L'hypothèse de Riemann
pour les corps de fonctions algébriques de caractéristique p ,
II.

Claude CHEVALLEY

Soit donnée une variété algébrique V dans un espace projectif sur un corps algébriquement fermé L ; nous supposons la variété V dépourvue de singularités, et nous désignerons sa dimension par n . On appelle cycle de dimension p sur V toute combinaison linéaire formelle à coefficients entiers de sous-variétés de dimension p de V . Si les coefficients des variétés qui interviennent dans un cycle sont tous ≥ 0 , on dit que le cycle est positif. Les variétés qui interviennent avec des coefficients $\neq 0$ dans un cycle sont appelées les composantes de ce cycle.

Si V est une courbe, les points de V correspondent d'une manière biunivoque aux places du corps des fonctions rationnelles sur V . Les notions de cycle de dimension 0 sur V et de diviseur du corps des fonctions rationnelles sur V sont donc équivalentes.

D'une manière générale, si V est de dimension n , les cycles de dimension $n - 1$ sur V sont appelés diviseurs de V . Les variétés de dimension $n - 1$ sur V correspondent de manière biunivoque aux valuations du corps $L(V)$ des fonctions rationnelles sur V dont les centres sont de dimension $n - 1$. On en déduit la possibilité d'attacher à tout $x \neq 0$ de $L(V)$ un diviseur $\delta(x)$. Les diviseurs $\delta(x)$ forment un sous-groupe du groupe de tous les diviseurs de V ; deux diviseurs dont la différence appartient à ce sous-groupe sont appelés équivalents.

Soient V et V' des variétés sans singularités dans des espaces projectifs. On peut alors former une variété $V \times V'$ sans singularité dans un espace projectif convenable dont les points correspondent biunivoquement aux couples (M, M') formés d'un point M de V et d'un point M' de V' . Le point de $V \times V'$ qui correspond à (M, M') se désigne par $M \times M'$. Soient W et W' des sous-variétés de V et de V' , de dimensions respectives p et p' ; les points $M \times M'$ tels que $M \in W$ et $M' \in W'$ forment alors une sous-variété $W \times W'$ de dimension $p + p'$ de $V \times V'$. On en déduit par linéarité la définition du cycle $X \times X'$ si X est un cycle sur V et X' un cycle sur V' .

Soit R un corps de fonctions algébriques d'une variable sur un corps fini K à q éléments. Soit L une clôture algébrique de K , et soit R_L le corps déduit de R par extension à L du corps de base. On peut alors former une courbe Γ sans singularité dans un espace projectif dont R_L soit le corps des fonctions rationnelles. Tout cycle de dimension 1 sur la surface $\Gamma \times \Gamma$ est appelé une correspondance sur Γ ; les courbes sur $\Gamma \times \Gamma$ sont appelées correspondances irréductibles sur Γ . Si C est une correspondance irréductible, on dit qu'un point M' de Γ correspond à un point M par la correspondance C si $M \times M'$ est sur C . Les points $M \times M'$ (pour $M \in \Gamma$) forment une courbe sur $\Gamma \times \Gamma$ que l'on appelle la diagonale de $\Gamma \times \Gamma$, ou la correspondance identique. Si C est une correspondance irréductible, les points $M' \times M$ tels que $M \times M' \in C$ forment une correspondance irréductible que l'on désigne par C' ; l'application $C \rightarrow C'$ s'étend par linéarité aux correspondances quelconques.

On peut supposer que Γ est définie par un système d'équations à coefficients dans K . Soit r un entier > 0 , et soient $x_0, \dots, x_N$ les coordonnées d'un point M de Γ . Alors le point M^{q^r} de coordonnées $x_0^{q^r}, \dots, x_N^{q^r}$ est encore un point de Γ , et les points $M \times M^{q^r}$ (pour tous les $M \in \Gamma$) forment une correspondance irréductible J_r sur Γ . Les points d'intersection de J_r avec la diagonale Δ sont les points $M \times M$, où M est un point de Γ qui a un système de coordonnées formé d'éléments du corps K_r algébrique de degré r sur K . Le nombre de ces points est le nombre c_r des places de degré 1 du corps R_{K_r} (cf. l'exposé précédent); c'est ce nombre qu'il faut évaluer pour démontrer l'hypothèse de Riemann. Pour ce faire on a besoin des notions relatives à l'intersection des cycles d'une variété algébrique.

Utilisant les mêmes notations que plus haut, soient W_1 et W_2 des sous-variétés de V de dimensions respectives p_1 et p_2 . Supposons que W_1 et W_2 n'aient en commun aucune variété de dimension $> p_1 + p_2 - n$. On peut alors associer à W_1 et à W_2 un cycle d'intersection $W_1.W_2$ de dimension $p_1 + p_2 - n$. C'est un cycle positif dans lequel interviennent les variétés de dimension $p_1 + p_2 - n$ communes à W_1 et W_2 et celles-là seulement. On en déduit par linéarité la notion de cycle d'intersection $X_1.X_2$ de deux cycles quelconques; ce cycle n'est défini que si l'intersection de toute composante de X_1 avec toute composante de X_2 est définie. Si X_1 est de dimension 1 et X_2 de dimension $n - 1$, le cycle $X_1.X_2$ (s'il est défini) est de dimension 0; la somme des coefficients d'un cycle de degré 0 s'appelle le degré de ce cycle; on pourra donc parler du degré de $X_1.X_2$, qu'on désigne par $\deg(X_1.X_2)$. Si de plus X_1 est une courbe sans singularité, $X_1.X_2$ peut être considéré comme un diviseur du corps des fonctions rationnelles sur X_1 ; on l'appelle le diviseur induit par X_2 sur X_1 .

Considérons le cas où $V = \Gamma \times \Gamma$. Soit X une correspondance sur Γ . Si X a des composantes de la forme $M \times \Gamma$, on en retire une correspondance de la forme $a \times \Gamma$ (où a est un diviseur sur Γ) tel que la différence $X_0 = (-a) \times \Gamma$ n'ait plus de composante de la forme $M \times \Gamma$. Pour tout $M \in \Gamma$, l'intersection $(M \times \Gamma).X_0$ est alors définie et s'écrit $M \times X(M)$, où $X(M)$ est un diviseur sur Γ . On en déduit par linéarité la définition de $X(b)$ pour tout diviseur b sur Γ . Le degré de $X(M)$ ne dépend pas de M et se désigne par $d(X)$. On pose $d'(X) = d(X')$. Soient X et Y des correspondances; si $X.Y$ est défini, $\deg(X.Y)$ se désigne par $I(X.Y)$. Ce nombre ne change pas si on remplace X et Y par des correspondances qui leur soient respectivement équivalentes. On en déduit la possibilité de définir $I(X.Y)$ pour des correspondances X et Y quelconques. Si $M \in \Gamma$, on voit facilement que $J_r(M) = M^{q^r}$, d'où $d(J_r) = 1$, $J_r'(M^{q^r}) = q^r M$, d'où $d'(J_r) = q^r$; de plus, les points d'intersection de J_r avec la diagonale Δ interviennent avec le coefficient 1 dans $J_r.\Delta$, d'où $I(J_r.\Delta) = c_r$. La quantité $1 + q^r - c_r$ est donc égale à $d(J_r) + d'(J_r) - I(J_r.\Delta)$.

Pour toute correspondance X nous poserons $\sigma(X) = d(X) + d'(X) - (X.\Delta)$.

Soient X et Y des correspondances sur Γ . On démontre alors qu'il existe une correspondance $Z = X \circ Y$ univoquement déterminée qui possède les propriétés suivantes : si $P \in \Gamma$, on a $Z(P) = X(Y(P))$, $Z'(P) = Y'(X'(P))$. On obtient ainsi une loi de composition bilinéaire non commutative dans l'ensemble des correspondances. A. WEIL a montré que l'on a

$$\sigma(X \circ X') \geq 0$$

pour toute correspondance X . Montrons comment ce résultat entraîne l'hypothèse de Riemann.

Soient x et y des entiers ; posons $X = xJ_r + y\Delta$, et écrivons que $\sigma(X \circ X') \geq 0$. Il est évident que $J_r \circ J'_r = q^r \Delta$; posons $k = \sigma(\Delta)$, d'où $\sigma(x^2 J_r \circ J'_r) = kq^r x^2$.

Si Y est une correspondance quelconque, on a évidemment $Y = \Delta = \Delta \circ Y = Y$; et la considération de l'application $M \times M' \rightarrow M' \times M$ de $\Gamma \times \Gamma$ dans lui-même montre que l'on a $\sigma(Y') = \sigma(Y)$.

Les nombres $\sigma(J_r \circ \Delta')$ et $\sigma(\Delta \circ J'_r)$ sont donc égaux à $1 + q^r - c_r$.

Il vient donc

$$kq^r x^2 + 2(1 + q^r - c_r)xy + ky^2 \geq 0$$

d'où $(1 + q^r - c_r)^2 \leq k^2 q^r$, ce qui entraîne déjà l'hypothèse de Riemann. De plus, on peut démontrer que $I(\Delta, \Delta) = 2g - 2$ si g est le genre de Γ ; le nombre k est donc égal à $2g$.

Bibliographie

WEIL (ANDRÉ). – Sur les courbes algébriques et les variétés qui s'en déduisent. – Paris, Hermann, 1948.

On trouvera dans cet ouvrage, outre la démonstration complète de l'hypothèse de Riemann pour la fonction dzêta, la démonstration de l'hypothèse analogue pour les séries L attachées à une courbe. Une autre démonstration de l'hypothèse de Riemann pour la fonction dzêta a été donnée par

ROQUETTE (PETER). – Arithmetischer Beweis der Riemannschen Vermutung in Kongruenz funktionenkörpern beliebigen Geschlechts, J. für die reine und angew. Math., t. 191, 1953, p. 199-252.

[Avril 1957]