

Zeitschrift: L'Enseignement Mathématique
Band: 19 (1973)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ÉQUATIONS ET VARIÉTÉS ALGÈBRIQUES SUR UN CORPS FINI
Kapitel: §3. Courbes de genre quelconque.
Autor: Joly, Jean-René
DOI: <https://doi.org/10.5169/seals-46287>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

Download PDF: 13.10.2024

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

§ 3. Courbes de genre quelconque.

3.1. L'égalité $N = q + 1$, pour une courbe de genre 0, et l'inégalité $|q + 1 - N| \leq 2q^{1/2}$, pour une courbe de genre 1 (th. 1, cor. 1, et th. 2, cor. 1), sont des cas particuliers du résultat suivant, dû à Weil (1940, 1948):

THÉORÈME 3 (« hypothèse de Riemann » pour V). — Si V est une courbe projective non singulière de genre g définie sur k , et si N désigne le nombre de points de V rationnels sur k , on a

$$(3.1.1) \quad |q + 1 - N| \leq 2gq^{1/2}.$$

Démonstration. — Soit $W = V \times V$ la surface produit de V par elle-même, c'est-à-dire le lieu sur k du point (x, y) , où x et y sont deux points génériques de V , indépendants sur k (voir [20], p. 29, ou Samuel (1967), § I et II). On appelle *correspondance sur V* ([20], p. 29) tout diviseur sur V , donc tout cycle de dimension 1 sur V ; si X est une correspondance sur V , on appelle *symétrique de X* et on note X' la correspondance image de X par la symétrie $(x, y) \mapsto (y, x)$ de W ; si X et Y sont deux correspondances sur V , on appelle *somme de X et Y* et on note $X + Y$ leur somme en tant que diviseurs sur V ; on appelle *produit* (de composition: rien à voir avec le produit d'intersection) *de X et Y* et on note $X \circ Y$ la correspondance déduite de X et Y par l'opération de composition des graphes dans le produit $V \times V$ (pour une définition précise, voir [20], pp. 35-38); enfin, on écrit $X \equiv Y$ s'il existe deux diviseurs m et n sur la courbe V et une fonction rationnelle f sur la surface W tels que

$$X - Y = (m \times V) + (V \times n) + (f),$$

(f) désignant le diviseur de la fonction f . On peut alors montrer ([20], pp. 38-41) que la relation \equiv est une relation d'équivalence dans l'ensemble des correspondances sur V , et qu'elle est compatible avec les opérations somme et produit introduites ci-dessus: l'ensemble quotient par \equiv de l'ensemble des correspondances sur V se trouve ainsi muni d'une structure d'anneau; on le note $A(V)$, et on l'appelle *anneau des correspondances de V* ; si $\xi, \eta \in A(V)$ sont les images de correspondances X et Y sur V , leur somme $\xi + \eta$ et leur produit $\xi\eta$ sont par définition les images dans $A(V)$ de $X + Y$ et de $X \circ Y$; noter que la symétrie $X \mapsto X'$ est évidemment compatible avec la relation \equiv ; elle définit donc par passage au quotient une involution $\xi \mapsto \xi'$ de $A(V)$ qui est en fait un anti-automorphisme de $A(V)$: si $\xi, \eta \in A(V)$, on a $(\xi + \eta)' = \xi' + \eta'$ et $(\xi\eta)' = \eta'\xi'$; noter aussi que si A

désigne la diagonale de W , c'est-à-dire le lieu sur k du point (\mathbf{x}, \mathbf{x}) , alors Δ est birégulièrement équivalente à V sur k , et δ , classe de la correspondance Δ sur V , est l'élément neutre de $A(V)$ pour la multiplication.

Pour toute correspondance X sur V , notons maintenant $d_1(X)$ et $d_2(X)$ les degrés des cycles $pr_1(X)$ et $pr_2(X)$, projections de X sur le premier et sur le second facteur de $W = V \times V$; notons d'autre part $i(X \cdot \Delta)$ le nombre d'intersection de X et Δ sur W (qui est défini même si Δ est une composante de X : voir par exemple Samuel (1967), p. 307), et posons

$$(3.1.2) \quad S(X) = d_1(X) + d_2(X) - i(X \cdot \Delta).$$

$S(X)$ est un entier rationnel, qui ne dépend que de la classe de la correspondance X ; si alors $\xi \in A(V)$, et si X désigne n'importe quelle correspondance d'image ξ dans $A(V)$, on peut définir un entier rationnel $\sigma(\xi)$, ne dépendant que de ξ , par l'égalité $\sigma(\xi) = S(X)$; $\sigma(\xi)$ est dit *trace de ξ* ; et on peut montrer ([20], pp. 41-54) que la trace possède les propriétés suivantes:

LEMME 1. — *Quels que soient $\xi, \eta \in A(V)$, on a $\sigma(\xi + \eta) = \sigma(\xi) + \sigma(\eta)$, $\sigma(\xi\eta) = \sigma(\eta\xi)$, et $\sigma(\xi') = \sigma(\xi)$.*

LEMME 2. — *δ désignant toujours la classe de Δ , on a $\sigma(\delta) = 2g$.*

LEMME 3. — *Quel que soit $\xi \neq 0$ dans $A(V)$, on a $\sigma(\xi\xi') > 0$.*

Le lemme 1 est immédiat; le lemme 2 résulte du fait que $d_1(\Delta) = d_2(\Delta) = 1$, de la formule classique $i(\Delta \cdot \Delta) = 2 - 2g$ (Samuel (1967), p. 307, (2)), et de la définition (3.1.2) de $\sigma(\delta) = S(\Delta)$. Le lemme 3 est la « clef de voûte » de la démonstration: c'est de l'inégalité $\sigma(\xi\xi') \geq 0$ convenablement appliquée que va résulter l'inégalité (3.1.1). Soit en effet Γ le lieu sur k du point $\mathbf{z} = (\mathbf{x}, \mathbf{x}^{(q)})$ (la notation $\mathbf{x}^{(q)}$ a été définie dans la sect. 2.1); Γ est une correspondance sur V (« correspondance de Frobenius »), et sa symétrique Γ' est le lieu sur k du point $\mathbf{z}' = (\mathbf{x}^{(q)}, \mathbf{x})$; on a évidemment $[k(\mathbf{x}):k(\mathbf{x}^{(q)})] = 1$ et $[k(\mathbf{x}^{(q)}):k(\mathbf{x})] = q$, donc $d_1(\Gamma) = 1$ et $d_2(\Gamma) = q$; on peut d'autre part montrer que chacun des points du cycle intersection $\Gamma \cdot \Delta$ a pour multiplicité 1: comme les composantes de ce cycle sont exactement les points (\mathbf{a}, \mathbf{a}) de $V \times V$ avec $\mathbf{a} = \mathbf{a}^{(q)}$, c'est-à-dire avec \mathbf{a} rationnel sur k , on voit que $i(\Gamma \cdot \Delta) = N$; si alors γ désigne la classe de la correspondance Γ , la formule de définition (3.1.2) permet d'écrire

$$(3.1.3) \quad \sigma(\gamma) = q + 1 - N.$$

On peut démontrer par ailleurs que $\gamma\gamma' = q\delta$; soit maintenant m un entier rationnel et posons $\xi = \gamma - m\delta$; on a $\xi' = \gamma' - m\delta$, et

$$\xi\xi' = m^2\delta - m(\gamma + \gamma') + \gamma\gamma';$$

prenons les traces des deux membres, tenons compte de la valeur de $\gamma\gamma'$ et utilisons les lemmes 1 et 2; il vient:

$$\sigma(\xi\xi') = 2gm^2 - \sigma(\gamma + \gamma')m + 2gq;$$

mais $\sigma(\gamma + \gamma') = 2\sigma(\gamma) = 2(q+1-N)$ (lemme 1 et formule (3.1.3)); ainsi:

$$\sigma(\xi\xi') = 2gm^2 - 2(q+1-N)m + 2gq;$$

le lemme 3 montre que le polynôme en m figurant dans le membre de droite de cette dernière égalité est positif; on a donc

$$(q+1-N)^2 - 4g^2q \leq 0,$$

ce qui implique l'inégalité (3.1.1) et prouve le théorème 3.

3.2. On peut également démontrer le théorème 3 à l'aide de la théorie des variétés abéliennes (structure de l'anneau des endomorphismes, propriétés du polynôme caractéristique d'un endomorphisme, etc.; voir par exemple [20], § VII à XI, ou [9], chap. 5) appliquée à la jacobienne de la courbe V . Pour $g = 1$, cette seconde démonstration coïncide avec la démonstration du « théorème de Hasse » donnée dans la section 2.2 (dans ce cas en effet, V , admettant un point rationnel sur k par le théorème de Schmidt, s'identifie à sa propre jacobienne); dans le cas général (g quelconque), cette seconde démonstration n'est pas essentiellement différente de celle esquissée dans la section 3.1, du fait que l'anneau des correspondances sur V est isomorphe à l'anneau des endomorphismes de la jacobienne de V ([20], pp. 161-163, th. 22 et cor. 2).

3.3. Revenons à l'inégalité (3.1.1). Considérons à titre d'exemple la courbe plane $X^4 + Y^4 = 1$, et supposons $q \equiv 1 \pmod{4}$. Si ψ est un caractère d'ordre 4 de k^* , la proposition 3 du chapitre 6 montre que le nombre de points « à distance finie » sur cette courbe est égal à $q + \sum_{1 \leq j_1 \leq j_2 \leq 3} \pi(\psi^{j_1}, \psi^{j_2})$; la somme comprend neuf termes, dont trois sont des sommes de Jacobi triviales (pour $j_1 + j_2 = 4$) et valent -1 (chap. 5, prop. 9, (i)), les six autres (notons-les $\alpha_1, \dots, \alpha_6$) étant des sommes de Jacobi non triviales, de module $q^{1/2}$: le nombre de points « à distance finie » est donc

$q - 3 + \alpha_1 + \dots + \alpha_6$. Maintenant, la courbe étudiée, considérée comme projective, est non-singulière, de genre $g = (4-1)(4-2)/2 = 3$, par la formule de Plücker, et elle admet quatre points à l'infini; ainsi, $N = q - 3 + 4 + \alpha_1 + \dots + \alpha_6$, et on a

$$|q + 1 - N| \leq |\alpha_1| + \dots + |\alpha_6| = 6q^{1/2} = 2gq^{1/2},$$

ce qui vérifie directement le théorème 3 dans ce cas particulier.

La même vérification est possible plus généralement, grâce à la proposition 3 du chapitre 6, pour la courbe $X^{d_1} + Y^{d_2} = 1$, avec $q - 1$ divisible par d_1 et d_2 : on laisse au lecteur le soin de faire les calculs, et notamment de montrer que le genre est égal à $((d_1 - 1)(d_2 - 1) - (d - 1))/2$, avec $d = (d_1, d_2)$.

3.4. Le théorème 3 admet deux conséquences importantes:

COROLLAIRE 1. — Soit N_m le nombre de points de V rationnels sur $k_m = \mathbf{F}_{q^m}$. Alors, quand m tend vers l'infini, N_m tend lui-même vers l'infini; en particulier, pour tout m assez grand, $N_m \geq 1$.

Démonstration. — En effet, le théorème 3 appliqué au corps de base k_m donne $N_m \geq q^m + 1 - 2gq^{m/2}$, et le membre de droite tend vers l'infini avec m .

COROLLAIRE 2. — La courbe V possède un diviseur de degré 1 rationnel sur k .

Démonstration. — Le corollaire 1 montre qu'on peut trouver deux entiers successifs m et $m + 1$ tels que V admette un point rationnel sur k_m et un point rationnel sur k_{m+1} ; V admet donc un diviseur de degré m et un diviseur de degré $m + 1$ rationnels sur k , et il suffit de retrancher le premier du second pour obtenir un diviseur de degré $(m + 1) - m = 1$ rationnel sur k .

Pour $g \geq 2$, V ne possède généralement pas de point rationnel sur k : le diviseur de degré 1 dont l'existence est affirmée par le corollaire 2 ne peut donc généralement pas (sauf pour $g = 0$ ou 1: th. 1, cor. 1, et th. 2) être supposé positif.

§ 4. Variétés de dimension quelconque.

4.1. Soit V une variété projective définie sur k , de dimension r , et supposée plongée dans \mathbf{P}_n , espace projectif de dimension n sur k ; rappelons