PIERRE SAMUEL

La conjecture de Mordell pour les corps de fonctions

Séminaire N. Bourbaki, 1966, exp. n° 287, p. 149-167

<http://www.numdam.org/item?id=SB_1964-1966__9__149_0>

Séminaire BOURBAKI
17e année, 1964/65, n° 287
Février 1965

LA CONJECTURE DE MORDELL POUR LES CORPS DE FONCTIONS

par Pierre SAMUEL

(d'après H. GRAUERT [1])

1. Introduction.

La conjecture de Mordell dit qu'une courbe algébrique de genre $g \geqslant 2$ sur le corps des rationnels, ou sur un corps de nombres K, n'a qu'un nombre fini de points rationnels sur K. Bien sûr, une courbe de genre 0 (droite) ou 1 (courbe elliptique de rang $\geqslant 1$) peut avoir une infinité de points rationnels. La conjecture de Mordell s'applique à la courbe $x^n + y^n = 1$ $(n \geqslant 4)$, et serait donc un pas important vers le problème de Fermat.

L'analogue de la conjecture de Mordell pour les corps de fonctions a été récemment démontré.

THÉORÈME de Manin-Grauert. - *Soient k un corps algébriquement clos de caractéristique 0, K un corps de fonctions algébriques sur k (i. e. une extension de type fini de k), et C une courbe algébrique définie sur K et de genre $g \geqslant 2$. Si C a une infinité de points rationnels sur K, alors C est birationnellement équivalente sur K à une courbe C' définie sur k.*

Comme C' a une infinité de points rationnels sur k, ce résultat est le meilleur possible. L'analogue en caractéristique p n'est pas vrai (cf. § 6 pour un contre-exemple), mais on peut dire pas mal de choses. L'algébriste MANIN [4] a donné une démonstration analytique du théorème, en prenant pour k le corps des complexes (d'où le cas général par le "principe de Lefschetz"). L'analyste GRAUERT en donne une démonstration de pure géométrie algébrique, qu'on va exposer ici [1].

Dans un certain sens, le théorème de Manin-Grauert va plus loin que la conjecture de Mordell. En effet, on peut y prendre pour K un corps de degré de transcendance 1 sur k, donc un "corps C_1" au sens de LANG (i. e. tout polynôme homogène sur K, de degré d et à n variables avec $n > d$, a un zéro non-trivial dans K^n), autrement dit un corps sur lequel les équations diophantiennes ont tendance à avoir facilement des solutions. Par contre, le corps $\mathbb{Q}$ est moins "bon" du point de vue diophantien : il n'est pas C_1, et tout ce qu'on peut espérer (par une conjecture lointaine et hardie) c'est qu'il soit à peu près C_2 (i. e. les polynômes homogènes de degré impair avec $n > d^2$ ont des zéros non triviaux dans $\mathbb{Q}^n$, la clause restrictive du degré impair est supprimée de la conjecture analogue pour les corps de nombres totalement imaginaires).

La clef de la démonstration de GRAUERT n'est pas l'inégalité

(1) $$g \geqslant 2 ,$$

mais l'inégalité équivalente

(2) $$2g - 2 > 0 ,$$

qui exprime que les diviseurs canoniques de la courbe C sont amples (cf. § 2).

Pour travailler géométriquement, on utilise le fait qu'une courbe sur un corps de fonctions n'est autre chose qu'une famille algébrique de courbes. On part donc (notations utilisées dans tout l'exposé) d'un corps algébriquement clos k de caractéristique quelconque, d'un corps de fonctions K sur k, et d'une courbe C de genre $g \geqslant 2$ sur K. On suppose que $K(C)$ est une extension régulière de K, hypothèse inoffensive en caractéristique 0 car, pour le théorème, on peut remplacer K par sa fermeture algébrique dans $K(C)$; en caractéristique p, on suppose de plus que C admet un modèle projectif absolument non-singulier, ceci afin d'éviter d'horribles canulars comme l'abaissement du genre par extension du corps de base et d'autres pires encore ! On prend un modèle affine non singulier R de K/k, de point générique r (i. e. $K = k(r)$), et un modèle projectif absolument non singulier de C sur K, de point générique y sur K ($y \in \underset{\sim}{P}_N$) ; on note alors X la sous-variété de $R \times \underset{\sim}{P}_N$ de point générique (r , y) sur k, et π la projection $X \to R$. Ainsi X est "fibrée" par les courbes $X_t = \pi^{-1}(t)$ ($t \in R$), et la fibre générique X_r est la courbe donnée C. Les points rationnels de C sur K correspondent alors aux sections rationnelles de $X \to R$. Nous poserons

(3) $$n = \dim(R) , \qquad \text{d'où } \dim(X) = n + 1 .$$

Une des règles du jeu est que, comme tout se passe au point générique de R, on peut rétrécir R arbitrairement, c'est-à-dire le remplacer par des ouverts (de Zariski, bien entendu, malgré les vertus de la topologie étale) affines convenables. Nous pouvons donc supposer que R et X sont lisses (i. e. non singulières), que π est de rang n en tout point de X (donc lisse lui aussi), et que toutes les fibres X_t ($t \in R$) sont des courbes projectives lisses toutes de même genre g que C (ici interviennent l'hypothèse d'extension régulière, et celle que C est absolument non-singulière). Par contre, on se gardera de rétrécir X dans le sens des fibres ("on caresse les fibrés dans le sens des fibres" !) : il est en effet commode qu'elles soient complètes, et que π soit un morphisme propre.

Un mot enfin sur la terminologie. Contrairement à l'usage grammatical courant où un adjectif restreint son substantif, l'adjectif "rationnel" élargira le domaine d'applicabilité de substantifs tels que "fonction", "application", "section" : une application rationnelle d'une variété V dans une autre W n'est pas une application de V dans W, mais un morphisme d'un ouvert de V dans W (ou encore un germe de morphisme au voisinage du point générique de W). Une application rationnelle peut avoir des points d'indétermination, par exemple $(0, 0)$ pour l'application rationnelle $(x, y) \mapsto y/x$ de k^2 dans $\underset{\sim}{P}_1(k)$.

2. Quelques espaces fibrés.

a. Présentation des acteurs.

Etant donné un espace fibré G de base Y, nous noterons G_y sa fibre au point y de Y, et $G|Y'$ sa restriction à une partie Y' de Y.

Nous désignerons par $T(.)$ le foncteur covariant "fibré des vecteurs tangents". Ainsi la projection $\pi : X \to R$ donne $T(\pi) : T(X) \to T(R)$. La rétrotirette (= "pull back" en "sabir atlantick") de $T(R)$ par $\pi : X \to R$ est un fibré vectoriel sur X, à fibres de dimension n, que nous noterons $\tilde{T}(R)$. Alors $T(\pi)$ donne un morphisme surjectif

$$\alpha : T(X) \to \tilde{T}(R)$$

de fibrés vectoriels sur X.

Une section $s : R \to X$ de π relève les vecteurs tangents de R à X, donc donne, en chaque point t de R, un homomorphisme

$$\beta_t : T(R)_{s(t)} \to T(X)_{s(t)} \qquad \text{tel que} \quad \alpha_{s(t)} \circ \beta_t = 1 .$$

Soit alors F le sous-fibré de $\mathrm{Hom}(T(R), T(X))$ formé des β tels que $\alpha \circ \beta = 1$. La section s définit alors une section $\tilde{s} : R \to F$ de F considéré comme fibré sur R. De même, une section rationnelle $s : R \to X$ définit une section rationnelle $\tilde{s} : R \to F$. Notant θ la projection $\theta : F \to X$, on a évidemment :

$$(4) \qquad \theta \circ \tilde{s} = s .$$

Le fibré F est un fibré affine sur X, à fibres de dimension n. Plongeons F canoniquement dans un fibré projectif $\hat{F}$ de même dimension, et notons

$$F_\infty = \hat{F} - F$$

le fibré des hyperplans à l'infini ; ainsi F_∞ définit un diviseur sur $\hat{F}$, que nous noterons (F_∞) [1]. La restriction du diviseur (F_∞) à la variété F_∞ sera notée N .

Pour $t \in R$, nous noterons F_t , $\hat{F}_t$ et $F_{\infty,t}$ les restrictions des fibrés F , $\hat{F}$, F_∞ à la courbe X_t (notation compatible avec la notation générale à condition de considérer F comme un fibré sur R au moyen de $\pi \circ \theta : F \to R$) ; le diviseur $(F_{\infty,t})$ sur $\hat{F}_t$ est la restriction de (F_∞) à $\hat{F}_t$. Soit $T(X_t)^*$ le fibré cotangent de la courbe X_t , c'est-à-dire le diviseur canonique de X_t ; notons $\tilde{T}_t^*$ sa rétrotirette sur $F_{\infty,t}$. On a d'autre part, sur $F_{\infty,t}$, qui est un fibré sur X_t à fibres $\underset{\sim}{P}_{n-1}$, un diviseur M qui induit sur chaque fibre le diviseur $\underset{\sim}{P}_{n-2}$. On démontre alors sans astuces extraordinaires le lemme suivant.

LEMME 1. - Pour tout $t \in R$, la restriction N_t à $F_{\infty,t}$ du diviseur $(F_{\infty,t})$ ("self intersection") est un diviseur isomorphe à $\tilde{T}_t^* \otimes M$.

On notera que N_t est aussi la restriction à $F_{\infty,t}$ du diviseur $N = (F_\infty)|F_\infty$.

b. Conséquences de l'amplitude.

Rappelons qu'un diviseur D sur une variété normale V est dit ample si, pour tout entier j suffisamment grand, les sections globales $\Gamma(V , D^{\otimes j})$ fournissent un plongement projectif birégulier de V . Si on considère D à l'ancienne, comme une combinaison linéaire de sous-variétés de codimension 1 , le plongement projectif est fourni par une base de l'espace vectoriel $\mathcal{L}(V , jD)$ des fonctions rationnelles f sur V telles que $(f) \geqslant - jD$. Sur une courbe, tout diviseur $D > 0$ est ample, de sorte que le diviseur canonique $T(X_t)^*$ est ample, car on a

$$2g - 2 > 0 .$$

On en déduit que $\tilde{T}_t^*$, et donc N_t par le lemme 1 (N. B. : on a $M > 0$), est un diviseur ample sur $F_{\infty,t}$.

Soient t un point générique de R sur k , et j un entier grand. A l'ancienne, le diviseur jN_t sur $F_{\infty,t}$ est induit sur $F_{\infty,t}$ par un diviseur $jF_{\infty,t} - (h)$ de $\hat{F}_t$, linéairement équivalent à $jF_{\infty,t}$ et sans composantes $F_{\infty,t}$; ainsi h est une fonction sur $\hat{F}_t$, nulle d'ordre j sur $F_{\infty,t}$. Soit $(u_1', \dots, u_r')$ une base de $\mathcal{L}(F_{\infty,t} , - jN_t)$, définie sur $k(t)$, fournissant un plongement $F_{\infty,t} \to P_{r-1}$, car j est grand. Les fonctions u_i' sont induites sur $F_{\infty,t}$ par des fonctions u_i sur $\hat{F}_t$, définies sur $k(t)$; vu l'amplitude, on a

---

[1] Nous identifions ici les diviseurs sur une variété (i. e. les combinaisons linéaires de sous-variétés de codimension 1), ou plutôt leurs classes de diviseurs, avec les fibrés vectoriels à fibres de dimension 1 qui leurs sont classiquement associés.

$$H^1(F_{\infty,t}\ ,\ N_t) = 0 \qquad \text{pour } j \text{ grand ,}$$

et on peut donc supposer que les u_i appartiennent à $\mathcal{L}(\hat{F}_t\ ,\ (h) - jF_{\infty,t})$. Alors $(h\ ,\ u_1\ ,\ \dots\ ,\ u_r)$ fournit un morphisme birationnel $g\ :\ \hat{F}_t \to P_r$ tel que :

1° g applique birégulièrement $F_{\infty,t}$ dans l'hyperplan à l'infini P_{r-1} ;

2° g applique $F_t = \hat{F}_t - F_{\infty,t}$ dans $P_r - P_{r-1}$ (en effet on a $(u_i/h) \geqslant -jF_{\infty,t}$).

Considérons maintenant l'application rationnelle $f\ :\ \hat{F} \to P_r$ définie sur k et dont la restriction à la fibre générique $\hat{F}_t$ est g . En rétrécissant R , on peut supposer que, pour tout $t' \in R$, la restriction $f|\hat{F}_{t'}$ jouit des mêmes propriétés 1° et 2° que g .

On a donc :

LEMME 2.

α. $f(F_\infty)$ <u>est contenu dans l'hyperplan à l'infini</u> H <u>de</u> $\underset{\sim}{P}_r$ (i. e. $X_0 = 0$), <u>et</u> f <u>est birégulière sur chaque</u> $F_{\infty,t}$;

β. <u>on a</u> $f(F) \subset \underset{\sim}{P}_r - H = k^r$;

γ. <u>l'application</u> $\varphi = (\pi\theta) \times (f|F)\ :\ F \to R \times k^r$ <u>est un morphisme propre et birationnel de fibrés sur</u> R .

3. L'ensemble d'éclatement E .

a. Définition des ensembles d'éclatement, et énoncé d'un théorème.

DÉFINITION. - <u>Etant données deux variétés algébriques</u> Y , Z <u>et un morphisme birationnel</u> $g\ :\ Y \to Z$, <u>on appelle ensemble d'éclatement de</u> g , <u>et on note</u> $E(g)$, <u>l'ensemble des points</u> y <u>de</u> Y <u>tels que</u> $\dim_y g^{-1}(g(y)) > 0$.

ZARISKI a montré que $E(g)$ est un <u>fermé</u> de Y . On a évidemment $\dim_y E(g) > 0$ en tout point y de $E(g)$.

Nous noterons E l'ensemble d'éclatement du morphisme

$$\varphi = (\pi\theta) \times (f|F)\ :\ F \to R \times k^r$$

défini à la fin du § 2. A cause du facteur $\pi\theta$, " φ n'éclate que dans le sens des fibres". Donc, pour tout $t \in R$, $E_t = E \cap F_t$ est l'ensemble d'éclatement de $f|F_t$, et aussi de $f|\hat{F}_t$ car f est birégulière sur $F_{\infty,t}$ (§ 2, lemme 2, α et β). Donc E_t est <u>complet</u>.

Nous allons démontrer le théorème suivant :

THÉORÈME 1. – S'il existe une infinité de sections rationnelles s de X telles que $\tilde{s}(R) \subset E$, alors E est une section du fibré $\theta : F \to X$.

L'existence d'une section rationnelle s telle que $\tilde{s}(R) \subset E$ implique, en rétrécissant éventuellement R, qu'on a $E_t \neq \emptyset$ pour tout $t \in R$ (il contient $\tilde{s}(t)$).

b. Les parties complètes maximales.

On va commencer la démonstration du théorème 1 par le lemme suivant :

LEMME 3. – Sous l'hypothèse du théorème 1 et pour tout $x \in X_t$, il existe un point e de E_t ; et un seul, tel que $\theta(e) = x$ (on a $e \neq 2,71828\ldots$).

On sait, en effet, que $\theta|E : E \to X$ et $f|F_t : F_t \to k^r$ sont des morphismes propres. Donc $f(E_t)$ est une partie fermée complète de k^r, donc finie. De même, pour toute partie fermée complète irréductible A de dimension > 0 de F_t, $f(A)$ est un point de k^r ; on a donc $A \subset E_t$, car E_t est l'ensemble d'éclatement de $f|F_t$. Nous exprimerons ce fait en disant que E_t est la partie complète maximale de F_t.

Soit maintenant S le fibré vectoriel sur X_t correspondant au fibré affine $F_t = F|X_t$ (i. e. son "fibré des translations"). Avec les notations du § 2 (a), on a

$$S = \mathrm{Hom}(\tilde{T}(R)|X_t , T(X_t)) , \tag{5}$$

car $T(X_t)$ est le noyau de $\alpha|X_t$. Le fibré dual S^* est $(\tilde{T}(R)|X_t) \otimes T(X_t)^*$, et est donc ample (au sens des fibrés vectoriels) car $2g - 2 > 0$. Le critère d'amplitude de Grauert ([2], p. 182) montre alors qu'on a un morphisme birationnel propre g de S sur une variété affine S', birégulier en dehors de la section nulle S_o, et tel que $g(S_o)$ soit un point de S'. Ainsi S_o est l'ensemble d'éclatement de g, et aussi la partie complète maximale de S.

Considérons alors le morphisme $u = \theta|E_t : E_t \to X_t$, et la rétrotirette G de F_t par u :

$$\begin{tikzcd} G \arrow[r, "v"] \arrow[d, "\psi"'] & F_t \arrow[d, "\theta"] \\ E_t \arrow[r, "u"] & X_t \end{tikzcd} .$$

Alors G est un fibré affine sur E_t, et $e \mapsto \psi^{-1}(e) \cap v^{-1}(e)$ (l'application diagonale du produit fibré de E_t par E_t sur X_t) est une section de G , dont nous noterons G_o l'image. Celle-ci munit G d'une structure de fibré vectoriel sur E_t , et l'identifie à la rétrotirette $u^*(S)$ de S . Le morphisme de fibrés vectoriels $G \to S$ (au-dessus de u) applique G_o dans S_o , de sorte que G_o est la partie complète maximale de G . Or $v^{-1}(E_t)$ est complet (car c'est le produit fibré de E_t par lui-même sur X_t), et contient G_o . On a donc

$$v^{-1}(E_t) = G_o ,$$

de sorte que ce produit fibré a au plus un point au-dessus de chaque point de X_t. D'où la même conclusion pour E_t , de sorte que $\theta|E_t$ est injective. Comme $E_t \neq \emptyset$ et que $\dim(E_t) > 0$, on a $\theta(E_t) = X_t$ (vu que X_t est irréductible de dimension 1).

C. Q. F. D.

c. Fin de la démonstration.

Nous venons de voir (lemme 3) que $\theta|E : E \to X$ est un morphisme bijectif. L'application réciproque $\rho : X \to E$ est donc "radicielle". Elle est par conséquent birationnelle en caractéristique 0 , donc birégulière par le "main theorem" (LANG, [3], p. 124) car X est normale. D'où le théorème 1.

En caractéristique $p \neq 0$, on se fatigue un peu plus, et on utilise un plus gros morceau de l'hypothèse sur l'infinité de sections rationnelles s telles que $\tilde{s}(R) \subset E$. Soient R' et $X' \subset \pi^{-1}(R)$ des ouverts affines de R et de X , assez petits pour qu'on ait n champs de vecteurs $\xi_1 , \dots , \xi_n$ linéairement indépendants sur R' , pour que $F' = F|X'$ s'identifie à $X' \times k^n$, et pour que la trace de E dans $X' \times k^n$ soit définie par des équations

$$y_j^{p(j)} + b_j(x) = 0 \qquad (j = 1 , \dots , n) \tag{6}$$

où x désigne les coordonnées sur X' , (y_j) celles sur k^n , et $p(j)$ une puissance de p , et où $b_j(x)$ n'est pas une puissance p-ième sur X' . Supposons, par l'absurde, que $p(1) \neq 1$.

Un point (x , y) de $X' \times k^n = F'$ correspond, par définition du fibré F (cf. § 2, (a)), à un homomorphisme $T(R)_t \to T(X)_x$ (où $t = \pi(x)$), qu'on va noter y^o. Posons

$$f_{ij}(x , y) = \langle db_i , y^o(\xi_j(t))\rangle$$

(dualité entre vecteurs tangents et différentielles). Notons que $f_{ij}(x , y)$ est linéaire en y . Soit $A \subset F'$ défini par les équations

$$f_{11}(x\ ,\ y) = \ldots = f_{1n}(x\ ,\ y) = 0\ .$$

Comme $b_1(x)$ n'est pas une puissance p-ième, on a $db_1 \neq 0$, et il y a un seul point de A au-dessus du point générique de X' ; vu la linéarité de A par rapport à y , ceci montre que la projection $A \to X$ est birationnelle.

Soit $s : R \to X$ une section rationnelle telle que $\tilde{s}(R) \subset E$. Comme $y_1^{p(1)} + b_1$ s'annule sur $\tilde{s}(R)$, on a

$$d((y_1^{p(1)} + b_1) \circ \tilde{s}) = 0\ ,$$

d'où

$$d(b_1 \circ \tilde{s}) = d(b_1 \circ s) = 0 \qquad \text{(cf. § 2, équation (4))}$$

car on a supposé $p(1) \neq 1$. On a donc $\tilde{s}(R) \cap F' \subset A$. Ainsi A contient les germes d'une infinité de sous-variétés de codimension 1 de E , à savoir les $\tilde{s}(R)$. Comme A est fermé dans F' , on en déduit $E \cap F' \subset A$, d'où $E \cap F' = A$, car ce sont des variétés irréductibles de même dimension $n + 1$. Vu la linéarité de A par rapport à y , ρ est donc birationnelle, et par conséquent birégulière par le "main theorem".

C. Q. F. D.

4. Les sections s de X telles que $\tilde{s}(R) \not\subset E$.

Nous allons ici démontrer le théorème suivant :

THÉORÈME 2. - L'ensemble Σ des sections rationnelles s de X telles que $\tilde{s}(R) \not\subset E$ est fini.

Rappelons (§ 2, (a)) qu'une section rationnelle $s : R \to X$ définit une section rationnelle $\tilde{s} : R \to F$, et qu'on a un morphisme birationnel propre $\varphi : F \to R \times k^r$ (§ 2, (b), lemme 2), dont E est l'ensemble d'éclatement (§ 3, (a)). Comme R est une variété affine, on a un plongement $R \to k^{r'}$, et l'on peut considérer φ comme un morphisme

$$\varphi : F \to k^m \quad (m = r + r')\ . \tag{7}$$

Quitte à changer m , on peut normaliser $\varphi(F)$, et supposer $\varphi(F)$ normale ; ceci ne change pas l'ensemble d'éclatement E .

Comme les fibres X_t $(t \in R)$ sont complètes, l'ensemble I des points d'indétermination d'une section rationnelle $s : R \to X$ est de codimension $\geqslant 2$, et c'est le même pour $\tilde{s}$. Posons

(8) $$s^{o} = \varphi \circ \tilde{s} : R \to k^{m} ;$$

c'est un m-uple de fonctions rationnelles $R \to k$, régulières sur $R - I$, donc sans pôles (car codim $I \geqslant 2$), donc régulières. Ainsi s^{o} est un élément de l'espace vectoriel $\mathrm{mor}(R , k^{m})$ des morphismes de R dans k^{m} .

LEMME 4. - <u>L'application</u> $s \mapsto s^{o}$ <u>de</u> Σ <u>dans</u> $\mathrm{mor}(R , k^{m})$ <u>est injective</u>.

En effet, soient s , s' deux éléments distincts de Σ , et r un point générique de R . Alors $\tilde{s}(r)$ et $\tilde{s}'(r)$ sont des points de $F - E$, et sont distincts, car

$$\theta(\tilde{s}(r)) = s(r) \neq s'(r) = \theta(\tilde{s}'(r)) .$$

Reste à montrer que φ est injective (et même birégulière) sur $F - E$; or ceci résulte de la définition de E comme ensemble d'éclatement et de la normalité de $\varphi(F)$ en vertu du "main theorem".

LEMME 5. - <u>Les</u> s^{o} <u>(pour</u> $s \in \Sigma$) <u>engendrent un sous-espace vectoriel</u> V <u>de dimension finie de</u> $\mathrm{mor}(R , k^{m})$.

Soit $\bar{R}$ une clôture projective normale de R ; posons $R_{\infty} = \bar{R} - R$. On peut plonger F dans un $R \times \underset{\sim}{P}_{N} \subset \bar{R} \times \underset{\sim}{P}_{N}$; soient $\bar{F}$ l'adhérence de F dans $\bar{R} \times \underset{\sim}{P}_{N}$, $F_{\infty} = (R_{\infty} \times \underset{\sim}{P}_{N}) \cap \bar{F}$, et $\bar{\varphi}$ le prolongement de φ à $\bar{F}$. C'est une application rationnelle $\bar{F} \to k^{m}$, qui peut avoir des pôles sur F_{∞} ; mais il existe une fonction rationnelle $h \neq 0$ sur $\bar{R}$, nulle sur R_{∞} , telle que $(h \circ \mathrm{pr}_{\bar{R}})\bar{\varphi}$ soit régulière sur F_{∞} . Alors $hs^{o} = (h \circ \mathrm{pr}_{\bar{R}})\bar{\varphi} \circ \tilde{s}$ est régulière sur R_{∞} . Donc les fonctions rationnelles (sur $\bar{R}$), qui forment le m-uple s^{o} , n'ont de pôles que sur R_{∞} , et pas pires que ceux de la fonction fixe $1/h$. D'où le lemme 5 par un théorème classique de finitude.

LEMME 6. - <u>L'ensemble</u> V' <u>des</u> s <u>(pour</u> $s \in \Sigma$) <u>est, soit un fermé de</u> V , <u>soit un fermé de</u> V <u>moins un point</u>.

Notons d'abord que, comme chaque E_{t} non vide est complet et irréductible (§ 3, lemme 3), $\varphi(E_{t})$ est réduit à un point. Donc, si $\pi\theta(E) = R$, $t \mapsto \varphi(E_{t})$ est une application w de R dans k^{m} . On peut avoir (ou ne pas avoir) $w \in V$.

Pour tout t de R , l'ensemble A_{t} des $v \in V$ ($\subset \mathrm{mor}(R , k^{m})$) tels que $v(t) \in \varphi(F_{t})$ est un fermé car φ est propre, et donc $\varphi(F_{t})$ est fermé. Soit $A = \bigcap_{t \in R} A_{t}$, qui est <u>fermé</u> dans V . Pour $v \in A$, $v \neq w$, et pour un point générique r de R , on a $v(r) \in \varphi(F_{r})$, $v(r) \notin \varphi(E_{r})$; or, on a vu au lemme 4 que

φ est birégulière sur $F - E$; il existe donc un élément z de F_r, et un seul, rationnel sur $k(v, r)$, tel que $v(t) = \varphi(z)$; soit v' la section rationnelle de $F \to R$ définie par $v'(r) = z$. Alors $\theta \circ v'$ est une section rationnelle de $X \to R$. L'ensemble V'' des $v \in A - \{w\}$ (si $w \notin A$, $A - \{w\}$ veut dire A) tels que $\widetilde{\theta \circ v'} = v'$ est <u>fermé</u> dans $A - \{w\}$, car la relation $\widetilde{\theta \circ v'} = v'$ est "algébrique" en v. On a $V'' \subset V'$ car, pour $v \in V''$ et r générique sur R, on a

$$(\theta \circ v')^{o}\ (r) = \varphi(v'(r)) = v(r)\ ,$$

d'où $v = (\theta \circ v')^{o}$. D'autre part, il est clair que $V' \subset V''$. D'où $V' = V''$.

C. Q. F. D.

LEMME 7. - <u>L'ensemble</u> V' <u>du lemme</u> 6 <u>est fini</u>.

Sinon, en effet, V' contiendrait une courbe affine non singulière Q. Considérons l'application $g : R \times Q \to X$ définie par $g(t, s^{o}) = s(t)$; alors $\pi \circ g$ est la première projection $R \times Q \to R$; d'autre part, l'ensemble des points d'indétermination de g ne contient aucune verticale $R \times \{v\}$ $(v \in Q)$. Plongeons Q dans une courbe complète non singulière $\bar{Q}$; comme les fibres de $\pi : X \to R$ sont complètes, g se prolonge en $\bar{g} : R \times \bar{Q} \to X$. Pour tout $q \in \bar{Q}$, l'application $t \mapsto \bar{g}(t, q)$ est une section rationnelle s_q de $X \to R$; ainsi, $(t, q) \mapsto s_q^{o}(t)$ est un m-uple de fonctions régulières sur $R \times \bar{Q}$. Comme $\bar{Q}$ est complète, s_q^{o} est indépendant de q, ce qui est absurde car $s_q^{o} = q$ (par construction) pour tout $q \in Q$.

C. Q. F. D.

Le théorème 2 résulte aussitôt des lemmes 4 et 7.

Avant de passer à la démonstration finale du théorème de Manin-Grauert, voici une remarque importante. La section E du fibré affine $F \to X$ s'interprète, par définition de F (§ 2, (a)), comme <u>un champ de sections infinitésimales de</u> $X \to R$, i. e. comme un champ de n-plans tangents à X et partout transversaux aux fibres X_t de X. Vu que E_t est la partie complète maximale de $F|X_t$, et qu'une section de $F|X_t \to X_t$ a une image complète dans $F|X_t$ (pour tout $t \in R$), E est l'<u>unique section</u> de $F \to X$ (ça se voit aussi en remarquant que le fibré vectoriel S des translations de $F|X_t$, défini au § 3 ((b), équation (5)), n'a d'autre section que la section nulle, vu que son dual est ample). Déduisons-en aussitôt un théorème classique et utile :

THÉORÈME 3. - Une courbe de genre $g \geqslant 2$ n'a qu'un nombre fini d'automorphismes. En caractéristique 0, elle n'a qu'un nombre fini d'applications rationnelles non constantes dans elle-même.

En effet, appelons cette courbe R, et posons $X = R \times R$. Les applications rationnelles de R dans R ne sont autres que les sections rationnelles de la première projection $X \to R$. Vu son unicité, le champ E n'est autre que le champ "horizontal" de $R \times R$. D'après le théorème 2, presque toutes les applications rationnelles $R \to R$ sont tangentes à ce champ, donc (en coordonnées affines) ont leur dérivée nulle. Elles sont donc constantes en caractéristique 0. En caractéristique p, un automorphisme de R ne peut avoir sa dérivée nulle (sinon l'automorphisme correspondant du corps de fonctions $k(R)$ appliquerait $k(R)$ dans $k(R^p)$).

C. Q. F. D.

5. Démonstration du théorème de Manin-Grauert.

THÉORÈME 4. - Soient p la caractéristique de k, et r un point générique de R sur k. On suppose que la courbe $C = X_r$ a une infinité de points rationnels sur $k(r)$. On plonge X_r "multicanoniquement" dans $\mathbb{P}_N$ (i. e. au moyen d'un multiple assez grand $j\mathfrak{b}$ d'un diviseur canonique $\mathfrak{b}$ de X_r). Alors, il existe un élément α de $\mathrm{PGL}(N, k(r))$ tel que la courbe $\alpha(X_r)$ soit définie sur $k(r^p)$ et ait une infinité de points rationnels sur ce corps.

Notons bien que p est la caractéristique de k, et non son exposant caractéristique ; ainsi pour $p = 0$, on a $r^p = 1$ et $k(r^p) = k$. Donc, le théorème 4 entraîne le théorème de Manin-Grauert pour $p = 0$. Le corps $k(r^p)$ va intervenir comme étant l'intersection des noyaux des k-dérivations de $k(r)$. En caractéristique $p \neq 0$, on obtient aussitôt le corollaire suivant par récurrence :

COROLLAIRE. - Avec les mêmes hypothèses et notations qu'au théorème 4, et pour tout $q \geqslant 0$, il existe $\alpha_q \in \mathrm{PGL}(N, k(r))$ tel que $\alpha_q(X_r)$ soit définie sur $k(r^{p^q})$ et ait une infinité de points rationnels sur ce corps.

a. Réduction du théorème 4 à un lemme.

On suppose X_r plongée multicanoniquement dans $\mathbb{P}_N$ (i. e. au moyen d'une base de $L(-j\mathfrak{b})$). D'après les théorèmes 2 et 3 on a un "champ de sections infinitésimales E" du fibré en courbes $X \to R$, et une infinité de sections rationnelles s de X sont tangentes à E (i. e. $\tilde{s}(R) \subset E$). Parmi ces dernières il y en a

$N+1$, soient s_i $(i = 0 , \ldots , N)$, telles que les points $s_i(r)$ de X_r soient à distance finie dans $\underset{\sim}{P}_N$ et affinement indépendants. Soit α la transformation affine (i. e. laissant l'hyperplan à l'infini invariant) de $\underset{\sim}{P}_N$ qui les envoie aux points $(1 , 0 , \ldots , 0)$, $(1 , 1 , 0 , \ldots , 0)$, ... , $(1 , 0 , \ldots , 0 , 1)$. Remplaçant X_r par sa transformée $\alpha(X_r)$, on voit que le plongement de X_r dans $\underset{\sim}{P}_N$ se fait maintenant au moyen d'une base $(1 , x_1 , \ldots , x_N)$ de $L(-j\mathfrak{b})$ (sur $k(r)$) telle que

$$x_i(s_j(r)) = \delta_{ij} \qquad (j = 0 , 1 , \ldots , N ; \ i = 1 , \ldots , N) . \tag{9}$$

On peut considérer les x_i comme des fonctions rationnelles sur le fibré X (elles sont cette fois définies sur k), d'où une application rationnelle

$$X \to R \times \underset{\sim}{P}_N .$$

En rétrécissant R , on peut supposer que c'est un plongement et que, pour tout $t \in R$, X_t est une courbe irréductible de même genre g que X_r , et que la seconde projection $X_t \to \underset{\sim}{P}_N$ est un plongement multicanonique.

Le champ E relève les vecteurs tangents à R en vecteurs tangents à X . En particulier, il prolonge toute k-dérivation D de $K = k(R) = k(r)$ en une k-dérivation D_E de $k(X) = k(r , x_1 , \ldots , x_N)$. Nous démontrerons un peu plus tard le lemme suivant :

LEMME 7. - <u>Pour toute</u> k-<u>dérivation</u> D <u>de</u> $k(R)$, <u>on a</u> $D_E(x_i) = 0$ $(i = 1 , \ldots , N)$.

Voyons comment le lemme 7 implique le théorème 4. Par un résultat "classique" à la délicieuse odeur de coordonnées de Chow, l'idéal de X_r (sur K) est engendré par les équations d'un suffisamment grand nombre de projections planes de X_r . Soient U et V deux combinaisons linéaires des coordonnées dans $\underset{\sim}{P}_N$, à coefficients <u>dans le petit corps</u> k , et u et v les combinaisons linéaires correspondantes de $1 , x_1 , \ldots , x_N$; soit

$$F(U , V) = \sum_{i,j} a_{ij} U^i V^j$$

l'équation minimale vérifiée par (u , v) sur $K = k(r)$ (de sorte que l'idéal de X_r est engendré par les homogénéisés des $F(U , V)$). Etant donnée une dérivation D de $K = k(r)$, appliquons D_E à $F(u , v) = 0$; comme $D_E u = D_E v = 0$, il vient

$$\sum_{i,j} (Da_{ij}) u^i v^j = 0 ;$$

il s'ensuit qu'il existe c dans K tel que $Da_{ij} = ca_{ij}$ pour tous i, j. Comme on peut supposer que l'un des a_{ij} est égal à 1, on a $c = 0$, d'où

$$Da_{ij} = 0 .$$

Ceci ayant lieu pour toute k-dérivation D de $k(r)$, on a $a_{ij} \in k(r^p)$, de sorte que X_r est définie sur $k(r^p)$.

D'autre part, on a une infinité de sections s tangentes à E et telles que $s(r)$ soit à distance finie sur X_r. Le contact de s et E implique qu'on a $D(x_i(s(r))) = (D_E\, x_i)(s(r))$ pour toute k-dérivation D de $k(r)$, et ceci est nul par le lemme 7. Comme les $x_i(s(r))$ sont les coordonnées affines du point $s(r)$, ce point est bien rationnel sur $k(r^p)$. Ceci démontre le théorème 4.

b. Démonstration du lemme 7.

Soit D une k-dérivation de $k(r)$. Il suffit de montrer que la restriction de la fonction $D_E\, x_i$ à chaque courbe X_t $(t \in R_k)$ est nulle. Soient $t \in R_k$, A l'anneau local de t sur R, et $\mathfrak{m}$ son idéal maximal. Vu que $D \mapsto D_E$ est K-linéaire, on peut supposer que D est une dérivation de A. Vu le caractère local de E, D_E est alors une dérivation de $B = A[x_1, \dots, x_N]$. En notant h l'homomorphisme canonique de B sur $B/\mathfrak{m}B$ (i. e. sur l'anneau affine de X_t), il suffit de montrer qu'on a $h(D_E\, x_i) = 0$. Or, $h \circ D_E$ est une dérivation $B \to B/\mathfrak{m}B$, et prolonge la dérivation $h \circ D : A \to A/\mathfrak{m} = k$. D'autre part,

$$(B/\mathfrak{m}B) \otimes_B \Omega_k(B)$$

est universel pour les dérivations de B dans les $(B/\mathfrak{m}B)$-modules, et

$$(A/\mathfrak{m}) \otimes_A \Omega_k(A) = \mathfrak{m}/\mathfrak{m}^2$$

est universel pour les dérivations de A dans les k-modules. Comme les premières s'annulent sur $\mathfrak{m}^2 B$, on a une dérivation

$$\Delta' : B/\mathfrak{m}^2 B \to (B/\mathfrak{m}B) \otimes_B \Omega_k(B) = (A/\mathfrak{m}) \otimes_A \Omega_k(B) . \tag{10}$$

Or la transposée ${}^tE$ de E "rétracte" les différentielles de X sur celles de R, d'où

$$B \otimes_A \Omega_k(A) \to \Omega_k(B) \xrightarrow{{}^tE} B \otimes_A \Omega_k(A) \tag{11}$$

où la première flèche est canonique et où la composée est l'identité. Comme

$$(A/\mathfrak{m}) \otimes_A (B \otimes_A \Omega_k(A)) = (\mathfrak{m}/\mathfrak{m}^2) \otimes_A B = \mathfrak{m}B/\mathfrak{m}^2 B ,$$

$(1_{A/m} \otimes {}^t E) \circ \Delta'$ est une dérivation Δ :

(12) $$\Delta : B/m^2 B \to mB/m^2 B ;$$

celle-ci prolonge la dérivation canonique $A/m^2 \to m/m^2$ (de noyau k). Il est clair que $h \circ D_E$ est composée de Δ et d'une application linéaire. Il suffit donc de montrer qu'on a $\Delta(x''_i) = 0$ pour tout i , si, pour $z \in B$, on convient de noter z'' (resp. z') la classe de $z \bmod m^2 B$ (resp. mB).

Or $\mathrm{Ker}(\Delta)$ est un <u>sous-anneau</u> de $B/m^2 B$, canoniquement isomorphe à

$$B/mB = k[x'_1 , \dots , x'_N] ,$$

et on a

(13) $$B/m^2 B \simeq (A/m^2) \otimes_k \mathrm{Ker}(\Delta) \simeq (A/m^2) \otimes_k k[x'_1 , \dots , x'_N] .$$

En notant z''_i l'élément de $B/m^2 B$ correspondant à $1 \otimes x'_i$ par cet isomorphisme, on a $\Delta(z''_i) = 0$.

Exprimons (13) géométriquement. Soit $X(t)$ le voisinage de X_t sur X , c'est-à-dire le A-schéma $\mathrm{Proj}(A[T , x_1 T , \dots , x_N T])$. D'après (13) (et ses analogues sur les autres morceaux affines), le voisinage infinitésimal du premier ordre $(A/m^2) \otimes X(t)$ est isomorphe au <u>produit</u> $\mathrm{Spec}(A/m^2) \times X_t$ (pas étonnant, E étant un champ de sections infinitésimales de $X \to R$). Ainsi, les systèmes

$$(1 , x''_1 , \dots , x''_N) \qquad \text{et} \qquad (1 , z''_1 , \dots , z''_N)$$

fournissent tous deux des plongements multicanoniqués (i. e. par une puissance du fibré cotangent) de la "courbe à éléments nilpotents"

$$(A/m^2) \otimes X(t) \simeq \mathrm{Spec}(A/m^2) \times X_t .$$

Ils engendrent donc le même (A/m^2)-module, de sorte qu'il existe des éléments b_i , a_{iq} de A/m^2 tels que

(14) $$x''_i = b_i + \sum_q a_{iq} z''_q .$$

Or, une section s tangente à E (et telle que $s(t)$ soit à distance finie) définit un homomorphisme $s'' : B/m^2 B \to A/m^2$ tel que $s'' \circ \Delta = \Delta \circ s''$. Pour les sections constantes s_j définies plus haut, on a

$$s''_j(x''_i) = \delta_{ij} \qquad \text{et} \qquad s''_j(z''_q) \equiv \delta_{iq} \qquad (\mathrm{mod}\ mB/m^2 B) .$$

On applique $s''_j \circ \Delta$ à (14), et un petit calcul montre qu'on a $\Delta b_i = \Delta a_{iq} = 0$, d'où b_i, $a_{iq} \in k$, et $\Delta x''_i = 0$.

C. Q. F. D.

Remarque. - Vu les hypothèses faites dans (b), § 1, X_r est encore un modèle multicanonique sur $k(r^p)$, ce qui justifie le corollaire. Avec $k(r^p)$ au lieu de $k(r)$, la base R, le fibré X et le champ E sont changés en R', X' et E'. Mais il n'y a aucune raison pour que les sections constantes s_j (qui sont maintenant des sections de $X' \to R'$) soient tangentes au champ E', ce qui force à soumettre X_r à une nouvelle transformation projective afin de la descendre à $k(r^{p^2})$.

6. Le cas de caractéristique p.

a. Utilisation de la théorie des modules.

Dans ce qui suit, K désigne un corps de fonctions sur un corps algébriquement clos k de caractéristique p, et C une courbe de genre $g \geqslant 2$ sur K, absolument non singulière, et admettant une infinité de points rationnels sur K. Le corollaire du théorème 3 nous dit que, pour tout $q \geqslant 0$, C est birationnellement équivalente sur K à une courbe C_q définie sur K^{p^q}. Or, la théorie des modules (cf. MUMFORD) nous dit qu'il existe une application m de "l'ensemble" U des courbes de genre g donné sur une variété algébrique M (la "variété des modules" ; elle est définie sur la clôture algébrique du corps premier, donc sur k) telle que :

α. pour que C', $C'' \in U$ soient birationnellement équivalentes, il faut et il suffit que $m(C') = m(C'')$;

β. pour toute courbe $C' \in U$, le point $m(C')$ est rationnel sur $k(C')$.

Il s'ensuit que le point $m(C)$ est rationnel sur $\bigcap_{q=0}^{\infty} K^{p^q} = k$. Donc C est birationnellement équivalente à une courbe C_0 définie sur k. Mais, comme la théorie des modules est une théorie "géométrique", on peut seulement dire qu'il y a une correspondance birationnelle $h : C_0 \to C$ définie sur la clôture algébrique de K. Naturellement, h est alors définie sur une extension algébrique finie K' de K.

b. Où l'on rend séparable l'extension K'.

Soit K_s la fermeture séparable de K dans K'. Par récurrence sur la hauteur de l'extension radicielle K'/K_s , on est ramené à démontrer que, si K_1 est un corps intermédiaire entre K_s et K' tel que $K'^p \subset K_1$, alors il existe une correspondance birationnelle $C_o \to C$ définie sur K_1 . Soit $h : C_o \to C$ une correspondance birationnelle définie sur K' . Soient R' un modèle affine non singulier de K'/k , et $X' = R' \times C_o$; d'après la fin du § 4, le champ "horizontal" E' sur X' est l'unique champ de sections infinitésimales de $X' \to R'$. Or on a une infinité de points P de C rationnels sur K ; les points correspondants $h^{-1}(P)$ (sur $(C_o)_{K'}$) définissent des sections rationnelles $s_P : R' \to X'$. D'après le théorème 2 du § 4 appliqué à X' , presque toutes ces sections s_P sont tangentes au champ horizontal E' , donc ont leurs dérivées nulles ; ceci signifie que, pour presque tout $P \in C_K$, le point $h^{-1}(P)$ est rationnel sur K'^p , donc sur K_1 .

On peut supposer C et C_o plongées dans un $\underset{\sim}{P}_N$ par des plongements multicanoniques de même degré (cf. § 5) ; alors les correspondances birationnelles $C_o \to C$ sont induites par des transformations projectives. Dans l'infinité de points de C_K , on peut en trouver $N + 2$, soient P_i $(i = 0 , \ldots , N + 1)$, qui forment un repère projectif, et tels que les $h^{-1}(P_i)$ soient rationnels sur K_1 . Alors la transformation projective u définie par $u(P_i) = h^{-1}(P_i)$ amène C sur C_o (et ne diffère de h^{-1} que par un automorphisme de C_o). Comme u est définie sur K_1 , on a gagné.

c. Où l'on voit que C s'obtient en tordant une courbe "constante" par un groupe de Galois.

En changeant un peu les notations, nous venons de voir qu'on a une correspondance birationnelle $h : C_o \to C$ définie sur une extension séparable finie de K , donc aussi sur une extension galoisienne finie K' de K . Soit G le groupe de Galois de K'/K . Pour $g \in G$, la correspondance conjuguée h^g (considérée, par exemple, comme sous-variété de $C_o \times C$) est encore birationnelle. Ainsi $h^{-1} h^g$ est un automorphisme de la courbe C_o , et $g \mapsto h^{-1} h^g$ est un homomorphisme de G dans $\mathrm{Aut}(C_o)$. Soit G^o son noyau ; pour $g \in G^o$, on a $h^g = h$, de sorte que h est rationnelle sur le corps des invariants de G^o . Remplaçant K' par ce corps des invariants (qui est encore galoisien sur K), on peut supposer que l'homomorphisme $G \to \mathrm{Aut}(C_o)$ est injectif. Remarquons que $\mathrm{Aut}(C_o)$ est fini (§ 4, théorème 3), de sorte que ses éléments sont définis sur le petit corps algébriquement clos k . Donc C s'obtient à partir de C_o par descente galoisienne du corps de base de K' à K au moyen de $G \to \mathrm{Aut}(C_o)$; c'est une situation classique, décrite dans SERRE ([5], chap. V, § 4, n° 20). Notons que, si $\mathrm{Aut}(C_o)$

(= Aut(C)) est trivial, on a $K' = K$, et C est birationnellement équivalente à C_o sur K.

En termes de fibrés en courbes, les choses s'expriment ainsi. Soit R' un modèle affine non singulier de K'/k. Alors, le groupe de Galois G opère sur R', et aussi sur C_o au moyen de l'homomorphisme $i : G \to \mathrm{Aut}(C_o)$. Il opère donc sur $R' \times X_o$ par

$$g(r', x) = (g(r'), ig(x)) .$$

Alors le fibré X (sur R') n'est autre que $(R' \times X_o)/G$.

d. Une réciproque.

PROPOSITION. - Soient Y_o une variété projective (ou une sous-variété localement fermée d'un espace projectif) définie sur k, K un corps de fonctions sur k, K' une extension galoisienne finie de K, G son groupe de Galois, et $i : G \to \mathrm{Aut}(Y_o)_k$ un monomorphisme. Notons Y la variété obtenue en descendant Y_o de K' à K au moyen des $i(g)$ $(g \in G)$. Alors, pour tout $j \geqslant 0$, Y est birégulièrement équivalente sur K à une variété Y_j définie sur K^{p^j}.

Notons d'abord que Y existe en vertu de SERRE, loco citato. Posons $q = p^j$. Par transport de structure au moyen de $x \mapsto x^q$, on a un isomorphisme canonique v de G sur le groupe de Galois G_q de K'^q sur K^q (c'est l'application de restriction). Soit Y_j la variété obtenue en descendant Y_o de K'^q à K^q au moyen des $iv^{-1}(g')$ $(g' \in G_q)$; notons que, par hypothèse, les $i(g)$ $(g \in G)$, et donc les $iv^{-1}(g')$ $(g' \in G_q)$, sont des automorphismes de Y_o définis sur k, donc aussi sur K'^q, ce qui donne un sens à notre descente. Comme les mêmes automorphismes $i(g)$ $(g \in G)$ de Y_o sont utilisés dans les deux descentes, Y_j est aussi obtenue par descente de K' à K. D'après l'unicité de la descente (SERRE, loco citato), Y_j est K-isomorphe à Y.

C. Q. F. D.

e. Un contre-exemple.

Comme d'habitude en géométrie algébrique, un contre-exemple est considéré comme une belle addition au théorème qu'il contre-exemple. Soient k un corps algébriquement clos de caractéristique impaire p (par exemple $p = 23$, ou $p = 3$), K' le corps $k(r, s)$ avec $r^4 + s^4 = 1$, et G le groupe de k-automorphismes de K' formé de l'identité et de l'automorphisme g tel que $g(r) = -r$ et $g(s) = -s$ ("la symétrie par rapport à l'origine"). Le corps des invariants de G

est alors $K = k(r^2, rs, s^2)$.

Soit C_o la courbe projective plane non-singulière d'équation affine $x^4 + y^4 = 1$. Alors, G opère sur C_o (avec 4 points fixes à l'infini) au moyen de

$$(ig)(x, y) = (-x, -y) .$$

Soit C la courbe obtenue en descendant C_o de K' à K au moyen des automorphismes $(1, ig)$; c'est, comme C_o , une courbe de genre 3 (pas de canular de changement de genre, C_o étant absolument non singulière). En notant (x, y) un point générique de C_o sur K' (on a $x^4 + y^4 = 1$), un point générique de C sur K est $(r^2, rs, s^2, x^2, xy, y^2, rx, sx, ry, sy) = P$ (N. B. : dans la descente, G opère à la fois sur (r, s) et sur (x, y)). Comme K contient r^2 , s^2 , rs , r/s et s/r , on a $K(P) = K(rx, ry)$, de sorte qu'un modèle de C sur K est la courbe plane

$$\text{(C)} \qquad u^4 + v^4 = r^4 = (r^2)^2 \qquad (\text{on a } r^2 \in K) .$$

Comme p^n est impair, on a $r^{1+p^n} \in K$ et $rs^{p^n} = (rs)s^{p^n-1} \in K$. Donc la courbe plane C a une infinité de points rationnels sur K , à savoir les points

$$(r^{1+p^n}, rs^{p^n})$$

(substituer dans l'équation (C) ci-dessus). En termes un peu plus savants, le Frobenius de C_o commutte à la descente.

Reste à savoir que C n'est pas K-isomorphe à une courbe définie sur k , c'est-à-dire à C_o . Comme C et C_o sont des modèles canoniques (genre 3), il suffit de voir que, si f est une transformation projective plane amenant C en C_o , alors f n'est pas définie sur K . Or nous connaissons une de ces transformations, à savoir l'homothétie f_1 telle que $f_1(u) = rx$ et $f_1(v) = ry$; comme $r \notin K$, f_1 n'est pas définie sur K . Mais alors les autres ne le sont pas non plus, car elles se déduisent de f_1 par composition avec un automorphisme de C_o, et que ces automorphismes sont définis sur le petit corps k (cf. § 4, théorème 3).

Pour nous rassurer sur le corollaire du théorème 4 (§ 5), notons que, si on soumet C à l'homothétie $(u' = r^{p^n-1} u ,\ v' = r^{p^n-1} v)$ (son rapport est dans K , car $p^n - 1$ est pair), la transformée de C a pour équation $u'^4 + v'^4 = (r^4)^{p^n}$, et est donc définie sur K^{p^n} . C'est beau la Science !

Remarque finale. - Supposons que la courbe C ait une infinité de points rationnels sur K. En caractéristique 0, ou si $\mathrm{Aut}(C)$ est trivial, on a vu que C est K-isomorphe à une courbe C_o définie sur k. Alors le fibré-en-courbes X s'identifie à $R \times C_o$ et le champ E au champ horizontal ; de plus, pour presque tout point P de C_K, la section s_P correspondante de X est tangente à E, donc a ses dérivées nulles. En caractéristique 0, il en résulte que presque tout point de C_K provient de $(C_o)_k$ (une fonction à dérivées nulles étant constante). Cette conclusion n'est pas vraie en caractéristique p, même si $\mathrm{Aut}(C)$ est trivial (prendre C_o définie sur un corps fini F_q, $X = C_o \times C_o$, et considérer les itèrées s_n du " q-Frobenius" s : $x \mapsto x^q$ de C_o).

BIBLIOGRAPHIE

[1] GRAUERT (H.). - Mordells Vermutung über Punkte auf algebraischen Kurven und Funktionenkörper, à paraître dans "Institut des hautes Etudes scientifiques, Publications mathématiques" [alias "Playboy"].

[2] GROTHENDIECK (Alexander). - Eléments de géométrie algébrique, Chapitre 2 : Etude globale élémentaire de quelques classes de morphismes. - Paris, Presses universitaires de France, 1961 (Institut des hautes Etudes scientifiques, Publications mathématiques, 8).

[3] LANG (Serge). - Introduction to algebraic geometry. - New York, Interscience Publishers, 1958 (Interscience Tracts in pure and applied Mathematics, 5).

[4] MANIN (Ju. I.). - Points rationnels des courbes algébriques sur les corps de fonctions [en russe], Izvestija Akad. Nauk SSSR, Ser. Mat., t. 27, 1963, p. 1395-1440.

[5] SERRE (Jean-Pierre). - Groupes algébriques et corps de classes. - Paris, Hermann, 1959 (Act. scient. et ind., 1264 ; Publ. Inst. Math. Univ. Nancago, 7).

Complément (ajouté en janvier, 1966).

La description complète de ce qui se passe en caractéristique $p \neq 0$ est maintenant connue (cf. P. Samuel "Compléments à un article de Hans Grauert," Publ. Math. IHES, 1966). Tout se passe comme en caractéristique 0, sauf pour les courbes définies sur un corps fini F_q; pour celles-ci l'itération de l'endomorphisme de Frobénius donne, à partir d'un point rationel x, une famille dénombrable de points rationnels (x^{q^n}); mais ces familles sont en nombre fini.

D'autre part on trouvera quelques simplifications d'exposé dans un cours fait par P. Samuel, au Tata Institute for Fundamental Research, Bombay ("Old and new results on algebraic curves," 1966, en cours de polycopie).