

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

Artikel: ÉQUATIONS ET VARIÉTÉS ALGÈBRIQUES SUR UN CORPS FINI
Kapitel: §4. Variétés de dimension 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: 09.11.2024

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

$q - 3 + \alpha_1 + \dots + \alpha_6$. 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

qu'on appelle *degré de V* le nombre de points d'intersection de V avec une sous-variété linéaire de \mathbf{P}_n de dimension $n - r$ « en position générique » (voir [15], chap. I, § 8.4); une variété projective plongée dans \mathbf{P}_n , de degré d et de dimension r sera dite « de type (n, d, r) ».

Cela étant, on a le théorème suivant, dû à Lang et Weil (1954) (voir aussi Nisnevich (1954): Nisnevich se limite au cas où le corps de base k est le corps premier \mathbf{F}_p):

THÉORÈME 4. — *Si V est une variété projective de type (n, d, r) définie sur k , et si $N = N_V$ désigne le nombre de points de V rationnels sur k , on a*

$$(4.1.1) \quad |N - q^r| \leq B(d) q^{r-(1/2)} + A(n, d, r) q^{r-1},$$

$A(n, d, r)$ désignant une constante qui ne dépend que de n, d et r , et $B(d)$ désignant une constante qui ne dépend que de d (et qu'on peut prendre égale à $(d-1)(d-2)$).

Démonstration. — On raisonne par double récurrence, d'abord sur n , puis sur r . Si $n = 0$, on a $N \leq d$, et le théorème est évident; supposons donc $n \geq 1$: si V est contenue dans un hyperplan de \mathbf{P}_n défini sur k , V peut être considérée comme de type $(n-1, d, r)$, et l'hypothèse de récurrence sur n permet d'écrire $|N - q^r| \leq B(d) q^{r-(1/2)} + A(n-1, d, r) q^{r-1}$: le théorème est également établi. Ainsi, on peut désormais supposer n fixé (≥ 1), faire l'hypothèse suivante:

(H) V n'est contenue dans aucun hyperplan de \mathbf{P}_n défini sur k ,

et raisonner par récurrence sur r . Pour $r = 0$, on a $N \leq d$, et le théorème est évident. Supposons maintenant $r = 1$; V est alors une courbe projective, éventuellement singulière: soit V_1 une courbe projective *non singulière* définie sur k et birationnellement équivalente à V sur k (via une équivalence birationnelle $\varphi: V_1 \rightarrow V$), et soit N_1 le nombre de points de V_1 rationnels sur k ; le théorème 3 montre que $|q + 1 - N_1| \leq 2gq^{1/2}$, g désignant le genre de V_1 , donc de V ; mais le genre de V et le nombre de points singuliers de V sont tous deux majorés par $(d-1)(d-2)/2$ (projeter V sur un plan, ce qui ne modifie ni g , ni d , et ne peut qu'augmenter le nombre de points singuliers; puis appliquer la formule de Plücker à cette projection); d'autre part, la correspondance birationnelle $\varphi: V_1 \rightarrow V$ est bijective en dehors des points singuliers de V (et fait correspondre, à des points rationnels sur k , des points rationnels sur k , puisqu'elle est définie sur k), et elle associe, à chaque point

singulier de V , au plus d points de V_1 ; ainsi, $|N - N_1| \leq d(d-1)(d-2)/2$, et finalement $|N - q| \leq B(d)q^{1/2} + A(n, d, 1)$, avec $B(d) = 2g \leq (d-1)(d-2)$ et $A(n, d, 1) = d(d-1)(d-2)/2 + 1$: le théorème est établi pour les variétés de type $(n, d, 1)$.

Supposons alors $r \geq 2$, et le théorème démontré jusqu'à la dimension $r - 1$. Soit \mathbf{P}'_n un second exemplaire de l'espace projectif \mathbf{P}_n sur k ; à tout point $\mathbf{w} = (w_0, \dots, w_n)$ de \mathbf{P}'_n , associons l'hyperplan $H_{\mathbf{w}}$ de \mathbf{P}_n d'équation $w_0X_0 + \dots + w_nX_n = 0$; les hyperplans $H_{\mathbf{w}}$ définis sur k correspondent bijectivement aux points \mathbf{w} de \mathbf{P}'_n rationnels sur k , et il y en a exactement

$$Q_n = (q^{n+1} - 1)/(q - 1) = q^n + \dots + q + 1.$$

Calculons de deux manières différentes le nombre C des couples $(\mathbf{x}, H_{\mathbf{w}})$, où \mathbf{x} est un point de V rationnel sur k , et où \mathbf{w} est un point de \mathbf{P}'_n rationnel sur k et tel que \mathbf{x} appartienne à $H_{\mathbf{w}}$:

(1) V_k contient par définition N points, et par chacun d'eux passent Q_{n-1} hyperplans définis sur k : d'où $C = NQ_{n-1}$;

(2) pour chaque hyperplan $H_{\mathbf{w}}$ défini sur k , le cycle intersection $V \cdot H_{\mathbf{w}}$ (voir [15], chap. II, § 6.1) est, en un sens évident, de type $(n, d, r - 1)$, en vertu de l'hypothèse (H); notons $N_{\mathbf{w}}$ le nombre de points de $V \cdot H_{\mathbf{w}}$ (c'est-à-dire de $V \cap H_{\mathbf{w}}$) rationnels sur k ; on a alors évidemment $C = \sum_{\mathbf{w}} N_{\mathbf{w}}$, \mathbf{w}

parcourant l'ensemble des Q_n points de \mathbf{P}'_n rationnels sur k .

Le rapprochement des résultats de ces deux calculs donne $NQ_{n-1} = \sum_{\mathbf{w}} N_{\mathbf{w}}$,

ou encore

$$(4.1.2) \quad N = Q_{n-1}^{-1} \sum_{\mathbf{w} \in I} N_{\mathbf{w}} + Q_{n-1}^{-1} \sum_{\mathbf{w} \in R} N_{\mathbf{w}},$$

I (resp. R) désignant l'ensemble des points $\mathbf{w} \in \mathbf{P}'_n$ rationnels sur k et tels que le cycle $V \cdot H_{\mathbf{w}}$ soit (resp. ne soit pas) une variété. On posera $N_I = \text{card}(I)$ et $N_R = \text{card}(R)$; il est clair que $N_I + N_R = Q_n$.

On a alors ces deux lemmes:

LEMME 1. — *Il existe une constante $A_1(n, d, r)$ ne dépendant que de n, d et r et ayant la propriété suivante: quel que soit Z , cycle positif de type (n, d, r) rationnel sur k , on a*

$$(4.1.3) \quad N_Z \leq A_1(n, d, r) q^r,$$

N_Z désignant le nombre de points de Z rationnels sur k (un point de Z est un point de la réunion des composantes de Z).

LEMME 2. — *Il existe une constante $A_2(n, d, r)$ ne dépendant que de n, d et r et possédant la propriété suivante : quelle que soit V , variété de type (n, d, r) définie sur k et vérifiant (H), le nombre N_R défini ci-dessus satisfait à*

$$(4.1.4) \quad N_R \leq A_2(n, d, r) q^{n-1}.$$

Le lemme 1 est élémentaire; il se démontre par récurrence sur r , en coupant Z par les éléments rationnels sur k d'un faisceau d'hyperplans convenablement choisi dans \mathbf{P}_n . Le lemme 2 est plus technique; on le déduit du lemme 1 en construisant, grâce à la théorie de la *forme de Chow* (à ce sujet, voir par exemple [15], chap. I, § 9.4), un ensemble algébrique E défini sur k , de type $(n, e, n-1)$, plongé dans \mathbf{P}'_n , dont le degré $e = e(n, d, r)$ ne dépend que de n, d et r , et qui contient l'ensemble R ; comme les points de R sont tous rationnels sur k , on a donc $N_R \leq N_E \leq A_1(n, e, n-1) q^{n-1}$, et la constante du lemme 2 est donnée par

$$A_2(n, d, r) = A_1(n, e(n, d, r), n-1).$$

(L'ensemble algébrique E dépend de V ; pour une démonstration détaillée de ces deux lemmes, voir Lang-Weil (1954), pp. 820-821).

Achevons alors la démonstration du théorème 4. Dans le membre de droite de (4.1.2), chaque terme N_w de la première somme est le nombre de points rationnels sur k de $V \cdot H_w$, qui est une *variété* de type $(n, d, r-1)$ définie sur k , puisque $w \in I$; par hypothèse de récurrence (sur r), on a donc

$$|N_w - q^{r-1}| \leq B(d) q^{r-(3/2)} + A(n, d, r-1) q^{r-2}.$$

D'autre part, le nombre de termes de cette première somme est $Q_n - N_R$; les valeurs de Q_{n-1} et Q_n sont connues, et celle de N_R est majorée par $A_2(n, d, r)$ (lemme 2); un calcul facile montre alors que

$$(4.1.5) \quad |Q_{n-1}^{-1} \sum_{w \in I} N_w - q^r - B(d) q^{r-(1/2)}| \leq A_3(n, d, r) q^{r-1},$$

$A_3(n, d, r)$ étant une constante qui ne dépend que de n, d et r . Considérons maintenant la seconde somme figurant dans le membre de droite de (4.1.2); chacun des termes N_w qui y apparaissent est le nombre de points rationnels sur k d'un cycle, $V \cdot H_w$, positif, rationnel sur k , et de type $(n, d, r-1)$; le lemme 1 donne donc $N_w \leq A_1(n, d, r-1) q^{r-1}$; comme cette seconde somme comporte N_R termes, le lemme 2 montre qu'elle est majorée par $A_4(n, d, r) q^{n+r-2}$, avec $A_4(n, d, r) = A_1(n, d, r-1) A_2(n, d, r) =$ une constante qui ne dépend que de n, d et r . Mais $Q_{n-1} = q^{n-1} + \dots + q + 1$; ainsi, $Q_{n-1}^{-1} \leq q^{1-n}$, et on arrive à la majoration

$$(4.1.6) \quad \left| Q_{n-1}^{-1} \sum_{w \in R} N_w \right| \leq A_4(n, d, r) q^{r-1}.$$

Il suffit alors de porter les inégalités (4.1.5) et (4.1.6) dans la formule (4.1.2) et de poser $A(n, d, r) = A_3(n, d, r) + A_4(n, d, r)$ pour obtenir l'inégalité (4.1.1). Le théorème 4 se trouve ainsi établi.

4.2. Le théorème 4 admet la conséquence suivante, qui généralise le corollaire 1 du théorème 3, et se démontre de la même manière:

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, $N_m \geq 1$.

La propriété « $N_m \geq 1$ pour tout m assez grand », c'est-à-dire « V admet un point rationnel sur toute extension algébrique de k de degré assez grand », est évidemment fausse en général sur un corps de base quelconque. Ainsi, l'hyperquadrique projective $X_0^2 + \dots + X_n^2 = 0$, définie sur le corps \mathbf{Q} , n'admet de point rationnel sur aucune extension de \mathbf{Q} de degré *impair* m , si grand que soit m ; en effet, \mathbf{Q} est un corps formellement réel ([10], chap. XI, § 2); si K/\mathbf{Q} est de degré impair, K est alors lui-même formellement réel (*ibid.*, prop. 2, (ii)), et une égalité $x_0^2 + \dots + x_n^2$ avec $x_0, \dots, x_n \in K$ n'est possible que si $x_0 = \dots = x_n = 0$. Un argument de ramification montrerait de même que la variété $X_0^{n+1} + pX_1^{n+1} + \dots + p^nX_n^{n+1} = 0$, définie sur le corps \mathbf{Q}_p des nombres rationnels p -adiques, n'admet de point rationnel sur aucune extension de \mathbf{Q}_p de degré m non divisible par $n + 1$, si grand que soit m .

Cette propriété « $N_m \geq 1$ pour tout m assez grand » est également fausse en général, même sur un corps de base fini, si on ne suppose pas V absolument irréductible. Ainsi, considérons le polynôme P défini par (4.1.1) (chap. 4, § 4), et supposons $n \geq 2$; l'équation $P(X_0, \dots, X_{n-1}) = 0$ définit alors une k -variété projective V (de type $(n-1, n, n-2)$), mais cette k -variété n'est pas absolument irréductible, donc n'est pas une variété (elle se décompose en n hyperplans définis sur $K = k_n$ et conjugués sur k); et il est facile de vérifier que si m est premier avec n , le nombre N_m de points de V rationnels sur k_m est nul, si grand que soit m (noter que si $(m, n) = 1$, k_m et k_n sont linéairement disjoints sur k (chap. 1, prop. 4, cor. 2); $\omega_1, \dots, \omega_n$ est alors une base de k_{mn} sur k_m , et on peut raisonner comme au chapitre 4, section 4.1, en remplaçant k par k_m et $K = k_n$ par k_{mn}).

4.3. Remarquons enfin que le théorème 4 reste vrai pour des variétés affines, moyennant une modification de la constante $A(n, d, r)$. Soit en effet

$V \subset \mathbf{A}_n$ une variété affine de type (n, d, r) ; plongeons \mathbf{A}_n dans \mathbf{P}_n de manière que l'hyperplan « à l'infini » H_0 ait pour équation (par exemple) $X_0 = 0$; adjoignons alors à V ses points « à l'infini » de la façon habituelle, et notons W la variété projective ainsi obtenue; elle est de type (n, d, r) , et on a, avec des notations évidentes, $N_V = N_W - N_{W.H_0}$; il suffit dans ces conditions d'appliquer le théorème 4 à N_W et le lemme 1 à $N_{W.H_0}$ pour obtenir

$$(4.3.1) \quad |N_V - q^r| \leq B(d) q^{r-(1/2)} + A'(n, d, r) q^{r-1},$$

avec $A'(n, d, r) = A(n, d, r) + A_1(n, d, r) =$ une constante qui ne dépend que de n, d et r .

Notes sur le chapitre 8

§ 2: le théorème 2 est dû à Schmidt (1931) (méthode analytique); ce théorème est un aspect d'un résultat général relatif aux espaces homogènes principaux sur un corps de base fini (Lang (1956); voir aussi Serre, *Groupes algébriques et corps de classes*, p. 119 (Hermann, 1959)). L'application $\mathbf{x} \mapsto \mathbf{x}^{(a)}$ utilisée dans la démonstration du théorème 2 est souvent dite « endomorphisme de Frobenius » (voir d'ailleurs chap. 1, prop. 8); le fait que les points fixes de cet endomorphisme sont exactement les points rationnels sur $k = \mathbf{F}_q$ est un trait caractéristique de la « géométrie diophantienne » sur un corps fini.

Un certain nombre de cas particuliers du théorème de Hasse avaient déjà été remarqués au cours du XIX^e siècle; citons notamment la « dernière inscription du journal de Gauss » (« letzte Eintragung im Gauss'schen Tagebuch », reproduite dans *Deuring* (1941), pp. 197-198), relative au nombre de solutions de la congruence $X^2 Y^2 + X^2 + Y^2 - 1 \equiv 0 \pmod{p}$, pour $p \equiv 1 \pmod{4}$ (à ce sujet, voir également [5], p. 307, et [4], p. 242, note 3). Pour la démonstration originale du théorème de Hasse, voir Hasse (1933, 1934, 1936).

Les courbes (projectives, non singulières) de genre 1 sur un corps fini k ne sont autres (d'après le théorème de Schmidt) que les variétés abéliennes de dimension 1 définies sur k ; les variétés abéliennes de dimension quelconque définies sur un corps fini ont été étudiées notamment par Honda, Milne, Serre, Tate, Waterhouse: pour une bibliographie sur ce sujet, voir Waterhouse (1969).

§ 3: le théorème 3, annoncé par Weil en 1940, est démontré dans Weil (1948) (= [20], 1^{ère} partie) par voie « géométrique »: c'est cette démonstration qu'on a résumée ici; pour des démonstrations « arithmétiques »,