

Notes sur le chapitre 7

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **19 (1973)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **11.07.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

théorèmes 2 et 3 et telle que N soit égal exactement à q^{b_1} . Pour la construction d'une telle famille de polynômes, et pour la démonstration du théorème 3, voir Katz (1971) (respectivement § 4 et § 3); voir également les Notes en fin de chapitre.

3.3. Pour des équations *de forme particulière*, le théorème 1 peut dans certains cas être amélioré. Ainsi, en combinant le théorème 1 du chapitre 6 avec les « relations de Stickelberger » (prop. 1), on obtient sans difficulté le résultat suivant:

THÉORÈME 4. — Soit $F = a_1 X_1^{d_1} + \dots + a_n X_n^{d_n}$ un polynôme diagonal à coefficients dans le corps premier $k = \mathbb{F}_p$. Pour $i = 1, \dots, n$, posons $\delta_i = (p-1, d_i)$, et soit b_2 le plus grand entier strictement inférieur à $1/\delta_1 + \dots + 1/\delta_n$. Alors, si $a \in k$, et si N désigne le nombre de solutions dans k^n de l'équation $F = a$, N est divisible par p^{b_2} .

Ce résultat reste d'ailleurs vrai sur un corps fini quelconque k à $q = p^f$ éléments, à condition de supposer que chaque $\delta_i = (q-1, d_i)$ divise $p-1$: N est alors divisible par q^{b_2} ; cet exposant b_2 peut encore être « amélioré » si $a = 0$ (voir Joly (1971)). On notera l'analogie entre le théorème 4 ci-dessus et le théorème 3 du chapitre 4.

Notes sur le chapitre 7

§ 1: la démonstration de la proposition 1 donnée ici est due à Hilbert (« Zahlbericht »); cette proposition est en fait une conséquence d'un résultat plus précis (« congruences de Stickelberger »):

$$\tau(j) \equiv -\lambda^{\sigma(j)}/\rho(j) \pmod{\mathfrak{P}^{\sigma(j)+1}}$$

(avec par définition $\rho(j) = j_0! j_1! \dots j_{f-1}!$); voir Stickelberger (1890), Davenport-Hasse (1934), ou [11], chap. IV, § 3. Pour une interprétation analytique p -adique de ces congruences, voir Dwork (1960).

§ 2-3: dans Ax (1964), le cadre de la démonstration du théorème 1 est, non pas le corps de nombres $L = \mathbb{Q}(\omega, \zeta)$, mais le corps $\mathbb{Q}_p(\omega, \zeta)$ des racines $p(q-1)$ -ièmes de l'unité dans une clôture algébrique du corps p -adique \mathbb{Q}_p (avec les notations du § 1, ce corps $\mathbb{Q}_p(\omega, \zeta)$ est d'ailleurs isomorphe à $L\mathfrak{P}$, complété \mathfrak{P} -adique de L); à cette différence près, la démonstration donnée ici est exactement celle d'Ax; elle est (selon Ax lui-même) « suggérée par certaines idées de Dwork [dans sa démonstration

de la rationalité des fonctions zêta des variétés algébriques] » (à ce sujet, voir chap. 9, § 2). La démonstration du théorème 3 donnée par Katz (1971) utilise également (et directement) les méthodes analytiques p -adiques de Dwork.

CHAPITRE 8

« HYPOTHÈSE DE RIEMANN »

Soient k un corps fini à q éléments, n un entier ≥ 1 , F un polynôme à n variables et à coefficients dans k , et N le nombre de solutions dans k^n de l'équation $F = 0$. On a remarqué aux chapitres 4 (sect. 4.2, th. 6, cor. 1) et 6 (sect. 1.2, th. 1, cor. 1, 2, 3; sect. 2.1, th. 2, cor. 1, 2) que, lorsque F est *multilinéaire* ou *diagonal* (et qu'il satisfait en outre à certaines hypothèses qui équivalent à supposer qu'il est absolument irréductible), alors N est de l'ordre de grandeur de q^{n-1} , l'exposant $n - 1$ s'interprétant d'ailleurs comme dimension de l'hypersurface affine $F = 0$. Le but du présent chapitre est d'étendre ce résultat à n'importe quel ensemble algébrique, affine ou projectif, *absolument irréductible*, défini sur k — autrement dit, à n'importe quelle *variété* définie sur k ; si V est une telle variété, et si N désigne maintenant le nombre de points de V rationnels sur k , on a en fait (§ 4, th. 4)

$$N = q^r + O(q^{r-(1/2)}),$$

q étant considéré comme « infiniment grand », et la constante impliquée par le symbole O ne dépendant que de $r = \dim(V)$, du degré de V , et de la dimension de l'espace affine ou projectif où V se trouve plongée.

Le théorème 4 (pour r quelconque) se déduit par récurrence sur r du cas particulier où $r = 1$, et où V est donc une *courbe*: ce cas est examiné en détail aux paragraphes 1 (courbes de genre 0), 2 (courbes de genre 1) et 3 (courbes de genre quelconque). Le résultat central de ce chapitre est d'ailleurs le théorème 3 (§ 3), dit « hypothèse de Riemann » pour la courbe V : on verra en effet (chap. 9, sect. 3.2) que ce théorème est équivalent au résultat suivant: tous les zéros de la fonction $\zeta(V; s)$ ont une partie réelle égale à $1/2$.

Le langage géométrique utilisé dans ce chapitre (et dans le suivant) est essentiellement celui des Foundations de Weil, c'est-à-dire le langage « classique » (à une différence près: si V est un ensemble algébrique défini sur k , on identifie V à l'ensemble de ses points algébriques sur k ; il en résulte