[1939a] Sur l'analogie entre les corps de nombres algébriques et les corps de fonctions algébriques

André Weil

On connaît diverses analogies entre les corps de nombres algébriques et les corps de fonctions algébriques d'une variable ; le but de cette note est, par des moyens tout élémentaires, de préciser en quelques points cette analogie.

Soit K un corps de nombres algébriques, de degré n. Comme on sait, on est conduit à introduire dans l'étude de K des éléments qui correspondent aux points de la surface de Riemann d'un corps de fonctions algébriques d'une variable, et que pour cette raison nous appellerons les "points" de K : on fait correspondre un tel "point" P à toute représentation isomorphe et partout dense de K dans un "corps local" $\mathrm{K_P}$ qui peut être, soit le corps des nombres réels, soit le corps des nombres complexes, soit un corps de nombres P-adiques (au sens de Hensel) ; bien entendu, deux représentations de K ne devront pas être considérées comme distinctes si elles se déduisent l'une de l'autre par un isomorphisme des corps locaux correspondants. Si $\mathrm{K_P}$ est le corps des nombres réels, P s'appellera un point réel à l'infini de K ; si $\mathrm{K_P}$ est le corps des nombres complexes, P s'appellera un point imaginaire à l'infini de K ; si $\mathrm{K_P}$ est un corps P-adique, P correspondra à un idéal premier $\mathfrak{p}$ de K.

Soit α un élément de K ; soit α_P l'élément de $\mathrm{K_P}$ qui correspond à α dans la représentation de K dans $\mathrm{K_P}$ définie par P. Nous poserons :

$I_\mathrm{P}(\alpha) = \log|\alpha_\mathrm{P}|$ si P est un point réel à l'infini ;

$I_\mathrm{P}(\alpha) = 2\log|\alpha_\mathrm{P}|$ si P est un point imaginaire à l'infini ;

$I_\mathrm{P}(\alpha) = -n\cdot\log \mathrm{N}(\mathfrak{p})$ si P est un point de K correspondant à l'idéal premier $\mathfrak{p}$, celui-ci figurant avec l'exposant n dans l'expression de l'idéal principal (α) comme produit de puissances d'idéaux premiers distincts.

Les théorèmes élémentaires connus sur la norme montrent qu'on a, avec ces notations :

$$\sum_\mathrm{P} I_\mathrm{P}(\alpha) = 0,$$

la sommation étant étendue à tous les points P de K. Bien entendu, $I_\mathrm{P}(\alpha)$ ne diffère de zéro que pour un nombre fini de points P de K, de sorte que la somme du premier membre ne comprend qu'un nombre fini de termes non nuls. Cette relation doit être considérée comme analogue arithmétique du théorème algébrique suivant : soit K un corps de fonctions algébriques d'une variable ; x étant un élément de K, et P un point de la surface de Riemann de K, soit $I_\mathrm{P}(x)$ l'ordre de x au point P, c'est-à-dire l'entier égal à n si x a en P un pôle d'ordre n, à $-n$ si x a en P un zéro d'ordre n, et à 0 si x n'est ni nul, ni infini en P ; on aura :

$$\sum_\mathrm{P} I_\mathrm{P}(x) = 0,$$

égalité qui peut être considérée comme un cas particulier du théorème de Cauchy, puisqu'elle résulte de l'égalité :

$$\int d(\log\ x) = 0,$$

lorsque l'intégrale est étendue à un contour formé de $2g$ rétrosections (g étant le *genre* de K).

Considérons maintenant, dans le corps de fonctions algébriques K, le théorème de Riemann-Roch. Celui-ci peut être énoncé sous la forme suivante[1]. Supposons donné, pour chaque point P, un entier n, de telle façon que n_{P} ne diffère de zéro que pour des points P en nombre fini ; soit $n = \sum n_{\mathrm{P}}$ (la sommation étant étendue à tous les points P). Le théorème de Riemann-Roch indique combien il y a d'éléments linéairement indépendants du corps K qui satisfassent, quel que soit P, à la condition

$$I_{\mathrm{P}}(x) \leq n_{\mathrm{P}}$$

En particulier, il indique que, dès que n est assez grand (et, d'une manière précise, dès que $n > 2g - 2$), ce nombre est $n - g + 1$.

Revenons à un corps K de nombres algébriques ; supposons donné pour tout "point" P de K, un nombre réel n_{P}, de façon que n_{P} ne diffère de zéro que pour des points P en nombre fini, et que de plus, si P correspond à un idéal premier $\mathfrak{p}$ de K, n_{P} soit de la forme $\nu(\mathfrak{p}) \cdot \log \mathrm{N}(\mathfrak{p})$, le facteur $\nu(\mathfrak{p})$ étant entier. Posons $n = \sum n_{\mathrm{P}}$. Soit N le nombre des éléments α de K qui satisfont, quel que soit P, à la condition :

$$I_{\mathrm{P}}(\alpha) \leq n_{\mathrm{P}}.$$

Cette condition, si on l'applique d'une part à tous les points P correspondant à des idéaux premiers $\mathfrak{p}$ de K, donne

$$\alpha \in \mathfrak{a} = \prod \mathfrak{p}^{-\nu(\mathfrak{p})}$$

où le second membre ne comprend, en vertu de la définition de n_{P} et de $\nu(\mathfrak{p})$, qu'un nombre fini de facteurs différents de 1, et a donc un sens bien défini. D'autre part, la même condition, appliquée aux points à l'infini de K, donne, pour chaque point réel à l'infini

$$|\alpha_{\mathrm{P}}| \leq e^{n_{\mathrm{P}}}$$

et, pour chaque point imaginaire à l'infini:

$$|\alpha_{\mathrm{P}}|^2 \leq e^{n_{\mathrm{P}}}$$

Si, alors, on désigne par $\alpha_1, \alpha_2, ..., \alpha_n$ une base de l'idéal $\mathfrak{a}$, de sorte que tout élément de $\mathfrak{a}$ soit de la forme :

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n,$$

N apparaîtra comme le nombre de points $(x_1, x_2, \ldots, x_n))$ à coordonnées entières qui se trouvent dans un domaine de l'espace à n dimensions défini par certaines inégalités élémentaires. Nous nous contenterons ici de l'évaluation assez grossière de N qui est fournie par le volume de ce domaine, volume qu'il est facile de calculer élémentairement. On trouve ainsi :

$$\log N = n - \log(2^{-r_1 - r_2}\pi^{-r_2}\sqrt{|d|}) + \varepsilon,$$

où r_1 est le nombre des points réels à l'infini de K, r_2 le nombre des points imaginaires à l'infini de K, d le discriminant de K, et où ε est aussi petit qu'on veut dès que, les $\nu(\mathfrak{p})$ étant supposés fixes,

[1] Cf. A. Weil, Zur algebraischen Theorie der algebraischen Funktionen, Journal de Crelle, t. 179 (1938), p. 129.

chacun des nombres n_{P} relatifs aux points à l'infini de K est suffisamment grand.

Pour avoir une formule entièrement analogue au théorème de Riemann-Roch, il faut observer de plus que les racines de l'unité dans K, et elles seules, satisfont à la condition $I_P(\alpha) = 0$ quel que soit P : elles jouent donc le rôle que jouent les constantes dans un corps de fonctions algébriques. Si, dans un corps K de fonctions algébriques, un élément x satisfait en tout point P à la condition $I_{\mathrm{P}}(x) \leq n_{\mathrm{P}}$, il en sera de même de même de cx si c est une constante arbitraire : on a le droit de voir dans ce facteur constant arbitraire l'origine du terme $+1$ du théorème de Riemann-Roch. De même, si, dans un corps de nombres K, un élément α satisfait quel que soit P à la condition $I_{\mathrm{P}}(\alpha) \leq n_{\mathrm{P}}$, le produit de α par une racine de l'unité contenue dans K y satisfait aussi. Cela conduit à poser, en désignant par w le nombre de racines de l'unité contenues dans K :

$$g = \log(2^{-r_1 - r_2}\pi^{-r_2} \cdot w\sqrt{|d|}),$$

et à écrire la formule ci-dessus sous la forme:

$$\log \mathrm{N} = n - g + \log w + \varepsilon;$$

le nombre g, qui apparaît ainsi comme le "*genre*" du corps K, joue, comme on sait, un rôle important dans la théorie de la fonction zêta de ce corps. On est conduit à penser, en même temps, que le rôle joué par la quantité $g - 1$ dans la théorie des corps de fonctions sera joué en arithmétique par $g - \log w$; ce qu'on peut confirmer par la remarque suivante. Soit K$'$ un corps contenant K, non ramifié par rapport à K, et de degré relatif f; s'il s'agit de corps de fonctions algébriques d'une variable, les genres g, g' de K, K$'$, sont liés entre eux par la relation :

$$g' - 1 = f(g - 1) \ ;$$

dans le cas arithmétique, le genre étant défini comme ci-dessus, on vérifie facilement que l'on a :

$$g' - \log w' = f(g - \log w).$$

Nous allons maintenant montrer qu'à côté de la formule :

$$\sum_{\mathrm{P}} I_{\mathrm{P}}(\alpha) = 0$$

qui est une traduction des résultats classiques sur les normes, l'on peut mettre une formule non moins élémentaire relative aux traces. Soit α un élément de K ; pour simplifier le langage dans ce qui va suivre, on supposera que α engendre K, c'est-à-dire que, n étant le degré de K, α est racine d'une équation *irréductible* de degré n, à coefficients rationnels :

$$F(t) = t^n - t \cdot t^{n-1} + \ldots = 0$$

Par rapport au corps des nombres réels F(t) se décompose en r_1 facteurs du premier degré, et r_2 facteurs du second degré, correspondant respectivement aux points à l'infini réels et imaginaires de K. Posons, si P est un point réel à l'infini de K, $\mathrm{T}_{\mathrm{P}}(\alpha_{\mathrm{P}}) = \alpha_{\mathrm{P}}$; si P est un point imaginaire à l'infini, $\mathrm{T}_{\mathrm{P}}(\alpha_{\mathrm{P}}) = \alpha_{\mathrm{P}} + \overline{\alpha}_{\mathrm{P}}$ (la barre dénotant suivant l'usage l'imaginaire conjugué). On aura donc l'expression suivante de la trace r de α :

$$r = \sum_{\mathrm{P}} \mathrm{T}_{\mathrm{P}}(\alpha_{\mathrm{P}})$$

la sommation étant étendue aux points à l'infini de K.

Soit de même p un nombre premier rationnel ; k désignant le corps des nombres rationnels, on désignera par k_{P} le corps *p-adique* correspondant à p. Le polynome $\mathrm{F}(t)$ se décomposera, par rapport à k_{P}, en autant de facteurs que p possède dans K de diviseurs premiers ; chacun de ceux-ci définira un point P de K, et le corps K_{P} contiendra k_{P} ; on désignera par $\mathrm{T}_{\mathrm{P}}(\alpha_{\mathrm{P}})$ la trace de α_{P} par rapport au corps k_{P} : c'est un nombre de k_{P}, et le facteur de $\mathrm{F}(t)$ correspondant à P, s'il est de degré m, commencera par les termes $t^m - \mathrm{T}_{\mathrm{P}}(\alpha_{\mathrm{P}}) \cdot t^{m-1} + ...$ On aura donc :

$$r = \sum_{\mathrm{P}} \mathrm{T}_{\mathrm{P}}(\alpha_{\mathrm{P}})$$

la sommation étant étendue cette fois à tous les points P correspondant aux idéaux premiers de K qui divisent p.

Mais, si u est un nombre quelconque de k_{P}, il existe des entiers rationnels a, b tels que $u - a \cdot p^{-b}$ soit un entier de k_{P} ; le nombre $u' = a \cdot p^{-b}$ est bien déterminé, modulo 1, par cette condition : il détermine donc un élément du groupe additif des nombres réels modulo 1, qu'on appellera la partie polaire de u. En particulier, désignons par $t_{\mathrm{P}}(\alpha)$ la partie polaire de $\mathrm{T}_{\mathrm{P}}(\alpha_{\mathrm{P}})$; posons

$$r' = \sum_{\mathrm{P}} t_{\mathrm{P}}(\alpha_{\mathrm{P}})$$

la sommation étant étendue cette fois aux points P correspondant à tous les idéaux premiers de K ; $t_{\mathrm{P}}(\alpha_{\mathrm{P}})$ étant nul chaque fois que α_{P} est entier, c'est-à-dire chaque fois que $I_{\mathrm{P}}(\alpha_{\mathrm{P}}) \leq 0$, la somme du second membre ne contient qu'un nombre fini de termes non nuls. Quel que soit le nombre premier p, le nombre rationnel $r - r'$ est entier dans k_{P} : $r - r'$ est donc entier rationnel, c'est-à-dire que $r \equiv r' \pmod 1$.

Posons alors, chaque fois que P est un point à l'infini de K, $t_{\mathrm{P}}(\alpha_{\mathrm{P}}) = -\mathrm{T}_{\mathrm{P}}(\alpha_{\mathrm{P}}) \pmod 1$. La combinaison des résultats ci-dessus donne la formule que nous avions en vue :

$$\sum_{\mathrm{P}} t_{\mathrm{P}}(\alpha_{\mathrm{P}}) \equiv 0 \pmod 1$$

la sommation étant étendue à tous les points de K.

Cette formule, bien entendu, reste vraie même si α n'engendre pas K.

Soit maintenant ω un élément de K ; l'application de la formule ci-dessus à $\omega\alpha$ donne :

$$\sum_{\mathrm{P}} t_{\mathrm{P}}(\omega_{\mathrm{P}}\alpha_{\mathrm{P}}) \equiv 0.$$

Si, ω étant laissé fixe, on pose $f_{\mathrm{P}}(\alpha_{\mathrm{P}}) = t_{\mathrm{P}}(\omega_{\mathrm{P}}\alpha_{\mathrm{P}})$, f_{P} est un caractère du groupe additif des nombres de K_{P} (c'est-à-dire une représentation continue de ce groupe dans le groupe additif des nombres réels modulo 1). On a ainsi une infinité de relations entre des caractères $f_{\mathrm{P}}(\alpha_{\mathrm{P}})$. Réciproquement, supposons qu'on ait fait correspondre, à tout point P de K, un caractère $f_{\mathrm{P}}(\alpha_{\mathrm{P}})$ du groupe additif des nombres de K_P, de telle manière que, pour α entier dans K, les $f_P(\alpha_P)$ soient tous nuls à l'exception d'un nombre fini d'entre eux, et qu'ils soient liés, quel que soit α dans K, par la relation

$$\sum_{P} f_P(\alpha_P) \equiv 0.$$

Il est facile de montrer que dans ces conditions il existe un nombre ω de K tel que l'on ait, quel que soit P :

$$f_P(\alpha_P) \equiv t_P(\omega_P \alpha_P)$$

Autrement dit, nous avons trouvé toutes les relations de la forme indiquée entre caractères locaux des nombres de K. Cela montre que la relation :

$$\sum_{P} t_P(\omega_P \alpha_P) \equiv 0$$

doit être considérée comme l'analogue arithmétique de la relation (cas particulier du théorème de Cauchy dans la théorie des fonctions algébriques) :

$$\int x\omega = 0,$$

où x est un élément quelconque d'un corps de fonctions algébriques K, ω une différentielle appartenant au même corps, et où l'intégrale est prise le long d'un contour formé de $2g$ rétrosections.