Charles Pisot

Diviseurs - Différentielles Théorème de Riemann-Roch

Séminaire de Mathématiques (Julia), tome 5 (1937-1938), exp. n° 2, p. 1-30
<http://www.numdam.org/item?id=SMJ_1937-1938__5__A2_0>

V.-E.

SEMINAIRE DE MATHEMATIQUES

Cinquième année 1937-1938

LES FONCTIONS ALGEBRIQUES

La Théorie algébrique des Fonctions algébriques-II

Diviseurs - Différentielles

Théorème de Riemann-Roch

Exposé fait par M. Charles PISOT, le lundi 31 Janvier 1938

Exemplaire n° 3

DIVISEURS

Dans ce qui suit, nous désignerons par $K = k(x, y_1, \dots, y_s)$ un corps de fonctions algébriques, c'est-à-dire une extension transcendante d'un corps de constantes k suivie d'un nombre fini d'extensions algébriques. Nous supposerons que k est le plus grand corps de constantes figurant dans K, mais nous ne ferons aucune restriction sur la nature de k.

Rappelons quelques propriétés établies dans la dernière conférence et qui vont principalement nous servir dans la suite : Dans K il y a une infinité de valuations et chacune est équivalente à un diviseur premier ou encore un point P de K. Une valuation est une manière d'attribuer à toute fonction z de K un nombre entier $\nu_P(z)$ appelé ordre de z en P, jouissant de certaines propriétés. Pour tout diviseur premier P, il y a des fonctions u de K, appelées uniformisantes locales en P, dont l'ordre $\nu_P(u) = 1$. Toute fonction z peut alors se mettre quel que soit r, sous la forme :

$$z = \alpha_e u^e + \alpha_{e+1} u^{e+1} + \dots + \alpha_r u^r + x_r u^{r+1}$$

x_r étant une fonction d'ordre 0 en P et $\alpha_o, \alpha_1, \dots, \alpha_r$

étant des éléments d'un certain corps de restes σ , extension algébrique de k , appelé <u>corps des valeurs</u> des fonctions de K en P . Sous cette forme, l'ordre $\nu_P(z)$ est en évidence ; on a en effet $\nu_P(z) = e$. Le degré $d = (\sigma : k)$ de l'extension σ est appelé le <u>degré absolu</u> $d = n(P)$ du diviseur premier P .

Un diviseur premier d'un sous-corps de K , transcendant sur k , se décompose dans K en un nombre fini de diviseurs premiers .

<u>Définitions</u>.

De façon générale, on appelle <u>diviseur</u> A d'un corps K , un produit formel, étendu à un ensemble de diviseurs premiers P_i de K , chacun avec un exposant entier $e_i \gtrless 0$, et dont un nombre fini seulement est $\neq 0$

$$A = \prod_i P_i^{e_i}$$

e_i est appelé l'<u>ordre</u> de P_i dans A et on le désigne par $\nu_{P_i}(A)$. Soit $d_i^* = n^*(P_i)$ le degré du diviseur P_i relativement à un sous-corps K^* de K , on appelle <u>degré relativement à K^*</u> du diviseur A l'expression :

$$n^*(A) = \sum_i d_i^* e_i$$

si $d_i = n(P_i)$ est le <u>degré absolu</u> de P_i . $n(A) = \sum d_i e_i$ est le degré absolu de A .

On appelle <u>produit</u> $AA' = B$ des diviseurs $A = \sum_i P_i^{e_i}$ et $A' = \sum_i P_i^{e'_i}$ le diviseur $B = \prod_i P_i^{e_i + e'_i}$

On en déduit immédiatement que :

$$n(AA') = n(A) + n(A')$$

Un diviseur B est dit <u>multiple</u> du diviseur A si l'on a $\nu_{P_i}(B) \geq \nu_{P_i}(A)$ pour tout diviseur premier P_i de B . On écrit alors $B \equiv 0 \pmod{A}$.

Les diviseurs forment un groupe multiplicatif dont le diviseur unité E est caractérisé par le fait que $\nu_P(E) = 0$ quel que soit le diviseur premier P de K .

Un diviseur A est <u>entier</u> s'il est multiple du diviseur E , c'est-à-dire si $\nu_P(A) \geq 0$ quel que soit P . Tout diviseur B peut se mettre sous la forme d'un quotient $\frac{A}{A'}$ de deux diviseurs entiers A et A' . Ces diviseurs entiers A et A' sont déterminés par B si on les suppose premiers entre eux, c'est-à-dire si aucun diviseur premier a un ordre non nul à la fois dans A et dans A' . Dans ce cas, A est appelé <u>diviseur numérateur</u> et A' <u>diviseur dénominateur</u> de B .

Diviseur d'une fonction

Considérons d'abord une extension simplement transcendante du corps de constantes k. Tout élément x n'appartenant pas à k engendre cette extension lorsqu'on adjoint x à k. Il n'y a que deux valuations de $k(x)$ donnant à x un ordre non nul, correspondant aux diviseurs premiers A et A' ; A correspond à x et A' à $\frac{1}{x}$ et l'on a $\nu_A(x) = - \nu_{A'}(x) = 1$ et $n(A) = n(A') = 1$.

On dira que $B = \frac{A}{A'}$ est le diviseur de x dans $k(x)$. Pour tout diviseur premier Q de $k(x)$ on aura $\nu_Q(x) = \nu_Q(B)$ et d'autre part $n(B) = 0$.

Soit alors K une extension algébrique de $k(x)$. Le diviseur A est la projection d'un nombre fini de diviseurs premiers $P_1, P_2, \ldots, P_r$ de K, avec les ordres de ramification $e_1, e_2, \ldots, e_r$. Dans K on peut écrire $A = \prod_{i=1}^{r} P_i^{e_i}$. Par définition de la projection d'un diviseur, on a $\nu_{P_i}(x) = e_i = \nu_{P_i}(A)$, et $\nu_P(x) > 0$ que si P est l'un des P_i. De même, nous avons :

$$A' = \prod_i P'^{e'_i}_i \quad \text{et} \quad \nu_{P'_i}(x) = - e'_i = \nu_{P_i}(A^{-1}) < 0.$$

Nous dirons encore que $\frac{A}{A'} = B$ est le diviseur de x dans

K et nous écrirons $B \backsim x$.

A et A' étant premiers entre eux , A est appelé le diviseur numérateur et A' le diviseur dénominateur de x .

On voit immédiatement que pour tout diviseur premier P de K on a $\nu_P(x) = \nu_P(B)$ et par suite si $x \backsim B$, on a $x x' \backsim B B'$. Nous allons également montrer que $n(B) = 0$.

Théorème

Si $x \backsim \frac{A}{A'}$, on a $n(A) = n(A') = (K:k(x))$

Soit $\mathfrak{o}$ l'anneau des fonctions t de $k(x)$ pour lesquelles $\nu_A(t) \geq 0$, A étant le diviseur numérateur de x dans $k(x)$. $\mathfrak{o}$ est formé des quotients $\frac{p(x)}{p'(x)}$ de polynomes $p(x)$ et $p'(x)$ en x où $p'(x)$ n'est pas divisible par x . Soit $\mathfrak{O}$ l'anneau des fonctions y de K telles que $\nu_{P_i}(y) \geq 0$ pour tous les P_i figurant effectivement dans le diviseur numérateur A de x dans K . Nous montrerons que $\mathfrak{O}$ possède une base par rapport à $\mathfrak{o}$. La démonstration est possible grâce à l'existence d'un anneau $\mathfrak{o}' = k\left[\frac{1}{x}\right]$ des polynomes en $\frac{1}{x}$ et de l'anneau $\mathfrak{O}'$ des fonctions de K entières par rapport à $\mathfrak{o}'$ (c'est à-dire vérifiant une équation $y^r + x_1 y^{r-1} + \ldots + x_r = 0$.

où les x_i appartiennent à $\mathcal{O}'$).

Posons $\nu^*(y) = \underset{P_i \in A}{\text{borne}} \left\{ E\left(\frac{\nu_{P_i}(y)}{\nu_{P_i}(A)}\right)\right\}$. $E(a)$ étant l'entier immédiatement inférieur à a. Si y appartient à $\mathcal{O}'$ on voit facilement que $\nu^*(y) = 0$. Toute fonction de K est quotient de deux éléments de $\mathcal{O}'$, on peut donc trouver $n = (K:k(x))$ fonctions linéairement indépendantes par rapport à $k(x)$ dans $\mathcal{O}'$. Soit y_1 une fonction de $\mathcal{O}'$ telle que $\nu^*(y_1) = \alpha_1$ soit le plus grand possible. De même, soit y_m $(m \leq n)$ un élément de $\mathcal{O}'$ linéairement indépendant par rapport à $k(x)$ de $y_1, y_2, \ldots, y_{m-1}$ et tel que $\alpha_m = \nu^*(y_m)$ soit le plus grand possible. $y_1, y_2, \ldots, y_n$ forment alors une base de K par rapport à $k(x)$ et $0 \geq \alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_n$.

La définition de $\nu^*(y)$ montre que $z_i = y_i\, x^{-\alpha_i}$ appartient à $\mathcal{O}$. Si alors $t_1, t_2, \ldots t_n$, sont des éléments de $k(x)$ tels que $\sum_{i=1}^{n} t_i z_i$ appartienne à $\mathcal{O}$, il en résulte que les t_i appartiennent à $\mathcal{O}$. En effet, supposons qu'il n'en soit pas ainsi. Il existe alors une fonction $y' = \sum_{i=1}^{n} t'_i z_i$ de $\mathcal{O}$, l'une des fonctions $t'_i = \frac{p_i(x)}{p'_i(x)}$ n'étant pas dans $\mathcal{O}$. $p'_i(x)$ est alors divisible par x, et il existe une puissance positive h telle que la fonction $y = \sum_{i=1}^{n} t_i z_i$ où $y = y'x^h$

appartient à $\mathfrak{V}x$, tandis que les fonctions $t_i = t'_i x^h$ appartiennent à $\mathfrak{v}$ sans appartenir toutes à $\mathfrak{v}x$. On peut donc trouver des constantes $\varepsilon_i \equiv u_i \pmod{\mathfrak{v}x}$ de k non toutes nulles telles que

$$z = \sum_{i=1}^{m} \varepsilon_i z_i \; , \; \varepsilon_m \neq 0 \; , \text{ soient}$$

contenues dans $\mathfrak{V}x$, c'est-à-dire que $\nu^*(z) > 0$. Il en résulte que $\nu^*(x^{\alpha_m} z) > \alpha_m$, or $z x^{\alpha_m} = \sum_{i=1}^{m} \varepsilon_i y_i x^{\alpha_m - \alpha_i}$ est contenu dans $\mathfrak{V}'$ et $\varepsilon_m \neq 0$, ceci contredit le choix de y_m .

Le système $z_1, z_2, \ldots. z_n$ forme une base de l'anneau $\mathfrak{V}$ par rapport à $\mathfrak{v}$. La base $y_1, y_2 \ldots . y_n$ correspondante de K par rapport à k(x) est dite <u>base normale</u> par rapport au diviseur A .

Comme il y a $e_i \, n(P_i)$ éléments de $\mathfrak{V}$ linéairement indépendants (mod $P_i^{e_i}$) on en déduit

$$n(A) = \sum_{i=1}^{r} e_i \, n(P_i) = n = \big(K : k(x)\big) .$$

En remplaçant x par $\frac{1}{x}$ on a de même

$$n(A') = \big(K : k(\tfrac{1}{x})\big) = \big(K : k(x)\big)$$

d'où le théorème annoncé .

Remarque .- On déduit facilement du théorème précédent la proposition suivante :

$\overline{K}$ étant une extension finie d'un corps K de fonctions algébriques, P un diviseur premier de K, $\overline{P}_1, \overline{P}_2, \dots, \overline{P}_r$ les diviseurs premiers de $\overline{K}$ se projetant sur P, e_i leurs ordres de ramification et d_i leurs degrés relatifs, on a :

$$\sum_{i=1}^{r} d_i \, e_i = (\overline{K} : K)$$

Cette proposition n'est en général plus vraie si K est un corps quelconque, on a construit effectivement des corps K où l'on a $\sum_{i=1}^{r} d_i \, e_i < (\overline{K}:K)$

Classes de diviseurs .

Comme le diviseur de toute constante de k est le diviseur unité E et réciproquement, toute fonction x de K est définie, à une constante de k près, par son diviseur B. En effet, si $x \backsim B$, et $x' \backsim B$, $\frac{x}{x'} \backsim E$ donc appartient à k.

Les diviseurs des fonctions de K s'appellent principaux, ils forment un sous-groupe $\mathcal{G}$ du groupe $\mathcal{A}$ de tous les diviseurs de K ; ils sont tous de degré 0.

Les classes de restes $\mathfrak{A}/\mathfrak{H}$ s'appellent <u>classes de diviseurs</u>. Tous les diviseurs d'une même classe $\mathcal{L}$ ont même degré appelé <u>degré de la classe</u>, c'est le degré $n(A)$ d'un diviseur quelconque de $\mathcal{L}$. Si A et A' sont deux diviseurs d'une même classe $\mathcal{L}$, $A\,A'^{-1}$ appartient à $\mathfrak{H}$ c'est-à-dire, il y a une fonction x de K dont le diviseur est $A\,A'^{-1}$ et réciproquement.

Soient $A_1, A_2, \ldots, A_r$ des diviseurs de la classe $\mathcal{L}$, A un diviseur quelconque de $\mathcal{L}$. Il y a donc des fonctions $z_1, z_2, \ldots, z_r$ de K telles que $z_i \backsim A_i A^{-1}$. Soit A' un autre diviseur de $\mathcal{L}$ et $z'_i \backsim A_i A'^{-1}$. Si alors $z \backsim A\,A'^{-1}$, on aura $z'_i = \varepsilon_i\, z\, z_i$, ε_i étant une constante de k. Les r fonctions z_i et les r fonctions z'_i sont donc simultanément linéairement dépendantes ou indépendantes par rapport à k. On dira qu'il en est ainsi des diviseurs A_1 $A_2, \ldots, A_r$ de $\mathcal{L}$.

Désignons par $L(A)$ l'ensemble des fonctions z de K multiples d'un diviseur A^{-1} (c'est-à-dire dont le diviseur est multiple de A^{-1}). C'est l ensemble des fonctions z telles que $\nu_P(z) \geq -\nu_P(A)$ pour tout diviseur premier P de K. Cette dernière définition montre immédiatement que $L(A)$ est <u>un module</u> par rapport à k. Nous démontrerons que ce module $L(A)$ est de dimension finie $\ell(A)$; $\ell(A)$ est égal au nombre de diviseurs entiers de la classe $\mathcal{L}$ de A, indépendants par rapport à k et ne dépend pas du diviseur particulier A de $\mathcal{L}$ choisi. Le nombre $\ell(A)$ s'appelle la <u>dimension de la classe</u> $\mathcal{L}$.

Soient donc $z_1, z_2, \ldots, z_r$ r fonctions de $L(A)$ linéairement indépendantes par rapport à k,

$$z = \sum_{i=1}^{r} \lambda_i z_i$$ est encore une fonction de $L(A)$ si les λ_i sont des constantes de k. Soit P un diviseur premier de K figurant alternativement dans A et u une uniformisante locale correspondante.

On aura :

$$z = \alpha_e u^e + \alpha_{e+1} u^{e+1} + \ldots$$

les constantes $\alpha_e, \alpha_{e+1}, \ldots$ appartenant au corps des restes $\mathfrak{S}$, de degré $n(P)$ par rapport à k, et
$\nu_P(z) = e \geq - \nu_P(A)$.

Soit alors B un autre diviseur tel que A soit multiple de B. Cherchons à déterminer les constantes λ_i de manière que z appartienne à $L(B)$. Nous avons à écrire que $\nu_P(z) \geq - \nu_P(B)$ $\left(\geq - \nu_P(A)\right)$, c'est-à-dire à annuler au plus $\nu_P(A) - \nu_P(B)$ des coefficients α_e,

$\alpha_{e+1}, \ldots$ Ces coefficients étant dans σ , nous avons donc au plus $n(P)\left[\nu_P(A) - \nu_P(B)\right]$ équations (S) à coefficients dans k pour chaque diviseur premier P de A , et par conséquent au plus $n(A) - n(B)$ équations de ce type. Il en résulte que parmi ces fonctions z il y a au plus $r - \left[n(A) - n(B)\right]$ fonctions linéairement indépendantes appartenant à $L(B)$ et par suite que :

$$\ell(B) \geq r - \left[n(A) - n(B)\right]$$

Prenons alors pour B l'inverse du diviseur dénominateur de A ou d'un multiple de ce diviseur dénominateur . Le degré $n(B)$ de B sera négatif et il n'y a aucune fonction z multiple de B^{-1} , donc $\ell(B) = 0$. Par suite, $r \leq n(A) - n(B)$ et le nombre r des fonctions de $L(A)$ linéairement indépendantes par rapport à k est borné .

Si B est un diviseur quelconque dont A est multiple, la même démonstration montre que

$$\ell(B) \geq \ell(A) - \left[n(A) - n(B)\right]$$

ou encore que

$$n(A) - \ell(A) \geq n(B) - \ell(B)$$

<u>Genre du corps K</u>

<u>L'expression</u> $n(A) - \ell(A) + 1$ <u>est bornée su-</u>

<u>périeurement par un nombre g qui ne dépend que du corps K, et qui est appelé genre de K</u>.

Pour démontrer ce théorème, nous allons prendre un élément quelconque x fixe de K, et utiliser le corps auxiliaire $k(x)$.

Soit d'abord A' un multiple entier de A, P un diviseur premier figurant effectivement dans A'. P se projette sur $k(x)$ en un diviseur premier Q de $k(x)$, qui dans K est multiple de P, car Q se décompose dans K en un produit de diviseurs premiers contenant en particulier P. Au diviseur $A' = \prod P^e$ correspond ainsi un diviseur $A'' = \prod Q^e$ de $k(x)$ qui dans K est multiple de A'. Au diviseur premier Q de $k(x)$, correspond un polynome irréductible f de degré α et $f \sim \frac{Q}{Q'^{\alpha}}$ si Q' est le diviseur dénominateur de x dans $k(x)$. Par suite :

$$\frac{A''}{Q'^{a}} \sim \prod f^e \qquad \text{où} \qquad a = \sum \alpha e$$

A'' et Q'^{a} envisagés comme diviseurs de K appartiennent à la même classe et $n(A'') = n(Q'^{a})$, $\ell(A'') = \ell(Q'^{a})$

Par suite

$$n(A) - \ell(A) \leq n(A'') - \ell(A'') = n(Q'^{a}) - \ell(Q'^{a})$$

On peut toujours déterminer un entier b et une base $y_1, y_2, \dots, y_n$ de K par rapport à $k(x)$ telle

que tous les y_i soient multiples de Q'^{-b} . En effet si Q_1 est le diviseur dénominateur commun dans K d'une base quelconque $y'_1, y'_2, \dots, y'_n$, on peut déterminer comme plus haut un multiple Q'_1 de Q_1 tel que $\frac{Q'_1}{Q^{-b}} \sim \prod f'^{e'}$.
La base $y_i = y'_i \prod f'^{e'}$ satisfait aux conditions .

Considérons alors les fonctions $z = \sum_{i=1}^{n} y_i p_i(x)$

où $p_i(x)$ est un polynome arbitraire en x de degré d au plus . $p_i(x)$ étant multiple de Q'^{-d} et y_i de Q'^{-b} z appartient à $L(Q'^{d+b})$. Il y a $(d+1)n$ fonctions $x^{d_i} y_i$, $d_i \leq d$, linéairement indépendantes par rapport à k donc $\ell(Q'^{d+b}) \geq (d+1)n$. D'autre part on a vu que , envisagé comme diviseur de K , on a $n(Q') = n$, donc $n(Q'^{d+b}) = (d+b)n$. Donc dès que $d > a-b$, Q'^{d+b} est multiple de Q'^a et

$$n(Q'^a) - \ell(Q'^a) = n(Q'^{d+b}) - \ell(Q'^{d+b}) \leq (b-1)n$$

ce qui constitue la proposition énoncée .

On a, en particulier, $n(E) = 0$, $\ell(E) = 1$, donc si A est un diviseur entier

$$g \geq n(A) - \ell(A) + 1 \geq n(E) - \ell(E) + 1 = 0$$

Il existe donc au moins un diviseur entier G tel que:

$$n(G) - \ell(G) + 1 = g$$

Tout multiple d'un diviseur G est encore un diviseur G.

Si B est un diviseur quelconque, $n(B) - \ell(B) + 1 \leq g$. Posons :

$$\ell(B) = n(B) + 1 - g + r(B) \qquad \text{alors} \quad r(B) \geq 0 .$$

Cette formule nous donne la dimension d'une classe de diviseurs, en fonction de son degré, dès que l'on connait $r(B)$. C'est ce nombre que nous allons déterminer dans la suite .

DIFFERENTIELLES

Définition de A. WEIL

Un diviseur quelconque B étant donné, considérons un multiple de B qui soit un diviseur G. Reprenons encore les $n(G) - n(B)$ équations (S), linéaires dans k, que l'on obtient en écrivant qu'un z de $L(G)$ appartient aussi à $L(B)$. Comme ici, $r(G) = 0$, on a :

$$\ell(B) = \ell(G) - \left[n(G) - n(B)\right] + r(B)$$

$r(B)$ est donc le nombre exact de relations linéaires distinctes existant entre les premiers membres des équations (S).

Soit $R(z) = 0$ une telle relation et considérons le développement

$$z = \alpha_e u^e + \alpha_{e+1} u^{e+1} + \dots + \alpha_r u^r$$

en un diviseur premier P figurant effectivement dans G ou dans B, u étant une uniformisante locale correspondante. En utilisant une base du corps de restes σ, contenant tous les coefficients α_r, par rapport à k, on voit que α_r apporte une contribution ε_r à $R(z)$, ε_r étant dans k. Ainsi $R(z) = 0$ s'écrit

$$\sum_P \left(\sum_{r=-\nu_P(G)}^{-\nu_P(B)-1} \varepsilon_r \right) = 0$$

Nous associerons alors à ε_r une constante ω_{-r-1} du corps σ telle que $\alpha_r \, \omega_{-r-1} = \varepsilon_r$. Considérons l'expression

$$\sum_{s=\nu_P(B)}^{\nu_P(G)-1} \omega_s \, u^s$$

comme étant les premiers termes du développement en P, d'un nouvel être ω que nous appellerons une <u>différentielle</u> du corps K. Dans ces conditions la contribution à $R(z) = 0$ des coefficients de z en P sera exactement le coefficient de u^{-1} dans le produit formel $z\,\omega$. On appelle ce coefficient <u>résidu</u> de $z\,\omega$ en P et on le notera

$\oint_P z\,\omega$. La définition montre que c'est un élément de R. La relation $R(z) = 0$ elle-même sera représentée par le symbole $\oint z\,\omega = \sum_P \oint_P z\,\omega = 0$. Comme L(G) forme un module, $\oint z\,\omega = 0$ sera évidemment vérifiée pour toute fonction z de L(G) .

Nous allons montrer que l'on peut obtenir le développement de la différentielle ω aussi loin que l'on veut , en tout point P de K .

En effet soit G' un diviseur multiple de G nous dirons que la relation $\oint z\,\omega = 0$ se prolonge dans L(G') et définit encore la même différentielle ω si pour toute fonction z de L(G') qui appartient aussi à L(G) la relation $\oint z\,\omega = 0$ se reduit à la relation de définition de ω . En effet on ne peut avoir deux relations distinctes se réduisant pour un z de L(G) à la même relation, sinon il y aurait une relation se réduisant identiquement à 0 pour tout z de L(G) et ce serait une relation entre les équations exprimant qu'un z de L(G') appartient à L(G) . Donc r(G) ne serait pas nul , contrairement à la définition de G . D'autre part, r(B) ne change pas si on remplace G par G' , chaque relation dans L(G') est donc exactement le prolongement d'une relation dans L(G) . Comme G' est un multiple arbitraire de G . nous pouvons prendre, en tout diviseur premier P de K , $\nu_P(G')$ aussi grand que l'on veut, on a donc en tout P les ω_s d'indice s aussi grands que l'on veut.

Ayant ainsi défini une différentielle ω de K soit $x \backsim \frac{A}{A'}$ une fonction donnée de K . Pour tout z de $L(G')$, où $G' = G\,A'$, $z\,x$ appartient à $L(G)$; donc $\oint z\,x\,\omega = 0$ est une relation vérifiée pour tout z de $L(G)$ et par suite définit une nouvelle différentielle que nous désignerons par $x\,\omega$. L'ensemble des différentielles de K forme un module et on voit que ce module admet les éléments de K comme opérateurs .

Différentielles de première espèce .

Si B n'est pas un diviseur G , il se peut que pour certaines différentielles ω la relation $\oint z\,\omega = 0$ se réduise identiquement à 0 . On dit alors que la différentielle ω est multiple de B .

D'après cette définition, aucune différentielle ne peut être multiple d'un diviseur G . On a déjà remarqué qu'une relation $\oint z\,\omega = 0$ se réduisant identiquement à 0 donne une relation entre les équations (S) ; il y a donc exactement $r(B)$ différentielles , linéairement indépendantes par rapport à k , multiples de B . Cette définition montre encore que si x est multiple de A et ω de B, la différentielle $x\omega$ est multiple de AB.

Une différentielle ω est dite <u>entière ou de première espèce</u> si elle est multiple du diviseur unité E. Comme $r(E) = \ell(E) - n(E) - 1 + g = g$, il y a g différentielles distinctes de première espèce.

<u>Diviseur d'une différentielle</u>

Soit ω une différentielle, supposons-là multiple d'un diviseur B. $x\omega$ est entier si x appartient à $L(B)$. Il y a $\ell(B)$ fonctions x linéairement indépendantes, donc aussi au moins $\ell(B)$ différentielles entières $x\omega$, donc $\ell(B) \leq g$. D'autre part $n(B) - \ell(B) + 1 < g$ (le signe $=$ est exclu car B ne peut être un diviseur G) On a donc :

$$n(B) \leq 2g - 2$$

Il existe donc un diviseur Ω de degré maximum dont ω est multiple et tout diviseur dont ω est multiple divise Ω. On appelle ce diviseur Ω le <u>diviseur de la différentielle</u> ω et $n(\Omega) = n(\omega)$ le <u>degré de la différentielle</u> ω. On a donc $n(\omega) \leq 2g - 2$.

<u>Les diviseurs</u> Ω <u>de toutes les différentielles du corps</u> K <u>appartiennent à la même classe</u> $\mathcal{G}^*$ <u>de divi-</u>

seurs appelée classe canonique .

Pour le démontrer, nous montrerons que toute différentielle θ de K est de la forme $x\omega$, ω étant une différentielle arbitraire donnée . Soit A un diviseur entier différent de E , alors $n(A) > 0$ et $\ell(A^{-1}) = 0$ donc $r(A^{-1}) = n(A) + g - 1$. Supposons qu'il existe deux différentielles ω et θ telles que, quelles que soient les fonctions x, y de K , on ait toujours $x\omega \neq y\theta$. Prenons alors x dans $L(A\Omega)$ et y dans $L(A\Theta)$, Θ étant le diviseur de θ . $x\omega$ et $y\theta$ sont ainsi multiples de A^{-1} et il y aura au moins $\ell(A\Omega) + \ell(A\Theta)$ différentielles distinctes multiples de A^{-1} . Donc

$$r(A^{-1}) = n(A) + g - 1 \geq \ell(A\Omega) + \ell(A\Theta)$$

Or :

$$\ell(A\Omega) = n(A)+n(\Omega)+1-g+r(A\Omega) \geq n(A)+n(\omega)+1-g$$

et de même pour $\ell(A\Theta)$.

Donc :

$$n(A) \leq 3(g-1) - n(\omega) - n(\theta)$$

Or A étant arbitraire, $n(A)$ est aussi arbitrairement grand, ce qui nous donne une contradiction .

Toute différentielle θ est donc de la forme $x\omega$, et si X est le diviseur de x , on a $\Theta = X\Omega$

d'où la proposition annoncée. Il en résulte en particulier que les diviseurs des différentielles ont tous même degré.

Soit B un diviseur quelconque, toute différentielle multiple de B étant de la forme $x\omega$, x est un multiple de $B\Omega^{-1}$ donc appartient à $L(B^{-1}\Omega)$ et réciproquement. On a donc $r(B) = \ell(B^{-1}\Omega)$.

En particulier, pour $B = E$, $r(E) = g = \ell(\Omega)$ donc la dimension de la base canonique $\mathcal{G}^*$ est g.

De même, prenons pour B un multiple entier $\neq E$ de $G\Omega^{-1}$. B étant entier, $r(B^{-1}) = n(B) + g - 1 = \ell(B\Omega) = n(B) + n(\Omega) + 1 - g$, car $B\Omega$ est multiple de G. On en déduit que le degré $n(\Omega)$ de la classe canonique $\mathcal{G}^*$ est $2g - 2$.

De façon générale, on désigne par $\mathcal{G}^*/\mathcal{B}$ la classe du diviseur $B^{-1}\Omega$, $\mathcal{B}$ étant la classe de B. $\mathcal{G}^*/\mathcal{B}$ s'appelle classe complémentaire de $\mathcal{B}$. Elle n'existe que si $n(b) = 2g - 2$. Nous sommes maintenant en mesure de donner une réponse plus précise à la question dont nous sommes partis, et qui était de déterminer la dimension d'une classe quelconque de diviseurs.

Théorème de Riemann-Roch .

La dimension d'une classe $\mathcal{L}$ de diviseurs de K est donnée par la formule :

$$\dim(\mathcal{L}) = \text{degré}(\mathcal{L}) + 1 - g + \dim(\mathcal{G}^* / \mathcal{L})$$

Différentielles de Hasse

Soit $x = \sum_\nu \alpha_\nu u^\nu$ et $y = \sum_\nu \beta_\nu u^\nu$ les développements de deux fonctions x et y de K avec une variable uniformisante u correspondant à un diviseur premier P . Considérons la série $\sum \nu \alpha_\nu u^{\nu-1}$ que nous désignons par le symbole $\frac{dx}{du}$. Nous appellerons différentielle y dx l'ensemble des séries formelles $\sum_\nu \gamma_\nu u^\nu = (\sum_\nu \nu \alpha_\nu u^{\nu-1})(\sum_\nu \beta_\nu u^\nu)$ pour toute uniformisante locale u et pour tout diviseur premier P .

Cette définition des différentielles, contrairement à la précédente, n'a de sens que si k est parfait En effet , soit $f(x,y) = 0$ l'équation irréductible reliant x à y en tout point P ; il en sera de même pour la relation $f'_x \frac{dx}{du} + f'_y \frac{dy}{du} = 0$, les dérivées partielles f'_x , f'_y d'un polynome $f(x,y)$ étant définies formellement .

Si $K/k(x)$ n'est pas séparable, $f'_y = 0$ f'_x d'autre part n'est pas nul, sinon $f(x,y)$ serait une puissance $p^{\text{ième}}$ d'un polynome, p étant la caractétistique de k, et par suite réductible. Donc $\frac{dx}{du} = 0$ quelle que soit la variable uniformisante u choisie.

Réciproquement supposons $K/k(x)$ séparable et k parfait. Si pour une variable u on a $\frac{dx}{du} = 0$ on a nécessairement $\frac{dy}{du} \neq 0$, sinon les indices ν des coefficients des développements des deux fonctions x et y seraient tous multiples de la caractéristique p. D'autre part, $K = k(x,y)$, il en serait donc ainsi de toutes les fonctions de K, ce qui n'est pas pour la fonction u par exemple. Par suite, $f'_y = 0$, ce qui est en contradiction avec l'hypothèse que $K/k(x)$ est séparable.

Une démonstration analogue nous montre aussi que le rapport de deux différentielles dx_1 et dx_2 est une fonction de K. Il suffit de considérer l'équation $f(x_1,x_2) = 0$ liant x_1 à x_2. Par suite toute différentielle de K se déduit de l'une d'elles par multiplication par une fonction de K.

<u>Dans le cas d'un corps k parfait, les deux notions de différentielles coincident</u>.

Pour démontrer ce fait, nous montrerons d'abord que le coefficient γ_{-1} de u^{-1} dans la différentielle de Hasse $y\,dx$ est indépendant de l'uniformisante u et ne dépend que du diviseur premier P. Nous appellerons ce coefficient <u>résidu</u> de $y\,dx$ en P. Ce n'est différent de zéro que pour un nombre fini de diviseurs premiers et nous démontrerons que <u>la somme des résidus en tous les diviseurs premiers de K est nulle</u>. On reconnait là exactement la définition de Weil de la différentielle dx, lorsqu'on écrit le résidu en P sous la forme $\oint_P y\,dx$ et la somme des résidus en tous les diviseurs premiers sous la forme $\oint y\,dx$. Or dans les deux définitions, toute différentielle de K se déduit de l'une quelconque d'entre elles par multiplication avec une fonction arbitraire de K ce qui montre bien l'identité des deux notions.

<u>Résidu en un diviseur premier P</u>.

Soit $\sum_\nu \gamma_\nu u^\nu$ le développement de la différentielle de Hasse $y\,dx$ en un diviseur premier P. Soit v une autre uniformisante en P, on aura

$$u = \lambda_1 v + \lambda_2 v^2 + \dots \qquad \text{avec } \lambda_1 \neq 0$$

Le développement de $y\,dx$ en v s'obtient par la substitution :

$$y \frac{dx}{dv} = y \frac{dx}{du}\frac{du}{dv} = \Big[\sum_{\nu} \gamma_\nu \big(\sum_{\mu} \mu \lambda_\mu v^{\mu-1}\big)^\nu\Big]\Big[\sum_{\mu} \mu \lambda_\mu v^{\mu-1}\Big]$$

$$= \sum_{\nu} \bar{\gamma}_\nu v^\nu$$

Nous avons à montrer que $\gamma_{-1} = \bar{\gamma}_{-1}$. Remplaçons alors dans ces formules les quantités γ_ν et λ_μ par des variables c_ν et ℓ_μ algébriquement indépendantes par rapport à l'anneau Γ des entiers rationnels ordinaires. L'égalité à démontrer est alors immédiate et donne une identité entre polynomes en c_ν et ℓ_μ . Ces identités restent vraies si on remplace Γ par le corps des restes Γ_p des entiers (mod p) et si on remplace alors c_ν et ℓ_μ par γ_ν et λ_μ qui appartiennent à une extension algébrique de Γ_p .

<u>Théorème des résidus</u>

<u>La somme des résidus d'une différentielle de Hasse pour tous les diviseurs premiers de K est nulle</u> .

Une différentielle de Hasse y dx ne peut avoir de résidu $\neq 0$ qu'en un diviseur premier P figurant dans le diviseur dénominateur de x ou dans celui de y , donc en un nombre fini de diviseurs premiers .

Le théorème à établir dans le cas d'un corps simplement transcendant $k(x)$ résulte immédiatement de la décomposition d'une fraction rationnelle en éléments simples. Nous allons ramener le cas général à celui-là. Pour cela, nous supposerons d'abord le corps k algébriquement fermé (complet). Soit P un diviseur premier de K se projetant en Q sur $k(x)$, nous montrerons que :

$$\sum_{P \in Q} \oint_P y \, dx = \oint_Q S(y) \, dx$$

la somme au premier membre étant étendue à tous les diviseurs premiers P se projetant sur Q, et $S(y)$ étant la trace de y par rapport à $k(x)$, donc étant un élément de $k(x)$. Soit alors u une uniformisante pour P et K_P le corps des séries formelles en u à coefficients dans k ; de même, soit v une uniformisante pour Q dans $k(x)$ et $k_Q(x)$ l'anneau des séries formelles en v à coefficients dans k. $k_Q(x)$ est alors la somme directe $\sum_{P \in Q} K_P$ pour tous les P se projetant en Q et il suffit de montrer la relation :

$$\oint_P y \, dx = \oint_Q S_P(y) \, dx$$

où $S_P(y)$ représente la trace de y de K_P par rapport à $k_Q(x)$.

Alors, $y \, dx = y \frac{dx}{dv} dv$ et $S_P(y) dx = S_P(y\frac{dx}{dv}) dv$

car $\frac{dx}{dv}$ est un élément de $k(x)$, donc aussi de $k_Q(x)$.

En utilisant le développement de $y \frac{dx}{dv}$ en u il suffit donc de montrer pour tout ν que :

$$\oint_P u^\nu \, dv = \oint_Q S_P(u^\nu) \, dv$$

Soit e l'ordre de ramification de P dans Q, alors $1, u, \ldots, u^{e-1}$ est une base de l'anneau $K_P / k_Q(x)$ et on a :

$$\frac{u^e}{v} = g_o(v) + u\, g_1(v) + \ldots + u^{e-1} g_{e-1}(v)$$

les $g_i(v)$ étant des séries formelles de $k_Q(x)$, et $g_o(v)$ une série unité, c'est-à-dire $g_o(0) \neq 0$.

La relation :

$$u^e = v \left[g_o(v) + u\, g_1(v) + \ldots + u^{e-1} g_{e-1}(v) \right]$$

est dite équation d'Eisenstein entre u et v.

1°) Supposons k de caractéristique 0. On peut alors toujours trouver deux uniformisantes u et v telles que l'équation d'Eisenstein qui les relie soit :

$$u^e = v$$

On a $\quad u^\nu \frac{dv}{du} = e\, u^{\nu+e-1}$ donc $\oint_P u\, dv = \begin{cases} e & \text{si } \nu = -e \\ 0 & \text{si } \nu \neq -e \end{cases}$

$$S_p(u^\nu) = \begin{cases} e\, v^{\frac{\nu}{e}} & \text{si } \nu \equiv 0 \pmod{e} \\ 0 & \text{dans les autres cas} \end{cases}$$

donc : $$\oint_Q S_p(u^\nu)\, dv = \begin{cases} e & \text{si } \nu = -e \\ 0 & \text{si } \nu \neq -e \end{cases}$$

Le théorème est donc démontré .

2°) Supposons k de caractéristique $p \neq 0$. En remplaçant au besoin u par l'uniformisante $\frac{u}{\gamma_o(v)}$

$\gamma_o(v)$ étant une fonction de $k_Q(x)$ telle que $\left[\gamma_o(v)\right]^e = g_o(v)$ ($\gamma_o(v)$ existe car k est complet) , on pourra réduire l'équation d'Eisenstein à la forme :

$$(1) \qquad u^e = v\left[1 + u\, g_1(v) + \ldots + u^{e-1} g_{e-1}(v)\right]$$

Dans $g_i(v) = \sum_{\mu=0}^{\infty} \gamma_{i,\mu}\, v^\mu$ remplaçons alors les $\gamma_{i,\mu}$ par des variables $c_{i,\mu}$ algébriquement indépendantes par rapport à l'anneau Γ des entiers rationnels ordinaires et considérons l'équation d'Eisenstein :

$$(2) \qquad \overline{u}^e = \overline{v}\left[1 + \overline{u}\, \overline{g}_1(\overline{v}) + \ldots + \overline{u}^{e-1} \overline{g}_{e-1}(\overline{v})\right]$$

où $\overline{g}_i(\overline{v}) = \sum_{\mu=0}^{\infty} c_{i,\mu}\, \overline{v}^\mu$ sont des séries entières en $\overline{v}$

à coefficients dans l'anneau $\Gamma[c_{i,\mu}]$ des polynomes en $c_{i,\mu}$ à coefficients entiers rationnels. Ces coefficients sont donc des éléments du corps $K_Q(x)$ de toutes les séries en $\overline{v}$ à coefficients dans le corps algébriquement fermé déduit du corps $\mathcal{R}(c_{i,\mu})$, $\mathcal{R}$ étant le corps des nombres rationnels. L'équation d'Eisenstein (2) définit alors une extension algébrique K_P de $K_Q(x)$ de degré e et on montre que cette extension peut être engendrée par une équation du type $\overline{u}^e = \overline{v}$. Le théorème précédent y est donc vérifié, c'est-à-dire pour tout ν on a les identités :

$$\oint_P \overline{u}^{\nu} \, d\overline{v} = \oint_Q S_P(\overline{u}^{\nu}) \, d\overline{v}$$

Or, le fait que dans (2) $\overline{g}_0(\overline{v}) = 1$ montre que les coefficients du développement de $\overline{v}$ en série de $\overline{u}$ appartiennent à $\Gamma[c_{i,\mu}]$, donc aussi les coefficients a_μ de $\dfrac{d\overline{v}}{d\overline{u}} = \sum a_\mu \overline{u}^\mu$.

On a alors $\oint_P \overline{u}^{\nu} \, d\overline{v} = a_{-\nu-1}$

D'autre part, les formules de Newton pour les racines de (2) envisagée comme équation en $\overline{u}$ montrent que les coefficients $b_{\nu,\mu}$ du développement de

$$S_P(\bar{u}^{\nu}) = \sum_{\mu} b_{\nu,\mu} \, \bar{v}^{\mu}$$

en série de $\bar{v}$ appartiennent aussi à $\Gamma[c_{i,\mu}]$. On a ici $\oint_Q S_P(\bar{u}^{\nu}) \, d\bar{v} = b_{\nu,-1}$

Nous avons donc l'identité des deux polynomes en $c_{i,\mu}$:

$$a_{-\nu-1} = b_{\nu,-1}$$

Elles restent vérifiées en remplaçant Γ par le corps des restes Γ_p modulo p , et en y remplaçant les variables $c_{i,\mu}$ par les quantités $\gamma_{i,\mu}$ de k , extension algébrique de Γ_p . Comme les opérations effectuées sont algébriquement identiques dans les deux cas, il en résulte le théorème des résidus .

Enfin, supposons k toujours parfait, mais non algébriquement fermé . Soit $\bar{K}$ le corps obtenu en complétant algébriquement le corps K . Tout diviseur premier P de K de degré m se décompose dans $\bar{K}$ en m diviseurs premiers P_i de degré 1 et le résidu $\oint_P y \, dx = \sum_{i=1}^{m} \oint_{P_i} y dx$

Comme on a démontré le théorème des résidus pour $\bar{K}$, il est donc aussi vérifié dans K .

BIBLIOGRAPHIE

DEDEKIND-WEBER   Theorie der algebraischen Functionen
J. de Crelle T.92 (1882) p.181-290

F.K.SCHMIDT   Zur arithmetischen Theorie der algebraischen Functionen I.
Math.Zeitschrift T.41 (1936) p.415-438

H.HASSE   Theorie der Differentiale in algebraischen Functionenkörpem mit collkommenen Konstantenkörper .
J. de Crelle T.172 (1935) p.55-64

La première définition des différentielles, ainsi que la démonstration exposée du théorème de Riemann-Roch sont dues à A.WEIL et n'ont pas encore été publiées .

Pour la définition des différentielles dans un corps quelconque, on peut aussi voir :

H.HASSE und F.K.SCHMIDT   Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Functionenkörper einer Unbestimmten
J. de Crelle T.177 (1937) p.215-237

O.TEICHMÜLLER   Differentialrechnung bei Characteristik p
J. de Crelle T.175 (1936) p.89