SÉMINAIRE N. BOURBAKI

ANDRÉ NÉRON

L'arithmétique sur les variétés algébriques

Séminaire N. Bourbaki, 1954, exp. n° 66, p. 167-173

<http://www.numdam.org/item?id=SB_1951-1954__2__167_0>

Séminaire BOURBAKI
(Mai 1952)

L'ARITHMÉTIQUE SUR LES VARIÉTÉS ALGÉBRIQUES

par André NÉRON

(d'après A. WEIL, [5]).

Les "distributions" introduites par WEIL dans sa thèse [4] pour l'étude des points algébriques sur les courbes et leurs jacobiennes, ont été utilisées par SIEGEL [3] et par NORTHCOTT [1] et [2], qui a défini une nouvelle notion très commode, la "complexité" d'un point. Ici WEIL reprend sa théorie sous une forme plus algébrique introduit la "hauteur", notion équivalente à celle de la complexité, et retrouve en les complétant les résultats de NORTHCOTT et de SIEGEL.

1. Préliminaires algébriques.

Les anneaux considérés sont commutatifs sans diviseurs de zéro, et ont un élément unité. Aux corps on adjoint, s'il y a lieu, un élément ∞ ; le groupe multiplicatif des éléments $\neq 0$ de K est noté K^* .

Une spécialisation d'un anneau A est une application f de A dans un anneau telle que $f(1) = 1$. On dit que f et f' sont équivalentes si $f' = g \circ f$, où f est un isomorphisme de $f(A)$ sur $f(A')$.

Un anneau A dont l'ensemble des éléments inversibles est un idéal $\mathfrak{p}$ est un anneau de spécialisation ; $\mathfrak{p}$ est son idéal de spécialisation. $\mathfrak{p}$ est toujours premier maximal, et $A/\mathfrak{p}$ est un corps, dit corps résiduel. L'application canonique de A dans $A/\mathfrak{p}$ est la spécialisation canonique de A .

Un sous-anneau R d'un corps K est un anneau de valuation si $K = R \cup R^{-1}$. R est toujours un anneau de spécialisation. L'idéal de spécialisation correspondant est son idéal de valuation. L'extension à K de la spécialisation canonique de R (ou de toute autre équivalente) est une place de K .

Une valuation de K est un homomorphisme ω de K sur un groupe totalement ordonné Γ , auquel sont adjoints des éléments $+\infty$ et $-\infty$, tel que $\omega(0) = +\infty$ $\omega(\infty) = -\infty$ et $\omega(x , y) \geqslant \inf[\omega(x) , \omega(y)]$. Si $U(R)$ est le groupe des éléments inversibles de l'anneau de valuation R , l'homomorphisme canonique de K^* sur $K^*/U(R)$ (muni de la relation d'ordre induite sur la relation de préordre $y \in R_x$ dans K) définit une valuation, dite canonique, de K .

Il y a correspondance biunivoque entre anneaux de valuation, valuations canoniques et classes de valuations équivalentes (modulo le remplacement de Γ par un groupe isomorphe) de K. L'anneau et l'idéal de valuation de ω sont définis respectivement par $\omega(x) \geqslant 0$ et $\omega(x) > 0$.

THÉORÈME 1. - Soient A un sous-anneau de K, $x = (x_\alpha)$ un sous-ensemble de K. Pour qu'il n'y ait pas de spécialisation g de $A[x]$ telle que $g(x_\alpha) = 0$, ou, ce qui est équivalent, pour qu'il n'y ait pas de valuation $\geqslant 0$ sur A et > 0 en les x_α, il faut et il suffit qu'il existe un polynôme $p \in A[X]$ tel que $P(x) = 0$ et $P(0) = 1$.

En effet, soit $\mathfrak{A}$ l'idéal des $P \in A[x]$ s'annulant aux x_i. Si $g(x_\alpha) = 0$, on a $g[P(x)] = g[P(0)] = 0$ pour tout $P \in \mathfrak{A}$.

Inversement, $P \to P(0)$ est un homomorphisme λ de $A[X]$ sur A. S'il n'existe pas de polynôme P, l'image $\mathfrak{a}$ de $\mathfrak{A}$ par λ est distincte de A, donc contenue dans un idéal $\mathfrak{p}$ maximal $\neq A$ et $P \to f[P(0)]$, qui s'annule sur $\mathfrak{a}$, définit une spécialisation g de $A(X)/\mathfrak{a}$ (c'est-à-dire de $A[x]$) telle que $g(x_\alpha) = 0$.

Le théorème d'extension des spécialisations permet ensuite de passer aux valuations.

2. Fonctions de valuation.

On considère l'ensemble de toutes les valuations ω canoniques non triviales sur K, et le groupe ordonné $F'(K) = \pi_\omega \omega(K^*)$. Pour tout $x \in K^*$, $\omega(x)$ définit un élément de $F'(K)$, noté $[x]$. On désigne par $F(K)$ le plus petit sous-groupe de $F^*(K)$ contenant les $[x]$ et fermé par rapport aux opérations sup et inf. Les éléments de $F(K)$ sont des fonctions de ω, dites fonctions de valuations. Si A est un sous-anneau de K, on note $F(K/A)$ la restriction de $F(K)$ aux valuations positives sur A.

D'après la distributivité de sup et inf, toute fonction de valuation se met sous la forme

$$X = \inf_\mu \sup_i [x_{\mu i}]$$

où les $x_{\mu i}$ sont en nombre fini.

D'après le théorème 1, on a $[y] > 0$ dans $F(K/A)$ si et si seulement y est entier sur A et $[y] > \inf_i [x_i]$ si et si seulement y est entier sur $A[x]$.

3. Fonctions de valuation et diviseurs.

Soient V une variété algébrique définie sur k, et K le corps des fonctions sur V. Pour toute $x \in K$, on désigne par $(x)_0$ et $(x)_\infty$ les diviseurs des zéros et des infinis de x, par $(x) = (x)_0 - (x)_\infty$ le diviseur de x.

L'anneau de spécialisation A_P de $P \in V$ est celui des x telles que $x(P)$ soit définie et finie en P. Si toute fonction x n'admettant pas la spécialisation ∞ en P (c'est-à-dire entière sur A_P) appartient à A_P, V est normale en P. Si V est normale en tous ses points, elle est dite normale.

THÉORÈME 2. - Soit V^r une variété complète sans sous-variétés multiples de dimension $r-1$, et soient $(x_1, \dots, x_n)$ des éléments $\neq 0$ de K. Alors si les $(x_i)_0$ sont sans point commun, on a $\inf_i[x_i] < 0$.

En effet, si $\inf_i[x_i]$ n'est pas < 0, alors $(0, 0 \dots 0)$ est une spécialisation de $(x_1, \dots, x_n)$ donc de $(x_1(M) \dots x_n(M))$, où M désigne un point générique de V. On étend cette spécialisation à une spécialisation P de M. On a $P \in V$ puisque V est complète. En utilisant les graphes des x_i ; on voit que $P \notin (x_i)_0$ pour tout i.

Soit T un V-diviseur rationnel sur k. On appelle élément de $F(K/k)$ attaché à T tout $X_T = \inf_\mu \sup_i[x_{\mu i}] \in F(K/k)$ tel que

$$(x_{\mu i}) = T + X_{\mu i} - U_{\mu i}$$

où les $X_{\mu i}$, $U_{\mu i}$ sont des V-diviseurs positifs tels que $\cap_\mu(\sum_i X_{\mu i}) = 0$ et $\cap_\mu U_{\mu i} = 0$ pour tout μ.

Pour $T = (x)$, on a $X_T = [x]$. On déduit du théorème 2 que $T \to X_T$ est un isomorphisme d'un sous-groupe du groupe ordonné des V-diviseurs dans $F(K/k)$. Il n'existe pas toujours d'élément X_T attaché à T. Il faut et il suffit pour cela que T soit partout "localement intersection complète" voir paragraphe 8 de cet exposé). Cette condition est réalisée pour tout T dans le cas d'une variété projective non singulière.

4. Valeurs absolues.

Par valeur absolue sur K, on entend une fonction v sur K, à valeurs dans $[0, +\infty]$, telle que $v(0) = 0$, $v(1) = 1$, $v(x+y) \leq v(x) + v(y)$ et $v(xy) = v(x)\,v(y)$. On dit que v est triviale si $v(x) = 1$ pour tout $x \neq 0$.

Supposons K de caractéristique 0. Une valeur absolue sur K est dite archimédienne si elle induit sur le corps Q des rationnels la valeur absolue

$|r|^{\rho}$. Toute valeur absolue archimédienne sur K est de la forme $|f(x)|^{\rho}$, où f est une place de K à valeurs complexes. Une valeur absolue est dite p-adique si elle induit sur Q une valeur absolue de la forme $v(r) = v(p)^n$, en posant $r = p^n \frac{a}{b}$ (a et b premiers avec p). Toute valuation non triviale sur Q appartient à l'une de ces 2 catégories. On dit que v est propre lorsqu'on a pris $\rho = 1$ dans le premier cas et $v(p) = \frac{1}{p}$ dans le second.

THÉORÈME 3. - Soient A un sous-anneau de K , v_o une valeur absolue $< \infty$ sur A , et x_i des éléments de K tels que $\inf_i[x_i] < 0$ dans F(K/A) . Alors il existe une constante γ telle que $\sup_i v(x_i) \geqslant \gamma$ pour toute v qui induit v_o sur A .

On a en effet, d'après le théorème 1, une relation $1 = \sum_{\lambda=1}^{n} A_\lambda M_\lambda(x)$, avec $a_\lambda \in A$ (tout λ), les M_λ désignant des monômes. On en tire $\sup_i v(x_i) \geqslant \inf_\lambda (1 , v(a_\lambda^{-1})/n)$.

5. Distributions.

On appelle distribution une fonction des valeurs absolues v sur K de la forme $\Delta(v) = \sup_\mu \inf_i v(x_{\mu i})$. La distribution Δ est dite associée à l'élément $X = \inf_\mu \sup_i[x_{\mu i}]$.

La "taille" de Δ est le nombre réel (dépendant de Δ et de la place $\overline{Q}$-valuée f)

$$\sum(\Delta , f) = [\prod_{v/k} \Delta(v \circ f)]^{1/d}$$

où d désigne le degré de k et où le produit $\prod$ est étendu à toutes les valeurs absolues propres (qui sont en nombre fini) sur k , chacune ayant un exposant égal à sa multiplicité. Ce nombre ne dépend pas de k .

La correspondance $X \to \Delta$ est telle qu'à $X = X'$ correspond $\Delta\Delta'^{-1}$. D'après le théorème 3, si $X < X'$, on a une constante γ telle que $\Delta \geqslant \gamma\Delta'$ et on en déduit une relation analogue entre les tailles.

6. Hauteurs.

Soit P un point rationnel sur k de S^n , k étant un sous-corps de $\overline{Q}$ de coordonnées $(\alpha_0 , \dots , \alpha_n)$. On désigne par hauteur de P le nombre réel > 0

$$h(P) = h(\alpha) = [\prod_{v/k} \inf_i v(\alpha_i)]^{1/d}$$

où d et $\prod_{v/k}$ sont définis comme plus haut.

Si Δ désigne la distribution attachée à $\sup_i[\alpha_i]$ et f l'automorphisme identique de k, on a $h(\alpha) = \Sigma(\Delta, f)$.

On a en explicitant

$$h(\alpha) = [(N\mathfrak{m})^{-1} \prod_\sigma \sup_i |\alpha_i^\sigma|]^{1/d}$$

où $\mathfrak{m}$ désigne le plus grand commun diviseur des x_i et où $\prod$ est étendu aux isomorphismes distincts σ de k dans $\bar{\mathbb{Q}}$. $h(\alpha)$ ne dépend que de P et des x_i, mais non de k.

Dans l'expression de la complexité de Northcott, $\sup_i$ est remplacé par $\sum_i$. D'après ([1], théorème 1), le nombre des points algébriques P de S^n tels que $h(P) < h_0$, $d < d_0$ est fini pour n, d_0 et h donnés.

Le théorème essentiel suivant sur les hauteurs se déduit des théorèmes 2 et 3.

THÉORÈME 4. - Soit V complète et normale définie sur $k \subset \bar{\mathbb{Q}}$. Soient φ et ψ des applications de V sur les espaces projectifs S^m, S^n, définies (sur k) par les fonctions $(x_0, \dots, x_m)$ et $(y_0, \dots, y_n)$ respectivement. Supposons qu'on ait $(x_i) = X_i - Z$ et $(y_j) = Y_j - Z$, avec $\bigcap_i X_i = 0$. Alors il existe une constante γ telle que, pour tout P algébrique $\notin \bigcup_j Y_j$ sur V on ait $h[\varphi(P)] \geq \gamma\, h[\psi(P)]$.

On en déduit en particulier que si φ applique V sur S^n et si L désigne un hyperplan de S^n la fonction h(P) ne dépend (au produit près par un nombre réel compris entre deux bornes fixes) que de la classe C de $\varphi^{-1}(L)$ modulo l'équivalence linéaire. On pose alors $h(P) = h(C, P)$. Sur une variété projective non singulière, on peut définir $h(C, P)$ pour toute C contenant des V-diviseurs algébriques sur k. Si V est une courbe, il existe une fonction $h_0(P)$ telle que, pour tout ε et pour toute classe C de V-diviseurs de degré d, on ait

$$\gamma\, h_0(P)^{d-\varepsilon} < h(C, P) \leq \gamma'\, h_0(P)^{d+\varepsilon}$$

On en tire, pour tout système de fonctions x_i tel que $\sup_i (x_i)_\infty$ soit de degré d, $\sup_{i,\sigma} |x_i(P)^\sigma| \geq \gamma\, h_0(P)^{d-\varepsilon}$ (généralisation de la 2e inégalité de Siegel).

7. Le théorème de décomposition.

Soient encore V, k (quelconque) et K (restreint aux fonctions définies sur k). Toute place k-valuée f de K admet un centre $P \in V$ (tel que $f(x) = x(P)$ pour toute x définie en P) qui est rationnel sur k. Soit Δ

une distribution, soit v une valeur absolue, supposée fixe, $< \infty$ sur k . Si $\Delta(v \circ f)$ prend la même valeur pour toutes les places de centre P , on dit que Δ est définie en P , et cette valeur est notée $\Delta(P)$.

En particulier, pour T et P rationnels sur k , on montre que la distribution Δ_T associée à X_T est partout définie et ne dépend (à un facteur borne près) que de T et P . La fonction $\Delta_T(P)$ s'annule si et seulement si $P \in T$, et est continue pour la topologie définie par v .

THÉORÈME 5. - Si V est projective non singulière, on a pour toute fonction z sur V définie sur k , telle que $(z) = \sum_i m_i W_i$, où les W_i sont premiers rationnels sur k , deux constantes γ , γ' telles que

$$\gamma \prod_i \Delta_{W_i}(P)^{m_i} \leq v[z(P)] \leq \gamma' \prod_i \Delta_{W_i}(P)^{m_i}$$

pour tout P rationnel sur k où z est définie.

Si k est le corps des complexes C , on retrouve par des méthodes topologiques élémentaires l'existence d'une fonction $\Delta_W(P)$ possédant ces propriétés, et le résultat s'étend aux variétés analytiques complexes.

Dans le cas où $k \subset \overline{Q}$ et où on ne considère que les W et les P algébriques, on définit de même une fonction $\Delta_W(P , v)$ des valeurs absolues propres sur k . La relation précédente peut être remplacée par

$$\delta(v) \prod_i \Delta_{W_i}(P , v)^{m_i} \leq v[z(P)] \leq \delta'(v) \Delta_{W_i}(P , v)^{m_i}$$

où $\delta(v)$ et $\delta'(v)$ désignent des k-diviseurs (c'est-à-dire des fonctions > 0 de V , à valeurs réelles, telles que $\delta(v) = 1$ sauf pour un nombre fini de v et que, pour toute v non-archimédienne, on ait un $\alpha \in k^*$ tel que $\delta(v) = v(\alpha)$) . La démontration utilise des variantes des théorèmes 2 et 3.

Si on se borne aux valuations non archimédiennes, $\Delta_W(P , v)$ détermine un idéal (entier) $\alpha_W(P)$ sur $k(W , P)$. Le théorème exprime qu'il existe des nombres rationnels r , r' tels que l'idéal principal $(z(P))$ soit multiple de $r \prod_i \alpha_{W_i}(P)^{m_i}$ et divise $r' \prod_i \alpha_{W_i}(P)^{m_i}$. Si V est une courbe, on a pour tout ε , un γ tel que $N(\alpha(A , P))^{1/d} \leq \gamma h_o(P)^{1+\varepsilon}$ (1re inégalité de Siegel).

8. Fonctions de valuation et idéaux locaux.

Soient A un anneau, K le corps des fractions de A, et considérons les A-idéaux fractionnaires de K de base finie $I = \sum_i x_i A$. L'élément $X = \inf_i[x_i]$ ne dépend que de I et non de la base choisie $I + J$ et $I.J$ correspondent respectivement à $\inf(X, Y)$ et $X + Y$. Si $I \supset J$, on a $X \prec Y$, mais la réciproque est fausse. I et J sont dits équivalents si $X = Y$.

Soient encore V, k et K (des fonctions définies sur k). On ne considère que les P rationnels sur k et les $\omega \geqslant 0$ sur k.

A_P désignant l'anneau de spécialisation de P, on associe à tout $K \in F(K/k)$ son image canonique X_P sur $F(K/A_P)$. Si, en tout P, cette image X_P est définie par un A_P-idéal I_P, on dit que X est définissable par un système d'idéaux locaux.

Considérons la topologie (non séparée) sur V dont les ensembles fermés sont les sous-ensembles normalement algébriques de V (c'est-à-dire réunions d'un nombre fini de variétés et de leurs conjuguées) sur k. Alors on dit qu'un système d'idéaux locaux I_P est cohérent s'il existe un recouvrement fini de V par des ouverts W_λ et, pour tout λ, des éléments $y_{\lambda j}$ de K tels que, pour tout λ et tout $P \in W_\lambda$, I_P soit équivalent à $\sum_j y_{\lambda j} A_P$. On montre que pour qu'un système d'idéaux locaux définisse un $X \in F(K/k)$, il faut et il suffit qu'il soit cohérent.

En appliquant ce résultat au cas où V^d est sans sous-variété multiple de dimension $d - 1$ et où X est défini par un système d'idéaux locaux principaux, on montre que l'application $X \to X_T$ est un isomorphisme du groupe des V-diviseurs qui sont partout localement intersections complètes sur le groupe des éléments de $F(K/k)$ définissable par idéaux locaux principaux.

BIBLIOGRAPHIE

[1] NORTHCOTT (D. G.). - An inequality in the theory of arithmetic on algebraic varieties, Proc. Cambridge philos. Soc., t. 45, 1949, p. 502-509.

[2] NORTHCOTT (D. G.). - A further inequality in the theory of arithmetic on algebraic varieties, Proc. Cambridge philos. Soc., t. 45, 1949, p. 510-518.

[3] SIEGEL (Carl Ludwig). - Über einige Anwendungen diophantischer Approximationen, Abh. Preuss. Akad. Wiss., n° 1, 1929, p. 1-70.

[4] WEIL (André). - L'arithmétique sur les courbes algébriques. Uppsala, Almquist et Wiksells, 1928 (Thèse Sc. math. Paris. 1928).

[5] WEIL (André). - Arithmetic on algebraic varieties, Annals of Math., Series 2, t. 53, 1951, p. 412-444.