéliennes.

CHAPITRE I

VARIETES DE GROUPE ET VARIETES ABELIENNES

Premières propriétés

(Le cours de l'année 1964-65 : "Notions élémentaires de Géométrie algébrique" est cité E ;

1. Variétés de groupe.

Définition : On appelle variété de groupe une variété algébrique G munie d'une structure de groupe vérifiant les conditions suivantes :

(a)- La loi de groupe λ de G est un morphisme $G \times G \to G$

(b)- L'application $\sigma : x \mapsto x^{-1}$ est un morphisme $G \to G$.

(n.b. : on convient d'identifier tout morphisme $V \to W$ avec l'application de V dans W qui lui correspond).

Dans le cas général (où l'on ne suppose pas nécessairement G commutatif), la loi est notée multiplicativement, i.e. on pose $\lambda(x,y) = x.y$; à partir du n° 6 de ce Chap., les groupes considérés seront presque toujours commutatifs, et on emploiera pour ceux-ci la notation additive $\lambda(x,y) = x + y$.

Soit k un corps. On dit qu'une variété de groupe G est définie sur k, ou que k est un corps de définition de G si G est définie sur k comme variété algébrique, et si les morphismes λ et σ sont définis sur k .

Il en résulte alors que l'élément neutre e de G est rationnel sur k . En effet, soit x un point générique de G sur le corps $k(e)$. D'après (b), le point x^{-1} est rationnel sur $k(x)$. Donc $e = x\,x^{-1}$ est rationnel sur $k(x)$. Comme $k(e)$ et $k(x)$ sont des extensions linéairement disjointes de k

.../...

(EA, I, 9, th. 5bis), on a $k(e) \cap k(x) = k$. Donc e est rationnel sur k .

Pour $a \in G$, on note τ_a (resp. τ'_a) la translation à gauche (resp. à droite) définie par $\tau_a(x) = ax$ (resp. $\tau'_a(x) = x.a$). Une telle translation est un isomorphisme de G pour la structure de variété algébrique. En effet, il résulte de la condition (a) de la définition que τ_a (resp. τ'_a) est un morphisme, et qu'il en est de même de l'application réciproque τ_a^{-1} (resp. τ'^{-1}_a).

THEOREME 1.

Toute variété de groupe G est sans point multiple.

Démonstration. En effet, il existe $a_o \in G$, simple sur G (E, Chap. III, 10, th. 8). Pour $a \in G$, on peut trouver une translation τ sur G telle que $\tau(a_o) = a$. Comme τ est un isomorphisme, a est simple sur G .

Remarque : le couple de conditions (a) et (b) de la définition d'une variété de groupe équivaut à la condition suivante :

(a')- L'application $\mu : G \times G \to G$ définie par $\mu(x,y) = y\, x^{-1}$ est un morphisme.

2. Groupes algébriques.

Définition : On appelle groupe algébrique un sous-ensemble algébrique H d'une variété (abstraite) admettant pour composantes des variétés H_α deux à deux disjointes, et muni d'une structure de groupe vérifiant les conditions suivantes :

(a)- Pour tout couple de composantes (H_α , H_β) de H , la loi de groupe λ de H induit un morphisme $\lambda_{\alpha\beta} : H_\alpha \times H_\beta \to H_\gamma$, où H_γ est une composante de H .

(b)- Pour toute composante H_α de H , l'application

.../...

$\sigma_\alpha : x \to x^{-1}$ induit un morphisme $\sigma_\alpha : H_\alpha \to H_{\alpha'}$, où $H_{\alpha'}$ est une composante de H.

La notion de variété de groupe est un cas particulier de celle de groupe algébrique et, plus précisément, s'identifie à celle de groupe algébrique à une seule composante.

On dit que H est <u>défini sur k</u> si les variétés H_α et les morphismes $\lambda_{\alpha\beta}$, σ_α sont définis sur k.

La notion de groupe algébrique possède les propriétés élémentaires suivantes, qu'on établira à titre d'exercice : si H est défini sur k, l'élément neutre e de H est un point rationnel sur k ; toute translation (à droite ou à gauche) sur H induit sur tout composante H_α de H un isomorphisme $H_\alpha \to H_\beta$ de H_α sur une composante H_β de H ; chacune des variétés H_α est sans point multiple (démonstrations calquées sur celles données plus haut dans le cas des variétés de groupe); la composante H_o de e est une variété de groupe ; c'est, de plus, un sous-groupe distingué de H, et les composantes H_α coïncident avec les classes de ce sous-groupe.

La dimension commune des H_α est appelée <u>dimension</u> de H.

<u>Remarque 2</u> : Comme dans le cas des groupes algébriques, on peut réduire le couple de conditions (a), (b) à une seule condition en utilisant, au lieu de la loi de groupe λ, la loi $\mu(x,y) = y\,x^{-1}$.

<u>THEOREME 2</u>.

Soit G une variété de groupe, définie sur k, et soit H un sous-groupe de G qui est en même temps un sous-ensemble fermé (i.e. un sous-ensemble algébrique) de G. Alors H est un sous-groupe algébrique de G.

.../...

Démonstration. Montrons que deux composantes distinctes quelconques H_α et H_β sont sans point commun. Supposons en effet qu'il existe $a \in H_\alpha \cap H_\beta$.

Considérons l'application $\psi : G \times G \to G$ obtenue en posant $(x,y) = x.a^{-1}.y$. Il résulte des définitions que ψ est un morphisme ; ce morphisme est de plus, défini sur le corps $k' = k(a)$. Soit x_α (resp. x_β) un point générique de H_α (resp. H_β) sur k' , et posons $z = \psi(x_\alpha , x_\beta) = x_\alpha . a^{-1}.x_\beta$. Comme H est un sous-groupe de G , on a $z \in H$. Comme H est fermé dans G , le lieu Z de z sur k' (i.e. la variété image $\psi_g(H_\alpha \times H_\beta)$ au sens de E , chap. I, 11) est contenue dans H . D'autre part, on a $\psi(x_\alpha,a) = x_\alpha \in Z$, d'où $H_\alpha = \mathrm{loc}_{k'} x_\alpha \subset Z$. On a donc $H_\alpha = Z$, puisque H_α est une composante de H . On a de même $\psi(a,x_\beta) = x_\beta \in Z$, et on en déduit $H_\beta = H_\alpha = Z$, contrairement à l'hypothèse $H_\alpha \neq H_\beta$.

Notons λ la loi de groupe sur G , et λ' celle induite sur H . Comme H est fermé dans G , la variété $\lambda_g(H_\alpha \times H_\beta)$ est contenue dans H , donc est contenue dans l'une des composantes H_γ de H . Donc le morphisme induit par λ (i.e. par λ') sur $H_\alpha \times H_\beta$ est à valeurs dans H_γ . La loi de groupe λ' de H vérifie donc la condition (a) ; de la même façon, on voit qu'elle vérifie (b). Donc H est bien un sous-groupe algébrique de G .

Remarque 3 : Les composantes de H sont définies sur la clôture algébrique $\bar{k}$ de k (donc sur une extension algébrique de k), et sont permutées par tout k-automorphisme de $\bar{k}$. Un tel automorphisme laisse invariant l'élément neutre e de H , donc laisse invariante la composante H_0 de e ; celle-ci est donc k-fermée dans H , et, par suite définie sur une extension

.../...

radicielle de k ; elle n'est pas, en général, définie sur k .

3. Homomorphismes.

Soient G et G' deux variétés de groupe. On dit qu'une application $\phi : G' \to G$ est un homomorphisme (pour la structure de variété de groupe) si ϕ est à la fois un morphisme et un homomorphisme pour la structure de groupe.

THEOREME 3.

Soit $\phi : G' \to G$ un homomorphisme de variétés de groupe. Alors

(a)- le noyau $H = \ker \phi$ est un sous-groupe algébrique de G'.

(b)- L'image $I = \mathrm{Im}\ \phi$ est une sous-variété de groupe G .

(c)- On a $\dim H = \dim G' - \dim I$.

Démonstration. L'assertion (a) résulte du théorème précédent, et au fait que $H = \phi^{-1}(0)$ est fermé dans G (puisque ϕ est un morphisme). D'autre part, l'image $\phi(G') = I$ est un sous-groupe de G . Pour prouver (b), il suffit de montrer que I coïncide avec l'image au sens générique $\overline{I} = \phi_g(G')$ (cf. E, I, 11, et EA, I, 11) ; comme on a $I \subset \overline{I}$, il suffit de prouver que $\overline{I} \subset I$.

Remarquons d'abord que $\overline{I}$ est un sous-groupe de G : en effet, on a $\lambda_g(\overline{I} \times \overline{I}) \subset \overline{I}$, et a fortiori $\lambda(\overline{I} \times \overline{I}) \subset \overline{I}$, i.e. $\overline{I}$ est stable par λ ; on voit de même que $\overline{I}$ est stable par $\sigma : x \mapsto x^{-1}$.

Soit maintenant $b \in \overline{I}$. Comme $\overline{I}$ est l'adhérence de I (EA, I, 11), tout point générique de $\overline{I}$ sur $k' = k(b)$ appartient à I . Soit u un tel point, et posons $v = u^{-1} b$; on a aussi $b = u v$, et $u = b^{-1} v$; on a donc $k'(u) = k'(v)$, et v est aussi un point générique de $\overline{I}$ sur k' , de sorte qu'on a

.../...

$v \in I$. Comme I est un sous-groupe de G , on a $b = u\,v \in I$. On a donc bien montré que $\overline{I} \subset I$, et prouvé l'assertion (b).

Soit x' un point générique de G' sur k . Alors $x = \phi(x')$ est générique de I sur k . L'image réciproque $\phi^{-1}(x')$, qui est une classe de G' suivant H coïncide avec le lieu $\mathrm{loc}_{k(x)}x'$. Donc on a $\dim H = \deg.\ \mathrm{tr}.(k(x')/k(x))$. On a d'autre part $\dim I = \deg.\ \mathrm{tr}.(k(x)/k)$. On a donc bien $\dim H = \dim G' - \dim I$

C.Q.F.D.

Signalons que le th. 3 admet la réciproque suivante, due à Rosenlicht (dont nous n'aurons pas à faire usage dans la suite) :

Soit H un sous-groupe algébrique d'une variété de groupe G . On peut munir le quotient G/H d'une structure de variété de groupe compatible avec la structure de groupe, et telle que l'application canonique $\phi : G \to G/H$ soit un morphisme séparable. Cette variété de groupe est unique à un isomorphisme près (on l'appelle variété de groupe <u>quotient</u> de G par H).

k étant un corps de définition pour G, H et ϕ , la condition ϕ séparable de l'énoncé signifie que, pour x générique de G sur k et pour $y = \phi(x)$, l'extension $k(x)/k(y)$ est séparable. Cette condition est essentielle pour la propriété d'unicité. En effet, si G est une variété de groupe définie sur un corps k non parfait de caractéristique $p \neq 0$, il existe des isomorphismes $\phi : G \to G$ pour la structure de groupe qui sont des morphismes, mais non des isomorphismes, pour la structure de variété algébrique. Il suffit de prendre pour ϕ l'application induite par l'une quelconque des puissances de l'automorphisme de Frobenius $x \to x^p$ du domaine universel.

.../...

4. Quelques propriétés des variétés complètes.

LEMME 1. Soient V une variété, W une variété complète, Z un sous-ensemble fermé de $V \times W$. Alors la projection $pr_1 Z$ est fermée dans V.

Démonstration. On peut supposer que Z est une sous-variété de $V \times W$. Soit k un corps de définition de V, W et Z, et soit x, y un point générique de Z sur k. Il suffit de prouver que $pr_1 Z$ coïncide avec sa k-adhérence ; or celle-ci est la variété $(pr_1)_g Z = loc_k x$. Soit $a \in (pr_1)_g Z$. On peut trouver une place ρ du domaine universel telle que $\rho(x) = a$. Comme V est complète, ρ est finie en y. Posons $\rho(y) = b$. Comme Z est fermée dans $V \times W$, on a $a \times b \in Z$. On a donc $a = pr_1(a \times b) \in$ $\in pr_1 Z$, C.Q.F.D.

LEMME 2. Soient V une variété complète, W une variété, et soit ϕ un morphisme $V \to W$. L'image $\phi(V)$ est une variété complète.

Démonstration. D'après le lemme 1, l'image $\phi(V) = pr_W(\Gamma_\phi)$ est fermée dans W, donc coïncide avec son adhérence dans W, i.e. avec la variété $\phi_g(V)$. Soit k un corps de définition pour V, W et ϕ, et soit x un point générique de V sur k. Alors $y = \phi(x)$ est un point générique de $\phi(V)$ sur k. Soit ρ une place du domaine universel Ω. Comme V est complète, ρ est finie en x. Si, de plus, on pose $\rho(x) = a$, ρ est finie sur l'anneau local $o(a,V)$. Or, puisque ϕ est morphique en a, les coordonnées de y appartiennent à cet anneau. Donc ρ est finie en y.

THEOREME 4.

Soient V une variété complète, U et W deux variétés,

.../...

ϕ un morphisme $U \times V \to W$. S'il existe $a_o \in U$ tel que $\phi(a_o,b)$ ne dépende pas de b, on a, quels que soient $a \in U$ et $b \in V$, $\phi(a,b) = \psi(a)$, où ψ est un morphisme $U \to W$.

Démonstration. (extraite du Séminaire Chevalley, 1958/59, Douady, exposé 9). Pour b_1, $b_2 \in V$, l'ensemble $E(b_1,b_2)$ des $a \in U$ tels que $\phi(a,b_1) = \phi(a,b_2)$ est un sous-ensemble fermé de U. L'intersection $E = \bigcap_{b_1,b_2} E(b_1,b_2)$ est donc un sous-ensemble fermé de U. Montrons que c'est aussi un ouvert de U. En effet, soit a_1 un point de E. Alors le point $c_1 = \phi(a_1,b)$ de W ne dépend pas de b. Soit S un ouvert affine de W contenant c_1, et soit $F = W - S$ le fermé complémentaire. Comme ϕ est un morphisme, $\phi^{-1}(F)$ est un fermé de $U \times V$. Comme V est complète, l'ensemble $G = pr_1\, \phi^{-1}(F)$ est fermé dans U, en vertu du lemme 2. On a $a_1 \in U - G$, et pour $u \in U - G$, l'application $\phi_u : V \to W$ obtenue en posant $\phi_u(y) = \phi(u,y)$ est un morphisme dont l'image est dans S. D'après le lemme 2, cette image est une sous-variété complète de S, donc est une variété affine complète, donc est réduite à un point. On a donc $U - G \subset E$, donc E est un voisinage de a_1. On a donc montré que E est un ouvert de U.

L'ensemble E, non vide (puisque $a_o \in E$), est à la fois ouvert et fermé dans U, donc coïncide avec U. Il existe donc une application $\psi : U \to W$ telle que $\phi(a,b) = \psi(a)$. En prenant $b = b_o$ fixe, on voit que f est un morphisme.

5. Variétés abéliennes.

On appelle variété abélienne une variété de groupe complète.

THEOREME 5. (Chevalley).

La loi de groupe d'une variété abélienne A est commutative.

.../...

Démonstration. En effet, considérons le morphisme $\phi : A \times A \to A$ obtenu en posant $\phi(x,y) = x.y.x^{-1}$. Pour tout $x \in A$, on a $\phi(x,e) = e$. D'après le th. 4, il existe donc un morphisme $\psi : A \times A \to A$, tel qu'on ait identiquement $\phi(x,y) = \psi(y)$. En faisant $x = e$, on obtient $\phi(e,x) = y = \psi(y)$ quel que soit y, d'où $x.y.x^{-1} = y$, C.Q.F.D.

LEMME 3. Soit ϕ une application rationnelle $V \to W$ d'une variété normale V dans une variété complète W. L'ensemble (fermé) E des points de V où ϕ n'est pas morphique est de codimension ≥ 2 sur V (i.e. chacune de ses composantes est de codimension ≥ 2).

Démonstration. Soit X une composante de E. Soit k un corps de définition de V, W, ϕ et X, et soit x un point générique de X sur k. Le sous-ensemble fermé $F = \phi_e(x) = pr_2(\Gamma_\phi \cap (x \times W))$ est non vide, puisque W est complète. Soit Y une $k(x)$-composante de F, et soit y un point générique de Y sur $k(x)$. Posons $n = \dim V$, et supposons qu'on ait $\operatorname{codim} X = 1$, i.e. $\dim X = n-1$. Alors $k(x)$ est de degré de transcendance $n-1$ sur k. Soit Z le lieu du point (x,y) sur k. On a $Z \subset \Gamma_\phi$; mais comme $pr_1 Z = X$, on a $Z \neq \Gamma_\phi$. Or $\dim \Gamma_\phi = n$. Donc le degré de transcendance de $k(x,y)$ sur k est $\leq n-1$. Par suite y est algébrique sur $k(x)$, i.e. on a $\dim Y = 0$. Donc l'ensemble $F = \phi_e(x)$ est fini. Comme V est normale, ϕ est morphique en x, et ceci contredit l'hypothèse $X \subset E$.

THEOREME 6. (Weil).

Toute application rationnelle $\phi : V \to A$ d'une variété sans

.../...

point multiple dans une variété abélienne est un morphisme.

Compte tenu du lemme 3, ce théorème se déduit du suivant, plus général :

THEOREME 7.

Soit $\phi : V \to G$ une application rationnelle d'une variété V sans point multiple dans une variété de groupe G. L'ensemble des points de V en lesquels ϕ n'est pas morphique est purement de codimension 1 (i.e. toutes ses composantes sont des sous-variétés de codimension 1 de V).

Démonstration. Soit k un corps de définition de V, G et ϕ, et soit ψ l'application rationnelle $V \times V \to G$, définie sur k, telle qu'on ait

$$(1) \qquad \psi(x,y) = \phi(x)\ \phi(y)^{-1},$$

où x et y sont deux points génériques indépendants de V sur k. Soit b un point de V. La loi de groupe de G étant un morphisme, si ϕ est morphique en a, ψ est morphique en (a,a). Inversement, montrons que, si ψ est morphique en (a,a), ϕ est morphique en a. En effet, on peut supposer x et y génériques indépendants sur le corps $k' = k(a)$. La relation (1) s'écrit encore

$$(2) \qquad \phi(x) = \phi(y)\ \psi(x,y).$$

Comme ψ est morphique en (a,a), ψ est a fortiori morphique en (a,y). Le second membre de (2) est donc morphique en (a,y). Il en résulte bien que ϕ est morphique en a. En outre, d'après (1), on a alors necessairement $\phi(a,a) = e$.

Introduisons un ouvert affine U de G contenant e, et soient $\psi_i(x,y)$ les coordonnées de $\psi(x,y)$ relativement à U.

.../...

Pour que ψ soit morphique en (a,a) (i.e. pour que ϕ le soit en a), il faut et il suffit que chacune des ψ_i le soit en (a,a). En particulier, si l'on suppose ϕ non morphique en a, il existe un i tel que ψ_i ne soit pas morphique en (a,a), donc (critère de morphicité, E, Chapitre IV, 5, th. 8), tel que $(a,a) \notin \text{supp } \Gamma(\psi_i)^-$. En d'autres termes, il existe une composante X de $\Gamma(\psi_i)^-$ contenant (a,a). Cette composante X ne peut contenir la diagonale Δ_V : dans ce cas, en effet, on aurait $(x,x) \in \text{supp } \Gamma(\psi_i)^-$, et ψ_i ne serait pas morphique en (x,x) ; donc ϕ ne serait pas morphique en x, ce qui est absurde. L'intersection $X \cap \Delta_V$ est donc distincte de Δ_V. Comme V est sans point multiple, il en est de même de $V \times V$. D'après le théorème de la dimension (E chap. III), il existe une composante Z de $X \cap \Delta_V$ contenant (a,a), et de dimension $\dim Z \geq \dim V - 1$. Comme $Z \neq \Delta_V$, on a $\dim Z = \dim V - 1$, et Z est nécessairement de la forme Δ_W, où W est une sous-variété de codimension 1 de V, contenant a. La fonction ψ_i n'est pas morphique sur Δ_W, et par suite ϕ ne l'est pas sur W.

On a finalement montré que, si E est l'ensemble (fermé) des points de V en lesquels ϕ n'est pas morphique, il passe par tout $a \in E$ une composante de E de codimension 1 sur V. Il en résulte bien que E est purement de codimension 1.

6. Application rationnelle d'un produit dans une variété abélienne.

(N.B. dans toute la suite, on utilisera la notation additive pour la loi de groupe sur une variété abélienne).

THEOREME 8.

Soient $\phi : V \times W \to A$ une application rationnelle, où V et W sont deux variétés quelconques, et A une variété abélienne.

.../...

Soit k un corps de définition pour V, W, A et ϕ ; soient x et y deux points génériques indépendants de V et W sur k. Alors il existe deux applications rationnelles $\alpha : V \to A$ et et $\beta : W \to A$ telles qu'on ait $\phi(x,y) = \alpha(x) + \beta(y)$.

Démonstration. On examine successivement les cas suivants :

a)- V est une courbe complète sans point multiple, et W est une variété sans point multiple. Alors $V \times W$ est une variété sans point multiple. Donc ϕ est un morphisme, d'après le th. 5. Le morphisme $\theta : V \times W \to A$ défini par $\theta(x,y) = \phi(x,y) - \phi(x,a)$ prend la valeur constante 0 sur $V \times a$. D'après le th. 4, il existe un morphisme $\beta : W \to A$ tel que $\theta(x,y) = \beta(y)$. On a donc $\phi(x,y) = \phi(x,a) + \beta(y)$, et le théorème est démontré dans ce cas.

b)- V est une courbe quelconque, et W est une variété quelconque. Remarquons que la propriété de l'énoncé est birationnellement invariante en V et W. D'après E, chap. IV, 4, on peut trouver une courbe V' normale (donc sans point multiple) et complète, birationnellement équivalente à V. On se ramène au cas (a) en remplaçant le couple (V,W) par le couple (V',W'), où W' est l'ouvert des points simples de W.

c)- Cas général.- On peut supposer V affine. On raisonne par récurrence sur $n = \dim V$, au moyen du lemme suivant :

LEMME 4. Soit V une variété affine $(V \subset \mathfrak{S}_m)$, et soit a un point simple de V. Soit k un corps de définition de V et de a. Soit L_u l'hyperplan générique $F_u(x) = \sum_{i=1}^{m} u_i(X_i - a_i) = 0$, où les u_i sont algébriques indépendants sur k. Alors, l'intersection $L_u \cap V$ contient une sous-variété Z de codimension 1 de V, passant par a, et telle que a soit simple sur Z

.../...

Si dim $V \geqslant 2$, tout point générique x de Z sur $\overline{k(u)}$ est aussi un point générique de V sur k.

Démonstration du lemme. Posons $n = \dim V$. D'après le théorème de la dimension, $L_u \subset V$ possède une composante W contenant a, de dimension $\geq n-1$. Comme on a $Z \subset L_u$, on a $Z \neq V$, donc dim $Z = n-1$. Comme $L_u \cap V$ est un $k(u)$-ensemble algébrique, Z est définie sur $k' = \overline{k(u)}$. Si x est générique de Z sur k', on a deg. tr. $(k'(x)/k') = n-1$, d'où deg. tr.$(k'(x)/k) = m + n-1$. On a de plus $\sum_i u_i(x_i - a_i) = 0$. Comme les $x_i - a_i$ ne sont pas tous nuls (car on a dim $V \geq 2$, d'où dim $Z \geq 1$), c'est là une relation de dépendance algébrique entre les u_i sur le corps $k(x)$. On a donc deg. tr. $(k'(x)/k(x)) \leq m-1$. On en déduit deg. tr.$(k(x)/(k) \geq m + n-1 - (m-1) = n$. Donc x est générique de V sur k.

Le fait que a est simple sur Z s'obtient en remarquant que la différentielle $(dF_u)_a$ n'appartient pas à l'espace engendré par les $(df_\alpha)_a$, où $\{f_\alpha\}$ est un système de générateurs de l'idéal $\mathfrak{J}_k(V)$, et en appliquant le critère jacobien de simplicité.

Remarque : On peut montrer en fait que, si dim $V \geq 2$, $L_u \cap V$ est une variété définie sur $k(u)$ (donc que $Z = L_u \cap V$).

Fin de la démonstration du th. 8. Soient V affine quelconque W quelconque, et $a \in V$, simple sur V. Introduisons L_u, Z et x vérifiant les conditions du lemme 4. Prenons y générique de W sur $k'(x)$. D'après l'hypothèse de récurrence appliquée à $\phi_o : Z \times W \to A$ induite par ϕ, il existe une application rationnelle $\alpha : W \to A$, définie sur $k(u)$, telle qu'on ait

$$\phi(x,y) - \phi(a,y) = \alpha(x) .$$

Le premier membre est un élément du corps $k(x,y)$, le second un élément de $k'(x)$. Or, d'après EA. I, 9, th. 5 bis, ces deux corps sont linéairement disjoints sur $k(x)$. Donc leur intersection est $k(x)$, et on a $\alpha(x) \in k(x)$, i.e. α est définie sur k. Le théorème 8 est donc démontré.

COROLLAIRE 1.- Soit $\phi : G \to A$ une application rationnelle d'une variété de groupe G dans une variété abélienne. Alors ϕ est le composé d'un homomorphisme $\phi_o : G \to A$ (de variétés de groupe) et d'une translation sur A, i.e. il existe $a \in A$ tel que $\phi(x) = \phi_o(x) + a$.

Démonstration. Comme G est sans point multiple, toute application rationnelle $G \to A$ est un morphisme, d'après le th.6. Notons e l'élément neutre de G, et posons $\phi_o(x) = \phi(x) - \phi(e)$. Appliquons le th. 8 au morphisme $\psi_o : G \times G \to A$ défini par $\psi_o(x,y) = \phi_o(x.y)$. Il existe des morphismes α et $\beta : G \to A$ tels qu'on ait

$$\phi_o(x.y) = \alpha(x) + \beta(y)$$

En faisant $y = e$, puis $x = e$, on obtient les relations

$$\phi_o(x) = \alpha(x) + \beta(e)$$

$$\phi_o(y) = \alpha(e) + \beta(y)$$

En faisant $x = y = e$, on obtient

$$0 = \alpha(e) + \beta(e)$$

On a donc

$$\phi_o(x.y) = \phi_o(x) + \phi_o(y)$$

i.e. ϕ_o est un homomorphisme.

COROLLAIRE 2.- Toute application rationnelle $f : \mathbb{S}_n \to A$ est constante.

.../...

Démonstration. Il suffit en effet de le montrer pour $n = 1$. Introduisons la droite projective $\mathbb{P}_1$, et l'application rationnelle $f^*: \mathbb{P}_1 \to A$ déduite de f. Comme $\mathfrak{S}_1$ et $\mathbb{P}_1$ sont sans point multiple de f et f^* sont des morphismes (le second prolongeant le premier). D'après le coroll. 1, appliqué à la loi additive sur $\mathfrak{S}_1$, on a

$$(3) \quad f(x+y) = f(x) + f(y) + a$$

où a est un point de A, et où x,y sont des points génériques indépendants de $\mathfrak{S}_1$ sur $k(a)$. On peut trouver une place ρ de Ω telle que $\rho(x) = x$ et $\rho(y) = \infty$. On a alors $\rho(x+y) = \infty$. En appliquant ρ aux deux membres de (3), on obtient

$$f^*(\infty) = f(x) + f^*(\infty) + a$$

d'où $f(x) = -a$, C.Q.F.D.

7. Théorème de réductibilité complète de Poincaré.

Si A est une variété abélienne, et si E, F sont deux sous-ensembles de A, on notera $E + F$ l'ensemble des points de A de la forme $a+b$, avec $a \in E$, et $b \in F$. Si E et F sont des sous-ensembles algébriques (i.e. fermés) de A, il en est de même de $E + F$ (car on a $E+F = \lambda(E \times F)$, et d'après le lemme 1 du n° 4). Pour tout entier n, on notera $n\delta$ l'homomorphisme $x \mapsto nx$ de A dans A. Dans ce n°, nous admettrons provisoirement le résultat suivant, qui sera démontré plus loin: pour $n \neq 0$, l'homomorphisme $n\delta$ est surjectif. Il revient au même de dire que $\ker(n\delta)$ est fini.

THEOREME 9.

Soient A une variété abélienne de dimension n, B une sous-variété abélienne de A de dimension q, k un corps de définition de A et B. Il existe une sous-variété abélienne

.../...

C de A , de dimension $r = n-q$, définie sur k , telle qu'on ait $B + C = A$. L'intersection $B \cap C$ est alors un sous-groupe fini de A .

Démonstration. Soit y un point générique de A sur k , et considérons la variété B_y déduite de B par la translation τ_y . Soit z un point générique de B_y sur $k(y)$. Alors z est aussi générique de A sur k (car y est spécialisation de z sur $k(u)$, donc aussi sur k). Posons $k_1 = k(y) \cap k(z)$. Le degré de transcendance de $k(z)/k_1$ est égal à celui de $k(y,z)/k(y)$, donc à $q = \dim B$. Celui de k_1/k est donc $r = n-q$ Comme l'extension $k(y,z)/k(y)$ est régulière, $k(y)$ est algébriquement fermé dans $k(y,z)$ (E, Chap. 0, C, 7, th. 19). Donc, si $w \in k(z)$ est algébrique sur k_1 , il appartient à $k(y) \cap k(z) = k_1$; autrement dit k_1 est algébriquement fermé dans $k(z)$. Comme $k(z)/k$ est séparable, il en est de même de $k(z)/k_1$. Donc $k(z)/k_1$ est régulière. La variété $\mathrm{loc}_{k_1} z$ est de dimension $q = \dim B = \dim B_y$, et elle contient $\mathrm{loc}_{k(y)} z = B_y$. Donc on a $\mathrm{loc}_{k_1} z = B_y$, i.e. B_y est définie sur k_1 . On peut trouver sur B_y un point t_1 rationnel sur une extension algébrique séparable de k_1 . Notons t_i $(1 \leq i \leq m)$ les conjugués distincts de t_1 sur k_1 . La somme $t = \sum_i t_i$ (au sens de la loi de groupe de A) est un point de A , invariant par tout k_1-automorphisme de la clôture algébrique $\bar{k}_1$, donc rationnel sur k_1 . Comme on a $k_1 \subset k(z)$, t est rationnel sur $k(z)$. Donc il existe une application rationnelle $\phi : A \to A$, définie sur k , telle que $t = \phi(z)$. D'après le coroll. 1 du th. 8, cette application est de la forme

$$(4) \quad \phi(x) = \phi_0(x) + a_0 ,$$

.../...

où $a_o \in A$, et où ϕ_o est un k-homomorphisme $A \to A$ (pour la structure de variété abélienne). D'après le th. 3 du n° 3, $\phi_o(A)$ est une sous-variété abélienne C de A . On a , pour tout i, $t_i \in B_y$, c'est-à-dire $t_i - y \in B$. On a donc aussi $\sum_i t_i - ny = t - ny = \phi(y) - ny \in B$. On a donc $\phi(a) - na \in B$ pour tout $a \in A$. En particulier, en prenant $a = 0$, on voit que $\phi(0) = a_o \in B$. Or nous avons admis (cf. plus haut) que l'endomorphisme $n\delta$ de A est surjectif. Donc, pour tout $u \in A$, il existe un point $v \in A$ tel que $nv = u$. On a $\phi(v) - nv = \phi_o(v) + a_o - u \in B$. Puisqu'on a $a_o \in B$, et $\phi_o(v) \in C$, on a $u \in B + C$. On a donc prouvé que $A = B + C$. On a de plus $\dim(B+C) = \dim \lambda(B \times C) \leq \dim B + \dim C$, d'où $\dim C \geq n-q = r$. Comme d'autre part le degré de transcendance de $k(t)/k$ est au plus égal à celui de k_1/k , i.e. à r , on a $\dim C \leq r$. On a donc $\dim C = r$. Puisque le morphisme $B \times C \to A$ induit par λ est surjectif, son noyau est de dimension 0 , d'après (c) du th. 3 du n° 3, donc fini. Or ce noyau se compose des points $(b, -b)$, avec $b \in B \cap C$. Donc $B \cap C$ est fini, C.Q.F.D.

8. Isogénies.

Soient V et W deux variétés, et soit $\phi : W \to V$ une application rationnelle. Soit k un corps de définition de V , W et ϕ . Soit y un point générique de W sur k , et posons $x = \phi(y)$. Si l'extension $k(y)/k(x)$ est algébrique est de degré fini, on dit que ϕ est de degré fini ; plus précisément, le degré $n = [k(y) : k(x)]$ est alors noté $\nu(\phi)$, et appelé degré de ϕ . Les degré séparable et inséparable de $k(y)/k(x)$ sont notés respectivement $\nu_s(\phi)$ et $\nu_i(\phi)$ et sont appelés respectivement degré séparable et degré inséparable de ϕ .

.../...

Remarquons que, pour que ϕ soit de degré fini, il faut et il suffit que l'image inverse $(\phi^{-1})_e(x)$ soit un ensemble fini : cette image n'est autre en effet que le lieu de y sur $k(x)$.

En particulier, soit $\phi : A \to B$ un homomorphisme de variétés abéliennes. Pour que ϕ soit de degré fini, il faut et il suffit que le noyau $\ker \phi$ soit fini (car $\phi^{-1}(x)$ est une classe de A suivant de noyau). On dit que ϕ est une <u>isogénie</u> si ϕ est <u>de degré fini</u> et <u>surjectif</u>. On dit aussi que A est <u>isogène à B</u>. On a alors <u>dim A = dim B</u>, d'après (c) du th. 3 du n° 3 .

(Remarque : deux quelconques des trois propriétés : "ϕ est de degré fini", " ϕ est surjectif" et " dim A = dim B " entraînent la troisième, et suffisent donc à caractériser une isogénie).

<u>THEOREME 10</u>.

La relation "A est isogène à B " est symétrique en A et B

<u>Démonstration</u>. Supposons qu'il existe une isogénie $\Phi : A \to B$. Il s'agit de prouver l'existence d'une isogénie $B \to A$.

(a) Supposons Φ <u>séparable</u>. Soient $k, ., y$ comme ci-dessus. Considérons le point $x' = \Sigma_i x_i$, somme des conjugués distincts de x sur $k(y)$. Ce point x' est invariant par tout $k(y)$-automorphisme de la clôture algébrique $\overline{k(y)}$. Comme d'autre part Φ est séparable, x' est séparable sur $k(y)$. Donc x' est rationnel sur $k(y)$. Donc il existe un morphisme $\psi : B \to A$, défini sur k , tel que $x' = \psi(y)$. Or on a, quel que soit i , $\Phi(x_i) = y$. On a donc $\Phi(x') = n\,y$, en posant $n = \nu(\Phi)$, d'où $\Phi \circ \psi = n\delta$. Or, d'après la propriété admise au début du n° 7, le morphisme $n\delta : A \to A$ est surjectif. Donc $\psi : B \to A$ est surjectif ; comme dim A = dim B , ψ est une isogénie.

(b) <u>Cas général</u> : compte tenu de (a), le cas général se ramène à celui

.../...

où Φ est un morphisme radiciel. Ce dernier cas sera traité plus loin (cours 66-67, lemme 2.1., p. 89).

La relation " A est isogène à B " étant d'autre part réflexive et transitive, c'est une relation d'équivalence. Il est immédiat qu'elle est compatible avec le produit $A \times B$. On dira qu'une variété abélienne A est <u>simple</u> si elle n'admet pas d'autre sous-variété abélienne que 0 et A elle-même. Toute variété isogène à A est alors également simple, i.e. la propriété " A est simple" ne dépend que de la classe de A pour la relation d'isogénie. Notons aussi que si A et B sont simples, tout homomorphisme $\phi : A \to B$ non nul est une isogénie (en effet le noyau de ϕ est nécessairement de dimension 0, et l'image de ϕ coïncide nécessairement avec B).

<u>THEOREME 11</u>.

Toute variété abélienne A est isogène à un produit de variétés abéliennes simples, et celles-ci sont uniques à des isogénies près.

(Autre énoncé équivalent : toute classe pour la relation d'isogénie s'exprime, d'une et d'une seule façon, sous forme d'un produit de classes simples).

<u>Démonstration</u>. Avec les notations du th. 9 , la variété abélienne A est isogène à $B \times C$. L'existence d'un produit de variétés abéliennes simples isogène à A s'en déduit aussitôt, par récurrence sur la dimension de A .

Quant à l'unicité, supposons qu'on ait une isogénie

$$\lambda : A_1 \times \ldots \times A_m \to B_1 \times \ldots \times B_n ,$$

où les A_i et les B_j sont simples. Nous allons montrer,

.../...

par récurrence sur $\inf(m,n)$, qu'on a nécessairement $m = n$, et qu'on peut ordonner les facteurs de façon que A_i soit isogène à B_i pour tout i.

Le résultat est en effet trivial pour $\inf(m,n) = 0$. Notons B_1' l'image par λ de $A_1 \times 0 \times \ldots \times 0$. Nécessairement λ induit une isogénie $A_1 \to B_1'$. Il existe un j tel que la projection de B_1' sur B_j ne soit pas réduite à C. On peut, par exemple, supposer $j = 1$. Notons π_1 la projection sur le premier facteur dans le produit $B_1 \times \ldots \times B_n$. Comme B_1 est simple, la relation $\pi_1(B_1') \neq 0$ entraîne $\pi_1(B_1') = B_1$, et π_1 induit une isogénie $B_1' \to B_1$.

Soit C_1 la composante de l'origine du noyau de $\lambda_1 = \pi_1 \circ \lambda$, et montrons que C_1 est isogène à $\overline{A}_1 = A_2 \times \ldots \times A_n$. En effet, soit k un corps de définition de toutes les variétés considérées, et soit $z = (z_1, z_2, \ldots, z_m)$ un point générique de C sur k_1. On a $\lambda_1(z) = \lambda_1(z_1, 0, \ldots, 0) + \lambda_1(0, z_2, \ldots, z_m) = 0$. D'après ce qui précède, λ_1 induit une isogénie sur $A_1 \times 0 \times \ldots \times 0$, d'image B_1. Donc z_1 est algébrique sur le corps $k(\lambda_1(z_1, 0, \ldots, 0)) \subset k(z_2, \ldots, z_m)$. Donc z est algébrique sur $k(z_2, \ldots, z_m)$, i.e. le morphisme $C_1 \to \overline{A}_1$ obtenu par projection, est une isogénie. De plus, λ induit une isogénie $C_1 \to C_1'$, où C_1' est contenue dans $\overline{B}_1 = B_2 \times \ldots \times B_n$. Or on a $\dim B_1 = \dim A_1$, donc $\dim \overline{B}_1 = \dim \overline{A}_1$, et, par suite, $\dim C_1' = \dim C_1 = \dim \overline{A}_1 = \dim \overline{B}_1$. On a donc $C_1' = \overline{B}_1$. Donc $\overline{A}_1$ est isogène à $\overline{B}_1$. Il suffit d'appliquer à cette isogénie l'hypothèse de récurrence,

C.Q.F.D.

CHAPITRE II

COURBES ALGEBRIQUES. THEOREME DE RIEMANN-ROCH

1. Conventions relatives aux diviseurs.

Si V est une variété sans point multiple, l'application canonique $D \mapsto \mathfrak{X}(D)$ du groupe des diviseurs sur V dans celui des cycles de codimension 1 sur V est un isomorphisme. (E et EA, Ch. IV, 5). Sur une telle variété, on conviendra d'indentifier canoniquement D et son image $X = \mathfrak{X}(D)$. En particulier, dans le cas où V est une courbe, tout diviseur $\underline{d}$ sur V s'écrira sous la forme $\underline{d} = \sum_i m_i a_i$, où les a_i sont des points de V.

Si f est une fonction sur V, la convention précédente conduit à identifier $\mathrm{div}(f)$ avec $\mathfrak{X}(f)$. Les diviseurs sur V de la forme $\mathrm{div}(f)$ forment un sous-groupe du groupe de tous les diviseurs $\mathfrak{D}(V)$, qu'on note $\mathfrak{D}_\ell(V)$. Deux diviseurs X et X' congrus mod $\mathfrak{D}_\ell(V)$ sont dit linéairement équivalents, ce qu'on écrit $X \sim X'$. En particulier, $\mathfrak{D}_\ell(V)$ est composé des diviseurs linéairement équivalents à zéro.

Si W est une sous-variété de codimension 1 de V, la valuation discrète du corps des fonctions $\mathfrak{F}(V)$ associée à W (et normée de façon que le groupe de ses valeurs soit $\mathbf{Z}$) sera notée v_W, et non ω_W, comme dans E, Ch. III, 10, p. 46, pour éviter une confusion fâcheuse avec les notations utilisées pour les différentielles. On notera parfois aussi v_W la restriction de cette valuation à un corps de la forme $\mathfrak{F}_k(V)$, où k est un corps de définition de V et W. Rappelons que, pour $f \in \mathfrak{F}(V)$, le coefficient de W dans $\mathrm{div}(f) = \mathfrak{X}(f)$ est $v_W(f)$. De même, si X est un diviseur sur V, le coefficient de W dans X

.../...

sera noté $v_W(X)$. Si f est une fonction $\neq 0$ sur V, et si f^* est l'application rationnelle correspondante $V \to \mathbb{P}_1$ de V dans la droite projective, le diviseur de f s'exprime sous la forme $\mathrm{div}(f)=(f^*)^{-1}(0)-(f^*)^{-1}(\infty)$, où l'on regarde 0 et ∞ comme des diviseurs sur $\mathbb{P}_1$.

Si X est un diviseur sur une variété V, et si W est une sous-variété de V non contenue dans le support de X, le diviseur <u>induit</u> par X sur W est défini ; par définition, ce diviseur est l'image inverse $i^{-1}(X)$ de X par l'immersion $i : W \to V$. On le désignera également par la notation $X.W$.

2. <u>Valuations associées aux points d'une courbe algébrique</u>.

Soit V une courbe, définie sur un corps k. Si a est un point de V, rationnel sur k, la valuation correspondante v_a du corps $\mathcal{F}_k(V)$ est associée à la place ρ_a de ce corps, à valeurs dans k, obtenue en posant $\rho_a(f) = f(a)$.

Supposons que V est complète, sans point multiple, et que k est <u>algébriquement clos</u> ; donnons-nous, inversement, une valuation v du corps $\mathcal{F}_k(V)$, triviale sur k. On peut trouver une place ρ de $\mathcal{F}_k(V)$, associée à v, et à valeurs dans k. Soit x un point générique de V sur k. Puisque V est complète, ρ est finie en x. Si on pose $\rho(x) = a$, la place ρ coïncide nécessairement avec ρ_a, donc la valuation v avec v_a. On a ainsi mis en évidence une <u>correspondance bijective</u> entre <u>les points de V rationnels sur k et les valuations (ou les places) de $\mathcal{F}_k(V)$ triviales sur k</u>. On a de même une correspondance bijective entre l'ensemble de tous les points de V et celui des valuations (ou des places) de $\mathcal{F}(V)$ triviales sur les constantes.

3. <u>Différentielles sur une courbe</u>.

Soit V une courbe définie sur un corps k. Les différentielles sur V, définies sur k, forment un espace vectoriel

.../...

de dimension 1 sur le corps $\mathcal{F}_k(V)$. Conformément aux notations de E, Chap III, 3, cet espace est noté $D_k(V)$. Si t est une fonction $\in \mathcal{F}_k(V)$, non constante, cet espace est engendré par la différentielle dt ; en d'autres termes, toute différentielle $\omega \in D_k(V)$ s'écrit de façon unique sous la forme $\omega = g\,dt$, avec $g \in \mathcal{F}_k(V)$.

On a (d'après E, Chap III, 3, th. 4), un isomorphisme canonique $\mu : D_k(V) \longrightarrow Z_k(\Delta_V, V \times V)$. Rappelons que μ est caractérisé par la propriété que si $\omega = df$, son image est représentée par l'élément $f(x) - f(y)$ de l'idéal $\underline{m}_k(\Delta_V, V \times V)$.

Rappelons d'autre part que si a est un point de V, on a un monomorphisme canonique $\alpha : Z_k(a,V) \longrightarrow D_k(V)_a$ de l'espace tangent de Zariski de V en a dans l'espace des différentielles au point a. Cet homomorphisme α est ici surjectif, i.e. est un <u>isomorphisme</u>. En effet, d'après E, Chap III, 7, le conoyau de α est l'espace $D_k(a)$ des différentielles sur la variété réduite au point a, donc est réduit à 0. On identifiera canoniquement au moyen de α les deux espaces $Z_k(a,V)$ et $D_k(V)_a$. Si, dans ces conditions, ω est une différentielle sur V, définie sur k, morphique en a, représentée par $f \in \underline{m}_k(\Delta_V, V \times V)$, morphique en (a,a), sa valeur ω_a n'est autre que l'élément de $Z(a,V)$ représenté par la fonction $f_a(x) = f(a,x)$.

<u>LEMME 1</u>. Soient V une courbe, a un point simple de V, et t un paramètre uniformisant de V en a. Alors la diagonale $\Delta = \Delta_V$ est représentée au point (a,a) par la fonction u sur le produit $V \times V$ définie par $u(x,y) = t(x) - t(y)$.

.../...

Démonstration. Soit en effet f une fonction sur $V \times V$ représentant Δ au point (a,a). La fonction u est morphique en (a,a), donc aussi sur Δ, et de plus s'annule sur Δ. D'après le critère de morphicité, on a donc $u = f g$, où g est une fonction sur $V \times V$ morphique en (a,a). Il suffit de prouver que g ne s'annule pas en (a,a). Or, si g s'annulait en (a,a), on aurait $u \in \underline{m}^2$, en posant $\underline{m} = \underline{m}(a \times a, V \times V)$. Mais comme $t(x)$ et $t(y)$ forment un système de générateurs de $\underline{m}$, on en déduirait, en passant à la fonction induite sur $a \times V$, la relation $t \in \underline{m}(a,V)^2$, ce qui est absurde.

THEOREME 1.

Soient V une courbe, a un point simple de V, ω une différentielle sur V, morphique en a, représentée par $f \in \underline{m}(\Delta_V, V \times V)$ sur le produit $V \times V$. Soit d'autre part t un paramètre uniformisant de V en a, et posons $\omega = g\,dt$. Alors les trois propriétés suivantes sont équivalentes

(a)- $\omega_a \neq 0$

(b)- f représente Δ_V en (a,a) sur le produit $V \times V$

(c)- g est inversible en a.

Démonstration.

(a) $\Longleftrightarrow$ (c), d'après la relation $\omega_a = g(a)(dt)_a$.

D'autre part, on a

(1) $f(x,y) \equiv g(x)\,(t(x) - t(y)) \pmod{\underline{m}^2}$, en posant $\underline{m} = \underline{m}(\Delta_V, V \times V)$. D'après le lemme 1, Δ_V est représentée en (a,a) par $t(x) - t(y) = u(x,y)$. En particulier, u est un générateur de $\underline{m}$. Puisque f s'annule sur Δ, la fonction f/u est toujours morphique en (a,a). La condition (b) signifie donc que f/u est inversible en (a,a). Compte tenu

.../...

de (1), il revient au même de dire que g est inversible en a. On a donc montré que (b) $\Leftrightarrow$ (c). C. Q. F. D.

Lorsque les conditions équivalentes (a), (b), (c) du Th. 1 sont vérifiées, on dit que la différentielle ω est inversible en a.

THEOREME 2.

L'ensemble U (resp. U^*) des points de V en lesquels ω est morphique (resp. inversible) est un ouvert non vide de V

Démonstration. En effet, si ω est représentée par $f \in \underline{m}(\Delta_V, V \times V)$, l'ensemble U (resp. U^*) est la projection sur V de l'intersection de Δ_V avec l'ouvert complémentaire du support de $\mathrm{div}(f)^-$ (resp. de $\mathrm{div}(f) - \Delta$).

4. Diviseur d'une différentielle sur une courbe.

Supposons donnée une différentielle ω sur une courbe V. Soit a un point de V, simple sur V, et associons-lui une différentielle ω_o sur V, inversible en a (on peut, par exemple, prendre $\omega_o = dt$, où t est un paramètre uniformisant de V en a). D'après le Th. 2, il existe un ouvert U de V, contenant a, tel que ω_o soit inversible en tout point de U. Posons alors $\omega = f\,\omega_o$, avec $f \in \mathcal{F}(V)$. Pour tout autre point $a' \in V$, et pour ω'_o, U', f' construits de façon analogue, la fonction f/f' est inversible en tout point de $U \cap U'$, d'après le th. 1. Autrement dit, les couples (U,f) et (U', f') sont équivalents au sens de E, chap. III, n° 11. Si V est sans point multiple, la collection de tous les couples (U,f) définit donc un diviseur sur V. Ce diviseur est appelé le diviseur de la différentielle ω, et noté $\mathrm{div}(\omega)$. Si $\omega \in D_k(V)$, il est clair que $\mathrm{div}(\omega)$ est rationnel sur k.

.../...

D'après cette définition, on a, pour toute fonction f sur V, la relation $\mathrm{div}(f\,\omega) = \mathrm{div}(f) + \mathrm{div}(\omega)$. Pour $a \in V$, le coefficient de a dans $\mathrm{div}(\omega)$ sera noté $v_a(\omega)$.

THEOREME 2bis.

Les ouverts U et U^* intervenant dans le th. 2 sont respectivement les complémentaires des supports de $\mathrm{div}(\omega)^-$ et $\mathrm{div}(\omega)$.

Démonstration. Il suffit de se reporter à la démonstration du th. 2, en tenant compte du th. 1, et de la définition ci-dessus de $\mathrm{div}(\omega)$.

THEOREME 3.

Soit V une courbe sans point multiple, et posons $\Delta = \Delta_V$. Soit ω une différentielle sur V, représentée par $f \in \underline{m}(\Delta, V\times V)$. Alors on a

(2) $\mathrm{div}(\omega) = \mathrm{pr}_V((\mathrm{div}(f) - \Delta) \,.\, \Delta)$.

Démonstration. En effet, soit $a \in V$, et associons-lui une différentielle ω_o sur V, inversible en a. Soit g la fonction sur V telle que $\omega = g\,\omega_o$, et soit f_o la fonction sur $V \times V$ définie par $f(x,y) = f_o(x,y)\,g(x)$. Alors ω_o est représentée par f_o sur le produit $V \times V$. D'après le th. 1, on a donc $(a,a) \notin \mathrm{supp}(\mathrm{div}(f_o) - \Delta)$. Donc le diviseur $\mathrm{div}(f) - \Delta$ est représenté par $g(x)$ en (a,a) sur $V \times V$. Donc la projection $\mathrm{pr}_V((\mathrm{div}(f)) - \Delta).\,\Delta)$ est représentée par g en a. Or $\mathrm{div}(\omega)$ est aussi, par définition, représenté par g en a,

Les deux membres de (2) induisent donc, quel que soit a, le même diviseur sur un voisinage de a. Donc ils coïncident.

.../...

5. Complétion de l'anneau local d'un point.

Soient K un corps, v une valuation de K, à valeurs réelles (i.e. telle que le groupe Γ de ses valeurs soit un sous-groupe ordonné du groupe additif ordonné des nombres réels), et soit R l'anneau de valuation associé. Il correspond à v une valeur absolue de K, définie par $|x|_v = \exp(-v(x))$. L'anneau $\hat{R}$ (resp. le corps $\hat{K}$) complète de R (resp. K) relativement à cette valeur absolue est dit complèté de R (resp. K) relativement à v.

En particulier, soit V une courbe définie sur un corps k, et soit a un point simple sur V, rationnel sur k. Soit $v = v_a$ la valuation correspondante du corps de fonctions $K = \mathfrak{F}_k(V)$; soient $\underline{o} = \underline{o}(a,V)$ l'anneau de valuation associé, $\underline{m}$ son idéal maximal, t un paramètre uniformisant de V en a (i.e. un générateur de $\underline{m}$). Considérons les complètés $\hat{\underline{o}}$ et $\hat{K}$ de $\underline{o}$ et K respectivement relativement à v. Alors, tout élément de $\hat{\underline{o}}$ s'écrit, d'une façon et d'une seule, sous la forme

$$x = \sum_{n=0}^{\infty} a_n t^n$$

où les a_i appartiennent à k. En effet, on remarque que tout élément $f \in \underline{o}$ est congru (mod $\underline{m}$) à un et un seul élément de k, à savoir $f(a)$. On peut donc par récurrence sur n, construire une suite $a_0, a_1, \ldots a_n, \ldots$ d'éléments de k telle qu'on ait $x = \sum_{i=1}^{n-1} a_i t^i \pmod{t^n}$ pour tout n. Il suffit de remarquer que $x - \sum_{i=1}^{n-1} a_i t^i$ est un élément de $\underline{o}\, t^n$, donc est congru (mod t^{n+1}) à un élément de la forme $a_n t^n$, avec $a_n \in k$. (Cette construction a déjà été utilisée pour démontrer le th. 1 de E, chap. IV, n°1).

.../...

Autrement dit, l'anneau $\hat{o}$ est isomorphe à l'anneau des séries formelles à coefficients dans k et on peut écrire $\hat{o} = k[[t]]$, en faisant l'identification canonique correspondante. De même, le corps $\hat{K}$ s'identifie à l'anneau de séries formelles $k((t))$, de sorte que l'un quelconque de ses éléments s'écrit sous la forme

$$x = \sum_{n=n_o}^{\infty} a_n t^n$$

avec $n_o \in Z$.

Remarque. On peut montrer que la même propriété est valable pour tout anneau de valuation discrète ayant même caractéristique que son corps résiduel.

Rappelons que, si $k[[t]]$ est l'anneau de séries formelles sur k, et si u est un générateur de son idéal maximal, i.e. un élément de la forme $u = c_1 t + c_2 t^2 + \ldots$, avec $c_1 \neq 0$, il existe un et un seul k-automorphisme de $k((t))$, pour la structure de corps complet, appliquant t sur u. On dit que u est une uniformisante de $k((t))$. En particulier, tout paramètre uniformisant de V en a est une uniformisante du corps complèté correspondant $\hat{K}$.

6. Complément : extension algébrique d'un corps valué.

LEMME 2. Soit K un corps complet relativement à une valuation v, à valeurs réelles. Soit L une extension algébrique de degré fini n de K. Il existe une et une seule valuation w de L prolongeant v. Cette valuation est donnée par la formule

$$(3) \quad w(y) = \frac{1}{n} v(N\, y)$$

où N est la norme relative à l'extension L/K. De plus, L est

.../...

complet relativement à w .

Démonstration. L'existence de w résulte du théorème de prolongement (E, chap. 0, A, 8, th. 7, coroll.)

Pour prouver l'unicité, introduisons une base (a_i) $(1 \leq i \leq n)$ de l'extension L/K. Pour $y \in L$, exprimé sous la forme $y = \sum_i x_i a_i$ $(x_i \in K)$, on a $Ny = P(x_1, \ldots, x_n)$, où P est un polynôme homogène de degré n à coefficients dans K .

Montrons que, pour $y \in L$, tel que $v(Ny) = 0$, on a nécessairement $w(y) = 0$. Supposons en effet qu'on ait, par exemple, $w(y) < 0$. Alors, lorsque l'entier m tend vers l'infini, y^m tend vers zéro pour la valeur absolue $| \ |_w$. Or $| \ |_w$ définit sur L une structure d'espace vectoriel normé compatible avec la valeur absolue $| \ |_v$ de K . D'après les propriétés des espaces normés, cette norme équivaut à celle définie par $\|y\| = \sup_i |x_i|_v$. Si, pour tout m , on pose $y^m = \sum_i x_{m_i} a_i$, chacun des x_{m_i} (pour i fixé) tend vers zéro quand $m \to \infty$. Donc $(Ny)^m = P(x_{m_1}, \ldots, x_{m_n})$ tend aussi vers zéro. Ceci implique $|Ny|_v < 1$, i.e. $v(Ny) > 0$, contrairement à l'hypothèse.

On a donc prouvé que $v(Ny) = 0$ implique $v(y) = 0$. Or on a $N(y^n/Ny) = 1$. On a donc $w(y^n/Ny) = 0$, d'où résulte la formule (3). Le raisonnement précédent montre en outre que L est complet relativement à w , C. Q. F. D.

Remarque 1. Le lemme précédent est valable en fait pour toute valeur absolue de K , archimédienne ou non ; la démonstration ci-dessus de l'existence de w reste alors valable en effet sans modification ; quant à l'unicité de w , elle résulte, dans le cas archimédien, du théorème d'Ostrowski.

Si K est un corps muni d'une valeur absolue v , si L

.../...

est une extension de K, munie d'une valeur absolue w prolongeant v, et si l'on note Γ et Δ les groupes de valeurs respectifs de v et w, l'indice $e = [\Delta : \Gamma]$ (éventuellement infini) est appelé ordre de ramification de l'extension L/K relativement à w (ou relativement à v, lorsque le prolongement est unique). Dans le cas du lemme 2, on a $n\Delta \subset \Gamma \subset \Delta$.

Si v est discrète, i.e. si Γ est cyclique, Δ est également cyclique, i.e. w est discrète, et l'indice de ramification e est un entier fini divisant n. Plus précisément, on démontre alors la formule $n = e f$, où f est le degré résiduel de l'extension L/K, i.e. le degré de l'extension L'/K', où K' et L' sont les corps résiduels respectifs de v et w. Dans le cas plus particulier qui nous intéresse, les corps K et L sont respectivement isomorphes à des corps de séries formelles $k((t))$ et $k((u))$, de sorte qu'on a $K' = L' = k$, d'où $f = 1$. Bornons-nous à vérifier que la formule a bien lieu dans ce cas, i.e. qu'on a alors $n = e$. En effet, Γ et Δ sont cycliques, et respectivement engendrés par $v(t)$ et $w(u)$. On a donc $v(t) = e\, w(u)$, de sorte que t/u^e est un élément inversible de $k[[u]]$. On en déduit que tout élément de $k[[u]]$ (resp. de $k((u))$) est de la forme $x_0 + x_1 u + \ldots + x_{e-1} u^{e-1}$, où les x_i appartiennent à $k[[t]]$ (resp. $k((t))$). En outre, la relation $x_0 + x_1 u + \ldots + x_{e-1} u^{e-1} = 0$ n'est possible que si les x_i sont tous nuls (sinon l'un des termes du premier membre aurait une valuation strictement plus petite que celles de tous les autres). Donc $1, u, \ldots, u^{e-1}$ forment une base de l'extension $k((u))/k((t))$,

.../...

et on a bien $n = e$.

Remarque 2. Si on norme w de façon que son groupe de valeurs Δ soit $\mathbb{Z}$, on a $\Gamma = e\,\mathbb{Z}$ (et non $\Gamma = \mathbb{Z}$). Si v' est la valuation de K équivalente à v , et admettant $\mathbb{Z}$ comme groupe de valeurs, on a, d'après le lemme 2,

$$w(y) = v'(N(x))$$

d'où,en particulier, pour $x \in K$

$$w(y) = e\, v'(k).$$

Considérons maintenant un corps K muni d'une valuation à valeurs réelles (ou, plus généralement d'une valeur absolue) v , non nécessairement complet. Soit L une extension algébrique de degré fini séparable de K , et soit w une valeur absolue de L prolongeant v . Soient $\hat{K}$ et $\hat{L}$ les complétés respectifs de K et L relativement à v et w . Le corps $\hat{K}$ est canoniquement isomorphe à un sous-corps de $\hat{L}$. L'extension L/K étant supposée séparable, on a $L = K(z)$, avec $z \in L$. D'après le lemme 2, le corps $\hat{K}(z)$ est complet pour la valeur absolue induite par w . Comme ce corps contient $L = K(z)$, il coïncide avec $\hat{L}$. Par suite $\hat{L}/\hat{K}$ est une extension algébrique de degré fini. Son degré $[\hat{L} : \hat{K}]$ est appelé degré local de l'extension L/K relativement à w .

LEMME 3. Soit K un corps, muni d'une valeur absolue v , et soit L une extension algébrique séparable de K de degré fini n . Il existe un nombre fini de valeurs absolues w_i de L prolongeant v , et on a $n = \sum_i n_i$, où n_i est le degré local de l'extension L/K relativement à w_i .

Démonstration. L'extension étant séparable, on a $L = K(z)$, avec $z \in L$. Soit P le polynôme irréductible de z sur K .

.../...

Notons encore $\hat{K}$ le complété de K relativement à v, et introduisons une clôture algébrique $\hat{K}^*$ de $\hat{K}$. Sur le corps $\hat{K}$, le polynôme P se décompose en facteurs irréductibles sous la forme $P = P_1 \dots P_r$. Montrons d'abord qu'à tout facteur P_i $(1 \leq i \leq r)$, il correspond une valuation w_i de L prolongeant v. En effet, soit z_i une racine de P_i, et posons $\hat{L}_i' = \hat{K}(z_i)$. D'après le lemme 2, il existe une et une seule valeur absolue w_i' de $\hat{L}_i'$ prolongeant v. De plus, $\hat{L}_i'$ est complet, et, plus précisément, est le complété de $K(z_i)$, pour cette valeur absolue. Puisque $P(z_i) = 0$, il existe un K-isomorphisme $\alpha_i : K(z_i) \longrightarrow L$, tel que $\alpha_i(z_i) = z$. En transportant w_i' par α_i, on obtient une valeur absolue w_i de L prolongeant v ; de plus, α_i se prolonge à un isomorphisme (pour la structure de corps complet) de $\hat{L}_i'$ sur le complété correspondant $\hat{L}_i$ de L. Le degré local n_i correspondant $[\hat{L}_i : \hat{K}] = [\hat{L}_i' : \hat{K}]$ est égal à $\deg P_i$.

Inversement, soit w une valeur absolue quelconque de L prolongeant v, et soit $\hat{L}$ le complété de L relativement à w. Comme on a vu, $\hat{K}$ est isomorphe à un sous-corps de $\hat{L}$, et on a $\hat{L} = \hat{K}(z)$. Il existe donc un $\hat{K}$-isomorphisme σ de $\hat{L}$ sur un sous-corps $\hat{L}'$ de $\hat{K}^*$. L'image $\sigma(z)$ est nécessairement une racine z_i de P, donc de l'un des facteurs P_i. De plus P_i est uniquement déterminé, car $\hat{L}'$ est unique à un $\hat{K}$-isomorphisme près. On a nécessairement $\hat{L}' = \hat{K}(z_i) = \hat{L}_i'$; par suite, la valeur absolue w' de $\hat{L}'$ transportée de w par σ coïncide nécessairement avec w_i', donc aussi w avec w_i.

On a donc montré que les valeurs absolues de L prolongeant v ne sont autres que les w_i. On a de plus $\deg P = \sum_i \deg P_i$;

.../...

ce qui donne bien $n = \sum_i n_i$.

7. Revêtements.

Soient V et W deux variétés complètes sans point multiple, et soit $\phi : W \to V$ un morphisme. Lorsque ϕ est de degré fini, génériquement surjectif (ce qui implique dim V = = dim W), et tel que l'ensemble $(\phi^{-1})_e(a)$ soit fini pour tout $a \in V$, on dit que ϕ est un revêtement de V . En particulier si A et B sont des variétés abéliennes, toute isogénie $B \to A$ est un revêtement de A . Autre exemple : tout modèle normal canonique d'une variété V au sens de E, IV, 4 est un revêtement de V .

THEOREME 4.

Soient V et W deux courbes complètes sans point multiple. Toute application rationnelle non constante $\phi : W \to V$ est un revêtement de V .

Démonstration. En effet, pour $a \in V$, l'ensemble $(\phi^{-1})_e(a)$ est distinct de W (car sinon on aurait $W \times a = \Gamma_\phi$, et ϕ serait constante, de valeur a). Donc l'ensemble $(\phi^{-1})_e(a)$ est fini. D'autre part, pour $b \in W$, l'ensemble $\phi_e(b)$ des valeurs de ϕ en b est distinct de V (car Γ_ϕ est distinct de $b \times V$), donc est fini. Comme b est simple sur W , ϕ est morphique en b , en vertu de E , chap. IV, 2, th. 3 . Donc ϕ est un morphisme. Donc ϕ est bien un revêtement de V , car Φ est génériquement surjective, puisque non constante.

Conservons les notations du th. 4 ; introduisons un corps k de définition de V, W, ϕ , un point générique y de W sur k, et son image $x = \phi(y)$, générique de V sur k . Posons $K = \mathcal{F}_k(V) = k(x)$, et $L = \mathcal{F}_k(W) = k(y)$. Soit $a \in V$, et considérons la valuation discrète $v = v_a$ de K , normée de façon que l'ensemble de ses valeurs soit Z . Soit w une valuation

.../...

de L prolongeant v . La place $\rho = \rho_a$ de K , associée à $v = v_a$, peut être prolongée à une place λ de L , associée à w, à valeurs dans Ω . Comme w est complète, λ est de la forme ρ_b, où b est un point de W, donc équivalente à v_b . De plus, on a nécessairement $a = \phi(b)$, i.e. b est l'un des composants de l'ensemble $(\phi^{-1})_e(a)$. Soient $\hat{K}$ et $\hat{L}$ sont les complétés respectifs de K et L relativement à v et w . Le degré local $[\hat{L} : \hat{K}]$ est encore égal à l'ordre de ramification de $\hat{L}/\hat{K}$ (cf. n° précédent), i.e. à celui de L/K. On l'appelle ordre de ramification de ϕ en b .

D'après le lemme 3, si on note b_i les composants de l'ensemble $(\phi^{-1})_e(a)$, le degré n de ϕ est égal à $\sum_i e_i$, où e_i est l'ordre de ramification de ϕ en b_i .

THEOREME 5.

Soient V et W deux courbes complètes sans point multiples, et soit $\phi : W \to V$ un revêtement de degré n . Pour tout point a de V , le degré du diviseur $\phi^{-1}(a)$ est égal à n .

Démonstration. En effet, le diviseur $\phi^{-1}(a)$ est par définition, représenté en l'un quelconque des points b_i par la fonction $t \circ \phi$ sur W , où t est un paramètre uniformisant de V en a . Or on a $v_a(t) = v_a(t(x)) = 1$. Pour tout i , le coefficient de b_i dans le diviseur $\phi^{-1}(a)$ est égal à $v_{b_i}(t)$, donc à l'ordre de ramification e_i de ϕ en b_i . Le degré du diviseur $\phi^{-1}(a)$ est donc $\sum e_i = n$ (dans le cas séparable, cf.6, lemme 3;dans le cas général, cf. cours 1966-67, ch.I, th.7.2.).

COROLLAIRE. Si V est une courbe complète sans point multiple, et si f est une fonction sur V , le degré du diviseur div(f) est nul.

.../...

En effet, considérons le morphisme $f^* : V \to \mathbb{P}_1$ déduit de f. Ce morphisme est un revêtement de $\mathbb{P}_1$, et on a $\mathrm{div}(f) = \varphi^{-1}(\underline{c})$, où $\underline{c}$ est le diviseur $0 - \infty$ de $\mathbb{P}_1$. D'après le th. 5, on a $\deg(\varphi^{-1}(0)) = \deg(\varphi^{-1}(\infty)) = n$, en posant $n = \deg(f^*)$. On a donc bien $\deg(\mathrm{div}(f)) = 0$.

8. Résidu d'une différentielle.

Il est commode d'introduire une variante de la notion de k-différentielle d'un corps K, particulière au cas où $K = \hat{K}$ est complet relativement à une valuation v triviale sur k. Cette notion se définit comme dans E, Chap. III, n°1, mais en remplaçant le K-espace vectoriel D par un $\hat{K}$-espace vectoriel topologique D', et en exigeant que l'application d soit continue. Cet espace $D' = D'_k(\hat{K})$ est unique à un isomorphisme près, pour la structure d'espace vectoriel topologique sur $\hat{K}$.

En particulier, prenons pour $\hat{K}$ le corps de séries formelles $k((t))$, muni de la valuation discrète canonique v, associée à l'anneau $\underline{\hat{o}} = k[[t]]$. Un élément $f \in k((t))$ peut s'écrire sous la forme

$$f = \sum_{n \geq n_o} a_n t^n .$$

La définition précédente entraîne

$$df = \left(\sum_{n \geq n_o} n\, a_n\, t^{n-1}\right) dt .$$

Dans ce cas, l'espace $D'_k(\hat{K})$ est donc de dimension 1 sur $\hat{K}$, et engendré par dt. Une différentielle $\omega \in D'_k(\hat{K})$ s'exprime sous la forme $g\,dt$, avec $g \in \hat{K}$, i.e. sous la forme

$$\omega = (a_{-q} t^{-q} + \ldots + a_{-1} t^{-1} + f_o)\, dt ,$$

avec $f_o \in \underline{\hat{o}}$. Le coefficient $c = a_{-1}$ est appelé le

.../...

résidu de ω relatif à t (terminologie proviscire), et noté $\mathrm{Res}_t\omega$. Ce symbole possède les propriétés évidentes suivantes :

(a) - $\mathrm{Res}_t\omega$ dépend k-linéairement de ω

(b) - Res_t s'annule sur $\hat{o}\,dt$, i.e. $f_o \in \hat{o} \Longrightarrow \mathrm{Res}_t f_o dt = 0$.

(c) - $f \in \hat{K} \Longrightarrow \mathrm{Res}_t(df) = 0$.

THEOREME 6.

$\mathrm{Res}_t\omega$ ne dépend pas du choix de l'uniformisante t .

Démonstration. En effet, soit u une autre unifermisante de $\hat{K}$. On a $u = gt$, où g est un élément inversible de $\hat{o}$. On a donc $u^{-1}du = g^{-1}\,dg + t^{-1}\,dt$.

Or on a $g^{-1}\,dg \in \hat{o}\,dt$. On a donc $\mathrm{Res}_t\, u^{-1}\,du = \mathrm{Res}_t t^{-1}dt = 1$. Puisque Res_t et Res_u s'annulent sur $\hat{o}\,dt = \hat{o}\,du$, il suffit de vérifier qu'on a

$$\mathrm{Res}_u\, t^{-m}\,dt = 0$$

pour tout $m \geq 2$. Ce résultat est immédiat en caractéristique 0 , d'après (c), car, dans ce cas, $t^{-m}dt$ est la différentielle de $(1/1-m)t^{1-m}$. Pour passer au cas où la caractéristique p est quelconque, exprimons t sous la forme

$$t = u + b_2u^2 + \ldots + b_nu^n + \ldots$$

De cette relation, on tire, pour tout m ,

$$t^{-m}dt = u^{-m}du(1+c_2u^2 + \ldots + c_nu^n + \ldots)$$

où les c_j s'expriment en fonction des b_i par des polynômes P_{m-1} universels, à coefficients dans Z . Or on a $\mathrm{Res}_u\, t^{-m}dt = c_{m-1}$. D'après ce qui précède, P_{m-1} s'annule en $(b_1, b_2, \ldots)$ lorsqu'on prend pour b_i des éléments arbitraires d'un corps quelconque de caractéristique 0 . Donc P_{m-1} est identiquement nul, et on a dans tous les cas $c_{m-1} = 0$. C.Q.F.D.

.../...

Tenant compte de ce théorème, on supprimera l'indice t dans la notation du résidu, i.e. on écrira $\mathrm{Res}\ \omega$ (ou $\mathrm{Res}_w\ \omega$) au lieu de $\mathrm{Res}_t \omega$.

Soient à nouveau V une courbe, a un point simple de V, k un corps de définition de V et de a, et t un paramètre uniformisant de V en a. Soit $v = v_a$ la valuation correspondante, et posons $\underline{o} = \underline{o}_k(a,V)$, $K = \mathcal{F}_k(V)$. Conformément aux conventions du n° 5, identifions K à son image canonique dans son complété $\hat{K}$, lui-même identifié au corps $k((t))$. L'espace $D_k(V) = D_k(K)$ des k-différentielles sur V se plonge canoniquement dans l'espace $D'_k(\hat{K})$, (et on a $D'_k(\hat{K}) = D_k(K) \otimes_k \hat{K}$. Convenons d'identifier canoniquement $D_k(V)$ avec son image dans $D'_k(\hat{K})$. Pour $f \in K$, la différentielle df a alors la même signification lorsqu'on regarde f comme élément de K, et lorsqu'on le regarde comme élément de $\hat{K}$.

Si ω est un élément de $D_k(V)$, le résidu $\mathrm{Res}_v \omega$ ne dépend que de ω et de a, mais non du choix du corps k. Pour cette raison, on l'appelle <u>résidu de ω en a</u>, et on le représente également par la notation $\mathrm{Res}_a \omega$. Lorsque ω est morphique en a, on a $\mathrm{Res}_a\ \omega = 0$. On voit sans peine que $\mathrm{Res}_a\ \omega$ est invariant par toute transformation birationnelle qui est bimorphique au point a.

9. <u>Formule des résidus</u>.

Soit V une courbe complète sans point multiple, et soit $\omega \in D(V)$. Pour tout point a de V n'appartenant pas au support de $\mathrm{div}(\omega)^-$, ω est morphique en a, et on a donc $\mathrm{res}_a \omega = 0$. Comme les composants de $\mathrm{div}(\omega)^-$ sont en nombre fini, la somme $\sum_a \mathrm{res}_a\ \omega$, étendue à tous les points de V, est définie.

.../...

THEOREME 7.

On a la formule dite formule des résidus)

$$\sum_a \mathrm{Res}_a \omega = 0 .$$

Bornons-nous, pour l'instant, à démontrer ce théorème dans le cas particulier où V est la droite projective $\mathbb{P}_1$. Soit k un corps de définition algébriquemant clos des composants de div(ω). Le corps $K = \mathcal{F}_k(V)$ est isomorphe à k(X), où X est une indéterminée, et ω est de la forme f dX, avec $f \in K$. Décomposons f en éléments simples sous la forme

$$f = \sum_{i,\mu} \frac{A_{i\mu}}{(X-a_i)^\mu} + f_o$$

où les a_i sont les pôles de f, les $A_{i\mu}$ des éléments de k, et f_o un polynôme.

En tout point à distance finie a distinct des pôles a_i, on a $\mathrm{Res}_a \omega = 0$. D'autre part, on a $\mathrm{Res}_{a_i} \omega = A_{i1}$.

Pour évaluer $\mathrm{Res}_\infty \omega$, posons $X = \frac{1}{u}$; cela donne

$$f(X) = g(u) = \sum_{i,\mu} \frac{A_{i\mu} u^\mu}{(1-a_i u)^\mu} + f_o(u^{-1})$$

d'où

$$\omega = -g(u)\frac{du}{u^2} = -\left(\sum_{i,\mu} \frac{A_{i\mu} u^{\mu-2}}{(1-a_i u)^\mu} + \frac{1}{u^2} f_o(u^{-1})\right)du$$

On en déduit $\mathrm{Res}_\infty \omega = -\sum_i A_{i1}$, d'où la formule des résidus, dans le cas particulier considéré.

Pour passer au cas général, on va utiliser une propriété de la trace d'une différentielle.

10. Trace d'une différentielle.

Soient K un corps, L une extension algébrique de degré fini. La trace d'un élément $y \in L$ relativement à

.../...

l'extension L/K est notée $\mathrm{Tr}\, y$, ou $\mathrm{Tr}_{L/K} y$. Si v est une valeur absolue de K, et si L est une valeur absolue de L prolongeant K on appelle <u>trace locale de y relativement à w</u>, et on note $\mathrm{Tr}_{w/v} y$, la trace de y relativement à l'extension $\hat{L}/\hat{K}$, où $\hat{K}$ et $\hat{L}$ sont les complétés correspondants.

<u>LEMME 4</u>. Soient K un corps muni d'une valeur absolue v, et L une extension algébrique séparable de degré fini de K. Alors, pour $y \in L$, on a

$$\mathrm{Tr}\, y = \sum_i \mathrm{Tr}_{w_i/v} y$$

où la somme est étendue à toutes les valeurs absolues w_i de L prolongeant v. (cf. Lemme 3).

<u>Démonstration</u>. Comme dans le lemme 3, introduisons un élément $z \in L$ primitif sur K, i.e. tel que $L = K(z)$, puis le polynôme P irréductible de z sur K, et sa décomposition $P = P_1 \ldots P_r$ en facteurs irréductibles sur $\hat{K}$. Alors $\mathrm{Tr}\, z$ est la somme des racines de P, tandis que $\mathrm{Tr}_{w_i} z$ est la somme des racines de P_i. On a donc $\mathrm{Tr}\, z = \sum_i \mathrm{Tr}_{w_i/v} z$, i.e. la formule de l'énoncé est satisfaite par z. On peut supposer K infini (sinon K et L n'admettraient que la valeur absolue triviale). Comme il n'existe qu'un nombre fini de corps intermédiaires entre K et L, il existe α et $\alpha' \in K$, distincts, tels qu'on ait $K(y + \alpha z) = K(y + \alpha' z)$. Désignons ce dernier corps par L'. On a $y + \alpha z \in L'$ et $y + \beta z \in L'$, d'où $(\alpha - \beta) z \in L'$, d'où $z \in L'$, d'où $L' = L$. Donc $z' = y + \alpha z$ est un élément primitif de L sur K. La formule de l'énoncé est satisfaite par z et z', donc aussi par y C. Q. F. D.

Soit $\phi : W \to V$ un revêtement défini sur k et posons

.../...

à nouveau $L = \mathfrak{K}_k(W)$, $K = F_k(V)$. La trace d'une fonction $f \in L$ relativement à l'extension L/K est encore appelée trace de f relativement à ϕ .

Supposons maintenant que ϕ est séparable. Soit θ un élément de $D_k(V) = D_k(K)$, i.e. une différentielle sur V , définie sur k (ou encore une k-différentielle de K). On a une injection canonique $D_k(V) \to D_k(W)$ obtenue en faisant correspondre à θ sa transposée $\theta \circ \phi$ sur W (c'est d'ailleurs aussi l'injection canonique $D_k(K) \to D_k(L)$ considérée dans E , Chap.III, n°2). On conviendra d'identifier θ avec son image par cette injection canonique. Soit maintenant $\omega \in D_k(W) = D_k(L)$. Pour $\theta \in D_k(V)_{\neq 0}$ quelconque, on a $\omega = g\,\theta$, avec $g \in L$. On appelle trace de ω relativement à ϕ , et on note $\mathrm{Tr}\,\omega$, ou $\mathrm{Tr}_\phi \omega$, la différentielle $(\mathrm{Tr}\,g)\theta$. Cette définition a un sens, car il est clair que cette différentielle ne dépend que de ω , mais non du choix de θ . On voit en outre que $\mathrm{Tr}_\phi \omega$ est linéaire en ω et que, pour $f \in L$, on a $\mathrm{Tr}_\phi(df) = d(\mathrm{Tr}_\phi f)$.

THEOREME 8.

Soit $\phi : W \to V$ un revêtement séparable. Soit $a \in V$, et notons b_i les composants de l'ensemble $(\phi^{-1})_e(a)$. Alors, pour toute différentielle ω sur W , on a

$$\sum_i \mathrm{Res}_{b_i} \omega = \mathrm{Res}_a(\mathrm{Tr}\,\omega).$$

Démonstration. Pour tout i , posons $w_i = v_{b_i}$. Si t est un paramètre uniformisant de V en a , et si $\omega = f\,dt$, on a $\mathrm{Tr}\,\omega = (\mathrm{Tr}\,f)dt$. D'après le lemme 4 , on a d'autre part $\mathrm{Tr}\,f = \sum_i \mathrm{Tr}_{w_i} f$. Il suffit donc de démontrer qu'on a, pour tout i

$$\mathrm{Res}_{w_i} \omega = \mathrm{Res}_v(\mathrm{Tr}_{w_i} f)\,dt$$

.../...

Désignant par b l'un quelconque des points b_i, il est naturel d'appeler trace locale de ω relativement à x la différentielle $(\mathrm{Tr}_{w/v} f)dt$, et de la désigner par $\mathrm{Tr}_{w/v}\,\omega$ (on vérifie sans peine que cette différentielle ne dépend pas du choix de t).

Il nous suffit, dans ces conditions, de démontrer le lemme suivant (où l'on pose $v = v_a$, $w = v_b$).

LEMME 5. On a $\mathrm{Res}_w \omega = \mathrm{Res}_v \mathrm{Tr}\,\omega$, où Tr désigne la trace locale $\mathrm{Tr}_{w/v}$.

Démonstration. Soit t (resp. u) une uniformisante de $\hat{K}$ (resp. $\hat{L}$). Par linéarité, il suffit de démontrer la formule lorsque ω est de la forme $\omega = u^m dt$, où $m \in \mathbf{Z}$. Si e est l'ordre de ramification de L/K relativement à v (i.e. le degré $[\hat{L}:\hat{K}]$), on a une relation de la forme

$$(4)\quad t = u^e(1 + a_1 u + \ldots + a_n u^n + \ldots)$$

Dans le cas où la caractéristique est 0, tout élément inversible de $\hat{o}$ admet une racine e-ième dans $\hat{o}$; en remplaçant, s'il y a lieu, u par une solution u' de $t = u'^e$, on se ramène au cas où $t = u^e$. La démonstration de la formule est alors élémentaire. En effet, on a $m = eq + r$, avec $q \in \mathbf{Z}$ et $0 \leq r < e-1$, ce qui donne $\omega = t^q u^r dt$, d'où

$$\mathrm{Tr}\,\omega = (\mathrm{Tr}\,u^r)\, t^q\, dt = \begin{cases} 0 & \text{si } r \neq 0 \\ e t^q dt & \text{si } r = 0. \end{cases}$$

On en déduit

$$\mathrm{Res}_v \mathrm{Tr}\,\omega = \begin{cases} 0 & \text{si } m \neq -e \\ e = -m & \text{si } m = -e \end{cases}$$

On a d'autre part

$$\mathrm{Res}_w \omega = \mathrm{Res}_w\, e\, u^{m+e-1}\, du = \begin{cases} 0 & \text{si } m \neq -e \\ e = -m & \text{si } m = -e\,. \end{cases}$$

.../...

et la formule est bien démontrée dans ce cas.

Supposons maintenant que la caractéristique est quelconque, t et u étant liés par (4).

On a

$$\mathrm{Res}_w u^m\, dt = -m\, a_{-m-e}\ .$$

D'autre part, comme on a vu, $1, u, \ldots u^{e-1}$ forment une base de l'extension $\hat{L}/\hat{K}$. Pour obtenir la trace de u^m, on peut considérer l'endomorphisme $y \mapsto u^m y$ dans $\hat{L}$, regardé comme espace vectoriel sur $\hat{K}$. Notons $M_m = (c_{mij})$ $(1 \leq i \leq e\ ,\ 1 \leq j \leq e)$ la matrice correspondante. Les c_{mij} sont des éléments de $k((t))$, donc de la forme $\sum_k c_{mijk} t^k$, où les coefficients c_{mijk} s'expriment par des polynômes universels à coefficients dans Z en fonction des a_n. La trace de u^m étant égale à celle de la matrice M_m, son résidu s'exprime aussi par un polynôme universel P_m en fonction des a_n. D'après ce qui précède, ce polynôme P_m prend la valeur $-m\, a_{-m-e}$ lorsqu'on prend pour $a_1, \ldots, a_n, \ldots$ des éléments arbitraires d'un corps quelconque de caractéristique 0. Donc $P_m(a)$ est identique à $-m\, a_{-m-e}$, et le lemme est démontré dans tous les cas.

<u>Fin de la démonstration du th. 7 (formule des résidus)</u>.

Soit f une fonction non constante sur V. Elle se prolonge à un morphisme $f^* : V \to \mathbb{P}_1$, qui est un revêtement séparable de $\mathbb{P}_1$ en choisissant pour f un élément formant une base de transcendance de $\mathcal{F}_k(V)^1$. Pour tout $a \in \mathbb{P}$, on a, d'après le th. précédent,

$$\sum_{b/a} \mathrm{Res}_b\, \omega = \mathrm{Res}_a\, \mathrm{Tr}\, \omega$$

où Tr est la trace relative à f_*, et où $\sum_{b/a}$ désigne la somme étendue aux composants b de l'ensemble $\varphi_e^{-1}(a)$.

.../...

On en déduit

$$\sum_b \mathrm{Res}_b\ \omega = \sum_a \sum_{b/a} \mathrm{Res}_b\ \omega$$
$$= \sum_a \mathrm{Res}_a(\mathrm{Tr}\ \omega)\ .$$

11. Répartitions.

Soit V une courbe complète sans point multiple, définie sur un corps algébriquement clos k. A tout point $a \in V$, associons le complété $\hat{K}_a$ du corps $K = \mathcal{F}_k(V)$ relativement à la valuation v_a.

Une répartition ξ sur V est définie par la donnée, pour tout $a \in V$, rationnel sur k, d'un élément $\xi_a \in \hat{K}_a$, avec la condition $v_a(\xi_a) = 0$ "pour presque tout $a \in V$", i.e. pour tout a n'appartenant pas à un sous-ensemble fini de V.

Les répartitions forment une algèbre sur k, qu'on notera R, ou R_k.

On a un isomorphisme canonique de K sur un sous-espace de R, obtenu en faisant correspondre à $f \in K$ la répartition définie par $\xi_a = f$ quel que soit a. On identifiera canoniquement K avec son image par cet isomorphisme.

Soit $\underline{d}$ un diviseur sur V. L'ensemble des repartitions $\xi \in R$, telles qu'on ait $v_a(\xi_a) \geq -v_a(\underline{d})$ pour tout $a \in V$, avec la convention $v_a(\mathrm{div}\ f) = v_a(f)$ prolongée à $\mathfrak{D}(V)$ d'après E, III, 14, th. 12). est un sous-k-espace vectoriel de R, qu'on désigne par $S(\underline{d})$.

L'intersection $S(\underline{d}) \cap K$ se compose des fonctions $f \in K$ telles qu'on ait $\mathrm{div}(f) \geq -\underline{d}$; cette intersection est donc l'espace $L(\underline{d})$ introduit dans E, Ch. IV, n° 6. On sait que la dimension de cet espace $L(\underline{d})$ est finie (E, ch. IV, 6, th. 12). On désignera cette dimension par $\ell(\underline{d})$.

Si $\underline{a}$ et $\underline{b}$ sont deux diviseurs sur V, il est clair que

.../...

les relations $\underline{a} \geq \underline{b}$ et $S(\underline{a}) \supset S(\underline{b})$ sont équivalentes.

LEMME 6. On a, pour $\underline{a} \geq \underline{b}$,

$[S(\underline{a}) : S(\underline{b})] = \deg \underline{a} - \deg \underline{b}$.

Démonstration. Pour tout diviseur $\underline{d}$ sur V , $S(\underline{d})$ est somme directe des $t_a^{-v_a(\underline{d})} \underline{\delta}_a$, regardés comme espaces vectoriels sur k (en désignant par t_a un paramètre uniformisant de V en a , défini sur k). Donc l'espace $S(\underline{a})/S(\underline{b})$ est k-isomorphe à la somme directe des espaces vectoriels $F_a = (t_a^{-\nu_a} \underline{\delta}_a)\, \underline{\delta}_a$, où l'on pose $\nu_a = v_a(\underline{a}) - v_a(\underline{b})$ pour tout a . Or F_a est de dimension ν_a . Donc on a

$$[S(\underline{a}) : S(\underline{b})] = \sum_a \nu_a = \deg \underline{a} - \deg \underline{b} .$$

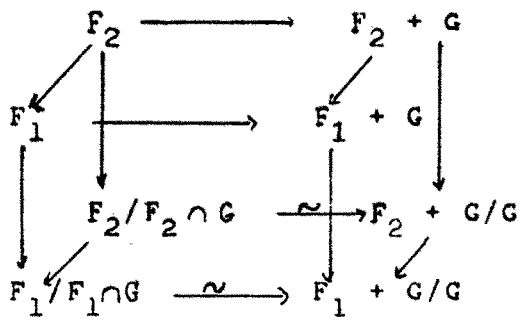
LEMME 7. On a pour $\underline{a} \geq \underline{b}$

(5) $\deg \underline{a} - \deg \underline{b} = [S(\underline{a}) + K : S(\underline{b}) + K] + \ell(\underline{a}) - \ell(\underline{b})$.

Démonstration. On a la propriété générale suivante des espaces vectoriels : soient F_1 , F_2 et G trois sous-espaces vectoriels d'un même espace vectoriel E , tels que $F_1 \supset F_2$; alors on a

$$[F_1 : F_2] = [F_1 + G : F_2 + G] + [F_1 \cap G : F_2 \cap G] .$$

En effet, on remarque que le diagramme suivant



est commutatif. D'après le "second théorème d'isomorphisme" les flèches horizontales du bas sont des isomorphismes. Il suffit de remarquer que les flèches obliques du bas sont injectives, et de comparer leurs conoyaux.

.../...

Pour en déduire le lemme, on prend $F_1 = S(\underline{a})$, $F_2 = S(\underline{b})$ et $G = K$.

Corollaire. $r(d) = \deg \underline{d} - \ell(\underline{d})$ est une fonction croissante de $\underline{d}$.

Remarquons que les entiers $\deg \underline{d}$ et $\ell(\underline{d})$ ne sont pas modifiés lorsqu'on ajoute à $\underline{d}$ le diviseur d'une fonction. Ces deux entiers ne dépendent donc que de la classe de $\underline{d}$ suivant la relation d'équivalence linéaire (cf. n° 1). Il en est donc de même de $r(\underline{d})$.

LEMME 8. L'entier $r(\underline{d})$ admet une borne supérieure r_o . Pour $\underline{d}$ tel que $r(\underline{d}) = r_o$, on a $R = S(\underline{d}) + K$.

Démonstration. Soit f une fonction sur V , non constante, définie sur k , et notons $\underline{b}$ le diviseur des pôles $\mathrm{div}(f)$ de f .

Commençons par montrer que, pour m entier ≥ 0 , le nombre $r(m\,\underline{b})$ admet en majorant indépendant de m . En effet, soit x un point générique de V sur k , et posons $y = f(x)$. L'extension $k(x)/k(y)$ est algébrique de degré fini n . Introduisons une base $z_1, \ldots, z_n$ de cette extension, et choisissons-la de façon que les z_j soient entiers sur l'anneau $k[y]$. Tout pôle b de l'un des z_j est contenu dans $\mathrm{supp}\,\underline{b}$, i.e. est un pôle de f : en effet, il existe une place ρ de $k(x)$ triviale sur k , telle que $\rho(x) = b$, et $\rho(z_1) = \infty$, donc, d'après E, ch. 0, B, 3, th. 2, on a aussi $\rho(y) = \infty$. On peut donc trouver un entier $m_o \geq 0$ tel que $-m_o\,\underline{b} \leq \mathrm{div}(z_j)$, i.e. $z_j \in L(m_o\,\underline{b})$ pour tout j . Pour tout couple d'entiers s, t tels que $0 \leq t \leq s$, on a donc $-(m_o+s)\underline{b} \leq \mathrm{div}(y^t z_j)$, i.e. $y^t z_j \in L((m_o+s)\underline{b})$. Or, pour s fixé, les $y^t z_j$

.../...

$(0 \leq t \leq s\ ,\ 1 \leq j \leq n)$ sont linéairement indépendants sur k . On a donc

$$\ell(m_o + s)\underline{b} \geq (s+1)n\ ,$$

ou encore, en posant $m = m_o + s$,

$$\ell(m\ \underline{b}) \geq (m - m_o + 1)n$$

Or (n° 7, th. 5, coroll 2), on a $\deg \underline{b} = n$. On a donc

$$r(m\ \underline{b}) \leq (m_o - 1)\ n$$

et on a bien montré que $r(m\ \underline{b})$ est majoré.

Soit maintenant $\underline{d}$ un diviseur quelconque sur V . Montrons qu'on peut trouver un élément u de $k[y]$ et un entier $m \geq 0$ tels que $\mathrm{div}(u) + m\ \underline{b} \geq \underline{d}$. Pour cela, posons $\underline{d} = \sum_i a_i + \underline{d}'$ où les a_i $(1 \leq i \leq i_o)$ n'appartiennent pas à $\mathrm{supp}\ \underline{b}$, et où $\underline{d}'$ est un diviseur sur $\underline{b}$ tel que $\mathrm{supp}\ \underline{d}'^{+} \subset \mathrm{supp}\ \underline{b}$; pour tout i , la fonction $u_i = f - f(a_i)$ est morphique et s'annule en a_i ; d'autre part, les pôles de u_i et de f sont les mêmes. On a donc $\mathrm{div}(u_i) + \underline{b} \geq a_i$; il existe d'autre part un entier q tel que $q\ \underline{b} \geq \underline{d}'^{+}$, d'où $q\ \underline{b} \geq \underline{d}'$; posant alors $\prod_i u_i = u$, et $m = i_o + q$, on a bien $\mathrm{div}(u) + m\underline{b} \geq \underline{d}$.

On a, dans ces conditions, $r(\underline{d}) \leq r(\mathrm{div}\ u + m\ \underline{b}) = r(m\ \underline{b})$. On a donc bien montré que $r(\underline{d})$ est majoré. Posons $\sup r(\underline{d}) = r_o$, et prenons maintenant pour $\underline{d}$ un diviseur tel que $r(\underline{d}) = r_o$. Pour tout diviseur $\underline{a}$ sur V , on a $S(\underline{d}) + K \supset S(\underline{a}+\underline{d}) + K \supset S(\underline{a}) + K$. On a donc $S(\underline{d}) + K \supset u_{\underline{a}}(S(\underline{a}) + K) \supset u_{\underline{a}}\ S(\underline{a}) = R$, d'où $S(\underline{d}) + K = R$.

COROLLAIRE. Pour tout diviseur $\underline{a}$ sur V , on a

$$[R : S(\underline{a}) + K] < \infty$$

.../...

12. Genre d'une courbe. Inégalité de Riemann-Roch.

Pour tout diviseur $\underline{a}$ sur V, on posera $i(\underline{a}) = [R : S(\underline{a}) + K]$. La relation (5) intervenant dans le lemme 7 s'écrit sous la forme

$$-\ell(\underline{a}) + \deg \underline{a} + i(\underline{a}) = -\ell(\underline{b}) + \deg \underline{b} + i(\underline{b}).$$

Autrement dit, le nombre entier $-\ell(\underline{a}) + \deg \underline{a} + i(\underline{a})$ ne dépend pas de $\underline{a}$, mais seulement de la courbe V. Le nombre

$$g = -\ell(\underline{a}) + \deg \underline{a} + i(\underline{a}) + 1$$

est appelé le genre de V. Comme $i(\underline{a})$ est positif, on a

$$\ell(\underline{a}) \geq \deg \underline{a} + 1 - g$$

(inégalité de Riemann-Roch).

Pour $\underline{a} = 0$, on a $\deg \underline{a} = 0$, et $\ell(\underline{a}) = 1$. On a donc toujours $g \geq 0$.

13. Le théorème de Riemann-Roch.

On va maintenant, pour calculer le terme $i(\underline{a})$, appelé indice de spécialité du diviseur $\underline{a}$, utiliser une propriété de dualité entre l'espace R des répartitions et celui $D = D_k(V)$ des différentielles sur V, définies sur k.

A tout couple (ω, ξ) composé d'une différentielle $\omega \in D$ et d'une répartition $\xi \in R$, on associe l'élément

$$\langle \omega, \xi \rangle = \sum_a \mathrm{Res}_a(\omega\, \xi_a)$$

de k ; dans cette formule, la somme $\sum_a$ est étendue à tous les points de V ; cette somme a un sens, car $\mathrm{Res}_a \omega\, \xi_a$ est nul pour presque tout a.

Il est clair que $\langle \omega, \xi \rangle$ est une forme k-bilinéaire en ω et ξ. On a de plus $\langle \omega f, \xi \rangle = \langle \omega, f\xi \rangle$ quelle que soit $f \in K$. D'autre part on a toujours $\langle \omega, \xi \rangle = 0$, quelle que soit ω, lorsque $\xi \in K$, d'après la formule des résidus.

.../...

Pour tout diviseur $\underline{a}$ sur V, nous désignerons par $E(\underline{a})$ le sous-espace vectoriel de D composé des différentielles $\omega \in D$ telles que $\mathrm{div}(\omega) \geq \underline{a}$. On a toujours $\langle \omega, \xi \rangle = 0$ lorsque $\omega \in E(\underline{a})$ et $\xi \in S(\underline{a})$ (car alors $\omega \xi_a$ est morphique en a quel que soit a, donc a un résidu nul en a).

Pour toute différentielle $\omega \in D$, notons ω^* la forme linéaire $R \to k$ définie par $\omega^*(\xi) = \langle \omega, \xi \rangle$. Pour $\omega \in E(\underline{a})$ ω^* s'annule sur $S(\underline{a}) + K$, d'après ce qui précède. Autrement dit, si l'on note $R^*(\underline{a})$ l'espace vectoriel composé des formes $\phi : R \to k$ s'annulant sur $S(\underline{a}) + K$, le k-homomorphisme $\theta : \omega \mapsto \omega^*$ induit un k-homomorphisme $\theta_{\underline{a}} : E(\underline{a}) \to R^*(\underline{a})$.

Soit R^* la réunion des espaces $R^*(\underline{a})$, pour tous les diviseurs $\underline{a}$ sur V, rationnels sur k (i.e. le sous-espace du dual de R composé des ξ qui s'annulent sur l'un au moins des $S(\underline{a}) + K$). Il est clair qu'on a $\mathrm{Im}\,\theta \subset R^*$, de sorte qu'on peut regarder θ comme un k-homomorphisme $D \to R^*$.

Remarquons en outre que R^* peut-être regardé comme un espace vectoriel sur K : on fait opérer K dans R^* en posant $(f\,\phi)(\xi) = \phi(f\,\xi)$, pour $\phi \in R^*$. De plus, le k-homomorphisme $\theta : D \to R^*$ est en fait un K-homomorphisme, car on a $(f\,\omega)^*(\xi) = \langle f\omega, \xi \rangle = \langle \omega, f\xi \rangle = \omega^*(f\,\xi)$, d'où $(f\,\omega)^* = f\,\omega^*$.

THEOREME 9.

Le K-homomorphisme $\theta : D \to R^*$ est un K-isomorphisme.

Démonstration.

(a) - θ est injectif. On utilise le lemme suivant

LEMME 9. Soit $\omega \in D$. Alors

$$\omega^* \in R^*(\underline{a}) \Longrightarrow \omega \in E(\underline{a}).$$

En effet, supposons que $\omega \notin E(\underline{a})$. Il existe alors $a \in V$,

.../...

rationnel sur k, tel que $\mu_a = v_a(\omega) < v_a(\underline{a})$. Soit t un paramètre uniformisant de V en a, et considérons la répartition ξ obtenue en posant

$$\begin{cases} \xi_a = t^{-(\mu_a+1)} \\ \xi_b = 0 \quad \text{pour} \quad b \neq a . \end{cases}$$

On a visiblement $\xi \in S(\underline{a})$. On a d'autre part $v_a(\omega\,\xi_a) = -1$, d'où $\mathrm{Res}_a(\omega\,\xi_a) \neq 0$, et $\omega\xi_b = 0$, d'où $\mathrm{Res}_b(\omega\,\xi_b) = 0$ pour $b \neq a$. On a donc $<\omega,\xi> \neq 0$, d'où contradiction, et le lemme est démontré.

L'injectivité de θ en résulte aussitôt : en effet, la relation $\theta(\omega) = \omega^* = 0$ entraîne $\omega^* \in R^*(\underline{a})$, d'où $\omega \in E(\underline{a})$ pour tout diviseur $\underline{a}$ sur V, d'où $\omega = 0$.

(b) - θ est <u>surjectif</u>. On raisonne sur les dimensions : on sait que $\dim_K D = 1$. Il suffit donc de montrer que $\dim_K R^* \leq 1$.

Supposons $\dim_K R^* > 1$, et soient α, α' deux éléments de R^* linéairement indépendants sur K. Si $(x_1, \ldots, x_m)$ sont des éléments linéairement indépendants sur k, αx_i, $\alpha' x_j$ $(1 \leq i \leq m\,,\ 1 \leq j \leq m)$ sont linéairement indépendants sur k.

Par définition de R^*, il existe deux diviseurs $\underline{a}$ et $\underline{a}'$ sur V tels que α et α' s'annulent respectivement sur $S(\underline{a})$ et $S(\underline{a}')$. Donc α et α' s'annulent sur $S(\underline{b})$, en posant $\underline{b} = \inf(\underline{a},\underline{a}')$. Soit maintenant $\underline{d}$ un diviseur quelconque sur V, et soit $y \in L(\underline{d})$. Les éléments αy et $\alpha' y$ s'annulent sur $S(\underline{b} + \mathrm{div}(y))$, donc a fortiori, sur $S(\underline{b}-\underline{d})$ (puisque $\mathrm{div}(y) \gg -\underline{d}$), i.e. appartiennent à $R^*(\underline{b}-\underline{d})$. On a donc, compte tenu de la remarque précédente,

$$\dim_k R^*(\underline{b}-\underline{d}) \geq 2\ell(\underline{d})$$

.../...

D'autre part $R^*(\underline{b}-\underline{d})$ s'identifie au dual de $R/S(\underline{b}-\underline{d}) + K$; sa dimension est donc $i(\underline{b}-\underline{d})$, et on a

$$i(\underline{b} - \underline{d}) \geq 2\ell(\underline{d})$$

c'est-à-dire

$$\ell(\underline{b} - \underline{d}) - \deg(\underline{b} - \underline{d}) + g - 1 \geq 2\ell(\underline{d})$$

Si on prend $\underline{d} > \underline{b}$, on a $\ell(\underline{b} - \underline{d}) = 0$, d'où

$$\deg \underline{d} + g - 1 - \deg \underline{b} \geq 2\ell(\underline{d})$$

D'autre part, d'après l'inégalité de Riemann-Roch, on a

$$\ell(\underline{d}) \geq \deg \underline{d} - g + 1$$

En comparant les deux inégalités ci-dessus, on trouve que $\deg \underline{d}$ est majoré par une constante, ce qui est absurde. Le th. 9 est donc démontré.

THEOREME 10.

Pour tout diviseur $\underline{a}$ sur V , rationnel sur k , le k-homomorphisme

$$\theta_{\underline{a}} : E(\underline{a}) \to R^*(\underline{a})$$

induit par θ est un k-isomorphisme. Autrement dit, la forme $< \omega, \xi >$ met en dualité des deux espaces $E(\underline{a})$ et $R/S(\underline{a}) + K$.

Démonstration. En effet, $\theta_{\underline{a}}$ est injectif, comme induit par θ . D'autre part, pour $\phi \in R^*(\underline{a})$, il existe, d'après le th. 9, une differentielle $\omega \in D$ telle que $\phi = \omega^*$. D'après le lemme 9 , on a $\omega \in \mathfrak{R}(\underline{a})$, et $\phi = \theta_{\underline{a}}(\omega)$. Donc $\theta_{\underline{a}}$ est surjectif.

On peut maintenant calculer l'entier $i(\underline{a})$. En effet, $i(\underline{a})$ est, par définition, égal à la dimension de l'espace $R/S(\underline{a}) + K$, donc aussi à celle de son dual $R^*(\underline{a})$. D'après le th. 10 on a donc

$$i(\underline{a}) = \dim E(\underline{a}) .$$

.../...

Puisque les différentielles forment un espace vectoriel de dimension 1 sur le corps $\mathcal{F}(V)$, deux différentielles non nulles quelconques ω et ω' sur V sont liées par $\omega' = f\omega$, avec $f \in \mathcal{F}(V)$, et on a $\mathrm{div}(\omega') = \mathrm{div}(f) + \mathrm{div}(\omega)$, d'où $\mathrm{div}(\omega') \sim \mathrm{div}(\omega)$. Par suite <u>la classe de $\mathrm{div}(\omega)$ pour l'équivalence linéaire</u> ne dépend pas de ω, mais seulement de V. Cette classe est appelée la <u>classe canonique</u>. Tout diviseur $\underline{c}$ sur V appartenant à cette classe est le diviseur d'une différentielle ω : en effet, soit ω_c une différentielle non nulle sur V ; on a $\underline{c} \sim \mathrm{div}(\omega_o)$, donc il existe $f \in \mathcal{F}(V)$ telle que $\mathrm{div}(f) = \underline{c} - \mathrm{div}(\omega_o)$, et on peut prendre $\omega = f\,\omega_o$. Un tel diviseur $\underline{c}$ est dit <u>canonique</u>. Remarquons que si $\underline{c}$ est rationnel sur un corps de définition k_1 de V ; on peut prendre $\omega \in D_{k_1}(V)$: en effet, ayant choisi $\omega_o \in D_{k_1}(V)$, il suffit de prendre $f \in \mathcal{F}_{k_1}(V)$, ce qui est possible d'après E, IV, 6, th. 11.

Soit $\underline{c}$ un diviseur canonique sur V, de la forme $\mathrm{div}(\omega)$, avec $\omega \in D$. Pour $\omega' \in D$, de la forme $\omega' = g\omega$, la relation $\omega' \in E(\underline{a})$ équivaut à $\mathrm{div}(g) \gg \underline{a} - \underline{c}$. On a donc $\dim E(\underline{a}) = \ell(\underline{c} - \underline{a})$, d'où

$$(5) \qquad i(\underline{a}) = \ell(\underline{c} - \underline{a}) .$$

Rappelons que si $\underline{a}$ est un diviseur sur V, rationnel sur un corps de définition k de V, la dimension $\ell(\underline{a})$ de l'espace $L(\underline{a})$ ne dépend pas du choix de k (cf. E, ch IV, 6).

On peut donc énoncer :

<u>THEOREME 11</u>. (<u>Riemann-Roch</u>)

Soit $\underline{c}$ un diviseur canonique sur V. Pour tout divi-

.../...

seur $\underline{a}$ sur V, on a

$$\ell(\underline{a}) = \deg \underline{a} - g + 1 + \ell(\underline{c} - \underline{a})$$

COROLLAIRE. On a les formules

$$\ell(\underline{c}) = g \text{ , et } \deg \underline{c} = 2g - 2$$

En effet, pour $\underline{a} = 0$, on a $\deg \underline{a} = 0$, $\ell(\underline{a}) = 1$, et le théorème donne $\ell(\underline{c}) = g$.

En faisant $\underline{a} = \underline{c}$, on obtient ensuite

$$\ell(\underline{c}) = \deg \underline{c} - g + 2 ,$$

ce qui donne $\deg \underline{c} = 2g - 2$.

CHAPITRE III

LA JACOBIENNE D'UNE COURBE ALGEBRIQUE.

1. Variétés de pré-groupe.

Soit V une variété, et soit ϕ une application rationnelle $V \times V \to V$. On dit que ϕ est une loi de pré-groupe, ou une"loi de composition normale" sur V, et qu'elle définit sur V une structure de variété de pré-groupe si les conditions suivantes sont satisfaites.

(*) Pour tout corps k de définition de V et de ϕ, et pour x, y génériques indépendants de V sur k, on a, en posant $z = \phi(x,y)$, les relations

(1) $k(x,y) = k(x,z) = k(y,z)$.

(**) Pour x, y, u génériques indépendants de V sur k, on a

(2) $\phi(\phi(x,y),u) = \phi(x,\phi(y,u))$

i.e. ϕ est "génériquement associative".

Exemple : Toute variété de groupe, ou encore tout ouvert d'une variété de groupe, est une variété de pré-groupe.

La relation (1) implique que deux quelconques des trois points x, y, z sont génériques indépendants sur k. Si ϕ est une application rationnelle $V \times V \to V$, définie sur k, vérifiant (*), on note $\overline{\phi}$ l'application rationnelle, définie sur k, obtenue en échangeant x et y, i.e. telle que $z = \phi(x,y) = \overline{\phi}(y,x)$; on note ϕ' et ϕ'' les applications rationnelles $V \times V \to V$, définies sur k, respectivement telles que $x = \phi'(y,z)$ et $y = \phi''(z,x)$.

On note respectivement τ_x et τ'_x les "translations génériques" à droite et à gauche, associées à x, i.e. les applications birationnelles $V \to V$, définies sur $k(x)$, respectivement

.../...

telles que $\phi(x,y) = \tau_x(y)$ et $\phi(y,x) = \tau'_x(y)$.

THEOREME 1.

Soit V une variété de pré-groupe. Alors V est birationnellement équivalente à une variété de groupe. Plus précisément il existe une variété de groupe G et une application birationnelle $\lambda : V \to G$ telle que la loi de groupe sur G soit transposée par λ de la loi de pré-groupe sur V.

Remarque 1. On sait montrer en outre que, si V est définie sur un corps k, on peut prendre G et λ définies sur k.

La démonstration qui va suivre nécessite deux lemmes intermédiaires.

Si W et W' sont deux variétés, et si $\theta : W \to W'$ est une application rationnelle, l'ouvert de W composé des points en lesquels θ est morphique sera appelé ouvert de morphicité de θ, et noté U_θ (cf. E, ch. II, 11, th. 9).

LEMME 1. Soient V une variété définie sur un corps k, ϕ une application rationnelle définie sur k vérifiant la condition (*). Il existe un corps k_1 contenant k, et un k_1-ouvert U_1 de V tels que, pour tout point $a \in U$, et pour u générique de V sur $k_1(a)$, les conditions suivantes soient satisfaites :

(a) - ϕ est morphique en (a,u)

(b) - $t = \phi(a,u)$ est générique de V sur $k_1(a)$

(c) - $\begin{cases} \phi' \text{ est morphique en } (u,t) \\ \phi'' \text{ est morphique en } (t,a). \end{cases}$

On a alors nécessairement $\phi'(u,t) = a$ et $\phi''(t,a) = u$.

Démonstration. Notons ψ' et ψ'' les applications birationnelles $V \times V \to V \times V$, définies sur k, respectivement

.../...

telles que

$$\psi'(x,y) = (y, \phi(x,y))$$

et

$$\psi''(x,y) = (\phi(x,y),x)$$

Les ouverts $U_{\psi'}$ et $U_{\psi''}$ coïncident avec U_ϕ. Notons respectivement β' et β'' les restrictions à U_ϕ de ψ' et ψ''. Considérons l'ouvert

$$T = \beta'^{-1}(U_{\phi'}) \cap \beta''^{-1}(U_{\phi''})$$

de $V \times V$. Soit (t_1,u_1) un point générique de $V \times V$ sur k. Ce point appartient à T, donc l'ouvert

$$U_1 = pr_1(T \cap (V \times u_1))$$

n'est pas vide (on note pr_1 la projection sur le premier facteur dans $V \times V$). Posons $k(u_1) = k_1$; il est clair que U_1 est un k_1-ouvert de V. Pour $a \in U_1$, on a $(a,u_1) \in T$. Si u est un point générique de V sur $k_1(a)$, on a a fortiori $(a,u) \in T$. Comme on a $T \subset U_\phi$, ϕ est morphique en (a,u). De plus, puisqu'on a $(a,u) \in \beta'^{-1}(U_{\phi'})$, et $(a,u) \in \beta''^{-1}(U_{\phi''})$, les applications rationnelles ϕ' et ϕ'' sont morphiques en $\beta'(a,u)$ et $\beta''(a,u)$ respectivement. En d'autres termes si on pose $\phi(a,u) = t$, ϕ' et ϕ'' sont morphiques en (u,t) et (t,a) respectivement. Le couple (k_1,U_1) vérifie donc les conditions (a) et (c). Puisque ϕ (resp. ϕ'') est définie sur k_1, le point t (resp. u) est rationnel sur $k(u,a)$ (resp. $k(t,a)$). On a donc $k(a,t) = k(a,u)$, et par suite t est générique de V sur $k(a)$, ce qui montre que (k_1,U_1) vérifie la condition (b).

COROLLAIRE : Les notations étant celles du lemme 1. il existe un corps k' contenant k et un k'-ouvert U vérifiant les conditions du lemme 1 relativement à chacune des

.../...

six applications rationnelles ϕ, ϕ', ϕ'', $\overline{\phi}$, $\overline{\phi}'$, $\overline{\phi}''$.

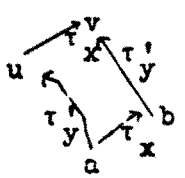
On peut en effet, à chacune de ces applications rationnelles associer une extension de k et un ouvert de V, vérifiant les conditions du lemme 1 . Il suffit de prendre pour k' le composé de ces corps et pour U la réunion de ces ouverts.

Il s'ensuit que, si a est un point de U, et si x est un point générique de V sur $k'(a)$, chacune des translations génériques τ_x, τ'_x est bimorphique en a, et a pour valeur un point générique de V sur $k'(a)$.

LEMME 2. Soit V une variété, et soit ϕ une loi de prégroupe sur V . Soit k' une extension de k, et U un k'-ouvert de V vérifiant les conditions du corollaire du lemme 1. Soit x un point générique de V sur k, et considérons le graphe $\Gamma = \Gamma_{\tau_x}$ de la translation générique τ_x . Si a et b sont deux points de U tels que $(a,b) \in \Gamma$, l'application τ_x est bimorphique en a, de valeur b .

Démonstration. Introduisons un point y générique de V indépendant de x sur $k'(a,b)$. D'après le coroll. du lemme 1, la translation générique τ'_y est bimorphique en chacun des points a et b, et chacun des points $u = \tau'_y(a)$, $v = \tau'_y(b)$ est générique de V sur $k'(a,b,x)$.

En vertu de la condition (**), l'application rationnelle $\mu = \tau'_y \circ \tau_x$ coïncide avec $\tau_x \circ \tau'_y$. Puisqu'on a $(a,b) \in \Gamma = \Gamma_{\tau_x}$, et puisque τ'_y est morphique en b, de valeur v, on a $(a,v) \Gamma_\mu$. Puisque y est générique de V sur $k'(a,b,x)$, il en est de même de u, d'après le coroll. du lemme 1 ; donc x est



.../...

générique de V sur $k'(u)$; donc τ_x est bimorphique en u ; donc $\mu = \tau_x \circ \tau'_y$ est morphique en a. On a donc nécessairement $v = \mu(a) = \tau_x(u)$. En définitive :

τ'_y est bimorphique en a, de valeur u

τ_x " " " u, " " v

τ'^{-1}_y " " " v, " " b

Donc $\tau_x = \tau'^{-1}_y \circ \tau_x \circ \tau'_y$ est bimorphique en a, de valeur b, C. Q. F. D.

Nous allons maintenant aborder la démonstration du th. 1, et donner la construction de la variété de groupe G. Pour cela introduisons un entier m (le choix de cet entier sera précisé plus loin), et des points $u_1, \ldots, u_m$ génériques indépendants de V sur le corps k' introduit ci-dessus. Pour tout indice α $(1 \leq \alpha \leq m)$, on pose $\tau_\alpha = \tau_{u_\alpha}$. Pour tout couple d'indices (α,β), l'application rationnelle $U \to U$, obtenue par restriction à U de $\tau_\beta \circ \tau_\alpha^{-1}$ est notée $\tau_{\beta\alpha}$. Son graphe $\Gamma_{\tau_{\beta\alpha}}$ est encore noté $\Gamma_{\beta\alpha}$. On a $\tau_{\beta\alpha} = \tau_{w_{\beta\alpha}}$, où $w_{\beta\alpha}$ est le point de V, nécessairement générique de V sur k, défini par $w_{\beta\alpha} = \psi(u_\alpha, u_\beta)$, en posant $\psi = \overline{\phi}''$. D'après le corollaire du lemme 1, pour a_α et $b_\beta \in U$, tels que $(a_\alpha, b_\beta) \in \Gamma_{\beta\alpha}$, l'application $\tau_{\beta\alpha}$ est bimorphique en a_α, de valeur b_β. Donc, si, pour tout α, on prend $G_\alpha = U$, la famille $\{G_\alpha, T_{\beta\alpha}\}$ définit une variété abstraite G (cf. E et EA, ch. II, n°1). On a de plus une application rationnelle $\lambda : V \to G$, définie sur le corps $K = k'(u_1, \ldots, u_m)$, obtenue en prenant pour image d'un point générique x de V sur K le point de G représenté, quel que soit α, par le point $x_\alpha = \tau_\alpha(x)$ de G_α.

Soit θ l'application rationelle $G \times G \to G$ transposée

.../...

par λ de la loi de pré-groupe $\phi : V \times V \to V$. Nous allons d'abord montrer que θ est un morphisme.

Pour tout triplet d'indices α, β, γ, notons $\theta_{\alpha\beta\gamma}$ l'application rationnelle $G_\alpha \times G_\beta \to G_\gamma$ qui représente θ, i.e. telle qu'on ait $z_\gamma = \theta_{\alpha\beta\gamma}(x_\alpha, y_\beta)$, en posant $x_\alpha = \tau_\alpha(x) = \phi(u_\alpha, x)$, $y_\beta = \tau_\beta(y) = \phi(u_\beta, y)$ et $z_\beta = \tau_\gamma(z) = \phi(u_\gamma, z)$, pour x et y génériques indépendants de V sur K, et en posant $z = \phi(x,y)$. On a aussi $z_\gamma = F(u_\alpha, u_\beta, u_\gamma, x_\alpha, y_\beta)$, en désignant par F la fonction sur $V \times V \times V \times V \times V$, définie sur k', telle que

(3) $F(u_\alpha, u_\beta, u_\gamma, x_\alpha, y_\beta) = \phi(\psi(\phi(\psi(u_\gamma, u_\alpha), x_\alpha), u_\beta), y_\beta)$.

Soient maintenant $\overline{a}$ et $\overline{b}$ deux points de V, respectivement représentés par $a_\alpha \in G_\alpha$ et par $b_\beta \in G_\beta$. Si on note n la dimension de V, le degré de transcendance de l'extension $k'(u_\alpha, u_\beta, a_\alpha, b_\beta)/k'$ est $\leq 4n$. Supposons qu'on ait pris $m > 4n$. Alors l'un au moins des u_γ est générique de V sur le corps $k'' = k'(u_\alpha, u_\beta, a_\alpha, b_\beta)$: sinon, en effet, on aurait deg. tr $(k''(u_\gamma)/k'') \leq n-1$ quel que soit γ, d'où deg.tr.$(k''(u_1, \ldots, u_m)/k'') \leq m(n-1)$, et on en déduirait deg. tr.$(k''(u_1, \ldots, u_m)/k') \leq m(n-1) + 4n$; or le premier membre de cette inégalité est $\geq$ deg.tr.$(k'(u_1, \ldots, u_m)/k') = mn$; on en tirerait $m \leq 4n$, ce qui est contradictoire.

Choisissons donc γ tel que u_γ soit générique de V sur k''. En appliquant trois fois le lemme 2, on trouve successivement :

(a) - que ϕ est morphique au point $(\psi(u_\gamma, u_\alpha), a_\alpha) = (\psi(w_{\alpha\gamma}), a_\alpha)$, de valeur un point c générique de V sur k''.

.../...

(b) - que ψ est morphique au point (c,t_β), de valeur un point d générique de V sur k" .

(c) - que ϕ est morphique au point (d,y_β).

On en déduit que F est morphique en $(u_\alpha,u_\beta,u_\gamma,a_\alpha,b_\beta)$, donc que $\theta_{\alpha\beta\gamma}$ est morphique en (a_α,b_β), et par suite que θ est morphique en $(\bar{a},\bar{b})$. Donc θ est un morphisme.

Puisque ϕ est une loi de pré-groupe sur V , θ est une loi de pré-groupe sur G . En particulier θ est associative. Les points $u_\alpha \in G_\alpha$ représentent un même point $\bar{e} \in G$. Montrons que $\bar{e}$ est élément neutre de G . Soit en effet $\bar{x}$ un point générique de G sur K . Pour tout α , soit x_α le représentant de $\bar{x}$ dans G_α . On trouve pour tout β (par exemple en appliquant la formule (3)), que les points $\theta(\bar{e},\bar{x})$ et $\theta(\bar{x},\bar{e})$ sont tous les deux représentés par $\phi(\psi(u_\beta,u_\alpha),x_\alpha) = x_\beta$ dans G_β . On a donc $\theta(\bar{e},\bar{x}) = \theta(\bar{x},\bar{e}) = \bar{x}$, donc on a bien montré que $\bar{e}$ est élément neutre de G .

Soit encore $\bar{x}$ un point générique de G sur K ; on a $\bar{x} = \lambda(x)$, où x est un point générique de V sur K. Il existe un point $\bar{x}' \in G$, représenté pour tout α par le point $x'_\alpha = \psi(t_\alpha,x)$ de G_α , et on a une application birationnelle $\sigma : G \to G$ telle que $\sigma(\bar{x}) = \bar{x}'$. On trouve, par exemple en appliquant la formule (3), que le composé $\theta(\bar{x},\bar{x}')$ est représenté dans G_β par t_β . On a donc $\theta(\bar{x},\bar{x}') = \bar{e}$, i.e. $\bar{x}'$ est inverse de $\bar{x}$ par θ .

Pour achever de prouver que G est une variété de groupe, il suffit de montrer que σ est un morphisme. Or soit $\bar{a} \in G$, représenté par a_α dans l'un des G_α . En raisonnant comme plus haut, on voit qu'on peut choisir β tel que u_β soit

.../...

générique de V sur $k'(a_\alpha)$. D'après le lemme 2, ϕ est morphique en (u_β, a_α), i.e. σ est morphique en $\bar{a}$ C.Q.F.D.

2. Construction de la jacobienne.

LEMME 3. Soit V une courbe définie sur un corps k Soit $\underline{d}$ un diviseur sur V, rationnel sur k, et soit u un point générique de V sur k. Alors

(a) - Si $\ell(\underline{d}) = 0$, on a $\ell(\underline{d}-u) = 0$

(b) - Si $\ell(\underline{d}) > 0$, on a $\ell(\underline{d}-u) = \ell(\underline{d})-1$.

Démonstration. L'assertion (a) est évidente, puisque $L(\underline{d}-u) \subset L(\underline{d})$.

Supposons donc $\ell(\underline{d}) > 0$. Puisque $\underline{d}$ est rationnel sur k, il existe une fonction $f_o \in L(\underline{d})$, non nulle et définie sur k. Les zéros de cette fonction sont des points algébriques sur k, donc distincts de u, de sorte que $f_o \notin L(\underline{d}-u)$. On a donc

(4) $\ell(\underline{d}-u) < \ell(\underline{d})$.

De plus, pour $f \in L(\underline{d})$, la fonction $h=f/f_o$ est morphique en u ; l'application $f \to h(u)$ induit une forme linéaire sur l'espace $L(\underline{d})$ dont le noyau coïncide avec $L(\underline{d}-u)$ (comparer à la démonstration de E, IV, th.12). On a donc $\dim L(\underline{d})/L(\underline{d}-u) = \ell(\underline{d}) - \ell(\underline{d}-u) \leq 1$. Ceci donne (b), compte tenu de la relation (4).

COROLLAIRE. Soient V, $\underline{d}$ et u comme dans le lemme ci-dessus. Alors

(a) - Si $i(\underline{d}) = 0$, on a $i(\underline{d}+u) = 0$

(b) - Si $i(\underline{d}) > 0$, on a $i(\underline{d}+u) = i(\underline{d})-1$

Soit V une variété définie sur un corps k, et soient $u_1, \ldots, u_n$ des points génériques indépendants de V sur k.

.../...

On appelle corps des fonctions symétriques à n variables sur V , définies sur k , et on note $k(u_1,\ldots,u_n)_s$ le sous-corps de $k(u_1,\ldots,u_n)$ composé des éléments invariants par le groupe des permutations des u_i . L'extension $k(u_1,\ldots,u_n)/k(u_1,\ldots,u_n)_s$ est algébrique, galoisienne et de degré n! . Dans le cas où V est une courbe, le diviseur $\underline{u} = u_1+\ldots+u_n$ est rationnel sur le corps $k(u_1,\ldots,u_n)_s$: en effet, soit f une fonction sur V, définie sur k, et telle que $df \neq 0$. On peut représenter u par la fonction $g = \prod_i (f-f(u_i))$ en l'un quelconque des points u_i , et par la constante 1 en tout point distinct des u_i ; comme g est définie sur $k(u_1,\ldots,u_g)_s$, le diviseur $\underline{u}$ est bien rationnel sur ce corps.

THEOREME 2.

Soit V une courbe de genre g définie sur un corps k . Soit $\underline{a}$ un diviseur sur V , de degré 0 , rationnel sur k . Soient $u_1,\ldots u_g$ des points génériques indépendants de V sur k, et soit $\underline{u}$ le diviseur positif de degré g sur V défini par $\underline{u} = u_1+\ldots+u_g$. Il existe un seul diviseur $\underline{v} = v_1+\ldots+ v_g$ sur V tel qu'on ait $\underline{v} \sim \underline{a} + \underline{u}$. Les composants $v_1,\ldots, v_g$ sont distincts, et sont génériques indépendants de V sur k . On a de plus

$$k(u_1,\ldots, u_g)_s = k(v_1,\ldots, v_g)_s$$

Démonstration : Puisqu'on a deg. $\underline{a} = 0$, on a $\ell(\underline{a}) = 0$ ou 1 . Si $\ell(\underline{a}) = 1$, on a d'après le théorème de Riemann-Roch, $i(\underline{a}) = g$. Tenant compte du coroll. du lemme 3, on en déduit $i(\underline{a}+u_1) = g-1$, $i(\underline{a}+u_1+u_2) = g-2,\ldots, i(\underline{a}+\underline{u}) = 0$. Si $\ell(\underline{a}) = 0$, on a $i(\underline{a}) = g-1)$ et on en déduit encore $i(\underline{a}+\underline{u}) = 0$. Appliquant à nouveau le théorème de Riemann-Roch

.../...

on en déduit $\ell(\underline{a}+\underline{u}) = 1$. Il existe donc bien un et un seul diviseur $\underline{v}$ sur V tel que $\underline{v} \sim \underline{a}+\underline{u}$. Posons $K = k(u_1,\ldots,u_g)_s$. Puisque $\underline{u}$ est rationnel sur $\overline{k}$, $\underline{v}$ est aussi rationnel sur K. En appliquant le résultat ci-dessus pour $\underline{a} = 0$, on voit en outre que $\ell(\underline{u}) = 1$, donc que $\underline{u}$ est l'unique diviseur sur V linéairement équivalent à $\underline{v}-\underline{a}$. Puisque $\underline{v}$ est rationnel sur $k(v_1,\ldots, v_g)$, il en est de même de $\underline{u}$ .Donc les composants $u_1,\ldots,u_g$ sont algébriques sur $k(v_1,\ldots,v_g)$. Le degré de transcendance de $k(v_1,\ldots,v_g)/k$ est donc $\geq$ deg.tr. $k(u_1,\ldots,u_g)/k = g$. Donc $v_1,\ldots, v_g$ sont génériques indépendants de V sur k, et sont algébriques sur K . Tout automorphisme de $\overline{K}/K$ qui permute les u_i laisse $\underline{u}$ et $\underline{v}$ invariants, donc permute les v_j , et induit l'identité sur le corps $L = k(v_1,\ldots,v_g)_s$. D'après la théorie de Galois on a donc $L \subset K$. On a de même $K \subset L$; d'où $K = L$ C. Q. F. D.

Comme l'extension $k(u_1,\ldots,u_g)/k$ est régulière, il en est de même de K/k . On peut trouver un <u>modèle</u> W de cette extension, c'est-à-dire une variété W , définie sur k, telle que $\mathfrak{F}_k(W)$ soit isomorphe à K : il suffit de choisir $x_1,\ldots, x_n \in K$ tels que $K = k(x_1,\ldots, x_n)$, et de prendre pour V le lieu sur k du point $x = (x_1,\ldots, x_n)$ dans l'espace affine S_n . Il est clair que W est de dimension g . Nous allons munir W d'une structure de variété de <u>pré-groupe</u>. Désignons par V^g le produit de g facteurs $V\times\ldots\times V$ et notons ξ l'application rationnelle $V^g \to W$ telle que $\xi(u_1,\ldots,u_g) = x$. Cette application est de degré fini, égal à $g!$, et l'image inverse $(\xi^{-1})_e(x)$ se compose des points déduits de $(u_1,\ldots,u_g)$ par permutation des indices dans V^g.

.../...

Soit q un diviseur sur V, de degré g, rationnel sur une extension k_1 de k. Considérons deux diviseurs sur V de la forme $\underline{u} = u_1 + \ldots + u_g$ et $\underline{v} = v_1 + \ldots + v_g$, où $u_1, \ldots, u_g$, $v_1, \ldots, v_g$ sont $2g$ points linéairement indépendants de V sur k_1. Les points $x = \xi(u_1, \ldots, u_g)$ et $y = \xi(v_1, \ldots, v_g)$ sont deux points génériques indépendants de W sur k_1, tels que $k_1(x) = k_1(u_1, \ldots, u_g)_s$, et $k_1(y) = k_1(v_1, \ldots, v_g)_s$. D'après le th. 2, il existe un et un seul diviseur $\underline{w}$ sur V tel qu'on ait $\underline{w} \sim \underline{u} + \underline{v} - q$, et ses composants $w_1, \ldots, w_g$ sont g points génériques indépendants de V sur k_1. Le point $z = \xi(w_1, \ldots, w_g)$ est donc défini. Puisque $\underline{v}-q$ est rationnel sur $k_1(y)$, on a, toujours d'après le th. 2, $k_1(y)(u_1, \ldots, u_g)_s = k_1(y)(w_1, \ldots, w_g)_s$, i.e. $k_1(x,y) = k_1(y,z)$. On voit de même que $k_1(x,y) = (x,z)$. Donc z est rationnel sur $k_1(x,y)$, et l'application rationnelle $\phi : V \times V \to V$, définie sur k_1, telle que $z = \phi(x,y)$, vérifie la condition (*) du n°1. Puisque l'addition des diviseurs est associative la loi ϕ vérifie également la condition (**), donc définit sur W une structure de variété de pré-groupe. D'après le th. 1, il existe une application birationnelle $\lambda : W \to J$ de W sur une <u>variété de groupe</u> J de dimension g. Nous montrerons au n° 4 que J est une variété abélienne, uniquement déterminée à un isomorphisme près. On l'appelle la <u>jacobienne</u> de la courbe V. Dans la suite, on désignera par η l'application rationnelle $\eta = \lambda \circ \xi : V^g \to J$. Si k^* est un corps de définition de V, q, λ et J, et si $u_1, \ldots, u_g$ sont g points génériques indépendants sur k, on a, d'après la construction qui précède, $k^*(u_1, \ldots, u_g)_s = k^*(x)$, en posant

.../...

$x = \eta(u_1, \ldots, u_g)$.

3. Symbole D(A). Diviseurs verticaux.

Soient U et V deux variétés, D un diviseur sur $U \times V$ et a un point de U . Lorsque le symbole $D.(a \times V)$ est défini, on note D(a) le diviseur sur V , rationnel sur k(a), défini par $D(a) = pr_V D.(a \times V)$, où pr_V désigne la projection sur V . On peut aussi exprimer D(a) sous la forme $i_a^{-1}(D)$, où i_a est l'immersion $V \to U \times V$ définie par $i_a(y) = (a,y)$. On dit que D est une correspondance (divisorielle) entre U et V , et que D(a) est la valeur de D en a . L'ensemble des diviseurs D(a) est appelé une famille algébrique de diviseurs sur V , dépendant du paramètre a .

Le diviseur ${}^tD$ sur $V \times U$ déduit de D par l'isomorphisme $(x,y) \to (y,x)$ est appelé correspondance réciproque de D . Pour $b \in V$, tel que le symbole ${}^tD(b)$ soit défini, on a ${}^tD(b) = pr_U (D.(U \times b))$. On a aussi ${}^tD(b) = {}^ti_b^{-1}(D)$, où ${}^ti_b$ est l'immersion $U \to U \times V$ définie par $i_b(x) = (x,b)$.

En particulier, soient U une variété sans point multiple, une courbe et Φ une application rationnelle $U \to V$. Le graphe Γ_ϕ est une sous-variété de codimension 1 de $U \times V$. Comme $U \times V$ est sans point multiple on peut regarder Γ_ϕ comme un diviseur sur $U \times V$, il résulte des définitions que ϕ est morphique en a si et seulement si $\Gamma_\phi(a)$ est défini, et qu'on a alors $\Gamma_\phi(a) = \phi(a)$. De même, si b est un point de V , et si ϕ n'est pas l'application constante, de valeur b , le symbole ${}^t\Gamma_\phi(b)$ est défini, et coïncide avec le diviseur $\phi^{-1}(b)$. (image inverse de b, regardé comme diviseur sur V).

.../...

Une sous-variété d'un produit $U \times V$ sera dite <u>verticale</u> si elle est de la forme $U' \times V$, où U' est une sous-variété de U. Un diviseur sur $U \times V$ sera dit <u>vertical</u> s'il est de la forme $pr_U^{-1}(D)$, où D est un diviseur sur U.

<u>LEMME 4</u>. Soient U et V deux variétés normales. Si D est un diviseur sur U, on a $\mathfrak{X}(pr_U^{-1}(D)) = \mathfrak{X}(D) \times V$.

<u>Remarque 2</u> : Ce lemme entraîne en particulier que, pour qu'un diviseur sur $U \times V$ soit vertical, il faut et il suffit que ses composantes soient verticales. Dans le cas où V est sans point multiple, si l'on identifie D avec $X = \mathfrak{X}(D)$ conformément aux conventions du n°1 au Chap. II, la formule ci-dessus s'écrit simplement $pr_U^{-1}(X) = X \times V$.

<u>Démonstration</u>. Soit W une composante de $Z = \mathfrak{X}(pr_U^{-1}(D))$. Soit k un corps de définition de U, V, D et W. Soit (x,y) un point générique de W sur k, et notons X la sous-variété $(pr_U)_g(W) = \mathrm{loc}_k x$ de U. Soit f une fonction sur U, définie sur k, représentant D au point x. Alors $pr_U^{-1}(D)$ est représenté en (x,y) par la fonction $g = f \circ pr_U$. Pour fixer les idées, supposons que le coefficient de W dans Z soit > 0. Alors g est morphique et s'annule en (x,y). Donc f est morphique et s'annule en x. Ceci implique $X \neq U$, donc $X \times V \neq U \times V$. Puisqu'on a $W \subset X \times V$, et puisque W est de codimension 1 sur $U \times V$, on a nécessairement $W = X \times V$, et X est de codimension 1 sur U, donc est une composante de $\mathrm{div}(f)$, de coefficient > 0. Il suffit de montrer que ce coefficient $v_X(f)$ est égal à celui $v_W(g)$ de $W = X \times V$ dans $\mathrm{div}(g)$. Par linéarité, on se ramène au cas où $v_X(f) = 1$ i.e. où f est un générateur de l'idéal $\underline{m}_k(X,U)$. Soit alors

.../...

h un élément de $\underline{m}_k(W, U \times V)$. Considérons la fonction h_y sur U, définie sur $k(y)$, telle que $h_y(x) = h(x,y)$. Cette fonction s'annule sur X, donc appartient à l'idéal $\underline{m}_{k(y)}(X,U)$, donc est de la forme $h_y = f\, h'_y$, avec $h'_y \in \underline{o}_{k(y)}(X,U)$. La fonction h' sur $U \times V$, définie sur k, telle que $h'(x,y) = h'_y(x)$ appartient donc à $\underline{o}_k(W, U \times V)$; on a de plus $h = g\, h'$. On a donc montré que g est un générateur de l'idéal $\underline{m}_k(W, U \times V)$, i.e. que $v_W(g) = 1$, C.Q.F.D.

LEMME 5. (changement de paramètre). Soient U, U', V trois variétés, et soit $\phi : U' \to U$ un morphisme. Soit k un corps de définition de U, U', V, ϕ, et soit $\overline{\phi}$ le morphisme $U' \times V \to U \times V$, défini sur k, tel que $\overline{\phi}(x,y) = (\phi(x), y)$. Soit D un diviseur sur $U \times V$, tel que $D' = \overline{\phi}^{-1}(D)$ soit défini. Soit a' un point de U', et posons $a = \phi(a')$. Pour que $D'(a')$ soit défini, il faut et il suffit que $D(a)$ le soit, et on a alors $D'(a') = D(a)$.

Démonstration. Soit $b \in V$. Si h est une fonction sur $U \times V$, définie sur k, qui représente D en (a,b), la fonction $h' = h \circ \overline{\phi}$ sur $U' \times V$ représente D' en (a',b) et h' est morphique en (a',b) si et seulement si h est morphique en (a,b). Il en résulte bien que $D'(a')$ est défini si et seulement si $D(a)$ est défini. Si y est générique de V sur $k(a')$, on a de plus $h'(a',x) = h(a,x)$, de sorte que $D'(a')$ et $D(a)$ sont représentés par la même fonction au point b. On a donc bien $D'(a') = D(a)$.

LEMME 6. Soient U et V deux variétés normales définies sur un corps k. Soit Z un diviseur sur $U \times V$, rationnel sur k, et soit u un point générique de U sur k.

.../...

Alors le symbole $Z(u)$ est toujours défini. Pour qu'on ait $Z(u) = 0$, il faut et il suffit que Z soit vertical. En supposant V complète, pour qu'on ait $Z(u) \sim 0$, il faut et il suffit qu'on ait $Z \sim Z'$, où Z' est un diviseur vertical. Dans ce dernier cas, pour tout $a \in U$ simple sur U tel que $Z(a)$ soit défini, on a $Z(a) \sim 0$.

Démonstration. Pour qu'on ait $Z(u) = 0$, il faut et il suffit qu'aucune des composantes de Z ne rencontre $u \times V$, i.e. que chacune de ces composantes soit verticale, donc, compte tenu du lemme 4, que Z soit vertical.

Supposons qu'on ait $Z(u) \sim 0$. Soit x un point générique de V sur $k(u)$. Il existe une fonction f sur V, définie sur $k(u)$, telle que $\mathrm{div}(f) = Z(u)$. Soit h la fonction sur $U \times V$, définie sur k, telle que $h(u,x) = f(x)$. Si on pose $Y = \mathrm{div}(h)$, et $Z' = Z - Y$, on a $Z(u) = Y(u)$, d'où $Z'(u) = 0$. Donc Z' est vertical, d'après la première partie de la démonstration, et on a $Z' \sim Z$. Réciproquement, supposons qu'on ait $Z \sim Z'$, avec Z' vertical, i.e. $Z = Z' + Y$, avec $Y \sim 0$. On peut supposer que u est générique de U sur un corps de définition k' de Z' contenant k. On a alors $Z'(u) = 0$ d'où $Z(u) = Y(u)$, et la relation $Y \sim 0$ entraîne $Z(u) = Y(u) \sim 0$.

Soit a un point simple de U. Posons $Z' = X' \times V$, on peut, en modifiant X', s'il y a lieu, par l'addition du diviseur d'une fonction convenable sur U, supposer que $a \notin \mathrm{supp}.\ X'$. Dans ces conditions, le symbole $Y(a)$ est défini, et on a $Z'(a) = 0$, d'où $Z(a) = Y(a)$, et la relation $Y \sim 0$ entraîne $Z(a) = Y(a) \sim 0$.

.../...

LEMME 7. Soient U et V deux variétés sans point multiple, définies sur un corps k . Soit u un point générique de U sur k , et soit X un diviseur sur V , rationnel sur k(u).

Alors il existe un et un seul diviseur Z sur U × V , sans composante verticale, rationnel sur k , et tel que X = Z(u).

Démonstration. (a). Unicité de Z. Si Z et Z' vérifient les conditions du lemme, et si on pose Y = Z' - Z , on a Y(u) = Z'(u) - Z(u) = 0 . De plus, Y n'a pas de composante verticale. On a donc Y = 0 , d'après le lemme 6, d'où Z' = Z .

(b). Construction de Z. Définissons le diviseur X par un nombre fini de couples (U_i, f_i), où les U_i sont des k(u)-ouverts de V recouvrant V , et les f_i des fonctions sur V , définies sur k(u). Pour tout i, soit F_i le fermé complémentaire de U_i dans V , et soit F_i' la k-adhérence de $u \times F_i$ dans le produit U × V . L'ensemble F_i' est un k-fermé de U × V , tel que $F_i' \cap (u \times V) = u \times F_i$. Le complémentaire U_i de F_i' dans U × V , est donc un k-ouvert non vide de U × V . Puisque les U_i recouvrent V , l'intersection $F' = \bigcap_i F_i'$ ne rencontre pas u × V . Cette intersection est donc "verticale", i.e. contenue dans un k-ensemble algébrique de la forme E × V , où E est un sous-ensemble k-fermé de U . Le complémentaire S de E dans U × V est un k-ouvert non vide de U , tel que S × U soit recouvert par les complémentaires U_i' des F_i' . Pour tout i , introduisons la fonction g_i sur U × V , définie sur k , telle que $g_i(x,y) = f_i(y)$. La réunion des composantes verticales des diviseurs $\mathrm{div}(g_i)$ est de la forme H × V , où H

.../...

est un sous-ensemble k-fermé de U . Notons T l'ouvert de U intersection de S avec le complémentaire de H . Les couples $(g_i, U'_i \cap (T \times V))$ définissent un diviseur sur $T \times V$. En effet les U'_i recouvrent $S \times V$, donc a fortiori recouvrent $T \times V$. D'autre part, soit (a,b) un point de $U'_i \cap U'_j \cap (T \times V)$; la fonction f_i/f_j est inversible en tout point de $(U_i \cap U_j)$, donc le support de div (f_i/f_j) est contenu dans $F_i \cup F_j$. Toutes les composantes non verticales de div (g_i/g_j) sont donc contenues dans $F'_i \cup F'_j$. Par suite, le point (a,b) n'appartient à aucune des composantes de div (g_i/g_j). D'après le critère de morphicité, (g_i/g_j) est inversible en (a,b). Ceci prouve notre assertion : les couples $(g_i, U'_i \cap T \times V)$ définissent bien un diviseur Y sur $T \times V$. On a de plus $Y(u) = X$. Il suffit de prendre pour Z le diviseur sur $U \times V$ admettant les mêmes composantes (prolongées à $U \times V$) que Y , affectées des mêmes coefficients.

4. Spécialisation d'un diviseur sur une courbe.

LEMME 8. Soit V une variété affine $(V \subset \$_n)$ de dimension n . Soit $a = (a_1, \ldots, a_m)$ un point de V , et soit k un corps de définition de V et a . Soient u_{ij} $(1 \leq i \leq m,\ 1 \leq j \leq n)$, des éléments du domaine universel algébriquement indépendants sur k , et soit K la clôture algébrique du corps engendré sur k par les u_{ij} . Pour tout entier r $(1 \leq r < n)$, considérons la"variété linéaire générique" L_r , de dimension n-r , passant par a , définie par le système d'équations

$$\sum_{i=1}^{m} u_{ij} (X_i - a_i) = 0 \qquad (1 \leq j \leq r).$$

.../...

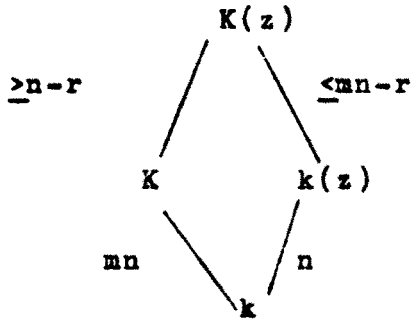
Il existe, quel que soit r, une composante Z de $L_r \cap V$ contenant a, et de dimension $n-r$. De plus, tout point générique de Z sur K est aussi un point générique de V sur k :

Remarque 3 : Dans le cas particulier $r = 1$, ce lemme est un renforcement du lemme 4 du n° 6 du chap. I ; il en diffère par le fait qu'on abandonne ici l'hypothèse que a est simple sur V ; pour le démontrer, on ne peut donc plus utiliser le théorème de la dimension.

Démonstration. Soit x un point générique de V sur K et, pour $1 \leq j \leq n$, posons $y_j = \sum_i u_{ij}(x_i - a_i)$. D'après la démonstration du lemme de normalisation de E. Noether (E, I, 4), les x_i sont algébriques entiers sur l'anneau $K[y_1, \ldots, y_n]$. Notons y le point (générique sur K) de S_n ayant pour coordonnées les y_j, et ϕ le morphisme $V \to S_n$, défini sur K, tel que $\phi(x) = y$. Considérons les points $y' = (0, \ldots, 0, y_{r+1}, \ldots, y_n)$ et $0 = (0, \ldots, 0)$ de S_n. Soient ρ et σ deux places du domaine universel Ω, à valeurs dans Ω, triviales sur K, respectivement telles que $\rho(y) = y'$, et $\sigma(y') = 0$. Notons τ la place composée $\tau = \sigma \circ \rho$. D'après le lemme de relèvement des spécialisations (E, III, 6, lemme 2), on a $\tau(\bar{x}) = a$, où $\bar{x}$ est l'un des conjugués de x sur $K(y)$. Le point $\bar{x}$ est générique de V sur K, et ses coordonnées sont entières sur $K[y]$. Donc ρ est finie en $\bar{x}$, et $\bar{x}' = \rho(\bar{x})$ est un point de V, tel que $\phi(\bar{x}') = y'$. De plus, $\bar{x}'$ est algébrique sur $K(y')$. Donc le lieu Y de $\bar{x}'$ sur K est une variété de dimension $\geq$ deg. tr. $(K(y')/K) = n-r$. Ce lieu est contenu dans $L_r \cap V$

.../...

et puisque $\sigma(\bar{x}') = \tau(\bar{x}) = a$, il contient le point a . Soit Z une composante de $L \wedge V$ contenant Y , et soit z un point générique de Z sur K . Puisqu'on a $\dim Y = n-r$



on a $\dim Z = \text{deg.tr.}(K(z)/K) \geq n-r$
on a donc deg. tr. $(K/k) = mn$
d'où deg. tr. $K(z)/K \geq mn-r$

Puisque $z \in L$, on a les relations

$$\sum_i u_{ij} (z_i - a_i) = 0 \quad (1 \leq j \leq r)$$

Puisqu'on a supposé $r < n$, on a $\dim Y \geq 1$, d'où $\dim Z \geq 1$, et par suite, $z \neq a$. Pour j fixé $(1 \leq j \leq r)$, on peut donc regarder la relation ci-dessus comme une relation de dépendance algébrique entre le u_{ij} , à coefficients dans $k(z)$. On en déduit

deg. tr. $(K(z)/k(z)) \leq mn-r$. On a donc nécessairement les égalités deg. tr. $(K(z)/k(z)) = mn - r$, deg. tr. $(k(z)/k) = n$, et deg. tr. $(K(z)/K) = n-r$. La seconde de ces relations entraîne que z est générique de V sur k ; la dernière entraîne $\dim Z = \dim Y$, d'où $Z = Y$.

C.Q.F.D.

LEMME 9. Soit V une variété définie sur un corps k et soient x et a deux points de V tels que a soit spécialisation de x sur k . Il existe une extension K de k , une courbe U complète sans point multiple définie sur K , une application rationnelle $\phi : U \to V$, et un point $b \in U$ tels que les conditions suivantes soient satisfaites

(a) - Pour u générique de U sur K , le point $x^* = \phi(u)$ est spécialisation générique de x sur k (i.e. Il existe un k-isomorphisme $\sigma : k(x) \to k(x^*)$ tel que $\sigma(x) = x^*$).

.../...

(b) - ϕ est morphique en b, de valeur a.

(Ce lemme permet de ramener l'étude d'une spécialisation quelconque à celle d'une spécialisation d'un point sur une courbe).

Démonstration. Posons $W = \mathrm{loc}_k x$, et notons W^* l'une des composantes de W contenant a. Cette variété W^* est définie sur la clôture algébrique $\bar{k}$ de k. D'après le lemme 8, appliqué en prenant $r = n-1$, on peut trouver une extension K de $\bar{k}$ et une courbe U^*, définie sur K, contenue dans W^* et contenant a, telle que tout point générique de U^* sur K soit générique de W^* sur $\bar{k}$. Par normalisation d'un modèle projectif de U^* on peut trouver une courbe U complète, sans point multiple, définie sur K, et une application birationnelle $\phi : U \to U^*$, définie sur K. Soit alors u un point générique de U sur K. Alors $x^* = \phi(u)$ est un point générique de U^* sur K donc de W^* sur $\bar{k}$. Comme $x^* \in W$, et comme $k(x^*)$ et $k(x)$ ont même degré de transcendance sur k, le point x^* est aussi générique de W sur k, i.e. est spécialisation générique de x sur k. D'autre part, puisque U^* est complète, l'ensemble $(\phi^{-1})_e(a)$ n'est pas vide ; soit b l'un quelconque des composants de cet ensemble ; puisque U est normale en b, ϕ est morphique en b, et nécessairement de valeur a. C.Q.F.D.

Remarque 4. Si l'extension $k(x)/k$ est régulière, on a $W^* = W$, donc on peut choisir K et U^* de façon que $x \in U^*$, puis choisir u générique de U sur K tel que $x = \phi(u)$, de sorte que σ est alors l'identité.

.../...

Soit V une variété définie sur un corps k, et soient $\underline{a} = \sum_{i=1}^{r} m_i a_i$, $\underline{a}' = \sum_{i=1}^{r} m_i a_i'$ deux cycles de dimension 0 sur V ($a_i, a_i' \in V$). On dit que $\underline{a}'$ est une spécialisation de $\underline{a}$ sur k si $(a_1', \ldots, a_r')$ est une spécialisation de $(a_1, \ldots, a_r)$ sur k ; il revient au même de dire qu'il existe une place ρ de Ω, triviales sur k, telle que $\rho(a_i) = a_i'$ pour tout i ; on pose alors $\underline{a}' = \rho(\underline{a})$.

LEMME 10. Soient U et V deux courbes sans point multiple, et supposons V complète. Soient Z un diviseur sur $U \times V$, a un point simple de U tel que le symbole $Z(a)$ soit défini, k un corps de définition de U, V, Z. Alors si u est un point générique de U sur k, le diviseur $Z(a)$ sur V est l'unique spécialisation de $Z(u)$ compatible avec la spécialisation $u \to a$ sur k.

Démonstration. On peut supposer Z positif. Le diviseur $\underline{v} = Z(u)$ étant exprimé sous la forme $\underline{v} = \sum_{i=1}^{r} v_i$ ($v_i \in V$), remarquons que le lemme est trivial lorsque les v_i sont rationnels sur $k(u)$: dans ce cas en effet, Z est la somme des graphes Γ_i des applications rationnelles $\phi_i : U \to V$, respectivement telles que $\phi_i(u) = v_i$, et il suffit de remarquer que l'unique spécialisation de v_i compatible avec $u \to a$ sur k est le point $b_i = \phi_i(a) = \Gamma_i(a)$. On va maintenant montrer que le cas général se ramène au cas ci-dessus, en utilisant le lemme 8. Soit en effet $(v_1, \ldots, v_r) \to (b_1, \ldots, b_r)$ une spécialisation compatible avec $u \to a$ sur k. Puisque chacun des v_i est générique de V sur k, l'extension $k(v_1, \ldots v_r)/k$ est régulière. D'après le lemme 9, et d'après la remarque 4,

.../...

on peut trouver une extension K de k, une courbe U' complète sans point multiple définie sur K, des applications rationnelles $\phi : U' \to U$ et $\psi_i : U' \to V$ $(1 \leq i \leq r)$, et un point générique u' de U' sur K, tels qu'on ait $\phi(u') = u$, $\psi_i(u') = v_i$ pour tout i, et tels de plus que les fonctions ϕ, $\psi_i (1 \leq i \leq r)$ soient morphiques en a', de valeurs respectives $\phi(a') = a$ et $\psi_i(a') = b_i$. Notons $\overline{\phi}$ l'application rationnelle $U' \times V \to U \times V$, définie sur K, qui, au point (u',x), fait correspondre $(u,x) = (\phi(u'), x)$. Posons $Z' = \overline{\phi}^{-1}(Z)$. Alors, d'après le lemme 5, le symbole $Z(a)$ est defini, et on a les relations

$$Z(u) = Z'(u') \qquad Z(a) = Z'(a').$$

On a donc ramené le problème au cas déjà traité, C.Q.F.D.

THEOREME 3.

Soit V une courbe définie sur un corps k. Soit $\underline{a}$ un diviseur sur V, et soit $\underline{a}'$ une spécialisation de $\underline{a}$ sur k. Si on a $\underline{a} \sim 0$, on a aussi $\underline{a}' \sim 0$.

Démonstration. Posons $\underline{a} = \sum_{i=1}^{r} n_i a_i$, et $\underline{a}' = \sum_{i=1}^{r} n_i a_i'$ de façon que $(a_1', \ldots, a_r')$ soit une spécialisation de $(a_1, \ldots, a_r)$ sur k. D'après le lemme 9, il existe un corps K contenant k, une courbe complète U sans point multiple, définie sur K, un point $u' \in U$ et des applications rationnelles $\phi_i : U \to V$, définies sur K, tels que, pour u générique de U sur K, et en posant $\phi_i(u) = a_i^*$, le point $(a_1^*, \ldots a_r^*)$ soit une spécialisation générique de $(a_1, \ldots, a_r)$ sur k, et tels de plus que ϕ_i soit morphique en u' pour tout i, et de valeur $\phi_i(u') = a_i'$. Puisqu'on a $\underline{a} \sim 0$,

.../...

$\underline{a}$ est le diviseur d'une fonction f sur V, qu'on peut prendre définie sur $k(a)$ (E, IV, 6, th. 11, corell.). Il existe un k-isomorphisme σ du corps $k(a)$ sur le corps $k(a^*) = k(a_1^*, \ldots, a_r^*)$, tel que $\sigma(a_i) = a_i^*$ pour tout i. Cet isomorphisme se prolonge canoniquement à un isomorphisme $\overline{\sigma}$ du corps de fonctions $\mathcal{F}_{k(a)}(V)$ sur le corps $\mathcal{F}_{k(a^*)}(V)$, et de telle façon que $f^* = \overline{\sigma}(f)$ ait pour diviseur $\underline{a}^* = \sum_i m_i a_i^*$. Considérons la fonction h sur $U \times V$, définie sur K, telle que $h(u,x) = f(x)$. On a $\mathrm{div}(h).(u \times V) = u \times \mathrm{div}(f^*) = u \times \underline{a}^*$. Notons m le coefficient de $u' \times V$ dans le diviseur $\mathrm{div}(h)$. Soit t un paramètre uniformisant de U en u', défini sur K ; on peut aussi regarder t comme un paramètre uniformisant de $U \times V$ en $u' \times V$ (cf. E, III, 5). La fonction $h' = ht^{-m}$ est alors telle que $u' \times V \notin \mathrm{supp}(\mathrm{div}(h'))$, donc (critère de morphicité) telle que h' soit génériquement inversible sur $u' \times V$. Soit alors f' la fonction sur V, définie sur $K(u')$, telle que $f'(x) = h'(u',x)$. Nous allons montrer qu'on a $\mathrm{div}(f') = \underline{a}'$. En effet, pour tout i, notons X_i le graphe de ϕ_i. On a $u \times a_i^* = X_i.(u \times V)$, et $u \times a_i' = X_i.(u' \times V)$ $(1 \leq i \leq r)$. Si l'on pose $X = \sum_i m_i X_i$, la première de ces relations entraîne $(\mathrm{div}(h') - X).(u \times V) = 0$. Donc toutes les composantes de $\mathrm{div}(h') - X$ sont verticales. Aucune d'elles ne coïncide avec $u' \times V$, donc aucune d'elles ne rencontre $u' \times V$. Donc on a $\mathrm{div}(h').(u' \times V) = X.(u' \times V) = u' \times \underline{a}'$, ce qui entraîne bien $\mathrm{div}(f') = \underline{a}'$, d'où $\underline{a}' \sim 0$, C.Q.F.D.

5. Le théorème des fonctions symétriques.

LEMME 11. Soient V et W deux courbes sans point multiple, et soit $\phi : W \to V$ une application rationnelle de

.../...

degré fini (non nécessairement séparable); soient respectivement n_o et p^μ les degrés séparable et inséparable de ϕ (cf. ch. I, n° 8). Alors, pour x générique de V sur k, l'ensemble $(\phi^{-1})_e(x)$ se compose de n_o points distincts $y_1, \ldots, y_{n_o}$, et le diviseur $\phi^{-1}(x)$ est égal à $p^\mu \sum_{i=1}^{n_o} y_i$.

Démonstration. Soit y l'un des composants de l'ensemble $(\phi^{-1})_e(x)$. Ce point est générique de W sur k, et $(\phi^{-1})_e(x)$ coïncide avec l'ensemble des conjugués de y sur $k(x)$; le nombre de ces conjugués est n_o. Notons F le morphisme de Frobenius $W \to W^p$ (induit par l'automorphisme de Frobenius $x \to x^p$ de Ω), et considérons son μ-ième itéré $F^\mu : W \to W^{p^\mu}$. Le point $z = F^\mu(y)$ est algébrique séparable sur $k(x)$; il admet pour conjugués les points distincts $z_i = F^\mu(y_i)$, donc z est algébrique séparable de degré n_o sur $k(x)$. L'extension purement inséparable $k(y)/k(x,z)$ est donc de degré p^μ. Soit h une fonction sur W, non constante, et constituant une base de transcendance séparante de l'extension $F_k(W)/k$. Posons $t = h(y)$, et $u = t^{p^\mu}$. Les extensions $k(y)/k(t)$ et $k(z)/k(u)$ étant séparables, on a $[k(y) : k(z)]_i = [k(t) : k(u)]_i$. Comme t est transcendant sur k, le second membre est égal à p^μ. On a donc $[k(y) : k(z)]_i = p^\mu$. Il en résulte $k(x,z) = k(z)$, i.e. x est rationnel sur $k(z)$. On peut donc factoriser $\phi : W \to V$ sous la forme

$$W \xrightarrow{F^\mu} W^{p^\mu} \xrightarrow{\psi} V$$

où ψ est l'application rationnelle $W \to V$ définie sur k, telle que $\psi(z) = x$. On a $\phi^{-1}(x) = (F^\mu)^{-1}(\psi^{-1}(x))$. Or $\psi^{-1}(x) = \sum_{i=1}^{n_o} z_i$. D'autre part $g = h^{p^\mu} - h^{p^\mu}(z)$ est un paramètre

.../...

uniformisant de W en z. Donc le diviseur $(F^\mu)^{-1}(z)$ est représenté en y par $g' \circ F^\mu = (h - h(y))^{p^\mu}$. Or g' est un paramètre uniformisant de W en y. Donc le coefficient de y dans $\phi^{-1}(x)$ est p^μ C.Q.F.D.

THEOREME 4. (théorème des fonctions symétriques).

Soit V une courbe sans point multiple, définie sur un corps k. Soit $\underline{a} = \sum_{i=1}^{m} a_i$ un diviseur positif sur V, de degré m, rationnel sur k. Pour toute fonction symétrique F à m variables sur V, définie sur k, on a $F(a_1,..,a_m) \in k$.

Démonstration. On remarque d'abord que si le théorème est vérifié pour deux diviseurs positifs $\underline{b}$ et $\underline{c}$ sur V, rationnels sur k, il l'est aussi pour leur somme $\underline{a} = \underline{b} + \underline{c}$ (car si $\underline{b} = b_1 +... b_r$, et $\underline{c} = c_1 +...+ c_s$, la fonction $F(b_1,..., b_r, z_1,..., z_s)$ est symétrique en $z_1,..z_s$ donc prend une valeur raticnnelle en $(c_1,..., c_s)$). D'autre part si $\underline{a}$ est un diviseur sur V, rationnel sur k, on peut le représenter par un couple (U,f), composé d'un k-ouvert U de V, et d'une fonction $f \in \mathcal{K}_k(V)$, tel que U contienne l'un au moins des composants de $\underline{a}$. La restriction $\underline{a}'$ de $\underline{a}$ à l'ouvert U est alors le diviseur de la fonction $f|U$, et comme $\underline{a}' \neq 0$, on a $\underline{a} = \underline{a}' + \underline{b}$, où $\underline{b}$ est un diviseur positif sur V, tel que $\deg \underline{b} < \deg \underline{a}$. Compte tenu de la remarque précedente, on se ramène, par récurrence sur le degré, au cas où V est une courbe affine ($V \subset \mathbb{S}_n$), et où $\underline{a}$ est le diviseur d'une fonction f sur V. Comme $\underline{a}$ est positif f est morphique sur V (critère de morphicité, E, IV, 5, th.8) Il suffit d'autre part de considérer le cas où F est induite par un polynôme sur $\mathbb{S}_{mn} = \mathbb{S}_n \times...\times \mathbb{S}_n$, qu'on désignera par

.../...

$P = P(X_1, \ldots, X_m)$ ou, plus explicitement, par $P(X_{11}, \ldots, X_{1n}, \ldots, X_{m1}, \ldots, X_{mn})$. Soit x un point générique de V sur k, et posons $u = f(x)$. On peut supposer que f n'est pas constante (sinon $\underline{a} = 0$). On a alors $\underline{a} = f^{-1}(0)$; de plus, d'après le lemme 9 du n° 4, si on pose $\underline{v} = f^{-1}(u)$, le diviseur $\underline{a}$ est l'unique spécialisation de $\underline{v}$ compatible avec $u \to 0$ sur k. Puisqu'on a $\deg \underline{a} = m$, on a aussi $\deg \underline{v} = m$. Donc f, regardée comme une application rationnelle $V \to \mathbb{P}_1$, est de degré m. Explicitons $\underline{v}$ sous la forme $\underline{v} = \sum_{i=1}^{m} v_i$ $(v_i \in V)$, et considérons le point $z = F(v_1, \ldots, v_m)$. Ce point z est algébrique sur $k(u)$, et invariant par tout $k(u)$-automorphisme de $\overline{k(u)}$; il est donc purement inséparable sur $k(u)$. Nous allons montrer qu'en fait z est rationnel sur $k(u)$. Le résultat est immédiat si f est séparable : en effet dans ce cas, les v_i sont séparables sur $k(u)$; donc z est séparable et, par suite, rationnel, sur $k(u)$. Il suffit donc d'examiner le cas où f est inséparable. Pour $1 \leq j \leq n$, notons v_{ij} les coordonnées de v_i. On a

$$z = P(v_1, \ldots, v_m) = P(v_{11}, \ldots, v_{1n}, \ldots, v_{m1}, \ldots, v_{mn}),$$

d'où

$$(5) \qquad dz = \sum_{i,j} \frac{\partial P}{\partial X_{i,j}} (v_1, \ldots, v_m)\, d\, v_{ij}$$

où d représente la différentielle relative à l'extension $k(v_1, \ldots, v_m)/k(u)$. Soit d'autre part σ l'une quelconque des permutations des entiers $1, 2, \ldots, m$. Puisque P induit une fonction symétrique sur V, on a

$$P(v_1, \ldots, v_m) = P(v_{\sigma(1)}, \ldots, v_{\sigma(m)}).$$

.../...

On en déduit, pour tout couple (i,j)

(6) $$\frac{\partial P}{\partial X_{\sigma(i),j}}(v_1,\ldots, v_m) = \frac{\partial P}{\partial X_{ij}}(v_{\sigma(1)},\ldots, v_{\sigma(m)}).$$

Soit Γ le groupe des permutations de $(1, 2,\ldots, m)$ telles que $v_{\sigma(i)} = v_i$ pour tout i. D'après (6), pour $\sigma \in \Gamma$, les dérivées partielles de P d'indices respectifs $(\sigma(i), j)$ et (i,j) prennent la même valeur en $(v_1,\ldots, v_m)$. Les termes correspondants du second membre de (5) sont donc égaux ; chaque terme figure donc un nombre q de fois égal à l'ordre de Γ. Or si p^μ est le degré inséparable de f (> 1, par hypothèse), chacun des composants de $\underline{v}$ figure p^μ fois dans la liste $v_1,\ldots, v_m$, en vertu du lemme 10. On en déduit que q est une puissance de $(p^\mu)!$. En particulier q est multiple de p. Il s'ensuit que $dz = 0$. Donc (E, III, 1, th. 2), z est séparable sur $k(u)$; donc z est rationnel sur $k(u)$.

On peut poser $z = g(u)$, avec $g \in \mathfrak{F}_k(V)$. D'après ce qui précède, $F(a_1,\ldots, a_m) = P(a_1,\ldots, a_m)$ est l'unique spécialisation de $z = g(u) = P(v_1,\ldots, v_m)$ compatible avec $u \to 0$ sur k. Donc g est morphique en 0, et on a $F(a_1,\ldots, a_n) = g(0)$ d'où $F(a_1,\ldots, a_m) \in k$, C.Q.F.D.

6. Propriétés de la Jacobienne.

Commençons par montrer que la jacobienne J d'une courbe V (complète sans point multiple) est une variété abélienne. Comme dans la construction de J (n° 2), introduisons un diviseur $\underline{a}$ quelconque de degré g sur V, et considérons l'application rationnelle $\eta : V^g \to J$ correspondante. Soit k un corps de définition quelconque pour V, $\underline{a}$, J et η.

.../...

Soit x un point generique de V sur k. Il nous suffit de prouver que toute place ρ_o de $k(x)$, à valeurs dans $\bar{k}$, est finie en x. Introduisons un point y générique de V sur k, indépendant de x. On peut prolonger ρ_o à une place ρ de $k(x,y)$ laissant invariant y. D'après les résultats du n° 2, l'ensemble $\eta_e^{-1}(x)$ (resp. $\eta_e^{-1}(y)$) est composé de g point génériques indépendants $u_1,\ldots, u_g$ (resp. $v_1,\ldots, v_g$) de V sur k, respectivement tels que $k(u_1,\ldots, u_g)_s = k(x)$, et $k(v_1,\ldots, v_g)_s = k(y)$; il existe de plus un et un seul diviseur $\underline{w}$ sur V, positif, de degré g, tel qu'on ait $\underline{w} \sim \underline{u} + \underline{v} - \underline{a}$, et dont les composants $w_1,\ldots, w_g$ sont encore g points génériques indépendants de V sur k ; le point $z = \eta(w_1,\ldots, w_g)$ coïncide avec le composé de x et y pour la loi de groupe de J. Puisque y est invariant par ρ, on a $\rho(\underline{v}) = \underline{v}$. Posons $\rho(\underline{u}) = \underline{u}'$ et $\rho(\underline{w}) = \underline{w}'$. Puisqu'on a $\underline{w} \sim \underline{u} + \underline{v} - \underline{a}$, on a aussi, d'après le th. 2, $\underline{w}' \sim \underline{u}' + \underline{v} - \underline{a}$. Or $\underline{u}' - \underline{a}$ est rationnel sur $\bar{k}$. Puisque les composants de $\underline{v}$ sont génériques indépendants de V sur $\bar{k}$, il en est de même de ceux $w_1',\ldots, w_g'$ de $\underline{w}'$. Donc η est morphique en $w_1',\ldots, w_g'$, et, si on pose $z' = \eta(w_1',\ldots, w_g')$, la place ρ est finie en z, de valeur z'. Notons ψ l'application rationnelle $J \times J \to J$, définie sur k, telle que $x = \psi(y,z)$. Puisque J est une variété de groupe, ψ est un morphisme. Puisque ρ est finie en y et z, ρ est finie en x, de valeur $x' = \psi(x,z')$ On a donc bien montré que J est complète, donc que J est une variété abélienne.

.../...

De plus, d'après le th. 6 du n° 5 du chap. I, l'application rationnelle $\eta : V^g \to J$ est un morphisme. D'après le th. 8 du n° 6 du chap. I, il existe des morphismes $\phi_1, \ldots, \phi_g : V \to J$ tels qu'on ait $\eta(u_1, \ldots, u_g) = \phi_1(u_1) + \ldots + \phi_g(u_g)$ quels que soient $u_1, \ldots, u_g \in V$. Ces morphismes ϕ_i sont égaux à des translations près. En effet, pour u, $a \in V$, on a $\phi_i(u) - \phi_i(a) = \eta(a, \ldots, a, u, a, \ldots, a) - \eta(a, \ldots, a)$ où le premier terme du second membre est obtenu en remplaçant u_i par u et u_j par a pour $j \neq i$. Comme η est symétrique, $\phi_i(u) - \phi_i(a)$ ne dépend pas de l'indice i. En d'autres termes, on a montré qu'il existe un morphisme $\phi : V \to J$, uniquement déterminé à une translation près sur J, tel qu'on ait $\eta(u_1, \ldots, u_g) = \phi(u_1) + \ldots + \phi(u_g) + c$, où c est un point de J.

En récapitulant les résultats qui précèdent, on obtient l'énoncé suivant

THEOREME 5.

Soit V une courbe complète de genre g, sans point multiple. Il existe une variété abélienne J de dimension g et un morphisme $\phi : V \to J$ tel que, si k est un corps de définition de V, J et ϕ, et si $u_1, \ldots, u_g$ sont des points génériques indépendants de V sur k, on ait, en posant $x = \sum_i \phi(u_i)$, la relation $k(u_1, \ldots, u_g)_s = k(x)$.

On a vu que toute application birationnelle $A \to B$, où A et B sont des variétés abéliennes, est un isomorphisme (pour la structure de variété algébrique) ou encore est le composé d'un isomorphisme (pour la structure de variété abélienne) et d'une translation. Il en résulte que le couple (J, ϕ)

.../...

est unique, à un isomorphisme et une translation près, et que le théorème ci-dessus fournit une caractérisation de la jacobienne.

Remarque 5. Pour V donnée, définie sur k, on peut montrer qu'on peut choisir J définie sur k. Mais on ne peut choisir J et Φ définies sur k que si V possède un diviseur de degré g rationnel sur k ; en particulier, il en est ainsi lorsque V possède un point rationnel sur k.

Remarque 5 bis. Si V est une courbe quelconque, il existe, comme on a vu, une application birationnelle $\alpha : V \to W$, où W est une courbe complète sans point multiple. Soit J la jacobienne de W ; soit Φ un morphisme canonique $W \to J$, et considérons l'application rationnelle

$$\psi = \alpha \circ \Phi : V \to J .$$

Alors le couple (J,ψ) est encore uniquement déterminé, à un isomorphisme près, par la donnée de V. On dit que J est la jacobienne de V, et que ψ est une application rationnelle canonique de V dans J.

7. Caractérisation de la jacobienne par une propriété d'application universelle.

THEOREME 6.

Soit V une courbe complète sans point multiple. Le couple (J,Φ) est caractérisé, à un isomorphisme près (pour la structure de variété algébrique), par la propriété suivante : si $\psi : V \to \mathbf{A}$ est une application rationnelle (donc un morphisme) de V dans une variété abélienne $\mathbf{A}$, il existe un et un seul morphisme $\alpha : J \to \mathbf{A}$ tel que le diagramme

$$\begin{array}{ccc} V & \xrightarrow{\Phi} & J \\ & {\scriptstyle\psi}\searrow \quad \swarrow{\scriptstyle\alpha} & \\ & \mathbf{A} & \end{array}$$

soit commutatif.

Démonstration. L'unicité de (J,Φ) à un isomorphisme près résulte trivialement de l'énoncé. Soit g le genre de V. Montrons maintenant que le couple (J,Φ) construit plus haut, vérifie la condition de l'énoncé. Soit k un corps de définition de V, J, $\mathbf{A}$, Φ, ψ, et soient $u_1, \ldots, u_g$ des points génériques indépendants de V sur k. Considérons les points $x = \Sigma_i \Phi(u_i) \in J$ et $y = \Sigma_i \psi(u_i) \in \mathbf{A}$, et les morphismes

.../...

$\mu : V^g \longrightarrow J$ et $\nu : V^g \longrightarrow A$ définis sur k, respectivement tels que $\mu(u_1, \ldots, u_g) = x$, et $\nu(u_1, \ldots, u_g) = y$. Le point y est invariant par toute permutation des u_i, donc est rationnel sur le corps $k(u_1, \ldots, u_g)_s = k(x)$, et il existe donc une application rationnelle $\alpha_o : A \to J$, qui est nécessairement un morphisme (I, 5, th. 6), telle que le diagramme

$$\begin{array}{ccc} V^g & \xrightarrow{\mu} & J \\ & {\scriptstyle\nu}\searrow \quad \swarrow{\scriptstyle\alpha_o} & \\ & A & \end{array}$$

soit commutatif. Considérons $a \in A$ fixe, et $u \in A$ variable. En comparant les images du point $(u, a, \ldots, a) \in V^g$ par ν et par $\alpha_o \circ \mu$, on trouve une relation de la forme

$$\alpha_o(\phi(u)) = \psi(u) + c$$

où c est un point fixe de A. On a donc $\psi = \alpha \circ \phi$, où α est le morphisme $J \to A$ défini par $\alpha(x) = \alpha_o(x) - c$.

Remarque 6. Le genre g de la courbe n'intervient pas dans l'énoncé précédent. La relation $g = \dim J$ peut donc être regardée comme une nouvelle définition du genre g.

8. Symbole $S(\underline{a})$. Caractérisation des diviseurs linéairement équivalents à zéro sur une courbe.

Soit V une courbe complète sans point multiple et soit $\phi : V \to J$ un morphisme canonique de V dans sa jacobienne. Si $\underline{a} = \sum_i m_i a_i$ est un diviseur sur V, le point $\sum_i m_i \phi(a_i)$ est noté $S(\underline{a})$, ou $S_\phi(\underline{a})$.

THEOREME 7.

Soit $\underline{a}$ un diviseur de degré 0 sur V. On a $\underline{a} \sim 0$ si et seulement si $S(\underline{a}) = 0$.

.../...

(En d'autres termes, si $\mathfrak{D}_0$ est le groupe des diviseurs de degré 0 sur V, le noyau de l'homomorphisme $\mathfrak{D}_0 \to J$ induit par S, coïncide avec le groupe $\mathfrak{D}_\ell$ des diviseurs linéairement équivalents à 0 sur V).

Démonstration. Supposons d'abord $\underline{a} \sim 0$. Soit k un corps de définition pour V, J, ϕ et $\underline{a}$. Il existe une fonction f sur V, définie sur k, telle que $\mathrm{div}(f) = \underline{a}$. Considérons le morphisme $f^* : V \to \mathbb{P}_1$ déduit de f. On sait que f^* est un revêtement de la droite projective $\mathbb{P}_1$, et on a $\mathrm{div}(f) = (f^*)^{-1}(0) - (f^*)^{-1}(\infty)$. Notons u un point générique de $\mathbb{P}_1$ sur k, et posons $\underline{u} = (f^*)^{-1}(u) = (f)^{-1}(u)$. D'après le théorème des fonctions symétriques, le point $w = S(\underline{u})$ de J est rationnel sur k(u). Il existe donc une application rationnelle $\theta : \mathbb{P}_1 \to J$, définie sur k, telle que $w = \theta(u)$. D'après I, 6, th. 8, coroll. 2, θ est nécessairement constante, et w est un point rationnel sur k. D'après le lemme 10, l'unique spécialisation de $\underline{u} = f^{-1}(u)$ compatible avec $u \to 0$ (resp. $u \to \infty$) sur k est $\underline{u}_0 = (f^*)^{-1}(0)$ (resp. $\underline{u}_\infty = (f^*)^{-1}(\infty)$). L'unique spécialisation correspondante de $S(\underline{u})$ est $S(u_0)$ (resp. $S(\underline{u}_\infty)$). On a $S(\underline{u}) = S(\underline{u}_0) = S(\underline{u}_\infty) = w$, d'où $S(\underline{a}) = S(\underline{u}_0) - S(\underline{u}_\infty) = 0$.

Réciproquement soit $\underline{a}$ un diviseur sur V, de degré 0, rationnel sur k, tel que $S(\underline{a}) = 0$. Soient $u_1, \ldots, u_g$ des points génériques indépendants de V sur k, et posons $\underline{u} = u_1 + \ldots + u_g$. D'après le théorème 2, il existe un et un seul diviseur $\underline{v}$ positif de degré g sur V tel que $\underline{v} \sim \underline{u} + \underline{a}$. Puisqu'on a $S(\underline{a}) = 0$, on a $S(\underline{u}) = S(\underline{v})$. D'après le th. 5, ceci entraîne $\underline{u} = \underline{v}$ d'où $\underline{a} \sim 0$.

CHAPITRE IV

DIVISEURS SUR LES VARIETES ABELIENNES.

1. Le théorème du carré.

THEOREME 1.

Soient U, V, W trois variétés définies sur un corps k, et soit T un diviseur sur $U \times V \times W$, rationnel sur k. Considérons quatre points $u_o \in U$, $u \in U$, $v_o \in V$, $v \in V$ génériques indépendants sur k. Alors le diviseur

$$(1) \quad D = T(u,v) - T(u_o,v) - T(u,v_o) + T(u_o,v_o)$$

sur W est linéairement équivalent à zéro.

Nous allons d'abord donner à cet énoncé une autre forme, dans laquelle U, V, W jouent des rôles symétriques. Les projections de $U \times V \times W$ sur $V \times W$, $U \times W$, et $U \times V$ sont respectivement notées α, β, γ.

THEOREME 1 bis.

Soient U, V, W, T comme dans le th. 1. Alors il existe des diviseurs X, Y, Z sur $V \times W$, $U \times W$ et $U \times V$ respectivement tels qu'on ait

$$(2) \quad T \sim \alpha^{-1}(X) + \beta^{-1}(Y) + \gamma^{-1}(Z).$$

Commençons par pouver l'équivalence des théorèmes 1 et 1 bis.

Soient d'abord U, V, W, T vérifiant les conditions du th. 1. Posons $K = k(u_o, u, v_o, v)$, et soit w un point générique de W sur k. Il existe une fonction f sur W, définie sur K, telle que $\mathrm{div}(f) = D$. Considérons la fonction h sur $U \times V \times W$, définie sur $K_o = k(u_o, v_o)$, telle que $h(u,v,w) = f(w)$. On a $\mathrm{div}(f) = E(u,v)$, en posant $E = \mathrm{div}(h)$ d'où

$$E(u,v) = T(u,v) - T(u_o,v) - T(u,v_o) + T(u_o,v_o)$$

.../...

D'après le lemme 5 du n° 3 du ch. III, appliqué au changement de paramètre défini par le morphisme $i_{u_o} : V \to U \times V$ tel que $i_{u_o}(x) = (u_o, x)$, on

$$T(u_o, v) = X_o(v)$$

où X_o est le diviseur sur $V \times W$ défini par $X_o = \alpha(T.(u_o \times V \times W))$. On a de même

$$T(u, v_o) = Y_o(u)$$

où Y_o est le diviseur sur $U \times W$ défini par $Y_o = \beta(T.(U \times v_o \times W))$.

Toujours d'après le lemme 5 du ch. III, appliqué au changement de paramètre défini par la projection $U \times V \to V$, on a

$$X_o(v) = \overline{X}_o(u, v),$$

en posant $\overline{X}_o = \alpha^{-1}(X_o)$, et de même

$$Y_o(u) = \overline{Y}_o(u, v),$$

en posant $\overline{Y}_o = \beta^{-1}(Y_o)$. Si d'autre part on pose $T_o = T(u_o, v_o)$ et $D_o = U \times V \times T_o = \alpha^{-1}(V \times T_o) = \beta^{-1}(U \times T_o)$, on a $T_o = D_o(u, v)$. Donc, si on prend (par exemple) $X = X_o$ et $Y = Y_o - U \times T_o$, on obtient

$$D(u, v) = T(u, v) - \overline{X}(u, v) - \overline{Y}(u, v),$$

avec $\overline{X} = \overline{X}_o = \alpha^{-1}(X)$, et $\overline{Y} = \overline{Y}_o - D_o = \beta^{-1}(Y)$.

Donc (III, 3, lemme 6), $T - E - \overline{X} - \overline{Y}$ est un diviseur vertical du produit $(U \times V) \times W$, i.e. est de la forme $\overline{Z} = \gamma^{-1}(Z)$, où Z est un diviseur sur $U \times V$. On a donc

$$T = E + \alpha^{-1}(X) + \beta^{-1}(Y) + \gamma^{-1}(Z),$$

ce qui donne bien le th. 1 bis, puisque $E \sim 0$.

Réciproquement, soient U, V, W, T, X, Y, Z vérifiant la relation (2) du th. 1 bis.

Il suffit de montrer que la relation $D \sim 0$ du th. 1

.../...

a lieu lorsque u_o, u, v_o, v sont des points génériques indépendants sur un corps de définition k' de U, V, W, T, X, Y, Z. Posons $\overline{X} = \alpha^{-1}(X)$, $\overline{Y} = \beta^{-1}(Y)$ et $\overline{Z} = \gamma^{-1}(Z)$. D'après III, 3, lemme 5, on a

$\overline{X}(u,v) = X(u)$, et $\overline{Y}(u,v) = Y(v)$; d'après III, 3, lemme 6, on a $\overline{Z}(u,v) = 0$. On en déduit

$$T(u,v) \sim X(u) + Y(v).$$

En combinant cette relation avec les relations analogues, respectivement obtenues en remplaçant le couple (u,v) par (u_o,v), (u,v_o) et (u_o,v_o) on trouve bien $D \sim 0$.

Démonstration des théorèmes 1 et 1 bis.

1º Cas où W est une courbe : On peut supposer W complète et sans point multiple. Soit J la jacobienne de W . Le point $S(X(u,v))$ est rationnel sur $k(u,v)$, et il existe donc une application rationnelle $\lambda : U \times V \to J$, définie sur k , telle que

$$\lambda(u,v) = S(T(u,v)).$$

D'après les th. 6 et 8 du chap. I, λ est de la forme

$$\lambda(u,v) = \mu(u) + \nu(v)$$

où μ et ν sont respectivement des morphismes $U \to J$ et $V \to J$. En combinant cette relation avec celles respectivement obtenues en remplaçant (u,v) par (u_o,v) (u,v_o) et (u_o,v_o). On obtient $D \sim 0$.

2º Cas général : Le fait que U, V, W jouent des rôles symétriques dans le th. 1 bis entraîne que les th. 1 et 1 bis sont vrais lorsque U est une courbe, V et W étant quelconques. Pour passer de là au cas général, considérons un point générique u_o de U sur k ; d'après le lemme 8 du n° 4

.../...

du ch. III, on peut trouver un corps $K \supset k(u_o)$, une courbe U' sur U contenant u_o, définie sur K, telle que tout point générique u de U' sur K soit aussi un point générique u de U' sur K soit aussi un point générique de U sur $k(u_o)$. Le lemme 5 de III, 3 appliqué au changement de paramètre défini par l'injection $U' \to U$, permet de remplacer U par U', et on est ramené au cas 1°.

THEOREME 2. (analogue au th. 1, mais avec des points non nécessairement génériques).

Soient U, V, W, T comme dans le th. 1. Soient a_o, a_1 deux points simples de U, et b_o, b_1 deux points simples de V tels que $T(a_i,b_j)$ soit défini quels que soient i et j. Alors on a

$$(3)\quad \sum_{i,j} (-1)^{i+j}\, T(a_i b_j) \sim 0 .$$

Démonstration. Reprenons les notations de la démonstration précédente, en supposant de plus que les points u_o, u, v_o, v sont génériques indépendants sur le corps $k(a_o,b_o)$. En modifiant Z par l'addition du diviseur d'une fonction convenable sur $U \times V$, on peut supposer $(a_o,b_o) \notin \operatorname{supp} T$. Puisque le symbole $T(a_o,b_o)$ est défini, il en est de même a fortiori de $T(u_o,b_o)$. Donc d'après III, 3, lemme 5, les symboles $X_o(b_o)$, $\overline{X}_o(a_o,b_o)$ sont définis, et on a

$$T(u_o,b_o) = X_o(b_o) = \overline{X}_o(a_o,b_o)$$

On a de même

$$T(a_o,u_o) = Y_o(a_o) = \overline{Y}_o(a_o,b_o)$$

D'autre part,

$$T(u_o,v_o) = T_o = D_o(a_o,b_o)$$

.../...

On en déduit que $E(a_o,b_o)$ est défini, et que

$$E(a_o,b_o) = T(a_o,b_o) - T(u_o,b_o) - T(a_o,v_o) + T(u_o,v_o)$$

Puisqu'on a $E \sim 0$, on a aussi $E(a_o,b_o) \sim 0$, d'où

$$T(a_o,b_o) - T(u_o,b_o) - T(a_o,v_o) + T(u_o,v_o) \sim 0$$

La relation (3) s'obtient en combinant cette relation avec celles respectivement obtenues en remplaçant (a_o,b_o) par (a_o,b_1), (a_1,b_o) et (a_1,b_1).

2. Application du théorème du carré aux variétés de groupe.

THEOREME 3.

Soit G une variété de groupe (non nécessairement commutative). Soient V une variété arbitraire, X un diviseur sur le produit $G \times V$. Pour $a, a', b, b' \in G$, tels que $a'a^{-1} = b'b^{-1}$ et tels que les symboles $X(a')$, $X(a)$, $X(b')$, $X(b)$, soient définis, on a

(4) $X(a') - X(a) - X(b') + X(b) \sim 0$.

Démonstration. Soit k un corps de définition de G, V, X, et soient u, v deux points génériques indépendants de G sur k. Notons ψ le morphisme $G \times G \to G$ défini par $\psi(u,v) = uv^{-1}$. D'après III, 3, lemme 5, on a $X(uv^{-1}) = Z(u,v)$, en posant $Z = \overline{\psi}^{-1}(X)$, où $\overline{\psi}$ est le morphisme $G \times G \times V \to G \times V$ défini par $\overline{\psi}(u,v,x) = (uv^{-1},x)$.

On peut trouver des points u_o, u_1, v_o, v_1 de G tels que

$$u_o\, v_o^{-1} = a$$
$$u_1\, v_o^{-1} = a'$$
$$u_o\, v_1^{-1} = b$$
$$u_1\, v_1^{-1} = b'$$

.../...

Posant en effet $a' a^{-1} = b' b^{-1} = c$, il suffit de prendre $u_o = 1$, $v_o = a^{-1}$, $u_1 = b^{-1}$ et $v_1 = c$. Toujours d'après III, 3, lemme 5, on en déduit

$$Z(u_i, v_j) = X(u_i v_j^{-1})$$

quels que soient i et j. Pour obtenir (4), il suffit alors d'appliquer le théorème du carré C.Q.F.D.

Soit G une variété de groupe commutative, et soit E (resp. X) un sous-ensemble de G (resp. un diviseur sur G). Pour $a \in G$, on notera E_a (resp. X_a) le transformé de E (resp. X) par la translation τ_a. On notera E^- (resp. X^-) le transformé de E (resp. X) par la symétrie $x \to -x$.

Corollaire 1. Soit G une variété de groupe commutative, et soit X un diviseur sur G. Alors, quels que soient a, $b \in G$, on a

(5) $X_{a+b} - X_a - X_b + X \sim 0$.

En effet, considérons le morphisme $\psi : G \times G \to G$ défini par $\psi(u,v) = v - u$ et l'immersion $G \to G \times G$ définie par $i_a(x) = (a,x)$. On a $\tau_a^{-1} = i_a \circ \psi$, d'où $X_a = \tau_a(X) = i_a^{-1}(\psi^{-1}(X))$, i.e. $X_a = Y(a)$, en posant $Y = \psi^{-1}(X)$, et il suffit d'appliquer le th. 3.

Corollaire 2. Soit G une variété de groupe commutative et soit X un diviseur sur G. Soient a_i $(1 \leq i \leq r)$ des points de G, et n_i $(1 \leq i \leq r)$ des entiers, tels que $\sum_i n_i = 0$ et $\sum_i n_i a_i = 0$. Alors on a

(6) $\sum_i n_i X_{a_i} \sim 0$.

En effet, un raisonnement élémentaire montre que le premier membre de (5) est la somme d'un nombre fini de la somme $X_{a+b} - X_a - X_b + X$, et on est ramené au coroll. 1.

.../...

3. Systèmes linéaires.

Soit V une variété complète, et soit D un diviseur sur V. Rappelons que l'espace vectoriel $L(D)$ est de dimension finie (E, IV, 6, th. 12). Par définition, $L(D)$ se compose des fonctions f sur V telles que $\mathrm{div}(f)$ soit de la forme $E - D$ où E est un diviseur positif sur V. L'ensemble $\mathfrak{L}$ des diviseurs E obtenus lorsqu'on fait parcourir à f un sous-espace vectoriel L de $L(D)$ est appelé un système linéaire sur V et, plus précisément le système linéaire sur V associé à L. Pour tout diviseur $D' \sim D$, le système linéaire $\mathfrak{L}$ est également associé à un sous-espace L' de $L(D')$: en effet, il existe une fonction g sur V telle que $\mathrm{div}(g) = D-D'$, et il suffit de prendre pour L' l'espace vectoriel composé des fonctions de la forme fg, avec $f \in L$. Le nombre $\dim L' - 1$ ne dépend que du système linéaire $\mathfrak{L}$. On l'appelle la dimension de $\mathfrak{L}$. L'ensemble de tous les diviseurs positifs sur V qui sont linéairement équivalents à D n'est autre que le système linéaire associé à $L(D)$. On le note $\mathfrak{L}(D)$. Tout système linéaire de ce type est dit complet.

$\mathfrak{L}$ étant le système linéaire associé au sous-espace L de $L(D)$, posons $n = \dim \mathfrak{L}$ et soit $f_0, \ldots, f_n$ une base de L. Tout corps k de définition de V, D, $f_0, \ldots, f_n$ est appelé un corps de définition de $\mathfrak{L}$. En particulier, tout corps k de définition de V et D est aussi un corps de définition de $\mathfrak{L}(D)$, comme il résulte de E, IV, 6, th. 11. Soit x un point générique de V sur k, et considérons le point y de l'espace projectif $\mathbb{P}_n$ ayant pour coordonnées homogènes

.../...

$y_0 = f_0(x), \ldots, y_n = f_n(x)$. L'application rationnelle $\phi : V \to \mathbb{P}_n$, définie sur k , telle que $y = \phi(x)$ est dite <u>associée à $\mathfrak{L}$</u> (ou à L). La donnée de $\mathfrak{L}$ détermine ϕ à un isomorphisme près (défini par un changement linéaire de coordonnées) de l'espace $\mathbb{P}_n$.

Inversement, soit $\phi : V \to \mathbb{P}_n$ une application rationnelle. Supposons, pour fixer les idées, que l'image $W = \phi_g(V)$ n'est pas contenue dans l'hyperplan H_0 de $\mathbb{P}_n$ défini par l'équation $X_0 = 0$. Le symbole $\phi^{-1}(H_0)$ est alors défini. Posons $D = \phi^{-1}(H_0)$. Pour toute forme linéaire homogène $F(X) = F(X_0, \ldots, X_n)$, la fonction $F(X)/X_0$ sur $\mathbb{P}_n$ se relève à une fonction f sur V . L'ensemble de ces fonctions f est un sous-espace vectoriel L de $L(D)$, de dimension $n+1$, et l'application rationnelle ϕ est associée au système linéaire $\mathfrak{L}$ correspondant. De plus, $\mathfrak{L}$ coïncide avec l'ensemble des diviseurs sur V de la forme $\phi^{-1}(H)$, où H est un hyperplan de $\mathbb{P}_n$ tel que ce symbole ait un sens, i.e. tel que $H \not\supset \phi_g(V)$.

Supposons la variété V normale. Si $\mathfrak{L}$ est un système linéaire sur V , et si ses éléments E ont une composante commune E_0 , on dit que E_0 est une <u>composante fixe</u> de $\mathfrak{L}$. L'ensemble des $E - E_0$ est alors encore un système linéaire, associé à la même application rationnelle ϕ . On pourra donc, pour étudier ϕ , supposer que $\mathfrak{L}$ est sans composante fixe. On appelle alors <u>point de base</u> de $\mathfrak{L}$ un point commun aux supports de tous les diviseurs $E \in \mathfrak{L}$. <u>Pour que</u> ϕ <u>soit morphique en</u> $a \in V$, <u>il faut et il suffit que</u> a <u>ne soit pas</u>

.../...

un point de base de $\mathcal{L}$. En effet, soient $f_0,\dots, f_n$ comme plus haut, et posons $\mathrm{div}(f_i) = D_i - D$. Supposons ϕ morphique en a . Il existe alors un i_o tel que f_i/f_{i_o} soit morphique en a pour tout i , donc tel que f/f_{i_o} soit morphique en a pour toute $f \in L$. Si a est un point fixe de $\mathcal{L}$, on a $a \in \mathrm{supp}\, D_{i_o}$, i.e. il existe une composante Z de D_{i_o} contenant a . D'après le critère de morphicité, Z est composante de E quel que soit f , i.e. est une composante fixe de $\mathcal{L}$, contrairement à notre hypothèse. Inversement, supposons que $\mathcal{L}$ est sans point de base. Il existe alors $f \in L$ telle que, en posant $\mathrm{div}(f) = E - D_o$, on ait $a \notin \mathrm{supp}\, E$. Alors f_i/f est morphique en a pour tout i . Puisque $f \in L$ le k-espace vectoriel engendré par les f_i/f contient 1 , et par suite il existe i_o tel que f_{i_o}/f ne s'annule pas en a . On a donc $a \notin \mathrm{supp}\, D_{i_o}$. Donc f_i/f_{i_o} est morphique en a pour tout i , donc ϕ est morphique en a .

V étant toujours supposée normale et complète, on dit qu'un système linéaire $\mathcal{L}$ sur V sépare les points si, pour tout couple (a,b) de points distincts de V , il existe $E \in \mathcal{L}$ tel que $a \in \mathrm{supp}\, E$ et $b \notin \mathrm{supp}\, E$. Dans ce cas, $\mathcal{L}$ n'a pas de point de base, donc ϕ est un morphisme. Ce morphisme est de plus injectif, (donc applique bijectivement V sur $W = \phi(V)$). En effet, soient $a, b \in V$ distincts ; il existe $E \in \mathcal{L}$ tel que $a \in \mathrm{supp}\, E$, et $b \notin \mathrm{supp}\, E$. Le diviseur E est de la forme $\phi^{-1}(H)$, où H est un hyperplan de $\mathbb{P}_n$. On a donc $\phi(a) \in H$, et $\phi(b) \notin H$, d'où $\phi(a) \neq \phi(b)$.

Remarquons que l'injectivité de ϕ n'entraine pas que ϕ

.../...

soit bimorphique en tout point. Lorsque cette dernière condition est remplie, i.e. lorsque ϕ est un isomorphisme de V sur une sous-variété de $\mathbb{P}_n$, on dit encore que ϕ est un plongement, ou une immersion de V dans $\mathbb{P}_n$. On dit alors que le système linéaire $\mathfrak{L}$ est ample. Lorsque $\mathfrak{L}(D)$ est ample, on dit que D est ample.

THEOREME 4.

Soient V une variété normale complète, W une variété projective, et soit D un diviseur sur V appartenant au système linéaire $\mathfrak{L}$ sur V associé à un revêtement $\phi : V \to W$. Alors il existe un entier $n > 0$ tel que $\mathfrak{L}(nD)$ soit ample.

Commencons par démontrer le lemme suivant :

LEMME 1. Soient V une variété normale complète, et D un diviseur positif sur V. Alors

(a) - $A = \bigcup_{n>0} L(n\,D)$ est un sous-anneau intégralement fermé du corps de fonctions $\mathcal{F}(V)$.

(b) - Pour $L \in L(D)$, tel que le système linéaire $\mathfrak{L}$ associé à L soit sans point de base, l'anneau A coïncide avec la fermeture intégrale de l'anneau $k[L]$ dans $\mathcal{F}(V)$.

Démonstration. A se compose des fonctions sur V n'admettant pas d'autres pôles que les composantes de D. Ceci entraîne que A est un sous-anneau de $\mathcal{F}(V)$.

Soit $t \in \mathcal{F}(V)$, entière sur A, et montrons que $t \in A$. En effet, t est racine d'une équation de la forme

$$(6)\quad t^m + a_1 t^{m-1} + \ldots + a_m = 0\ ,$$

avec $a_i \in A$ $(1 \leq i \leq m)$. Il existe un entier $q > 0$ tel que $a_i \in L(q\,D)$ pour tout i. Soit Z un pôle de t. Soit k

.../...

un corps de définition de A, L et Z. Soient x un point générique de V sur k, et z un point générique de Z sur k. Soit ρ une place de Ω telle que $\rho(x) = z$. On a $\rho(t) = \infty$; d'après (6), on ne peut avoir $\rho(a_i/t) = 0$ pour tout i. Il existe donc un i tel que $\rho(a_i/t) \neq 0$, ou encore tel que $v_Z(a_i) \leq v_Z(t)$, où v_Z est la valuation de $\mathfrak{F}(V)$ associée à Z. Puisque $a_i \in L(q\,D)$, on a $\mathrm{div}(a_i) \geq -q\,D$. On a donc aussi $\mathrm{div}(t) \geq -q\,D$, donc $t \in L(q\,D)$, d'où $t \in A$. On a donc démontré (a).

Il reste à prouver que pour $n > 0$, dans les hypothèses de (b), tout élément $u \in L(n\,D)$ est entier sur $k[L]$. Or soit ρ une place de $k(x)$ telle que $\rho(u) = \infty$. Le point $a = \rho(x)$ de V appartient au support du diviseur des pôles de u, donc appartient à $\mathrm{supp}\,D$. Puisque L est sans point de base, il existe $E \in \mathfrak{D}$ tel que $a \notin \mathrm{supp}\,E$. Soit $f \in L$ telle que $\mathrm{div}(f) = E - D$. Cette fonction f est définie en a, de valeur ∞, donc on a $\rho(f(x)) = \infty$. D'après E, Chap. 0, B, 3, th. 2, u est entier sur $k[L]$, C.Q.F.D.

Démonstration du théorème 4. Soit k un corps de définition de V, D et ϕ. Supposons ϕ définie au moyen d'une base $f_0, \ldots, f_m$ de l'espace vectoriel L. Soit x un point générique de V sur k. La variété W est le lieu sur k du point $y = \phi(x)$ de $\mathbb{P}_m$, admettant pour coordonnées homogènes les $y_i = f_i(x)$ $(0 \leq i \leq m)$. Posons $\mathrm{div}(f_i) = D_i - D$. Pour $0 \leq i \leq m$, notons U_i l'ouvert de W induit par le complémentaire de l'hyperplan $X_i = 0$ de $\mathbb{P}_m$. Introduisons un modèle normale canonique (W^*, λ) de W au sens de

.../...

E, IV, 4, th. 7. Rappelons qu'un tel modèle peut être obtenu par recollement de modèles affines canoniques (W_i^*, λ_i) des ouverts affines W_i. Le point générique $z = \lambda^{-1}(y)$ de W^* est représenté par un point $z_i \in W_i^*$ dont les coordonnées z_{ij} $(1 \leq j \leq s_i)$ sont des générateurs sur k de la clôture intégrale B_i^* de l'anneau de coordonnées $B_i = k[(y_0/y_i), \ldots, (y_m/y_i)]$ de W_i. Or on a $y_j/y_i \in L(D_i)$ $(0 \leq j \leq m)$. D'après le lemme 1, on a donc, pour tout j, $z_{ij} \in A_i$, où A_i est l'anneau $A_i = \bigcup_n L(n\,D_i)$. Pour tout i, il existe un entier q_i tel que les z_{ij} appartiennent à $L(q_i\,D_i)$. D'après le lemme 1, A_i est la clôture intégrale de B_i dans $k(x)$. Or B_i a pour corps des fractions $k(y)$; puisque Φ est un revêtement, l'extension $k(x)/k(y)$ est de degré fini. Donc (E, ch. 0, B, 3, th. 2, coroll. 1), A_i est un B_i^*-module de type fini, nécessairement noethérien. La suite croissante des B_i-modules $B_i^*[L(n\,D)]$ $(n = 1, 2, \ldots)$ est donc stationnaire, et il existe un entier r_i tel que $B_i^*[L(r_i D)] = A_i$, donc tel que $k[L(r_i D)] = A_i$. Posons $n_i = \sup(q_i, r_i)$ pour tout i, et prenons $n = \sup_i n_i$. Soit $\phi' : V \to \mathbb{P}_m$, une application rationnelle, définie sur k, associée au système linéaire $\mathfrak{L}(n\,D)$. Posons $y' = \phi'(x)$, et $W' = \phi'(V) = \mathrm{loc}_k y'$. Puisque $k[L(n\,D_i)] = A_i$ a pour corps de fractions $k(x)$, on a $k(y') = k(x)$, i.e. ϕ' est <u>birationnelle</u>. Puisque ϕ est un morphisme, $\mathfrak{L}$ est sans point de base ; il en est de même a fortiori de $\mathfrak{L}(n\,D)$, donc ϕ' est un <u>morphisme</u>. Pour tout i, le diviseur $n\,D_i$ est de la forme $(\phi'^{-1})(H'_i)$, où H'_i est un hyperplan de $\mathbb{P}_m$. Notons W'_i l'ouvert de W'

.../...

induit par le complémentaire de H_i' . Les W_i' recouvrent W' , et l'anneau de coordonnées de W_i' est $A_i = k[L(n\ D_i)]$, donc est intégralement clos. Donc W' est normale. Comme de plus les z_{ij} appartiennent à A_i , il existe un morphisme $\theta : W' \longrightarrow W^*$, défini sur k , tel que $z = \theta(y')$. On a le diagramme commutatif suivant de morphismes

$$\begin{array}{ccc} V & \xrightarrow{\phi} & W \\ {\scriptstyle \phi'}\downarrow & & \uparrow{\scriptstyle \lambda} \\ W' & \xrightarrow{\theta} & W^* \end{array}$$

Puisque ϕ est un revêtement, tous les morphismes intervenant dans ce diagramme sont des revêtements. Donc ϕ' est un revêtement birationnel de W' . Comme W' est normale ϕ' est nécessairement un isomorphisme, d'après E, IV, 2, th. 3 C.Q.F.D.

Corollaire 1. Soit W une variété projective. Il existe un modèle normal canonique projectif de W .

Il suffit en effet d'appliquer la construction précédente en prenant pour (V,ϕ) un modèle normal canonique arbitraire de W .

Corollaire 2. Soit V une variété normale, et soit D un diviseur sur V . Si le système linéaire $\mathfrak{L}(D)$ sépare les points, il existe un entier $n > 0$ tel que $\mathfrak{L}(n\ D)$ soit ample.

En effet, dans ce cas, toute application rationnelle $V \to W$ $(W \subset \mathbb{P}_m)$ associée à $\mathfrak{L}(D)$ est comme on a vu, un morphisme bijectif, donc est un revêtement de W .

.../...

4. Plongement projectif d'une variété abélienne.

THEOREME 5.

Toute variété abélienne A admet un plongement projectif.

Démonstration : Il revient au même de dire qu'il existe sur A un diviseur ample. D'après le th. 4, il suffit de montrer qu'il existe un diviseur D sur A tel que L(D) sépare les points.

Si a et b sont deux points distincts de A, on peut trouver une sous-variété de codimension 1 de A contenant a et non b (on se ramène en effet, par translation, au cas où a et b appartiennent à un même ouvert affine de A, auquel cas la solution est triviale). Donc, si E est un sous-ensemble fermé de A contenant l'origine 0, et distinct de $\{0\}$, on peut trouver une sous-variété X de A, de codimension 1, telle que $0 \in X$ et $E \not\subset X$. Il en résulte qu'on peut trouver un nombre fini de sous-variétés X_i $(1 \leq i \leq m)$ de codimension 1 de A telles que $\bigcap_i X_i = \{0\}$.

Si u et v sont deux points de A, et si X est un diviseur sur A, on a $X_u + X_v + X_{-u-v} \sim 3\,X$, en vertu du coroll. 2 du th. 3 du n° 2. Donc, quels que soient $u_i, v_i \in A$ $(1 \leq i \leq m)$, le diviseur $Z = \sum_i ((X_i)_{u_i} + (X_i)_{v_i} + (X_i)_{-u_i-v_i})$ est linéairement équivalent à $D = 3 \sum_i X_i$. Nous allons montrer que $\mathfrak{L}(D)$ sépare les points. En effet, pour $a, b \in A$, il existe i tel que $b-a \notin X_i$. Supposons par exemple $i = 1$. Pour $u_1 = a$, et pour $u_2, \ldots, u_n$, $v_1, \ldots, v_n$ génériques indépendants sur k(a), on a $b \notin (X_1)_{u_1}$ $a \in (X_1)_{u_1}$; les autres composantes de Z ne contiennent

.../...

aucun des deux points a et b. Donc on a $a \in \text{supp } Z$, et $b \notin \text{supp } Z$ C.Q.F.D.

5. Variété abélienne engendrée par une sous-variété de A.

Soit A une variété abélienne, et soient $E_1, \ldots, E_r$ des sous-ensembles de A. Conformément à la notation déjà utilisée au n° 7 du chap. I, on note $E_1 + \ldots + E_r$ l'ensemble E des points de A qui sont de la forme $a_1 + \ldots + a_r$, avec $a_i \in E_i$. Si les E_i sont des sous-ensembles fermés (resp. des sous-variétés) de A, il en est de même de E. La somme $E + \ldots + E$ (r termes) est notée $E^{(r)}$.

THEOREME 6.

Soit A une variété abélienne et soit V une sous-variété de A contenant l'origine. Alors

(a) - Il existe une plus petite sous-variété abélienne B de A contenant V.

(b) - Il existe un entier r tel qu'on ait $B = V^{(r)}$.

(On dit alors que B est la sous-variété abélienne de A engendrée par V).

Démonstration.

(a) - Notons $S = S(V)$ l'ensemble des sous-variétés abéliennes de A contenant V. Soit $B \in S$ de dimension minimum, et soit $B' \in S$. La composante de l'origine B_o de $B \cap B'$ appartient à S. On a $B_o \subset B$, d'où $\dim B_o \leq \dim B$, ce qui entraîne $\dim B_o = \dim B$, d'où $B_o = B$, et $B' \supset B$.

(b) - La suite croissante $V \subset V^{(2)} \subset \ldots \subset V^{(n)}$ de sous-variétés de A est nécessairement stationnaire, i.e. il existe un r tel que $V^{(s)} = V^{(r)}$ pour tout $s \geq r$.

.../...

En particulier, on a $V^{(2r)} = V^{(r)} + V^{(r)} = V^{(r)}$. Donc $V^{(r)}$ est un sous-groupe de A , et par suite une sous-variété abélienne de A . D'autre part $B' \in S$ (i.e. $V \subset B'$) entraîne $V^{(n)} \subset B'$ pour tout n et, en particulier $V^{(r)} \subset B'$. On a donc $V^{(r)} = B$.

6. Une propriété des translatés d'un diviseur positif sur A .

THEOREME 7.

Soit X un diviseur positif sur une variété abélienne A , et soit V une sous-variété de A contenant l'origine. Soient k un corps de définition de A, V, X et u un point générique de V sur k . Si on a $X_u \sim X$, on a $X_u = X$, et on a aussi $X_b = X$ pour tout $b \in V$.

Démonstration : Pour que la propriété soit vraie pour V_1 et V_2 (avec X donné), il faut et il le suffit qu'elle le soit pour $V_1 + V_2$ (d'après le fait que $u = u_1 + u_2$ entraîne $X_u - X \sim (X_{u_1} - X) + (X_{u_2} - X)$). Par passage à la variété engendrée par V , on se ramène donc au cas où $V = B$ est une variété abélienne.

Si $X_u \sim X$, il existe une fonction g_u sur A , définie sur $k(u)$, telle que $\mathrm{div}(g_u) = X_u - X$. Pour tout autre point générique v de B sur k , le k-isomorphisme $\sigma : k(u) \longrightarrow k(v)$ tel que $\sigma(u) = v$ se prolonge canoniquement à un k-isomorphisme $\mathcal{F}_{k(u)}(V) \xrightarrow{\bar{\sigma}} \mathcal{F}_{k(v)}(V)$. On note g_v l'image de g_u par σ . On a nécessairement $\mathrm{div}(g_v) = X_v - X$.

Soit $f \in L = L(X)$ non nulle, et posons $\mathrm{div}(f) = Y - X$. La fonction $\lambda_u(f) = (f \circ \tau_u^{-1})\, g_u$ a pour diviseur $(Y_u - X_u) + (X_u - X) = Y_u - X$. En particulier, on a

.../...

$\mathrm{div}(\lambda_u(g_v)) = X_{u+v} - X$. Si u et v sont génériques indépendants de B sur k, $u+v$ est aussi générique de B sur k, et on a $\mathrm{div}\,\lambda_u(g_v) = \mathrm{div}(g_{u+v})$. Il existe donc une constante $c(u,v) \in k(u,v)$ telle qu'on ait

$$\lambda_u(g_v) = c(u,v)\, g_{u+v} .$$

On en déduit, quelle que soit $f \in L$,

(7) $\lambda_v(\lambda_u(f)) = c(u,v)\, \lambda_{u+v}(f)$.

Posons $\dim \mathfrak{L}(X) = \dim L - 1 = q$. On peut regarder l'application $\lambda_u : L \longrightarrow L$ comme un élément du groupe linéaire d'ordre $q+1$, et lui associer canoniquement un élément $\alpha(u)$ du groupe linéaire projectif G d'ordre q (en passant au quotient, dans $L^* = L - \{0\}$, par la relation d'équivalence définie par la proportionalité des coordonnées). La relation (7) entraîne que l'application $\alpha : B \longrightarrow G$ ainsi définie est un homomorphisme. Tout élément de G peut être regardé comme une matrice d'ordre $q+1$, inversible, déterminée au produit près par une constante non nulle. Si on lui associe le point de l'espace projectif $\mathbb{P} = \mathbb{P}_{(q+1)^2-1}$ ayant pour coordonnées homogènes les éléments de cette matrice (ordonnés de façon arbitraire), on obtient un isomorphisme $\tau : G \to U$ de G sur l'ouvert U de $\mathbb{P}$ complémentaire de l'hypersurface H des zéros du déterminant de M . Or l'image $\tau(\alpha(B))$ est une sous-variété complète de l'ouvert affine U, donc est réduite à un point. Donc $\alpha(B)$ est réduite à un point, et ce point est nécessairement l'élément neutre de G . On a donc $\mathrm{div}(\lambda_u(f)) = \mathrm{div}(f)$ pour toute $f \in L$. En particulier, en prenant $f=1$, on obtient $X_u = X$.

.../...

Soit maintenant $b \in B$, et prenons u générique de B sur $k(b)$. Considérons une k-composante Y de X, et soit y un point générique de Y sur $k(u,b)$. Le point $y+b$ est une spécialisation de $y+u$ sur k, autrement dit on a $Y_b \in Z$, en posant $Z = \mathrm{loc}_k(y+u)$. Or on a $y+u \in \mathrm{supp}\ X$, donc $Y_u \subset Z \subset \mathrm{supp}\ X$, et la considération des dimensions montre que $Y_b = Y_u = Z$. Il en résulte $X_b = X_u = X$, C.Q.F.D.

Corollaire : Soit A une variété abélienne. Pour $n \neq 0$, l'homomorphisme $n_\delta : A \longrightarrow A$ est surjectif, i.e. de noyau fini.

(C'est le résultat qui avait été annoncé au n° 7 du chap. I ; rappelons que n_δ est défini par $n_\delta(x) = nx$).

Démonstration. La composante de l'origine de $\ker(n_\delta)$ est une sous-variété abélienne B de A. Supposons $\dim B > 0$. On peut trouver une sous-variété X de A, de codimension 1, contenant 0 et ne contenant pas B. Soit k un corps de définition de A, B, X, et soit u un point générique de B sur k. On a $nu = 0$, d'où $n(X_u - X) \sim X_{nu} - X = 0$. D'après le théorème précédent, ceci entraîne $nX_u = n\,X$, d'où $X_u = X$. On en tire $u \in X$, d'où $B \subset X$, ce qui est contradictoire. On a donc montré que $\dim B = 0$. Donc $\ker(n_\delta)$ est fini.

7. Diviseurs non dégénérés sur une variété abélienne.

Soit A une variété abélienne. Considérons le groupe $\mathcal{D}(A)$ des diviseurs sur A, et le sous-groupe $\mathcal{D}_\ell(A)$ de $\mathcal{D}(A)$ composé des diviseurs linéairement équivalents à zéro sur A. Pour $X \in \mathcal{D}(A)$, on note η_X l'application

$$\eta_X : A \longrightarrow \mathcal{D}(A)/\mathcal{D}_\ell(A)$$

.../...

qui, à tout point $a \in A$, fait correspondre la classe de X modulo l'équivalence linéaire. La relation $X_{a+b} - X_a - X_b + X \sim 0$ du coroll. 1 du th. 3 s'écrit encore $X_{a+b} - X \sim (X_a - X) + (X_b - X)$, et s'interprète par le fait que η_X est un homomorphisme pour la structure de groupe.

On dira que X est dégénéré si $\ker \eta_X$ est infini.

THEOREME 8.

Soit X un diviseur positif sur une variété abélienne A. Alors $\ker \eta_X$ est un sous-groupe algébrique de A. De plus, les conditions suivantes sont équivalentes :

(a) - X est non dégénéré (i.e. $\ker \eta_X$ est fini).

(b) - Le groupe des translations sur A qui laissent X invariant est fini.

(c) - Pour toute sous-variété abélienne B de A non réduite à un point, il existe $b \in B$ tel que $X_b \neq X$.

(d) - Il existe un entier $n > 0$ tel que $n X$ soit ample.

Démonstration. Soit k un corps de définition algébriquement clos de A et X. Commençons par montrer que $\ker \eta_X$ est un sous-ensemble k-fermé de A. Soit w un point de $\ker \eta_X$, et posons $W = \mathrm{loc}_k w$. Il existe (cf. démonstration du coroll. 1 du th. 3) un diviseur Z sur $A \times A$ tel qu'on ait $X_a - X = Z(a)$ pour tout $a \in A$. D'après II, 3, lemme 5, si $a \in W$, on a aussi $X_a - X = T(a)$, en posant $T = Z.(W \times A)$. Or on a, par hypothèse, $T(w) = Z(w) = X_w - X \sim 0$. On a donc également, d'après II, 3, lemme 6, $T(a) = Z(a) = X_a - X \sim 0$. On a donc $W \subset \ker \eta_X$, et on a bien montré que $\ker \eta_X$ est un sous-ensemble k-fermé de A. Comme c'est un sous-groupe

.../...

de A , c'est un sous-groupe algébrique de A .

Il est clair que (a) $\Longrightarrow$ (b) et que (b) $\Longrightarrow$ (c).

(c) $\Longrightarrow$ (a). En effet, si $\ker \eta_X$ est infini, la composante de l'origine B du groupe algébrique $\ker \eta_X$ est une sous-variété abélienne de A non réduite à un point, telle que $X_b \sim X$ pour tout $b \in B$. D'après le th. 7, ceci implique $X_b = X$ pour tout b , contrairement à l'hypothèse.

(d) $\Longrightarrow$ (c). D'après le th. 5, on peut supposer que A est projective, et que $Y = m\,X$ est une section hyperplane de A . Soit B une sous-variété abélienne de A non réduite à un point, et supposons que, pour tout $b \in B$, on ait $X_b = X$, d'où $Y_b = Y$: On peut trouver une section hyperplane Y' de A telle que $0 \in \operatorname{supp} Y'$ et $B \not\subset \operatorname{supp} Y'$. Puisqu'on a $Y' \sim Y$, on a $Y'_b \sim Y'$. D'après le th. 7, on a donc $Y'_b = Y'$, d'où $b \in \operatorname{supp} Y'$. On en déduit $B \subset \operatorname{supp} Y'$, ce qui est contradictoire.

(b) $\Longrightarrow$ (d). Notons G le sous-groupe de A composé des points $a \in A$ tels que $\operatorname{supp} X_a = \operatorname{supp} X$, et H le sous-groupe de G composé des $a \in A$ tels que $X_a = X$. Il est clair que G est un sous-ensemble k-fermé de A ; donc G est un sous-groupe algébrique de A . Montrons que H contient la composante de l'origine G_o de G . En effet, soit Y une composante de X , et soient $y \in Y$, $t \in G_o$ génériques indépendants sur k . On a $y + t \in \operatorname{supp} X_t = \operatorname{supp} X$, donc $W \subset \operatorname{supp} X$, en posant $W = \operatorname{loc}_k(y+t)$. Puisqu'on a $0 \in G_o$, on a $y \in W$, d'où $Y \subset W$. La considération des dimensions montre que $Y = W$. Pour tout point $b \in G_o$, on a de même

.../...

$Y_b \subset W$, d'où $Y_b = Y = W$. On en déduit $X_b = X$. On a donc bien montré que $G_o \subset H$.

Puisqu'on suppose H fini, G_o est réduit à un point, donc G est fini. Pour $a \in A$, tel que $a \notin G$, on a $\mathrm{supp}(X_{-a}) \neq \mathrm{supp}\, X$. Soit $u \in A$, tel que $u \in \mathrm{supp}\, X$, et $u \notin \mathrm{supp}(X_{-a})$, c'est-à-dire tel que $0 \in \mathrm{supp}(X_{-u})$, et $a \notin \mathrm{supp}(X_{-u})$. Si v est un point générique de A sur $k(u)$, et si on pose $Y = X_{-u} + X_{-v} + X_{u+v}$, on voit qu'on a $0 \in \mathrm{supp}\, Y$ et $a \notin \mathrm{supp}\, Y$. On a d'autre part $Y \sim 3X$, d'après le coroll. 1 du th. 3. Donc le système linéaire $\mathfrak{L}(3X)$ sépare les points 0 et a . De même $\mathfrak{L}(3X)$ sépare deux points a et a' de A pourvu qu'on ait $a' - a \notin G$; en particulier $\mathfrak{L}(3X)$ est sans point de base. Donc toute application rationnelle $\phi : A \longrightarrow A'$ $(A' \subset \mathbb{P}_n)$ associée à $\mathfrak{L}(3X)$ est un morphisme, tel que l'image inverse de tout point de A' soit composée de points de A congrus (mod G). Cette image inverse est donc un ensemble fini, i.e. ϕ est un revêtement de A' . Il suffit alors d'appliquer le th. 4.

8. Le théorème de Chow.

Remarque 1 : D'après (d), et d'après le th. 5 il existe sur toute variété abélienne un diviseur positif non dégénéré.

THEOREME 9.(Chow)

Soit A une variété abélienne définie sur un corps k . Toute sous-variété abélianne B de A est définie sur une extension algébrique de degré fini de k .
(En d'autres termes, il n'existe pas de "famille algébrique infinie" de sous-variétés abéliennes de A).

.../...

Démonstration. Soit en effet K un corps de définition de B, de type fini sur k, contenant la clôture algébrique $\bar{k}$. Choisissons un modèle U du corps K, défini sur $\bar{k}$, i.e. une variété définie sur $\bar{k}$, telle que $K = \bar{k}(u)$, avec u générique de U sur $\bar{k}$.

Soit u' un point générique de U sur k indépendant de u. Posons $B = B_u$, et notons $B_{u'}$ la sous-variété abélienne de A transformée de B par le k-isomorphisme $\sigma : k(u) \longrightarrow k(u')$ tel que $\sigma(u) = u'$. La sous-variété $B_u + B_{u'}$ de A est une variété abélienne C. Si x et x' sont deux points génériques indépendants de B_u et $B_{u'}$ respectivement sur $L = k(u,u')$, la variété C est le lieu de $y = x + x'$ sur L. Soit Z la sous-variété de $U \times U \times A$ lieu de (u, u', y) sur $\bar{k}$, et considérons l'intersection $E = Z \cap (u \times u \times A)$. Soit $b \in E$. La spécialisation $(u, u', y) \longrightarrow (u, u, b)$ sur $\bar{k}$ se prolonge à des spécialisations $x \to a$ et $x' \to a'$, où a et a' sont deux points de B, et on a $a + a' = b$, d'où $b \in B$. On en déduit $Z \cap (u \times u \times A) \subset u \times u \times B$. Le théorème de la dimension appliqué à $X \cap (u \times u \times A)$ dans le produit $U \times U \times A$, entraîne $\dim B \geq \dim Z = \dim A - \dim(U \times U \times A)$, et comme $\dim Z = \dim C + 2 \dim U$, on en déduit $\dim B \geq \dim C$. Puisqu'on a $B \subset C$, on a $B = C$, d'où $B = B_u = B_{u'}$. Donc B est définie sur $\bar{k}(u) \cap \bar{k}(u') = \bar{k}$. Donc B est définie sur un sous-corps k' de $\bar{k}$ qui est extension de type fini de k, donc algébrique de degré fini sur k.

Remarque 2 : On peut montrer en fait que B est définie

.../...

sur une extension algébrique séparable de degré fini de k .

9. Relation $\equiv$. Equivalence numérique.

Soit A une variété abélienne. Notons (provisoirement) $\mathcal{D}'(A)$ le groupe des diviseurs X sur A tels que $\eta_X = 0$. La relation de congruence suivant $\mathcal{D}'(A)$ sera notée par le signe $\equiv$. La relation $X \equiv 0$ équivaut donc à $\eta_X = 0$, ou encore à $X_a \sim X$ pour tout $a \in A$.

LEMME 2. Soit A une variété abélienne, et soit X un diviseur $\equiv 0$ sur A . Alors, si $\lambda : A \times A \to A$ est la loi de groupe de A on a

$$\lambda^{-1}(X) \sim A \times X + X \times A .$$

Démonstration. Posons $Y = \lambda^{-1}(X)$. Pour $a \in A$, on a $\tau_a = \lambda \circ i_a$, où i_a est l'immersion $x \to (a,x)$ de A dans $A \times A$, d'où $X_{-a} = i_a^{-1}(Y) = Y(a)$.

Puisqu'on a $X_{-a} \sim X$, on a $Y'(a) \sim 0$, en posant $Y' = Y - (A \times X)$. Donc (III, 3, lemme 6), on a

(8) $Y' \sim X' \times A$

où X' est un diviseur sur A . Pour $b \in A$, on a de même $X_b = {}^tY(b)$. Si on prend $b \notin \operatorname{supp} X$, on a $(A \times b)(A \times X) = 0$, donc ${}^tY'(b) = {}^tY(b) = X_b$. La relation (8) entraîne d'autre part ${}^tY'(b) = X'$. Puisqu'on a $X_b \sim X$, on a $X' \sim X$, d'où le lemme.

Ce lemme admet la généralisation suivante :

Corollaire : Soit A une variété abélienne. Pour tout entier $m > 0$, notons λ_m le morphisme $A \times \ldots \times A$ (m facteurs) $\longrightarrow A$ défini par $\lambda_m(x_1, \ldots, x_m) = x_1 + \ldots + x_m$. Soit X un diviseur $\equiv 0$ sur A . Alors on a

$$\lambda_m^{-1}(X) \sim \textstyle\sum_i X_i$$

.../...

avec $X_i = \pi_i^{-1}(X)$, où $\pi_i = pr_i$ est la projection de $A \times .. \times A$ sur le ième facteur.

Démonstration : Procédons par récurrence sur m. Le résultat est trivial pour $m = 1$. D'autre part, on a

$$\lambda_m(x_1, \ldots, x_m) = \lambda(\lambda_{m-1}(x_1, \ldots, x_{m-1}), x_m).$$

En d'autres termes, si μ est le morphisme $A \times \ldots \times A$ (m facteurs) $\longrightarrow A \times A$ obtenu en posant $\mu(x_1, \ldots, x_m) = (\lambda_{m-1}(x_1, \ldots, x_{m-1}), x_m)$, on a $\lambda_m = \lambda \circ \mu$, d'où $\lambda_m^{-1}(X) = \mu^{-1}(\lambda^{-1}(X))$.

Notons π'_m la projection de $A \times \ldots \times A$ (m facteurs) sur le produit des $m-1$ premiers facteurs ; notons ψ_1 et ψ_2 les projections respectives de $A \times A$ sur le premier et le second facteur.

On a, d'après le lemme précédent

$$\lambda^{-1}(X) \sim (X \times A) + (A \times X) \quad = \quad \psi_1^{-1}(X) + \psi_2^{-1}(X)$$

d'où

$$\lambda_m^{-1}(X) \sim \mu^{-1}(\psi_1^{-1}(X)) + \mu^{-1}(\psi_2^{-1}(X)).$$

Or on a $\psi_1 \circ \mu = \pi_{m-1} \circ \pi'_m$, et $\psi_2 \circ \pi = \pi_m$. On en déduit

$$\lambda_m^{-1}(X) \sim \pi_m'^{-1}(\pi_{m-1}(X)) + \pi_m^{-1}(X) = \pi_{m-1}^{-1}(X) \times A + \pi_m^{-1}(X).$$

Il suffit alors d'appliquer l'hypothèse de récurrence.

Soit A une variété abélienne, et soit V une courbe sur A. Soit d'autre part X un diviseur sur V, tel que le diviseur induit $X.V$ soit défini, et que ses composants soient simples sur V. Explicitons $X.V$ sous la forme $X.V = \sum_i m_i (a_i)$ (où l'on met des parenthèses pour signifier qu'il s'agit de l'addition au sens des cycles). Le point $a = \sum_i m_i a_i$ de A (addition au sens de la loi de groupe)

.../...

est alors désigné par la notation $S_A(X.V)$.

La courbe V et le diviseur X étant maintenant supposés quelconques, on peut, d'après E III 13, th. 12, trouver un diviseur $X' \sim X$ sur A tel que le symbole $X'.V$ soit défini ; on peut en outre choisir X' de façon que son support ne contienne aucun des points multiples de V. La classe du diviseur $X'.V$ pour l'équivalence linéaire ne dépend pas du choix de X', mais seulement de X et de V. Tenant compte de II, 7, th. 5, corcll., on en déduit, par passage à un modèle sans point multiple de V, que le degré $\deg(X'.V)$ ne dépend que de X et de V, mais non du choix de X'. On désigne ce nombre par $\deg(X * V)$. De même, le point $a = S_A(X'.V)$ ne dépend pas du choix de X' : considérons en effet deux choix possibles X' et X'' ; posant $Y = X' - X''$, on a $Y \sim 0$, d'où $Y.V = 0$ et $\deg(Y.V) = 0$; introduisons la jacobienne J de V, et soit ϕ une application rationnelle canonique $V \to J$; d'après la propriété d'application universelle du couple (J,ϕ) (III, 7, th. 6). On peut factoriser ϕ sous la forme $\phi = \nu \circ i$, où i est l'inclusion $V \to A$, et où ν est un morphisme $J \to A$, d'après I, 6, th. 8, coroll. 1, ν est de la forme $\nu = \tau \circ \mu$, où $\tau = \tau_c$ est une translation sur A, et où μ est un homomorphisme $J \to A$; d'après III, 8, th. 7, on a $S_\phi(Y.V) = 0$; on a donc $S_A(Y.V) = \nu(S_\phi(Y.V)) = \mu(S_\phi(Y.V) + \deg(Y.V)c = 0$, ce qui donne bien $S_A(X'.V) = S_A(X''.V)$. Le point a est donc déterminé par la donnée de X et de V. On le désignera par $S_A(X * V)$. Il est clair qu'on a $S_A(X * V) = S_A(X.V)$ lorsque ce dernier symbole est défini.

.../...

THEOREME 10.

Soit A une variété abélienne de dimension n. Il existe une courbe V sur A contenant l'origine 0, telle que V engendre A (au sens introduit au n° 5). On a alors $V^{(n)} = A$. Pour tout diviseur $X \equiv 0$ sur A, on a $\deg(X * V) = 0$.

Posons d'autre part $W = V^{(n-1)}$. Il existe deux entiers q et r positifs $\neq 0$ tels que, pour tout diviseur $X \equiv 0$ sur A, on ait

(9) $qX \sim r(W_a - W)$

en posant $a = S_A(X * V)$.

Démonstration. Soit k un corps de définition algébriquement clos de A. On peut prendre pour V l'une quelconque des courbes sur A contenant l'origine, et contenant un point générique u de A sur k : une telle courbe V existe d'après I, 6, lemme 4 (ou d'après III, 4, lemme 8) ; la sous-variété abélienne de A engendrée par V est définie sur k, d'après le th. de Chow, et contient u, donc coïncide avec A.

Soit m le plus petit entier tel que $V^{(m)} = A$. C'est aussi le plus petit entier tel que $V^{(m)} = V^{(m+1)}$, et on a donc une suite strictement croissante de variétés $0 \subset V \subset V^{(2)} \subset \ldots \subset V^{(m)} = A$. Pour $1 \leq i \leq m-1$, on a $V^{(i+1)} = V^{(i)} + V$, donc $\dim V^{(i+1)} \leq \dim V^{(i)} + 1$. Puisque $\dim V^{(i+1)} > \dim V^{(i)}$, ceci implique $\dim V^{(i+1)} = \dim V^{(i)} + 1$. On a donc $m = \dim A = n$. Il en résulte que le morphisme $\mu : V^n = V \times \ldots \times V \to A$ induit par λ_n, i.e. défini par

.../...

$\mu(x_1,\ldots, x_n) = x_1 +\ldots+ x_n$ est génériquement surjectif ; puisque V est complète, μ est surjectif et de degré fini q .

Soit maintenant X un diviseur $\equiv 0$ sur A . On peut supposer que $X.V$ est défini. D'après le lemme 2, on a

$$\lambda_n^{-1}(X) \sim \sum_{i=1}^{n} \pi_i^{-1}(X),$$

où π_i est la projection $A \times\ldots\times A \to A$ sur le i-ème facteur On en déduit

$$\mu^{-1}(X) \sim \sum_i (\pi_i^{-1}(X)).(V \times\ldots\times V)$$

d'où compte tenu de la commutativité du diagramme

$$\begin{array}{ccc} V \times\ldots\times V & \longrightarrow & A \times\ldots\times A \\ \downarrow{\scriptstyle \psi_i} & & \downarrow{\scriptstyle \pi_i} \\ V & \longrightarrow & A \end{array}$$

(où les flèches horizontales désignent les inclusions, et où chacune des flèches verticales désigne la projection sur le i-ème facteur).

$$(10)\quad \mu^{-1}(X) \sim \sum_i \psi_i^{-1}(X.V).$$

Soit $x = (x_1,\ldots, x_n)$ un point générique de $V^n = V \times\ldots\times V$ sur k . Le point $y = \lambda_n(x) = \mu(x)$ est générique de A sur k, et on a $[k(x) : k(y)] = q$. Pour tout point $b \in V$, et pour tout i $(1 \leq i \leq n)$, on a

$$\mu_g(\psi_i^{-1}(b)) = \mu(\psi_i^{-1}(b)) = W_b ,$$

et si t est un paramètre uniformisant de b sur V , la norme $N\, h_t$ de $h_t = \prod_i (\psi_i \quad t)$ relativement à l'extension $k(x)/k(y)$ s'annule sur W_b . Il est clair que l'entier $r = r(b) = v_{W_b}(N\, h_t)$ ne dépend pas du chois de t . Nous allons montrer qu'il ne dépend pas du choix de b . En effet, soit u une fonction sur U telle que $(du)_b \neq 0$. La fonction

.../...

$t_1 = u - u(b)$ sur V est un paramètre uniformisant de b sur V. Alors $r = r(b)$ est l'unique entier tel que la fonction

$$f_b(x) = N(\prod_i (u(x_i) - u(b))/(s(x_1+\ldots+ x_n - b))^r$$

soit génériquement inversible sur $\psi_i^{-1}(b)$ pour tout i ; si v est un point générique de V sur $k(b)$, la fonction $f_v(x)$ est alors a fortiori génériquement inversible sur $\psi_i^{-1}(v)$ pour tout i. Autrement dit, on a $r(b) = r(v)$, ce qui montre bien que r ne dépend pas de b.

Soit maintenant Z une sous-variété de codimension 1 quelconque de V, définie sur k, et soit z un point générique de Z sur k. L'ensemble $(\mu^{-1})_e(z)$ est nécessairement fini (car sinon $(\mu^{-1})_e(Z)$ aurait une composante de dimension $n = \dim V^n$, ce qui est impossible). Soient $u = (u_{\ell_1},..,u_{\ell_n})$ les composants de $(\mu^{-1})_e(z)$ $(1 \leq \ell \leq q)$.

Il existe une fonction f sur A, définie sur k, qui représente X au point z. La fonction $f' = f \circ \mu$ sur V^n représente alors $\mu^{-1}(X)$ en l'un quelconque des points u_ℓ. D'autre part, on peut trouver une fonction g sur V, définie sur k, représentant $X.V$ en l'un quelconque des points $u_{\ell i}$ $(1 \leq \ell \leq q\ ,\ 1 \leq i \leq n)$. Le diviseur $\psi_i^{-1}(X.V)$ est alors représenté par $g_i(x) = g(x_i)$ au point u_ℓ quels que soient ℓ et i. Explicitons le cycle $X.V$ sous la forme $X.V = \sum_j m_j (a_j)$ (avec la même convention d'écriture que plus haut). D'après ce qui précède, la norme Ng_i de g_i relativement à l'extension $k(x)/k(y)$ représente le diviseur $r \sum_j W_{a_j}$ au point z.

.../...

Compte tenu de (10), il existe une fonction h sur V^n, définie sur k, telle que

$$\mathrm{div}(h) = \mu^{-1}(X) - \sum_i \psi_i^{-1}(X.V).$$

La fonction $h f'^{-1}(\prod_i g_i)$ sur V^n est inversible en chacun des points u. Donc sa norme $(Nh) f^{-q}(\prod_i Ng_i)$ est une fonction sur A inversible en z, et on a

$$v_Z(Nh) - q\, v_Z(f) + \sum_i v_Z(Ng_i) = 0,$$

d'où

$$v_Z(Nh) - q\, v_Z(X) + r\, v_Z(\textstyle\sum_j W_{a_j}) = 0.$$

Cette relation ayant lieu quel que soit Z, on a

$$\mathrm{div}(Nh) = qX - r \textstyle\sum_j W_{a_j} \sim 0$$

Tenant compte du th. du carré (th. 3, coroll. 2), on en déduit

$$qX - r(W_a - W) - dW \sim 0$$

en posant $d = \deg(X.V)$. Or on a $X \equiv 0$, et $W_a - W \equiv 0$. On a donc $dW \equiv 0$. Comme W est positif $\neq 0$, ceci implique $d = 0$, d'après le th. 7, d'où

$$qX \sim r(W_a - W), \qquad \text{C.Q.F.D.}$$

Corollaire. Soient A et V comme dans le théorème précédent. Si X est un diviseur $\equiv 0$ sur A, tel que $S_A(X * V) = 0$, il existe un entier $m > 0$ tel que $mX \sim 0$.

Deux diviseurs X et Y sur A (ou, plus généralement sur une variété sans point multiple quelconque) sont dits numériquement équivalents si on a $\deg(X * V) = \deg(Y * V)$ pour toute courbe V sur A. L'ensemble des diviseurs numériquement équivalents à zéro sur A (i.e. tels que $\deg(X * V) = 0$ quelle que soit V) est un sous-groupe $\mathfrak{D}_n(A)$ du groupe

.../...

$\mathfrak{D}(A)$ de tous les diviseurs sur A, admettant comme sous-groupe le groupe $\mathfrak{D}_\ell(A)$ des diviseurs linéairement équivalents à zéro.

THEOREME 11.

Soit A une variété abélienne. Tout diviseur $\equiv 0$ sur A est numériquement équivalent à zéro.

Démonstration. Soient V, W, q, r, X comme dans le th. 10, et soit V_o une courbe quelconque sur A. Posons $d_o = \deg(X * V_o)$. On a, d'après le th. 10, $q\, d_o = r \deg((W_a - W) * V_o)$. On peut trouver un diviseur $W' \sim W$ sur A tel que le symbole $(W'_a - W').V_o$ ait un sens ; on a alors $q\, d_o = r \deg((W'_a - W').V_o)$. Désignant par ψ le morphisme $A \times A \to A$ tel que $\psi(x,y) = x-y$, on a, quel que soit $b \in A$, $W'_b = Z(b)$, en posant $Z = \psi^{-1}(W')$ (Cf. Démonstration du coroll. 1 du th. 3). Compte tenu de III, 3, lemme 5, on en déduit $W'_b \cdot V_c = Z_o(b)$, en posant $Z_o = Z.(A \times V)$. On a donc $\deg((W_a - W) * V_o) = \deg Z_o(a) - \deg Z_o(0)$. Or si k est un corps de définition de V, W, X, et si u est un point générique de A sur k, on a $\deg Z_o(u) = \deg Z_o(a) = \deg Z_o(0)$, d'après III, 4, lemme 10. On a donc $d_o = 0$ C.Q.F.D.

THEOREME 12.

Soient A et V comme dans le th. 10. Pour tout diviseur Y sur A, l'application $\alpha = \alpha_Y : A \to A$ obtenue en posant

$$\alpha(a) = S_A((Y_a - Y) * V)$$

est un endomorphisme de A, pour la structure de variété abélienne. Pour que α soit surjectif (i.e. soit une isogénie)

.../...

il faut et il suffit que Y soit non dégénérée.

En particulier, le diviseur $W = V^{(n-1)}$ intervenant dans le th. 10 est non dégénéré.

Demonstration. Le point $a \in A$ étant fixé, soit k un corps de définition de A, V, Y, a, et considérons deux points $u \in A$ et $v \in V$ génériques indépendants sur k. Il existe comme on sait, un diviseur Z sur $A \times A$ tel qu'on ait $Y_b - Y = Z(b)$ pour tout $b \in A$. Soit h une fonction sur $A \times A$, définie sur k, qui représente Z au point (a,v), et posons $Z' = Z - \mathrm{div}(h)$. Alors on a $v \notin \mathrm{supp}\, Z'(a)$. Donc le symbole $Z'(a).V$ est défini. On a d'autre part $Z' \sim Z$, donc d'après III, 3, lemme 6, $Z'(a) \sim Z(a)$, d'où $S_A((Y_a - Y) * V) = S_A(Z'(a).V)$. Comme Z est encore représenté par h au point (u,v), on a de même $S_A((Y_u - Y) * V) = S_A(Z'(u).V)$. Le point $y = S_A(Z'(u).V)$ de A est rationnel sur $k(u)$, et il existe donc une application rationnelle $\bar{\alpha} : A \to A$, définie sur k, telle que $\bar{\alpha}(u) = y$. D'après III, 8, th. 7, on voit, en utilisant la jacobienne de V, que $\bar{\alpha}$ ne dépend pas de a ni de h ; on a de plus $\bar{\alpha}(0) = 0$. Donc, d'après I, 6, th. 8, coroll. 1, $\bar{\alpha}$ est un endomorphisme pour la structure de variété abélienne. Compte tenu de III, 3, lemme 5, on a $Z'(u).V = T(u)$, et de même $Z'(a).V = T(a)$, en posant $T = Z'.(A \times V)$. D'après III, 4, lemme 10, le diviseur $T(a)$ sur V est l'unique spécialisation de $T(u)$ compatible avec $u \to a$ sur k. Donc $S_A(T(a))$ est l'unique spécialisation de $S(T(u)) = \bar{\alpha}(u)$ compatible avec $u \to a$ sur k. On en déduit $S(T(a)) = \bar{\alpha}(a)$,

.../...

i.e. $\alpha(a) = \overline{\alpha}(a)$. On a donc $\alpha = \overline{\alpha}$.

Soit maintenant $c \in \ker \alpha$, et posons $Y' = Y_c - Y$. On a $Y' \equiv 0$, et $S_A(Y' * V) = 0$. D'après le coroll. 1 du th. 10, il existe un entier $m > 0$ tel que $m Y' \sim 0$, et on a donc $m(Y_c - Y) \sim Y_{mc} - Y \sim 0$, d'où $m c \in \ker \eta_Y$. On a donc montré que $m \ker \alpha_Y \subset \ker \eta_Y$. Il est clair d'autre part que $\ker \eta_Y \subset \ker \alpha_Y$. Puisque $\ker(m \delta)$ est fini, $\ker \alpha_Y$ est fini si et seulement si $\ker \eta_Y$ est fini, i.e. si Y est non dégénéré.

Remarquons enfin que, pour tout diviseur Y sur A, on a $Y_b - Y \equiv 0$ pour tout $b \in A$; on a donc, avec les notations du th. 10, $q(Y_b - Y) \sim r(W_a - W) \sim W_{ra} - W$, en posant $a = \alpha_Y(b)$. En passant aux diviseurs induits sur V , on en déduit $q \operatorname{Im} \alpha_Y \subset \operatorname{Im} \alpha_W$. Prenons Y non dégénéré. Alors α_Y est surjectif. Puisque $q\delta$ est surjectif, il en est de même de α_W , i.e. W est non dégénéré C.Q.F.D.

THEOREME 13.

Soit A une variété abélienne, et soit Y un diviseur non dégénéré sur A . Si X est un diviseur sur A , les conditions suivantes sont équivalentes

(a) - $X \equiv 0$

(b) - Il existe un entier $m > 0$ tel que $m X \equiv 0$

(c) - Il existe un entier $m > 0$ et un point a A tels que $m X \sim Y_a - Y$.

Démonstration. Il est clair que (c) $\Longrightarrow$ (b) et que (b) $\Longrightarrow$ (a). Montrons que (a) $\Longrightarrow$ (c). En effet, α_Y est surjectif, d'après le th. 12. On peut donc trouver un point $b \in A$

.../...

tel que $S_A(X * V) = a_Y(b) = S_A((Y_b - Y) * V)$, on a $X \equiv 0$ par hypothèse et $Y_b - Y \equiv 0$ d'après le théorème du carré. D'après le coroll. 1 du th. 10, il existe un entier $m > 0$ tel que $mX \sim m Y_b - Y$, d'om $m X \sim Y_{mb} - Y$; C.Q.F.D.

10. Complément : équivalence algébrique :

Soit V une variété sans point multiple. On dit que deux diviseurs X et Y sur V sont algébriquement équivalents s'il existe une variété U, un diviseur Z sur le produit $U \times V$, et deux points a et $b \in U$, simples sur U, tels qu'on ait $X = Z(a)$ et $Y = Z(b)$. On montre qu'on obtient une définition équivalente en exigeant de plus que U soit une courbe, ou en exigeant que U soit la jacobienne d'une courbe. On montre en outre que l'ensemble de tous les diviseurs algébriquement équivalents à zéro sur V forment un sous-groupe $\mathfrak{D}_a(V)$ du groupe $\mathfrak{D}(V)$. Il est clair que $\mathfrak{D}_\ell(V) \subset \mathfrak{D}_a(V)$; en raisonnant comme dans la démonstration du th. 11, on voit aussi que $\mathfrak{D}_a(V) \subset \mathfrak{D}_n(V)$, de sorte qu'on a $\mathfrak{D}(V) \subset \mathfrak{D}_a(V) \subset \mathfrak{D}_n(V) \subset \mathfrak{D}(V)$. Dans le cas d'une variété abélienne A, on a en outre $\mathfrak{D}_a(A) \subset \mathfrak{D}'(A) \subset \mathfrak{D}_n(A)$. La première de ces deux inclusions résulte du th. du carré (th. 3, coroll. 1) ; la seconde résulte du th. 11. Le th. 13 s'interprète par le fait que le groupe quotient $\mathfrak{D}'(A)/\mathfrak{D}_a(A)$ est de torsion, i.e. que tous ses éléments sont d'ordre fini. On sait en fait démontrer que $\mathfrak{D}_a(A) = \mathfrak{D}'(A) = \mathfrak{D}_n(A)$, i.e. que l'équivalence $\equiv$ sur une variété abélienne coïncide avec l'équivalence algébrique et avec l'équivalence numérique.

N° d'impression 367

2ème trimestre 1979