

# Notes sur le chapitre 6

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **23.09.2024**

## **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.

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  $\varphi$  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

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

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  $X_1^k + \dots + X_s^k \equiv m \pmod{p}$  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

Jacobsthal (1907). Pour  $q = p \equiv 1 \pmod{4}$ , la formule (3.4.1) peut, avec les notations de l'appendice du chapitre 5 (sect. A.1, exemple 2) et compte de la proposition 12 (*ibid.*), s'écrire  $N_4 = p - \lambda - \bar{\lambda}$ . Plus généralement, si  $D \in \mathbf{Z}$ , et si  $N_4(D)$  désigne le nombre de solutions de la congruence  $Y^2 \equiv DX - X^3 \pmod{p}$  (ou, ce qui revient au même, de  $Y^2 \equiv X^3 - DX \pmod{p}$ ), on a

$$N_4(D) = p - \left(\frac{D}{\bar{\lambda}}\right)_4 \lambda - \left(\frac{D}{\lambda}\right)_4 \bar{\lambda};$$

cette formule est due à Davenport-Hasse (1934), et a été redémontrée par Rajwade (1970); Morlaye (1972) vient de donner une version élémentaire de la démonstration de Davenport-Hasse. La courbe  $Y^2 = X^3 - DX$ , considérée comme variété abélienne de dimension 1 définie sur  $\mathbf{Q}$ , a servi de « banc d'essai » aux conjectures de Birch et Swinnerton-Dyer; voir Birch-Swinnerton-Dyer (1965), ou Cassels-Fröhlich, *Algebraic Number Theory*, chap. XII (Academic Press, 1967).

## CHAPITRE 7

### THÉORÈME D'AX

Le résultat central de ce chapitre est le théorème suivant, dû à Ax (1964), et qui précise le théorème de Chevalley-Warning (chap. 3, sect. 1.1):

**THÉORÈME 1.** — *Soient  $k$  un corps fini à  $q = p^f$  éléments,  $F$  un polynôme de degré  $d$ , à  $n$  variables et à coefficients dans  $k$ , et  $b$  le plus grand entier strictement inférieur à  $n/d$ . Si alors  $N$  désigne le nombre de zéros de  $F$  dans  $k^n$ ,  $N$  est divisible par  $q^b$ .*

La démonstration de ce théorème est un peu analogue à celle du théorème 1 du chapitre 6 (ou plus précisément de son corollaire 1): elle consiste (du moins en principe): (1) à exprimer  $N$  à l'aide de sommes de Gauss, donc d'entiers du corps  $L$  des racines  $p(q-1)$ -ièmes de l'unité; (2) à calculer la « valeur absolue  $\mathfrak{P}$ -adique » de ces sommes en chaque idéal premier  $\mathfrak{P}$  de  $L$  au-dessus de  $p$ ; (3) à en déduire enfin l'inégalité  $|N|_{\mathfrak{P}} \leq |q^b|_{\mathfrak{P}}$ , où  $|\cdot|_{\mathfrak{P}}$