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

Artikel: ÉQUATIONS ET VARIÉTÉS ALGÉBRIQUES SUR UN CORPS FINI
Autor: Joly, Jean-René
Kapitel: §3. « Exemplis gaudeamus ».
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: 10.07.2025

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

§ 3. « *Exemplis gaudeamus* ».

A titre d'application des théorèmes 1 et 2, on va calculer dans ce paragraphe le nombre de solutions de certains types simples (et classiques) d'équations diagonales.

3.1. On s'intéresse d'abord aux équations de la forme

$$a_1X_1^2 + \dots + a_nX_n^2 = b\,;$$

on peut se limiter au cas où p est impair; $q = p^f$ est alors impair, et on a $\delta_i = 2$ pour $i = 1, \dots, n$; l'ensemble J des paragraphes 1 et 2 est formé du seul élément $\mathbf{j} = (1, \dots, 1)$; enfin, les caractères $\chi_i = \theta^{(q-1)/\delta_i}$ sont tous égaux à l'unique caractère d'ordre 2 de k^*, c'est-à-dire au caractère de Legendre de k, qu'on notera φ (voir chap. 5, sect. 1.5).

(1) Supposons d'abord *n impair*. Si $b = 0$, on utilise le corollaire 1 du théorème 1, en remarquant que I est vide: on a donc $N = q^{n-1}$. Si $b \neq 0$, on utilise le théorème 2, qui donne ici

$$N(b) = q^{n-1} + \varphi(b^{-n}a_1 \dots a_n)\,\pi(\varphi, \dots, \varphi)\,; \tag{3.1.1}$$

comme $\varphi^n = \varphi \neq \varepsilon$ et que $\bar{\varphi} = \varphi$, on a $\pi(\varphi, \dots, \varphi) = \tau(\varphi)^{n-1}$ et $\tau(\varphi)^2 = q\varphi(-1)$ (chap. 5, prop. 10, (ii) et prop. 7); ainsi,

$$\pi(\varphi, \dots, \varphi) = \big(q\varphi(-1)\big)^{(n-1)/2}\,; \tag{3.1.2}$$

le rapprochement de (3.1.1) et (3.1.2), et le fait que φ vaut 1 sur les carrés et -1 sur les non carrés de k^*, permettent alors de conclure:

PROPOSITION 1. — *Pour n impair (et $p \neq 2$), le nombre N de solutions dans k^n de l'équation $a_1X_1^2 + \dots + a_nX_n^2 = b$ (où les a_i sont supposés tous différents de 0) est donné par les formules suivantes :*

(i) *Si* $b = 0, N = q^{n-1}$.

(ii) *Si* $b \neq 0, N = \begin{cases} q^{n-1} + q^{(n-1)/2}, & si\ (-1)^{(n-1)/2}a_1 \dots a_nb \in k^{*2}, \\ q^{n-1} - q^{(n-1)/2}, & si\ (-1)^{(n-1)/2}a_1 \dots a_nb \notin k^{*2}. \end{cases}$

(2) Supposons maintenant *n pair*. Si $b = 0$, on utilise le théorème 1, en remarquant que $I = J$; on trouve

$$N = q^{n-1} + q^{-1}(q-1)\,\varphi(a_1 \dots a_n)\,\tau(\varphi)^n\,;$$

mais $\tau(\varphi)^n = \big(\tau(\varphi)^2\big)^{n/2} = \big(q\varphi(-1)\big)^{n/2}$; ainsi

(3.1.3) $$N = q^{n-1} + q^{-1}(q-1)\varphi((-1)^{n/2}a_1 \dots a_n)\, q^{n/2}.$$

Si $b \neq 0$, on utilise le théorème 2, en remarquant que

$$\pi(\varphi, \dots, \varphi) = -\varphi(-1)\tau(\varphi)^{n-2} = -\varphi(-1)(q\varphi(-1))^{(n-2)/2}$$

(chap. 5, prop. 10, (i) puis (ii), et prop. 7; noter que $\varphi^n = \varepsilon$). Au total:

PROPOSITION 2. — *Pour n pair (et $p \neq 2$), N est donné par les formules suivantes :*

(i) $$\text{Si } b = 0, N = \begin{cases} q^{n-1} + q^{n/2} - q^{(n/2)-1}, & \text{si } (-1)^{n/2}a_1 \dots a_n \in k^{*2}, \\ q^{n-1} - q^{n/2} + q^{(n/2)-1}, & \text{si } (-1)^{n/2}a_1 \dots a_n \notin k^{*2}; \end{cases}$$

(ii) $$\text{Si } b \neq 0, N = \begin{cases} q^{n-1} - q^{(n/2)-1}, & \text{si } (-1)^{n/2}a_1 \dots a_n \in k^{*2}, \\ q^{n-1} + q^{(n/2)-1}, & \text{si } (-1)^{n/2}a_1 \dots a_n \notin k^{*2}. \end{cases}$$

On retrouve ainsi, et de manière plus naturelle, les résultats du chapitre 5, section 4.3, (3) et (4).

3.2. On s'intéresse maintenant aux équations de la forme $a_1X_1^{d_1} + a_2X_2^{d_2} = b$, avec a_1, a_2 et $b \neq 0$. Pour simplifier, on écrira X, Y au lieu de X_1, X_2, et on se limitera au cas où $a_1 = a_2 = b = 1$; on supposera d'autre part $q - 1$ divisible par d_1 et d_2 (on a toujours le droit de le faire: voir chap. 4, sect. 1.3 et 3.1). Si alors on note χ_1 et χ_2 des caractères multiplicatifs d'ordre d_1 et d_2 de k, et si J désigne l'ensemble des couples d'entiers (j_1, j_2) tels que $1 \leqslant j_1 \leqslant d_1 - 1$, $1 \leqslant j_2 \leqslant d_2 - 1$, le théorème 2 permet d'énoncer:

PROPOSITION 3. — *Le nombre N de solutions sur k de l'équation $X^{d_1} + Y^{d_2} = 1$ est donné par*

(3.2.1) $$N = q + \sum_{j \in J} \pi(\chi_1^{j_1}, \chi_2^{j_2}).$$

3.3. La proposition 3 permet notamment de calculer le nombre de points rationnels sur k de certaines courbes de genre 1 [1]).

(1) *La courbe* $Y^2 = 1 - X^3$ (*avec* $q \equiv 1 \pmod 6$). Si φ désigne le caractère de Legendre et si χ est un caractère d'ordre 3 de k^* (donc tel que $\chi^2 = \bar{\chi}$), (3.2.1) donne

(3.3.1) $$N_1 = q + \pi(\varphi, \chi) + \pi(\varphi, \bar{\chi}).$$

[1]) Les exemples ci-dessous resserviront aux chapitres 8 et 9.

(2) *La courbe* $Y^2 = 1 - X^4$ (*avec* $q \equiv 1 \pmod 4$). Si φ désigne toujours le caractère de Legendre, et si ψ est un caractère d'ordre 4 de k^* (donc tel que $\psi^2 = \varphi$ et $\psi^3 = \bar{\psi}$), (3.2.1) donne

$$N_2 = q - 1 + \pi(\varphi, \psi) + \pi(\varphi, \bar{\psi}). \tag{3.3.2}$$

(Se rappeler que $\pi(\varphi, \varphi) = -\varphi(-1)$, et noter que $\varphi(-1) = 1$, puisque $q \equiv 1 \pmod 4$, et que -1 est donc un carré dans k).

(3) *La courbe* $Y^3 = 1 - X^3$ (*avec* $q \equiv 1 \pmod 3$). Si χ désigne un caractère d'ordre 3 de k^* (donc tel que $\chi^2 = \bar{\chi}$), (3.2.1) donne

$$N_3 = q - 2 + \pi(\chi, \chi) + \pi(\bar{\chi}, \bar{\chi}). \tag{3.3.3}$$

(Noter que $\pi(\chi, \bar{\chi}) = \pi(\bar{\chi}, \chi) = -\chi(-1)$: chap. 5, prop. 9, (i); et remarquer que $\chi(-1) = 1$, puisque $-1 = (-1)^3$).

3.4. Considérons maintenant *la courbe* V_4 *d'équation* $Y^2 = X - X^3$; elle est également de genre 1 (on suppose pour simplifier $q \equiv 1 \pmod 4$); l'équation, en revanche, n'est plus diagonale: on peut toutefois, grâce à (3.3.2), calculer le nombre N_4 de points de C_4 rationnels sur k; en fait (et avec les notations de la section 3.3, (2)):

$$N_4 = q + \pi(\varphi, \psi) + \pi(\varphi, \bar{\psi}). \tag{3.4.1}$$

Un procédé de démonstration est le suivant (on laisse au lecteur le soin de régler les détails); tout d'abord, la congruence $q \equiv 1 \pmod 4$ entraîne que -1 est un carré dans k, et que -4 est une puissance 4-ième dans k: pour vérifier ce dernier point, appliquer les « lois complémentaires »

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

([**17**], p. 15), et se rappeler que $q = p^f$; soient donc a et i deux éléments de k tels que $i^2 = -1$, $a^4 = -4$, et $a^2 = 2i$. Soient d'autre part V_2, V_2' et V_4' les courbes d'équations respectives $Y^2 = 1 - X^4$, $Y^2 = a^4 - X^4$ et $2a^2 Y^2 = X + X^3$, et soient N_2, N_2' et N_4' leurs nombres de points rationnels sur k (toutes ces courbes sont considérées comme *affines*). Il est clair que $N_2 = N_2'$, et comme $2a^2 = 4i$, on voit également sans peine que $N_4 = N_4'$: compte tenu de (3.3.2), il suffit alors de prouver que $N_4' = N_2' + 1$, ce qui se déduit facilement de l'existence d'une application birationnelle $\lambda: V_2' \to V_4'$, définie par

$$\lambda(x, y) = \left(x^2/(y + a^2),\ x/(y + a^2)\right).$$

La relation (3.4.1) (c'est-à-dire l'égalité $N_4 = N_2 + 1$) peut aussi se démontrer en appliquant aux deux polynômes $P_2(X) = 1 - X^4$ et $P_4(X) = X - X^3$ le lemme suivant (qui se prouve sans difficulté):

LEMME 1. — *(On suppose $p \neq 2$). Soit $P(X)$ un polynôme à une variable X et à coefficients dans k. Si φ désigne le caractère de Legendre de k, le nombre N_P de solutions sur k de l'équation $Y^2 = P(X)$ est donné par*

$$N_P = q + \sum_{x \in k} \varphi(P(x)). \tag{3.4.2}$$

Au sujet de cette seconde méthode, voir Morlaye (1972).

3.5. Dans la section 3.3, on a supposé q congru à 1 modulo 6 (ou modulo 4, ou modulo 3) pour pouvoir calculer N_1, N_2 et N_3 par application directe de la proposition 3. On laisse au lecteur le soin de vérifier (ce qui est immédiat) les assertions suivantes:

si $q \equiv -1 \pmod 6$, *on a* $N_1 = q$; *si* $q \equiv -1 \pmod 4$, *on a* $N_2 = q + 1$; *si* $q \equiv -1 \pmod 3$, *on a* $N_3 = q$; *enfin, si* $q \equiv -1 \pmod 4$, *on a* $N_4 = q$.

Notes sur le chapitre 6

§ **1-2**: le lien entre nombre de solutions d'une congruence diagonale modulo p et sommes de Gauss et de Jacobi avait déjà été remarqué par Gauss et Jacobi eux-mêmes, notamment pour les congruences $aX^3 - bY^3 \equiv 1 \pmod p$, $aX^4 - bY^4 \equiv 1 \pmod p$, $Y^2 \equiv aX^4 - b \pmod p$; à ce sujet, voir Weil (1949), pp. 497-498. La congruence $X^n + Y^n + 1 \equiv 0 \pmod p$ a été étudiée par Libri (1832) pour $n = 3, 4$, puis, beaucoup plus tard, par Pellet, Jacobsthal, ainsi que Dickson (1909), Hurwitz (1909), Schur (1916), Mordell (1922), etc., pour n quelconque, en relation avec le théorème de Fermat. La congruence $X_1^k + \ldots + X_s^k \equiv m \pmod p$ a été étudiée notamment par Hardy-Littlewood (1922) dans leurs travaux sur le problème de Waring. Le théorème 2, pour deux variables, est dû à Davenport-Hasse (1934), et, indépendamment, à Hua-Vandiver (1949, a; b) et Weil (1949) pour un nombre de variables quelconque.

§ **3**: les propositions 1 et 2 (pour $q = p$) figurent déjà dans Lebesgue (1837), où elles sont d'ailleurs démontrées d'une autre manière. La proposition 3 et les exemples de la section 3.3 sont empruntés à Davenport-Hasse (1934). Le lien entre nombre de solutions de $Y^2 = X - X^3$ et de $Y^2 = 1 - X^4$ semble avoir été remarqué (incidemment) pour la première fois par