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: Chapitre 8 « HYPOTHÈSE DE RIEMANN »
DOI: https://doi.org/10.5169/seals-46287

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 $\geqslant 1$, 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

notamment que si V est une variété de dimension $\geqslant 1$ et si $\mathbf{x}$ est un *point générique* de V, $\mathbf{x}$ n'est pas considéré comme un *élément de* V: autrement dit, on n'a pas le droit d'écrire $\mathbf{x} \in V$). Pratiquement, pour la terminologie et les résultats de géométrie algébrique dont on aura effectivement besoin, le lecteur pourra se reporter au livre de Lang [**12**] ou à celui de Samuel [**15**].

Dans ce chapitre, k désigne (comme toujours) un corps fini à $q = p^f$ éléments, et $\bar{k}$ une clôture algébrique de k. $\mathbf{A}_n$ et $\mathbf{P}_n$ désignent respectivement l'espace affine et l'espace projectif de dimension n sur k. Enfin, si V est un ensemble algébrique défini sur k, *l'ensemble des points de* V *rationnels sur* k *est désormais noté* V_k.

§ 1. *Courbes de genre* 0 (*).

1.1. THÉORÈME 1. — *Si V est une courbe projective non singulière de genre* 0 *définie sur k, elle est birégulièrement équivalente (sur k) à la droite projective définie sur k.*

Démonstration. — D'après un théorème classique de Poincaré (voir [**18**], pp. 71-72), V, de genre 0, est birégulièrement équivalente sur k soit à une droite, soit à une conique (ceci, sans hypothèse sur k; ce théorème de Poincaré peut d'ailleurs se déduire facilement du théorème de Riemann-Roch: voir par exemple [**2**], chap. XVI, th. 6). On peut donc se borner à démontrer le théorème 1 lorsque V est une conique définie dans le plan projectif $\mathbf{P}_2$ par une équation homogène et de degré 2, $F(X_0, X_1, X_2) = 0$, à coefficients dans k: le théorème de Chevalley (chap. 3, th. 1, cor. 1) montre alors que cette équation admet une solution (a_0, a_1, a_2) non triviale dans k^3, donc que V admet un point $\mathbf{a}$ rationnel sur k. Soit maintenant Δ une droite projective du plan $\mathbf{P}_2$, définie sur k et ne passant pas par $\mathbf{a}$ (si par exemple $a_0 \neq 0$, on peut prendre pour Δ la droite d'équation $X_0 = 0$); pour tout point $\mathbf{y}$ de Δ, notons $\varphi(\mathbf{y})$ le second point d'intersection de V et de la droite joignant $\mathbf{a}$ à $\mathbf{y}$; alors l'application $\mathbf{y} \mapsto \varphi(\mathbf{y})$ est évidemment une équivalence birégulière $\Delta \to V$ définie sur k, et le théorème 1 est démontré.

1.2. COROLLAIRE 1. — *Si N désigne le nombre de points de V rationnels sur k, on a exactement $N = q + 1$.*

---

*) Pour un résumé rapide et élémentaire des propriétés des courbes algébriques (genre, théorème de Riemann-Roch), voir SAMUEL (1967).

Démonstration. — Le théorème 1 permet de se limiter au cas où $V = \Delta$ (la droite projective); mais l'ensemble Δ_k des points de Δ rationnels sur k comporte évidemment q éléments « à distance finie » (correspondant bijectivement aux éléments de k), plus un élément « à l'infini » — soit au total $q + 1$ éléments, C.Q.F.D.

§ 2. *Courbes de genre* 1.

Pour la géométrie des courbes de genre 1, voir [**4**], notamment pp. 209-233.

2.1. THÉORÈME 2 (théorème de Schmidt). — *Si V est une courbe projective non singulière de genre* 1 *définie sur k, V admet au moins un point rationnel sur k.*

Démonstration. — D'après un théorème de Châtelet (voir par exemple [**4**], pp. 230-233), il existe une courbe projective non singulière G (la jacobienne de V), définie sur k, ayant un point $\mathbf{o}$ rationnel sur k, et birégulièrement équivalente à V sur $\bar{k}$ (ce qui permet d'identifier $\bar{k}(G)$ à $\bar{k}(V)$). G est évidemment de genre 1, comme V, et on peut la munir d'une loi de groupe rationnelle, définie sur k, notée additivement, ayant $\mathbf{o}$ pour élément neutre, et faisant de G une variété abélienne de dimension 1 sur k ([**4**], pp. 210-211). De plus, l'identification $\bar{k}(G) = \bar{k}(V)$ permet de munir V d'une structure d'espace homogène principal sur G ([**4**], pp. 226-227), c'est-à-dire de construire deux applications rationnelles $\mu\colon V \times G \to V$, et $\upsilon\colon V \times V \to G$, définies sur k, et possédant les propriétés suivantes:

(i) quel que soit $\mathbf{x} \in V$, on a $\mu(\mathbf{x}, \mathbf{o}) = \mathbf{o}$;

(ii) quels que soient $\mathbf{x} \in V$ et $\mathbf{a}, \mathbf{b} \in G$, on a $\mu(\mu(\mathbf{x}, \mathbf{a}), \mathbf{b}) = \mu(\mathbf{x}, \mathbf{a}+\mathbf{b})$;

(iii) quels que soient $\mathbf{x}, \mathbf{y} \in V$, il existe un $\mathbf{a} \in G$ et un seul tel que $\mu(\mathbf{x}, \mathbf{a}) = \mathbf{y}$, et $\mathbf{a}$ est égal à $\upsilon(\mathbf{y}, \mathbf{x})$.

Concrètement, G opère sur V par translations: $\mu(\mathbf{x}, \mathbf{a})$ est le transformé de $\mathbf{x}$ par la translation $\mathbf{a}$, et $\upsilon(\mathbf{y}, \mathbf{x})$ est la translation qui transforme $\mathbf{x}$ en $\mathbf{y}$; ainsi, il n'y a aucun risque de confusion à écrire $\mathbf{x} + \mathbf{a}$ au lieu de $\mu(\mathbf{x}, \mathbf{a})$ et $\mathbf{y} - \mathbf{x}$ au lieu de $\upsilon(\mathbf{y}, \mathbf{x})$; on adoptera cette écriture dans le reste de la démonstration.

Convenons d'autre part, pour tout point $\mathbf{x} = (x_0, x_1, \ldots)$ d'un espace projectif de dimension quelconque sur k, de noter $\mathbf{x}^{(q)}$ le point $(x_0^q, x_1^q, \ldots)$. Il est clair que $\mathbf{x}$ est rationnel sur k si et seulement si $\mathbf{x}^{(q)} = \mathbf{x}$ (chap. 1, prop. 2 ou prop. 8). Il est clair également que si U est un ensemble algébrique

défini sur k et si $\mathbf{x} \in U$, alors $\mathbf{x}^{(q)} \in U$ (représenter U par un système d'équations à coefficients dans k, et remarquer que l'élévation à la puissance q-ième est un automorphisme de k qui laisse invariante lesdits coefficients).

Appliquons ceci à V et G. Soit $\mathbf{x}$ un élément quelconque de V, et posons $\mathbf{a} = \mathbf{x} - \mathbf{x}^{(q)}$. Considérons d'autre part l'application rationnelle $\mathbf{z} \mapsto \mathbf{z}^{(q)} - \mathbf{z}$ de G dans G; elle n'est certainement pas constante (sinon, on aurait $\mathbf{z}^{(q)} - \mathbf{z} = \mathbf{o}^{(q)} - \mathbf{o} = \mathbf{o}$, soit $\mathbf{z}^{(q)} = \mathbf{z}$, pour tout $\mathbf{z} \in G$; tout point de G serait rationnel sur k, et G serait de dimension 0: absurde); comme G est irréductible, projective (donc complète), non singulière et de dimension 1, cette application est surjective. En particulier, il existe $\mathbf{b} \in G$ tel que $\mathbf{a} = \mathbf{b}^{(q)} - \mathbf{b}$, donc, en revenant à la définition de $\mathbf{a}$, tel que $\mathbf{x} + \mathbf{b} = \mathbf{x}^{(q)} + \mathbf{b}^{(q)} = (\mathbf{x}+\mathbf{b})^{(q)}$ (cette dernière égalité parce que l'application rationnelle μ: $V \times G \to V$, qui à $(\mathbf{x}, \mathbf{b})$ associe $\mathbf{x} + \mathbf{b}$, est définie sur k); mais alors $\mathbf{x} + \mathbf{b}$ est un point de V rationnel sur k, C.Q.F.D.

2.2. COROLLAIRE 1 (théorème de Hasse). — *Si N désigne le nombre de points de V rationnels sur k, on a l'inégalité*

$$|q + 1 - N| \leqslant 2q^{1/2}. \tag{2.2.1}$$

Démonstration. — Soit $\mathbf{o}$ un point de V rationnel sur k (th. 2), et munissons V de sa structure de variété abélienne définie sur k et ayant $\mathbf{o}$ pour élément neutre. Soit M l'anneau des endomorphismes de V, et, pour tout $\lambda \in M$, soit $\deg(\lambda)$ le degré de l'application rationnelle λ ([**4**], pp. 215-216). Soit enfin F l'endomorphisme $\mathbf{x} \mapsto \mathbf{x}^{(q)}$ de V. Alors $F - 1$ (c'est-à-dire l'endomorphisme $\mathbf{x} \mapsto \mathbf{x}^{(q)} - \mathbf{x}$ de V) est un élément non nul de M (raisonner comme dans la sect. 2.1), donc une *isogénie* de V ([**4**], pp. 215-216) dont le noyau est exactement l'ensemble des points de V rationnels sur k (voir sect. 2.1). On peut démontrer que cette isogénie est *non ramifiée* ([**4**], p. 217), donc que l'ordre du noyau de $F - 1$ est égal au degré de $F - 1$; ainsi,

$$N = \deg(F - 1). \tag{2.2.2}$$

On peut démontrer également que M est un $\mathbf{Z}$-module libre de rang fini, sans diviseurs de zéro, et qu'il est muni d'un anti-automorphisme $\lambda \mapsto \lambda'$ tel que $\lambda\lambda' = \deg(\lambda)$ pour tout $\lambda \in M$ (voir par exemple Deuring (1941)); il en résulte notamment que, quel que soit $m \in \mathbf{Z}$, on a

$$\deg(F - m.1) = (F - m.1)(F - m.1)' = m^2 - tm + q, \tag{2.2.3}$$

avec $t = F + F' \in \mathbf{Z}$, et $q = FF' = \deg(F)$ (puisque $F(\mathbf{x}) = \mathbf{x}^{(q)}$). Etant

donné sa définition, le polynôme $m^2 - tm + q$ est toujours positif, d'où $t^2 - 4q \leqslant 0$, ou encore

$$|t| \leqslant 2q^{1/2}. \tag{2.2.4}$$

Mais faisons $m = 1$ dans (2.2.3) et utilisons (2.2.2); il vient

$$t = q + 1 - N, \tag{2.2.5}$$

et il suffit de porter (2.2.5) dans (2.2.4) pour obtenir l'inégalité (2.2.1).

2.3. La démonstration esquissée ci-dessus est essentiellement la démonstration originale de Hasse (voir Hasse (1933, 1934, 1936)). Manin en a donné une version « élémentaire » dont voici le principe (Manin (1956); pour les détails des calculs, voir [**6**], chap. 10, pp. 197-206). On suppose pour simplifier $p \neq 2, 3$ (mais cette restriction n'est pas essentielle). Comme V admet un point rationnel sur k, on peut supposer V écrite sous forme normale de Weierstrass

$$Y^2 = X^3 - aX - b, \tag{2.3.1}$$

$a, b \in k$, $4a^3 - 27b^2 \neq 0$. Soit alors ξ un élément transcendant sur k, et soit W la courbe définie sur $K = k(\xi)$ et ayant pour équation

$$Y^2 = \frac{X^3 - aX - b}{\xi^3 - a\xi - b}. \tag{2.3.2}$$

C'est une courbe de genre 1, dont on connaît (au moins) deux points rationnels sur K: $\mathbf{a}_0 = (\xi^q, \eta^{(q-1)/2})$ (avec $\eta = \xi^3 - a\xi - b$) et $\mathbf{b} = (\xi, 1)$. Munissons W de sa structure de variété abélienne définie sur K, ayant le point à l'infini $\mathbf{o}$ pour élément neutre, et pour laquelle trois points ont une somme nulle si, et seulement si, ils sont alignés ([**4**], pp. 211-214); pour tout $m \in \mathbf{Z}$, posons $\mathbf{a}_m = \mathbf{a}_0 - m.\mathbf{b}$, puis définissons un entier d_m de la façon suivante: si $\mathbf{a}_m = \mathbf{o}$, posons $d_m = 0$; si au contraire $\mathbf{a}_m \neq \mathbf{o}$, donc si le point $\mathbf{a}_m$ est « à distance finie », de coordonnées affines x_m, y_m, avec $x_m = P_m(\xi)/Q_m(\xi)$ et P_m, Q_m premiers entre eux, posons $d_m = \deg(P_m)$. On peut alors démontrer (à l'aide des formules d'addition sur une cubique de Weierstrass: voir [**4**], p. 214) les deux relations suivantes:

$$d_{-1} - d_0 = N - q\,; \quad d_{m-1} + d_{m+1} = 2d_m + 2\,;$$

ces deux formules permettent de calculer d_m:

$$d_m = m^2 - (q + 1 - N)\,m + q\,; \tag{2.3.3}$$

comme par définition $d_m \geqslant 0$, le polynôme en m figurant au second membre de (2.3.3) est positif; d'où

$$(q+1-N)^2 \leqslant 4q\,,$$

ce qui implique bien l'inégalité (2.2.1).

La parenté entre ces deux démonstrations tient au fait que $d_m = \deg(F - m.1)$.

2.4. On a vu au chapitre 6 (sect. 3.3, (1) et 3.5) que la courbe *affine* $Y^2 = 1 - X^3$ (qui est de genre 1 pour $p \neq 2, 3$) a un nombre de points rationnels sur k égal à q si $q \equiv -1 \pmod 6$ et à $q + \alpha + \bar{\alpha}$ (avec $\alpha = \pi(\varphi, \chi)$) si $q \equiv 1 \pmod 6$. Si on remarque que cette courbe, considérée maintenant comme *projective*, admet *un* point à l'infini rationnel sur k, on voit que le nombre total N de ses points rationnels sur k satisfait à $|q + 1 - N| = 0$ dans le premier cas, et à $|q + 1 - N| \leqslant |\alpha| + |\bar{\alpha}| = 2q^{1/2}$ dans le second cas (voir chap. 5, prop. 9, cor. 1): le théorème de Hasse se trouve ainsi vérifié directement pour cette courbe.

Raisonnement analogue pour la courbe $Y^2 = X - X^3$, qui admet *un* point à l'infini rationnel sur k, et pour la courbe $Y^3 = 1 - X^3$, qui admet un ou trois points à l'infini rationnels sur k selon que q est congru à -1 ou à 1 (mod 3) (on suppose naturellement $p \neq 3$).

Considérons enfin la courbe *affine* $Y^2 = 1 - X^4$ (qui est de genre 1 pour $p \neq 2$) et dont le nombre de points rationnels sur k est égal à $q + 1$ si $q \equiv -1 \pmod 4$ et à $q - 1 + \alpha + \bar{\alpha}$ (avec $\alpha = \pi(\varphi, \chi)$: chap. 6, sect. 3.3, (2), et 3.5) si $q \equiv 1 \pmod 4$. Dans le premier cas, cette courbe, envisagée maintenant comme *projective*, admet à l'infini *un point double* rationnel sur k, mais ce point est « isolé » (par désingularisation, il donnerait deux points conjugués sur k, mais non rationnels sur k): ce point ne doit donc pas être pris en considération; on a donc ici $N = q + 1$, ou $|q + 1 - N| = 0$. Dans le second cas, la courbe admet encore un point double à l'infini, rationnel sur k, mais « non isolé » (par désingularisation, il donnerait deux points rationnels sur k): ce point doit donc être compté deux fois, d'où maintenant $N = q + 1 + \alpha + \bar{\alpha}$, donc, comme précédemment, $|q + 1 - N| \leqslant 2q^{1/2}$: le théorème de Hasse se trouve également vérifié directement pour cette courbe *).

*) En fait, on a raisonné ici, non sur la courbe $Y^2 = 1 - X^4$, mais sur sa *normalisée* (voir d'ailleurs chap. 9, sect. 5.2, (2) et (4)).

§ 3. *Courbes de genre quelconque.*

3.1. L'égalité $N = q + 1$, pour une courbe de genre 0, et l'inégalité $|q + 1 - N| \leqslant 2q^{1/2}$, pour une courbe de genre 1 (th. 1, cor. 1, et th. 2, cor. 1), sont des cas particuliers du résultat suivant, dû à Weil (1940, 1948):

THÉORÈME 3 (« hypothèse de Riemann » pour V). — *Si V est une courbe projective non singulière de genre g définie sur k, et si N désigne le nombre de points de V rationnels sur k, on a*

$$|q + 1 - N| \leqslant 2gq^{1/2}. \tag{3.1.1}$$

Démonstration. — Soit $W = V \times V$ la surface produit de V par elle-même, c'est-à-dire le lieu sur k du point $(\mathbf{x}, \mathbf{y})$, où $\mathbf{x}$ et $\mathbf{y}$ sont deux points génériques de V, indépendants sur k (voir **[20]**, p. 29, ou Samuel (1967), § I et II). On appelle *correspondance sur V* ([**20**], p. 29) tout diviseur sur V, donc tout cycle de dimension 1 sur V; si X est une correspondance sur V, on appelle *symétrique de X* et on note X' la correspondance image de X par la symétrie $(\mathbf{x}, \mathbf{y}) \mapsto (\mathbf{y}, \mathbf{x})$ de W; si X et Y sont deux correspondances sur V, on appelle *somme de X et Y* et on note $X + Y$ leur somme en tant que diviseurs sur V; on appelle *produit* (de composition: rien à voir avec le produit d'intersection) *de X et Y* et on note $X \circ Y$ la correspondance déduite de X et Y par l'opération de composition des graphes dans le produit $V \times V$ (pour une définition précise, voir [**20**], pp. 35-38); enfin, on écrit $X \equiv Y$ s'il existe deux diviseurs $\mathfrak{m}$ et $\mathfrak{n}$ sur la *courbe V* et une fonction rationnelle f sur la *surface W* tels que

$$X - Y = (\mathfrak{m} \times V) + (V \times \mathfrak{n}) + (f),$$

(f) désignant le diviseur de la fonction f. On peut alors montrer ([**20**], pp. 38-41) que la relation $\equiv$ est une relation d'équivalence dans l'ensemble des correspondances sur V, et qu'elle est compatible avec les opérations somme et produit introduites ci-dessus: l'ensemble quotient par $\equiv$ de l'ensemble des correspondances sur V se trouve ainsi muni d'une structure d'anneau; on le note $A(V)$, et on l'appelle *anneau des correspondances de V*; si $\xi, \eta \in A(V)$ sont les images de correspondances X et Y sur V, leur somme $\xi + \eta$ et leur produit $\xi\eta$ sont par définition les images dans $A(V)$ de $X + Y$ et de $X \circ Y$; noter que la symétrie $X \mapsto X'$ est évidemment compatible avec la relation $\equiv$; elle définit donc par passage au quotient une involution $\xi \mapsto \xi'$ de $A(V)$ qui est en fait un anti-automorphisme de $A(V)$: si $\xi, \eta \in A(V)$, on a $(\xi+\eta)' = \xi' + \eta'$ et $(\xi\eta)' = \eta'\xi'$; noter aussi que si Δ

désigne la diagonale de W, c'est-à-dire le lieu sur k du point $(\mathbf{x}, \mathbf{x})$, alors Δ est birégulièrement équivalente à V sur k, et δ, classe de la correspondance Δ sur V, est l'élément neutre de $A(V)$ pour la multiplication.

Pour toute correspondance X sur V, notons maintenant $d_1(X)$ et $d_2(X)$ les degrés des cycles $pr_1(X)$ et $pr_2(X)$, projections de X sur le premier et sur le second facteur de $W = V \times V$; notons d'autre part $i(X \cdot \Delta)$ le nombre d'intersection de X et Δ sur W (qui est défini même si Δ est une composante de X: voir par exemple Samuel (1967), p. 307), et posons

$$S(X) = d_1(X) + d_2(X) - i(X \cdot \Delta). \tag{3.1.2}$$

$S(X)$ est un entier rationnel, qui ne dépend que de la classe de la correspondance X; si alors $\xi \in A(V)$, et si X désigne n'importe quelle correspondance d'image ξ dans $A(V)$, on peut définir un entier rationnel $\sigma(\xi)$, ne dépendant que de ξ, par l'égalité $\sigma(\xi) = S(X)$; $\sigma(\xi)$ est dit *trace de* ξ; et on peut montrer ([**20**], pp. 41-54) que la trace possède les propriétés suivantes:

LEMME 1. — *Quels que soient* $\xi, \eta \in A(V)$, *on a* $\sigma(\xi+\eta) = \sigma(\xi) + \sigma(\eta)$, $\sigma(\xi\eta) = \sigma(\eta\xi)$, *et* $\sigma(\xi') = \sigma(\xi)$.

LEMME 2. — δ *désignant toujours la classe de* Δ, *on a* $\sigma(\delta) = 2g$.

LEMME 3. — *Quel que soit* $\xi \neq 0$ *dans* $A(V)$, *on a* $\sigma(\xi\xi') > 0$.

Le lemme 1 est immédiat; le lemme 2 résulte du fait que $d_1(\Delta) = d_2(\Delta) = 1$, de la formule classique $i(\Delta \cdot \Delta) = 2 - 2g$ (Samuel (1967), p. 307, (2)), et de la définition (3.1.2) de $\sigma(\delta) = S(\Delta)$. Le lemme 3 est la « clef de voûte » de la démonstration: c'est de l'inégalité $\sigma(\xi\xi') \geqslant 0$ convenablement appliquée que va résulter l'inégalité (3.1.1). Soit en effet Γ le lieu sur k du point $\mathbf{z} = (\mathbf{x}, \mathbf{x}^{(q)})$ (la notation $\mathbf{x}^{(q)}$ a été définie dans la sect. 2.1); Γ est une correspondance sur V (« correspondance de Frobenius »), et sa symétrique Γ' est le lieu sur k du point $\mathbf{z}' = (\mathbf{x}^{(q)}, \mathbf{x})$; on a évidemment $[k(\mathbf{x}): k(\mathbf{x})] = 1$ et $[k(\mathbf{x}): k(\mathbf{x}^{(q)})] = q$, donc $d_1(\Gamma) = 1$ et $d_2(\Gamma) = q$; on peut d'autre part montrer que chacun des points du cycle intersection $\Gamma \cdot \Delta$ a pour multiplicité 1: comme les composantes de ce cycle sont exactement les points $(\mathbf{a}, \mathbf{a})$ de $V \times V$ avec $\mathbf{a} = \mathbf{a}^{(q)}$, c'est-à-dire avec $\mathbf{a}$ *rationnel sur* k, on voit que $i(\Gamma \cdot \Delta) = N$; si alors γ désigne la classe de la correspondance Γ, la formule de définition (3.1.2) permet d'écrire

$$\sigma(\gamma) = q + 1 - N. \tag{3.1.3}$$

On peut démontrer par ailleurs que $\gamma\gamma' = q\delta$; soit maintenant m un entier rationnel et posons $\xi = \gamma - m\delta$; on a $\xi' = \gamma' - m\delta$, et

$$\xi\xi' = m^2\delta - m(\gamma+\gamma') + \gamma\gamma';$$

prenons les traces des deux membres, tenons compte de la valeur de $\gamma\gamma'$ et utilisons les lemmes 1 et 2; il vient:

$$\sigma(\xi\xi') = 2gm^2 - \sigma(\gamma+\gamma')\,m + 2gq;$$

mais $\sigma(\gamma+\gamma') = 2\sigma(\gamma) = 2(q+1-N)$ (lemme 1 et formule (3.1.3)); ainsi:

$$\sigma(\xi\xi') = 2gm^2 - 2(q+1-N)\,m + 2gq;$$

le lemme 3 montre que le polynôme en m figurant dans le membre de droite de cette dernière égalité est positif; on a donc

$$(q+1-N)^2 - 4g^2q \leqslant 0,$$

ce qui implique l'inégalité (3.1.1) et prouve le théorème 3.

3.2. On peut également démontrer le théorème 3 à l'aide de la théorie des variétés abéliennes (structure de l'anneau des endomorphismes, propriétés du polynôme caractéristique d'un endomorphisme, etc.; voir par exemple **[20]**, § VII à XI, ou **[9]**, chap. 5) appliquée à la jacobienne de la courbe V. Pour $g = 1$, cette seconde démonstration coïncide avec la démonstration du « théorème de Hasse » donnée dans la section 2.2 (dans ce cas en effet, V, admettant un point rationnel sur k par le théorème de Schmidt, s'identifie à sa propre jacobienne); dans le cas général (g quelconque), cette seconde démonstration n'est pas essentiellement différente de celle esquissée dans la section 3.1, du fait que l'anneau des correspondances sur V est isomorphe à l'anneau des endomorphismes de la jacobienne de V (**[20]**, pp. 161-163, th. 22 et cor. 2).

3.3. Revenons à l'inégalité (3.1.1). Considérons à titre d'exemple la courbe plane $X^4 + Y^4 = 1$, et supposons $q \equiv 1 \pmod 4$. Si ψ est un caractère d'ordre 4 de k^*, la proposition 3 du chapitre 6 montre que le nombre de points « à distance finie » sur cette courbe est égal à $q + \sum_{1 \leqslant j_i \leqslant 3} \pi(\psi^{j_1}, \psi^{j_2})$; la somme comprend neuf termes, dont trois sont des sommes de Jacobi triviales (pour $j_1 + j_2 = 4$) et valent -1 (chap. 5, prop. 9, (i)), les six autres (notons-les $\alpha_1, \ldots, \alpha_6$) étant des sommes de Jacobi non triviales, de module $q^{1/2}$: le nombre de points « à distance finie » est donc

$q - 3 + \alpha_1 + \ldots + \alpha_6$. 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, $N = q - 3 + 4 + \alpha_1 + \ldots + \alpha_6$, et on a

$$|q + 1 - N| \leqslant |\alpha_1| + \ldots + |\alpha_6| = 6q^{1/2} = 2gq^{1/2},$$

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-meme vers l'infini; en particulier, pour tout m assez grand, $N_m \geqslant 1$.*

Démonstration. — En effet, le théorème 3 appliqué au corps de base k_m donne $N_m \geqslant q^m + 1 - 2gq^{m/2}$, 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 $g \geqslant 2$, 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*

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

$A(n, d, r)$ 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 $N \leqslant d$, et le théorème est évident; supposons donc $n \geqslant 1$: 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 $|N - q^r| \leqslant B(d)\, q^{r-(1/2)} + A(n-1, d, r)\, q^{r-1}$: le théorème est également établi. Ainsi, on peut désormais supposer n fixé ($\geqslant 1$), 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 $N \leqslant d$, 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 $\varphi: V_1 \to V$), et soit N_1 le nombre de points de V_1 rationnels sur k; le théorème 3 montre que $|q + 1 - N_1| \leqslant 2gq^{1/2}$, 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 $\varphi: V_1 \to V$ 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, $|N - N_1| \leqslant d(d-1)(d-2)/2$, et finalement $|N - q| \leqslant B(d)\, q^{1/2} + A(n, d, 1)$, avec $B(d) = 2g \leqslant (d-1)(d-2)$ 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 $r \geqslant 2$, 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 $\mathbf{w} = (w_0, \ldots, w_n)$ de $\mathbf{P}'_n$, associons l'hyperplan $H_{\mathbf{w}}$ de $\mathbf{P}_n$ d'équation $w_0X_0 + \ldots + w_nX_n = 0$; 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

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

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

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

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*

$$N_Z \leqslant A_1(n, d, r)\, q^r , \tag{4.1.3}$$

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*

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

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 $N_R \leqslant N_E \leqslant A_1(n, e, n-1)\, q^{n-1}$, et la constante du lemme 2 est donnée par

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

(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 $N_{\mathbf{w}}$ de la première somme est le nombre de points rationnels sur k de $V \cdot H_{\mathbf{w}}$, qui est une *variété* de type $(n, d, r-1)$ définie sur k, puisque $\mathbf{w} \in I$; par hypothèse de récurrence (sur r), on a donc

$$|N_{\mathbf{w}} - q^{r-1}| \leqslant B(d)\, q^{r-(3/2)} + A(n, d, r-1)\, q^{r-2}.$$

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

$$|Q_{n-1}^{-1} \sum_{\mathbf{w} \in I} N_{\mathbf{w}} - q^r - B(d)\, q^{r-(1/2)}| \leqslant A_3(n, d, r)\, q^{r-1}, \tag{4.1.5}$$

$A_3(n, d, r)$ 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 $N_{\mathbf{w}}$ qui y apparaissent est le nombre de points rationnels sur k d'un cycle, $V \cdot H_{\mathbf{w}}$, positif, rationnel sur k, et de type $(n, d, r-1)$; le lemme 1 donne donc $N_{\mathbf{w}} \leqslant A_1(n, d, r-1)\, q^{r-1}$; 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 $Q_{n-1} = q^{n-1} + \ldots + q + 1$; ainsi, $Q_{n-1}^{-1} \leqslant q^{1-n}$, et on arrive à la majoration

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

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, $N_m \geqslant 1$.*

La propriété « $N_m \geqslant 1$ 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 $X_0^2 + \ldots + X_n^2 = 0$, 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 $x_0^2 + \ldots + x_n^2$ avec $x_0, \ldots, x_n \in K$ n'est possible que si $x_0 = \ldots = x_n = 0$. Un argument de ramification montrerait de même que la variété $X_0^{n+1} + pX_1^{n+1} + \ldots + p^n X_n^{n+1} = 0$, 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 « $N_m \geqslant 1$ 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 $n \geqslant 2$; l'équation $P(X_0, \ldots, X_{n-1}) = 0$ 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); $\omega_1, \ldots, \omega_n$ 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

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

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 $X^2Y^2 + X^2 + Y^2 - 1 \equiv 0 \pmod{p}$, 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-