ANDRÉ NÉRON

Variétés abéliennes

Séminaire N. Bourbaki, 1956, exp. nº 104, p. 35-41
<http://www.numdam.org/item?id=SB_1954-1956__3__35_0>

Séminaire BOURBAKI
(Décembre 1954)

VARIÉTÉS ABÉLIENNES.

par André NÉRON

(d'après A. WEIL [5] et en introduction à l'exposé de P. SAMUEL [2])

Dans le cas classique où le domaine fondamental est le corps des nombres complexes, la théorie des variétés abéliennes utilise leur structure topologique (tores à $2n$ dimensions) et leur représentation au moyen de fonctions abéliennes. Il s'agit ici d'une théorie abstraite (c'est-à-dire valable pour un domaine fondamental quelconque) et qui ne peut donc être développée que par des moyens purement algébriques.

Le terme variété désignera toujours dans ce qui suit une variété abstraite au sens de A. Weil. Rappelons qu'une variété abstraite V est définie par la donnée d'un ensemble fini $\mathcal{V} = \{V_\alpha\}$ de variétés affines birationnellement équivalentes et munies de "frontières" F_α . Un point de V est défini par un ensemble de points M_{α_i} régulièrement correspondants appartenant respectivement à $V_{\alpha_i} - F_{\alpha_i}$, où $\{V_{\alpha_i}\}$ désigne un sous-ensemble non vide de $\mathcal{V}$. Une variété V est dite complète si toute "spécialisation" finie ou infinie d'un point de V appartient à V (par exemple, une variété affine est non complète, une variété projective, ou un produit de variétés projectives, est une variété complète).

Une fonction f sur une variété U , à valeurs dans une variété V , est définie par une sous-variété W de $U \times V$, appelée graphe de f , ayant une projection d'indice 1 sur U . La fonction f peut n'être pas définie en certains points de U .

1. Variétés de groupe.

On appelle variété de groupe une variété G munie d'une loi de groupe $x.y$ (non nécessairement commutative) satisfaisant aux conditions suivantes :

(A) L'application $f : \{x , y\} \rightarrow x.y$ est une fonction partout définie sur $G \times G$, à valeurs dans G ;

(B) L'application $g : x \rightarrow x^{-1}$ est une fonction partout définie sur G , à valeurs dans G .

EXEMPLES. - Le groupe multiplicatif à 1 variable (droite affine privée de l'origine), l'espace k^n pour l'addition des vecteurs, l'espace à n^2 dimensions des matrices d'ordre n privé de la variété des zéros du déterminant (pour la multiplication matricielle), un produit de deux variétés de groupe quelconques.

Une variété de groupe est toujours <u>non singulière</u>. On le voit en constatant que pour tout $a \in G$, il résulte des définitions que la translation à gauche $T_a : x \to a.x$ sur G est définie par une transformation birationnelle et birégulière, donc transforme tout point simple de G en un point simple de G.

On appelle <u>corps de définition</u> de la variété de groupe G un corps de définition pour sa variété algébrique de support et pour les fonctions f et g. En fait, si k est un corps de définition pour f, c'en est un pour g, donc aussi pour l'élément neutre e de G (démonstration : les applications $f' : \{x , y\} \to y\,x^{-1}$ et $f'' : \{x , y\} \to x^{-1}\,y$ sont des fonctions dont le graphe se déduit de celui de f par permutation des facteurs de $G \times G \times G$; ces fonctions sont donc définies sur k ; il en est de même de la fonction h définie par

$$h(x , y) = f'(y , f''(x , y)) = x^{-1} ,$$

donc aussi de g).

2. <u>Variétés abéliennes</u>.

THÉORÈME 1 (CHEVALLEY). - <u>Sur toute variété de groupe complète, la loi de groupe est commutative</u>.

Soient x et y des points génériques indépendants de G. La seule spécialisation de $z = y\,x\,y^{-1}$ compatible avec la spécialisation $x \to e$ sur k est $z \to e$ (car une telle spécialisation peut être étendue à une spécialisation $y \to a$ et on a $a \in G$, puisque G est complète). Donc la sous-variété de $G \times G$ lieu de $x \times z$ sur k est de même dimension que G. Donc z est algébrique sur $k(x)$. De plus, x est une spécialisation de z sur $k(x)$ (spécialiser y en e). Donc $z = x$.

On appelle <u>variété abélienne</u> une variété de groupe complète. Une variété abélienne est donc un groupe abélien.

THÉORÈME 2. - <u>Soit V^n une variété quelconque. Toute fonction f sur V, à valeurs dans une variété abélienne A, est définie en tout point simple de V</u>.

Soient P et Q deux points génériques indépendants de V et considérons la fonction F sur $V \times V$, à valeurs dans A, définie par

$$F(P \times Q) = f(P)^{-1}\, f(Q)$$

Pour que f soit définie en P_o, il faut et il suffit que F le soit (et prenne la valeur e) en $P_o \times P_o$. La condition est évidemment nécessaire ; elle est suffisante, car si F est définie en $P_o \times P_o$, elle l'est a fortiori en $P \times P_o$; il suffit alors de spécialiser Q en P_o dans la relation $f(Q) = f(P \times Q).f(P)$.

Soit φ une fonction numérique sur G, définie et nulle en e. Alors $\Psi = \varphi \circ F$ est définie et nulle en $P \times P$, donc telle que $\Delta_V \subset (\Psi)_o$ et $\Delta_V \not\subset (\Psi)_\infty$, en désignant par Δ_V la diagonale de $V \times V$ et, comme d'habitude, par $(\Psi)_o$ et $(\Psi)_\infty$ les diviseurs des zéros et des infinis de la fonction Ψ. On a de plus

$$\Delta_V . (\Psi)_\infty = 0 \tag{1}$$

car sinon Ψ serait indéterminée en tout point d'une sous-variété simple X^{n-1} de Δ_V. Donc F serait indertiminée en tout point de X et de même f en tout point de $Y = pr_V(X)$. Ceci est impossible, car toute fonction numérique sur une variété de dimension n ne peut être indéterminée que sur un ensemble algébrique dont les composantes simples sont de dimension $\leq n-2$. La relation (1) entraîne que Ψ (donc aussi F) est définie en tout point simple de Δ_V, donc f en tout point simple de V.

REMARQUE. - La fonction Ψ représente une <u>différentielle</u> sur V (voir WEIL [4] paragraphe 2, pour la définition abstraite des différentielles) induite par une différentielle invariante sur G. La relation (1) signifie qu'une telle différentielle n'a jamais de pôles, autrement dit est toujours de <u>première espèce</u> sur V.

THÉORÈME 3. - <u>Soient, V et W deux variétés quelconques, A une variété abélienne. Toute fonction sur $V \times W$, à valeurs dans A, est de la forme $g(M).h(N)$ où g et h sont des fonctions sur V et W respectivement, à valeurs dans A.</u>

On se ramène facilement au cas où W est une courbe sans point multiple. Soit M_o un point simple de V et considérons la fonction u sur $V \times W$, à valeurs dans A, définie par

$$u(M\,,\,N) = f(M_o\,,\,N).f(M\,,\,N)^{-1}$$

Soit k un corps de définition pour V, W, A et u. On peut supposer l'image A' de u sur A non réduite à un point. D'après le théorème 2 la fonction u est définie (et prend la valeur e) en tout point de $M_o \times W$. Ces propriétés entraînent, pour a générique de A' sur k,

$$u^{-1}(a) \cap (M_o \times W) = 0\,.$$

Donc a fortiori pour M générique de V sur $k(a)$ on a

$$\overset{-1}{u}(a) \cap (M \times W) = 0$$

Donc $\overset{-1}{u}(a)$ est de la forme $V' \times W$, où V' est un sous-ensemble algébrique de V. On peut trouver dans V' un point générique M' de V sur k. La fonction u induit la constante a sur $M' \times W$, donc induit une constante sur $M \times W$ quel que soit M, et ne dépend donc que de M.

COROLLAIRE 1. - Toute fonction sur S^n, à valeurs dans une variété abélienne A est constante.

Il suffit de montrer que toute fonction f sur une droite projective D, à valeurs dans A, est constante. Soit en effet g la fonction sur $D \times D$, à valeurs dans A, définie par $g(x, y) = f(x + y)$. D'après le théorème 3, elle est de la forme $g(x).h(y)$. La relation $f(\infty) = g(x).h(\infty)$ montre que g est constante ; il en est de même de h, donc aussi de f.

On appelle homomorphisme d'une variété A dans une variété B une fonction partout définie sur A, à valeurs dans B, qui est un homomorphisme pour les structures de groupe.

COROLLAIRE 2. - Toute fonction f sur une variété abélienne A, à valeurs dans une variété abélienne B, est le produit d'un homomorphisme de A dans B par une translation dans B.

Il suffit d'appliquer le théorème 3 à la fonction F sur $A \times A$, à valeurs dans B, définie par $F(x, y) = f(x.y)$.

Il résulte de là que l'ensemble des homomorphismes de A dans B, qu'on notera $\mathcal{H}(A, B)$ admet (pour la loi $f.g$) une structure de module sur l'anneau des entiers. L'ensemble $\mathfrak{a}(A) = \mathcal{H}(A, A)$ des endomorphismes de A est de plus un anneau (pour les lois de compositions $f.g$ et $f \circ g$).

3. Homomorphismes et sous-variétés abéliennes.

Les résultats qui précédent sont les seuls utilisés dans l'exposé de SAMUEL. Il y a lieu cependant de les compléter par quelques-uns des autres résultats les plus importants contenus dans WEIL (mais qui utilisent tous, à l'exception du théorème 4, sa propre théorie des jacobiennes).

THÉORÈME 4. - Soit f un homomorphisme d'une variété abélienne A dans une variété abélienne B. L'image f est une sous-variété abélienne de B ; le noyau C de f se compose d'un nombre fini de sous-variétés de B déduites d'une sous-variété abélienne C_o de B par des translations.

La première partie est évidente. De plus, le noyau de f est un sous-ensemble algébrique C de B qui est en même temps un sous-groupe de B.

Soient X et Y deux composantes de C et montrons qu'elles se déduisent l'une de l'autre par translation. Pour x et y génériques indépendants de X et de Y respectivement, considérons dans B la translation $T_{x^{-1}y}$ amenant x sur y. Comme X et Y sont les seules composantes de C contenant respectivement x et y, on a $T_{x^{-1}y}(X) = Y$. On a aussi, pour tout $a \in X$ et tout $b \in Y$, $T_{a^{-1}b}(X) = Y$. Si en particulier on prend pour X et Y deux composantes contenant e, on trouve $T_{x^{-1}}(X) = Y$, donc $X \subset Y$. Comme on aurait de même $Y \subset X$, on a $X = Y$, $X = T_{x^{-1}}(X)$ entraîne que cette composante est une variété abélienne.

THÉORÈME 5. - Soient A^n une variété abélienne et B^r une sous-variété abélienne de A. Alors il existe une sous-variété abélienne C^{n-r} de A telle que $B \cap C$ soit un sous-groupe fini de A. Tout point de A est alors de la forme $y.z$, avec $y \in B$ et $z \in C$.

(Dans le cas classique, c'est le théorème de réductibilité complète de Poincaré).

La démonstration de ce théorème repose sur le résultat préliminaire suivant :

(I) Soient a un entier >0 et A une variété abélienne. Alors le nombre des points t de A tels que $t^a = e$ est fini.

Il suffit en fait, d'après le théorème 4, de montrer que l'ensemble de ces points est distinct de A. La démonstration de ce résultat (facile si la caractéristique p est nulle ou si a n'est pas multiple de p) est dans le cas général délicate ; elle utilise (entre autres) la théorie des correspondances sur une courbe et la représentation du "groupe des classes de correspondances" sur C par des endomorphismes de la jacobienne J de C. Il est à signaler que WEIL obtient ultérieurement un résultat beaucoup plus précis (évident, comme on sait, dans le cas classique) :

(II) Soient A une variété abélienne et u_a l'endomorphisme $x \to x^a$ de A. Alors le cycle $u_a^{-1}(0)$ est toujours défini (donc de dimension 0) et de degré a^{2n} ; si a n'est pas multiple de p, ses composants ont pour multiplicité 1

<u>et forment donc un sous-groupe d'ordre</u> a^{2n} <u>de</u> A .

Pour obtenir le théorème 5 à partir de (I), on considère une sous-variété X^{n-r} de A transversale à B en e (c'est-à-dire telle que e soit composante simple de l'intersection B , C). Pour tout $a \in A$, on pose $X_a = T_a(X)$, T_a étant la translation définie par a . Soit k un corps de définition pour A , B et X . Pour a générique sur k , le cycle $B.X_a = \sum_{i=1}^{q} b_i$ est défini, a ses composants b_i distincts, et est rationnel sur $k(a)$. On en déduit que le point $b = b_1 . b_2 \ldots b_q$ de B est rationnel sur $k(a)$, c'est-à-dire que $b = f(a)$, où f est une fonction sur A , à valeur dans B . D'après le corollaire 2 du théorème 3, on a donc $b = b_0 . g(a)$ où $b_0 \in B$ ne dépend pas de a , et où g est un homomorphisme de A dans B . De plus, pour tout $C \in B$, on a

$$B.X_{a.c} = \sum b_i' \quad , \quad \text{avec} \quad b_i' = c.b_i$$

$$B.X_{a.o} = \sum b_i' \quad , \quad \text{avec} \quad b_i' = c.b_i$$

d'où $g(a.c) = c^q.b$ et $g(c) = c^q$. D'après (I) et d'après le théorème 1 , g est donc un homomorphisme de A <u>sur</u> B ; de plus, son noyau contient une sous-variété abélienne C^{n-s} de A dont les points de rencontre avec B satisfont à $t^q = e$, donc sont en nombre fini. Pour montrer que tout point de A est de la forme $y.z$, on remarque que l'application $\{y , z\} \rightarrow y.z$ est un homomorphisme de $B \times C$ dans A dont le noyau est de dimension 0 et dont l'image est par conséquent A .

COROLLAIRE. - <u>S'il existe un homomorphisme</u> f <u>d'une variété abélienne</u> A^n <u>sur une variété abélienne</u> B^n , <u>il en existe un de</u> B^n <u>sur</u> A^n .

On applique le théorème 5 au graphe L de f considéré comme sous-variété abélienne de $A \times B$. On dit alors que les variétés abéliennes A et B sont <u>isogènes</u>. C'est une relation d'équivalence. On appelle <u>catégorie de</u> A la classe de A . La catégorie de $A \times B$, qui ne dépend que des catégories de A et de B est, par définition, leur <u>produit</u>. On appelle <u>catégorie simple</u> une catégorie non décomposable en produit, et variété <u>abélienne simple</u> une variété abélienne dont la catégorie est simple (c'est-à-dire, d'après le théorème 5, qui ne contient pas de sous-variété abélienne). Un raisonnement par récurrence sur la dimension permet de voir facilement que <u>toute catégorie est un produit de catégories simples</u>. On montre de plus l'<u>unicité</u> de cette décomposition, par exemple en constatant que si f est un homomorphisme de A sur B et C la composante abélienne du noyau de f , la catégorie de C ne dépend que de celles de A et B , et est telle que $cat(A) = cat(B) \times cat(C)$.

4. Structure de $\mathfrak{A}(A)$ et de $\mathcal{H}(A, B)$

THÉORÈME 6. - Soient A et B deux variétés abéliennes. Le module $\mathcal{H}(A, B)$ des homomorphismes de A dans B a une base finie sur l'anneau des entiers.

On peut étudier $\mathcal{H}(A, B)$ en utilisant une représentation de ce module au moyen de matrices ℓ-diques. On remarque en effet (en utilisant uniquement le résultat (I) du paragraphe précédent et les propriétés élémentaires des groupes abéliens finis) que pour ℓ entier premier $\neq p$, le groupe $g_\ell(A)$ des points de A dont l'ordre est une puissance de ℓ est isomorphe au produit d'un nombre fini d de groupes isomorphes au groupe additif des nombres ℓ-adiques modulo 1. Chaque élément de $g_\ell(A)$ est donc représenté par un système de 2n coordonnées ℓ-adiques. Un homomorphisme f de A dans B induit un homomorphisme de $g_\ell(A)$ dans $g_\ell(B)$. Le changement correspondant est défini par une matrice $M_\ell(f)$ à coefficients entiers ℓ-adiques, uniquement déterminée par la donnée de f.

On commence par traiter le cas de l'anneau $\mathfrak{A}(A)$ lorsque A est une variété abélienne simple, en montrant que pour que des éléments f_i de $\mathfrak{A}(A)$ soient indépendants sur l'anneau des entiers, il faut et il suffit que les matrices correspondantes le soient sur l'anneau des entiers ℓ-adiques. On trouve que le rang de $\mathfrak{A}(A)$ sur l'anneau des entiers est $\leq 4n^2$. Pour passer de là au cas général, on utilise des décompositions des catégories de A et de B en produit de catégories simples.

BIBLIOGRAPHIE

[1] LANG (Serge). - Abelian Varieties. - New York et Londres, Interscience Publishers (à paraître).

[2] SAMUEL (Pierre). - La jacobienne d'une courbe algébrique [d'après W. L. Chow], Séminaire Bourbaki, t. 7, 1954/55.

[3] Séminaire C. CHEVALLEY, Classification des groupes de Lie algébriques, t. 1, 1956-1958.

[4] WEIL (André). - Sur les courbes algébriques et les variétés qui s'en déduisent. - Paris, Hermann, 1948 (Act. scient. et ind., n° 1041 ; Publ. Inst. Math. Univ. Strasbourg, 7).

[5] WEIL (André). - Variétés abéliennes et courbes algébriques. - Paris, Hermann, 1948 (Act. scient. et ind., n° 1064 ; Publ. Inst. Math. Univ. Strasbourg, 8).