

**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:** §2. Courbes de genre 1.  
**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:** 27.04.2026

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

Démonstration. — Le théorème 1 permet de se limiter au cas où  $V = \Delta$  (la droite projective); mais l'ensemble  $\Delta_k$  des points de  $\Delta$  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

défini sur  $k$  et si  $\mathbf{x} \in U$ , alors  $\mathbf{x}^{(q)} \in U$  (représenter  $U$  par un système d'équations à coefficients dans  $k$ , et remarquer que l'élévation à la puissance  $q$ -ième est un automorphisme de  $k$  qui laisse invariante lesdits coefficients).

Appliquons ceci à  $V$  et  $G$ . Soit  $\mathbf{x}$  un élément quelconque de  $V$ , et posons  $\mathbf{a} = \mathbf{x} - \mathbf{x}^{(q)}$ . Considérons d'autre part l'application rationnelle  $\mathbf{z} \mapsto \mathbf{z}^{(q)} - \mathbf{z}$  de  $G$  dans  $G$ ; elle n'est certainement pas constante (sinon, on aurait  $\mathbf{z}^{(q)} - \mathbf{z} = \mathbf{o}^{(q)} - \mathbf{o} = \mathbf{o}$ , soit  $\mathbf{z}^{(q)} = \mathbf{z}$ , pour tout  $\mathbf{z} \in G$ ; tout point de  $G$  serait rationnel sur  $k$ , et  $G$  serait de dimension 0: absurde); comme  $G$  est irréductible, projective (donc complète), non singulière et de dimension 1, cette application est surjective. En particulier, il existe  $\mathbf{b} \in G$  tel que  $\mathbf{a} = \mathbf{b}^{(q)} - \mathbf{b}$ , donc, en revenant à la définition de  $\mathbf{a}$ , tel que  $\mathbf{x} + \mathbf{b} = \mathbf{x}^{(q)} + \mathbf{b}^{(q)} = (\mathbf{x} + \mathbf{b})^{(q)}$  (cette dernière égalité parce que l'application rationnelle  $\mu: V \times G \rightarrow V$ , qui à  $(\mathbf{x}, \mathbf{b})$  associe  $\mathbf{x} + \mathbf{b}$ , est définie sur  $k$ ); mais alors  $\mathbf{x} + \mathbf{b}$  est un point de  $V$  rationnel sur  $k$ , C.Q.F.D.

**2.2. COROLLAIRE 1** (théorème de Hasse). — *Si  $N$  désigne le nombre de points de  $V$  rationnels sur  $k$ , on a l'inégalité*

$$(2.2.1) \quad |q + 1 - N| \leq 2q^{1/2}.$$

Démonstration. — Soit  $\mathbf{o}$  un point de  $V$  rationnel sur  $k$  (th. 2), et munissons  $V$  de sa structure de variété abélienne définie sur  $k$  et ayant  $\mathbf{o}$  pour élément neutre. Soit  $M$  l'anneau des endomorphismes de  $V$ , et, pour tout  $\lambda \in M$ , soit  $\deg(\lambda)$  le degré de l'application rationnelle  $\lambda$  ([4], pp. 215-216). Soit enfin  $F$  l'endomorphisme  $\mathbf{x} \mapsto \mathbf{x}^{(q)}$  de  $V$ . Alors  $F - 1$  (c'est-à-dire l'endomorphisme  $\mathbf{x} \mapsto \mathbf{x}^{(q)} - \mathbf{x}$  de  $V$ ) est un élément non nul de  $M$  (raisonner comme dans la sect. 2.1), donc une *isogénie* de  $V$  ([4], pp. 215-216) dont le noyau est exactement l'ensemble des points de  $V$  rationnels sur  $k$  (voir sect. 2.1). On peut démontrer que cette isogénie est *non ramifiée* ([4], p. 217), donc que l'ordre du noyau de  $F - 1$  est égal au degré de  $F - 1$ ; ainsi,

$$(2.2.2) \quad N = \deg(F - 1).$$

On peut démontrer également que  $M$  est un  $\mathbf{Z}$ -module libre de rang fini, sans diviseurs de zéro, et qu'il est muni d'un anti-automorphisme  $\lambda \mapsto \lambda'$  tel que  $\lambda\lambda' = \deg(\lambda)$  pour tout  $\lambda \in M$  (voir par exemple Deuring (1941)); il en résulte notamment que, quel que soit  $m \in \mathbf{Z}$ , on a

$$(2.2.3) \quad \deg(F - m.1) = (F - m.1)(F - m.1)' = m^2 - tm + q,$$

avec  $t = F + F' \in \mathbf{Z}$ , et  $q = FF' = \deg(F)$  (puisque  $F(\mathbf{x}) = \mathbf{x}^{(q)}$ ). Etant

donné sa définition, le polynôme  $m^2 - tm + q$  est toujours positif, d'où  $t^2 - 4q \leq 0$ , ou encore

$$(2.2.4) \quad |t| \leq 2q^{1/2}.$$

Mais faisons  $m = 1$  dans (2.2.3) et utilisons (2.2.2); il vient

$$(2.2.5) \quad t = q + 1 - N,$$

et il suffit de porter (2.2.5) dans (2.2.4) pour obtenir l'inégalité (2.2.1).

**2.3.** La démonstration esquissée ci-dessus est essentiellement la démonstration originale de Hasse (voir Hasse (1933, 1934, 1936)). Manin en a donné une version « élémentaire » dont voici le principe (Manin (1956); pour les détails des calculs, voir [6], chap. 10, pp. 197-206). On suppose pour simplifier  $p \neq 2, 3$  (mais cette restriction n'est pas essentielle). Comme  $V$  admet un point rationnel sur  $k$ , on peut supposer  $V$  écrite sous forme normale de Weierstrass

$$(2.3.1) \quad Y^2 = X^3 - aX - b,$$

$a, b \in k$ ,  $4a^3 - 27b^2 \neq 0$ . Soit alors  $\xi$  un élément transcendant sur  $k$ , et soit  $W$  la courbe définie sur  $K = k(\xi)$  et ayant pour équation

$$(2.3.2) \quad Y^2 = \frac{X^3 - aX - b}{\xi^3 - a\xi - b}.$$

C'est une courbe de genre 1, dont on connaît (au moins) deux points rationnels sur  $K$ :  $\mathbf{a}_0 = (\xi^q, \eta^{(q-1)/2})$  (avec  $\eta = \xi^3 - a\xi - b$ ) et  $\mathbf{b} = (\xi, 1)$ . Munissons  $W$  de sa structure de variété abélienne définie sur  $K$ , ayant le point à l'infini  $\mathbf{o}$  pour élément neutre, et pour laquelle trois points ont une somme nulle si, et seulement si, ils sont alignés ([4], pp. 211-214); pour tout  $m \in \mathbf{Z}$ , posons  $\mathbf{a}_m = \mathbf{a}_0 - m \cdot \mathbf{b}$ , puis définissons un entier  $d_m$  de la façon suivante: si  $\mathbf{a}_m = \mathbf{o}$ , posons  $d_m = 0$ ; si au contraire  $\mathbf{a}_m \neq \mathbf{o}$ , donc si le point  $\mathbf{a}_m$  est « à distance finie », de coordonnées affines  $x_m, y_m$ , avec  $x_m = P_m(\xi)/Q_m(\xi)$  et  $P_m, Q_m$  premiers entre eux, posons  $d_m = \deg(P_m)$ . On peut alors démontrer (à l'aide des formules d'addition sur une cubique de Weierstrass: voir [4], p. 214) les deux relations suivantes:

$$d_{-1} - d_0 = N - q; \quad d_{m-1} + d_{m+1} = 2d_m + 2;$$

ces deux formules permettent de calculer  $d_m$ :

$$(2.3.3) \quad d_m = m^2 - (q + 1 - N)m + q;$$

comme par définition  $d_m \geq 0$ , le polynôme en  $m$  figurant au second membre de (2.3.3) est positif; d'où

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

ce qui implique bien l'inégalité (2.2.1).

La parenté entre ces deux démonstrations tient au fait que  $d_m = \deg(F - m.1)$ .

**2.4.** On a vu au chapitre 6 (sect. 3.3, (1) et 3.5) que la courbe *affine*  $Y^2 = 1 - X^3$  (qui est de genre 1 pour  $p \neq 2, 3$ ) a un nombre de points rationnels sur  $k$  égal à  $q$  si  $q \equiv -1 \pmod{6}$  et à  $q + \alpha + \bar{\alpha}$  (avec  $\alpha = \pi(\varphi, \chi)$ ) si  $q \equiv 1 \pmod{6}$ . Si on remarque que cette courbe, considérée maintenant comme *projective*, admet *un* point à l'infini rationnel sur  $k$ , on voit que le nombre total  $N$  de ses points rationnels sur  $k$  satisfait à  $|q + 1 - N| = 0$  dans le premier cas, et à  $|q + 1 - N| \leq |\alpha| + |\bar{\alpha}| = 2q^{1/2}$  dans le second cas (voir chap. 5, prop. 9, cor. 1): le théorème de Hasse se trouve ainsi vérifié directement pour cette courbe.

Raisonnement analogue pour la courbe  $Y^2 = X - X^3$ , qui admet *un* point à l'infini rationnel sur  $k$ , et pour la courbe  $Y^3 = 1 - X^3$ , qui admet un ou trois points à l'infini rationnels sur  $k$  selon que  $q$  est congru à  $-1$  ou à  $1 \pmod{3}$  (on suppose naturellement  $p \neq 3$ ).

Considérons enfin la courbe *affine*  $Y^2 = 1 - X^4$  (qui est de genre 1 pour  $p \neq 2$ ) et dont le nombre de points rationnels sur  $k$  est égal à  $q + 1$  si  $q \equiv -1 \pmod{4}$  et à  $q - 1 + \alpha + \bar{\alpha}$  (avec  $\alpha = \pi(\varphi, \chi)$ ): chap. 6, sect. 3.3, (2), et 3.5) si  $q \equiv 1 \pmod{4}$ . Dans le premier cas, cette courbe, envisagée maintenant comme *projective*, admet à l'infini *un point double* rationnel sur  $k$ , mais ce point est « isolé » (par désingularisation, il donnerait deux points conjugués sur  $k$ , mais non rationnels sur  $k$ ): ce point ne doit donc pas être pris en considération; on a donc ici  $N = q + 1$ , ou  $|q + 1 - N| = 0$ . Dans le second cas, la courbe admet encore un point double à l'infini, rationnel sur  $k$ , mais « non isolé » (par désingularisation, il donnerait deux points rationnels sur  $k$ ): ce point doit donc être compté deux fois, d'où maintenant  $N = q + 1 + \alpha + \bar{\alpha}$ , donc, comme précédemment,  $|q + 1 - N| \leq 2q^{1/2}$ : le théorème de Hasse se trouve également vérifié directement pour cette courbe \*).

\*) En fait, on a raisonné ici, non sur la courbe  $Y^2 = 1 - X^4$ , mais sur sa *normalisée* (voir d'ailleurs chap. 9, sect. 5.2, (2) et (4)).