SUR LES COURBES ALGÉBRIQUES ET LES VARIÉTÉS QUI S'EN DÉDUISENT

Par André WEIL.

Dans le développement de la géométrie sur les variétés algébriques, les variétés déduites des courbes algébriques ont toujours occupé une place privilégiée, due à la fois à l'importance de leurs propriétés particulières, et à la simplicité de leur mode de génération, qui fait de leur étude une introduction naturelle à toute théorie générale. Déjà dans les mémorables travaux de Riemann, la variété jacobienne d'une courbe algébrique joue un rôle essentiel, bien qu'encore implicite ; et la théorie des correspondances sur une courbe, abordée pour la première fois dans toute sa généralité par Hurwitz au moyen des méthodes de Riemann, et reprise ensuite par les géomètres italiens, et en particulier Castelnuovo et Severi par voie algébrico-géométrique, n'est pas autre chose, comme ces derniers l'ont bien mis en évidence, que l'étude de la variété des couples de points d'une courbe algébrique, c'est-à-dire du produit de la courbe par elle-même.

C'est principalement de ces variétés qu'il va être question dans le présent mémoire et dans ceux qui lui feront suite : je me propose d'en reprendre l'étude ab oro, par des méthodes apparentées à celles de l'école italienne, mais non sans tirer parti en même temps (autant qu'il est possible lorsqu'il s'agit de corps abstraits) des lumières que jettent sur ces questions la topologie et les méthodes transcendantes.

Ce n'est pas le lieu de revenir ici sur l'insuffisance, maintes fois signalée, des démonstrations des géomètres italiens : j'espère au contraire montrer par l'exemple qu'il est possible de donner à leurs méthodes toute la rigueur nécessaire sans leur rien faire perdre en puissance ni en fécondité. La plupart des résultats qui seront démontrés ici n'ont rien d'essentiellement nouveau dans le cas où le corps des constantes est celui des nombres complexes ; mais, comme on le verra, quelques-unes des applications les plus intéressantes de notre théorie portent sur le cas où la caractéristique du corps de base n'est pas nulle.

Nous aurions eu le droit, compte tenu de la différence de langage, d'adapter à notre usage les résultats des travaux de F. K. Schmidt, de H. Hasse, et d'autres auteurs, sur les corps de fonctions algébriques d'une variable, travaux qui contiennent entre autres la démonstration du théorème de Riemann-Roch dans toute sa généralité, c'est-à-dire pour un corps de base quelconque. Il a paru préférable de retrouver d'abord ces mêmes résultats directement, sans rien supposer connu des travaux en question ; c'est ce qui sera fait dans la première partie, par la considération du produit de la courbe par elle-même, dont justement l'étude détaillée formera le sujet principal de ce qui doit suivre : dans le § I, nous donnerons la démonstration, par cette voie, du théorème de

Retranscription en Latex Denise Vella-Chemla, juillet 2022.

Riemann-Roch et des résultats qui s'y rattachent ; le § II contient la théorie des différentielles sur une courbe algébrique. La deuxième partie est consacrée à la théorie élémentaire des correspondances sur une courbe, et aux applications de cette théorie, parmi lesquelles se trouvera entre autres la démonstration de l'hypothèse de Riemann et de la conjecture d'Artin, pour une courbe à corps de base fini. Dans le mémoire suivant se trouveront les résultats plus profonds de la théorie des correspondances qui dépendent de l'étude de la variété jacobienne et des représentations matricielles déduites des diviseurs d'ordre fini.

PREMIÈRE PARTIE
THÉORIE DES COURBES

§ I. Le théorème de Riemann-Roch.

1. Il sera constamment fait usage des définitions et des résultats de mon livre *Foundations of Algebraic Geometry*[1], qui seront supposés connus du lecteur.

Nous renvoyons à F-VII$_1$, pour la définition des Variétés, ou variétés abstraites : comme ce sera uniquement de variétés abstraites qu'il sera question, nous nous dispenserons de la majuscule employée dans F-VII et F-VIII pour les désigner. Par une *courbe*, nous entendons une variété (abstraite) de dimension 1.

Les conventions et définitions étant celles de F-I$_1$, nous supposons donnés une fois pour toutes une *courbe complète* Γ sans point multiple (pour la définition des variétés complètes, cf. F-VII$_1$) et un corps de définition k de Γ qui sera appelé le *corps de base*. Aux restrictions apportées dans F-I$_1$, à l'emploi du mot "corps", nous ajoutons la suivante : *tout corps dont il sera question par la suite est supposé contenir le corps de base k.*

Soient K un corps, et M un point générique de Γ par rapport à K : d'après F-VIII$_1$, la relation $z = \varphi(M)$ détermine une correspondance biunivoque entre les éléments du corps $K(M)$ et les fonctions φ sur Γ qui ont K pour corps de définition ; et il résulte de F-VIII$_1$ que cette correspondance est un isomorphisme entre $K(M)$ et le corps abstrait Ω_K des fonctions sur Γ qui ont K pour corps de définition. De plus, cet isomorphisme applique le sous-corps K de $K(M)$ sur l'ensemble des fonctions constantes appartenant à Ω_K, comme il résulte du lemme suivant :

LEMME 1. — Soient K un corps, M un point générique de Γ par rapport à K, z un élément de $K(M)$, et φ la fonction sur Γ définie par rapport à K par $z = \varphi(M)$. Alors, si φ est constante, z est un élément de K ; et, si φ n'est pas constante, z est une quantité variable sur K.

Considérons en effet le graphe de φ, c'est-à-dire (F-VIII$_1$, pr. 2) le lieu de $M \times (z)$ par rapport à K sur le produit $\Gamma \times D$ de Γ et de la droite projective D ; et considérons la projection de ce graphe sur D, qui est le lieu de (z) par rapport à K sur D. Comme cette projection admet K pour corps de définition, elle ne peut se réduire

[1] A. Weil, *Foundations of Algebraic Geometry*, Am. Math. Soc. Colloq, vol. 29, New-York 1946. Nous renverrons à ce livre par la lettre F, saisis de l'indication du chapitre et du § ; par exemple F-IV$_2$, signifiera Found. of. Alg. Geom., chap. IV, § 3 ; F-IV$_2$ th. 6 signifiera le théorème 6 de F-IV$_2$, F-IV$_2$, th. 6, cor. 3 signifiera le corollaire 3 du théorème 6 de F-IV$_2$; F-IV$_4$ pr. 10 signifiera la proposition 10 de F-IV$_4$, etc.

à un point que si z est dans K ; alors le graphe de φ est la variété $\Gamma \times (z)$, et φ est la constante z. Si au contraire la projection sur D du graphe de φ n'est pas un point, alors elle n'est autre que D, et φ n'est pas constante ; en ce cas, z est de dimension 1 sur K. On observera que notre démonstration n'a pas fait usage du fait que Γ est de dimension 1 ; notre lemme reste valable pour une variété de dimension quelconque.

Pour la commodité du langage, nous identifierons une fonction constante sur Γ, prenant en tout point la valeur c, avec la quantité c ; le corps abstrait des constantes sur Γ se trouve ainsi identifié avec le "domaine universel" $\mathbf{K}$ (cf. F-1_1)[2]. Avec cette convention, on voit que l'isomorphisme entre $K(M)$ et Ω_K dont la définition a été rappelée plus haut laisse invariants les éléments de K.

Dans ce qui suit, nous aurons à nous servir du lemme suivant, sur l'indépendance linéaire des fonctions sur Γ :

Lemme 2. — Soient φ_λ des fonctions sur Γ, K un corps de définition commun pour ces fonctions, et M un point générique de Γ par rapport à K. Alors, pour que les φ_λ soient linéairement indépendantes sur le corps des constantes, il faut et il suffit qu'elles le soient sur le corps K ; et pour cela, il faut et il suffit que les quantités $z_\lambda = \varphi_\lambda(M)$ soient linéairement indépendantes sur K.

Supposons en effet qu'on ait une relation $\sum_\lambda c_\lambda \varphi_\lambda = 0$, à coefficients constants c_λ non tous nuls ; soient K' un corps contenant K et les c_λ, et M' un point générique de Γ par rapport à K', donc a fortiori par rapport à K. Les quantités $z'_\lambda = \varphi_\lambda(M')$ sont alors des éléments de $K(M')$, et l'on a $\sum_\lambda c_\lambda z'_\lambda = 0$. Comme, en vertu de F-$\mathrm{IV}_2$, th. 1. K' et $K(M')$ sont linéairement disjoints sur K (cf. F-I_2), cette dernière relation implique que les z'_λ ne sont pas linéairement indépendants sur K, donc qu'ils satisfont à une relation $\sum_\lambda \bar{c}_\lambda z'_\lambda = 0$ à coefficients $\bar{c}_\lambda$ dans K et non tous nuls. On a alors $\sum_\lambda \bar{c}_\lambda \varphi_\lambda = 0$. Quant à la dernière assertion de notre lemme, c'est une conséquence de l'isomorphisme entre $K(M)$ et Ω_λ. La démonstration ci-dessus, et le présent lemme, restent d'ailleurs valables si, au lieu de Γ, on considère une variété de dimension arbitraire.

2. L'*équivalence* des diviseurs sur Γ, qui sera notée $\sim$, devra toujours être entendue au sens de l'équivalence linéaire (cf. F-IX_7). Autrement dit, dans le groupe additif des diviseurs sur Γ, on considère l'ensemble des diviseurs de la forme (φ), où φ est une

[2]Pour abréger, nous dirons parfois "corps des constantes" au lieu de "corps abstrait des constantes". On observera que, dans notre langage, le "corps de base" est le corps k, et le "corps (abstrait) des constantes" est le "domaine universel" K ; ces expressions sont donc à distinguer soigneusement l'une de l'autre.

fonction quelconque sur Γ, autre que la constante 0 ; ce dernier ensemble, en vertu de F-VIII$_2$, th. 6. forme un sous-groupe du groupe de tous les diviseurs ; on écrira $\mathfrak{a} \sim 0$ si $\mathfrak{a}$ est un élément de ce sous-groupe, et $\mathfrak{a} \sim \mathfrak{b}$ si $\mathfrak{a}$ et $\mathfrak{b}$ appartiennent à une même classe suivant ce sous-groupe, c'est-à-dire s'il existe une fonction φ sur Γ, telle que l'on ait $(\varphi) = \mathfrak{a} - \mathfrak{b}$. Le groupe quotient du groupe de tous les diviseurs par le groupe des diviseurs de la forme (φ) sera appelé le groupe additif des classes de diviseurs sur Γ, et par une *classe de diviseurs* sur Γ, on entendra un élément de ce groupe quotient.

Le résultat suivant n'est autre chose que l'application, au cas qui nous occupe ici, du principe général en vertu duquel l'équivalence linéaire implique l'équivalence numérique (cf. F-IX$_7$).

Proposition 1. — Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux diviseurs sur Γ : alors la relation $\mathfrak{a} \sim \mathfrak{b}$ entraîne $\deg(\mathfrak{a}) = \deg(\mathfrak{b})$.

Soit en effet φ une fonction sur Γ, telle que $(\varphi) = \mathfrak{a} - \mathfrak{b}$. Si φ est constante, on a $(\varphi) = 0$ d'après F-VIII$_2$, th. 3. cor. 3. donc $\mathfrak{a} = \mathfrak{b}$. Supposons φ non constante ; et soit Λ le graphe de φ. Alors Λ est une courbe sur $\Gamma \times D$ qui a la projection D sur D ; dans ces conditions, il résulte des définitions (F-VIII$_2$), de F-VIII$_2$ th. 1. et de F-VII$_6$, th. 15, que l'on a $\deg[(\varphi)_0] = \deg[(\varphi)_\infty] = [\Lambda : D]$, donc $\deg[(\varphi)] = 0$, c'est-à-dire $\deg(\mathfrak{a} - \mathfrak{b}) = 0$.

Proposition 2. — Soit $\mathfrak{a}$ un diviseur sur Γ ; alors, pour qu'il existe sur Γ un diviseur positif $\mathfrak{b}$ équivalent à $\mathfrak{a}$, il faut et il suffit qu'il existe une fonction φ sur Γ, autre que la constante 0, telle que $(\varphi) \succ -\mathfrak{a}$. Si de plus $\mathfrak{a}$ est rationnel par rapport à un corps K, et équivalent à un diviseur positif sur Γ, il existe un diviseur positif $\mathfrak{b}$ sur Γ, rationnel par rapport à K, et équivalent à $\mathfrak{a}$; et, pour qu'il en soit ainsi, il faut et il suffit qu'il existe une fonction φ sur Γ, autre que la constante 0, ayant K pour corps de définition, et telle que $(\varphi) \succ -\mathfrak{a}$.

Si en effet $\mathfrak{b}$ est un diviseur positif, équivalent à $\mathfrak{a}$, et que φ soit une fonction telle que $(\varphi) = \mathfrak{b} - \mathfrak{a}$, on a bien $(\varphi) \succ -\mathfrak{a}$; réciproquement, si φ est telle que $(\varphi) \succ -\mathfrak{a}$, le diviseur $\mathfrak{b} = (\varphi) + \mathfrak{a}$ est positif et équivalent à $\mathfrak{a}$. Le reste de notre proposition est une conséquence immédiate de ce qui précède et de F-VIII$_2$. th. 10.

Si $\mathfrak{a}$ est un diviseur quelconque sur Γ, nous désignerons une fois pour toutes par $L(\mathfrak{a})$ l'ensemble composé de la constante 0 et de toutes les fonctions φ sur Γ telles que $(\varphi) \succ -\mathfrak{a}$. Il résulte de F-VIII$_2$, th. 6. que toute combinaison linéaire d'éléments de $L(\mathfrak{a})$, à coefficients constants, appartient à $L(\mathfrak{a})$: $L(\mathfrak{a})$ est donc un module sur le corps des constantes : le rang (fini ou infini) de ce module sera désigné, une fois pour toutes, par $l(\mathfrak{a})$: on va démontrer dans un instant que $l(\mathfrak{a})$ est toujours un entier

fini. Il résulte de F-VIII$_2$ th. 2, que $L(0)$ est le corps des constantes, donc que l'on a $l(0) = 1$, et que, si $\mathfrak{a}$ est un diviseur positif autre que 0, le module $L(-\mathfrak{a})$ se réduit à la constante 0, de sorte qu'on a $l(-\mathfrak{a}) = 0$. Pour que le corps des constantes soit contenu dans $L(\mathfrak{a})$, il faut et il suffit qu'on ait $\mathfrak{a} \succ 0$; lorsqu'il en est ainsi, on a donc $l(\mathfrak{a}) \geqslant 1$.

3. Si les diviseurs $\mathfrak{a}$ et $\mathfrak{b}$ sont équivalents, c'est-à-dire s'il existe une fonction θ telle que $(\theta) = \mathfrak{a} - \mathfrak{b}$, alors (d'après F-VIII$_2$, th. 6) la relation $\psi = \theta\varphi$ définit une correspondance linéaire et biunivoque entre les éléments φ de $L(\mathfrak{a})$ et les éléments ψ de $L(\mathfrak{b})$: il s'ensuit qu'on a alors $l(\mathfrak{a}) = l(\mathfrak{b})$.

Proposition 3. — Soit $\mathfrak{a}$ un diviseur sur Γ, rationnel par rapport à un corps K. Alors l'ensemble de toutes les fonctions de $L(\mathfrak{a})$ qui ont K pour corps de définition est un module de rang $l(\mathfrak{a})$ sur le corps K ; et toute base de ce module est aussi une base du module $L(\mathfrak{a})$ sur le corps des constantes.

C'est là une conséquence immédiate du lemme 2 (n° 1), et de F-VIII$_2$, th. 10.

Proposition 4. — Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux diviseurs sur Γ, tels que l'on ait $\mathfrak{a} \succ \mathfrak{b}$. Alors on a $L(\mathfrak{a}) \supset L(\mathfrak{b}), l(\mathfrak{a}) \geqslant l(\mathfrak{b})$, et

$$l(\mathfrak{a}) - \deg(\mathfrak{a}) \leqslant l(\mathfrak{b}) - \deg(\mathfrak{b}).$$

De plus, $\mathfrak{a}$ étant un diviseur quelconque, on a

$$l(\mathfrak{a}) \leqslant \max[\deg(\mathfrak{a}) + 1, 0] \ ;$$

et par suite $l(\mathfrak{a})$ est toujours un entier fini.

La relation $L(\mathfrak{a}) \supset L(\mathfrak{b})$ résulte des définitions, et entraîne $l(\mathfrak{a}) \geqslant l(\mathfrak{b})$. Posons $\mathfrak{m} = \mathfrak{a} - \mathfrak{b}$ et $m = \deg(\mathfrak{m})$; nous avons à démontrer que, si $\mathfrak{m} \succ 0$, on a $l(\mathfrak{a}) \leqslant l(\mathfrak{b}) + m$; c'est ce que nous ferons par récurrence sur m. Si $m = 1$, $\mathfrak{m}$ se réduit à un point M ; nous avons donc à démontrer d'abord que l'on a $l(\mathfrak{b} + M) \leqslant l(\mathfrak{b}) + 1$. Il en est bien ainsi si $L(\mathfrak{b} + M) = L(\mathfrak{b})$: supposons donc qu'il existe dans $L(\mathfrak{b} + M)$ une fonction φ_0 qui n'appartienne pas à $L(\mathfrak{b})$. Soit b le coefficient de M dans le diviseur $\mathfrak{b}$: posons $\mathfrak{c} = \mathfrak{b} - b.M$, de sorte que M ne figure pas dans l'expression réduite du diviseur $\mathfrak{c}$, ou, comme nous dirons, n'est pas un *composant* de $\mathfrak{c}$. Alors $L(\mathfrak{b})$ est l'ensemble des fonctions φ telles qu'on ait à la fois $(\varphi) \succ -\mathfrak{c}$, et $v_M(\varphi) \geqslant -b$, et $L(\mathfrak{b} + M)$ est l'ensemble des fonctions φ telles qu'on ait à la fois $(\varphi) \succ -\mathfrak{c}$ et $v_M(\varphi) \geqslant -b - 1$. On a donc

$$v_M(\varphi_0) = -b - 1;$$

et $L(\mathfrak{b})$ est l'ensemble des fonctions φ de $L(\mathfrak{b}+M)$ telles que $v_M(\varphi) \geqslant -b$. Soit φ une fonction quelconque de $L(\mathfrak{b}+M)$: d'après F-VIII$_2$, th. 6, on a alors $v_M(\varphi/\varphi_0) \geqslant 0$, c'est-à-dire que (d'après F-VIII$_2$, th. 3) la fonction φ/φ_0 est finie en M ; si donc c est la valeur en M de cette dernière fonction, la fonction $\varphi/\varphi_0 - c = (\varphi - c\varphi_0)/\varphi_0$ prend en M la valeur 0, de sorte que l'on a (F-VIII$_2$, th. 3)

$$v_M[(\varphi - c\varphi_0)/\varphi_0] \geqslant 1.$$

donc, d'après F-VIII$_2$ th. 6, $v_M(\varphi - c\varphi_0) \geqslant -b$. Comme d'ailleurs φ et φ_0, donc aussi $\varphi - c\varphi_0$ sont dans $L(\mathfrak{b}+M)$, il résulte de là que $\varphi - c\varphi_0$ est dans $L(\mathfrak{b})$. Ceci démontre qu'en adjoignant la fonction φ_0 à une base du module $L(\mathfrak{b})$, on obtient une base du module $L(\mathfrak{b}+M)$, de sorte qu'on a, dans le cas que nous considérons $L(\mathfrak{b}+M) = l(\mathfrak{b}) + 1$. Revenons maintenant au cas où $\mathfrak{m}$ est un diviseur positif de degré quelconque, et montrons, par récurrence sur le degré m de $\mathfrak{m}$, qu'on a alors $l(\mathfrak{b}+\mathfrak{m}) \leqslant l(\mathfrak{b}) + m$. Soit en effet M l'un des composants de $\mathfrak{m}$: on a alors

$$\mathfrak{m} - M \succ 0, \ \deg(\mathfrak{m} - M) = m - 1.$$

donc, par l'hypothèse de récurrence, $l(\mathfrak{b}+\mathfrak{m}-M) \leqslant l(\mathfrak{b}) + m - 1$. D'autre part, d'après ce qu'on vient de démontrer, on a

$$l(\mathfrak{b}+\mathfrak{m}) \leqslant l(\mathfrak{b}+\mathfrak{m}-M) + 1 \ ;$$

on a donc bien $l(\mathfrak{b}+\mathfrak{m}) \leqslant l(\mathfrak{b})+m$. Ceci démontre la première partie de la proposition. Soit maintenant $\mathfrak{a}$ un diviseur quelconque ; si l'on a $l(\mathfrak{a}) > 0$, $\mathfrak{a}$ est, d'après la prop. 2, équivalent à un diviseur positif $\mathfrak{a}'$, et l'on a alors $l(\mathfrak{a}) = l(\mathfrak{a}'), \deg(\mathfrak{a}) = \deg(\mathfrak{a}')$, et $\mathfrak{a}' \succ 0$: si donc nous appliquons aux diviseurs $\mathfrak{a}'$ et 0 la première partie de notre proposition, nous obtenons $l(\mathfrak{a}') - deg(\mathfrak{a}') \leqslant l(0) = 1$. Ceci achève la démonstration.

PROPOSITION 5. — Il existe un entier G tel que l'on ait

$$l(\mathfrak{a}) \geqslant \deg(\mathfrak{a}) - G$$

quel que soit le diviseur $\mathfrak{a}$ sur Γ.

Soient φ une fonction non constante sur Γ, K un corps de définition pour φ, et M un point générique de Γ par rapport à K : posons $x = \varphi(M), \mathfrak{d} = (\varphi)_\infty$, et $d = [K(M) : K(x)]$. Le graphe Λ de φ est alors une courbe sur $\Gamma \times D$, ayant D pour projection sur D, et telle que $[\Lambda : D] = d$; en vertu de F-VIII$_2$. th. 1. et de F-VII$_6$, th. 15, on a donc $\deg(\mathfrak{d}) = d$. Comme d est le degré de $K(M)$ sur $K(x)$, il y a, dans $K(M)$, d quantités $z_1, \ldots, z_d$, linéairement indépendantes sur le corps $K(x)$; il n'y a alors entre les z_ρ aucune relation de la forme

$$\sum_\rho P_\rho(x).z_\rho = 0$$

où les $P_\rho(X)$ soient des polynomes non tous nuls dans $K[X]$: si donc n est un entier quelconque, les $(n+1)d$ quantités $x^\mu z_\rho$, pour $0 \leqslant \mu \leqslant n, 1 \leqslant \rho \leqslant d$, sont linéairement indépendantes sur le corps K. Si donc nous désignons par ψ_ρ, pour $1 \leqslant \rho \leqslant d$, la fonction sur Γ, définie par rapport à K par la relation $z_\rho = \psi_\rho(M)$, il résulte du lemme 2 que les $(n+1)d$ fonctions $\varphi^\mu \psi_\rho$ pour $0 \leqslant \mu \leqslant n, 1 \leqslant \rho \leqslant d$, sont linéairement indépendantes sur le corps des constantes. Choisissons maintenant (ce qui est évidemment possible) un diviseur $\mathfrak{m}$, tel que l'on ait, pour $1 \leqslant \rho \leqslant d, \mathfrak{m} \succ (\psi_\rho)_\infty$; on aura alors $(\psi_\rho) \succ -\mathfrak{m}$ pour $1 \leqslant \rho \leqslant d$, et par suite, d'après F-VIII$_2$, th. 6, $(\varphi^\mu \psi_\rho) \succ -n\mathfrak{d} - \mathfrak{m}$ pour $0 \leqslant \mu \leqslant n, 1 \leqslant \rho \leqslant d$. Il s'ensuit qu'on a, quel que soit n, $l(n\mathfrak{d} + \mathfrak{m}) \geqslant (n+1)d$.

Cela posé, soit $\mathfrak{a}$ un diviseur quelconque sur Γ ; soit $\mathfrak{a}'$ un diviseur positif tel que $\mathfrak{a} \prec \mathfrak{a}'$; on peut mettre $\mathfrak{a}'$ sous la forme

$$\mathfrak{a}' = \sum_\alpha A_\alpha + \sum_\beta A'_\beta,$$

où les A_α, sont tels que $\varphi(A_\alpha) \neq \infty$, et les A'_β tels que $\varphi(A'_\beta) = \infty$. Posons $\mathfrak{a}_0 = \sum_\alpha A_\alpha$, et $\mathfrak{a}_1 = \sum_\beta A'_\beta$; il y a alors un entier n_1 tel que l'on ait $\mathfrak{a}_1 \prec n_1\mathfrak{d}$. Posons $a_\alpha = \varphi(A_\alpha)$; on a $(\varphi - a_\alpha) \succ -\mathfrak{d}$; comme de plus $\varphi - a_\alpha$ prend la valeur 0 en A_α, A_α est un composant de $(\varphi - a_\alpha)_0$, de sorte qu'on a $(\varphi - a_\alpha) \succ A_\alpha - \mathfrak{d}$; si donc les A_α sont en nombre n_0, et qu'on pose $\theta = \prod_{\alpha=1}^{n_0} (\varphi - a_\alpha)$, on aura $(\theta) \succ \mathfrak{a}_0 - n_0\mathfrak{d}$. Il suit de là qu'on a $\mathfrak{a}' = \mathfrak{a}_0 + \mathfrak{a}_1 \prec (n_0 + n_1)\mathfrak{d} + (\theta)$, donc a fortiori, en posant de plus $n = n_0 + n_1, \mathfrak{a} \prec n\mathfrak{d} + \mathfrak{m} + (\theta)$, où $\mathfrak{m}$ est le diviseur positif défini plus haut. Posons $\mathfrak{b} = n\mathfrak{d} + \mathfrak{m} + (\theta)$; nous avons donc, d'après la prop. 4, $l(\mathfrak{a}) - \deg(\mathfrak{a}) \geqslant l(\mathfrak{b}) - \deg(\mathfrak{b})$. D'autre part, puisque $\mathfrak{b} \sim n\mathfrak{d} + \mathfrak{m}$, on a $l(\mathfrak{b}) = l(n\mathfrak{d} + \mathfrak{m})$, donc $l(\mathfrak{b}) \geqslant (n+1)d$ d'après ce qui a été démontré plus haut, et

$$\deg(\mathfrak{b}) = \deg(n\mathfrak{d} + \mathfrak{m}) = nd + \deg(\mathfrak{m}).$$

Il suit de là qu'on a $l(\mathfrak{a}) - \deg(\mathfrak{a}) \geqslant d - \deg(\mathfrak{m})$.

4. D'après la prop. 5, les valeurs prises par l'entier

$$\deg(\mathfrak{a}) - l(\mathfrak{a}) + 1,$$

quand on prend pour $\mathfrak{a}$ tous les diviseurs sur Γ, ont une borne supérieure qui est un entier fini ; cet entier sera appelé le *genre* de la courbe Γ, et sera désormais désigné par g. Comme on a en particulier $\deg(0) - l(0) + 1 = 0$, on a $g \geqslant 0$.

Soit $\mathfrak{a}$ un diviseur quelconque sur Γ : nous désignerons par $r(\mathfrak{a})$ l'entier $r(\mathfrak{a}) = \deg(\mathfrak{a}) - l(\mathfrak{a}) + 1 - g$. On a donc, quel que soit $\mathfrak{a}$:

$$l(\mathfrak{a}) = \deg(\mathfrak{a}) - g + 1 + r(\mathfrak{a}), \qquad r(\mathfrak{a}) \geqslant 0.$$

L'entier $r(\mathfrak{a})$ a alors les propriétés suivantes, qui résultent immédiatement de sa définition et des propriétés établies ci-dessus pour $l(\mathfrak{a})$. Si $\mathfrak{a} \sim \mathfrak{b}$, on a $r(\mathfrak{a}) = r(\mathfrak{b})$. Si $a \succ b$, on a $r(\mathfrak{a}) \leqslant r(\mathfrak{b})$ et

$$r(\mathfrak{a}) + \deg(\mathfrak{a}) \geqslant r(\mathfrak{b}) + \deg(\mathfrak{b}).$$

On a $r(0) = g$. donc $r(\mathfrak{a}) \leqslant g$ pour tout diviseur positif $\mathfrak{a}$. Enfin, par définition de g, il existe au moins un diviseur $\mathfrak{a}$ tel que $r(\mathfrak{a}) = 0$.

PROPOSITION 6. — Il existe un entier N tel que l'on ait $r(\mathfrak{a}) = 0$ pour tout diviseur $\mathfrak{a}$ sur Γ, de degré au moins égal à N.

Soit $\mathfrak{a}_0$, un diviseur tel que $r(\mathfrak{a}_0) = 0$; soit $\mathfrak{a}$ un diviseur tel que $\deg(\mathfrak{a} - \mathfrak{a}_0) \geqslant g$; on a $l(\mathfrak{a} - \mathfrak{a}_0) \geqslant \deg(\mathfrak{a} - \mathfrak{a}_0) - g + 1 \geqslant 1$, donc, d'après la prop. 2, il existe un diviseur positif $\mathfrak{b}$ tel que $\mathfrak{b} \sim \mathfrak{a} - \mathfrak{a}_0$. On a alors $\mathfrak{a} \sim \mathfrak{a}_0 + \mathfrak{b}$, et par suite $r(\mathfrak{a}) = r(\mathfrak{a}_0 + \mathfrak{b})$. Mais, puisque $\mathfrak{a}_0 + \mathfrak{b} \succ \mathfrak{a}_0$, on a $r(\mathfrak{a}_0 + \mathfrak{b}) \leqslant r(\mathfrak{a}_0) = 0$. L'entier $N = \deg(\mathfrak{a}_0) + g$ possède donc bien la propriété énoncée dans notre proposition.

PROPOSITION 7. — Soit $\mathfrak{a}$ un diviseur sur Γ, rationnel par rapport à un corps K ; soit M un point générique de Γ par rapport à K. Alors, pour que l'on ait $r(\mathfrak{a}) > 0$, il faut et il suffit qu'on ait $L(\mathfrak{a} + M) = L(\mathfrak{a})$.

En effet, si $L(\mathfrak{a} + M) = L(\mathfrak{a})$, on a $l(\mathfrak{a} + M) = l(\mathfrak{a})$, donc

$$r(\mathfrak{a} + M) = r(\mathfrak{a}) - 1,$$

donc $r(\mathfrak{a}) \geqslant 1$. Supposons d'autre part qu'on ait $L(\mathfrak{a}+M) \neq L(\mathfrak{a})$; comme $L(\mathfrak{a}+M)$ possède, d'après la prop. 3, une base formée de fonctions ayant $K(M)$ pour corps de définition, il existe donc une telle fonction φ dans $L(\mathfrak{a} + M)$ qui ne soit pas dans $L(\mathfrak{a})$. Soit N un point générique de Γ par rapport à $K(M)$; alors la quantité $z = \varphi(N)$ est dans $K(M, N)$. D'après la prop. 6, on peut choisir un entier n tel que l'on ait $r(\mathfrak{a} + \mathfrak{m}) = 0$ pour tout diviseur $\mathfrak{m}$ de degré au moins égal à n ; soient $M_1, \ldots, M_n$, n points génériques indépendants de Γ par rapport à $\overline{K}(N)$. Alors, pour $1 \leqslant \nu \leqslant n$, il y a un isomorphisme σ_ν, de $\overline{K}(M, N)$ sur $\overline{K}(M_\nu, N)$, laissant invariants tous les éléments de $\overline{K}(N)$, et transformant M en M_ν ; soit z_ν le transformé de z par cet isomorphisme, et soit φ_ν la fonction sur Γ, définie par rapport à $K(M_\nu)$ par $z_\nu = \varphi_\nu(N)$. Soient Λ le graphe de φ, et Λ_ν celui de φ_ν ; ce sont respectivement les lieux de $N \times (z)$ par rapport à $K(M)$, et de $N \times (z_\nu)$ par rapport à $K(M_\nu)$, sur $\Gamma \times D$. Il résulte alors de F-IV$_2$, th. 3. que Λ_ν est le transformé de Λ par σ_ν ; il suit de là, de F-IV$_4$, th. 8. cor. 3, de F-VI$_2$, th. 3, et de la définition des diviseurs (φ) et (φ_ν), que (φ_ν) est le transformé de (φ) par σ_ν. Comme σ_ν transforme $\mathfrak{a}$ en lui-même, et M en M_ν, on a donc $(\varphi_\nu) \succ -\mathfrak{a} - M_\nu$; et, puisqu'on n'a pas $(\varphi) \succ -\mathfrak{a}$, on n'a pas

$(\varphi_\nu) \succ -\mathfrak{a}$. Par conséquent, l'on a, pour $1 \leqslant \nu \leqslant n, v_{M_\nu}(\varphi_\nu) = -1$; et, puisque les M_ν sont distincts les uns des autres et distincts des composants de $\mathfrak{a}$, on a $v_{M_\nu}(\varphi_\mu) \geqslant 0$ pour $\mu \neq \nu$. Soient d'autre part θ_λ, pour $1 \leqslant \lambda \leqslant l(\mathfrak{a})$, des fonctions formant une base du module $L(\mathfrak{a})$; on a $v_{M_\nu}(\theta_\lambda) \geqslant 0$ quels que soient ν et λ. Il suit de là que les $n+l(\mathfrak{a})$ fonctions $\varphi_\nu, \theta_\lambda$ sont dans $L(\mathfrak{a} + \sum_\nu M_\nu)$, et qu'elles sont linéairement indépendantes. Supposons en effet qu'on ait une relation à coefficients constants $\sum_\nu c_\nu\varphi_\nu + \sum_\lambda d_\lambda\theta_\lambda = 0$; si l'on avait $c_\nu \neq 0$, on aurait $\varphi_\nu = -1/c_\nu \cdot \left(\sum_{\mu\neq\nu} c_\mu\varphi_\mu + \sum_\lambda d_\lambda\theta_\lambda\right)$, donc, d'après ce qui précède et d'après F-VIII$_2$, th. 6. $v_{M_\nu}(\varphi_\nu) \geqslant 0$; comme il n'en est pas ainsi, on a donc $c_\nu = 0$ quel que soit ν, donc $\sum_\lambda d_\lambda\theta_\lambda = 0$, donc $d_\lambda = 0$ quel que soit λ puisque les θ_λ sont linéairement indépendants par définition. On a donc $l\left(\mathfrak{a} + \sum_\nu M_\nu\right) \geqslant n+l(\mathfrak{a})$. Comme d'autre part on a $\deg\left(\mathfrak{a} + \sum_\nu M_\nu\right) = n + deg(\mathfrak{a})$, il s'ensuit qu'on a

$$r\left(\mathfrak{a} + \sum_\nu M_\nu\right) \geqslant r(\mathfrak{a}).$$

Comme le premier membre de cette dernière inégalité est nul en raison de la manière dont a été choisi l'entier n, on a donc bien $r(\mathfrak{a}) = 0$.

PROPOSITION 8. — Soit $\mathfrak{a}$ un diviseur sur Γ, rationnel par rapport à un corps K ; soient $M_1, \ldots, M_n$ des points génériques indépendants de Γ par rapport à K, en nombre quelconque ; et soit $\mathfrak{m} = \sum_{\nu=1}^{n} M_\nu$. Alors on a $r(\mathfrak{a}+\mathfrak{m}) = r(\mathfrak{a})-n$ et $l(\mathfrak{a}+\mathfrak{m}) = l(\mathfrak{a})$ si $n \leqslant r(\mathfrak{a})$; et l'on a $r(\mathfrak{a}+\mathfrak{m}) = 0$ et $l(\mathfrak{a}+\mathfrak{m}) = l(\mathfrak{a}) + n - r(\mathfrak{a})$ si $n \geqslant r(\mathfrak{a})$.

Soit d'abord $n = 1$. Alors, si $r(\mathfrak{a}) = 0$, on a $r(\mathfrak{a}+\mathfrak{m}) \leqslant r(\mathfrak{a}) = 0$, donc $r(\mathfrak{a}+\mathfrak{m}) = 0$, donc $l(\mathfrak{a}+\mathfrak{m}) = l(\mathfrak{a}) + 1$; si d'autre part $r(\mathfrak{a}) > 0$, on a, d'après la prop. 7. $l(\mathfrak{a}+\mathfrak{m}) = l(\mathfrak{a})$, donc

$$r(\mathfrak{a}+\mathfrak{m}) = r(\mathfrak{a}) - 1.$$

La démonstration pour n quelconque suit immédiatement de là par récurrence sur n.

PROPOSITION 9. — Soit $\mathfrak{a}$ un diviseur sur Γ, rationnel par rapport à un corps K, et tel que $l(\mathfrak{a}) > 0$. Alors, si M est un point générique de Γ par rapport à K, on a $l(\mathfrak{a} - M) = l(\mathfrak{a}) - 1$.

En effet, d'après la prop. 4, on a, soit $l(\mathfrak{a} - M) = l(\mathfrak{a})$, soit $l(\mathfrak{a} - M) = l(\mathfrak{a}) - 1$; et l'on a $L(\mathfrak{a} - M) \subset L(\mathfrak{a})$. Il nous suffit donc de montrer que, dans les conditions ci-dessus, on n'a pas $L(\mathfrak{a} - M) = L(\mathfrak{a})$. Puisque $l(\mathfrak{a}) > 0$, il existe, d'après la prop. 3, au moins une fonction φ dans $L(\mathfrak{a})$, autre que la constante 0, ayant K

pour corps de définition. Alors le diviseur $(\varphi) + \mathfrak{a}$ est rationnel par rapport à K. de sorte que tous ses composants sont algébriques sur K ; M ne peut donc être un de ces composants, de sorte qu'on n'a pas $(\varphi)+\mathfrak{a} \succ M$; donc φ n'est pas dans $L(\mathfrak{a}-M)$.

5. Jusqu'ici, nous n'avons pas eu à faire usage de la variété $\Gamma \times \Gamma$, produit de la courbe Γ par elle-même ; cette variété va au contraire jouer un rôle essentiel dans ce qui suit ; d'après F-VII$_3$, th. 6, cor., et F-IV$_6$, th. 13, c'est une variété complète et sans point multiple. Une fois pour toutes, on désignera par Δ la *diagonale* du produit $\Gamma \times \Gamma$. Si M est un point générique de Γ par rapport à k, Δ est, comme on sait (F-VI$_1$, et F-VII$_4$), le lieu de $M \times M$ par rapport à k sur $\Gamma \times \Gamma$; $M \times M$ et M sont alors des points génériques correspondants de Δ et de Γ, par rapport à k, dans une correspondance hirationnelle, partout birégulière, entre ces courbes, correspondance dans laquelle, à tout point de Δ, correspond sa projection sur l'un on l'autre facteur du produit $\Gamma \times \Gamma$. A tout cycle X sur Δ correspond donc, dans cette même correspondance, un cycle $\mathfrak{a}$ sur Γ qui peut s'écrire $\mathfrak{a} = pr_1 X = pr_2 X$, où pr_1 et pr_2 désignent comme d'habitude les projections algébriques, sur le premier et le second facteur de $\Gamma \times \Gamma$ respectivement, de cycles dans $\Gamma \times \Gamma$. Réciproquement, d'après F-VII$_6$, th. 17. cor. 3, si $\mathfrak{a}$ est un diviseur sur Γ, les expressions $\Delta.(\Gamma \times \mathfrak{a})$ et $\Delta.(\mathfrak{a} \times \Gamma)$ définissent un même cycle X sur Δ, à savoir celui qui satisfait à la relation $\mathfrak{a} = pr_1 X = pr_2 X$. En particulier, si P est un point quelconque de Γ, on a

$$\Delta.(\Gamma \times P) = \Delta.(P \times \Gamma) = P \times P.$$

Enfin, la correspondance birationnelle ci-dessus entre Δ et Γ détermine une correspondance biunivoque entre fonctions ψ sur Δ et fonctions φ sur Γ, telle que, siψ et φ se correspondent ainsi, on a, quel que soit P sur Γ, $\psi(P \times P) = \varphi(P)$; on a alors aussi

$$(\varphi) = pr_1[(\psi)] = pr_2[(\psi)],$$

et $(\psi) = \Delta.[\Gamma \times (\varphi)] = \Delta.[(\varphi) \times \Gamma]$ (cf. aussi F-VIII$_2$ th. 4, cor. 1-2, et F-VIII$_2$, th. 7).

Comme Δ est définie sur le corps k, il existe sur $\Gamma \times \Gamma$, d'après F-VIII$_3$, th. 9, des fonctions ω ayant k pour corps de définition et telles que $v_\Delta(\omega) = 1$. Soit ω une fonction quelconque sur $\Gamma \times \Gamma$ telle que $v_\Delta(\omega) = 1$; alors Δ n'est pas une composante de $(\omega) - \Delta$, et par conséquent le cycle $X = \Delta.[(\omega) - \Delta]$ est défini ; comme c'est un cycle sur Δ, on a $pr_1 X = pr_2 X$; dans ces conditions, le diviseur $\mathfrak{k} = pr_1 X = pr_2 X$ s'appellera le *diviseur canonique* sur Γ, défini au moyen de la fonction ω. L'étude détaillée des diviseurs canoniques sera faite au § II : pour le moment, nous n'avons besoin que du résultat partiel suivant :

Proposition 10. — Tous les diviseurs canoniques sur Γ sont équivalents les uns aux autres.

Soient ω_1, ω_2 deux fonctions sur $\Gamma \times \Gamma$, telles que l'on ait

$$v_\Delta(\omega_1) = v_\Delta(\omega_2) = 1.$$

Soit, pour $i = 1, 2$, $X = \Delta.[(\omega_i) - \Delta]$, et $\mathfrak{k}_i = pr_i(X_i)$. Posons

$$\varphi = \omega_2/\omega_1;$$

on a $(\varphi) = (\omega_2) - (\omega_1)$, d'où $X_2 - X_1 = \Delta.(\varphi)$, et $\mathfrak{k}_2 - \mathfrak{k}_1 = pr_1[\Delta.(\varphi)]$; comme d'ailleurs on a $v_\Delta(\varphi) = 0$, φ induit sur Δ une fonction qui n'est pas la constante 0. Notre conclusion suit de là, par exemple en vertu de F-VIII$_2$, th. 7.

PROPOSITION 11. — Soit $\mathfrak{a}$ un diviseur sur Γ, tel que

$$l(\mathfrak{a}) = r(\mathfrak{a}) = 0;$$

et soit $\mathfrak{k}$ un diviseur canonique sur Γ. Alors on a $r(\mathfrak{k} - \mathfrak{a}) = 0$; et il existe une fonction φ sur $\Gamma \times \Gamma$, telle que l'on ait

$$(\varphi) = -\Delta - \Gamma \times \mathfrak{a} - (\mathfrak{k} - \mathfrak{a}) \times \Gamma + Z$$

Z étant un diviseur positif sur $\Gamma \times \Gamma$ dont toutes les composantes sont sans point commun avec Δ ; si de plus K est un corps par rapport auquel $\mathfrak{a}$ et $\mathfrak{k}$ soient rationnels, il existe une telle fonction φ, ayant K pour corps de définition.

Soit K tel qu'il est dit plus haut et soient M et N deux points génériques indépendants de Γ par rapport à K. Puisqu'on a $l(\mathfrak{a}) = 0$, le module $L(\mathfrak{a})$ se réduit à la constante 0 ; puisque $r(\mathfrak{a}) = 0$, on a, d'après la prop. 7, $L(\mathfrak{a} + M) \neq L(\mathfrak{a})$; d'après la propr. 3, il existe donc dans $L(\mathfrak{a} + M)$ une fonction θ, autre que la constante 0, ayant $K(M)$ pour corps de définition : alors (θ) est de la forme

$$(\theta) = -M - \mathfrak{a} + \mathfrak{m},$$

où $\mathfrak{m}$ est un diviseur positif, rationnel par rapport à $K(M)$. Soit ψ la fonction sur $\Gamma \times \Gamma$, définie par rapport à K par la relation

$$\theta(N) = \psi(M \times N);$$

d'après F-VIII$_2$, th. 1, cor. 3, on a

$$(\psi).(M \times \Gamma) = M \times (\theta) = M \times (-M - \mathfrak{a} + \mathfrak{m}).$$

D'après F-VII$_6$, th. 12 (iii), il existe sur $\Gamma \times \Gamma$ un diviseur positif Z et un seul, rationnel par rapport à K, sans composante de la forme $A \times \Gamma$, tel que l'on ait $Z.(M \times \Gamma) = M \times \mathfrak{m}$. On a alors

$$[(\psi) + \Delta + \Gamma \times \mathfrak{a} - Z].(M \times \Gamma) = 0 ;$$

d'après F-VII$_6$, th. 12 (ii), il suit de là que le premier facteur du premier membre de cette relation est de la forme $\mathfrak{b} \times \Gamma$, où $\mathfrak{b}$ est un diviseur sur Γ ; on a donc $(\psi) = -\Delta - \Gamma \times \mathfrak{a} - \mathfrak{b} \times \Gamma + Z$. Soit B un point de Γ, et soit b son coefficient (nul ou non) dans $\mathfrak{b}$; soit τ une fonction sur Γ, telle que $v_B(\tau) = 1$; soit ω la fonction sur $\Gamma \times \Gamma$, telle que l'on ait $\omega(P \times Q) = \tau(P)$ quels que soient P et Q sur Γ (F-VIII$_1$, pr. 7) ; on a alors, d'après F-VIII$_2$, th 1. cor. 4. $(\omega) = (\tau) \times \Gamma$. Si donc nous posons $\mathfrak{b}_1 = \mathfrak{b} - b.(\tau)$, et $\psi_1 = \omega^b.\psi$, on aura $(\psi_1) = b.(\tau) \times \Gamma + (\psi) = -\Delta - \Gamma \times \mathfrak{a} - \mathfrak{b}_1 \times \Gamma + Z$. Comme B n'est pas un composant de $\mathfrak{b}_1$, $B \times \Gamma$ n'est alors pas une composante de (ψ_1), de sorte que ψ_1 induit sur $B \times \Gamma$ une fonction qui n'est pas la constante 0 (F-VIII$_2$, th. 3) : il s'ensuit (d'après F-VIII$_2$, th. 4. cor. 2. ou bien encore d'après F-VIII$_2$, th. 7) que le cycle

$$pr_2[(\psi_1).(B \times \Gamma)]$$

est un diviseur équivalent à 0 sur Γ. Mais on a

$$(\psi_1).(B \times \Gamma) = -(B \times B) - (B \times \mathfrak{a}) + Z.(B \times \Gamma).$$

On a donc

$$-B - \mathfrak{a} + pr_2[Z.(B \times \Gamma)] \sim 0, \qquad \text{d'où} \qquad \mathfrak{a} \sim pr_2[Z.(B \times \Gamma)] - B.$$

Dans cette dernière relation, le second membre ne peut être un diviseur positif, en raison de l'hypothèse $l(\mathfrak{a}) = 0$ et d'après la prop. 2 ; par conséquent, $B \times B$ ne peut être un composant du cycle $Z.(B \times \Gamma)$: comme Z est un diviseur positif, ceci implique que le point $B \times B$ ne peut être contenu dans aucune composante de Z. Comme B a été pris quelconque sur Γ, nous avons donc montré qu'aucune composante de Z ne peut avoir de point commun avec Δ. En particulier, Δ ne peut être une composante de Z ; on a donc $v_\Delta(\psi) = -1$, donc $v_\Delta(1/\psi) = 1$; si donc on pose

$$X = \Delta.[(1/\psi) - \Delta],$$

le cycle $\mathfrak{k} = pr_1 X$ est un diviseur canonique sur Γ, équivalent à $\mathfrak{k}$ d'après la prop. 10. Mais on a $X = \Delta.[\Gamma \times \mathfrak{a} + b \times \Gamma - Z]$: on a d'ailleurs $Z.\Delta = 0$; par suite $\mathfrak{k}_1 = \mathfrak{a} + \mathfrak{b}$. Soit ζ une fonction sur Γ, telle que l'on ait $(\zeta) = \mathfrak{k}_1 - \mathfrak{k} = \mathfrak{a} + \mathfrak{b} - \mathfrak{k}$; soit η la fonction sur $\Gamma \times \Gamma$, telle que l'on ait (F-VIII$_1$, pr. 7) $\eta(P \times Q) = \zeta(P)$ quels que soient P et Q sur Γ ; on a donc (F-VIII$_2$, th. 1, cor. 4) $(\eta) = (\zeta) \times \Gamma$. Si donc nous posons $\varphi_1 = n\psi$, on a

$$(\varphi_1) = -\Delta - \Gamma \times \mathfrak{a} - (\mathfrak{k} - \mathfrak{a}) \times \Gamma + Z.$$

Comme alors le diviseur (φ_1) est rationnel par rapport à K, il existe, d'après F-VIII$_3$, th 10, cor. 1. une fonction φ sur $\Gamma \times \Gamma$, ayant K pour corps de définition, et telle que $(\varphi) = (\varphi_1)$; alors φ a toutes les propriétés requises par notre proposition. Il nous reste à montrer qu'on a $r(\mathfrak{k} - \mathfrak{a}) = 0$. En effet, M et N étant comme plus haut des

points génériques indépendants de Γ par rapport à K ; considérons la fonction λ sur Γ, définie par rapport à $K(N)$ par la relation

$$\lambda(M) = \varphi(M \times N).$$

On a, d'après F-VIII$_2$, th. 1, cor. 3. $(\varphi).(\Gamma \times N) = (\lambda) \times N$, d'où, en utilisant l'expression obtenue plus haut pour (φ),

$$(\lambda) = -N - (\mathfrak{k} - \mathfrak{a}) + \mathfrak{z}.$$

où $\mathfrak{z}$ est le diviseur positif défini par $Z.(\Gamma \times N) = \mathfrak{z} \times N$. Comme $N \times N$ n'est contenu dans aucune composante de Z, N n'est pas un composant de $\mathfrak{z}$: comme $\mathfrak{k} - \mathfrak{a}$ est rationnel par rapport à K, et N générique sur Γ par rapport à K, N n'est pas un composant de $\mathfrak{k} - \mathfrak{a}$; on a donc $v_N(\lambda) = -1$. Par conséquent, λ appartient à $L(\mathfrak{k} - \mathfrak{a} + N)$, et non à $L(\mathfrak{k} - \mathfrak{a})$; d'après la prop. 7, ceci démontre bien qu'on a $r(\mathfrak{k} - \mathfrak{a}) = 0$.

Proposition 12. — Soient $\mathfrak{k}$ un diviseur canonique sur Γ, et $\mathfrak{a}$ un diviseur sur Γ, tel que l'on ait $l(\mathfrak{k} - \mathfrak{a}) = 0$. Alors on a $r(\mathfrak{a}) = 0$.

Soit K un corps par rapport auquel $\mathfrak{a}$ et $\mathfrak{k}$ soient rationnels. Posons $\rho = r(\mathfrak{k} - \mathfrak{a})$; soient $M_1, \ldots, M_\rho$, des points génériques indépendants de Γ par rapport à K ; et posons $\mathfrak{m} = \sum_{\nu=1}^{\rho} M_\nu$. D'après la prop. 8, on a alors $r(\mathfrak{k} - \mathfrak{a} + \mathfrak{m}) = l(\mathfrak{k} - \mathfrak{a} + \mathfrak{m}) = 0$, et par conséquent, d'après la prop. 11, on a $r(\mathfrak{a} - \mathfrak{m}) = 0$; puisque $\mathfrak{a} \succ \mathfrak{a} - \mathfrak{m}$, on a donc a fortiori $r(\mathfrak{a}) = 0$.

6. Afin d'avoir en main tous les éléments nécessaires à la démonstration du théorème de Riemann-Roch, il nous reste encore à faire voir que, si $\mathfrak{k}$ est un diviseur canonique, on a $r(\mathfrak{k}) > 0$. En tenant compte de la prop. 7, et de l'interprétation des diviseurs canoniques qui sera donnée au § II, la relation $r(\mathfrak{k}) > 0$ équivaut à l'assertion qu'il n'existe pas sur Γ de différentielle ayant un pôle simple et un seul en un point générique de Γ par rapport à k. C'est là bien entendu un cas particulier du théorème des résidus (démontré pour la première fois par H. Hasse dans le cas d'un corps de base quelconque). Nous démontrerons le même résultat par voie directe, en nous appuyant sur la prop. 11.

Proposition 13. — Si $\mathfrak{k}$ est un diviseur canonique sur Γ, on a $r(\mathfrak{k}) > 0$.

Comme $r(\mathfrak{k})$ ne dépend que de la classe de $\mathfrak{k}$, et que tous les diviseurs canoniques, d'après la prop. 10, appartiennent à une même classe, nous pouvons supposer, de

plus, que $\mathfrak{k}$ est rationnel par rapport à k. Soient $A_1, \ldots, A_g$, et P $g+1$ points génériques indépendants de Γ par rapport à k ; posons

$$\mathfrak{a} = \sum_{\nu=1}^{g} A_\nu - P, \qquad \text{et} \qquad K = k(A_1, \ldots, A_g, P).$$

On a $\deg(-P) = -1$ et $l(-P) = 0$, donc $r(-P) = g$, et par suite, d'après la prop. 8 appliquée au diviseur $-P$ et aux points A_ν, $l(\mathfrak{a}) = r(\mathfrak{a}) = 0$. D'après la prop. 11, il existe donc sur $\Gamma \times \Gamma$ une fonction φ, ayant K pour corps de définition, telle que l'on ait $(\varphi) = -\Delta - \Gamma \times \mathfrak{a} - (\mathfrak{k} - \mathfrak{a}) \times \Gamma + Z$, Z étant un diviseur positif rationnel par rapport à K, dont les composantes sont sans point commun avec Δ. D'après F-VIII$_2$, th. 1, φ a une valeur $\varphi(M \times N)$ déterminée et finie en tout point $M \times N$ de $\Gamma \times \Gamma$ qui n'est contenu dans aucune composante du diviseur $(\varphi)_\infty$, donc a fortiori en tout point $M \times N$ tel que M et N soient distincts l'un de l'autre et distincts de tous les composants des diviseurs $\mathfrak{a}$ et $\mathfrak{k}$. Soient M et N de tels points : alors $M \times \Gamma$ et $\Gamma \times N$ ne sont pas des composantes de (φ), et par suite φ induit, sur l'une et l'autre de ces courbes, des fonctions autres que la constante 0 ; de plus, d'après les remarques qui suivent dans F-VIII$_1$ la définition d'une fonction induite, ces fonctions prennent toutes deux au point $M \times N$ la valeur $\varphi(M \times N)$. Autrement dit, si R est un point générique de Γ par rapport à $K(M, N)$, et qu'on désigne d'une manière générale par θ_M et par η_N les fonctions sur Γ respectivement définies par rapport à $K(M, N)$, par $\theta_M(R) = \varphi(M \times R)$ et par $\eta_N(R) = \varphi(R \times N)$, on a, quand M et N sont tels qu'il a été dit, $\theta_M(N) = \eta_N(M) = \varphi(M \times N)$. D'autre part, il résulte de F-VIII$_2$, th. 4, cor. 1, ou bien de F-VIII$_2$, th. 7, que les diviseurs des fonctions θ_M, η_N qu'on vient de définir sont donnés par $(\theta_M) = -M - \mathfrak{a} + Z(M), (\eta_N) = -N - (\mathfrak{k} - \mathfrak{a}) + Z'(N)$, où $Z(M)$ et $Z(N)$ sont les diviseurs sur Γ, respectivement définis par $Z.(M \times \Gamma) = M \times Z(M)$ et par $Z.(\Gamma) = Z'(N) \times N$.

Soient maintenant r et s des entiers quelconques ; soient $M_1, \ldots, M_r, N_1, \ldots, N_s$, des points de Γ, distincts les uns des autres et distincts des composants de $\mathfrak{a}$ et de $\mathfrak{k}$; soient $\theta_i = \theta_{M_i}$ pour $1 \leqslant i \leqslant r$, et $\eta_j = \eta_{N_j}$ pour $1 \leqslant j \leqslant s$, les fonctions sur Γ, respectivement définies au moyen de φ et des points M_i et N_j comme il a été dit ci-dessus ; on aura donc, quels que soient i et j,

$$\theta_i(N_j) = \eta_j(M_i) = \varphi(M_i \times N_j).$$

De plus, d'après ce qu'on a vu, aucune des fonctions θ_i et η_j n'est la constante 0, et l'on a, pour $1 \leqslant i \leqslant r$, $(\theta_i) = -M_i - \mathfrak{a} + Z(M_i)$, donc $(\theta_i) \succ -M_i - \mathfrak{a}$. D'ailleurs, comme on a $l(\mathfrak{a}) = 0$, on n'a pas $(\theta_i) \succ -\mathfrak{a}$; on a donc $v_{M_i}(\theta_i) = -1$; l'on a d'ailleurs $v_{M_i}(\theta_j) \geqslant 0$ pour $i \neq j$. Il suit de là que les θ_i sont linéairement indépendants ; car, si l'on avait une relation $\sum_i c_i \theta_i = 0$, à coefficients constants c_i avec par exemple $c_i \neq 0$, on aurait

$$\theta_i = -1/c_i . \sum_{j \neq i} c_j \theta_j, \qquad \text{d'où} \qquad v_{M_i}(\theta_i) \leqslant 0.$$

ce qui n'est pas le cas. Comme les θ_i sont tous dans $L(\mathfrak{a} + \sum_i M_i)$, et qu'on a

$$r\left(\mathfrak{a} + \sum_i M_i\right) \leqslant r(\mathfrak{a}) = 0,$$

donc $$l\left(\mathfrak{a} + \sum_i M_i\right) = \deg\left(\mathfrak{a} + \sum_i M_i\right) - g + 1 = r,,$$

il suit de là que les θ_i forment une base du module $L(\mathfrak{a} + \sum_i M_i)$.

Posons $\mathfrak{m} = \mathfrak{a} + \sum_i M_i - \sum_j N_j$, alors $L(\mathfrak{m})$ est contenu dans $L(\mathfrak{a} + \sum_i M_i)$. Par conséquent, pour qu'une fonction sur Γ soit dans $L(\mathfrak{m})$, il faut et il suffit que ce soit une combinaison linéaire des θ_i, à coefficients constants, qui prenne la valeur 0 en chacun des points N_j. L'entier $l(\mathfrak{m})$ est donc égal au nombre de solutions linéairement indépendantes du système d'équations linéaires à r inconnues

$$\sum_i c_i.\theta_i(N_j) = 0 \qquad (1 \leqslant j \leqslant s);$$

on a donc $l(\mathfrak{m}) = r - s + \rho$, ρ étant le nombre de solutions linéairement indépendantes du système transposé

$$\sum_j t_j.\theta_i(N_j) = 0 \qquad (1 \leqslant i \leqslant r),$$

qui peut aussi s'écrire $\sum_j t_j.\eta_j(M_i) = 0$ $(1 \leqslant i \leqslant r)$. Comme d'ailleurs on a $\deg(\mathfrak{m}) = g - 1 + r - s$, il s'ensuit qu'on a $r(\mathfrak{m}) = \rho$. On conclut de là, en particulier, que, si le système

$$\sum_j t_j.\eta_j(M_i) = 0 \qquad (1 \leqslant i \leqslant r)$$

possède au moins une solution $(t_1, \ldots, t_s)$ non nulle, on a $r(\mathfrak{m}) > 0$. Nous allons maintenant faire voir qu'il en est bien ainsi pour un certain choix des points M_i, N_j, pour lequel on a en même temps $\mathfrak{m} \sim \mathfrak{k}$; il suivra de là qu'on a $r(\mathfrak{k}) = r(\mathfrak{m}) > 0$, ce qui démontrera notre proposition.

Pour cela, nous prendrons $s = 2$, et nous prendrons pour N_1 et N_2 deux points génériques indépendants de Γ par rapport à K. Les fonctions $\eta_j = \eta_{N_j}$ pour $j = 1, 2$, étant définies comme plus haut, soit t une quantité variable sur le corps $K(N_1, N_2)$, et posons $\eta = \eta_1 - t\eta_2$. On a, d'après ce qui a été démontré plus haut,

$$(\eta_j) = -N_j - (\mathfrak{k} - \mathfrak{a}) + Z'(N_j), \quad \text{d'où} \quad (\eta) \succ -N_1 - N_2 - (\mathfrak{k} - \mathfrak{a}).$$

Par conséquent, le diviseur $(\eta) + N_1 + N_2 + (\mathfrak{k} - \mathfrak{a})$ est un diviseur positif, qui peut donc être mis sous la forme $\sum_i M_i$, où les M_i sont des points de Γ, distincts ou non. On a alors

$$\mathfrak{a} + \sum_i M_i - N_1 - N_2 = (\eta) + \mathfrak{k} \sim \mathfrak{k}.$$

Si donc nous montrons que les M_i sont distincts les uns des autres, distincts de N_1 et N_2, et distincts des composants de $\mathfrak{a}$ et de $\mathfrak{k}$, notre démonstration sera achevée. Pour cela, posons $\omega = \eta_1/\eta_2$; on a

$$\eta = (\omega - t)\eta_2, \qquad \text{donc} \qquad (\eta) = (\omega - t) + (\eta_2),$$

et par suite, d'après les formules écrites plus haut.

$$\sum_i M_i = (\omega - t) + N_1 + Z'(N_2).$$

Mais, d'après F-VIII$_2$, th. 6. on a $(\omega - t)_\infty = (\omega)_\infty$; d'autre part, on a $(\omega) = (\eta_1) - (\eta_2) = N_2 + Z'(N_1) - N_1 - Z'(N_2)$; on va déduire de là que l'on a $N_1 + Z'(N_2) = (\omega)_\infty = (\omega - t)_\infty$, ce qui donnera

$$\sum_i M_i = (\omega - t)_0.$$

En effet, puisque $N_1 \times N_1$ n'est contenu dans aucune composante de Z, il résulte de la définition de $Z'(N_1)$ que N_1 n'est pas un composant de $Z'(N_1)$; de même, N_2 n'est pas un composant de $Z'(N_2)$. D'autre part, $Z'(N_1)$ et $Z'(N_2)$ ne peuvent avoir de composant commun ; supposons en effet que R soit un composant de $Z'(N_1)$ et de $Z'(N_2)$; alors, en vertu de F-VII$_6$, th. 12, le lieu de $R \times N_1$, par rapport à $\overline{K}$, sur $\Gamma \times \Gamma$ sera une composante de Z ; comme Z ne peut avoir de composante de la forme $R \times \Gamma$, il s'ensuit que R n'est pas algébrique sur K, et que N_1 est algébrique sur $K(R)$; de même, N_2 devra être algébrique sur $K(R)$: le corps $K(N_1, N_2)$ sera donc algébrique sur $K(R)$, contrairement à la définition de N_1, N_2, en vertu de laquelle il a la dimension 2 sur K.

Nous avons ainsi démontré que les diviseurs

$$N_2 + Z'(N_1) \qquad \text{et} \qquad N_1 + Z'(N_2)$$

n'ont pas de composant commun ; comme la différence de ces diviseurs est (ω), ces diviseurs sont donc égaux respectivement à $(\omega)_0$, et à $(\omega)_\infty$. On a donc bien $N_2 + Z'(N_1) = (\omega)_\infty = (\omega - t)_\infty$, d'où, d'après ce qui a été trouvé plus haut,

$$\sum_i M_i = (\omega - t) + (\omega - t)_\infty = (\omega - t)_0.$$

Mais soit Λ le graphe de la fonction ω ; soit Λ_t celui de $\omega - t$. Si (u) est un point générique de la droite projective D par rapport à $K(t)$, il y a une correspondance birationnelle partout birégulière (une "translation") dans laquelle (u) et $(u+t)$ sont des points génériques correspondants de D par rapport à $K(t)$; cette translation détermine une correspondance birationnelle partout birégulière entre la variété $\Gamma \times D$ et elle-même, qui transforme les courbes Λ_i et $\Gamma \times (0)$ en Λ et en $\Gamma \times (t)$, respectivement. Il s'ensuit qu'on a $(\omega - t)_0 = (\omega)_t$: l'on a d'ailleurs, par définition, $\Lambda.[\Gamma \times (t)] = (\omega)_t \times (t)$. On a donc

$$\Lambda.[\Gamma \times (t)] = \sum_i M_i \times (t).$$

Mais $K(N_1, N_2)$ est un corps de définition pour η_1 et η_2, donc pour ω, donc aussi pour Λ ; alors F-VI$_3$, th. 12, montre que chacun des points $M_i \times (t)$ est un point générique de Λ par rapport à $K(N_1, N_2)$; chacun des points M_i est donc un point générique, par rapport à $K(N_1, N_2)$, de la projection Γ de Λ sur Γ : ceci implique qu'ils sont distincts de N_1, de N_2, et de tous les composants de $\mathfrak{a}$ et de $\mathfrak{k}$, puisque ces derniers points sont tous algébriques sur K. Enfin, encore d'après F-VI$_3$, th. 12, il y a un entier $p^{\int}$ tel que, parmi les M_i, il y en ait exactement $p^{\int}$ qui coïncident avec l'un quelconque d'entre eux ; et cet entier $p^{\int}$ divise le coefficient, dans le cycle $\Lambda.[\Gamma \times (\infty)]$ de chacun des composants de ce cycle, qui n'est autre que

$$(\omega)_\infty \times (\infty) = [N_1 + Z'(N_2)] \times (\infty) ;$$

mais N_1, n'étant pas algébrique sur $K(N_2)$, n'est pas un composant de $Z'(N_2)$, de sorte que, dans ce cycle, le point $N_1 \times (\infty)$ a le coefficient 1. On a donc $p^{\int} = 1$, c'est-à-dire que tous les M_i sont distincts les uns des autres. Ceci achève notre démonstration.

7. Nous sommes maintenant en mesure de démontrer le théorème de Riemann-Roch :

Théorème de Riemann-Roch. —Soient $\mathfrak{k}$ un diviseur canonique, et $\mathfrak{a}$ un diviseur quelconque, sur la courbe Γ de genre g. Alors on a

$$l(\mathfrak{a}) = \deg(\mathfrak{a}) - g + 1 + r(\mathfrak{a}), \qquad r(\mathfrak{a}) = l(\mathfrak{k} - \mathfrak{a}).$$

Nous avons à montrer que la relation $l(\mathfrak{k} - \mathfrak{a}) = \rho$ entraîne $r(\mathfrak{a}) = \rho$. C'est ce que nous ferons par récurrence sur ρ. Pour $\rho = 0$, notre assertion est contenue dans la prop. 12. Soit donc $\rho > 0$. Alors, d'après la prop. 2, il y a un diviseur positif $\mathfrak{a}$ tel que $\mathfrak{b} \sim \mathfrak{k} - \mathfrak{a}$, d'où

$$l(\mathfrak{b}) = l(\mathfrak{k} - \mathfrak{a}) = \rho, \qquad \mathfrak{a} \sim \mathfrak{k} - \mathfrak{b}, \qquad r(\mathfrak{a}) = r(\mathfrak{k} - \mathfrak{b}).$$

Comme on a $\mathfrak{k} - \mathfrak{b} \prec \mathfrak{k}$, on a $r(\mathfrak{k} - \mathfrak{b}) \geqslant r(\mathfrak{k})$, donc, d'après la prop. 13, $r(\mathfrak{k} - \mathfrak{b}) > 0$. Soient K un corps par rapport auquel $\mathfrak{a}, \mathfrak{b}$ et $\mathfrak{k}$ soient rationnels, et M un point

générique de Γ par rapport à K ; d'après la prop. 9, on a $l(\mathfrak{b}-M) = l(\mathfrak{b})-1 = \rho-1$, donc, d'après l'hypothèse de récurrence, $r(\mathfrak{k}-\mathfrak{b}+M) = \rho-1$. D'autre part, d'après la prop. 8, on a $r(\mathfrak{k}-\mathfrak{b}+M) = r(\mathfrak{k}-\mathfrak{b})-1$. La comparaison de ces résultats donne bien $r(\mathfrak{a}) = r(\mathfrak{k}-\mathfrak{b}) = \rho$.

Corollaire. — Si $\mathfrak{k}$ est un diviseur canonique, on a

$$\deg(\mathfrak{k}) = 2g-2, \qquad l(\mathfrak{k}) = g, \qquad \text{et} \qquad r(\mathfrak{k}) = 1.$$

En effet, si, dans le théorème de Riemann-Roch, on fait $\mathfrak{a} = 0$, on obtient $l(\mathfrak{k}) = g$; si on y fait $\mathfrak{a} = \mathfrak{k}$, on obtient $r(\mathfrak{k}) = l(0) = 1$, et $l(\mathfrak{k}) = deg(\mathfrak{k}) - g + 2$.

Observons pour terminer qu'il résulte du théorème de Riemann-Roch, ou même simplement de la définition du genre g que, si $g = 0$ et si $\mathfrak{m}$ est un diviseur quelconque de degré 0, on a

$$l(-\mathfrak{m}) = 1$$

donc qu'il existe une fonction φ, autre que 0, telle que $(\varphi) \succ \mathfrak{m}$; comme d'ailleurs on a $\deg(\varphi) = 0$, ceci implique que $(\varphi) = \mathfrak{m}$. Autrement dit, quand le genre g a la valeur 0 (et, comme il est facile de le voir, seulement dans ce cas), les relations $\deg(\mathfrak{m}) = 0$ et $\mathfrak{m} \sim 0$ sont équivalentes.

§ II. Les différentielles sur une courbe.

8. En vertu de F-VIII$_2$, th. 6, les fonctions θ sur $\Gamma \times \Gamma$, telles que $v_\Delta(\theta) > 0$, forment un groupe additif $\mathscr{D}_1$, dont les fonctions θ, telles que $v_\Delta(\theta) > 1$, forment un sous-groupe $\mathscr{D}_2$; le groupe quotient $\mathscr{D}_1/\mathscr{D}_2$ s'appellera par définition le *groupe additif des différentielles sur* Γ, et ses éléments, c'est-à-dire les classes de $\mathscr{D}_1$ suivant $\mathscr{D}_2$, s'appelleront les *différentielles* sur Γ. Si θ est une fonction dans $\mathscr{D}_1$, la classe suivant $\mathscr{D}_2$ à laquelle appartient θ dans $\mathscr{D}_1$ sera appelée la différentielle sur Γ *déterminée par* θ, et sera notée $\{\theta\}$: on écrira 0 pour la différentielle $\mathscr{D}_2 = \{0\}$. On dira qu'un corps K est un *corps de définition* pour une différentielle ω sur Γ, s'il existe une fonction θ dans $\mathscr{D}_1$ ayant K pour corps de définition, et telle que $\omega = \{\theta\}$.

Nous allons vérifier maintenant, au moyen d'un raisonnement bien connu, que le groupe $\mathscr{D}_1/\mathscr{D}_2$, des différentielles sur Γ est isomorphe au groupe additif des fonctions sur Δ, donc aussi (cf. § 1. n° 5) au groupe additif des fonctions sur Γ et peut donc être considéré comme module de rang 1 sur le corps abstrait des fonctions sur Γ. Soient en effet θ et ψ deux fonctions sur $\Gamma \times \Gamma$, telles que $v_\Delta(\theta) > 0$ et $v_\Delta(\psi) \geqslant 0$, d'où $v_\Delta(\psi\theta) > 0$. D'après F-VIII$_2$. th. 1, ψ induit sur Δ une fonction ψ_Δ ; soit φ la fonction correspondante sur Γ, c'est-à-dire la fonction sur Γ, telle que l'on ait $\varphi(P) = \psi_\Delta(P \times P)$ quel que soit P sur Γ. Dans ces conditions, nous allons montrer

que la différentielle $\{\psi\theta\}$ ne dépend que de $\{\theta\}$ et de φ. Si en effet θ_1 est une fonction dans $\mathscr{D}_1$, déterminant la même différentielle que θ, et ψ_1 une fonction sur $\Gamma \times \Gamma$, induisant sur Δ la même fonction que ψ, $\theta_1 - \theta$ est dans $\mathscr{D}_2$, de sorte qu'on a $v_\Delta(\theta_1 - \theta) > 1$, et $\psi_1 - \psi$ induit sur Δ la constante 0, de sorte qu'on a (F-VIII$_2$, th. 1) $v_\Delta(\psi_1 - \psi) > 0$; comme on a d'autre part $\psi_1\theta_1 - \psi\theta = \psi_1(\theta_1 - \theta) + \theta(\psi_1 - \psi)$, il suit de là, d'après F-VIII$_2$, th. 6, que l'on a $v_\Delta(\psi_1\theta_1 - \psi\theta) > 1$, donc $\{\psi_1\theta_1\} = \{\psi\theta\}$. Réciproquement, soient $\{\theta\}$ une différentielle sur Γ, déterminée par une fonction θ de $\mathscr{D}_1$ et φ une fonction quelconque sur Γ ; soit $\overline{\varphi}$ la fonction sur Δ, correspondant à φ, c'est-à-dire telle que l'on ait $\overline{\varphi}(P \times P) = \varphi(P)$ quel que soit P sur Γ : il existe des fonctions ψ sur $\Gamma \times \Gamma$, induisant sur Δ la fonction $\overline{\varphi}$, car on peut prendre par exemple pour ψ, d'après F-VIII$_1$, pr. 7, la fonction sur $\Gamma \times \Gamma$ qui est telle que l'on ait, quels que soient P et Q sur Γ, $\psi(P \times Q) = \varphi(P)$. Dans ces conditions, il existe une différentielle $\{\psi\theta\}$ sur Γ, qui ne dépend, comme nous l'avons fait voir, que de φ et de $\{\theta\}$; de plus, il résulte de notre construction que, si K est un corps de définition à la fois pour φ et pour la différentielle $\{\theta\}$, c'en est un aussi pour la différentielle $\{\psi\theta\}$; alors, si ω désigne la différentielle $\{\theta\}$, nous noterons, par e définition, $\varphi.\omega$ la différentielle $\{\psi\theta\}$. Comme, avec ces notations, on a $v_\Delta(\psi\theta) = v_\Delta(\psi) + v_\Delta(\theta)$, on ne peut avoir $\varphi.\omega = 0$ que si l'on a $\varphi = 0$ ou $\omega = 0$. Il est clair que le "produit" $\varphi.\omega$ est distributif par rapport au premier et au second facteur ; il résulte aussi des définitions ci-dessus que, si φ_1 et φ_2 sont deux fonctions sur Γ, et ω une différentielle sur Γ, on a

$$\varphi_1.(\varphi_2.\omega) = (\varphi_1\varphi_2).\omega.$$

Nous avons donc bien défini le groupe additif des différentielles sur Γ comme module sur le corps abstrait des fonctions sur Γ. De plus, ce module est de rang 1 ; soient en effet ω et ω_1 des différentielles sur Γ, déterminées respectivement par des fonctions θ et θ_1 de $\mathscr{D}_1$; et supposons qu'on ait $\omega \neq 0$, donc $v_\Delta(\theta) = 1$. Alors, si nous posons $\psi = \theta_1/\theta$, on aura $v_\Delta(\psi) \geqslant 0$, donc par définition $\omega_1 = \varphi.\omega$ si φ est la fonction sur Γ, correspondant à la fonction induite par ψ sur Δ.

De plus, dans ces conditions, la fonction φ est déterminée d'une manière unique par la relation $\omega_1 = \varphi.\omega$; si en effet φ' est une fonction ayant la même propriété, on a $(\varphi' - \varphi).\omega = 0$, donc $\varphi' = \varphi$ puisque $\omega \neq 0$: on écrira alors $\varphi = \omega_1/\omega$. Il résulte de plus de ce calcul, et de nos définitions, que, si K est un corps de définition commun pour les différentielles ω et ω_1, c'en est un aussi pour la fonction $\varphi = \omega_1/\omega$. Comme nous avons déjà vu que, si K est un corps de définition commun pour φ et ω, c'en est un aussi pour $\varphi.\omega$, il s'ensuit que, si K est un corps de définition pour une différentielle $\omega \neq 0$, les différentielles sur Γ qui ont K pour corps de définition sont celles qui sont de la forme $\varphi.\omega$ où φ est une fonction sur Γ ayant K pour corps de définition, et celles-là seulement.

9. Soit θ une fonction de $\mathscr{D}_1$, déterminant une différentielle autre que 0 ; alors on a $v_\Delta(\theta) = 1$, et par suite, d'après les définitions du § 1, n° 5, θ détermine un diviseur

canonique $\mathfrak{k}$ sur Γ au moyen des relations $X = \Delta.[(\theta) - \Delta].\mathfrak{k} = pr_1 X$. On va voir maintenant que ce diviseur $\mathfrak{k}$ ne dépend que de la différentielle $\{\theta\}$. Ce résultat est inclus dans la proposition suivante, qui n'est d'ailleurs qu'une forme plus précise de la prop. 10 du § 1 (n° 5) :

PROPOSITION 14. — Soient ω_1 et ω_2 deux différentielles sur Γ, autres que 0 ; et soit $\varphi = \omega_2/\omega_1$. Soit θ_i, pour $i = 1, 2$, une fonction sur $\Gamma \times \Gamma$, telle que l'on ait $\omega_i = \{\theta_i\}$; posons

$$X_i = \Delta.[(\theta_i) - \Delta], \qquad \text{et} \qquad \mathfrak{k}_i = pr_1(X_i).$$

Alors on a $\mathfrak{k}_2 - \mathfrak{k}_1 = (\varphi)$.

Posons $\psi = \theta_2/\theta_1$; on a $v_\Delta(\theta_1) = v_\Delta(\theta_2) = 1$, donc $v_\Delta(\psi) = 0$, de sorte que ψ induit sur Δ une fonction ψ_Δ ; si donc φ' est la fonction correspondante sur Γ, on a $\omega_2 = \varphi'.\omega_1$, donc $\varphi' = \omega_2/\omega_1 = \varphi$. Les fonctions φ sur Γ, et ψ_Δ sur Δ, se correspondent donc l'une à l'autre, c'est-à-dire qu'on a, quel que soit P sur Γ, $\varphi(P) = \psi_\Delta(P \times P)$: ceci implique qu'on a $(\varphi) = pr_1[(\psi_\Delta)]$. D'autre part, on a

$$X_2 = \Delta.[(\psi\theta_1) - \Delta] = \Delta.[(\psi) + (\theta_1) - \Delta] = \Delta.(\psi) + X_1;$$

on a donc $\mathfrak{k}_2 - \mathfrak{k}_1 = pr_1[\Delta.(\psi)]$; comme on a. d'après F-VIII$_2$, th. 4, cor. 1., $\Delta.(\psi) = (\psi_\Delta)$, ceci achève la démonstration.

Les notations restant les mêmes que dans la prop. 14, prenons en particulier $\omega_2 = \omega_1$; alors on a $\mathfrak{k}_2 = \mathfrak{k}_1$; notre proposition montre donc bien que $\mathfrak{k}_1$ ne dépend que de ω_1, et non du choix de θ_1.

Soit alors ω une différentielle sur Γ, autre que 0 ; soit θ une fonction sur $\Gamma \times \Gamma$ telle que l'on ait $\omega = \{\theta\}$; alors le diviseur canonique $\mathfrak{k}$ défini par les relations $X = \Delta.[(\theta) - \Delta]$, $\mathfrak{k} = pr_1 X$, diviseur qui ne dépend que de ω d'après ce qui précède, s'appellera le diviseur de la différentielle ω, et se notera (ω) : si de plus P est un point quelconque sur Γ, on désignera par $v_P(\omega)$ le coefficient de P dans (ω). La prop. 14 montre que, si ω est une différentielle, et φ une fonction sur Γ, et si l'on a $\omega \neq 0, \varphi \neq 0$, on a $(\varphi.\omega) = (\varphi) + (\omega)$. Il résulte de plus de notre définition que, si K est un corps de définition pour ω, le diviseur (ω) est rationnel par rapport à K.

10. Soit φ une fonction sur Γ. Il y a, d'après F. VIII$_1$, pr. 7, une fonction φ_1 et une seule sur $\Gamma \times \Gamma$, telle que l'on ait $\varphi_1(P \times Q) = \varphi(P)$ quels que soient P et Q sur Γ : il y a de même une fonction φ_2 et une seule sur $\Gamma \times \Gamma$, telle que l'on ait $\varphi_2(P \times Q) = \varphi(Q)$ quels que soient P et Q sur Γ ; la fonction $\varphi_2 - \varphi_1$ sur $\Gamma \times \Gamma$ sera, dans ce qui suit, désignée une fois pour toutes par φ_∂. On a donc $\varphi_\partial(P \times Q) = \varphi(Q) - \varphi(P)$ chaque fois que P et Q sont deux points sur Γ tels que $\varphi(P) \neq \infty, \varphi(Q) \neq \infty$. Si K est un

corps de définition pour φ, et que M et N soient deux points génériques indépendants de Γ par rapport à K, φ_∂ est la fonction sur $\Gamma \times \Gamma$ définie par rapport à K par la relation $\varphi_\partial(M \times N) = \varphi(N) - \varphi(M)$; on a alors, d'autre part, $\varphi_\partial(M \times M) = 0$, c'est-à-dire que φ_∂ induit sur Δ la constante 0. On a donc, quelle que soit la fonction φ sur Γ, $v_\Delta(\varphi_\partial) > 0$: par suite, φ_∂ détermine une différentielle $\{\varphi_\partial\}$ sur Γ : celle-ci s'appellera, par définition, la *différentielle de* φ, et se notera $d\varphi$. Il s'ensuit que, si K est un corps de définition pour φ, c'en est un aussi pour $d\varphi$.

Si φ est une constante, on a, d'après ces définitions, $\varphi_\partial = 0$, donc $d\varphi = 0$. Pour faire voir qu'il existe des fonctions φ telles que $d\varphi \neq 0$, nous introduirons la définition suivante. Soient φ une fonction sur Γ, et P un point de Γ ; posons $c = \varphi(P)$; on dira que φ est une *uniformisante* pour Γ au point P si l'on a $c \neq \infty$ et $v_P(\varphi - c) = 1$. L'existence d'uniformisantes pour tout point de Γ résulte par exemple de F-VIII$_2$, th. 9. Il est clair qu'une constante n'est uniformisante en aucun point.

Proposition 15. — Soient φ une fonction sur Γ, et P un point de Γ. Alors, pour que φ soit uniformisante en P, il faut et il suffit que l'on ait $\varphi(P) \neq \infty, d\varphi \neq 0$, et $v_P(d\varphi) = 0$.

Si l'on a $\varphi(P) = \infty$, ou bien si φ est constante, φ n'est pas uniformisante en P, et les conditions ci-dessus ne sont pas satisfaites ; nous avons donc le droit de supposer que φ n'est pas constante et a une valeur finie en P. Soient K un corps de définition pour φ et M un point générique de Γ par rapport à $K(P)$: alors $P \times M$ est un point générique de $P \times \Gamma$ par rapport à $K(P)$. D'après le lemme du § 1, n° 1, puisque φ n'est pas constante, $\varphi(M)$ est une quantité variable sur le corps $K(P)$: on a donc $\varphi(M) \neq \varphi(P)$, donc

$$\varphi_\partial(P \times M) = \varphi(M) - \varphi(P) \neq 0,$$

c'est-à-dire que φ_∂ induit sur $P \times \Gamma$ une fonction qui n'est pas la constante 0. Soit ψ la fonction sur Γ, définie par rapport à $K(P)$ par la relation $\psi(M) = \varphi(M) - \varphi(P)$; on a alors, d'après F-VIII$_2$, th. 7, $(\psi) = pr_2[(\varphi_\partial).(P \times \Gamma)]$; comme d'ailleurs le cycle $(\varphi_\partial).(P \times \Gamma)$ est contenu dans $P \times \Gamma$, donc de la forme $P \times \mathfrak{a}$, on a

$$(\varphi_\partial).(P \times \Gamma) = P \times (\psi).$$

Mais, pour que φ soit uniformisante en P, il faut et il suffit, par définition, que P ait le coefficient 1 dans le diviseur (ψ) : donc, pour qu'il en soit ainsi, il faut et il suffit que le point $P \times P$ ait le coefficient 1 dans le cycle $(\varphi_\partial).(P \times \Gamma)$. Soit a le coefficient de $P \times P$ dans $(\varphi_\partial).(P \times \Gamma)$; posons $b = v_\Delta(\varphi_\partial)$, et $X = (\varphi_\partial) - b.\Delta$; et soient c et c' les coefficients de $P \times P$ dans $X.(P \times \Gamma)$ et dans $X.\Delta$, respectivement : on a alors $a = b + c$, et $b > 0$. De plus, comme la fonction φ_∂ est définie et a la valeur 0 en $P \times P$, ce point n'est contenu (d'après F-VIII$_2$, th. 1) dans aucune composante du diviseur $(\varphi_\partial)_\infty$; on a donc $c \geqslant 0, c' \geqslant 0$; et l'on a $c = c' = 0$ si

$P \times P$ n'est contenu dans aucune composante de X, et $c > 0, c' > 0$ dans le cas contraire. Cela posé, pour que φ soit uniformisante en P, il faut et il suffit, d'après ce qui précède, qu'on ait $b + c = 1$, donc qu'on ait $b = 1$ et $c = 0$, c'est-à-dire qu'on ait $v_\Delta(\varphi_\partial) = 1$ et $c' = 0$, ou encore qu'on ait $d\varphi \neq 0$ et que le point $P \times P$ ne soit pas un composant du cycle $X.\Delta = \Delta.[(\varphi_\partial) - \Delta]$. C'est bien ce qu'il fallait démontrer.

Observons que, si le corps de base est de caractéristique 0, la relation $\varphi(P) = \infty$ entraîne $v_P(d\varphi) < 0$, de sorte qu'en ce cas la première condition de l'énoncé ci-dessus est superflue : il n'en est pas de même si la caractéristique p n'est pas nulle.

11. On peut maintenant énoncer les principales propriétés de l'opération $d\varphi$ comme suit :

THÉORÈME. — Sur la courbe Γ il existe des fonctions φ telles que $d\varphi \neq 0$. Si c est une constante, on a $d(c) = 0$. Si φ et ψ sont des fonctions quelconques sur Γ, on a

$$d(\varphi + \psi) = d\varphi + d\psi \qquad \text{et} \qquad d(\varphi\psi) = \varphi.d\psi + \psi.d\varphi.$$

Il ne nous reste en effet à démontrer que la dernière formule. Pour cela, soit K un corps commun de définition pour φ et ψ, et soient M et N deux points génériques indépendants de Γ par rapport à K. Posons $\theta = (\varphi\psi)_\partial$; ou a alors $d(\varphi\psi) = \{\theta\}$, et θ est la fonction sur $\Gamma \times \Gamma$, définie par rapport à K par

$$\theta(M \times N) = \varphi(N)\psi(N) - \varphi(M)\psi(M).$$

Soient θ_1 et θ_2 les fonctions sur $\Gamma \times \Gamma$, respectivement définies par rapport à K par

$$\theta_1(M \times N) = \varphi(N).\psi_\partial(M \times N) \qquad \text{et} \qquad \theta_2(M \times N) = \psi(M).\varphi_\partial(M \times N);$$

on a $\theta = \theta_1 + \theta_2$, et il résulte immédiatement des définitions qu'on a $\{\theta_1\} = \varphi.\{\psi_\partial\} = \varphi.d\psi$, et $\{\theta_2\} = \psi.\{\varphi_\partial\} = \psi.d\varphi$.

COROLLAIRE. — Soient φ une fonction sur Γ, et K un corps de définition pour φ. Alors, pour qu'on ait $d\varphi \neq 0$, il faut et il suffit que le corps abstrait Ω_K des fonctions sur Γ ayant K pour corps de définition soit une extension algébrique séparable de $K(\varphi)$. De plus, s'il en est ainsi, et qu'on pose, pour $\psi \in \Omega_K, D\psi = d\psi/d\varphi$, l'opérateur D est la dérivation dans Ω_K, s'annulant sur K, et telle que $D\varphi = 1$.

Soit M un point générique de Γ par rapport à K ; alors $K(M)$ est une extension régulière de K (F-1_7, et F-IV_1), et est donc séparablement engendré, et de dimension 1 sur K ; par suite, d'après F-I_5, pr. 16, il existe dans $K(M)$ une dérivation non triviale, s'annulant sur K, et, à un facteur près, il n'en existe qu'une. En vertu de

l'isomorphisme entre $K(M)$ et Ω_K dont la définition a été rappelée au § 1, n° 1, le corps abstrait Ω_K a donc les mêmes propriétés. Soit φ une fonction appartenant à Ω_K, et telle que $d\varphi \neq 0$: alors K est un corps de définition pour $d\varphi$, et aussi pour de $d\psi$ si $\psi \in \Omega_K$ de sorte que

$$D\psi = d\psi/d\varphi$$

est alors dans Ω_K. Il résulte alors de notre théorème que D est une dérivation dans Ω_K, s'annulant sur K, et telle que $D\varphi = 1$. Comme toute autre dérivation dans Ω_K, s'annulant sur K, doit alors, à un facteur près, coïncider avec D, il s'ensuit qu'une telle dérivation ne peut s'annuler sur $K(\varphi)$; donc, d'après F-1_5, th. 1, Ω_K est alors séparablement algébrique sur $K(\varphi)$. Supposons maintenant que φ_1 soit dans Ω_K, et telle que l'on ait $d\varphi_1 = 0$; alors on a $D\varphi_1 = 0$, et par conséquent la dérivation D s'annule sur $K(\varphi_1)$; en vertu de F-I_5, th. 1, il s'ensuit qu'alors Ω_K n'est pas séparablement algébrique sur $K(\varphi_1)$.

Donnons, pour terminer, l'interprétation, au moyen des différentielles, de l'entier $r(\mathfrak{a}) = l(\mathfrak{k} - \mathfrak{a})$ qui apparaît dans le théorème de Riemann-Roch. Soit ω une différentielle sur Γ, autre que 0 ; posons $\mathfrak{k} = (\omega)$; c'est là, comme on a vu, un diviseur canonique. Toute différentielle η sur Γ est alors de la forme $\eta = \varphi.\omega$ où φ est une fonction sur Γ, et on a $(\eta) = (\varphi) + \mathfrak{k}$. Si donc $\mathfrak{a}$ est un diviseur sur Γ, il faut et il suffit, pour qu'on ait $(\eta) \succ \mathfrak{a}$, qu'on ait $\varphi \in L(\mathfrak{k} - \mathfrak{a})$. L'ensemble des différentielles η, telles qu'on ait $(\eta) \succ \mathfrak{a}$, est donc un module sur le corps des constantes, de rang égal à $l(\mathfrak{k} - \mathfrak{a})$.

En particulier, on appelle différentielle de première espèce sur Γ toute différentielle η telle que $(\eta) \succ 0$. Il résulte de ce qui précède, et du corollaire du théorème de Riemann-Roch, que les différentielles de première espèce sur Γ forment un module de rang g sur le corps des constantes. De plus, d'après la prop. 5, ce module possède une base formée de g différentielles ayant k pour corps de définition.

DEUXIÈME PARTIE
THÉORIE ÉLÉMENTAIRE
DES CORRESPONDANCES SUR UNE COURBE

Nous abordons maintenant la théorie des correspondances. Des résultats de la 1re partie, il n'est nécessaire de retenir ici que la définition des diviseurs canoniques (1re partie, § 1, no 5), et le théorème de Riemann-Roch ; ces résultats ne nous serviront d'ailleurs qu'à partir du § II, le § I dépendant seulement de la théorie générale des intersections.

Comme on le reconnaîtra sans peine, le présent mémoire est directement inspiré des travaux de Castelnuovo et Severi sur le même sujet. Avec Severi, nous entendons par une correspondance sur la courbe Γ un diviseur sur la surface $\Gamma \times \Gamma$. Au § I, nous définissons, pour les correspondances, une notion d'équivalence, et l'opération du produit de composition : les classes de correspondances se trouvent ainsi former un anneau, sur lequel on définit une fonction linéaire $\sigma(\xi)$, à valeurs entières rationnelles, possédant les propriétés formelles d'une trace. Le § II est consacré à l'étude de cette fonction. Les §§ suivants donnent des applications des résultats du § II, en particulier à la théorie des courbes définies sur un corps de base à un nombre fini d'éléments : dans le § IV se trouvent établies les propriétés élémentaires de la fonction zêta d'une telle courbe (y compris l'hypothèse de Riemann pour cette fonction), et le § V donne les résultats correspondants pour les fonctions L, abéliennes ou non abéliennes.

§ I. L'anneau des correspondances.

1. Les conventions et définitions restent celles de la 1re partie, c'est-à-dire que nous supposons donnés une fois pour toutes une courbe complète Γ sans point multiple, et un corps de définition pour Γ, le corps de base k. Rappelons que tout corps est supposé implicitement contenir le corps de base.

Notre objet est de faire l'étude des diviseurs sur la variété $\Gamma \times \Gamma$ produit de la courbe Γ par elle-même ; c'est là une variété de dimension 2 (une "surface") complète et sans point multiple, définie sur le corps k. Par une *correspondance* appartenant à Γ (ou, comme on dit aussi, une correspondance sur Γ), on entend un diviseur sur $\Gamma \times \Gamma$.

Soient M et N deux points génériques indépendants de Γ par rapport à k : alors $M \times N$ et $N \times M$ sont tous deux des points génériques de $\Gamma \times \Gamma$ par rapport à k. Comme on a $k(M \times N) = k(N \times M)$, il existe (F-IV$_7$, th. 16, cor. 1) une correspondance birationnelle entre la surface $\Gamma \times \Gamma$ et elle-même, dans laquelle $M \times N$ et $N \times M$ sont des points génériques correspondants par rapport à k : cette correspondance, qui est évidemment partout birégulière, sera appelée la *symétrie* sur

$\Gamma \times \Gamma$. Le transformé par symétrie de tout point, de toute courbe ou de tout cycle sur $\Gamma \times \Gamma$ sera appelé son *symétrique*, et dénoté par le signe ' : par exemple, si P et Q sont deux points quelconques de Γ, on a $(P \times Q)' = Q \times P$. La diagonale Δ de $\Gamma \times \Gamma$ est sa propre symétrique, c'est-à-dire qu'on a $\Delta' = \Delta$: et, pour qu'un point de $\Gamma \times \Gamma$ soit son propre symétrique, il faut et il suffit qu'il soit sur Δ. Si φ est une fonction sur $\Gamma \times \Gamma$, elle est transformée par symétrie en une fonction φ' telle que l'on ait $\varphi'(P \times Q) = \varphi(Q \times P)$ chaque fois que $Q \times P$ est un point de $\Gamma \times \Gamma$ où φ soit définie.

Dans le groupe additif $\mathscr{G}$ des correspondances, soit $\mathscr{G}_0$ l'ensemble des diviseurs de la forme (φ), où φ est une fonction sur $\Gamma \times \Gamma$, autre que la constante 0 ; soit $\mathscr{G}_1$, l'ensemble des diviseurs de la forme $(\varphi) + \Gamma \times \mathfrak{a} + \mathfrak{b} \times \Gamma$, où φ est une fonction sur $\Gamma \times \Gamma$, autre que la constante 0, et où $\mathfrak{a}$ et $\mathfrak{b}$ sont deux diviseurs sur Γ ; il résulte de F-VIII$_2$, th. 6, que $\mathscr{G}_0$ et $\mathscr{G}_1$ sont des sous-groupes de $\mathscr{G}$. Si X et Y sont deux correspondances, on écrira $X \sim Y$ si $X - Y$ est dans $\mathscr{G}_0$ et $X \equiv Y$ si $X - Y$ est dans $\mathscr{G}_1$; la relation $X \equiv Y$ signifie donc qu'il existe deux diviseurs $\mathfrak{a}, \mathfrak{b}$ sur Γ tels que l'on ait

$$X \sim Y + \Gamma \times \mathfrak{a} + \mathfrak{b} \times \Gamma.$$

On réservera le nom d'*équivalence*, quand il s'agira de correspondances, à la relation $\equiv$ et, quand il sera question de classes d'équivalence dans l'ensemble des correspondances, ou plus brièvement de *classes de correspondances*, il faudra toujours entendre par là les classes dans le groupe $\mathscr{G}$ suivant le sous-groupe $\mathscr{G}_1$. En conséquence, le groupe quotient $\mathscr{G}/\mathscr{G}_1$ sera appelé le groupe additif des classes de correspondances. L'application $X \to X'$ du groupe $\mathscr{G}$ sur lui-même transforme en eux-mêmes les sous-groupes $\mathscr{G}_0$ et $\mathscr{G}_1$: les relations $X \sim Y$ et $X \equiv Y$ sont donc respectivement équivalentes à $X' \sim Y'$ et à $X' \equiv Y'$; il suit aussi de là que, si ξ est une classe de correspondances (c'est-à-dire une classe dans $\mathscr{G}$ suivant $\mathscr{G}_1$), l'application $X \to X'$ la transforme en une classe de correspondances, qui sera notée ξ'.

Proposition 1. — Soient X, Y deux diviseurs sur $\Gamma \times \Gamma$, tels que le cycle $X.Y$ soit défini. Alors, si $X \sim 0$, on a $\deg(X.Y) = 0$.

Si $X \sim 0$, il y a φ sur $\Gamma \times \Gamma$, telle que $X = (\varphi)$. Si $X.Y$ est défini, Y n'a donc aucune composante commune avec le diviseur (φ), et par suite, d'après F-VIII$_2$, th. 3, φ induit, sur chacune des composantes de Y une fonction qui n'est pas la constante 0. D'après F-VIII$_2$, th. 7, il suit de là que $pr_1[Y.(\varphi)]$ est un diviseur équivalent à 0 sur Γ, donc de degré 0 d'après la prop. 1 de la 1ère partie (n° 2) ; comme la projection algébrique de tout cycle a même degré que ce cycle lui-même, le cycle $Y.(\varphi) = X.Y$ est donc bien de degré 0.

De la prop. 1 résulte la possibilité de définir un symbole $I(X.Y)$, attaché à tout couple de correspondances X, Y, et dont la valeur est égale à $\deg(X.Y)$ quand $X.Y$ est

défini. Pour cela, nous poserons d'abord, par définition, $I(A.B) = \deg(A.B)$ chaque fois que A et B sont des courbes distinctes sur $\Gamma \times \Gamma$; en effet, d'après F-VII$_6$, pr. 16, le cycle $A.B$ est alors défini. Soit d'autre part A une courbe quelconque sur $\Gamma \times \Gamma$; il existe des diviseurs X tels que l'on ait $X \sim A$, et que $X.A$ soit défini ; on obtiendra en effet un tel diviseur en posant $X = A - (\varphi)$, φ étant une fonction sur $\Gamma \times \Gamma$ telle que $v_A(\varphi) = 1$, et il existe de telles fonctions d'après F-VIII$_3$, th. 9 : on posera alors $I(A.A) = \deg(X.A)$: cet entier est bien indépendant du choix de X puisque si X_1 est un diviseur satisfaisant aus conditions imposées à X, on a, d'après la prop. 1.

$$\deg[(X_1 - X).A] = 0,$$

donc $\deg(X_1.A) = \deg(X.A)$. Enfin, si X et Y sont deux correspondances quelconques, et si $\sum_\alpha a_\alpha.A_\alpha$ et $\sum_\beta b_\beta.B_\beta$ sont respectivement des expressions pour X et pour Y, nous poserons

$$I(X.Y) = \sum_{\alpha,\beta} a_\alpha b_\beta . I(A_\alpha.B_\beta)$$

Théorème 1. — Soient X, X_1, et Y, Y_1, des correspondances telles que l'on ait $X \sim X_1$ et $Y \sim Y_1$. Alors on a $I(X.Y) = I(X_1.Y_1)$. Il suffit de montrer qu'on a

$$I(X.Y) = I(X_1.Y) \qquad \text{et} \qquad I(X_1.Y) = I(X_1.Y_1)\ ;$$

démontrons par exemple la première de ces relations. En vertu de la linéarité du symbole I, il suffit de montrer qu'on a

$$I(X.B) = I(X_1.B)$$

si B est une courbe quelconque. Soit m le coefficient de B dans $X - X_1$; alors, si nous posons $Z = X - X_1 - m.B$, B n'est pas une composante de Z, et l'on a $Z \sim -m.B$. Soit W une correspondance telle que l'on ait $W \sim B$ et que $W.B$ soit défini. On a alors, par définition.

$$I[(X - X_1).B] = \deg(Z.B) + m.\deg(W.B) = \deg[(Z + m.W).B]\ ;$$

et le dernier membre de cette relation est nul en vertu de la prop. 1 puisque l'on a $Z + m.W \sim Z + m.B \sim 0$.

2. Par pr_1 et pr_2, nous entendons comme d'habitude (F-VII$_6$) les projections algébriques, sur le premier et le second facteur de $\Gamma \times \Gamma$ respectivement, des cycles sur $\Gamma \times \Gamma$. Si X est une correspondance, nous dénoterons par $d(X)$ et $d'(X)$ les entiers respectivement définis par $pr_1 X = d(X).\Gamma$ et par $pr_2 X = d'(X).\Gamma$. Il est clair que l'on a

$$d'(X) = d(X') \qquad \text{et} \qquad d(X) = d'(X').$$

Soit X une correspondance ; on peut, d'une manière et d'une seule, la mettre sous la forme $X = X_0 + \mathfrak{a} \times \Gamma$, où $\mathfrak{a}$ est un diviseur sur Γ et où X_0 n'a aucune composante de la forme $A \times \Gamma$. Il résulte alors de F-VII$_6$, pr. 16, que $X_0.(P \times \Gamma)$ est défini quel que soit P sur Γ ; de plus, comme deux courbes $P \times \Gamma$ et $Q \times \Gamma$ ne peuvent avoir de point commun à moins de coïncider, on a

$$X.(P \times \Gamma) = X_0.(P \times \Gamma)$$

chaque fois que le premier membre a un sens. Nous conviendrons, une fois pour toutes, si X est une correspondance, X_0 la correspondance définie comme ci-dessus à partir de X, et P un point quelconque de Γ, de désigner par $X(P)$ le diviseur sur Γ défini par la relation $X_0.(P \times \Gamma) = P \times X(P)$: il résulte de F-VII$_6$, th. 13, que cette notation a toujours un sens, et qu'elle comprend comme cas particulier celle qui est définie dans ce dernier théorème. Il revient au même d'écrire $X(P) = pr_2[X_0.(P \times \Gamma)]$; nous généraliserons cette notation en posant $X(\mathfrak{a}) = pr_2[X_0.(\mathfrak{a} \times \Gamma)]$ quand $\mathfrak{a}$ est un diviseur quelconque sur Γ. Il résulte de ce qui précède que $X(\mathfrak{a})$ a toujours un sens, et qu'on a $X(\mathfrak{a}) = pr_2[X.(\mathfrak{a} \times \Gamma)]$ chaque fois que $X.(\mathfrak{a} \times \Gamma)$ est défini, c'est-à-dire chaque fois que les cycles X et $\mathfrak{a} \times \Gamma$ n'ont pas de composante commune. De plus, $X(\mathfrak{a})$ dépend linéairement de X et de $\mathfrak{a}$; autrement dit, on a $X(\mathfrak{a}+\mathfrak{b}) = X(\mathfrak{a})+X(\mathfrak{b})$, et, si l'on a $Z = X + Y$, on a $Z(\mathfrak{a}) = X(\mathfrak{a}) + Y(\mathfrak{a})$.

Cela posé, l'application des th. 12 et 15 de F-VII$_6$, donne les résultats suivants

Théorème 2. — Soient K un corps, et M un point générique de Γ par rapport à K. Soit X un élément du groupe additif $\mathscr{G}_K$ des correspondances rationnelles par rapport à K : alors $X(M)$ est un diviseur sur Γ, rationnel par rapport à $K(M)$: et l'on a $X(M) = 0$ si X est de la forme $\mathfrak{a} \times \Gamma$, où $\mathfrak{a}$ est un diviseur sur Γ, et dans ce cas seulement. De plus, l'application $X \to X(M)$ est un homomorphisme de $\mathscr{G}_K$ sur le groupe additif des diviseurs sur Γ, rationnels par rapport à $K(M)$; et, si $\mathfrak{m}$ est un élément quelconque de ce dernier groupe, il existe un élément X et un seul de $\mathscr{G}_K$, sans composante de la forme $A \times \Gamma$, tel que $X(M) = \mathfrak{m}$: si de plus on a $\mathfrak{m} \succ 0$, on a $X \succ 0$.

C'est là en effet un cas particulier de F-VII$_6$, th, 12, que nous reproduisons ici en raison de l'importance de ce résultat pour la theorie qui nous occupe.

Théorème 3. — Soient X une correspondance, et P un point de Γ : alors on a $\deg[X(P)] = I[X.(P \times \Gamma)] = d(X)$. Plus généralement, si $\mathfrak{a}$ est un diviseur quelconque sur Γ , on a

$$\deg[X(\mathfrak{a})] = I[X.(\mathfrak{a} \times \Gamma)] = d(X).\deg(\mathfrak{a}).$$

Soient $\mathfrak{b}$ le diviseur sur Γ, et X_0 la correspondance sans composante de la forme $A \times \Gamma$ tels que l'on ait $X = X_0 + \mathfrak{b} \times \Gamma$. On a $pr_1(\mathfrak{b} \times \Gamma) = 0$, donc $d(X) = d(X_0)$. D'autre

part, d'après F-VII$_6$, th. 15, on a $\deg[X(P)] = \deg[X_0.(P \times \Gamma)] = d(X_0)$. Alors, pour compléter la démonstration de la première partie de notre théorème, il suffit de faire voir qu'on a $I[(\mathfrak{b} \times \Gamma).(P \times \Gamma)] = 0$. Soit τ une fonction sur Γ, telle que l'on ait $v_P(\tau) = 1$, et posons $\mathfrak{c} = P - (\tau)$, de sorte que P n'est pas un composant de $\mathfrak{c}$. Soit φ la fonction sur $\Gamma \times \Gamma$, telle que l'on ait, quels que soient M et N sur Γ

$$\varphi(M \times N) = \tau(M);$$

alors on a, d'après F-VIII$_2$, th. 1, cor. 4,

$$(\varphi) = (\tau) \times \Gamma = (P - \mathfrak{c}) \times \Gamma.$$

Soit b le coefficient de P dans $\mathfrak{b}$; posons $\mathfrak{b}' = \mathfrak{b} - b.(P - \mathfrak{c})$; alors P n'est pas un composant de $\mathfrak{b}'$, donc $P \times \Gamma$ n'est pas une composante de $\mathfrak{b}' \times \Gamma$; et l'on a $\mathfrak{b} \times \Gamma \sim \mathfrak{b}' \times \Gamma$, donc

$$I[(\mathfrak{b} \times \Gamma).(P \times \Gamma)] = I[(\mathfrak{b}' \times \Gamma).(P \times \Gamma)]$$

d'après le th. 1. Comme on a $(\mathfrak{b}' \times \Gamma).(P \times \Gamma) = 0$, ceci achève la démonstration de la première partie de notre théorème : la seconde s'en déduit immédiatement par linearité.

3. Pour formuler le théorème suivant, il est commode d'introduire dès maintenant une notation générale qui ne nous servira guère dans le présent travail, mais sera très utile dans ceux qui lui feront suite. Soit φ une fonction sur Γ : soit $\mathfrak{a}$ un diviseur sur Γ , sans composant commun avec le diviseur (φ) : si donc $\sum_\alpha a_\alpha.A_\alpha$ est l'expression réduite de $\mathfrak{a}$, on a, quel que soit α, $\varphi(A_\alpha) \neq 0$ et $(A_\alpha) \neq \infty$; dans ces conditions, on posera $\varphi(\mathfrak{a}) = \prod_\alpha \varphi(A_\alpha)^{a_\alpha}$. Si le diviseur $\mathfrak{a}$ se réduit à un point A, le symbole $\varphi(\mathfrak{a})$, s'il est défini, désigne donc la quantité $\varphi(A)$; on a d'autre part $\varphi(\mathfrak{a} + \mathfrak{b}) = \varphi(\mathfrak{a}).\varphi(\mathfrak{b})$ chaque fois que $\varphi(\mathfrak{a})$ et $\varphi(\mathfrak{b})$ sont définis.

Théorème 4. — Soient K un corps, M un point générique de Γ par rapport à K, et φ une fonction sur Γ, ayant K pour corps de définition. Soit X une correspondance, rationnelle par rapport à K, et sans composante de la forme $A \times \Gamma$. Alors il y a une fonction θ sur Γ, définie par rapport à K par la relation $\varphi[X'(M)] = \theta(M)$; et l'on a $(\theta) = X[(\varphi)]$.

C'est là en effet une conséquence immédiate de F-VIII$_2$, th. 7, de F-VIII$_2$, th. 1, cor. 4. et de nos définitions.

Corollaire. — Soient X une correspondance, et $\mathfrak{a}, \mathfrak{b}$ deux diviseurs sur Γ. Alors la relation $\mathfrak{a} \sim \mathfrak{b}$ entraîne $X(\mathfrak{a}) \sim X(\mathfrak{b})$. En particulier, si l'on a $\mathfrak{a} \sim 0$, on a $X(\mathfrak{a}) \sim 0$.

En effet, si l'on a $\mathfrak{a} - \mathfrak{b} = (\varphi)$, il résulte de nos définitions, et du th. 4, qu'on peut construire une fonction θ telle que $X(\mathfrak{a} - \mathfrak{b}) = (\theta)$.

THÉORÈME 5. — Soient K un corps, M un point générique de Γ par rapport à K, et X une correspondance rationnelle par rapport à K. Alors, pour qu'on ait $X(M) \sim 0$, il faut et il suffit qu'il existe un diviseur $\mathfrak{a}$ sur Γ, tel que l'on ait $X \sim \mathfrak{a} \times \Gamma$; et, s'il en est ainsi, on a $X(P) \sim 0$ quel que soit P sur Γ.

Supposons qu'on ait $X(M) \sim 0$; d'après le th. 2, $X(M)$ est rationnel par rapport à $K(M)$; d'après F-VIII$_3$, th. 10, cor. 1, il existe donc sur Γ une fonction θ, ayant $K(M)$ pour corps de définition, telle qu'on ait $(\theta) = X(M)$. Soit N un point générique de Γ par rapport à $K(M)$; alors $\theta(N)$ est un élément de $K(M \times N)$. Soit φ la fonction sur $\Gamma \times \Gamma$, définie par rapport à K par la relation $\theta(N) = \varphi(M \times N)$; et posons $X_1 = (\varphi)$. Il résulte alors de F-VIII$_2$, th. 1. cor. 3, qu'on a $(\varphi).(M \times \Gamma) = M \times (\theta)$, donc $X_1(M) = X(M)$; en vertu du th. 2, $X - X_1$ est donc de la forme $\mathfrak{a} \times \Gamma$, de sorte qu'on a bien $X \sim \mathfrak{a} \times \Gamma$. Soit maintenant P un point quelconque de Γ ; soit τ une fonction sur Γ, telle que $v_P(\tau) = 1$; soit ψ la fonction sur $\Gamma \times \Gamma$, telle que $\psi(R \times S) = \tau(R)$ quels que soient R et S sur Γ ; on a donc, d'après F-VIII$_2$, th. 1, cor. 4, $(\psi) = (\tau) \times \Gamma$. Posons $m = v_{P \times \Gamma}(\varphi)$, et $\varphi_0 = \psi^{-m}.\varphi$, d'où $(\varphi_0) = (\varphi) - m.(\tau) \times \Gamma$; $P \times \Gamma$ n'est donc pas une composante de (φ_0), et par suite φ_0 induit sur $P \times \Gamma$ une fonction qui n'est pas la constante 0 : on a de plus

$$(\varphi_0) = X - [\mathfrak{a} + m.(\tau)] \times \Gamma, \qquad \text{d'où} \qquad (\varphi_0).(P \times \Gamma)) = P \times X(P).$$

Il résulte alors de F-VIII$_2$, th. 4, cor. 1, que $P \times X(P)$ est le diviseur de la fonction induite par φ_0 sur $P \times \Gamma$; on a donc bien $X(P) \sim 0$. Réciproquement, soient X une correspondance, et $\mathfrak{a}$ un diviseur sur Γ, tels que $X \sim \mathfrak{a} \times \Gamma$. Soit φ une fonction telle que ait $(\varphi) = X - \mathfrak{a} \times \Gamma$. Soit K' un corps de définition pour φ, par rapport auquel X et $\mathfrak{a}$ soient rationnels : soient M' et N' des points génériques indépendants de Γ par rapport à K' : soit θ la fonction sur Γ, définie par rapport à $K'(M')$ par la relation $\theta(N') = \varphi(M' \times N')$. Alors, d'après F.VIII$_2$, th. 1, cor. 3, on a $(\varphi).(M' \times \Gamma) = M' \times (\theta)$, donc $(\theta) = X(M')$, et par suite $X(M') \sim 0$. D'après ce qui a été démontré ci-dessus, ceci implique qu'on a $X(P) \sim 0$ quel que soit P sur Γ.

COROLLAIRE. — Soit X une correspondance. Pour qu'on ait $X \equiv 0$, il faut et il suffit qu'on ait $X(\mathfrak{m}) \sim 0$ pour tout diviseur de degré 0 sur Γ.

Supposons en effet qu'on ait $X \equiv 0$, donc $X \sim \mathfrak{a} \times \Gamma + \Gamma \times \mathfrak{b}$ où $\mathfrak{a}$ et $\mathfrak{b}$ sont deux diviseurs sur Γ. En appliquant le th. 5 à $X - \Gamma \times \mathfrak{b}$, on voit qu'on a quel que soit P sur Γ, $X(P) - \mathfrak{b} \sim 0$, donc en général, quel que soit le diviseur $\mathfrak{m}$ sur Γ, $X(\mathfrak{m}) \sim \deg(\mathfrak{m}).\mathfrak{b}$, donc $X(\mathfrak{m}) \sim 0$ si $\mathfrak{m}$ est de degré 0. Réciproquement, supposons que $\deg(\mathfrak{m}) = 0$ entraîne $X(\mathfrak{m}) \sim 0$; soient P un point de Γ, K un corps par rapport auquel X soit rationnel, et M un point générique de Γ par rapport à $K(P)$.

On a $X(M-P) = X(M) - X(P) \sim 0$. Posons $X(P) = \mathfrak{b}$ et $X_1 = X - \Gamma \times \mathfrak{b}$; X_1 est rationnel par rapport à $K(P)$, et l'on a $X_1(M) = X(M) - \mathfrak{b} \sim 0$; d'après le th. 5, il existe donc un diviseur $\mathfrak{a}$ tel que l'on ait $X_1 \sim \mathfrak{a} \times \Gamma$, d'où $X \sim \mathfrak{a} \times \Gamma + \Gamma \times \mathfrak{b}$.

4. Nous définirons maintenant une opération bilinéaire, non commutative, entre correspondances, au moyen du théorème suivant :

THÉORÈME 6. — Soient X et Y deux correspondances. Alors il existe une correspondance Z et une seule, telle que l'on ait, quel que soit le point P sur Γ, $Z(P) = X[Y(P)]$ et $Z'(P) = Y'[X'(P)]$; si de plus K est un corps par rapport auquel X et Y soient rationnels, Z aussi est rationnel par rapport à K : et, si l'on a $X \succ 0, Y \succ 0$, on a $Z \succ 0$. Enfin, Z est donné par la formule

$$Z = pr_{13}[(\Gamma \times X).(Y \times \Gamma)]$$

chaque fois que le second membre a un sens.

Il ne peut exister plus d'une correspondance Z avec les propriétés énoncées dans notre première assertion ; en effet, s'il en existait deux, Z et Z_1, on aurait, quel que soit P,

$$Z_1(P) = Z(P) \qquad \text{et} \qquad Z_1(P) = Z'(P) \ ;$$

si en particulier on prend P générique sur Γ par rapport à un corps par rapport auquel Z et Z_1 soient rationnels, on voit, d'après le th. 2. que $Z - Z_1$, et $Z' - Z'_1$ doivent être tous deux de la forme $\mathfrak{a} \times \Gamma$, donc que $Z - Z_1$ doit être à la fois de la forme $\mathfrak{a} \times \Gamma$ et de la forme $\Gamma \times \mathfrak{a}_1$; et cela n'est possible que si l'on a $Z - Z_1 = 0$. Nous allons maintenant calculer le diviseur $X[Y(P)]$ au moyen de nos définitions et des théorèmes de F-VII$_6$. Supposons d'abord que ni X ni Y n'aient de composante de la forme $A \times \Gamma$. On a alors

$$Y.(P \times \Gamma) = P \times Y(P),$$

donc, d'après F-VII$_6$, th. 11,

$$(Y \times \Gamma).(P \times \Gamma \times \Gamma) = P \times Y(P) \times \Gamma,$$

et par suite

$$(\Gamma \times X).[(Y \times \Gamma).(P \times \Gamma \times \Gamma)] = P \times \{X.[Y(P) \times \Gamma]\}.$$

Le premier membre de cette dernière relation a un sens, en vertu du calcul ci-dessus et par suite de l'hypothèse faite sur X et Y et l'on voit de même, au moyen de F-VII$_6$, pr. 17, que les trois cycles

$$\Gamma \times X, \qquad Y \times \Gamma \qquad P \times \Gamma \times \Gamma$$

se coupent proprement sur $\Gamma \times \Gamma \times \Gamma$: de plus, d'après F-VII$_6$, pr. 16, $\Gamma \times X$ et $Y \times \Gamma$ se coupent proprement sur la même variété, car autrement ils devraient avoir une composante commune, qui serait alors nécessairement de la forme $\Gamma \times A \times \Gamma$, et $A \times \Gamma$ devrait être une composante de X. Dans ces conditions, on peut appliquer à

$$(\Gamma \times X).[(Y \times \Gamma).(P \times \Gamma \times \Gamma)]$$

le principe d'associativité des intersections [F-VII$_6$, th. 10 (v)], qui montre que ce cycle peut aussi s'écrire

$$[(\Gamma \times X).(Y \times \Gamma)].(P \times \Gamma \times \Gamma).$$

Si donc on pose $U = (\Gamma \times X).(Y \times \Gamma)$, on a

$$U.(P \times \Gamma \times \Gamma) = P \times \{X.[Y(P) \times \Gamma]\},$$

d'où, par définition de $X[Y(P)]$ et par application de F-VII$_6$, th. 16,

$$P \times X[Y(P)] = pr_{12}[U.(P \times \Gamma \times \Gamma)] = (pr_{12}U).(P \times \Gamma) ;$$

dans cette formule, comme d'ailleurs dans l'énoncé de notre théorème, pr_{12} désigne bien entendu la projection algébrique de cycles dans $\Gamma \times \Gamma \times \Gamma$ sur le produit partiel formé du premier et du dernier facteur de $\Gamma \times \Gamma \times \Gamma$. Si donc nous posons $Z = pr_{12}U$, on a

$$X[Y(P)] = Z(P).$$

Montrons maintenant que ce résultat reste valable même si X et Y ont des composantes de la forme $A \times \Gamma$, pourvu seulement que le cycle $U = (\Gamma \times X).(Y \times \Gamma)$ soit défini. Posons en effet, dans ce cas, $X = X_0 + \mathfrak{a} \times \Gamma, Y = Y_0 + \mathfrak{b} \times \Gamma$, $\mathfrak{a}$ et $\mathfrak{b}$ étant des diviseurs sur Γ, et X_0 et Y_0 n'ayant pas de composante de la forme $A \times \Gamma$. On a alors, par définition, $Y(P) = Y_0(P)$ et $X[Y(P)] = X_0[Y_0(P)]$: si donc on pose $U_0 = (\Gamma \times X_0).(Y_0 \times \Gamma)$, et $Z_0 = pr_{13}(U_0)$, on a, d'après ce qui a été démontré plus haut, $X_0[Y_0(P)] = Z_0(P)$; d'autre part, il résulte des formules ci-dessus et de F-VII$_6$, th. 11, que, si l'on pose $W = (\Gamma \times \mathfrak{a}).Y_0 + \mathfrak{b} \times \mathfrak{a}$, on a $U = U_0 + W \times \Gamma + \mathfrak{b} \times X_0$, d'où, d'après F-VII$_6$, th. 14, $Z = Z_0 + \mathfrak{c} \times \Gamma$ avec $\mathfrak{c} = pr_1 W + d'(X_0).\mathfrak{b}$, et par conséquent $Z(P) = Z_0(P)$. Considérons maintenant la correspondance birationnelle partout birégulière, entre le produit $\Gamma \times \Gamma \times \Gamma$ et lui-même, qui échange entre eux le premier et le dernier facteur de ce produit, c'est-à-dire qui transforme tout point $M_1 \times M_2 \times M_3$ de ce produit en le point $M_3 \times M_2 \times M_1$; cette correspondance birationnelle transforme les cycles $\Gamma \times X$ et $Y \times \Gamma$ en $X' \times \Gamma$ et $\Gamma \times Y'$, respectivement ; il s'ensuit que si Z est défini comme ci-dessus, on a $Z' = pr_{12}[(X' \times \Gamma).(\Gamma \times Y')]$, et par suite, d'après ce que nous avons démontré, $Z'(P) = Y'[X'(P)]$ quel que soit P. Si donc le cycle $(\Gamma \times X).(Y \times \Gamma)$ est défini, la correspondance Z que nous venons d'étudier a bien les propriétés énoncées dans notre théorème. Si d'autre part le cycle

$(\Gamma \times X).(Y \times \Gamma)$ n'est pas défini alors, d'après F-VII$_0$, pr. 16, $\Gamma \times X$ et $Y \times \Gamma$ ont une composante commune, qui est nécessairement de la forme $\Gamma \times A \times \Gamma$, de sorte que X a une composante de la forme $A \times \Gamma$. Si donc nous posons $X = X_0 + \mathfrak{a} \times \Gamma$, X_0 et $\mathfrak{a}$ ayant le même sens que plus haut, le cycle $Z_0 = pr_{13}[(\Gamma \times X_0).(Y \times \Gamma)]$ aura un sens, et l'on aura, quel que soit P, $Z_0(P) = X_0[Y(P)] = X[Y(P)]$, et $Z_0(P) = Y'[X'_0(P)]$: comme d'ailleurs on a $X'(P) = X'_0(P) + \mathfrak{a}$, on a

$$Y'[X'(P)] = Z'_0(P) + Y'(\mathfrak{a})$$

Il suit de là que, si l'on pose $Z = Z_0 + Y'(\mathfrak{a}) \times \Gamma$, cette correspondance a toutes les propriétés requises par notre théorème.

5. Si X et Y sont deux correspondances, on appellera *produit de composition* de X et Y (on simplement *produit* quand il ne pourra y avoir de confusion) la correspondance Z telle que $Z(P) = X[Y(P)]$ et $Z'(P) = Y'[X'(P)]$ quel que soit P ; ce produit sera noté $X \circ Y$. Il résulte de cette définition qu'on a $(X \circ Y)' = Y' \circ X'$, et aussi, par linéarité, que, si $Z = X \circ Y$, on a $Z(\mathfrak{a}) = X[Y(\mathfrak{a})]$ quel que soit le diviseur $\mathfrak{a}$ sur Γ. De cette dernière propriété, et de la définition du produit de composition, il résulte immédiatement que ce produit est associatif. Comme d'autre part on a $\Delta(P) = P$ quel que soit P sur Γ, donc $\Delta(\mathfrak{a}) = \mathfrak{a}$ quel que soit le diviseur $\mathfrak{a}$, il résulte de notre définition qu'on a $\Delta \circ X = X \circ \Delta = X$ quelle que soit la correspondance X, c'est-à dire que Δ est élément neutre (ou "élément unité") à droite et à gauche pour le produit de composition. Il résulte d'autre part de la définition, et du th. 3, que l'on a $d(X \circ Y) = d(X).d(Y)$, et de même $d'(X \circ Y) = d'(X).d'(Y)$, quelles que soient les correspondances X et Y.

Il résulte d'autre part du Corollaire du th. 5, et du th. 3, que, si l'on a $X \equiv 0$, et si Y est une correspondance quelconque, on a $X \circ Y \equiv 0$: et il résulte du Corollaire du th. 5, et de celui du th. 4, que, si $Y \equiv 0$, et si X est une correspondance quelconque, on a $X \circ Y \equiv 0$. Il suit de là que la *classe* du produit de composition $X \circ Y$ (au sens de la relation d'équivalence $\equiv$) ne dépend que des classes des facteurs X et Y ; si l'on désigne par ξ et η les classes de X et de Y respectivement, la classe de $X \circ Y$ sera désignée par $\xi \cdot \eta$, et sera appelée le produit de ξ et η. La multiplication des classes de correspondances est évidemment distributive, à droite et à gauche, par rapport à l'addition : de ce qui précède, il résulte qu'elle est associative, et qu'elle possède un élément unité, à savoir la classe de Δ ; celle-ci sera désormais désignée par δ. Au moyen de ces définitions, l'ensemble des classes de correspondances se trouve défini comme anneau ; cet anneau sera désigné par $\mathcal{A}$. La transformation $\xi \to \xi'$ de $\mathcal{A}$ en lui-même est alors une anti-involution (ou "anti-automorphisme involutif"), c'est-à-dire que c'est un automorphisme du groupe additif de $\mathcal{A}$ sur lui-même, et qu'on a

$$(\xi')' = \xi \qquad\qquad (\xi \cdot \eta)' = \eta' \cdot \xi'$$

quels que soient ξ et η dans $\mathcal{A}$.

PROPOSITION 2. — Soient X et Y deux correspondances quelconques. Alors on a $I(X.Y') = I[\Delta.(X \circ Y)]$.

Comme les deux membres de la relation à démontrer dépendent linéairement de X et de Y, il nous suffira de démontrer cette relation d'une part dans le cas où X et Y' sont sans composante commune, et d'autre part dans le cas où on a $X = Y' = C$, C étant une courbe quelconque sur $\Gamma \times \Gamma$. Supposons donc d'abord X et Y' sans composante commune. Dans ce cas, le cycle

$$U = (\Gamma \times X).(Y \times \Gamma)$$

est défini sur $\Gamma \times \Gamma \times \Gamma$; en effet, s'il ne l'était pas, $\Gamma \times X$ et $Y \times \Gamma$ auraient une composante commune, qui serait nécessairement de la forme $\Gamma \times A \times \Gamma$, et alors X aurait la composante $A \times \Gamma$, et Y la composante $\Gamma \times A$, de sorte que $A \times \Gamma$ serait une composante commune de X et de Y'. On a donc alors, d'après le th. 6,

$$Z = X \circ Y = pr_{12}U.$$

D'autre part, M et N étant deux points génériques indépendants de Γ par rapport à k, soit Θ le lieu de $M \times N \times M$ par rapport à k sur $\Gamma \times \Gamma \times \Gamma$; la projection de Θ sur le produit partiel formé des deux premiers facteurs de $\Gamma \times \Gamma \times \Gamma$ est partout régulière, et, si $P \times Q$ est un point quelconque de ce produit partiel, le point de Θ dont il est la projection est $P \times Q \times P$. D'après F-VII$_6$, th. 17, cor. 3, il y a donc une correspondance hiunivoque entre les cycles Y sur $\Gamma \times \Gamma$ et les cycles $\overline{Y}$ contenus dans Θ sur $\Gamma \times \Gamma \times \Gamma$, correspondance déterminée par les relations

$$Y = pr_{12}(\overline{Y}), \qquad \overline{Y} = (Y \times \Gamma).\Theta.$$

Si de plus Y est une courbe sur $\Gamma \times \Gamma$, lieu d'un point $P \times Q$ par rapport à un corps K, $\overline{Y}$ est alors la courbe sur Θ qui a Y pour projection, c'est-à-dire que c'est le lieu du point $P \times Q \times P$ par rapport à K ; on a donc alors $Y' = pr_{23}(\overline{Y})$, et, par linéarité, cette relation s'étend à une correspondance quelconque. Nous avons donc, quelle que soit la correspondance $Y.Y' = pr_{23}[(Y \times \Gamma).\Theta]$. Si donc X est une correspondance telle que le cycle

$$T = (\Gamma \times X).[(Y \times \Gamma).\Theta]$$

soit défini sur $\Gamma \times \Gamma \times \Gamma$, il résulte de F-VII$_6$, th. 16, que $X.Y'$ est défini sur $\Gamma \times \Gamma$ et qu'on a $X.Y' = pr_{23}T$, et par suite

$$I(X.Y') = \deg(T).$$

Mais, si une composante C de Y est le lieu d'un point $P \times Q$ par rapport à un corps K, il résulte de ce qui précède que l'intersection $(C \times \Gamma) \cap \Theta$ est le lieu de $P \times Q \times P$

par rapport à K, et ne peut donc être contenue dans une composante de $\Gamma \times X$ que si une composante de X se confond avec le lieu C' de $Q \times P$ par rapport à K, c'est-à-dire si C' est une composante commune de X et de Y'. Si donc, comme nous l'avons supposé, X et Y' n'ont pas de composante commune, les trois cycles $\Gamma \times X, Y \times \Gamma$ et Θ satisfont à la condition de F-VII$_6$, pr. 17, et se coupent donc proprement sur $\Gamma \times \Gamma \times \Gamma$. D'ailleurs, dans ces conditions, $(\Gamma \times X).(Y \times \Gamma)$ est défini, comme nous l'avons montré plus haut. Par conséquent le principe d'associativité des intersections [F-VII$_6$, th. 10 (v)] s'applique aux cycles $\Gamma \times X, Y \times \Gamma$ et Θ ; le cycle désigné plus haut par T est donc défini et peut aussi s'écrire $T = U.\Theta$, avec

$$U = (\Gamma \times X).(Y \times \Gamma).$$

On a donc, dans ces conditions $I(X.Y') = \deg(U.\Theta)$.

Cela posé, si, dans le produit $\Gamma \times \Gamma \times \Gamma$, on échange le second et le troisième facteur (ou, ce qui revient au même, si, après avoir écrit ce produit sous la forme $\Gamma \times (\Gamma \times \Gamma)$, on applique une symétrie au second facteur $\Gamma \times \Gamma$ de ce dernier produit), Θ se trouve transformé en le lieu de $M \times M \times N$ par rapport à k, c'est-à-dire en la variété $\Delta \times \Gamma$. Soit W le cycle transformé de U par la même opération ; comme on a $Z = X \circ Y = pr_{13}U$, on a alors $Z = pr_{12}W$. Comme on a d'autre part $I(X.Y') = \deg(U.\Theta)$, on a

$$I(X.Y') = \deg[W.(\Delta \times \Gamma)].$$

Mais il suit de F-VII$_6$, th. 16, que, puisque $W.(\Delta \times \Gamma)$ est défini, $Z.\Delta$ l'est aussi, et qu'on a $Z.\Delta = pr_{12}[W.(\Delta \times \Gamma)]$. Ceci achève notre démonstration dans le cas où X et Y' sont sans composante commune.

Soit maintenant C une courbe quelconque sur $\Gamma \times \Gamma$, et considérons le cas $X = C, Y = C'$. Soit X_1 une correspondance telle que l'on ait $X_1 \sim C$, et que C ne soit pas une composante de X_1 ; on a alors, par définition, $I(C.C) = I(X_1.C)$, donc, d'après ce que nous avons démontré, $I(C.C) = I[(X_1 \circ C').\Delta]$. Posons

$$d = d(C), \qquad d' = d'(C) = d(C') \ ;$$

on a, d'après le th. 1 du n° 1, et le th. 3 du n° 2,

$$d(X_1) = d \qquad \text{et} \qquad d'(X_1) = d'.$$

D'autre part, la relation $X_1 \sim C$ entraîne a fortiori $X_1 \equiv C$, et par suite $X_1 \circ C' \equiv C \circ C'$; il existe donc des diviseurs $\mathfrak{a}$ et $\mathfrak{b}$ sur Γ tels que l'on ait $X_1 \circ C' \sim C \circ C' + \mathfrak{a} \times \Gamma + \Gamma \times \mathfrak{b}$; on a alors, d'après le th. 1 du n° 1 et le th. 3 du n° 2, $d(X_1 \circ C') = d(C \circ C') + \deg(\mathfrak{b})$, et par suite $\deg(\mathfrak{b}) = 0$ puisque l'on a $d(X_1 \circ C') = d(C \circ C') = d.d'$, et de même $\deg(\mathfrak{a}) = 0$. Mais on a, d'après le th. 1 du n° 1,

$$I[{}'X_1 \circ C').\Delta] = I[(C \circ C' + \mathfrak{a} \times \Gamma + \Gamma \times \mathfrak{b}).\Delta],$$

donc

$$I[(X_1 \circ C').\Delta] = I[(C \circ C').\Delta] + \deg(\mathfrak{a}) + \deg(\mathfrak{b}) = I[(C \circ C').\Delta].$$

On a donc bien $I(C.C) = I[(C \circ C').\Delta]$, ce qui achève notre démonstration.

6. Soit X une correspondance : considérons l'entier

$$S(X) = d(X) + d'(X) - I(X.\Delta).$$

Il est clair que $S(X)$ dépend linéairement de X, et qu'on a

$$S(X') = S(X)$$

Si M est un point générique de Γ par rapport à un corps par rapport auquel X soit rationnel, on a, d'après le th. 3 du n° 2,

$$S(X) = I[X.(M \times \Gamma + \Gamma \times M - \Delta)],$$

et par suite, d'après le th. 1 du n° 1, $S(X) = 0$ si $X \sim 0$, donc aussi $S(X) = S(Y)$ si $X \sim Y$. Si d'autre part A est un point quelconque de Γ, on a $d(A \times \Gamma) = 0, d'(A \times \Gamma) = 1$, et

$$\Gamma[(A \times \Gamma).\Delta] = \deg[\Delta(A)] = 1.$$

et par suite $S(A \times \Gamma) = 0$; on a de même $S(\Gamma \times A) = 0$; par linéarité, il suit de là que l'on a $S(\mathfrak{a} \times \Gamma + \Gamma \times \mathfrak{b}) = 0$ quels que soient les diviseurs $\mathfrak{a}$ et $\mathfrak{b}$ sur Γ. Comme la relation $X \equiv 0$ signifie qu'il existe $\mathfrak{a}$ et $\mathfrak{b}$ tels que l'on ait $X \sim \mathfrak{a} \times \Gamma + \Gamma \times \mathfrak{b}$, il s'ensuit que $X \equiv 0$ entraîne $S(X) = 0$. Par conséquent, si X est une correspondance, l'entier $S(X)$ que nous venons de définir ne dépend que de la classe à laquelle appartient X ; si ξ est cette classe, nous poserons $\sigma(\xi) = S(X)$.

Théorème 7. — L'entier $\sigma(\xi)$ est une fonction linéaire, définie sur l'anneau $\mathcal{A}$ des classes de correspondances ; et l'on a, quels que soient ξ et η dans cet anneau, $\sigma(\xi') = \sigma(\xi)$, et $\sigma(\xi \cdot \eta) = \sigma(\eta.\xi)$.

Il ne nous reste en effet à démontrer que la dernière formule.

Quant à celle-ci, soient X et Y des correspondances de classes respectives ξ et η : d'après la prop. 2 du n° 5, on a

$$\sigma(\xi \cdot \eta) = d(X).d'(Y) + d'(X).d(Y) - I(X.Y');$$

mais, dans cette dernière formule, le second membre ne change pas si on échange X et Y puisqu'on a

$$Y.X' = (X.Y')' \qquad \text{et par suite} \qquad I(Y.X') = I(X.Y').$$

Le th. 7 montre que $\sigma(\xi)$, considérée comme fonction de ξ sur l'anneau $\mathcal{A}$, possède les propriétés formelles d'une trace : nous l'appellerons désormais la *trace* de ξ.

§ II. Propriétés de la trace.

7. Jusqu'ici, nous n'avons fait aucun usage de la théorie des courbes algébriques, telle qu'elle a été exposée dans la 1ère partie ; cette théorie va maintenant être appliquée aux questions qui nous occupent. Nous allons d'abord en déduire la valeur de la trace $\sigma(\delta)$ de l'élément unité δ dans l'anneau des classes de correspondances.

THÉORÈME 8. — On a $\sigma(\delta) = 2g$.

Par définition, on a $\sigma(\delta) = d(\Delta) + d'(\Delta) - I(\Delta.\Delta) = 2 - I(\Delta.\Delta)$. Soit φ une fonction sur $\Gamma \times \Gamma$, telle que l'on ait $v_\Delta(\varphi) = 1$; posons $X = (\varphi) - \Delta$; par définition du symbole I, on a

$$I(\Delta.\Delta) = -\deg(X.\Delta)$$

D'autre part, par définition aussi (1ère partie, § 1, n° 5), le diviseur $\mathfrak{k} = pr_1(X.\Delta)$ est un diviseur canonique sur Γ, de sorte qu'on a, d'après le corollaire du théorème de Riemann-Roch (1ère partie, § I, n° 7), $\deg(\mathfrak{k}) = 2g - 2$, donc $I(\Delta.\Delta) = 2 - 2g$.

Il résulte du th. 8 que, si n est un entier rationnel, on a

$$\sigma(n.\delta) = 2g.n;$$

si donc $g \neq 0, n.\delta$ ne peut être l'élément 0 de l'anneau $\mathcal{A}$ des classes de correspondances que si l'on a $n = 0$. Il s'ensuit que, pour $g \neq 0$, l'ensemble des éléments $n.\delta$ forme un sous-anneau de $\mathcal{A}$, isomorphe à l'anneau des entiers rationnels. On voit en particulier que, pour $g \neq 0$, l'anneau $\mathcal{A}$ a des éléments autres que 0. En revanche, il résulte du corollaire du th. 5, § 1, n° 3, et de la remarque finale du § 1, n° 7, de la 1ère partie, que, si $g = 0$, l'anneau $\mathcal{A}$ se réduit à l'élément 0 ; c'est là, du point de vue des questions qui nous occupent, un cas trivial qui sera désormais laissé de côté ; autrement dit, nous supposons à partir de maintenant, une fois pour toutes, que la courbe Γ est de genre $g \geq 1$.

8. Dans ce qui va suivre, nous aurons besoin du résultat auxiliaire suivant :

LEMME 1. — Soient φ_i, pour $1 \leqslant i \leqslant d$, des fonctions sur Γ, ayant un corps K pour corps de définition, et linéairement indépendantes sur le corps K. Soient $M_1, \ldots, M_d$ d points génériques indépendants de Γ par rapport à K. Alors il n'existe aucune combinaison linaire $\varphi = \sum_{i=1}^{d} c_i \varphi_i$ des φ_i, à coefficients c_i constants et non tous nuls telle que l'on ait $\varphi(M_j) = 0$ pour $1 \leqslant j \leqslant d$; et le déterminant $|\varphi_i(M_j)|$ pour $1 \leqslant i \leqslant d, 1 \leqslant j \leqslant d$, n'est pas nul.

Supposons qu'il existe une fonction φ avec les propriétés ci-dessus, et supposons par exemple que c_1 ne soit pas nul. Posons $c'_k = c_k/c_1$ pour $2 \leqslant h \leqslant d$, et $\psi = \varphi_i + \sum_{h=2}^{d} c'_h \varphi_h$; alors le corps $K(c'_2, \ldots, c'_d)$ est un corps de définition pour ψ ; comme on a $\psi(M_i) = 0$ pour $1 \leqslant i \leqslant d$, les M_i sont des composants du diviseur (ψ), et doivent par conséquent être algébriques sur $K(c'_2, \ldots, c'_d)$; comme ce dernier corps a au plus la dimension $d-1$ sur K, le corps $K(M_1, \ldots, M_d)$ a donc aussi au plus la dimension $d-1$ sur K, ce qui contredit l'hypothèse faite sur les M_i. Si maintenant on avait $|\varphi_i(M_j)| = 0$, on pourrait trouver, dans le corps $K(M_1, \ldots, M_d)$, des quantités c_i non toutes nulles, telles qu'en posant $\varphi = \sum_i c_i \varphi_i$, on ait $\varphi(M_j) = 0$ pour $1 \leqslant j \leqslant d$; ceci contredirait ce qu'on vient de démontrer.

Nous passons maintenant à l'application du théorème de Riemann-Roch à la théorie des correspondances. Cette application se fait par l'intermédiaire du résultat suivant :

PROPOSITION 3. — Dans toute classe de correspondances, il existe une correspondance positive X, sans composante de la forme $A \times \Gamma$, telle que l'on ait $d(X) = g$ et telle de plus que, si K est un corps par rapport auquel X soit rationnel, et M un point générique de Γ par rapport à K, le diviseur $X(M)$ soit de la forme

$$X(M) = \sum_{i=1}^{g} N_i,$$

où les N_i sont g points génériques indépendants de Γ par rapport au corps de base k.

Soit X_1 une correspondance quelconque : posons $d = d(X_1)$. Soit $\mathfrak{a}$ un diviseur de degré d sur Γ. Soit K_1 un corps par rapport auquel X_1 et $\mathfrak{a}$ soient rationnels ; soient $M, M_1, \ldots, M_g$ $g+1$ points génériques indépendants de Γ par rapport à K_1 ; et posons

$$K = K_1(M_1, \ldots M_g).$$

Considérons le diviseur $\mathfrak{m}_1 = X_1(M) - \mathfrak{a} + \sum_{i=1}^{g} M_i$: il est de degré g, et rationnel par rapport à $K(M)$: d'après le théorème de Riemann-Roch, on a $l(\mathfrak{m}_i) > 0$, donc

il existe au moins une fonction φ ayant $K(M)$ pour corps de définition, telle que $(\varphi) \succ -\mathfrak{m}_1$. Posons

$$\mathfrak{m} = \mathfrak{m}_1 + (\varphi);$$

$\mathfrak{m}$ est alors un diviseur positif de degré g, rationnel par rapport à $K(M)$: d'après le th, 2, il existe donc une correspondance positive X, sans composante de la forme $A \times \Gamma$, rationnelle par rapport à K, et telle que $X(M) = \mathfrak{m}$. Posons $Z = X - X_1 + \Gamma \times (\mathfrak{a} - \sum_i M_i)$; la correspondance Z est rationnelle par rapport à K, et l'on a

$$Z(M) = \mathfrak{m} - \mathfrak{m}_1 = (\varphi) \sim 0.$$

donc, d'après le th. 5, $Z \equiv 0$, d'ou $X \equiv X_1$. Posons maintenant

$$\mathfrak{m} = \sum_{i=1}^{g} N_i;$$

$\mathfrak{m}$ est alors rationnel sur le corps $K_2 = K(M, N_1, \ldots, N_g)$; il en est donc de même du diviseur $\mathfrak{b} = \mathfrak{m} - X_1(M) + \mathfrak{a}$. On a

$$(1/\varphi) = \mathfrak{m}_1 - \mathfrak{m} = \sum_{i=1}^{g} M_i - \mathfrak{b},$$

donc $\sum_i M_i \sim \mathfrak{b}$. Mais, d'après la prop. 8 de la 1ère partie, § 1, n° 4 (ou encore, comme il est facile de le vérifier, d'après le lemme 1 ci-dessus et le théorème de Riemann-Roch), on a $l\left(\sum_i M_i\right) = 1$; on a donc aussi $l(\mathfrak{b}) = 1$. Puisque $\mathfrak{b}$ est rationnel par rapport à K_2, il y a donc une fonction ψ sur Γ, ayant K_2 pour corps de définition, telle que l'on ait $(\psi) \succ -\mathfrak{b}$, et toute fonction du module $L(\mathfrak{b})$ ne peut différer de ψ que par un facteur constant ; comme $1/\varphi$ est une telle fonction, on a donc $(1/\varphi) = (\psi)$, d'où $\sum_i M_i = (\psi) + \mathfrak{b}$; le diviseur $\sum_i M_i$ est donc rationnel par rapport à K_2. Il s'ensuit que chacun des M_i est algébrique sur le corps $K_2 = K_1(M, N_1, \ldots N_g)$; si alors la dimension de ce dernier corps sur $K_1(M)$ était moindre que g, il en serait de même de celle de $K_1(M, M_1, \ldots, M_g)$ sur $K_1(M)$, ce qui serait contraire à nos hypothèses sur les points $M, M_1, \ldots, M_g$. Par conséquent les N_i sont des points génériques indépendants de Γ par rapport à $K_1(M)$ et a fortiori par rapport au corps de base k. Soit maintenant K' l'un quelconque des corps par rapport auxquels X est rationnel : soit M' un point générique quelconque de Γ par rapport à K', et posons $X(M') = \sum_i N'_i$. Alors, d'après F-VII$_6$, th. 13, $\sum_i N_i$ est une spécialisation de $\sum_i N'_i$, par rapport à K', donc a fortiori par rapport à k ; si donc les N'_i n'étaient pas des points génériques indépendants de Γ par rapport à k, c'est-à-dire si la dimension de $(N'_1, \ldots, N'_g)$ sur k était moindre que g, il en serait de même a fortiori de celle de $(N_1, ..., N_g)$ sur k,

ce qui contredirait ce que nous venons de démontrer. Ceci achève la démonstration de notre proposition. Remarquons en outre que, d'après ce qui précède, M et N_i sont, quel que soit i, des points génériques indépendants de Γ par rapport à K_1, c'est-à-dire que chacun des points $M \times N_i$ a la dimension 2 sur le corps K_1 ; il en est donc de même de toute spécialisation générique de l'un des $M \times N_i$ par rapport à K_1, et à fortiori de toute spécialisation générique de l'un des $M \times N_i$ par rapport à K. Or, d'après F-VII$_6$, th. 12, (i), appliqué à chacun des cycles premiers rationnels par rapport à $K(M)$ qui figurent dans l'expression de $\mathfrak{m}$ au moyen de tels cycles (F-VII$_6$, th. 9), chaque composante de X est le lieu, par rapport au corps K, de l'un des points $M \times N_i$ ou d'une spécialisation générique de l'un de ces points par rapport à K : si alors une telle composante était algébrique par rapport à K_1, ce serait le lieu du même point par rapport à $\overline{K}_1$, ce qui est impossible, puisque la dimension d'un tel point par rapport à K_1 est 2.

Aucune composante de X n'est donc algébrique par rapport à K_1. Comme d'ailleurs, dans ce qui précède, on peut prendre pour K_1 n'importe quel corps par rapport auquel X_1 et $\mathfrak{a}$ soient rationnels, on peut supposer que K_1 contient un corps arbitrairement donné à l'avance. Il résulte donc de notre démonstration qu'il existe, dans toute classe de correspondances, une correspondance dont aucune composante ne soit algébrique par rapport à un corps donné. Cette remarque nous servira dans la démonstration du th. 11 (§ III, n° 15).

9. La prop. 3 montre en particulier que, si $g = 1$, il existe, dans toute classe de correspondances, une correspondance positive X telle que $d(X) = 1$: on déduit facilement de là les principales propriétés élémentaires de l'anneau des classes de correspondances sur une courbe de genre 1, telles qu'elles ont déjà été établies par Hasse dans des travaux bien connus. Pour cela, nous nous servirons du résultat suivant valable pour les courbes de genre quelconque.

Proposition 4. — Soit X une correspondance positive, sans composante de la forme $A \times \Gamma$, et telle que l'on ait $d(X) = 1$. Alors on a $X \circ X' = d'(X).\Delta$.

Posons $e = d'(X)$, et soit P un point quelconque de Γ. Alors, d'après le th. 3 du § 1, n° 2, $X'(P)$ est un diviseur positif de degré e, qu'on peut écrire sous la forme $X'(P) = \sum_{i=1}^{e} Q_i$: et l'on a alors

$$X.(\Gamma \times P) = \sum_i Q_i \times P,$$

de sorte que chacun des points $Q_i \times P$ est contenu dans une composante de X. D'autre part, d'après le même théorème, $X(Q_i)$ est un diviseur positif de degré 1, donc réduit à un point : comme on a $X.(Q_i \times \Gamma) = Q_i \times X(Q_i)$, et que $Q_i \times P$ est contenu

dans X et dans $Q_i \times \Gamma$, P est un composant de $X(Q_i)$, de sorte qu'on a $X(Q_i) = P$ pour $1 \leqslant i \leqslant e$, et par conséquent $X[X'(P)] = e.P$. Si donc on pose $Z = e.\Delta$, on a bien $Z(P) = X[X'(P)]$ quel que soit P ; comme on a d'autre part $Z' = Z$ et $(X \circ X')' = X \circ X'$, il en résulte bien, par définition de $X \circ X'$, que $Z = X \circ X'$.

THÉORÈME 9. — Si $g = 1$, et si ξ est un élément quelconque, autre que 0, de l'anneau $\mathcal{A}$ des classes de correspondances, on a

$$\xi \cdot \xi' = N.\delta,$$

N étant un entier positif, et par suite $\sigma(\xi \cdot \xi') = 2N > 0$. De plus, on a quel que soit ξ, $\xi + \xi' = \sigma(\xi).\delta$. Plus généralement, tout élément ζ de l'anneau $\mathcal{A}$, tel que l'on ait $\zeta' = \zeta$ est de la forme $n.\delta$, où n est un entier rationnel.

Si on applique la prop. 4 à la correspondance X, de classe ξ, dont l'existence résulte de la prop. 3, on voit qu'on a $\xi \cdot \xi' = N.\delta$ avec $N = d'(X) \geqslant 0$; d'ailleurs, une correspondance positive X pour laquelle on a $d'(X) = 0$ est nécessairement, d'après le th. 2 du § 1, n° 2, de la forme $\Gamma \times \mathfrak{a}$, donc de classe 0, de sorte qu'on a $N > 0$ si $\xi \neq 0$. Il suit de là qu'on a aussi $(\xi + \delta).(\xi' + \delta) = N'.\delta$, avec $N' \geqslant 0$, donc $\xi + \xi' = (N' - N - 1).\delta$, d'où

$$\sigma(\xi) = \sigma(\xi') = 1/2.(N' - N - 1).\sigma(\delta)$$

et par suite $N' - N - 1 = \sigma(\xi)$. Soit alors ζ tel que $\zeta' = \zeta$; on a donc, d'après ce qui précède, $2\zeta = \sigma(\zeta).\delta$; il s'ensuit qu'il y a un entier n tel qu'en posant $\zeta_1 = \zeta - n.\delta$, on ait, suivant que $\sigma(\zeta)$ est pair ou impair, soit $2\zeta_1 = 0$, soit $2\zeta_1 = \delta$: dans le premier cas, on a $0 = \sigma(2\zeta_1.2\zeta_1') = 4\sigma(\zeta_1\zeta_1')$, donc $\zeta_1 = 0$: dans le second cas, on a $2\zeta_1.2\zeta_1' = \delta$, donc $4\sigma(\zeta_1\zeta_1') = \sigma(\delta) = 2$, ce qui est impossible. On a donc $\zeta_1 = 0$, d'où $\zeta = n.\delta$. Observons que l'entier N, attaché au moyen de la première formule de notre théorème à tout élément ξ de $\mathcal{A}$, n'est autre que l'invariant fondamental $N(\mu)$ employé par Hasse dans les travaux auxquels nous avons fait allusion plus haut.

10. Passons à l'étude des courbes de genre quelconque. Soit d'abord, d'une manière générale, X une correspondance positive, rationnelle par rapport à un corps K, et sans composante de la forme $A \times \Gamma$. Posons $d(X) = d, d'(X) = e$. Soit M un point générique de Γ par rapport à K, et posons $X(M) = \sum_{i=1}^{d} N_i$. Posons d'autre part $U = (\Gamma \times X).(X' \times \Gamma)$; ce cycle est bien défini sur $\Gamma \times \Gamma \times \Gamma$, car, si $\Gamma \times X$ et $X' \times \Gamma$ avaient une composante commune, celle-ci serait de la forme $\Gamma \times A \times \Gamma$, et $A \times \Gamma$ serait une composante de X. Cela étant, U est un cycle rationnel par rapport à K, et l'on a, d'après le th. 6 du § 1, n° 4, $X \circ X' = pr_{13}U$. Calculons le cycle $U.(\Gamma \times M \times \Gamma)$; il est défini, en vertu de F-VII$_6$, th. 12 (ii) ; de plus, d'après F-VII$_6$, th. 12 (ii) et

F-VII$_6$, th. 11, les cycles $\Gamma \times M \times \Gamma$ et $\Gamma \times X$ se coupent proprement sur $\Gamma \times \Gamma \times \Gamma$ et l'on a

$$(\Gamma \times M \times \Gamma).(\Gamma \times X) = \Gamma \times M \times X(M);$$

il s'ensuit, d'après F-VII$_6$, th. 10, cor., qu'on a

$$U.(\Gamma \times M \times \Gamma) = [\Gamma \times M \times X(M)].(X' \times \Gamma),$$

donc, d'après F-VII$_6$, th. 11,

$$U.(\Gamma \times M \times \Gamma) = [(\Gamma \times M).X'] \times X(M).$$

On a d'autre part $(\Gamma \times M).X' = [(M \times \Gamma).X]' = X(M) \times M$. Par conséquent, on a $U.(\Gamma \times M \times \Gamma) = X(M) \times M \times X(M)$. Désignons maintenant par $\tilde{U}$ le cycle transformé de U par la correspondance birationnelle entre le produit $\Gamma \times \Gamma \times \Gamma$ et lui-même qui échange entre eux les deux premiers facteurs de ce produit ; on a alors

$$X \circ X' = pr_{23}\tilde{U}, \qquad \text{et} \qquad \tilde{U}.(M \times \Gamma \times \Gamma) = M \times X(M) \times X(M).$$

D'ailleurs $\tilde{U}$ est un cycle positif, dont aucune composante n'a, sur le premier facteur de $\Gamma \times \Gamma \times \Gamma$, une projection réduite à un point : en effet, si une composante de $\tilde{U}$ avait, sur ce facteur, une projection réduite à un point A, elle serait contenue dans $A \times \Gamma \times \Gamma$ et U aurait donc une composante W contenue dans $\Gamma \times A \times \Gamma$; W serait aussi contenue dans une composante de $\Gamma \times X$, donc, puisque $X \succ 0$, dans une composante de $(\Gamma \times A \times \Gamma).(\Gamma \times X) = \Gamma \times A \times X(A)$, de sorte que sa projection sur le troisième facteur de $\Gamma \times \Gamma \times \Gamma$ serait l'un des composants B de $X(A)$; on voit de même que la projection de W sur le premier facteur du même produit serait un point C, de sorte que W devrait se réduire au point $C \times A \times B$, ce qui est impossible puisque U est de dimension 1.

On voit donc que $\tilde{U}$ est un cycle rationnel par rapport à K, dont aucune composante n'a, sur le premier facteur de $\Gamma \times \Gamma \times \Gamma$, une projection réduite à un point, et qu'on a

$$\tilde{U}.(M \times \Gamma \times \Gamma) = M \times X(M) \times X(M);$$

et, d'après F-VII$_6$, th. 12 (iii), $\tilde{U}$ est caractérisé d'une manière unique par ces propriétés. Avec les notations de ce théorème, nous pouvons écrire

$$\tilde{U}(M) = X(M) \times X(M) = \sum_{i,j} N_i \times N_j = \sum_i N_i \times N_i + \sum_{i \neq j} N_i \times N_j.$$

Mais, puisque le cycle $X(M) = \sum_i N_i$ est rationnel par rapport à $K(M)$, il en est de même, en vertu des définitions, du cycle $\sum_i N_i \times N_i$; il suit alors de là et de la formule

qui précède (ou bien de F-VII$_6$, pr. 18) que le cycle $\sum_{i\neq j} N_i \times N_j$ aussi est rationnel par rapport à $K(M)$. D'après F-VII$_6$, th. 12 (iii), il existe donc sur $\Gamma\times\Gamma\times\Gamma$ deux cycles V_0 et V_1 rationnels par rapport à K et dont aucune composante n'a sur le premier facteur de $\Gamma\times\Gamma\times\Gamma$ une projection réduite à un point, tels respectivement que l'on ait

$$V_0(M) = \sum_i N_i \times N_i, \qquad \text{et} \qquad V_1(M) = \sum_{i\neq j} N_i \times N_j \ ;$$

et, d'après ce même théorème, on a alors $\tilde{U} = V_0 + V_1$, donc, d'après ce qui précède, $X \circ X' = pr_{23}(V_0) + pr_{23}(V_1)$. Si de plus Λ est l'une quelconque des composantes de V_0, il résulte de F-VII$_6$, th. 12 (i) que Λ est le lieu de l'un des points $M \times N_i \times N_i$, par rapport à K, ou le conjugué de l'un de ces lieux sur le corps K ; de toute manière, Λ est donc contenue dans $\Gamma\times\Delta$, de sorte que la projection de Λ sur le produit des deux derniers facteurs de $\Gamma\times\Gamma\times\Gamma$ est contenue dans Δ : on a donc $pr_{23}(V_0) = m.\Delta$, m étant un certain entier ; et l'on a alors $pr_2(V_0) = m.\Gamma$. Mais, si on applique l'opérateur pr_{12} aux deux membres de la relation $\sum_i M \times N_i \times N_i = V_0.(M\times\Gamma\times\Gamma)$, on obtient, en vertu de F-VII$_6$, th. 16, $\sum_i M \times N_i = pr_{12}(V_0).(M\times\Gamma)$, donc, d'après le th. 2 du § I, n° 2, et en tenant compte de ce qui précède, $pr_{12}(V_0) = X$, d'où $pr_2(V_0) = pr_2(X) = e.\Gamma$; ceci donne $m = e$, et par conséquent $pr_{23}(V_0) = e.\Delta$. Nous avons donc démontré qu'on a $X \circ X' = e.\Delta + pr_{23}(V_1)$.

11. Si, dans ce qui précède, on suppose qu'on a $d = 1$, on a $V_1(M) = 0$, donc $V_1 = 0$ et $X \circ X' = e.\Delta$; on retrouve ainsi le résultat de la prop 4 du n° 9. Supposons donc, à partir de maintenant, qu'on a $d \geqslant 2$. Sur la variété $\Pi = \Gamma\times\Gamma\times\ldots\times\Gamma$, produit de $d+1$ facteurs identiques à Γ, il existe, en vertu de F-VII$_6$, pr. 18, et de F-VII$_6$, th. 12 (iii), un cycle positif Z, rationnel par rapport à K, dont aucune composante n'ait sur le premier facteur du produit Π une projection réduite à un point, et satisfaisant à la relation

$$Z.(M\times\Gamma\times\ldots\times\Gamma) = M \times \sum_{(i)} N_{i_1} \times N_{i_2} \times \ldots \times N_{i_d},$$

la somme du second membre étant étendue aux d ! permutations $(i_1, \ldots, i_d)$ des entiers $(1, 2, \ldots, d)$. Nous allons montrer que la projection algébrique de Z sur le produit partiel de Π formé des trois premiers facteurs est donnée par $pr_{123}Z = (d-2)\,!\,V_1$, V_1 étant le cycle défini au n° 10. Soit en effet $V_2 = pr_{123}Z$; en appliquant à la relation $Z.(M\times\Gamma\times\ldots\times\Gamma) = M \times \sum_{(i)} N_{i_1} \times \ldots N_{i_d}$, l'opérateur pr_{123}, on obtient, d'après F-VII$_6$, th. 16,

$$V_2.(M\times\Gamma\times\Gamma) = (d-2)\,!\,M \times \sum_{i\neq j} N_i \times N_j,$$

c'est-à-dire $V_2.(M\times\Gamma\times\Gamma) = (d-2)\,!\,V_1.(M\times\Gamma\times\Gamma)$. De plus, d'après la définition de Z, V_2 ne peut avoir de composante dont la projection sur le premier facteur

de $\Gamma \times \Gamma \times \Gamma$ soit réduite à un point. D'après F-VII$_6$, th. 12 (iii), on a donc bien $V_2 = (d-2)\,!\,V_1$. Il s'ensuit que l'on a $pr_{23}Z = (d-2)\,!\,pr_{23}(V_1)$. Si donc on pose $Y = pr_{23}(V_1)$, on a d'une part $pr_{23}Z = (d-2)\,!\,Y$, et de l'autre, d'après ce qu'on a démontré plus haut, $Y = X \circ X' - e.\Delta$.

Posons maintenant $T = pr_{2,3,\ldots,d+1}(Z)$: en d'autres termes, désignons par T la projection algébrique du cycle Z sur le produit partiel de Π formé des d derniers facteurs. Nous avons alors $pr_{23}T = (d-2)\,!\,Y$. D'ailleurs Z, et par conséquent T, ne changent pas si on effectue sur les d derniers facteurs du produit Π une permutation quelconque : il s'ensuit qu'on a $pr_{ij}T = (d-2)\,!\,Y$ pour tout couple d'indices distincts (i,j) pris parmi les entiers $2, 3, \ldots, d+1$. De plus, en vertu de F-VII$_6$, th. 12 (i), appliqué aux cycles premiers rationnels par rapport à $K(M)$ dont le cycle

$$\sum_{(i)} N_{i_1} \times \ldots \times N_{i_d}$$

est combinaison linéaire, toute composante de Z est le lieu, par rapport à $\overline{K}$, de l'un des points $M \times N_{i_1} \times \ldots \times N_{i_d}$, ou bien est le conjugué d'un tel lieu par rapport à K.

12. Nous avons ainsi défini, sur le produit $\Omega = \Gamma \times \Gamma \times \ldots \times \Gamma$ de d facteurs identiques à Γ, un cycle positif T dont la projection algébrique sur tout produit partiel de Ω formé de deux facteurs soit le cycle $(d-2)\,!\,Y$. Comme c'est uniquement de Ω qu'il va être question maintenant, et que nous n'avons plus besoin de la variété Π, nous numéroterons $1, 2, \ldots, d$ (au lieu de $2, 3, \ldots, d+1$) les facteurs du produit Ω. On a donc, après ce changement de notation, $pr_{ij}T = (d-2)\,!\,Y$ pour tout couple d'indices distincts (i,j) pris parmi les entiers $1, 2, \ldots, d$. Comme d'ailleurs on a

$$d(Y) = d(X).d(X') - e = (d-1).e,$$

il s'ensuit qu'on a $pr_iT = (d-1)\,!\,e.\Gamma$ pour $1 \leqslant i \leqslant d$.

Designons maintenant par Δ_{12} la sous-variété du produit définie par $\Delta_{12} = \Delta \times \Gamma \times \ldots \times \Gamma$, les facteurs Γ dans le second membre étant en nombre $d-2$; et désignons par Δ_g la variété qui se déduit de Δ_{12} par une permutation des facteurs de Ω qui transforme les premier et second facteurs en les $i^{ième}$ et $j^{ième}$ facteurs, respectivement ; Δ_g est donc la sous-variété de Ω, de dimension $d-1$, dont les points ont même projection sur le $i^{ième}$ et sur le $j^{ième}$ facteur de Ω. Comme T n'est pas changé par une permutation des facteurs de Ω, les cycles $T.\Delta_g$ sont tous définis si l'un d'entre eux est défini, et ils ont alors tous même degré, égal par exemple au degré de

$$T.\Delta_{12} = T.(\Delta \times \Gamma \times \ldots \times \Gamma).$$

Mais, en appliquant à ce dernier cycle l'opérateur pr_{12}, on obtient, d'après F-VII$_6$, th. 16, $pr_{12}(T.\Delta_{12}) = (pr_{12}T).\Delta = (d-2)\,!\,(Y.\Delta)$; si donc les cycles $T.\Delta_{ij}$ sont

définis, ils sont tous de degré égal à $(d-2)\,!\deg(Y.\Delta)$.

Soit de même $\mathfrak{d}$ un diviseur sur Γ ; désignons par D_1 le diviseur sur Ω défini par $D_1 = \mathfrak{d} \times \Gamma \times \ldots \times \Gamma$, les facteurs Γ dans le second membre étant en nombre $d-1$, et par D_i, pour $i = 1, 2, ..., d$, les diviseurs qui se déduisent de D_1 par les permutations des facteurs de Ω ; on a donc $D_i = \Gamma \times \ldots \times \Gamma \times \mathfrak{d} \times \Gamma \times \ldots \times \Gamma$, le second membre étant formé de $i-1$ facteurs égaux à Γ, du facteur $\mathfrak{d}$ et de $d-i$ facteurs Γ, pris dans cet ordre. On voit comme plus haut, au moyen de F-VII$_6$, th. 16, appliqué à l'opérateur pr_1 et à la relation

$$T.D_1 = T.(\mathfrak{d} \times \Gamma \times \ldots \times \Gamma),$$

et au moyen de la relation $pr_1 T = (d-1)\,!\,e.\Gamma$, que, si l'un des cycles $T.D_i$ est défini, ils le sont tous, et qu'ils sont alors de degré égal à $(d-1)\,!\,e.\deg(\mathfrak{d})$.

13. Supposons maintenant qu'il existe d fonctions φ_i sur Γ, linéairement indépendantes sur le corps des constantes, ayant le corps K pour corps de définition, telles que l'on ait $(\varphi_i) \succ -\mathfrak{d}$ pour $1 \leqslant i \leqslant d, \varphi_i(N_j) \neq \infty$ pour $1 \leqslant i \leqslant d, 1 \leqslant j \leqslant d$, et telles que déterminant $|\varphi_i(N_j)|$ ne soit pas nul. Soient $M_1, \ldots, M_d$ d points génériques indépendants de Γ par rapport à K, de sorte que

$$M_1 \times M_2 \times \ldots \times M_d$$

est un point générique de Ω par rapport à K. Considérons la fonction Φ sur Ω, définie par rapport à K par la relation

$$\Phi(M_1 \times \ldots \times M_d) = |\varphi_i(M_j)|;$$

il résulte des hypothèses ci-dessus que Φ est définie au point $N_1 \times \ldots \times N_d$, et en chacun des points $N_{i_1} \times \ldots \times N_{i_d}$ qui se déduisent de celui-ci par une permutation des facteurs, et qu'elle prend en chacun de ces points une valeur finie non nulle. Comme on a vu que toute composante du cycle T est le lieu d'un de ces points par rapport à K, ou bien est le conjugué d'un tel lieu par rapport à K, il s'ensuit que Φ est définie sur toute composante de T et induit sur chacune de ces composantes une fonction autre que la constante 0. En vertu de F-VIII$_2$, th. 7, il suit de là que le cycle $T.(\Phi)$ est défini sur Ω, et que sa projection sur l'un quelconque des facteurs de Ω est un diviseur équivalent à 0, donc de degré 0 ; par conséquent le cycle $T.(\Phi)$ lui-même est de degré 0.

Nous allons maintenant faire voir qu'on a $(\Phi) \succ \sum_{i \neq j} \Delta_{ij} - \sum_i D_i$. Soit en effet $(i) = (i_1, \ldots, i_d)$ l'une quelconque des $d\,!$ permutations de $(1, 2, \ldots, d)$; soit $\Phi_{(i)}$ la fonction sur Ω, définie par rapport à K par la relation $\Phi_{(i)}(M_1 \times \ldots \times M_d) = \varphi_{i_1}(M_1) \ldots \varphi_{i_d}(M_d)$; il résulte de F-VIII$_2$, th. 1, cor. 4, et de F-VIII$_2$, th. 6, que l'on a

$$(\Phi_{(i)}) = (\varphi_{i_1}) \times \Gamma \times \ldots \times \Gamma + \Gamma \times \varphi_{i_2}) \times \ldots \times \Gamma + \Gamma \times \ldots \times \Gamma \times (\varphi_{i_d}),$$

et par conséquent $(\Phi_{(i)}) \succ -\sum_i D_i$; comme Φ elle-même est combinaison linéaire des $\Phi_{(i)}$ avec des coefficients égaux à ± 1, on a donc anssi, d'après F-VIII$_2$, th. 6, $(\Phi) \succ -\sum_i D_i$. D'autre part, d'après F-VIII$_1$, pr. 5, Φ est définie sur chacune des variétés Δ_{ij} ; considérons par exemple la variété Δ_{12} ; le point $M_1 \times M_1 \times M_3 \times \ldots \times M_d$ est un point générique de Δ_{12} par rapport à K, et la valeur de Φ en ce point est un déterminant dont deux colonnes sont identiques et par suite s'annule ; Δ_{12}, et de même tous les Δ_{ij} sont donc des composantes du diviseur $(\Phi)_0$; comme toutes ces variétés sont distinctes les unes des autres et distinctes aussi de toutes les variétés D_i, on a donc bien $(\Phi) \succ \sum_{(i,j)} \Delta_{ij} - \sum_i D_i$. Nous pouvons donc écrire $(\Phi) = R + \sum_{(i,j)} \Delta_{ij} - \sum_i D_i$, R étant un diviseur positif. Comme les variétés Δ_{ij} sont des composantes de (Φ), et qu'on a vu que le cycle $T.(\Phi)$ est défini, les cycles $T.\Delta_{ij}$ sont donc définis. Supposons d'autre part que les cycles $T.D_i$ soient définis : d'après ce qu'on a vu sur les composantes de T, il faut et il suffit pour cela qu'aucun des points N_i ne soit un composant de $\mathfrak{d}$. Dans ces conditions, la relation $R = (\Phi) - \sum_{(i,j)} \Delta_{ij} + \sum_i D_i$ implique que le cycle $T.R$ est défini ; c'est alors nécessairement un cycle positif, puisque T et R sont positifs, de sorte qu'on a $\deg(T.R) \geqslant 0$.

On a donc

$$T.(\Phi) = T.R + \sum_{(i,j)} (T.\Delta_{ij}) - \sum_i (T.D_i), \qquad \deg\,[T.(\Phi)] = 0,$$

$$\deg\,(T.R) \geqslant 0, \qquad \deg\,(T.\Delta_{ij}) = (d-2)\,!\,\deg\,(Y.\Delta).$$

$$\deg(T.D_i) = (d-1)\,!\,e.\,\deg\,(\mathfrak{d}).$$

De toutes ces relations résulte qu'on a $\deg(Y.\Delta) \leqslant 2e.\deg(\mathfrak{d})$.

Mais on a $X \circ X' = Y + e.\Delta$, donc, si l'on désigne par ξ et η, respectivement, les classes des correspondances X et Y,

$$\xi \cdot \xi' = \eta + e.\delta, \qquad \text{d'où} \qquad \sigma(\xi \cdot \xi') = \sigma(\eta) + 2eg\ ;$$

on a d'autre part, par définition, $\sigma(\eta) = d(Y) + d'(Y) - \deg(Y.\Delta)$; comme on a déjà vu plus haut qu'on a $d(Y) = d'(Y) = (d-1)e$, on a donc $\sigma(\eta) \geqslant 2e[d - 1 - \deg(\mathfrak{d})]$, et par conséquent

$$\sigma(\xi \cdot \xi') \geqslant 2e[d + g - 1 - \deg(\mathfrak{d})].$$

14. Maintenant, supposant qu'on a $g \geqslant 2$, et supposant la classe ξ donnée, prenons pour X la correspondance de classe ξ dont l'existence résulte de la prop. 3 ; prenons pour $\mathfrak{d}$ un diviseur canonique $\mathfrak{k}$ sur Γ, rationnel par rapport au corps de base k ; et

prenons pour $\varphi_1, \ldots, \varphi_g$ une base du module $L(\mathfrak{d}) = L(\mathfrak{k})$, composée de g fonctions ayant k pour corps de définition (cf. 1ère partie, § 1. n° 3, prop. 3, et le corollaire du théorème de Riemann-Roch, ibid., n° 7). On a $\deg(\mathfrak{k}) = 2g - 2$. D'autre part, d'après la prop. 3, on a $d = d(X) = g$; comme d'ailleurs, d'après la prop. 3, les N_i sont des points génériques indépendants de Γ par rapport à k, ils ne peuvent être des composants de $\mathfrak{k}$, de sorte que les cycles $T.D_i$ considérés ci-dessus sont bien définis ; pour une raison analogue, on a bien $\varphi_i(N_j) \neq \infty$ pour $1 \leqslant i \leqslant g, 1 \leqslant j \leqslant g$ et il résulte du lemme 1 du n° 8 qu'on a $|\varphi_i(N_j)| \neq 0$. Toutes les hypothèses qui ont été introduites au cours de la discussion des nos 10-13 au sujet de X, de $\mathfrak{d}$, et des φ_i, sont donc bien vérifiées ici. Il s'ensuit que l'inégalité finale du n° 13 est satisfaite si l'on y fait $d = g$, et $\deg(\mathfrak{d}) = 2g - 2$, e désignant comme précédemment l'entier $e = d'(X)$ défini au moyen de la correspondance X ci-dessus. On a donc $\sigma(\xi \cdot \xi') \geqslant 2e$. Mais, X étant une correspondance positive, on a $e \geqslant 0$; et on ne peut avoir $e = 0$, en vertu du th. 2 du n° 2, que si X est de la forme $\Gamma \times \mathfrak{a}$, donc si l'on a $\xi = 0$. Il est donc démontré que, si $g \geqslant 2$, on a $\sigma(\xi \cdot \xi') > 0$ pour $\xi \neq 0$. En tenant compte des résultats obtenus plus haut pour $g = 1$ (th. 9 du n° 9) et pour $g = 0$, nous pouvons énoncer notre résultat sous une forme indépendante de la valeur de g :

THÉORÈME 10. — Quel que soit l'élément ξ, autre que 0, de l'anneau $\mathcal{A}$ des classes de correspondances, on a $\sigma(\xi \cdot \xi') > 0$.

§ III. Conséquences de $\sigma(\xi\xi') > 0$.

15. Le th. 10 va nous permettre en premier lieu d'établir la relation entre la notion d'équivalence des correspondances, telle qu'elle a été définie ci-dessus, et les notions d'"équivalence numérique" et d'"équivalence continue" (cf. F-IX$_7$). Cette relation est donnée par les résultats suivants :

THÉORÈME 11. — Soit X une correspondance telle que $X = 0$; alors il existe des entiers a, b tels que l'on ait, quelle que soit la correspondance Y.$I(X.Y) = a.d(Y) + b.d'(Y)$. Réciproquement, soit X une correspondance telle qu'il existe des entiers a, b et des courbes A_i en nombre fini sur $\Gamma \times \Gamma$, ayant la propriété suivante : quelle que soit la courbe B sur $\Gamma \times \Gamma$, distincte des A_i et des composantes de X, on a $\deg(X.B) = a.d(B) + b.d'(B)$; alors on a $X \equiv 0$.

La première partie est une conséquence immédiate du th. 1, du th. 3 et des définitions ; on doit y prendre $a = d'(X), b = d(X)$. Quant à la réciproque, supposons d'abord qu'on a $a = b = 0$. Soit K un corps de définition commun pour les A_i et pour toutes les composantes de X : il résulte de la remarque qui termine la démonstration de la prop. 3 du n° 8 qu'il y a une correspondance Z, équivalente à X, dont aucune

composante n'est algébrique sur K ; les composantes de Z sont alors distinctes des A_i et des composantes de X de sorte que notre hypothèse sur X implique qu'on a

$$\deg(X.Z) = 0.$$

D'autre part, d'après notre hypothèse sur X, si M est un point générique de Γ par rapport à K, on a $\deg[X.(M \times \Gamma)] = 0$, donc, d'après le th. 3, $d(X) = 0$; et l'on a de même $d'(X) = 0$. Soit alors ξ la classe de X ; comme on a $Z \equiv X$, $X \circ Z'$ est de classe $\xi\xi'$, et on a donc, d'après la prop. 2 du n° 5,

$$\sigma(\xi\xi') = d(X).d(Z') + d'(X).d'(Z') - \deg(X.Z) :$$

de plus, d'après ce qu'on vient de démontrer, le second membre de cette dernière relation est nul. On a donc $\sigma(\xi\xi') = 0$, d'où $\xi = 0$, c'est-à-dire $X \equiv 0$, d'après le th. 10. Ceci achève la démonstration dans le cas où l'on a $a = b = 0$. Si maintenant a et b ont des valeurs quelconques, il suffit, pour démontrer notre assertion, de prendre sur Γ des diviseurs $\mathfrak{a}$ et $\mathfrak{b}$ de degrés respectifs a et b, et d'appliquer ce qui précède à $X - \Gamma \times \mathfrak{a} - \mathfrak{b} \times \Gamma$.

THÉORÈME 12. — Soient W une variété, Z un diviseur sur le produit $W \times \Gamma \times \Gamma$, et P, Q deux points simples de W tels que les cycles $Z.(P \times \Gamma \times \Gamma)$ et $Z.(Q \times \Gamma \times \Gamma)$ soient définis sur $W \times \Gamma \times \Gamma$. Alors les correspondances X et Y respectivement définies par

$$Z.(P \times \Gamma \times \Gamma) = P \times X \qquad \text{et par} \qquad Z.(Q \times \Gamma \times \Gamma) = Q \times Y$$

sont équivalentes.

Par linéarité, il suffit de considérer le cas où Z se réduit à une variété. D'autre part, d'après le th. 11, il suffira de montrer que, si A est une courbe quelconque sur $\Gamma \times \Gamma$, distincte des composantes de X et de Y, on a $\deg(X.A) = \deg(Y.A)$. Considérons en effet, sur $W \times \Gamma \times \Gamma$, les trois variétés Z, $P \times \Gamma \times \Gamma$ et $W \times A$; $Z.(P \times \Gamma \times \Gamma)$ est défini par hypothèse ; $(P \times \Gamma \times \Gamma).(W \times A)$ est défini et égal à $P \times A$ d'après F-VII$_6$, th. 11 ; et $Z.(W \times A)$ est défini car autrement, d'après F-VII$_6$, pr. 16, on aurait $Z = W \times A$, donc

$$Z.(P \times \Gamma \times \Gamma) = P \times A$$

d'où $X = A$. contrairement à l'hypothèse que A n'est pas une composante de X. De plus, Z et $P \times A$ se coupent proprement sur $W \times \Gamma \times \Gamma$, car autrement, d'après F-VII$_6$, pr. 16, $P \times A$ devrait être contenu dans Z, et serait donc une composante de $Z.(P \times \Gamma \times \Gamma)$, de sorte que A serait une composante de X. Il suit de là qu'on peut appliquer à $Z.P \times \Gamma \times \Gamma$ et $W \times A$ le principe d'associativité des intersections [F-VII$_3$, th. 10 (v)] si l'on pose $U = Z.(W \times A)$, il s'ensuit qu'on a $(W \times A).(P \times X) = U.(P \times \Gamma \times \Gamma)$, c'est-à-dire $P \times (A.X) = U.(P \times \Gamma \times \Gamma)$, ou, avec les notations de F-VII$_6$, th. 13,

$A.X = U(P)$. On voit de même qu'on a $A.Y = U(Q)$, II résulte de là, et de F-VII$_6$, th. 13, que les cycles $A.X = U(P)$ et $A.Y = U(Q)$, étant tous deux spécialisations d'un même cycle de dimension 0, ont même degré, on peut aussi se servir de F-VII$_6$, th. 15, d'où résulte que, si on définit un entier m par $pr_w U = m.W$, on a deg $[U(P)]$ = deg $[U(Q)]$ = m. On a donc bien, dans les conditions indiquées, deg $(A.X)$ = deg $(A.Y)$, ce qui, comme nous l'avons dit, démontre notre théorème.

Corollaire. — Dans toute classe de correspondances, il existe une correspondance rationnelle par rapport au corps $\overline{k}$.

Nous allons montrer d'abord que, si K est un corps, $K(u)$ une extension de K de dimension 1, et X une correspondance rationnelle par rapport à $K(u)$, il existe une correspondance X_1, équivalente à X, et rationnelle par rapport à $\overline{K}$. Soit en effet C la courbe lieu du point (u) par rapport au corps $\overline{K}$; d'après F-IV$_1$, pr. 3, et F-IV$_6$, th. 12, il existe sur C un point simple (u') algébrique par rapport à K. Sur $C \times \Gamma \times \Gamma$, il existe, d'après F-VII$_6$, th. 12 (iii), un cycle Z, rationnel par rapport à K, tel que l'on ait

$$Z.[(u) \times \Gamma \times \Gamma] = (u) \times X,$$

et sans composante dont la projection sur C soit réduite à un point. La variété $(u') \times \Gamma \times \Gamma$ n'est donc pas une composante de Z, et par suite, d'après F-VII$_6$, pr. 16, le cycle $Z.[(u') \times \Gamma \times \Gamma]$ est défini ; il est alors de la forme $(u') \times X_1$, X_1 étant une correspondance rationnelle par rapport à K, et équivalente à X en vertu du th. 12 ; ceci démontre l'assertion faite plus haut. Soit maintenant X une correspondance quelconque d'après F-VII$_1$, th. 3. cor., il y a un plus petit corps (contenant, comme il est toujours implicitement supposé, le corps de base k) qui soit corps de définition pour toutes les composantes de X : de plus, ce corps est une extension de k, engendrée sur k par des quantités en nombre fini : soit n sa dimension sur k. Il résulte alors de ce qui précède, par récurrence sur n, que X est équivalente à une correspondance rationnelle par rapport à k.

16. Il résulte de l'inégalité $\sigma(\xi\xi') > 0$ pour $\xi \neq 0$ que, si ξ est un élément quelconque, autre que 0, de l'anneau $\mathcal{A}$ des classes de correspondances, et si n est un entier rationnel non nul, on a $n.\xi \neq 0$. Autrement dit, le groupe additif des éléments de $\mathcal{A}$ n'a pas d'élément d'ordre fini.

On sait qu'on peut alors, comme suit, plonger $\mathcal{A}$ dans un anneau qui soit aussi un module sur le corps des rationnels. Considérons l'ensemble des couples (ξ, n) d'un élément ξ de $\mathcal{A}$ et d'un entier n non nul ; la relation $n_2\xi_1 = n_1\xi_2$ entre éléments (ξ_1, n_1) et (ξ_2, n_2) de cet ensemble est une relation d'équivalence ; car elle est réflexive et symétrique et, si l'on a $n_2\xi_1 = n_1\xi_2$ et $n_3\xi_2 = n_2\xi_3$, on a

$$n_2(n_3\xi_1 - n_1\xi_3) = 0,$$

donc, d'après ce qui précède, $n_3\xi_1 = n_1\xi_3$. On note alors ξ/n la classe d'équivalence à laquelle appartient, par rapport à la relation ainsi définie, l'élément (ξ, n). Alors, comme il est facile de le vérifier, si ξ/n et η/m sont de telles classes, les classes $(n\eta + m\xi)/nm$ et $\xi\eta/nm$ dépendent seulement des classes ξ/n et η/m ; et les opérations sur les classes qui sont ainsi définies ont toutes les propriétés requises de l'addition et de la multiplication dans un anneau. Soit $\mathcal{A}_0$ l'anneau dont les éléments sont les classes ξ/n, et dont les opérations d'addition et de multiplication sont celles qu'on vient de définir ; les éléments de $\mathcal{A}_0$ de la forme $\xi/1$ forment un sous-anneau de $\mathcal{A}_0$, isomorphe à l'anneau $\mathcal{A}$, qui sera identifié avec celui-ci. D'autre part, si ξ/n est un élément de $\mathcal{A}_0$, et si $\rho = r/s$ est un nombre rationnel, r et s étant des entiers rationnels dont le second n'est pas nul, il est facile de voir que l'élément $(r\xi)/(sn)$ de $\mathcal{A}_0$ ne dépend que de ρ et de ξ/n ; on l'écrira $\rho.(\xi/n)$; on vérifie facilement aussi que $\mathcal{A}_0$ se trouve ainsi défini comme module sur le corps des rationnels, et que les éléments $\rho.\delta$ de $\mathcal{A}_0$, quand ρ parcourt le corps des rationnels, forment un sous-anneau de $\mathcal{A}_0$ isomorphe à ce dernier corps. On étendra l'anti-involution $\xi \to \xi'$, et la trace $\sigma(\xi)$, à l'anneau $\mathcal{A}_0$, en posant

$$(\xi/n)' = \xi'/n, \qquad \text{et} \qquad \sigma(\xi/n) = \sigma(\xi)/n \ ;;$$

il est clair que toutes les propriétés principales de ces deux symboles, telles qu'elles ont été établies plus haut, s'étendent immédiatement à l'anneau $\mathcal{A}_0$.

L'anneau $\mathcal{A}_0$ étant un module sur le corps des rationnels, il possède sur ce corps une base formée d'éléments α, linéairement indépendants, en nombre égal à son rang, fini ou infini (on démontrera d'ailleurs plus tard que ce rang est toujours fini). La loi de multiplication dans $\mathcal{A}_0$ peut alors être définie par la table de multiplication des α_ρ qui est de la forme $\alpha_\mu\alpha_\nu = \sum_\rho c_{\mu\nu\rho}\alpha_\rho$, les seconds membres étant des sommes à coefficients rationnels, contenant au plus un nombre fini de termes non nuls. Cela posé, on désignera par $\mathcal{A}_c$ l'anneau dont le groupe additif est un module sur le corps des nombres complexes, ayant pour base l'ensemble des α_ν, la table de multiplication des α_ν étant la même que dans $\mathcal{A}_0$. Si alors α est un élément quelconque de $\mathcal{A}_c$, défini par conséquent par une somme finie $\alpha = \sum_\nu u_\nu\alpha_\nu$ à coefficients complexes u_ν, on posera $\alpha' = \sum_\nu \overline{u}_\nu\alpha'_\nu$ (en désignant comme d'habitude par $\overline{u}_\nu$ l'imaginaire conjugué de u_ν), et $\sigma(\alpha) = \sum_\nu u_\nu.\sigma(\alpha_\nu)$. Dans ces conditions, l'application $\alpha \to \alpha'$ est une anti-involution de l'anneau $\mathcal{A}_c$. Quant à la trace σ, il est clair que c'est une fonction linéaire à valeurs complexes, et qu'on a $\sigma(\alpha\beta) = \sigma(\beta\alpha)$ et $\sigma(\alpha') = \overline{\sigma(\alpha)}$ quels que soient α et β dans $\mathcal{A}_c$. De plus, on a aussi $\sigma(\alpha\alpha') > 0$ quel que soit α autre que 0, dans $\mathcal{A}_c$. Si en effet α est un élément de $\mathcal{A}_c$, autre que 0, on peut l'écrire sous la forme $\alpha = \sum_\lambda (u_\lambda + i.v_\lambda).\xi_\lambda$, où les u_λ et v_λ sont des nombres réels non tous nuls et où les ξ_λ sont des éléments de $\mathcal{A}$. Posons $F(u) = \sum_{\lambda,\mu} \sigma(\xi_\lambda, \xi'_\mu).u_\lambda u_\mu$; c'est là une forme quadratique à coefficients entiers, et il résulte du th. 10 (n° 14) qu'elle prend

des valeurs positives (non nulles) chaque fois qu'on donne aux u_λ des valeurs entières non nulles ; elle est donc définie positive. On a alors $\sigma(\alpha\alpha') = F(u) + F(v) > 0$.

De ce qui précède, on déduit le résultat suivant :

PROPOSITION 5. — L'anneau $\mathcal{A}_c$ ne contient pas d'élément symétrique nilpotent, autre que 0, c'est-à-dire qu'il ne contient pas d'élément $\alpha \neq 0$ tel que l'on ait $\alpha' = \alpha$, et $\alpha^n = 0$ pour n assez grand.

Supposons en effet qu'on ait $\alpha = \alpha' \neq 0$; posons, pour $m \geqslant 0, \alpha_m = \alpha^{2^m}$; on a donc $\alpha'_m = \alpha_m$ donc $\alpha_{m+1} = \alpha_m.\alpha'_m$. On voit alors, par récurrence sur m, qu'on a $\alpha_m \neq 0$ quel que soit m ; en effet, si $\alpha_m \neq 0$, on doit avoir $\sigma(\alpha_m.\alpha'_m) \neq 0$, donc $\alpha_{m+1} = \alpha_m.\alpha'_m \neq 0$.

Si donc $\mathscr{B}$ est un sous-anneau symétrique de $\mathcal{A}_c$ (c'est-à-dire un sous-anneau transformé en lui-même par la symétrie $\alpha \to \alpha'$), il ne peut y avoir dans $\mathscr{B}$ d'idéal autre que (0) dont tous les éléments soient nilpotents. En effet, soit $\mathfrak{N}$ un tel idéal, par exemple un idéal à droite, et soit η un élément de $\mathfrak{N}$: alors $\eta\eta'$ est symétrique et est dans $\mathfrak{N}$, donc nilpotent ; on a donc $\eta\eta' = 0$ d'après la prop. 5, donc $\sigma(\eta\eta') = 0$ et par suite $\eta = 0$. Si en particulier un sous-anneau symétrique de $\mathcal{A}_c$ est un module de rang fini sur un certain corps, c'est une algèbre semi-simple sur ce corps.

17. Convenons pour un moment, pour abréger le langage. d'appeler algèbre de type S une algèbre $\mathscr{B}$ sur le corps des rationnels où sont définies une anti-involution $\beta \to \beta'$ et une fonction $\sigma(\beta)$ à valeurs complexes, cette dernière dépendant linéairement de β et satisfaisant aux conditions

$$\sigma(\beta_1, \beta_2) = \sigma(\beta_2, \beta_1), \qquad \sigma(\beta') = \overline{\sigma(\beta)}, \qquad \text{et} \qquad \sigma(\beta\beta') > 0 \ \text{ pour } \ \beta \neq 0.$$

Il résulte du raisonnement ci-dessus que toute algèbre de type S est semi-simple. Toute algèbre de matrices à coefficients complexes, de rang fini sur le corps des rationnels, et douée de symétrie hermitienne (c'est-à-dire qui, en même temps qu'une matrice M, contient toujours la transposée ${}^i\overline{M}$ de l'imaginaire conjuguée de M), est de type S ; car l'anti-involution $M \to {}^i\overline{M}$, et la trace $\mathrm{Tr}(M)$, y possèdent les propriétés requises ; en particulier, toute algèbre de groupe définie au moyen d'un groupe fini (sur le corps des rationnels, ou plus généralement sur un corps de nombres algébriques de degré fini qui soit son propre imaginaire conjugué) est donc de type S. Plus généralement, si S est une matrice hermitienne positive définie, toute algèbre de matrices à coefficients complexes, de rang fini sur le corps des rationnels, transformée en elle-même par l'anti-involution $M \to M' = S.{}^i\overline{M}.S^{-1}$ est de type S si l'on prend pour trace la fonction $\mathrm{Tr}(S.M)$: ce cas se ramène d'ailleurs au précédent en écrivant S sous la forme $S = X.{}^i\overline{X}$ et passant à la représentation de l'algèbre

en question, définie par $N = X^{-1}.M.X$. On voit que le problème de la recherche de toutes les algèbres de type S généralise le problème dit des matrices de Riemann (comme il est naturel si on songe à l'origine de celui-ci, et aux considérations qui nous ont amenés à définir les algèbres de type S) ; il peut être traité par la méthode qui a servi à H. Weyl dans l'étude de ce dernier problème[3]. Observons seulement ici que, si une algèbre de type S est décomposée en somme directe d'algèbres simples, chacune de celles-ci, comme il est facile de le voir, est nécessairement symétrique, c'est-à-dire transformée en elle-même par l'anti-involution $\beta \to \beta'$, et est donc elle-même de type S : le problème se ramène donc à la recherche des algèbres simples de type S. L'étude d'une telle algèbre peut alors se poursuivre par l'extension du corps de base, soit au corps des nombres réels, soit au corps des nombres complexes, et par l'extension correspondante (semblable à celle qui a été effectuée plus haut pour passer de l'anneau $\mathcal{A}_0$ à l'anneau $\mathcal{A}_c$) de l'anti-involution $\beta \to \beta'$ et de la trace $\sigma(\beta)$; on déduit facilement de là, entre autres, que toute algèbre de type S est isomorphe à une algèbre de matrices douée de symétrie hermitienne.

On peut se demander si l'anneau $\mathcal{A}_0$ lui-même, tel que nous l'avons défini au n° 16, est une algèbre de type S (c'est-à-dire s'il est de rang fini sur le corps des rationnels), et si σ est la trace d'une représentation matricielle de $\mathcal{A}_0$. Dans le mémoire qui fait suite à celui-ci, on démontrera que la réponse à ces deux questions est affirmative. Plus précisément, on définira, par la considération des classes de diviseurs d'ordre fini sur la courbe Γ, des représentations de l'anneau $\mathcal{A}$ par des matrices de degré $2g$ sur l'anneau des entiers l-adiques, l étant un nombre premier quelconque autre que la caractéristique p du corps de base : ces représentations auront toutes la trace σ ; et, de leur étude, on déduira que le groupe additif des éléments de $\mathcal{A}$ possède une base finie, donc que $\mathcal{A}_0$ est de rang fini sur le corps des rationnels. Le fait que $\mathcal{A}_0$ est de type S apporte alors, comme on a vu, des renseignements assez précis un sujet des structures dont cet anneau est susceptible ; il s'y ajoute les indications fournies par les représentations l-adiques auxquelles nous venons de faire allusion. En revanche, la recherche de toutes les structures que peut présenter l'anneau $\mathcal{A}$ reste un problème fort peu avancé, et cela même dans le cas classique où le corps des constantes est celui des nombres complexes, et où l'on peut donc faire usage de la topologie combinatoire et des fonctions thêta.

§ IV. Application à la fonction ζ (hypothèse de Riemann).

18. Dans ce §, nous supposerons, en plus des hypothèses faites précédemment, que le corps de base k n'a qu'un nombre fini q d'éléments, ce qui implique bien entendu que la caractéristique p n'est pas 0, et que q est une puissance de p. Alors, comme on sait, si n est un entier quelconque, il existe, dans la fermeture algébrique $\overline{k}$ de k,

[3] H. Weyl, Generalized Riemann matrices and factor sets, *Ann. of Math.*, 37 (1936), p. 709.

une extension de k de degré n et une seule, qui est un corps à q^n éléments que nous désignerons par k_n ; on a donc $k_1 = k$; de plus, m et n étant deux entiers quelconques, on a $k_m \subset k_n$, si n est multiple de m, et dans ce cas seulement. Les éléments de k sont les racines du polynome $X^{q^n} - X$; l'application $(\alpha \to \alpha^q)$ est un automorphisme du domaine universel $\mathbf{K}$, dont la $n^{ième}$ puissance, c'est-à-dire l'automorphisme $(\alpha \to \alpha^{q^n})$ de $\mathbf{K}$, laisse invariants les éléments de k_n, et ceux-là seulement.

Sur chacun des représentants de la courbe (abstraite) Γ, il ne peut y avoir, pour une valeur donnée de n, qu'un nombre fini de points à coordonnées dans k_n. Il s'ensuit que les points P de Γ, tels que l'on ait $k(P) \subset k_n$, sont en nombre fini : ce nombre sera désigné par ν_n.

Si $\mathfrak{a}$ est un diviseur positif de degré m sur Γ, rationnel par rapport à k, il pout (d'après F-VII$_6$, th. 9) être exprimé comme somme de diviseurs premiers rationnels par rapport à k, dont chacun est de degré au plus égal à m ; si donc P est l'un quelconque des composants de $\mathfrak{a}$, on voit (d'après F-VII$_6$, pr. 15) que $k(P)$ est une extension algébrique de k de degré au plus égal à m : d'après ce qui précède, il n'y a donc, pour chacun des composants de $\mathfrak{a}$, et par suite pour $\mathfrak{a}$ lui-même, qu'un nombre fini de possibilités. Autrement dit, si m est un entier donné, les diviseurs positifs de degré m sur Γ , rationnels par rapport à k, sont en nombre fini ; ce nombre sera désigné par D_m.

Considérons maintenant l'identité formelle

$$\sum_{\mathfrak{a}} u^{\deg(\mathfrak{a})} = \prod_{\mathfrak{p}} (1 - u^{\deg(\mathfrak{p})})^{-1},$$

où la somme du premier membre est étendue à tous les diviseurs positifs $\mathfrak{a}$ sur Γ, rationnels par rapport à k, et le produit du second membre à tous les diviseurs $\mathfrak{p}$ premiers rationnels par rapport à k sur Γ. D'après un raisonnement classique d'Euler, cette identité est formellement une conséquence du théorème en vertu duquel tout diviseur positif sur Γ, rationnel par rapport à k, peut s'écrire d'une manière et d'une seule comme somme de diviseurs premiers rationnels par rapport à k (F-VII$_6$, th. 9). D'autre part, il est facile de vérifier qu'en tout point où la série est absolument convergente, le produit l'est aussi et a même valeur que la série.

Il résulte d'ailleurs de la définition de l'entier D_m que le premier membre de l'identité ci-dessus peut aussi s'écrire $\sum_{m=0}^{\infty} D_m u^m$; nous allons montrer que cette série a un rayon de convergence positif et définit une fonction rationnelle de u. Ce sera là une conséquence du théorème de Riemann-Roch et de la proposition suivante :

Proposition 6. — Soit $\mathfrak{a}$ un diviseur sur la courbe Γ, rationnel par rapport au corps de base k à q éléments. Alors le nombre de diviseurs positifs sur Γ, rationnels

par rapport à k et équivalents à $\mathfrak{a}$, est égal à $(q^{l(\mathfrak{a})}-1)/(q-1)$.

Désignons en effet par $L_0(\mathfrak{a})$ l'ensemble des fonctions φ sur Γ autres que la constante 0, ayant k pour corps de définition, et telles que $(\varphi) \succ -\mathfrak{a}$. D'après la prop. 3 de la 1ère partie (§ 1, n° 3), si l'on adjoint à l'ensemble $L_0(\mathfrak{a})$ la constante 0, on obtient un module de rang $l(\mathfrak{a})$ sur le corps k, qui a donc $q^{l(\mathfrak{a})}$ éléments : l'ensemble $L_0(\mathfrak{a})$ a donc lui-même $q^{l(\mathfrak{a})}-1$ éléments. Soit φ un élément de $L_0(\mathfrak{a})$, et posons $\mathfrak{b}=(\varphi)+\mathfrak{a}$; alors $\mathfrak{b}$ est un diviseur positif, rationnel par rapport à k, et équivalent à $\mathfrak{a}$. Réciproquement, si $\mathfrak{b}$ est un tel diviseur, il y a (d'après F-VIII$_2$, th. 10, cor. 1) une fonction φ dans $L_0(\mathfrak{a})$, telle que l'on ait $(\varphi)=\mathfrak{b}-\mathfrak{a}$; de plus, les fonctions dans $L_0(\mathfrak{a})$ qui ont la même propriété sont les $q-1$ fonctions $c\varphi$, où c est un élément quelconque de k autre que 0, et celles-là seulement ; en effet, pour que φ_1 soit une telle fonction, il faut et il suffit que φ_1 soit dans $L_0(\mathfrak{a})$ et qu'on ait $(\varphi_1)=(\varphi)$, donc $(\varphi_1/\varphi)=0$, c'est-à-dire, d'après F-VIII$_2$, th. 2, que φ_1/φ soit une constante, dont la valeur (par exemple d'après le lemme 1 de la 1ère partie, n° 1) est alors nécessairement un élément de k autre que 0. La relation $(\varphi)=\mathfrak{b}-\mathfrak{a}$ établit donc une correspondance, entre diviseurs positifs $\mathfrak{b}$ sur Γ, rationnels par rapport à k et équivalents à $\mathfrak{a}$, et fonctions φ appartenant à $L_0(\mathfrak{a})$, où, à toute fonction φ correspond un seul diviseur $\mathfrak{a}$, et où tout diviseur $\mathfrak{a}$ correspond à $q-1$ fonctions φ. Comme les éléments de $L_0(\mathfrak{a})$ sont en nombre $q^{l(\mathfrak{a})}-1$, ceci démontre notre proposition.

Considérons maintenant les degrés de tous les diviseurs rationnels par rapport à k sur Γ : ces degrés forment un module d'entiers, et leur ensemble est donc identique à l'ensemble des multiples d'un certain entier positif δ. Soit $\mathfrak{a}_0$ un diviseur de degré δ, rationnel par rapport à k. Choisissons d'autre part un entier ν tel que l'on ait $\nu\delta \geqslant g$; et, parmi les diviseurs positifs de degré $\nu\delta$, rationnels par rapport à k, diviseurs qui sont en nombre fini, choisissons un ensemble maximal de diviseurs $\mathfrak{a}_1,\ldots,\mathfrak{a}_h$ inéquivalents. Il résulte alors de la prop. 6, et du théorème de Riemann-Roch, que tout diviseur de degré $\nu\delta$, rationnel par rapport à k, est équivalent à l'un des diviseurs $\mathfrak{a}_1,\ldots,\mathfrak{a}_h$ et à un seul.

Soit maintenant $\mathfrak{a}$ un diviseur positif quelconque, rationnel par rapport à k : son degré est de la forme $n\delta$: alors le diviseur $\mathfrak{a}-(n-\nu)\mathfrak{a}_0$, est de degré $\nu\delta$, donc équivalent à l'un des $\mathfrak{a}_i$, et à un seul. Si donc nous posons, pour $1 \leqslant i \leqslant h$, et pour $n \geqslant 0$, $\mathfrak{a}_{i,n}=\mathfrak{a}+(n-\nu)\mathfrak{a}_0$, tout diviseur positif, rationnel par rapport à k, est équivalent à l'un des $\mathfrak{a}_{i,n}$, et à un seul ; et s'il est équivalent à $\mathfrak{a}_{i,n}$, son degré est $n\delta$.

On voit donc que l'entier désigné plus haut par D_m est nul si $m \not\equiv 0 \pmod{\delta}$, et que l'on a, quel que soit l'entier n

$$D_{n\delta}=\sum_{i=1}^{h}\frac{q^{l(\mathfrak{a}_{i,n})}-1}{q-1}.$$

En particulier, pour $n > (2g-2)/\delta$, on a, d'après le théorème de Riemann-Roch, $l(\mathfrak{a}_{i,n}) = n\delta - g + 1$ pour $1 \leqslant i \leqslant h$, et par conséquent $D_{n\delta} = h(q^{n\delta-g+1}-1)/(q-1)$. Il résulte de là que la série $\sum_{m=0}^{\infty} D_m u^m$ coïncide, à un nombre fini de termes près, avec le développement suivant les puissances de u de la fraction rationnelle

$$\frac{h}{q-1} \cdot \left[\frac{q^{1-g}}{1-q^{\delta}u^{\delta}} - \frac{1}{1-u^2} \right] ;$$

elle a donc un rayon de convergence égal à $1/q$, et définit elle-même une fonction rationnelle de u ; celle-ci sera désormais désignée par $Z(u)$, et s'appellera la fonction zêta attachée à la courbe Γ et au corps de base k. Nous avons donc, pour $|u| < 1/q$:

$$Z(u) = \sum_{\mathfrak{a}} u^{\deg(\mathfrak{a})} = \sum_{m=0}^{\infty} D_m u^m = \prod_{\mathfrak{p}} (1 - u^{\deg(\mathfrak{p})})^{-1}.$$

19. Avant d'aller plus loin, observons que notre définition de la fonction zêta, qui diffère en apparence de celle qui a été donnée par F. K. Schmidt (à la suite des travaux d'Artin) au moyen de la théorie des corps de fonctions algébriques à corps de constantes fini, lui est substantiellement équivalente. Tout d'abord, en effet, il résulte de F-App. I que toute courbe, définie par rapport à un corps k, est birationnellement équivalente, par rapport à k, à une courbe complète et il résulte de F-App. II que toute courbe complète, définie par rapport à un corps "parfait" k, est birationnellement équivalente, par rapport à k, à une courbe complète, sans point multiple. Comme tout corps fini est parfait, il s'ensuit que tout corps de fonctions algébriques d'une variable sur un corps de base fini k, au sens des travaux de F. K. Schmidt et de H. Hasse, est isomorphe au corps abstrait Ω_k des fonctions ayant k pour corps de définition sur une courbe complète Γ sans point multiple, définie par rapport à k. Cela posé, soit $\mathfrak{p}$ un diviseur premier rationnel par rapport à k sur Γ, et soit P l'un des composants de $\mathfrak{p}$; alors l'entier $v_P(\varphi)$ définit une valuation du corps Ω_K donc un "diviseur premier du corps Ω_K", au sens des travaux des auteurs cités ci-dessus. On voit facilement alors que cette correspondance, entre nos diviseurs premiers rationnels par rapport à k sur Γ , et les "diviseurs premiers du corps Ω_K" au sens de ces auteurs, est biunivoque ; et, si l'on identifie ceux-ci avec ceux-là, il en résulte une identification du groupe additif de nos diviseurs rationnels par rapport à k sur Γ avec le groupe (écrit multiplicativement dans les travaux cités) des diviseurs attachés au corps Ω_K par la théorie des valuations. De plus, si l'on fait cette identification, les notions de "diviseur d'une fonction", et de "degré d'un diviseur", se trouvent être les mêmes dans l'une et l'autre théorie. De ces faits, dont la vérification ne présente pas de difficulté, il résulte que nos fonctions zêta sont les mêmes que celles de F. K. Schmidt.

Nous aurions donc le droit d'appliquer à nos fonctions zêta tous les résultats des auteurs cités, et en particulier l'équation fonctionnelle de $Z(u)$. Pour la commodité

du lecteur, nous allons reproduire la démonstration de celle-ci. Observons d'abord que, puisqu'il existe des diviseurs canoniques rationnels par rapport à k, le degré $2g-2$ d'un tel diviseur est multiple de l'entier δ défini plus haut : posons $2g-2=\rho\delta$. De l'expression donnée tout à l'heure pour $D_{n\delta}$ résulte que l'on peut écrire

$$(q-1).Z(u)=F(u)+h.R(u).$$

où $F(u)$ et $R(u)$ sont un polynome, et une fonction rationnelle, respectivement définis par

$$F(u)=\sum_{n=0}^{\rho}\sum_{i=1}^{h}q^{l(\mathfrak{a}_{i,n})}.u^{n\delta}$$

et par

$$\begin{aligned}R(u) &= -\sum_{n=0}^{\rho}u^{n\delta}+\sum_{n=\rho+1}^{\infty}(q^{n\delta-g+1}-1).u^{n\delta}\\ &= -\frac{1}{1-u^{\delta}}+q^{1-g}.\frac{(qu)^{(\rho+1)\delta}}{1-(qu)^{\delta}}\end{aligned}$$

On vérifie immédiatement, par calcul direct, qu'on a

$$R(1/qu)=q^{1-g}.u^{2-2g}.R(u).$$

Pour voir que $F(u)$ satisfait à une relation analogue, appliquons le théorème de Riemann-Roch. Soit $\mathfrak{k}$ un diviseur canonique, rationnel par rapport à k ; on a $l(\mathfrak{a}_{i,n})=\deg(\mathfrak{a}_{i,n})-g+1+l(\mathfrak{k}-\mathfrak{a}_{i,n})$. Mais on a $\deg(\mathfrak{a}_{i,n})=n\delta$; d'autre part, puisque tout diviseur de degré $n\delta$ est équivalent à l'un des diviseurs $\mathfrak{a}_{1,n},\ldots,\mathfrak{a}_{h,n}$ et à un seul, tout diviseur de degré $(\rho-n)\delta$ est équivalent à l'un des diviseurs $\mathfrak{k}-\mathfrak{a}_{i,n}\ \ (1\leqslant i\leqslant h)$ et à un seul : ceci implique que les classes d'équivalence auxquelles appartiennent les h diviseurs $\mathfrak{a}_{i,\rho-n},\ \ (1\leqslant i\leqslant h)$ sont les mêmes, à une permutation près, que celles auxquelles appartiennent les h diviseurs $\mathfrak{k}-\mathfrak{a}_{i,n}\ \ (1\leqslant i\leqslant h)$. Les h entiers $l(\mathfrak{k}-\mathfrak{a}_{i,n})$, pour $1\leqslant i\leqslant h$, sont donc les mêmes, à l'ordre près, que les entiers $l(\mathfrak{a}_{i,\rho-n})$ pour $1\leqslant i\leqslant h$. On a donc :

$$F(u)=\sum_{n=0}^{\rho}\sum_{i=1}^{h}q^{n\delta-g+1+l(\mathfrak{a}_{i,\rho-n})}.u^{n\delta},$$

et par suite

$$\begin{aligned}F(1/qu) &= q^{1-g}.\sum_{n=0}^{\rho}\sum_{i=1}^{h}q^{l(\mathfrak{a}_{i,\rho-n})}.u^{-n\delta}\\ &= q^{1-g}.u^{2-2g}.\sum_{n=0}^{\rho}\sum_{i=1}^{h}q^{l(\mathfrak{a}_{i,\rho-n})}.u^{(\rho-n)\delta}\\ &= q^{1-g}.u^{2-2g}.F(u).\end{aligned}$$

On a donc l'équation fonctionnelle de $Z(u)$:

$$Z(1/qu) = q^{1-g}.u^{2-2g}.Z(u).$$

Les auteurs cités plus haut ont démontré aussi que l'entier δ a nécessairement la valeur 1, et que $Z(u)$ est donc de la forme $P(u)/(1-u)(1-qu)$, $P(u)$ étant un polynôme de degré $2g$; nous retrouverons plus loin ces résultats par une autre voie.

20. De l'expression de $Z(u)$ par un produit infini, telle qu'elle a été donnée plus haut, on déduit immédiatement le développement en série de $d[\log\ Z(u)]$ dans le cercle $|u| < 1/q$:

$$d[\log\ Z(u)] = \sum_{\mathfrak{p}} \sum_{\rho=1}^{\infty} \deg(\mathfrak{p}).u^{\rho.\deg(\mathfrak{p})}.du/u.$$

ce qui peut aussi s'écrire :

$$d[\log\ Z(u)] = \sum_{n=1}^{\infty} c_n u^n.du/u, \qquad c_n = \sum_{deg(\mathfrak{p})/n} \deg(\mathfrak{p}).$$

la somme dans l'expression de c_n étant étendue à tous les diviseurs $\mathfrak{p}$ premiers rationnels par rapport à k sur Γ dont le degré divise n. Mais, puisque k est parfait, il résulte de F-VII$_6$, pr. 15, que tout diviseur $\mathfrak{p}$ sur Γ, premier rationnel par rapport à k, est de la forme $\mathfrak{p} = \sum_i P_i$, où les P_i sont des points distincts en nombre égal à $d = \deg(\mathfrak{p})$; de plus, si P est l'un quelconque des P_i, on a $d = [k(P) : k]$, donc $k(P) = k_d$, et par suite $k(P) \subset k_n$, si d divise n. Réciproquement, si P est l'un quelconque des ν_n points de Γ tels que $k(P) \subset k_n$, la somme des conjugués du point P par rapport à k est un diviseur premier rationnel par rapport à k, dont le degré est égal à $[k(P) : k]$ et divise n. Comme d'ailleurs tout point P, algébrique sur le corps k, est un composant d'un diviseur premier rationnel par rapport à k et d'un seul, on voit que l'entier désigné par c_n dans les formules ci-dessus n'est pas autre chose que le nombre ν_n des points P de Γ tels que $k(P) \subset k_n$. Ceci démontre la relation :

$$d[\log\ Z(u)] = \sum_{n=1}^{\infty} \nu_n u^n.du/u.$$

21. Nous allons maintenant obtenir une expression de l'entier ν_n au moyen de la théorie des correspondances.

Nous désignerons par ω l'automorphisme $(\xi \to \xi^q)$ du domaine universel $\mathbf{K}$; alors, si n est un entier positif, ω_n est l'automorphisme $(\xi \to \xi^{q^n})$, laissant invariants les éléments de k_n et ceux-là seulement ; de plus, ω^n induit, sur un corps quelconque K, un isomorphisme de K sur un sous-corps de K (éventuellement sur K lui-même),

qu'on désignera aussi par ω^n. Nous ne préciserons la relation entre un corps K et son transformé par ω^n que dans le cas particulier suivant, qui nous servira dans la démonstration du th. 13 :

LEMME 2. — Soit $K = k(t)$ une extension séparablement engendrée du corps de base k, de dimension 1 sur k : alors K est une extension algébrique purement inséparable de son transformé K' par ω^n, et l'on a $[K : K'] = q^n$.

Soit u un élément de K, tel que K soit séparable sur $k(u)$; posons $(t) = (t_1, \ldots, t_m)$. Comme ω^n transforme k en k, et (t) en $(t_1^{q^n}, \ldots, t_m^{q^n})$, on a $K' = k(t_1^{q^n}, \ldots, t_m^{q^n})$. On a $K = K'(u, t_1, \ldots, t_m)$; les t_i sont séparables sur $k(u)$, donc a fortiori sur $K'(u)$, et ils sont purement inséparables sur K', donc a fortiori sur $K'(u)$; ils sont donc dans $K'(u)$, de sorte qu'on a $K = K'(u)$. Or u est racine de $U^{q^n} - u^{q^n} = 0$; notre proposition sera donc démontrée si nous faisons voir que cette équation est irréductible dans K'. Comme l'isomorphisme ω^n transforme K en K', et u en u^{q^n}, il revient au même de montrer que l'équation $U^{q^n} - u = 0$ est irréductible dans K. En effet, s'il n'en était pas ainsi, u serait puissance $p^{\text{ième}}$ d'un élément v de K ; alors v serait purement inséparable sur $k(u)$, et, d'après la définition de u, devrait en même temps être séparable sur $k(u)$; v serait donc dans $k(u)$. Mais, u étant une quantité variable sur k, les éléments de $k(u)$ peuvent s'écrire d'une manière et d'une seule comme fractions rationnelles en u à coefficients dans k, et u ne peut être puissance $p^{\text{ième}}$ d'un tel élément.

Soit P un point de Γ ; comme d'habitude (cf. F-VII$_2$), on désignera par P^{ω^n} son transformé par ω^n. Si Γ_α est un représentant de la courbe (abstraite) Γ, sur lequel P ait un représentant

$$P_\alpha = (x_1, \ldots, x_m),$$

le point $Q = P^{\omega^n}$ a sur Γ_α un représentant, à savoir le point

$$Q_\alpha = (x_1^{q^n}, \ldots, x_m^{q^n}) ;$$

l'on a alors

$$k(P) = k(P_\alpha) = k(x_1, \ldots, x_m) \quad \text{et} \quad k(P^{\omega^n}) = k(Q_\alpha) = k(x_1^{q^n}, \ldots, x_m^{q^n}),$$

Si de plus M est un point générique de Γ par rapport à k, il en est de même de M^{ω^n} ; et la considération des représentants de M, M^{ω^n}, P et P^{ω^n} sur Γ_α montre que P^{ω^n} est l'unique spécialisation de M^{ω^n} sur $M \to P$ relativement à k.

Cela posé, soit M un point générique de Γ par rapport à k ; on a $k(M^\omega) \subset k(M)$, donc $k(M \times M^\omega) = k(M)$. Le point $M \times M^\omega$ a donc un lieu par rapport à k sur $\Gamma \times \Gamma$: ce lieu est une courbe qui sera désignée par I. La correspondance réduite

à la courbe I est donc rationnelle par rapport à k ; cette correspondance joue un rôle essentiel dans la théorie de la fonction zêta ; sa classe sera désignée par ι. On désiguera par I_n, pour $n > 0$, la correspondance définie par récurrence au moyen des relations $I_1 = I, I_n = I_{n-1} \circ I$; c'est là une correspondance de classe ι^n.

En vue de la démonstration du th. 13, introduisons une définition. Soit $\sum$ une surface, c'est-à-dire une variété (abstraite) de dimension 2 : nous dirons que deux courbes C et D sur $\sum$ sont *tangentes* l'une à l'autre en un point P, simple sur C et sur D si C et D ne sont pas transversales l'une à l'autre en P sur $\sum$. Soient P un point quelconque sur $\sum$ et $\sum_\alpha$, un représentant de $\sum$ sur lequel P ait un représentant P_α : alors, d'après F-VII$_1$, th. 4, toute courbe sur $\sum$ passant par P, a un représentant sur $\sum_\alpha$; comme deux courbes sur $\sum$, passant par P, sont transversales l'une à l'autre en P si les variétés linéaires tangentes en P_α à leurs représentants sur $\sum_\alpha$ ont une intersection réduite à P_α, c'est-à-dire si ces variétés linéaires sont distinctes, il s'ensuit que ces courbes sont tangentes l'une à l'autre en P si leurs représentants sur $\sum_\alpha$ ont même variété linéaire tangente en P_α. Donc deux courbes sur $\sum$, tangentes en un point P à une même courbe, sont tangentes l'une à l'autre en P ; et, si deux courbes sur $\sum$ sont tangentes l'une à l'autre en P, toute courbe transversale à l'une en P l'est aussi à l'autre.

Après ces préliminaires, nous pouvons passer à la démonstration des principales propriétés élémentaires de la correspondance I, propriétés qui sont contenues dans le théorème suivant :

Théorème 13. — La correspondance I_n se réduit à une courbe, lieu du point $M \times M^{\omega^n}$ par rapport à k sur $\Gamma \times \Gamma$ si M est un point générique quelconque de Γ par rapport à k ; et, si P est un point quelconque de Γ, on a $I_n(P) = P^{\omega^n}$. On a $d(I_n) = 1, d'(I_n) = q^n$, et $\deg(I_n, \Delta) = \nu_n$. De plus, on a $I_n.\Delta = \sum_{\rho=1}^{\nu_n} (P_\rho \times P_\rho)$ si les P_ρ sont tous les points distincts de Γ tels que $k(P_\rho) \subset k_n$.

Soit M un point générique de Γ par rapport à k ; on a

$$k(M \times M^{\omega^n}) = k(M) ;$$

par suite, le point $M \times M^{\omega^n}$ a un lieu J_n par rapport à k sur $\Gamma \times \Gamma$, et l'on a $d(J_n) = 1$; de plus, comme $k(M^{\omega^n})$ est le corps transformé de $k(M)$ par ω^n, on a, d'après le lemme 2, $[\mathrm{k(M)} : \mathrm{k(M^{\omega^n})}] = q^n$, donc, par définition de $d'(J_n)$, $d'(J_n) = q^n$. Le point $M \times M^{\omega^n}$ est un composant du cycle $J_n.(M \times \Gamma) = M \times J_n(M)$, donc M^{ω^n} est un composant de $J_n(M)$; comme $J_n(M)$ est un cycle positif, de degré 1 d'après le th. 3 du n° 2, on a donc $J_n(M) = M^{\omega^n}$. On a observé plus haut que, si P est un point quelconque de Γ, P^{ω^n} est l'unique spécialisation de M^{ω^n} sur $M \to P$ par rapport à

k ; de là, et de F-VII$_8$, th. 13, il résulte qu'on a $J_n(P) = P^{\omega^n}$ quel que soit P sur Γ. Comme on a $J_1 = I$, il suit de là, en particulier, qu'on a $I(P) = P^{\omega}$ quel que soit P, et par suite, par définition de I_n et du produit de composition,

$$I_n(P) = P^{\omega^n} = J_n(P).$$

D'après le th. 2, ceci implique qu'on a $I_n = J_n + \mathfrak{a} \times \Gamma$; comme d'ailleurs J_n est une courbe, et qu'on a $I_n \succ 0$, on a $\mathfrak{a} \succ 0$. Mais on a $d'(I) = d'(J_1) = q$, donc $d'(I_n) = q^n$, c'est-à-dire

$$0 = d'(I_n - J_n) = \deg(\mathfrak{a}),$$

et par suite $\mathfrak{a} = 0$, donc $I_n = J_n$. Considérons maintenant l'intersection $I_n \cap \Delta$; tout point de Δ est de la forme $P \times P$, P étant un point de Γ ; pour qu'un tel point soit sur I_n, il faut et il suffit que ce soit un composant de $I_n.(P \times \Gamma) = P \times I_n(P)$, c'est-à-dire qu'on ait $P = I_n(P) = P^{\omega^n}$; pour cela, il faut et il suffit, si P_α est l'un des représentants de P, que P_α soit son propre transformé par ω^n, c'est-à dire que P_α ait toutes ses coordonnées dans le corps k_n, dont les éléments sont les quantités invariantes par ω^n. Il suit de là que les points de $I_n \cap \Delta$, c'est-à-dire les composants distincts de $I_n.\Delta$, sont bien les points $P_\rho \times P_\rho$, en nombre ν_n, qui sont définis dans l'énoncé de notre théorème. Pour achever notre démonstration, il ne reste plus donc qu'à faire voir que chacun de ces points est une intersection de multiplicité 1 de I_n et de Δ, ou autrement dit (d'après F-VI$_2$, th. 6) que I_n et Δ sont transversales l'une à l'autre en chacun de leurs points d'intersection. Pour cela, posons $N = M^{\omega^n}$ et soit $P \times Q$ un point quelconque de I_n ; d'après F-VII$_6$, pr. 16, $P \times Q$ est intersection propre de I_n et de $\Gamma \times Q$; il suit alors de F-VI$_3$, th. 12, et du lemme 2, d'abord que $M \times N$ est une intersection de I_n et de $\Gamma \times N$ de multiplicité $[\mathrm{k(M}\times N) : k(N]_i = q^n$, et ensuite que $P \times Q$ est une intersection de I_n et de $\Gamma \times Q$ ayant cette même multiplicité. De plus, on a $I_n.(P \times \Gamma) = P \times Q$. Il s'ensuit donc, d'après F-VI$_2$, th. 6, que $P \times Q$ est simple sur I_n, et que I_n est tangente à $\Gamma \times Q$ en ce point. En particulier, si $P \times P$ est un composant de $I_n.\Delta$, I_n y est tangente à $\Gamma \times P$; comme d'autre part on a $\Delta.(\Gamma \times P) = P \times P$, il suit de F-VI$_2$, th. 6, que Δ est transversale en $P \times P$ à $\Gamma \times P$, donc aussi à I_n, ce qui achève la démonstration.

Corollaire 1. — Quel que soit $n > 0$, on a $I_n \circ I'_n = q^n.\Delta$.

C'est là une conséquence immédiate du th. 13, et de la prop. 4 du n° 9.

Corollaire 2. — ι étant la classe de I, on a $\iota\iota' = \iota'\iota = q.\delta$, et $\sigma(\iota^n) = 1 + q^n - \nu_n$ pour $n > 0$.

La dernière formule suit immédiatement des définitions et du th. 13, et la formule $\iota\iota' = q.\delta$ suit du cor. 1. Posons maintenant $\xi = \iota'\iota - q.\delta$; comme on a $\sigma(\iota'\iota) =$

$\sigma(\iota\iota') = \sigma(q.\delta)$, on a $\sigma(\xi) = 0$. On a d'autre part $(\iota'\iota)(\iota'\iota) = \iota'(\iota\iota')\iota = q.\iota'\iota$, d'où

$$\xi\xi' = (\iota'\iota - q.\delta).(\iota'\iota - q.\delta) = q.(q.\delta - \iota'\iota).$$

et par suite $\sigma(\xi\xi') = -q.\sigma(\xi) = 0$, donc $\xi = 0$ d'après le th. 10 du n° 14.

Corollaire 3. — Quel que soit $n > 0$, on a

$$|\sigma(\iota^n)| = |1 + q^n - \nu_n| \leqslant 2g.q^{n/2}.$$

En effet, soient x, y deux entiers ; en appliquant l'inégalité $\sigma(\xi\xi') \geqslant 0$ à $\xi = x.\delta + y.\iota^n$, on obtient, d'après le cor. 2,

$$2g.x^2 + 2\sigma(\iota^n).xy + 2gq^n.y^2 \geqslant 0 ;$$

comme cette inégalité est satisfaite quels que soient x et y entiers, le premier membre est une forme définie ou semi-définie positive, d'où le résultat annoncé.

22. L'hypothèse de Riemann pour la fonction zêta est une conséquence immédiate du cor. 3 du th. 13. Posons en effet

$$P(u) = (1 - u)(1 - qu).Z(u) ;$$

on a alors, d'après le cor. 2 du th. 13 et l'expression trouvée pour $d[\log Z(u)]$ à la fin du n° 20 :

$$d[\log P(u)] = -\sum_{n=1}^{\infty} \sigma(\iota^n).u^n.du/u.$$

Du cor. 3 du th. 13, il résulte que la série du second membre est convergente pour $|n| < q^{-1/2}$, donc que $P(u)$ ne peut avoir ni pôle ni zéro dans ce cercle ; par conséquent, dans ce cercle, $Z(u)$ n'a pas de zéro, et n'a pas d'autre pôle que $u = 1/q$. De l'équation fonctionnelle de $Z(u)$ résulte alors que $Z(u)$ n'a, à l'extérieur de ce même cercle, aucun zéro, et aucun autre pôle que $u = 1$. Donc tous les séros de $Z(u)$ sont sur le cercle $|u| = q^{-1/2}$; c'est l'hypothèse de Riemann.

Comme d'ailleurs on a trouvé que $Z(u)$ est la somme d'un polynôme et de la fonction rationnelle $h.R(u)/(q-1)$, où $R(u)$ est la fonction dont l'expression a été donnée au n° 19, on voit que $R(u)$ comme $Z(u)$, ne peut avoir d'autre pôle que $u = 1$ et $u = 1/q$; l'expression donnée au n° 19 montre qu'il ne peut en être ainsi que si l'on a $\delta = 1$. Il existe donc sur Γ, quel que soit l'entier n, des diviseurs de degré n, rationnels par rapport à k.

Ce qui précède montre que $P(u)$ est un polynôme ; son degré est $2g$, comme on le voit par exemple au moyen de l'équation fonctionnelle de $P(u)$, conséquence immédiate de celle de $Z(u)$;

$$P(u) = q^g.u^{2g}.P(1/qu).$$

Comme on a $Z(0) = 1$, donc $P(0) = 1$, on peut alors écrire :

$$P(u) = \prod_{i=1}^{2g}(1 - \alpha_i u),$$

où les α_i sont tels que $\alpha_i\overline{\alpha}_i = q$ $(1 \leqslant i \leqslant 2g)$. Il résulte d'ailleurs de la définition de $P(u)$ que c'est un polynôme à coefficients entiers rationnels ; comme on a $P(0) = 1$, tous les α_i sont entiers algébriques.

De plus, la formule écrite ci-dessus pour $P(u)$ donne :

$$d[\log P(u)] = -\sum_{i=1}^{2g}\sum_{n=1}^{\infty}\alpha_i^n.u^n.du/u,$$

d'où, par comparaison avec l'expression donnée plus haut :

$$\sigma(\iota^n) = \sum_{i=1}^{2g}\alpha_i^n.$$

Cette formule, obtenue pour $n > 0$, reste valable pour $n = 0$ si l'on pose $\iota^0 = \delta$; et elle reste valable pour $n < 0$ si l'on pose

$$\iota^{-n} = q^{-n}.\iota'^n$$

pour $n > 0$ (les ι^{-n} étant ainsi définis comme éléments de l'anneau $\mathcal{A}_0$ du n° 16), notation justifiée par le fait que, d'après le cor. 2 du th. 13, l'élément $q^{-1}.\iota'$ de l'anneau $\mathcal{A}_0$ est, dans cet unneau, inverse de ι à droite et à gauche. En effet, on a

$$\sigma(q^{-n}.\iota'^n) = q^{-n}.\sigma(\iota^n) = \sum_i(\alpha_i/q)^n\ ;$$

et en vertu de l'équation fonctionnelle de $P(u)$, les $2g$ nombres α_i/q sont les mêmes, à une permutation près, que les nombres $1/\alpha_i$.

Si alors on prend pour $Q(u)$ toutes les sommes finies de la forme $Q(u) = \sum_\rho a_\rho.u^\rho$, où les exposants ρ sont des entiers positifs, négatifs ou nuls, et où les coefficients a_ρ sont des nombres rationnels, les éléments $Q(\iota)$ de l'anneau $\mathcal{A}_0$ forment un sous-anneau $\mathcal{A}_\iota$

engendré par ι, ι' et les multiples rationnels de δ ; et la trace σ est donnée sur ce sous-anneau par la formule

$$\sigma[Q(\iota)] = \sum_{i=1}^{2g} Q(\alpha_i).$$

Soit en particulier $Q_0(u)$ un polynôme, à coefficients entiers rationnels, tel que l'on ait $Q_0(\alpha_i) = 0$ pour $1 \leqslant i \leqslant 2g$; on peut par exemple prendre pour $Q_0(u)$ le polynôme de plus bas degré qui ait cette propriété, ou bien encore le polynôme $u^{2g}.P(1/u)$. Si l'on pose $\xi = Q_0(\iota)$, on aura $\xi' = Q_0(\iota') = Q_0(q.\iota^{-1})$, donc

$$\sigma(\xi\xi') = \sum_i Q_0(\alpha_i).Q_0(q/\alpha_i) = 0,$$

et par suite $\xi = Q_0(\iota) = 0$. L'anneau $\mathcal{A}_\iota$ est donc une algèbre, de rang au plus égal au degré de $Q_0(u)$, sur le corps des rationnels ; c'est de plus une algèbre commutative, semi-simple d'après ce qui a été démontré au n° 16 : c'est donc un produit direct de corps de nombres algébriques.

§ V. Application à la théorie de Galois (fonctions L ; conjecture d'Artin).

23. Nous revenons maintenant au cas général où le corps de base k est un corps quelconque.

Soit X un diviseur premier rationnel par rapport à k sur $\Gamma \times \Gamma$; supposons que X ne soit ni de la forme $\mathfrak{a} \times \Gamma$, ni de la forme $\Gamma \times \mathfrak{a}$, et soit $M \times N$ un point générique par rapport à k de l'une quelconque des composantes de X ; alors M et N sont des points génériques de Γ par rapport à k, et sont donc spécialisations génériques l'un de l'autre par rapport à k, de sorte qu'il y a un isomorphisme α de $k(M)$ sur $k(N)$, laissant invariants les éléments de k, et tel que l'on ait $N = M^\alpha$; de plus, le point N est alors algébrique sur $k(M)$, et M sur $k(N)$, de sorte que les corps $k(M)$ et $k(N)$ ont même fermeture algébrique, et que α peut être prolongé à un automorphisme de celle-ci. Réciproquement, M étant un point générique de Γ par rapport à k, soit α un automorphisme de la fermeture algébrique de $k(M)$, laissant invariants les éléments de k ; alors α transforme M en un point $N = M^\alpha$, algébrique sur $k(M)$; le point $M \times N$ a donc la dimension 1 sur k, et par suite, d'après F-VII$_6$, pr. 15, il y a sur $\Gamma \times \Gamma$ un diviseur X et un seul, premier rationnel par rapport à k, ayant $M \times N$ pour point générique par rapport à k. Si de plus $(N_1, \ldots, N_d)$ est un système complet de conjugués de N sur le corps $k(M)$, on a alors, d'après F-VII$_6$, pr. 15, et F-VII$_6$, th. 12 (i), $X(M) = \sum_{i=1}^{d} N_i$.

Le cas qui intéresse la théorie de Galois est celui où l'on considère, non un automorphisme quelconque de la fermeture algébrique du corps $k(M)$ défini ci-dessus, mais un

automorphisme qui laisse invariants tous les éléments d'un corps K sur lequel $k(M)$ soit algébrique ; comme d'ailleurs un tel automorphisme laisse alors invariants tous les éléments de $k(M)$ qui sont purement inséparables sur le corps K, on peut toujours, après avoir remplacé K par le corps formé de ces derniers éléments, supposer que K est un sous-corps de $k(M)$ sur lequel $k(M)$ est séparablement algébrique (cf. F-1_1). D'autre part, si t est un élément de K, variable sur k, on a $k(t) \subset K \subset k(M)$, et $k(M)$ est une extension algébrique de $k(t)$, de degré fini ; K est donc aussi une extension algébrique de $k(t)$, de degré fini, et est donc une extension de k, de dimension 1, engendrée par des quantités en nombre fini, de sorte qu'on peut écrire $K = k(x)$, (x) étant un système d'éléments de $k(M)$.

Soient donc M un point générique de Γ par rapport à k, et (x) un système d'éléments de $k(M)$, tel que $k(M)$ soit séparablement algébrique sur le corps $K = k(x)$. À tout automorphisme α de la fermeture algébrique $\overline{K}$ de K, laissant les éléments de K invariants, correspond un diviseur X_α sur $\Gamma \times \Gamma$, premier rationnel par rapport à k, à savoir celui qui a le point $M \times M^\alpha$ pour point générique par rapport à k. Comme dans ces conditions M^α est un conjugué de M relativement à K, M^α est séparablement algébrique sur K, et a fortiori sur $k(M)$, de sorte que le cycle $X_\alpha(M)$ est la somme des conjugués distincts de M^α par rapport à $k(M)$; chacun de ces conjugués est d'ailleurs de la forme $M^{\alpha\beta} = (M^\alpha)^\beta$, β étant un automorphisme de K qui laisse invariants les éléments de $k(M)$.

Le cas le plus simple est celui où $k(M)$ est une extension "normale" ou "galoisienne" de K, c'est-à-dire où le corps $k(M)$ est transformé en lui-même par tout automorphisme de $\overline{K}$ laissant les éléments de K invariants. En ce cas, tout automorphisme α de K, laissant invariants les éléments de K, induit sur $k(M)$ un automorphisme de $k(M)$, que nous noterons aussi α : les automorphismes de $k(M)$ ainsi obtenus forment le groupe de Galois de $k(M)$ sur K ; soit G ce groupe. À tout élément α de G correspond alors, par les définitions ci-dessus, une correspondance X^α ; et, comme on a $k(M^\alpha) = k(M)$, donc $k(M \times M^\alpha) = k(M)$, le point $M \times M^\alpha$ a un lieu par rapport au corps k, lieu qui n'est donc autre que X_α ; il s'ensuit qu'on a, dans ces conditions, $d(X_\alpha) = d'(X_\alpha) = 1$, et $X_\alpha(M) = M^\alpha$. Comme de plus α^{-1} transforme M en $M^{\alpha^{-1}}$, et M^α en M, X_α est aussi le lieu de $M^{\alpha^{-1}} \times M$ par rapport à k ; on a donc

$$(X_\alpha)' = X_{\alpha^{-1}} \qquad \text{et} \qquad X'_\alpha(M) = M^{\alpha^{-1}}.$$

De même, si β est un élément quelconque du groupe G, β transforme M en M^β, et M^α en $M^{\alpha\beta}$, de sorte que X_α est aussi le lieu de $M^\beta \times M^{\alpha\beta}$ par rapport à k ; on a donc $X_\alpha(M^\beta) = M^\alpha$. Si donc on pose $Z = X_\alpha \circ X_\beta$, on a $Z(M) = X_{\alpha\beta}(M)$, et par suite, d'après le th. 2 du § 1, n° 2, la correspondance $Z - X_{\alpha\beta}$ est de la forme $\mathfrak{a} \times \Gamma$; comme on a alors $Z' = X_{\beta^{-1}} \circ X_{\alpha^{-1}}$, et $(X_{\alpha\beta})' = X_{\beta^{-1}\alpha^{-1}}$, on voit de même que $Z' - (X_{\alpha\beta})'$ est de la forme $\mathfrak{b} \times \Gamma$, donc $Z - X_{\alpha\beta}$, de la forme $\Gamma \times \mathfrak{b}$; ceci implique qu'on a $Z = X_{\alpha\beta}$. Autrement dit, on a $X_{\alpha\beta} = X_\alpha \circ X_\beta$ quels que soient α et β dans

G. En particulier, si ε désigne l'élément neutre (ou "élément unité") du groupe G, on $X_\varepsilon = \Delta = X_\alpha \circ X_{\alpha^{-1}}$, quel que soit α dans G.

Il suit de là que, si l'on désigne par ξ_α la classe de la correspondance X_α, les éléments ξ_α de l'anneau $\mathcal{A}$ des classes de correspondances forment un groupe multiplicatif isomorphe au groupe G, et que leurs combinaisons linéaires à coefficients entiers forment un sous-anneau de $\mathcal{A}$, isomorphe à l'anneau de groupe formé au moyen du groupe G.

24. Indiquons brièvement comment ce qui précède se généralise au cas où $k(M)$ n'est plus supposé normal sur K ; cette généralisation ne nous servira pas dans ce qui suit. Soit K_1 une extension normale de K, contenant $k(M)$; pour fixer les idées, on pourra prendre pour K_1 le composé de tous les conjugués du corps $k(M)$ sur le corps K. Soit G le groupe de Galois de K_1 sur K et soit g le sous-groupe de G, formé de tous les éléments de G qui laissent invariants les éléments de $k(M)$. Comme plus haut, si α est un élément de G, on notera X_α le diviseur sur $\Gamma \times \Gamma$, premier rationnel par rapport à k, ayant $M \times M^\alpha$ pour point générique par rapport à k ; $X_\alpha(M)$ est alors le diviseur sur Γ, premier rationnel par rapport à $k(M)$, qui a le composant M^α. Il suit de là qu'on a $X_\alpha = X_{\alpha'}$, si M^α et $M^{\alpha'}$ sont conjugués l'un de l'autre par rapport à $k(M)$, et dans ce cas seulement ; il faut et il suffit pour cela qu'il y ait un élément β du groupe g, tel que l'on ait $M^{\alpha'} = M^{\alpha\beta}$, c'est-à-dire $M^{\alpha'\beta^{-1}\alpha^{-1}} = M$, ou, ce qui revient au même, tel que l'on ait $\alpha'\beta^{-1}\alpha^{-1} \in g$, c'est-à-dire $\alpha' \in g\alpha\beta$; en d'autres tormes, pour qu'on ait $X_\alpha = X_{\alpha'}$, il faut et il suffit qu'on ait $' \in g\alpha g$ c'est-à-dire que α' appartienne à la "classe bilatère" $g\alpha g$ déterminée par α dans le groupe G suivant le sous-groupe g. Il y a donc correspondance biunivoque entre les X_α et les "classes bilatères" dans G suivant g.

Pour aller plus loin, convenons, si γ est un élément quelconque de l'annean de groupe de G, c'est-à-dire une combinaison lineaire (formelle) $\sum_\alpha a_\alpha.\alpha$, à coefficients entiers a_α des éléments α de G, de désigner par M^γ le cycle $\sum_\alpha a_\alpha.M^\alpha$. D'autre part, notons par γ_α ,si α est un élément quelconque de G, l'élément de l'anneau de groupe de G défini par $\gamma_\alpha = \sum_{\rho \in g\alpha g} \rho$, la somme du second membre étant étendue à tous les éléments ρ distincts de la "classe bilatère" $g\alpha g$. Il est facile de voir que les combinaisons linéaires, à coefficients entiers, des éléments γ_α de l'anneau de groupe de G forment un sous-anneau de celui-ci.

Soient alors α et β deux éléments de G ; X_α peut être défini comme le diviseur sur $\Gamma \times \Gamma$, premier rationnel par rapport à k, qui a $M^\beta \times M^{\alpha\beta}$ pour point générique par rapport à k ; on voit alors, comme plus haut, que $X_\alpha(M^\beta)$ est le diviseur sur Γ qui a pour composants les conjugués de $M^{\alpha\beta}$ par rapport à $k(M^\beta)$, chacun de ces composants étant pris avec le coefficient 1. Mais on vérifie facilement que le diviseur $M^{\gamma_\alpha.\beta}$ a pour composants ces mêmes points, pris chacun avec un coefficient égal au nombre

d'éléments du groupe g ; si donc n est ce nombre d'éléments, on a $n.X_\alpha(M^\beta) = M^{\gamma_\alpha.\beta}$. Il suit de là, par linearité, que, si γ est un élément quelconque de l'anneau de groupe de G, on a $n.X_\alpha(M^\gamma) = M^{\gamma_\alpha.\gamma}.En particulier, on a donc cn^2.X_\alpha[X_\beta(M)] = M^{\gamma_\alpha.\gamma_\beta}$.

Il résulte de là, par un raisonnement semblable à celui qui a été fait un n° 23, que, si l'on dénote par ξ_α la classe de la correspondance X_α, les combinaisons linéaires, à coefficients entiers, des éléments $n.\xi_\alpha$ de l'anneau $\mathcal{A}$ des classes de correspondances forment un sous anneau de $\mathcal{A}$, isomorphe au sous-anneau de l'anneau de groupe de G formé des combinaisons linéaires des γ_α à coefficients entiers.

25. Le calcul de la trace, dans l'anneau $\mathcal{A}$, des classes de correspondances qu'on vient de définir conduit tout naturellement aux "groupes de Hilbert" et à leur généralisation au cas non galoisien[4], ainsi qu'à la théorie de la différente, du discriminant et du conducteur (ce dernier au sens d'Artin). Nous nous bornerons à des indications sommaires sur le cas galoisien.

Soient, comme au n° 23, M un point générique de Γ par rapport à k, et $K = k(x)$ une extension de k telle que $k(M)$ soit séparablement algébrique et galoisien sur K. Soit G le groupe de Galois de $k(M)$ sur K ; soit ε l'élément neutre de G ; soit α un élément de G, autre que ε ; soient X_α le lieu de $M \times M^\alpha$ par rapport à k sur $\Gamma \times \Gamma$, et ξ_α la classe de X_α. D'après les définitions du §1, on a

$$\sigma(\xi_\alpha) = d(X_\alpha) + d'(X_\alpha) - I(X_\alpha.\Delta) ;$$

on a d'ailleurs $d(X_\alpha) = d'(X_\alpha) = 1$; et, puisque $\alpha \neq \varepsilon$, les courbes X_α et Δ sont distinctes ; on a donc $\sigma(\xi_\alpha) = 2 - \deg(X_\alpha.\Delta)$, de sorte que le calcul de $\sigma(\xi_\alpha)$ se ramène à l'étude du cycle $X_\alpha.\Delta$ sur $\Gamma \times \Gamma$.

Mais, si P est un point quelconque de Γ, le cycle $X_\alpha.(P \times \Gamma)$ est défini, et on a donc $X_\alpha.(P \times \Gamma) = P \times X_\alpha(P), X_\alpha(P)$ étant, d'après le th. 3 du § 1, n° 2, un diviseur positif de degré 1, donc réduit à un point. Donc, pour qu'un point $P \times Q$ de $\Gamma \times \Gamma$ soit sur X_α, il faut et il suffit qu'on ait $Q = X_\alpha(P)$. En particulier, les composants de $X_\alpha.\Delta$ sont les points de la forme $P \times P$, où P est un point de Γ tel que $X_\alpha(P) = P$.

Si P est un point quelconque de Γ, on désignera par $T(P)$ l'ensemble des éléments α de G tels que $X_\alpha(P) = P$; $T(P)$ est un sous-groupe de G, qui s'appelle le *groupe d'inertie* de P dans G. Il résulte de ce qui précède que les seuls points de Γ auxquels

[4]Une généralisation des groupes de Hilbert au cas non galoisien par les "hyper-groupes" a été donnée par M. Krasner (Thèse, Paris 1938) pour les corps de nombres algébriques. Mais c'est plutôt dans la considération des anneaux introduits ci-dessus (et auxquels conduisent également les résultats de L. Kaloujnine, C.R. t. 214 (1942), p. 597) qu'il convient de chercher le principe d'une généralisation adéquate.

appartienne dans G un groupe d'inertie non réduit à l'élément neutre sont les composants du diviseur $\mathfrak{d} = pr_1[(\sum_{\alpha\neq 1} X_\alpha).\Delta]$; $\mathfrak{d}$ s'appelle la *différente* de $k(M)$ sur K.

La définition des groupes de ramification résulte alors de la proposition suivante, où les notations restent les mêmes que jusqu'ici :

PROPOSITION 6. — Soient P un point de Γ, et α, β deux éléments de G, autres que ε et tels que $\alpha\beta \neq \varepsilon$. Soient a, b, c les coefficients de $P \times P$ dans les cycles $X_\alpha.\Delta$, $X_\beta.\Delta$ et $X_{\alpha\beta}.\Delta$, respectivement. Alors on a $c \geqslant \min(a, b)$.

Si $a = 0$ ou $b = 0$, notre assertion est triviale ; supposons donc qu'on a $a > 0$ et $b > 0$, donc que α et β sont dans $T(P)$: il en est alors de même de $\alpha\beta$, et on a $c > 0$. Soit φ une uniformisante pour Γ en P (cf. 1ère partie, § II, n° 10) ; soient K, un corps de définition pour φ, et M un point générique de Γ par rapport à K_1. Posons $N = X_\beta(M)$ et $R = X_\alpha(N) = X_{\alpha\beta}(M)$. Alors $M \times N$ est sur X_β, et a la dimension 1 sur K_1; X_β est donc le lieu de $M \times N$ par rapport à K_1, et, puisqu'on a $d(X_\beta) = 1$, et $d'(X_\beta) = 1$, on a $K_1(M) = K_1(N)$; on voit de même que X_α et $X_{\alpha\beta}$ sont les lieux de $N \times R$ et de $M \times R$, respectivement, par rapport à K_1, et qu'on a $K_1(M) = K_1(R)$. Considérons la fonction φ_0 sur $\Gamma \times \Gamma$, définie à partir de φ comme dans la 1ère partie, § II, n° 10, c'est-à-dire telle que $\varphi_0(Q \times S) = \varphi(S) - \varphi(Q)$ chaque fois que $\varphi(Q)$ et $\varphi(S)$ sont finis ; et posons $Y = (\varphi_0) - \Delta$. D'après la prop. 15 de la 1ère partie, § II, n° 10, on a $d\varphi \neq 0$, c'est-à-dire, par définition, que Δ n'est pas une composante de Y ; et on a $v_P(d\varphi) = 0$, c'est-à-dire que $P \times P$ n'est pas un composant de $Y.\Delta$; comme de plus $P \times P$ n'est contenu dans aucune composante de $(\varphi_0)_\infty$, $P \times P$ n'est donc contenu dans aucune composante de Y. Comme $P \times P$ est contenu dans X_α, dans X_β et dans $X_{\alpha\beta}$, il suit de là qu'aucune de ces trois courbes n'est une composante de (φ_0), donc que φ_0 induit sur chacune d'elles une fonction autre que la constante 0. D'après F-VIII$_2$, th. 7, il y a alors sur Γ trois fonctions θ_1, θ_2, θ_3, respectivement définies par rapport à K_1 par les relations

$$\begin{array}{lll} \theta_1(N) & = \varphi_0(N \times R) & = \varphi(R) - \varphi(N), \\ \theta_2(M) & = \varphi_0(M \times N) & = \varphi(N) - \varphi(M), \\ \theta_3(M) & = \varphi_0(M \times R) & = \varphi(R) - \varphi(M), \end{array}$$

et on a

$$(\theta_1) = pr_1[(\varphi_0).X_\alpha], \qquad (\theta_2) = pr_1[(\varphi_0).X_\beta], \qquad (\theta_3) = pr_1[(\varphi_0).X_{\alpha\beta}]$$

Soit de plus θ_1' la fonction sur Γ, définie par rapport à K_1 par $\theta_1'(M) = \theta_1(N)$, c'est-à-dire par $\theta_1'(M) = \theta_1[X_\beta(M)]$; on a alors, d'après le th. 4 du § 1, n° 3, $(\theta_1') = X_\beta'[(\theta_1)] = X_{\beta^{-1}}[(\theta_1)]$; et on a

$$\theta_3(M) = \theta_1'(M) + \theta_2(M) \qquad \text{donc} \qquad \theta_3 = \theta_1' + \theta_2.$$

On va montrer maintenant qu'on a $v_P(\theta_1) = v_P(\theta'_1) = a, v_P(\theta_2) = b, v_P(\theta_3) = c$, ce qui achèvera la démonstration d'après F-VIII$_2$, th. 6.

En effet, comme $P \times P$ n'est contenu dans aucune composante de (φ_0) autre que Δ, le coefficient de $P \times P$ dans $(\varphi_0).X_\alpha$ est égal à celui de $P \times P$ dans $\Delta.X_\alpha$; de plus, aucun composant de $(\varphi_0).X_\alpha$ autre que $P \times P$, ne peut avoir la projection P sur le premier facteur Γ de $\Gamma \times \Gamma$, puisqu'un tel composant serait de la forme $P \times Q$ et serait dans X_α, de sorte qu'on aurait $Q = X_\alpha(P) = P$. Il s'ensuit que le coefficient $v_P(\theta_1)$ de P dans (θ_1) est bien égal au coefficient a de $P \times P$ dans $\Delta.X_\alpha$; on voit de même qu'on a $v_P(\theta_2) = b, v_P(\theta_3) = c$. Enfin, on a $X_{\beta^{-1}}(P) = P$; et, si Q est un point de Γ autre que P, $X_{\beta^{-1}}(Q)$ est un point de Γ autre que P, car, si on avait $X_{\beta^{-1}}(Q) = P$, $P \times Q$ serait dans X_β et on aurait $Q = X_\beta(P) = P$. Il suit de là que P a même coefficient dans les diviseurs (θ_1) et $(\theta_1) = X_{\beta^{-1}}[(\theta_1)]$; on a donc bien $v_P(\theta'_1) = v_P(\theta_1) = a$.

Soient alors P un point de Γ, et a un entier positif ; soit $V_a(P)$ l'ensemble formé de l'élément neutre ε de G, et de tous les éléments α de G, autres que ε, tels que $P \times P$ ait dans $X_\alpha.\Delta$ un coefficient au moins égal à a ; comme on a $X'_\alpha = X_{\alpha^{-1}}$, $P \times P$ a même coefficient dans $X_\alpha.\Delta$ et dans $X_{\alpha^{-1}}.\Delta$; il suit de là, et de la prop. 6, que $V_a(P)$ est un sous-groupe de G : $V_a(P)$ s'appelle le a-ième *groupe de ramification* de P dans G. On a $V_1(P) = T(P)$, et $V_a(P) \supset V_{a+1}(P)$ quel que soit a.

D'autre part, soit $\mathfrak{p}$ un diviseur premier rationnel par rapport à k sur Γ : alors, quel que soit $\alpha \in G, X_\alpha(\mathfrak{p})$ est aussi un diviseur premier rationnel par rapport à k. En effet, $X_\alpha(\mathfrak{p})$ est un diviseur positif, rationnel par rapport à k, et on a $\mathfrak{p} = X_{\alpha^{-1}}[X_\alpha(\mathfrak{p})]$; si donc l'expression de $X_\alpha(\mathfrak{p})$ comme somme de diviseurs premiers rationnels par rapport à k ne se réduisait pas à un seul diviseur avec le coefficient 1, il en serait de même de $\mathfrak{p}$, contrairement à l'hypothèse. Donc, pour qu'on ait $X_\alpha(\mathfrak{p}) = \mathfrak{p}$, il faut et il suffit que $\mathfrak{p}$ et $X_\alpha(\mathfrak{p})$ aient au moins un composant commun, ou encore, si P est l'un quelconque des composants de $\mathfrak{p}$, que $X_\alpha(P)$ soit un conjugué de P relativement à k. Il suit de là que l'ensemble des éléments α de G tels que $X_\alpha(\mathfrak{p}) = \mathfrak{p}$ forme un sous-groupe $Z(\mathfrak{p})$ de G qui contient $T(P)$ quel que soit le composant P de $\mathfrak{p}$; $Z(\mathfrak{p})$ s'appelle le *groupe de décomposition* de $\mathfrak{p}$ dans G. D'ailleurs, comme tous les composants de $\mathfrak{p}$ sont conjugués les uns des autres par rapport à k, ils ont tous même groupe d'inertie et mêmes groupes de ramification.

26. Il résulte de ce qui précède que, si on désigne par $a_P(\alpha)$, pour $\alpha \neq \varepsilon$ la multiplicité d'intersection de X_α et de Δ en $P \times P$, $a_P(\alpha)$ est le plus grand des entiers a tels que α soit dans $V_a(P)$; si ξ_α est la classe de X_α, on a, avec cette notation, $\sigma(\xi_\alpha) = 2 - \sum_P a_P(\alpha)$ pour $\alpha \neq \varepsilon$, et $\xi_\varepsilon = \delta$, donc $\sigma(\xi_\varepsilon) = 2g$. Comme d'ailleurs on a $\xi_{\alpha\beta} = \xi_\alpha \xi_\beta$, on a, en vertu des propriétés de la trace σ, $\sigma(\xi_{\alpha\beta}) = \sigma(\xi_{\beta\alpha})$; ceci exprime que l'entier $\sigma(\xi_\alpha)$, considéré comme fonction de α sur G, est une "fonction centrale" qui peut s'exprimer comme combinaison linéaire à coefficients complexes des carac-

tères $\chi(\alpha)$ des représentations irréductibles de G. On a donc $\sigma(\xi_\alpha) = \sum_\chi c_\chi.\chi(\alpha)$, les coefficients c_χ pouvant, en vertu des relations d'orthogonalité des caractères, se calculer par les formules $c_\chi = 1/N. \sum_{\alpha\in G} \chi(\alpha^{-1}).\sigma(\xi_\alpha)$, où N désigne le nombre d'éléments de G.

On démontrera dans un mémoire qui fera suite à celui-ci, que $\sigma(\xi)$ est la trace d'une représentation matricielle de l'anneau $\mathcal{A}$ dans un corps de caractéristique 0 ; il résulte de ce qui précède que, s'il en est ainsi, la fonction $\sigma(\xi_\alpha)$ définie ci-dessus sur le groupe G est la trace d'une représentation de G, et est donc une combinaison linéaire à coefficients entiers des caractères simples de G ; autrement dit, s'il en est ainsi, les coefficients c_χ définis plus haut sont des entiers $\geqslant 0$. Ce résultat peut d'ailleurs être retrouvé par une autre voie, du moins si on suppose que k est parfait, et que les théorèmes d'Artin[5] sur les conducteurs s'appliquent aux extensions galoisiennes du corps des séries formelles à une variable à coefficients dans k. En effet, si k est parfait, le raisonnement fait au début du n° 19 montre qu'on peut écrire $K = k(M_0), M_0$ étant un point générique par rapport à k d'une courbe complète Γ_0 sans point multiple définie sur k. Soit alors g_0 le genre de Γ_0 ; et soit $\mathfrak{f}_\chi$ le conducteur du caractère χ de G, qui, d'après les résultats d'Artin (si on les suppose applicables au cas qui nous occupe) est un diviseur sur Γ_0 ; de la définition donnée par Artin pour $\mathfrak{f}_\chi$, jointe aux résultats ci-dessus, on conclut que les c_χ sont donnés par les formules $\mathrm{c}_\chi = (2g_0 - 2).\chi(\varepsilon) + \deg(\mathfrak{f}_\chi) + 2\rho_\chi$, l'entier $\rho\chi$ ayant la valeur 1 si χ est le caractère principal de G, et la valeur 0 en tout autre cas.

27. Nous allons maintenant appliquer les résultats des n^{os} 23 et 25 au cas où le corps de base k a un nombre fini q d'éléments. Les notations seront les mêmes qu'au § IV ; en particulier, nous aurons de nouveau à considérer l'automorphisme ω du corps des constantes, et la correspondance I, définis au n° 21, et la classe ι de I. Soient d'autre part, comme au n° 23, M un point générique de Γ par rapport à k, et K un corps tel que $k(M)$ soit une extension séparablement algébrique et galoisienne de K ; nous désignerons de nouveau par G le groupe de Galois de $k(M)$ sur K, et par X_α et ξ_α, pour $\alpha \in G$, le lieu de $M \times M^\alpha$ par rapport à k, et la classe de X_α, respectivement ; comme l'automorphisme ω laisse invariants les éléments de k, et que les X_α sont définies sur k, ω transforme chacune des courbes X_α en elle-même.

Soit P un point quelconque de Γ ; posons $Q = X_\alpha(P)$; alors $P_\alpha \times Q$ est un point de X_α ; comme ω transforme X_α en elle-même, $P^\omega \times Q^\omega$ est donc aussi un point de X_α, de sorte qu'on a $Q^\omega = X_\alpha(P^\omega)$; comme on a $P^\omega = I(P)$ et $Q^\omega = I(Q)$, ceci peut s'écrire $I[X_\alpha(P)] = X_\alpha[I(P)]$. Il suit de là, d'après le th. 2 du n° 2, que la correspondance $(I \circ X_\alpha) - (X_\alpha \circ I)$ est de la forme $\mathfrak{a} \times I$, donc équivalente à 0

[5] E. Artin, Di gruppentheoretische Struktur der Diskriminante algebraicher Zahlkörper Crelles J., Bd. 154 (1931) p. 1.

; on a donc $\iota\xi_\alpha = \xi_\alpha\iota$. En multipliant cette relation à droite et à gauche par ι', on obtient $q.(\xi_\alpha\iota') = q.(\iota'\xi_\alpha)$, donc, d'après ce qu'on a démontré au n° 16, $\xi_\alpha\iota' = \iota'\xi_\alpha$. Autrement dit, ι et ι' sont permutables avec tous les ξ_α dans l'anneau $\mathcal{A}$ des classes de correspondances.

Considérons alors, dans l'anneau $\mathcal{A}_0$ défini au n° 16, les éléments de la forme $\xi_\alpha\iota^n$, où α est un élément de G, et n un entier positif, négatif ou nul ; la définition des ι^n, pour $n \leqslant 0$, reste bien entendu celle qui a été donnée au n° 22. Il résulte de ce qui précède que les combinaisons linéaires de ces éléments, à coefficients rationnels, forment un anneau $\mathcal{A}_{G,\iota}$, dont le centre contient l'anneau $\mathcal{A}_\iota$ défini au n° 22 ; de plus, $\mathcal{A}_{G,\iota}$ est un sous-anneau symétrique de $\mathcal{A}_0$, c'est à-dire qu'il est transformé en lui-même par la symétrie $\xi \to \xi'$; et, comme il a été démontré au n° 22 que $\mathcal{A}_\iota$ est un module de rang fini sur le corps des rationnels, c'est-à-dire qu'il n'y a parmi les ι^n qu'un nombre fini d'éléments linéairement indépendants sur ce corps, $\mathcal{A}_{G,\iota}$ est aussi un module de rang fini sur ce corps ; c'est donc, d'après ce qu'on a vu au n° 16, une algèbre semi-simple sur le corps des rationnels. On voit de même que les combinaisons linéaires des $\xi_\alpha\iota^n$ à coefficients algébriques forment un sous-anneau symétrique $\mathcal{A}^*_{G,\iota}$ de l'anneau $\mathcal{A}_c$ défini au n° 16, et que c'est là une algèbre semi-simple sur le corps des nombres algébriques (donc une somme directe d'algèbres complètes de matrices sur ce corps).

Comme on a $\xi_\alpha\iota^{-n} = q^{-n}.(\iota^n\xi_{\alpha^{-1}})'$, la trace σ sera connue sur l'anneau $\mathcal{A}_G$, dès qu'on connaltra les entiers $\sigma(\xi_\alpha\iota^n)$ pour $\alpha \in G, n \geqslant 0$.

On a d'ailleurs $d(X_\alpha \circ I_n) = 1, d'(X_\alpha \circ I_n) = q^n$; si donc on pose, pour $\alpha \in G, n > 0, \nu_n(\alpha) = \deg(I_n.X_\alpha)$, on aura, d'après la prop. 2 du n° 5, $\sigma(\xi_\alpha\iota^n) = 1+q^n-\nu_n(\alpha^{-1})$.

Soit alors χ un caractère simple du groupe G ; soit N le nombre d'éléments de G ; nous définirons une fonction $L_\chi(u)$ comme la fonction analytique de u, prenant la valeur 1 pour $u = 0$, et satisfaisant au voisinage de $u = 0$ à la relation

$$d[\log L_\chi(u)] = 1/N.\sum_{n=1}^{\infty}\left[\sum_{\alpha\in G}\chi(\alpha).\nu_n(\alpha)\right].u^n.du/u.$$

On voit que, si $k(M) = K$, et si par suite G se réduit à son élément neutre, il n'y a qu'un seul caractère simple χ, à savoir le caractère principal de G, et la fonction $L_\chi(u)$ correspondante n'est autre que la fonction zêta attachée à Γ et au corps k. Il résulte d'autre part de ce qui précède que, si on pose en général

$$\Phi_\chi(u) = 1/N.\sum_{n=1}^{\infty}\left[\sum_{\alpha\in G}\chi(\alpha^{-1}).\sigma(\xi_\alpha\iota^n)\right].u^n,$$

on aura

$$L_\chi(u) = \frac{e^{-\int_0^u \Phi_\chi(u).du/u}}{(1-u)^{\rho_\chi}.(1-qu)^{\rho_\chi}}$$

si ρ_χ est de nouveau l'entier qui a la valeur 1 lorsque χ est le caractère principal de G, et la valeur 0 en tout autre cas. D'autre part, si on pose $r_\chi = \chi(\varepsilon)$, et qu'on désigne par ε_χ l'élément de l'anneau $\mathcal{A}^*_{G,\iota}$ défini par $\varepsilon_\chi = r_\chi/N. \sum_{\alpha\in G} \chi(\alpha^{-1}).\xi_\alpha$, la formule qui définit $\Phi_\chi(u)$ peut s'écrire

$$\Phi_\chi(u) = 1/r_\chi. \sum_{n=1}^{\infty} \sigma(\varepsilon_\chi \iota^n).u^n.$$

Pour justifier les définitions ci-dessus, il faut montrer que les séries de puissances qui y figurent ont un rayon de convergence non nul. Pour cela, observons d'abord que, d'après ce qui précède, ε_χ est permutable avec ι^n quel que soit n ; comme d'autre part on a $(\xi_\alpha)' = \xi_{\alpha^{-1}}$, et $\xi_{\alpha\beta} = \xi_\alpha \xi_\beta$, quels que soient α et β dans G, il résulte de la théorie des représentations des groupes finis qu'on a $(\varepsilon_\chi)' = \varepsilon_\chi$ et $\varepsilon_\chi^2 = \varepsilon_\chi$; on a donc, quels que soient les entiers m et n

$$(\varepsilon_\chi \iota^n)' = q^n.\varepsilon_\chi \iota^{-n} \quad \text{et} \quad (\varepsilon_\chi \iota^m).(\varepsilon_\chi \iota^n) = \varepsilon_\chi \iota^{m-n}.$$

Il s'ensuit que les combinaisons linéaires à coefficients algébriques des éléments $\varepsilon_\chi \iota^n$ de l'anneau $\mathcal{A}^*_{G,\iota}$ forment un sous-anneau commutatif symétrique $\mathcal{A}^*_{\chi,\iota}$ et de $\mathcal{A}^*_{G,\iota}$; de plus, comme il n'y a, parmi les ι^n, qu'un nombre fini d'éléments linéairement indépendants sur le corps des rationnels, $\mathcal{A}^*_{\chi,\iota}$ est un module de rang fini sur le corps des nombres algébriques ; c'est donc une algèbre commutative semi-simple sur ce corps, c'est-à-dire une somme directe de corps isomorphes à celui-ci. Autrement dit, il existe une base $\varepsilon_1, \ldots, \varepsilon_r$ de $\mathcal{A}^*_{\chi,\iota}$ sur le corps des nombres algébriques, telle que, si deux éléments de $\mathcal{A}^*_{\chi,\iota}$ sont exprimés comme combinaisons linéaires $\sum_i u_i\varepsilon_i, \sum_i v_i\varepsilon_i$ des ε_i, à coefficients algébriques u_i, v_i, on ait

$$\left(\sum_i u_i\varepsilon_i\right).\left(\sum_i v_i\varepsilon_i\right) = \sum_i u_i v_i.\varepsilon_i \ ;$$

on a donc $\varepsilon_i^2 = \varepsilon_i$, et $\varepsilon_i\varepsilon_j = 0$ pour $i \neq j$. Comme de plus les ε_i sont déterminés par ces conditions d'une manière unique, à une permutation près, et que la symétrie $\xi \to \xi'$ induit sur $\mathcal{A}^*_{\chi,\iota}$ un automorphisme, les ε'_i sont les mêmes, à l'ordre près, que les ε_i. Comme d'ailleurs on a $\sigma(\varepsilon_i\varepsilon'_i) > 0$ donc $\varepsilon_i\varepsilon'_i \neq 0$, il suit de là qu'on a $\varepsilon'_i = \varepsilon_i$ donc aussi $\varepsilon_i\varepsilon'_i = \varepsilon_i$ quel que soit i ; si donc on pose $a_i = \sigma(\varepsilon_i)$, on $a_i > 0$ pour $1 \leqslant i \leqslant r$.

Mais ε_χ est l'élément unité de $\mathcal{A}^*_{\chi,\iota}$; on a donc $\varepsilon_\chi = \sum_i \varepsilon_i$. Posons $\varepsilon_\chi \iota = \sum_i \lambda_i\varepsilon_i$, les λ_i étant des nombres algébriques. On a alors $\varepsilon_\chi \iota' = \sum_i \overline{\lambda_i}\varepsilon_i$, d'où $(\varepsilon_\chi\iota).(\varepsilon_\iota\iota') = \sum_i \lambda_i\overline{\lambda_i}\varepsilon_i$; comme le premier membre de cette dernière relation est égal à $q.\varepsilon_\chi$, on a donc $\lambda_i\overline{\lambda_i} = q$ pour $1 \leqslant i \leqslant r$. On a d'autre part $\varepsilon_\chi \iota^n = \sum_i \lambda_i^n\varepsilon_i$, pour $n > 0$, et par suite

$\sigma(\varepsilon_\chi \iota^n) = \sum_i a_i \lambda_i^n$. La série qui définit la fonction $\Phi_\chi(u)$ est donc convergente pour $|u| < q^{-1/2}$, et on

$$\Phi_\chi(u) = 1/r_\chi . \sum_i a_i . \lambda_i u/(1 - \lambda_i u),$$

et par suite :

$$L_\chi(u) = [(1-u)(1-qu)]^{-\rho_\chi} . \prod_i (1 - \lambda_i u)^{a_i/r_\chi}.$$

Le fait que les exposants a_i/r_χ, dans cette formule, sont tous positifs, constitue l'analogue d'une conjecture d'Artin, bien connue, au sujet des fonctions L dans les corps de nombres algébriques. La relation $\lambda_i \overline{\lambda_i} = q$ est l'hypothèse de Riemann pour les fonctions $L_\chi(u)$; elle entraîne l'équation fonctionnelle de $L_\chi(u)$, qui est de la forme :

$$L_\chi(1/qu) = w_\chi . u^{-c\chi} . L_{\overline{\chi}}(u),$$

où w_χ est une constante, et où c_χ est donné par

$$c_\chi = \sum_i a_i/r_\chi = \sigma(\varepsilon_\chi)/r_\chi,$$

c'est-à-dire $c_\chi = 1/N . \sum_{\alpha \in G} \chi(\alpha^{-1}) . \sigma(\xi_\alpha)$, et n'est donc autre que le nombre c_χ défini au n° 26.

28. Il résulte de la théorie des représentations des groupes finis que l'élément ε_χ de $\mathcal{A}^*_{G,\iota}$ est permutable avec tous les ξ_α, donc aussi avec tous les éléments $\xi_\alpha \iota^n$; comme il en est de même de ι, $\mathcal{A}^*_{\chi,\iota}$ est donc contenu dans le centre de l'anneau $\mathcal{A}^*_{G,\iota}$; par suite, chacun des ε_i est permutable avec les ξ_α. On va déduire de là que, si $M(\xi)$, pour $\xi \in \mathcal{A}^*_{G,\iota}$, est une représentation de l'algèbre $\mathcal{A}^*_{G,\iota}$ par des matrices $M(\xi)$ à coefficients algébriques, les traces $\mathrm{Tr}(M_i)$ des matrices $M_i = M(\varepsilon_i)$ sont multiples de r_χ. En effet, puisque $M_1^2 = M_1$, on peut, par un changement de base dans l'espace vectoriel où opèrent les matrices $M(\chi)$, mettre M_1 sous la forme $\begin{Vmatrix} 1_m & 0 \\ 0 & 0 \end{Vmatrix}$ où m est un entier et 1_m la matrice unité de degré m ; on a alors $\mathrm{Tr}(M_i) = m$. Comme les matrices $M(\xi_\alpha)$ sont permutables avec M_1, elles sont alors de la forme $\begin{Vmatrix} A_\alpha & 0 \\ 0 & B_\alpha \end{Vmatrix}$, où les A_α et les B_α constituent deux représentations de G. De même, comme on a $M(\varepsilon_\chi).M_1 = M_1.M(\varepsilon_\chi) = M_1$, $M(\varepsilon_\chi)$ est de la forme $\begin{Vmatrix} 1_m & 0 \\ 0 & 0 \end{Vmatrix}$. On a donc alors $1_m = r_\chi/N . \sum_\alpha \chi(\alpha^{-1}) . A_\alpha$, d'où, en prenant les traces des deux membres,

$$m = r_\chi . \left[1/N . \sum_\alpha \chi(\alpha^{-1}) . \mathrm{Tr}(A^1_\alpha) \right] ;$$

comme le second facteur du second membre est entier en vertu des relations d'orthogonalité entre les caractères, ceci démontre notre assertion.

En particulier, quand nous aurons démontré (dans un mémoire qui fera suite à celui-ci) que σ est, sur l'anneau $\mathcal{A}$ et par suite aussi sur $\mathcal{A}^*_{G,\iota}$, la trace d'une représentation matricielle de ces anneaux, il s'ensuivra que les exposants $a_i/r_\chi = \sigma(\varepsilon_i)/r_\chi$, qui figurent dans l'expression de $L_\chi(u)$ donnée plus haut, sont entiers, et que par conséquent les fonctions $(1-u)^{\rho_\chi}(1-qu)^{\rho_\chi}.L_\chi(u)$ sont des polynômes en u, de degrés respectifs c_χ. Ceci complétera la démonstration des conjectures d'Artin.

29. Donnons, pour terminer, quelques indications sur le calcul de $\nu_n(\alpha) = \deg(I_n.X_\alpha)$. Soit $P \times Q$ un composant du cycle $I_\alpha.X_\alpha$; d'après ce qu'on a vu au cours de la démonstration du th. 13, n° 21, la courbe I_n est tangente à $\Gamma \times Q$ en $P \times Q$. Mais on a

$$X_\alpha.(\Gamma \times Q) = P \times Q\ ;$$

par suite, d'après F-VI$_2$, th. 6, X_α est transversale en $P \times Q$ à $\Gamma \times Q$, donc aussi à I_n ; $P \times Q$ est donc un point d'intersection de I_n et de X_α de multiplicité 1. De plus, pour qu'un point $P \times Q$ de $\Gamma \times \Gamma$ soit dans $I_n \cap X_\alpha$, il faut et il suffit qu'on ait $Q = P^{\omega^n} = X_\alpha(P)$. Il suit de là que $\nu_n(\alpha)$ est égal au nombre des points P de Γ qui satisfont à la condition $X_\alpha(P) = P^{\omega^n}$; comme ces points sont les projections, sur le premier facteur Γ de $\Gamma \times \Gamma$, des composants de $I_n.X_\alpha$, ils sont tous algébriques sur k, et tout conjugué de l'un d'eux par rapport à k satisfait à la même condition. De plus, si P est un tel point, P^{ω^n} est l'un des conjugués de P sur k ; si donc $\mathfrak{p}$ est le diviseur premier rationnel par rapport à k qui a P pour composant, on a alors, d'après les résultats du n° 26, $X_\alpha(\mathfrak{p}) = \mathfrak{p}$, donc $\alpha \in Z(\mathfrak{p})$.

Réciproquement, soit $\mathfrak{p}$ un diviseur premier rationnel par rapport à k sur Γ ; soient d le degré de $\mathfrak{p}$, et P un composant de $\mathfrak{p}$; on a alors $[k(P) : k] = d$, donc $k(P) = k_d$; et, si m est un entier quelconque, ω^m est un automorphisme de $k(P)$, laissant invariants les éléments de k, qui se réduit à l'automorphisme identique si $m \equiv 0 \pmod{d}$ et dans ce cas seulement. Il s'ensuit, comme on sait, que les d conjugués de P sur k sont les points $P^{\omega^n} = I_m(P)$ pour $1 \leqslant m \leqslant d$. Soit de plus ζ un élément du groupe $Z(\mathfrak{p})$; alors $X_\zeta(P)$ est un composant de $\mathfrak{p}$, et il y a donc un entier $m = m(\zeta)$, bien déterminé modulo d, tel que $X_\zeta(P) = P^{\omega^n}$, c'est-à-dire tel que $P \times P^{\omega^n}$ soit sur X_ζ ; comme ω^μ transforme la courbe X_ζ en elle-même quel que soit μ, il s'ensuit que, si $P' = P^{\omega^\mu}$ est l'un quelconque des composants de $\mathfrak{p}$, le point $P' \times P'^{\omega^m} = P^{\omega^\mu} \times P^{\omega^{m-\mu}}$ est aussi sur X_ζ, c'est-à-dire qu'on a $X_\zeta(P') = P'^{\omega^m}$. On dira, dans ces conditions, que $m = m(\zeta)$ est l'exposant auquel appartient ζ dans $Z(\mathfrak{p})$. On a alors

$$m(\zeta_1\zeta_2) = m(\zeta_1) + m(\zeta_2) \pmod{d}$$

quels que soient ζ_1 et ζ_2 dans $Z(\mathfrak{p})$; et on a $m(\zeta) \equiv 0 \pmod{d}$ si ζ est dans le groupe d'inertie $T(P)$ et alors seulement. Il suit de là que $T(P)$ est un sous-groupe invari-

ant de $Z(\mathfrak{p})$, et que le groupe quotient $Z(\mathfrak{p})/T(P)$ est cyclique ; de plus, l'ensemble des valeurs prises par $m(\zeta)$ pour $\zeta \in Z(\mathfrak{p})$ est l'ensemble des multiples d'un certain diviseur d_0 de d ; et, si ζ_0 est un élément de $Z(\mathfrak{p})$ tel que $m(\zeta_0) \equiv d_0 \pmod{d}$, les éléments de $Z(\mathfrak{p})$ qui ont la même propriété sont les éléments de $\zeta_0.T(P)$; c'est là une classe suivant $T(P)$ dans $Z(\mathfrak{p})$, qui s'appelle l'élément de Frobenius du groupe $Z(\mathfrak{p})/T(P)$. Enfin, pour que le point $P \times X_\alpha(P)$ soit un composant de $I_n.X_\alpha$, il faut et il suffit, d'après ce qui précède, que n soit multiple de d_0, et qu'on ait $\alpha \in \zeta_0^{n/d_0}.T(P)$.

Mais, comme on a vu à la fin du n° 26, on peut écrire $K = k(M_0)$, M_0 étant un point générique par rapport à k d'une courbe complète Γ_0 sans point multiple, définie sur k. Alors le point $M \times M_0$ a un lieu C par rapport à k sur $\Gamma \times \Gamma_0$; et il résulte de F. VI_2, th. 12, qu'on a $C.(M \times \Gamma_0) = M \times M_0$ et

$$C.(\Gamma \times M_0) = \left(\sum_{\alpha \in G} M^\alpha\right) \times M_0 = \left[\sum_{\alpha \in G} X_\alpha(M)\right] \times M_0,$$

et par suite, quel que soit le point $P \times P_0$ sur C,

$$C.(P \times \Gamma_0) = P \times P_0 \qquad \text{et} \qquad C.(\Gamma \times P_0) = \left[\sum_{\alpha \in G} X_\alpha(P)\right] \times P_0 \ ;$$

par suite, $P \times P_0$ est alors une intersection de C et de $\Gamma \times P_0$, de multiplicité égale au nombre d'éléments du groupe $T(P)$. Supposons de plus, comme plus haut, que P soit algébrique sur k, et soient $\mathfrak{p}$ et $\mathfrak{p}_0$ les diviseurs premiers rationnels par rapport à k, sur Γ et sur Γ_0 respectivement, tels que P soit un composant de $\mathfrak{p}$ et P_0 un composant de $\mathfrak{p}_0$. Si μ est un entier quelconque, ω^μ transforme la courbe C en elle-même, et $P^{\omega^\alpha} \times P_0^{\omega^\mu}$ est donc un point de C ; il suit de là, et des relations obtenues plus haut, que P^{ω^α} est l'un des points $X_\alpha(P)$ si on a $P_0^{\omega^\mu} = P_0$, et dans ce cas seulement, c'est-à-dire si μ est un multiple de l'entier $d_0' = [k(P_0) : k] = \deg(\mathfrak{p}_0)$, et dans ce cas seulement. De là résulte que d_0' n'est autre que l'entier d_0 qui a été défini plus haut.

On déduit facilement de là, par un raisonnement analogue à celui du n° 20, que nos fonctions $L_\chi(u)$ sont les mêmes que celles qu'on aurait obtenues en transportant au corps des fonctions sur Γ_0 la définition donnée par Artin pour les fonctions L sur un corps de nombres algébriques. En particulier, la fonction $L_{\chi_0}(u)$ qui correspond au caractère principal χ_0 du groupe G n'est autre que la fonction zêta attachée à la courbe Γ_0 et au corps k. Quant à l'identité des fonctions $L_\chi(u)$, dans le cas où G est un groupe abélien, avec celles qu'on définit an moyen de caractères du groupe des diviseurs sur Γ_0, elle résulte, comme on sait, de la loi de réciprocité d'Artin, que nous examinerons, du point de vue de la géométrie algébrique, dans un mémoire suivant.