ANDRÉ NÉRON

Modèles p-minimaux des variétés abéliennes

Séminaire N. Bourbaki, 1962, exp. nº 227, p. 65-80
<http://www.numdam.org/item?id=SB_1961-1962__7__65_0>

Séminaire BOURBAKI
14e année, 1961/62, n° 227

Décembre 1961

MODÈLES p-MINIMAUX DES VARIÉTÉS ABÉLIENNES

par André NÉRON

1. Langage et notations.

On désigne par k un corps muni d'une valuation discrète v. On note respectivement R et p l'anneau et l'idéal de valuation correspondants, et par k^o le corps résiduel. On suppose d'autre part que k^o est parfait. On note $\hat{k}$ et $\hat{R}$ les complétés respectifs de k et R relativement à v. On est alors, comme on sait, dans l'une des deux situations suivantes

a. k et k^o ont même caractéristique. Alors $\hat{R}$ est isomorphe à l'anneau de séries formelles $k^o[[t]]$ sur k^o.

b. k est de caractéristique 0, et k^o de caractéristique $p \neq 0$. Alors, si $v(p) = e$ est l'ordre de ramification de k relativement à v, l'anneau $\hat{R}$ est isomorphe à un module de rang e sur l'anneau des vecteurs de Witt $W(k^o)$, à coefficients dans k^o ; ce module admet pour base $(1, \pi, \dots, \pi^{e-1})$, si π est une uniformisante locale de R ; on sait qu'une telle uniformisante est toujours solution d'une équation d'Eisenstein

$$\pi^e + a_1 \pi^{e-1} + \dots + a_e = 0$$

où les a_i appartiennent à $W(k^o)$, et satisfont à $v_p(a_i) \geq 1$, $v_p(a_e) = 1$. En particulier, si $e = 1$ (k non ramifié), $\hat{R}$ est isomorphe à $W(k^o)$.

Pour les notions de géométrie algébrique que nous allons maintenant introduire, nous utiliserons essentiellement le langage des "Foundations" de WEIL [3], et, lorsqu'il sera question de réduction (mod p), celui de SHIMURA [2]. (Une mise au point définitive des questions abordées ici nécessitera sans doute l'utilisation systématique du langage des "schémas" ; faute d'une connaissance suffisante de ce langage, nous nous bornerons à indiquer la traduction de l'un des résultats essentiels).

Rappelons que le point de vue adopté comporte l'introduction de "domaines universels" pour k et k^o. On choisit d'abord arbitrairement un domaine universel $\mathfrak{t}^o$

pour k^o (qu'il est commode ici de supposer pourvu d'une base de transcendance non dénombrable sur k^o, étant donnés les types d'extensions de k^o qui interviendront). On désigne par $\mathfrak{R}$ l'anneau déduit de $\hat{R}$ "par extension de k^o à $\mathfrak{k}^o$", c'est-à-dire défini en posant $\mathfrak{R} = \mathfrak{k}^o[[t]]$ dans le cas (a), et $\mathfrak{R} = \hat{R} \otimes_{W(k^o)} W(\mathfrak{k}^o)$ dans le cas (b) ; on note $\mathfrak{k}$ le corps des quotients de $\mathfrak{R}$. Ainsi $\hat{R}$ s'identifie naturellement à un sous-anneau de $\mathfrak{R}$, et $\hat{k}$ à un sous-corps de $\mathfrak{k}$. De plus, $\mathfrak{R}$ est un anneau de valuation, et on peut normer la valuation correspondante de manière qu'elle prolonge v (on la désigne encore par v). On choisit enfin arbitrairement un domaine universel Ω pour $\mathfrak{k}$ (donc aussi a fortiori pour k).

Si V est une variété (resp. une variété affine) définie sur k, les points de V à coordonnées dans $\mathfrak{k}$ (resp. dans $\mathfrak{R}$) sont appelés <u>points rationnels (resp. entiers) p-adiques de</u> V. Si V est une variété affine ou projective, définie sur k, on sait, d'après SHIMURA [2], lui appliquer l'opération de <u>réduction</u> (mod p). Rappelons que cette opération fait correspondre à V un cycle positif, rationnel sur k^o, que nous noterons $\rho(V)$, ou $\rho_p(V)$. Remarque : ces notions peuvent, en réalité, être définies pour une classe plus étendue de variétés, qui sont les " p-variétés" au sens de SHIMURA ; mais nous pourrons, pour la suite, nous borner à considérer des variétés affines ou projectives.

2. p-<u>simplicité</u>.

Soit V une variété affine définie sur k, et posons $V^o = \rho(V)$. Soit de plus x^o un point de support $\operatorname{Supp} V^o$ du cycle V^o. Soit f une fonction sur V, définie sur $\mathfrak{k}$. Une telle fonction f est induite par un quotient $\frac{P}{Q}$, où P et Q sont des polynômes à coefficients dans $\mathfrak{R}$. Notons P^o et Q^o les polynômes réduits (mod p) de P et Q respectivement. S'il est possible de choisir P et Q de manière qu'on ait $Q^o(x^o) \neq 0$, on dit que f est p-<u>morphique</u> en x^o, et l'expression $\frac{P^o(x^o)}{Q^o(x^o)}$ est appelée <u>valeur de</u> f <u>en</u> x^o. L'ensemble de toutes les fonctions sur V qui sont p-morphiques en x^o est un anneau local, que nous désignons par $\rho(V, x^o)$.

Nous dirons que x^o est p-<u>simple sur</u> V si cet anneau local est <u>régulier</u>. En particulier, si x^o <u>est simple sur</u> V^o (c'est-à-dire s'il n'appartient qu'à une composante du cycle V^o, de coefficient 1, et s'il est simple sur cette composante), il est a fortiori p-simple sur V. La réciproque de cette propriété est inexacte ; mais en utilisant le lemme de Hensel, et les propriétés élémentaires des anneaux locaux, on voit que x^o est simple sur V^o si et seulement s'il satisfait aux deux conditions suivantes :

1° Il est p-simple sur V ,

2° Il existe x appartenant à $V_{\mathfrak{R}}$ tel que $x^o = \rho(x)$ (i. e. on peut remonter x^o à un point entier p-adique de V).

Soient V et W deux variétés affines définies sur k , et soit $\varphi : V \to W$ une application rationnelle, définie sur k . Nous dirons que φ est p-morphique en un point x^o de Supp V^o si chacune des fonctions coordonnées φ_i de φ est p-morphique en ce point. Le point y^o ayant pour coordonnées les $y_i^o = \varphi_i^o(x^o)$ s'appelle valeur de φ en x^o , et est noté $\varphi^o(x^o)$. Si φ est birationnelle, et si φ^{-1} est p-morphique en x^o , on a $x^o = (\varphi^{-1})^o\ (y^o)$; on dit alors que φ est p-isomorphique en x^o . Toutes ces définitions s'étendent d'une manière naturelle au cas où V est une " p-variété", et, en particulier, une variété projective définie sur k .

3. Énoncé des résultats.

a. Modèles p-simples p-minimaux des courbes elliptiques. - Nous dirons que V , définie sur k , est p-simple, si tous les points du support du cycle réduit V^o sont p-simples sur V . Par k-modèle de V , nous entendrons toujours un couple (W , φ) composé d'une variété W définie sur k , et d'un k-isomorphisme $\varphi : V \to W$.

THÉORÈME 1. - Soit A une courbe elliptique définie sur k , et possédant un point rationnel sur k . Alors il existe un k-modèle projectif p-simple (A_* , α) de A satisfaisant à la propriété suivante : pour tout autre k-modèle (B , φ) de A , l'application composée $\alpha \circ \varphi^{-1} : B \to A_*$ est p-morphique en tout point de Supp B^o qui est p-simple sur B .

Conséquences :

1° Si (A_* , α) et (A'_* , α') sont deux tels modèles, alors

$$\beta = \alpha' \circ \alpha^{-1} : A_* \to A'$$

est p-isomorphique en tout point du cycle réduit A^o . Ceci se traduit, dans le langage des schémas, par la propriété d'unicité suivante : le schéma sur R défini à partir de l'ensemble des anneaux locaux $p(A_*, x^o)$, avec $x^o \in \mathrm{Supp}\, A_*^o$ est unique à un R-isomorphisme près. Plus précisément, il est déterminé par la donnée de k, de p, et de la classe de A modulo les k-isomorphismes ; ou encore par la donnée de k, de p, et du schéma sur k représenté par A.

De cette propriété d'unicité, résulte en particulier l'unicité du nombre des composantes du cycle A_*^o, des coefficients de chacune d'elles dans ce cycle, de leurs relations de connexion, et de leurs multiplicités d'intersection deux à deux (on donnera à ce sujet, au n° 5, une classification complète de tous les cas possibles).

2° D'après la propriété d'application universelle du théorème 1, la loi de groupe sur A_* est partout p-morphique. De plus, notons $S(A_*^o)$ l'ensemble des points de $\mathrm{Supp}\, A_*^o$ qui sont simples sur A_*^o. Alors on déduit de la loi de composition sur A_*, par réduction (mod p), une loi de composition sur $S(A_*^o)$, qui fait de cet ensemble un groupe algébrique. Ce groupe algébrique, qui est uniquement déterminé à un k^o-isomorphisme près, sera noté $G_p(A)$.

b. Modèles faiblement p-simples p-minimaux des variétés abéliennes. - Soit V une variété affine ou projective, définie sur k, et posons $V^o = \rho(V)$. On dira que V est faiblement p-simple si tout point rationnel p-adique de V se réduit (mod p) en un point simple sur V^o (ou, ce qui revient au même, d'après le n° 2, en un point p-simple sur V). Toute variété V, p-simple, est a fortiori faiblement p-simple, mais la réciproque est fausse. Soit, par exemple, $k = k^o[[t]]$, et prenons pour V la courbe plane projective, définie sur k, d'équation $X^3 + t^5 Z^3 = Y^2 Z$. Le point $(0, 0, 1)$ est le seul point de $\mathrm{Supp}\, V^o$ qui est p-multiple sur V, mais, comme on voit immédiatement, il est impossible de remonter ce point à un point rationnel p-adique de V. Donc V est faiblement p-simple, mais n'est pas p-simple.

THÉORÈME 2. - Supposons k complet ($\hat{k} = k$). Soit A une variété abélienne définie sur k. Alors il existe un k-modèle projectif, faiblement p-simple (A_*, α) de A, tel que, pour tout couple (V, φ) composé d'une variété algébrique V, définie sur k, et d'une application rationnelle $\varphi : V \to A$, définie sur k, l'application composée $\alpha_* = \alpha \circ \varphi : V \to A_*$ soit p-morphique en tout point de $\mathrm{Supp}\, V^o$ simple sur V^o.

Conséquences. Comme dans le théorème 1, notons $S(A_*^o)$ l'ensemble des points de Supp A_*^o qui sont simples sur A_*^o. Alors en réduisant (mod p) la loi de composition sur A_*, on obtient encore sur $S(A_*^o)$ une structure de groupe algébrique (uniquement déterminé à un k-isomorphisme près par la donnée de A, k, et p), qu'on peut continuer à noter $G_p(A)$.

Toute courbe elliptique qui satisfait au théorème 1 satisfait aussi au théorème 2. Par contre, la cubique plane de l'exemple donné au début de ce paragraphe satisfait au théorème 2, mais non au théorème 1.

Le théorème 2 est encore valable lorsqu'on y remplace A par un espace homogène principal sur une variété abélienne (noter que, d'après l'hypothèse " k complet", si k^o est algébriquement clos, un tel espace est toujours k-isomorphe à une variété abélienne, pourvu qu'il contienne au moins un point rationnel p-adique).

c. Problèmes globaux. Modèles p-minimaux pour tout p. - Soit K un "corps global" et, plus précisément, supposons que K est ou bien

(i) un corps de nombres algébriques, de degré fini sur $\mathbb{Q}$, ou bien

(ii) un corps de fonctions algébriques d'une variable sur un corps de base algébriquement clos (c'est-à-dire un corps de la forme $K = K_o(u)$, où u est un point générique sur K_o d'une courbe algébrique U définie sur K_o - qu'on peut supposer non singulière). Notons $\mathfrak{S}$ l'ensemble de tous les p respectivement associés, dans le cas (i) aux valuations non triviales de K (i. e. aux idéaux premiers de K) et, dans le cas (ii), aux valuations non triviales de K s'annulant sur K_o (i. e. aux points de U rationnels sur K_o).

THÉORÈME 3. - Soit A une courbe elliptique définie sur K, et possédant un point rationnel sur K. Alors il existe un K-modèle projectif (A_*, α) de A qui est p-simple et p-minimal pour tout $p \in \mathfrak{S}$.

Dans le cas (ii), on peut donner une interprétation "géométrique" de ce résultat. Soient $\mathbb{P}$ et $\mathbb{P}_o$ des espaces projectifs contenant A et U respectivement, et soit x un point générique de A sur $K = K_o(u)$; considérons la surface $\tilde{A}$, lieu du couple (x, u) dans le produit $\mathbb{P} \times \mathbb{P}_o$. Cette surface apparaît comme fibrée par une famille de courbes paramétrée par U, la fibre générique étant $A \times u$. Notons $\tilde{A}_*$ la surface analogue construite à partir de A_*, et considérons l'application rationnelle $\tilde{\alpha} : \tilde{A} \to \tilde{A}_*$, définie sur K_o, telle qu'on ait

$$\tilde{\alpha}(x , u) = (\alpha(x) , u) \quad .$$

Alors la condition pour A_* d'être p-simple pour tout p équivaut à celle pour $\tilde{A}_*$ d'être non singulière. La condition minimale du théorème 1 signifie que, pour tout autre modèle (A'_* , α') de A possédant la même propriété, l'application composée $\tilde{\alpha} \circ (\tilde{\alpha}')^{-1} : \tilde{A}'_* \to \tilde{A}_*$ est un morphisme.

Cette propriété est analogue à celle affirmant l'existence des modèles non singuliers minimaux des surfaces en géométrie algébrique classique. Elle en diffère cependant par le fait que la condition précédente ne fait intervenir que les modèles "fibrés" de base U , et les morphismes respectant la fibration. On peut montrer par des exemples simples, que $\tilde{A}_*$ n'est pas toujours un modèle minimal au sens classique.

<u>Problème</u>. - Peut-on lever la restriction " k complet" dans le théorème 2 ? On pourrait alors déduire de ce dernier un résultat global, analogue au théorème 3 .

4. <u>Démonstration du théorème</u> 2.

Nous ne pouvons donner ici sur cette démonstration que des indications sommaires. Nous nous bornerons à énoncer quelques définitions, et quelques résultats intermédiaires essentiels.

a. <u>Pro-variétés</u>. - On appelle <u>pro-variété</u> définie sur k^o la limite projective X d'une suite

$$X^o \xleftarrow[\theta^o]{} X^1 \xleftarrow[\theta^1]{} \dots X^\mu \xleftarrow[\theta^\mu]{} \dots$$

où les X^μ sont des variétés définies sur k^o , et les θ^μ des morphismes (qu'on supposera toujours génériquement surjectifs) définis sur k^o .

Un <u>point</u> x de X est une suite $(x^o , \dots , x^\mu \dots)$, où, pour tout μ , on a $x^\mu \in X^\mu$, et $x^\mu = \theta^\mu(x^{\mu+1})$. On note $k^o(x)$ le corps $k^o(x^o , \dots , x^\mu \dots)$. L'application $X \to X^\mu$ qui fait correspondre x^μ à x est notée ρ_μ .

Soient x et y deux points de X . On dit que y est une <u>spécialisation de</u> x <u>sur</u> k^o si, pour tout μ , y^μ est une spécialisation de x^μ sur k^o . Un point de X tel que, pour tout μ ; le point x^μ soit générique de X^μ sur k^o , s'appelle un <u>point générique de</u> X <u>sur</u> k^o .

On définit d'une manière évidente la notion de sous-pro-variété d'une pro-variété donnée (Y^μ , sous-variété de X^μ pour tout μ). Une sous-pro-variété Y de X est déterminée par la donnée de l'un de ses points génériques y sur k^o , et est alors appelé lieu de y sur k^o .

On appelle sous-ensemble algébrique (resp. constructible) de X un sous-ensemble S de l'ensemble des points de X tel que, pour tout μ , $S^\mu = \rho_\mu(S)$ soit un sous-ensemble algébrique (resp. constructible) de X , et tel qu'on ait $x \in S$ si et seulement si $x^\mu \in S^\mu$ pour tout μ .

b. Pro-variétés et ensembles attachés au couple $(V , \mathfrak{p})$. - Bornons-nous, pour simplifier, au cas où k est non ramifié par rapport à v . Considérons d'abord l'espace affine $\mathfrak{S} = \Omega^n$, et soit $x = (x_1 , \dots , x_n)$ un point de $\mathfrak{S}_{\mathfrak{R}} = \mathfrak{R}^n$. Pour tout i , notons $x_i^{(\mu)}$ le μ-ième coefficient du développement en série de x_i (lorsque x_i est une série formelle), ou bien la μ-ième composante de x_i (lorsque x_i est un vecteur de Witt). Nous désignerons par ρ^μ l'application $\mathfrak{R}^n \to (\mathfrak{k}^o)^{n(\mu+1)}$ qui, au point x , fait correspondre le point

$$x^\mu = (x_1^{(o)} , \dots , x_n^{(o)} , \dots , x_1^{(\mu)} , \dots , x_n^{(\mu)}) \quad ,$$

et nous noterons θ^μ la projection $(k^o)^{n(\mu+2)} \to (k^o)^{n(\mu+1)}$ qui, à $x^{\mu+1}$, fait correspondre x^μ . L'ensemble $\mathfrak{S}_{\mathfrak{R}} = \mathfrak{R}^n$ peut être identifié à la pro-variété définie par la suite

$$(\mathfrak{k}^o)^n \leftarrow (\mathfrak{k}^o)^{2n} \leftarrow \dots (\mathfrak{k}^o)^{n(\mu+1)} \leftarrow \dots$$

Soit V une vériété affine, de dimension r , définie sur k , non singulière. Les restrictions des applications ρ et θ^μ à l'ensemble des points entiers $\mathfrak{p}$-adiques de V sont notées ρ_V et θ_V^μ .

On appellera $(V , \mathfrak{p})$-pro-variété définie sur k^o toute sous-pro-variété X de $\mathfrak{R}^n$ satisfaisant aux conditions suivantes :

(i) tout point générique de X sur k^o appartient à V ,

(ii) pour μ assez grand, et pour x^μ générique de X^μ sur k^o , on a

$$(\theta_V^\mu)^{-1} (x^\mu) \subset X^{\mu+1}$$

(on montre, par ailleurs, l'existence d'un μ_0 tel que, pour tout $\mu \geq \mu_0$, et pour tout $x^\mu \in \rho^\mu(V_{\mathfrak{R}})$, l'ensemble $(\theta_V^\mu)^{-1}(x^\mu)$ soit une variété linéaire, de dimension r, définie sur $k^0(x^\mu)$)).

La condition (ii) équivaut encore à la suivante : les $x_i^{(\mu)}$ associés à x générique de X sur k^0 ne satisfont qu'à un nombre fini de relations algébriques, outre celles exprimant l'appartenance à V.

On appellera (V, p)-ensemble tout sous-ensemble constructible S de $\underset{\sim}{S}_{\mathfrak{R}}$, contenu dans V, et tel que, pour μ assez grand, on ait

$$(\rho_V^\mu)^{-1}(S^\mu) = S^{\mu+1} \quad .$$

Autre définition équivalente : un (V, p)-ensemble est l'ensemble de tous les points $x \in V_{\mathfrak{R}}$ (points entiers p-adiques de V) dont les coefficients $x_i^{(\mu)}$ des coordonnées satisfont à un nombre fini de relations $F_\alpha = 0$, $G_\beta \neq 0$ (les F_α, G_β étant des polynômes à coefficients dans $\mathfrak{k}^0$).

Une (V, p)-pro-variété X (resp. un (V, p)-ensemble S) sera dit simple (mod p), si tout point générique de X^0 sur k^0 (resp. tout point de $S^0 = \rho(S)$) est simple sur V^0.

PROPOSITION 1. - Soient V et W deux variétés affines, définies sur k, et soit φ : $V \to W$ une application séparable, génériquement surjective, définie sur k. Soit X une (V, p)-pro-variété, définie sur k^0, et soit x un point générique de X sur k^0 ; supposons que φ est p-morphique en $x^0 = \rho(x)$. Alors $y = \varphi(x)$ est générique sur k^0 d'une (W, p)-pro-variété.

Cette pro-variété sera, dans la suite, notée $Y = \varphi_g(X)$. Remarque : φ_g ne respecte pas l'inclusion.

PROPOSITION 2. - Soient V, W et φ comme dans la proposition 1. Soit S un (V, p)-ensemble, et supposons φ définie en tout point de $S^0 = \rho(S)$. Alors $T = \varphi(S)$ est un (W, p)-ensemble ;

Ces deux propositions (auxquelles on doit ajouter certaines précisions concernant la correspondance entre les X^μ et les Y^ν (resp. entre les S^μ et les T^ν)), permettent, en particulier, d'étendre les définitions précédentes au cas où V une " p-variété" (le seul cas utile pour nous étant celui d'une variété projective).

Elles permettent en outre de montrer que si $\varphi : V \to W$ est un k-isomorphisme entre variétés projectives, le symbole φ_g (resp. φ) définit une correspondance biunivoque entre $(V , \mathfrak{p})$-pro-variétés et $(W , \mathfrak{p})$-pro-variétés (resp. entre $(V , \mathfrak{p})$-ensembles et $(W , \mathfrak{p})$-ensembles).

PROPOSITION 3 (désingularisation et éclatement d'une pro-variété). - *Soit* V *de dimension* r , *définie sur* k , *et soit* X *une* $(V , \mathfrak{p})$-*pro-variété. Alors il existe un* k-*modèle* (W , φ) *de* V *tel que* φ^{-1} *soit partout* $\mathfrak{p}$-*morphique, et tel que :*

(i) $Y = \varphi_g(X)$ *soit simple* (mod $\mathfrak{p}$)

(ii) $\dim Y^o = r$

(iii) φ *soit* $\mathfrak{p}$-*isomorphique en tout point de* Supp V^o *n'appartenant pas à* X^o .

PROPOSITION 4 (existence d'un recouvrement fini de $V_{\mathfrak{R}}$). - *Soit* V *une variété projective non singulière, de dimension* r , *définie sur* k . *Alors il existe un nombre fini de* k-*modèles* (W_i , φ_i) *et, pour tout* i , *un* $(V , \mathfrak{p})$-*ensemble* S_i , *tels que*

(i) *les* S_i *recouvrent* $V_{\mathfrak{R}}$

(ii) *les* $T_i = \varphi_i(S_i)$ *soient simples* (mod $\mathfrak{p}$) .

c. *Différentielles*. - Soit V une variété projective non singulière, de dimension r , définie sur k , et soit ω une k-différentielle d'ordre r du corps des fonctions sur V .

Soit x^o un point de Supp V^o , simple sur V^o , et soient $(u_1 , \ldots , u_r)$ un système de paramètres uniformisants de V en x^o (i. e. de fonctions sur V , définies sur k , induisant des paramètres uniformisants en x^o sur la composante de V^o qui contient x^o).

On peut écrire ω sous la forme $\omega = f\, du_1 \wedge \ldots \wedge du_r$. Si f est $\mathfrak{p}$-morphique en x^o , on dira que ω est *$\mathfrak{p}$-morphique* en x^o .

Dans tout ce qui suit, on supposera que ω n'admet sur V *ni pôles ni zéros* (ce qui est le cas, en particulier, pour la différentielle invariante sur une variété abélienne). Dans ce cas, pour tout $x^o \in$ Supp V^o , simple sur V^o , il existe nécessairement un et un seul entier ν tel que la fonction $ft^{-\nu}$ (cas des séries formelles) ou $fp^{-\nu}$ (cas des vecteurs de Witt) soit p-morphique et non nulle en x^o. Cet entier sera noté $\nu_\omega(x^o)$, ou $\nu(x^o)$. Il ne dépend que de la composante C^o de V^o à laquelle appartient x^o. Il est de plus invariant par une application p-isomorphique ; plus précisément :

PROPOSITION 5. - Soit $\varphi : V \to W$ un k-isomorphisme ; soient x^o simple sur V^o et y^o simple sur W^o ; supposons que φ est p-morphique en x^o, et que $y^o = \varphi^o(x^o)$. Alors on a $\nu(x^o) \leqslant \nu(y^o)$, et l'égalité a lieu si et si seulement φ est p-isomorphique en x^o.

Pour toute (V, p)-pro-variété X, on peut trouver, d'après la proposition 3, un k-modèle (W, φ) de V, tel que la variété Y^o réduite de $Y = \varphi_g(x)$ soit l'une des composantes simples de W^o. On voit alors, d'après la proposition 5, que l'entier $\nu(Y^o)$ ne dépend pas alors du choix du modèle (W, φ), mais seulement de ν, ω et X. On peut donc le désigner par $\nu_\omega(X)$ (ou $\nu(X)$).

PROPOSITION 6. - L'entier $\nu(X)$ admet une borne inférieure ν_o qui ne dépend que de V et de ω.

Autre énoncé équivalent (sans pro-variétés) : A tout k-modèle (W, φ) de V, et à tout point $y^o \in \operatorname{Supp} W^o$, simple sur W^o, associons l'entier $\nu(y^o)$. Cet entier admet une borne inférieure ν_o (la même que plus haut), qui ne dépend que de V et ω, mais non de W, de φ, ni de y^o.

La proposition 6 se déduit des propositions 4 et 5 : ν_o est la plus petite valeur prise par l'entier ν sur les composantes des T_i^o. Un point $x^o \in \operatorname{Supp} V^o$ tel que $\nu(x^o) = \nu_o$, une composante C^o de V^o telle que $\nu(C^o) = \nu_o$, seront dits ω-maximaux. De même, une (V, p)-pro-variété sera dite ω-maximale si $\nu(X) = \nu_o$, et s'il existe un k-modèle (W, φ) de V tel que $\varphi_g(X)$ soit simple (mod p) et soit maximale au sens de l'inclusion.

PROPOSITION 7. - Pour V donnée, il n'existe qu'un nombre fini de (V, p)-pro-variété ω-maximales.

(On le montre encore en se servant du recouvrement fini de la proposition 4.)

d. Cas d'une variété abélienne. Composition des points simples ω-maximaux. - $\varphi : V \to W$ étant une application rationnelle définie sur k, et x^o un point de $\operatorname{Supp} V^o$, on appellera transformé ensembliste de x^o par φ l'ensemble des points

$y^o \in \operatorname{Supp} W^o$ tels que $(x^o, y^o) \in \operatorname{Supp} \Gamma^o$ où Γ^o est la réduction (mod p) du graphe Γ de φ. Cet ensemble sera noté $\varphi_e^o(x^o)$.

On considère maintenant une variété abélienne A, définie sur k, de dimension r. On note ω la différentielle invariante de degré r sur A. On peut, sans inconvénient, supposer A projective et p-normale (anneaux locaux intégralement clos en tous les points de $\operatorname{Supp} A^o$). On peut en outre supposer, d'après les propositions 3 et 7, que toutes les (A, p)-pro-variétés ω-maximales sont simples (mod p). On notera d'autre part γ_A l'application $A \times A \times A \to A$ telle que $\gamma_A(x, y, z) = x + y - z$.

PROPOSITION 8. - Si x_1^o, x_2^o, y_1^o sont trois points génériques indépendants sur k^o de trois composantes simples ω-maximales de A^o, l'application γ_A est p-morphique en (x_1^o, x_2^o, y_1^o) et le point $y_2^o = \gamma_A^o(x_1^o, x_2^o, y_1^o)$ est aussi générique sur k^o d'une composante simple ω-maximale de A^o.

(D'où l'on déduit une structure de groupe abélien fini sur l'ensemble des composantes simples ω-maximales.)

Par applications répétées de la proposition 8, et en introduisant d'autre part une variété abélienne auxiliaire B (obtenue comme lieu des points de Chow des images, dans un modèle projectif de $A \times A$, des graphes des translations sur A), on obtient diverses propositions analogues à la proposition 8, mais où interviennent des points ω-maximaux non génériques. On est alors en mesure de démontrer :

PROPOSITION 9. - Soit V une variété quelconque, définie sur k, et soit $\varphi : V \to A$ une application rationnelle, définie sur k. Soient z^o un point simple sur V^o, et x^o un point simple ω-maximal sur A^o, tels que $z^o \in \varphi_e^o(x^o)$. Alors φ est p-morphique en z^o (et on a donc $x^o = \varphi^o(z^o)$)

On peut reprendre la méthode suivie par WEIL pour démontrer la propriété bien connue : toute application rationnelle d'une variété V dans une variété abélienne est morphique en tout point simple de V ([4], chap. 2, n° 5, th. 6).

e. Contraction. - Dans ce qui suit, on supposera k^o algébriquement clos (on se ramène à ce cas par une technique de "descente du corps de base").

Soit $\varphi : V \to W$ une application rationnelle, et soit x^o un point de $\operatorname{Supp} W^o$. On dit que φ est p-antimorphique en x^o si φ est morphique en tout point de

$(\varphi^{-1})^o_e\ (x^o)$. Adoptant alors une terminologie rappelant celle de ZARISKI [5], on dira que l'ensemble $(\varphi^{-1})^o_e\ (x^o)$ est "exceptionnel de première espèce".

On dira qu'une variété abélienne A , satisfaisant aux conditions précisées plus haut, est p-contractile si, pour tout k-isomorphisme $A' \to A$, φ est p-antimorphique en tout point $x^o \in \mathrm{Supp}\ A^o$ simple ω-maximal sur A^o . On montre, en particulier, que la variété B introduite plus haut (définie à partir des graphes des translations sur A) est toujours p-contractile.

LEMME (contraction des ensembles exceptionnels de première espèce). - Soient V et W deux variétés projectives, définies sur k , p-normales, et soit $\varphi : V \to W$ un k-isomorphisme. Soit T^o un sous-ensemble constructible de l'ensemble des points simples sur W^o , et supposons que φ est p-antimorphique en tout point de T^o . Alors il existe un k-modèle (W', φ') de V tel que

(i) φ' soit p-isomorphique en tout point de V^o n'appartenant pas à l'adhérence de $S^o = (\varphi^{-1})^o_e\ (T^o)$.

(ii) $\psi = \varphi' \circ \varphi^{-1} : W \to W'$ soit p-isomorphique en tout point de T^o .

De ce lemme on déduit la possibilité de "recoller" deux (A , p)-ensembles S_1 et S_2 dont les images respectives sur deux modèles (A_1 , φ_1) et (A_2 , φ_2) de A (l'un de ces deux modèles étant p-contractile) sont composées de points simples et ω-maximaux (mod p) : il existe alors un k-modèle (A', φ') de A , tel que l'image S' sur A' de $S = S_1 \cup S_2$ soit composée de points simples ω-maximaux (mod p) .

D'autre part, compte tenu de la proposition 9, on peut démontrer la proposition suivante, qui est une forme, particulière aux variétés abéliennes, du lemme de recouvrement fini (proposition 4).

PROPOSITION 10. - Soit A une variété abélienne, définie sur k . Alors il existe un nombre fini de (A , p)-ensembles S_i et, pour tout i , une translation τ_i définie sur k , tels que

(i) les S_i recouvrent A ;

(ii) les (A , p)-ensembles $T_i = \tau_i(S_i)$ ne contiennent que des points simples et ω-maximaux (mod p) .

Pour construire un modèle faiblement p-simple et p-minimal de A , on remplace

A par B (qui lui est k-isomorphe, et qui est p-contractile) ; on applique à B la proposition 10, puis on "recolle" les ensembles S_i par le procédé indiqué plus haut.

5. Cas des courbes elliptiques. Discussion du type de la réduction de $A_*(\mathrm{mod}\ p)$. — La démonstration du théorème 1 utilise certains des résultats exposés au numéro précédent (paragraphes (c) et (d)), mais comporte l'examen séparé de nombreux cas particuliers, et utilise la construction explicite d'un bon modèle dans chacun de ces cas.

Nous bornerons ici à énumérer ces cas, et à indiquer, dans chacun d'eux, le type de réduction obtenu, ainsi que la structure du groupe $G_p(A)$. Cette discussion est analogue à celle que donne KODAIRA dans [1], où il étudie le même problème dans le cas classique $(k^o = \underset{\sim}{C})$, en vue d'applications à la classification des surfaces analytiques compactes. Nous ne considérerons, d'autre part, pour simplifier l'exposé, que le cas où la caractéristique de k^o n'est pas égale à 2 ni à 3 (en fait, on obtient la même liste de cas possibles en caractéristiques 2 et 3, mais la discusiion est plus pénible). Par hypothèse, A est une courbe elliptique possédant un point rationnel sur k. On peut donc supposer que c'est une cubique plane de Weierstrass

$$Y^2 = X^3 + pX + q$$

avec p et $q \in R$. On pose $\Delta = 4p^3 + 27q^2$, et on note $j = j(A)$ l'invariant de A, qu'on peut ici prendre égal à $\frac{p^3}{\Delta}$. Les deux cas suivants sont à distinguer :

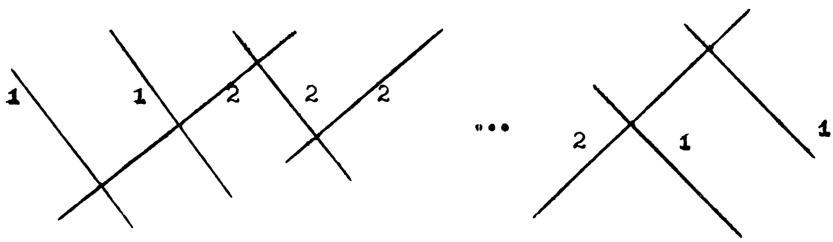
a. $v(j) < 0$ (ou encore $j \notin R$). — Alors la classe de A à un k-isomorphisme près ne dépend que de j, et de la classe de l'entier pq, dans le groupe multiplicatif k^* de k, modulo les carrés des éléments de k^*. En fait, seuls interviendront dans la discussion l'entier $v(j)$, et la parité de l'entier $v(pq)$.

(i) $v(pq)$ pair. - On trouve que le cycle réduit A_*^o admet $n = v(j)$ composantes, qui sont des courbes de genre zéro. Pour $n = 1$, l'unique courbe obtenue admet un seul point multiple (double, à tangentes distinctes). Pour $n \geq 2$, les n courbes sont sans point multiple, et connectées comme l'indique la figure

$n = 1$  $n \geqslant 2$

Le groupe $G_p(A)$ est, dans ce cas, une extension du groupe multiplicatif par le groupe cyclique fini $\mathbb{Z}/n\mathbb{Z}$.

(ii) $v(pq)$ impair. - Le cycle obtenu est alors du type représenté par la figure ci-dessous (les chiffres indiquent les ceofficients des différentes composantes du cycle ; on a ici quatre composantes de coefficient 1 et $n+1$ de coefficient 2).

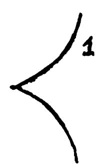
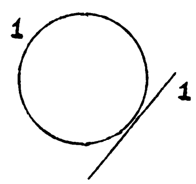
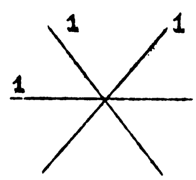
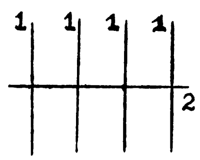


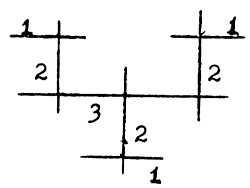
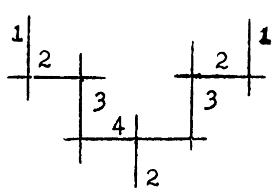
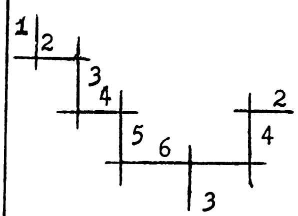
Le groupe algébrique $G_p(A)$ est ici une extension du groupe additif par un groupe fini d'ordre 4 , qui est le groupe non cyclique $(\mathbb{Z}/2\mathbb{Z})^2$, ou le groupe cyclique $\mathbb{Z}/4\mathbb{Z}$ suivant que n est pair ou impair.

REMARQUE. - Lorsqu'on est dans le cas (ii), ou bien dans le cas (i), avec $n \geqslant 4$, le cycle A^o_* possède au moins quatre composantes et, par suite A_* est de degré projectif $\geqslant 4$. La courbe A_* , qui est elliptique et non singulière, ne peut donc pas être une courbe plane (même si l'on n'adopte que le point de vue du théorème 2).

b. $v(j) \geqslant 0$ (ou encore $j \in R$). - Alors la classe de A modulo les k-isomorphismes est déterminée par la connaissance de j , et par celle de la classe de Δ dans le groupe multiplicatif k^* , modulo les puissances douzièmes des éléments de k^* . Seule intervient en fait dans la discussion la classe de l'entier $v(\Delta)$ (mod 12) . Cette classe est d'ailleurs nécessairement un diviseur de 0 , c'est-à-dire est représentée par l'un des entiers 0, 2 , 3 , 4 , 6 , 8, 9 ou 10 .

Si $v(\Delta) \equiv 0 \pmod{12}$, on a une réduction <u>non dégénérée</u>, i. e. A_*^o est réduit à une courbe elliptique. Les résultats obtenus dans les autres cas sont donnés par le tableau ci-dessous. Les composantes du cycle A_*^o sont toujours des courbes de genre 0, sans point multiple (sauf pour $v(\Delta) \equiv 2 \pmod{12}$, auquel cas on a un point de rebroussement) et qui se coupent transversalement deux à deux (sauf pour $v(\Delta) \equiv 3 \pmod{12}$, auquel cas on a deux composantes admettant un contact du premier ordre). Le groupe $G_p(A)$ est toujours isomorphe à une extension du <u>groupe additif</u> par un groupe fini Γ d'ordre 1, 2, 3, ou 4.

$v(\Delta)$ (mod 12)	2	3	4	6
Cycle A_*^o				
Ordre de Γ	1	2	3	4 (non cyclique)

$v(\Delta)$ (mod 12)	8	9	10
Cycle A_*^o			
Ordre de Γ	3	2	1

BIBLIOGRAPHIE

[1] KODAIRA (Kunihiko). - On compact analytic surfaces, Conference on Analytic functions [1957. Princeton] ; p. 121-135. - Princeton, Princeton University Press, 1960 (Princeton mathematical Series, 24).

[2] SHIMURA (G.). - Reduction of algebraic varieties with respect to a discrete valuation of the basic field, Amer. J. of Math., t. 77, 1955, p. 134-176.

[3] WEIL (André). - Foundations of algebraic geometry. - New York, American mathematical Society, 1946 (Amer. math. Soc., Coll. Publ., 29).

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

[5] ZARISKI (O.). - Introduction to the problem of minimal models in the theory of algebraic surfaces, - Tokyo, Mathematical Society of Japan, 1958 (Publ. Math. Soc. Japan, 4).