Notes sur le chapitre 8

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **22.09.2024**

$V \subset \mathbf{A}_n$ 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, $N_V = N_W - N_{W \cdot H_0}$; il suffit dans ces conditions d'appliquer le théorème 4 à N_W et le lemme 1 à $N_{W \cdot H_0}$ pour obtenir

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

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 $\mathbf{x} \mapsto \mathbf{x}^{(q)}$ 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 de 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$^{\text{ère}}$ partie) par voie « géométrique »: c'est cette démonstration qu'on a résumée ici; pour des démonstrations « arithmétiques », voir Igusa (1949) et Roquette (1953) (voir aussi **[5]**, chap. V, §§ 1-5); dans tous les cas, le point essentiel est l'inégalité $\sigma(\xi\xi') > 0$ (inégalité (23), p. 292, dans **[5]**, par exemple); pour un commentaire sur cette inégalité (dite « de Castelnuovo »), voir Weil (1954), p. 553. Pour une application aux « sommes exponentielles », voir Weil (1948, b).

§ **4**: la constante $A_1(n, d, r)$ (lemme 1) peut être prise égale à $(2d)^r$ (en fait, elle ne dépend donc pas de n); en revanche, la constante $A_2(n, d, r)$ (lemme 2) et par conséquent la constante $A(n, d, r)$ (th. 4) dépendent de n; on ne sait d'ailleurs pas en général les majorer explicitement, faute de renseignements précis sur le degré $e(n, d, r)$ de l'ensemble algébrique E.

Pour d'autres remarques sur les résultats ci-dessus, voir également le chapitre 9.

Chapitre 9

FONCTIONS ZÊTA

Dans ce dernier chapitre, on se donne comme toujours un corps fini k à $q = p^f$ éléments, de clôture algébrique $\bar{k}$; pour tout entier $m \geqslant 1$, k_m désigne l'unique extension de degré m de k contenue dans $\bar{k}$ (chap. 1, § 1). A tout ensemble algébrique V défini sur k, on peut alors associer la série formelle $Z(V; t) = \exp\left(\sum_{m \geqq 1} N_m t^m/m\right)$, où N_m désigne le nombre de points de V rationnels sur k_m, et où t est une indéterminée. Il se trouve que cette série formelle est en fait une fraction rationnelle en t, et que, moyennant des hypothèses convenables sur V, cette fraction rationnelle peut être décrite avec précision. Le paragraphe 1 de ce chapitre énonce diverses définitions équivalentes de $Z(V; t)$, et justifie le nom de « fonction zêta de V » qui lui est attribué. Le paragraphe 2 donne une esquisse de la démonstration de la rationalité de $Z(V; t)$. Le paragraphe 3 montre comment le théorème de Riemann-Roch et le théorème 3 du chapitre 8 permettent d'obtenir une description très complète de $Z(V; t)$ quand V est une courbe projective non singulière. Le paragraphe 4 indique sans démonstration diverses généralisations des résultats du paragraphe 3. Enfin, le paragraphe 5 donne des exemples de calcul explicite de fonctions zêta; ce paragraphe peut d'ailleurs être lu directement après le paragraphe 2: on y utilise uniquement les défi-