

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 19 (1973)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ÉQUATIONS ET VARIÉTÉS ALGÈBRIQUES SUR UN CORPS FINI
Autor: Joly, Jean-René
Kapitel: §1. Courbes de genre 0 (*).
DOI: <https://doi.org/10.5169/seals-46287>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. 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. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

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. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

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. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 28.11.2025

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

notamment que si V est une variété de dimension ≥ 1 et si \mathbf{x} est un *point générique* de V , \mathbf{x} n'est pas considéré comme un *élément de V* : autrement dit, on n'a pas le droit d'écrire $\mathbf{x} \in V$). Pratiquement, pour la terminologie et les résultats de géométrie algébrique dont on aura effectivement besoin, le lecteur pourra se reporter au livre de Lang [12] ou à celui de Samuel [15].

Dans ce chapitre, k désigne (comme toujours) un corps fini à $q = p^f$ éléments, et \bar{k} une clôture algébrique de k . \mathbf{A}_n et \mathbf{P}_n désignent respectivement l'espace affine et l'espace projectif de dimension n sur k . Enfin, si V est un ensemble algébrique défini sur k , l'ensemble des points de V rationnels sur k est désormais noté V_k .

§ 1. Courbes de genre 0 (*).

1.1. THÉORÈME 1. — *Si V est une courbe projective non singulière de genre 0 définie sur k , elle est birégulièrement équivalente (sur k) à la droite projective définie sur k .*

Démonstration. — D'après un théorème classique de Poincaré (voir [18], pp. 71-72), V , de genre 0, est birégulièrement équivalente sur k soit à une droite, soit à une conique (ceci, sans hypothèse sur k ; ce théorème de Poincaré peut d'ailleurs se déduire facilement du théorème de Riemann-Roch: voir par exemple [2], chap. XVI, th. 6). On peut donc se borner à démontrer le théorème 1 lorsque V est une conique définie dans le plan projectif \mathbf{P}_2 par une équation homogène et de degré 2, $F(X_0, X_1, X_2) = 0$, à coefficients dans k : le théorème de Chevalley (chap. 3, th. 1, cor. 1) montre alors que cette équation admet une solution (a_0, a_1, a_2) non triviale dans k^3 , donc que V admet un point \mathbf{a} rationnel sur k . Soit maintenant Δ une droite projective du plan \mathbf{P}_2 , définie sur k et ne passant pas par \mathbf{a} (si par exemple $a_0 \neq 0$, on peut prendre pour Δ la droite d'équation $X_0 = 0$); pour tout point \mathbf{y} de Δ , notons $\varphi(\mathbf{y})$ le second point d'intersection de V et de la droite joignant \mathbf{a} à \mathbf{y} ; alors l'application $\mathbf{y} \mapsto \varphi(\mathbf{y})$ est évidemment une équivalence birégulière $\Delta \rightarrow V$ définie sur k , et le théorème 1 est démontré.

1.2. COROLLAIRE 1. — *Si N désigne le nombre de points de V rationnels sur k , on a exactement $N = q + 1$.*

*) Pour un résumé rapide et élémentaire des propriétés des courbes algébriques (genre, théorème de Riemann-Roch), voir SAMUEL (1967).

Démonstration. — Le théorème 1 permet de se limiter au cas où $V = \Delta$ (la droite projective); mais l'ensemble Δ_k des points de Δ rationnels sur k comporte évidemment q éléments « à distance finie » (correspondant bijectivement aux éléments de k), plus un élément « à l'infini » — soit au total $q + 1$ éléments, C.Q.F.D.

§ 2. Courbes de genre 1.

Pour la géométrie des courbes de genre 1, voir [4], notamment pp. 209-233.

2.1. THÉORÈME 2 (théorème de Schmidt). — *Si V est une courbe projective non singulière de genre 1 définie sur k , V admet au moins un point rationnel sur k .*

Démonstration. — D'après un théorème de Châtelet (voir par exemple [4], pp. 230-233), il existe une courbe projective non singulière G (la jacobienne de V), définie sur k , ayant un point \mathbf{o} rationnel sur k , et birégulièrement équivalente à V sur \bar{k} (ce qui permet d'identifier $\bar{k}(G)$ à $\bar{k}(V)$). G est évidemment de genre 1, comme V , et on peut la munir d'une loi de groupe rationnelle, définie sur k , notée additivement, ayant \mathbf{o} pour élément neutre, et faisant de G une variété abélienne de dimension 1 sur k ([4], pp. 210-211). De plus, l'identification $\bar{k}(G) = \bar{k}(V)$ permet de munir V d'une structure d'espace homogène principal sur G ([4], pp. 226-227), c'est-à-dire de construire deux applications rationnelles $\mu: V \times G \rightarrow V$, et $\nu: V \times V \rightarrow G$, définies sur k , et possédant les propriétés suivantes:

- (i) quel que soit $\mathbf{x} \in V$, on a $\mu(\mathbf{x}, \mathbf{o}) = \mathbf{o}$;
- (ii) quels que soient $\mathbf{x} \in V$ et $\mathbf{a}, \mathbf{b} \in G$, on a $\mu(\mu(\mathbf{x}, \mathbf{a}), \mathbf{b}) = \mu(\mathbf{x}, \mathbf{a} + \mathbf{b})$;
- (iii) quels que soient $\mathbf{x}, \mathbf{y} \in V$, il existe un $\mathbf{a} \in G$ et un seul tel que $\mu(\mathbf{x}, \mathbf{a}) = \mathbf{y}$, et \mathbf{a} est égal à $\nu(\mathbf{y}, \mathbf{x})$.

Concrètement, G opère sur V par translations: $\mu(\mathbf{x}, \mathbf{a})$ est le transformé de \mathbf{x} par la translation \mathbf{a} , et $\nu(\mathbf{y}, \mathbf{x})$ est la translation qui transforme \mathbf{x} en \mathbf{y} ; ainsi, il n'y a aucun risque de confusion à écrire $\mathbf{x} + \mathbf{a}$ au lieu de $\mu(\mathbf{x}, \mathbf{a})$ et $\mathbf{y} - \mathbf{x}$ au lieu de $\nu(\mathbf{y}, \mathbf{x})$; on adoptera cette écriture dans le reste de la démonstration.

Convenons d'autre part, pour tout point $\mathbf{x} = (x_0, x_1, \dots)$ d'un espace projectif de dimension quelconque sur k , de noter $\mathbf{x}^{(q)}$ le point (x_0^q, x_1^q, \dots) . Il est clair que \mathbf{x} est rationnel sur k si et seulement si $\mathbf{x}^{(q)} = \mathbf{x}$ (chap. 1, prop. 2 ou prop. 8). Il est clair également que si U est un ensemble algébrique