PUBLICATIONS MATHÉMATIQUES DE L'I.H.É.S.

ANDRÉ NÉRON

Modèles minimaux des variétés abéliennes sur les corps locaux et globaux

Publications mathématiques de l'I.H.É.S., tome 21 (1964), p. 5-128

<http://www.numdam.org/item?id=PMIHES_1964__21__5_0>

INTRODUCTION

Ce travail a pour principal objet la démonstration de l'existence de certains modèles privilégiés des variétés abéliennes définies sur un corps de valuation discrète k (et, en particulier, sur un corps *local*, tel qu'un corps $\mathfrak{p}$-adique, ou un corps de séries formelles), ou sur un corps *global* K (c'est-à-dire sur un corps de nombres ou de fonctions algébriques). De tels modèles paraissent présenter un intérêt particulier pour l'étude des propriétés arithmétiques de ces variétés [1]; on les définit, dans le cas local (resp. global), par la propriété d'être *minimaux* parmi ceux qui vérifient une condition de « bonne réduction », consistant en la non-existence de certaines singularités de leur ensemble réduit (mod. $\mathfrak{p}$), où $\mathfrak{p}$ est l'idéal associé à la valuation donnée de k (resp. à l'une quelconque des valuations non triviales de K).

On peut, en particulier, exiger que tous les points de cet ensemble réduit aient un anneau local régulier, auquel cas les modèles considérés sont dits « $\mathfrak{p}$-simples ». C'est seulement dans le cas des courbes elliptiques définies sur k, et possédant un point rationnel sur k, que nous obtenons la démonstration d'un théorème général d'existence des modèles « $\mathfrak{p}$-simples $\mathfrak{p}$-minimaux »; nous en déduisons ensuite le théorème global correspondant (chap. III, th. 1 et 2). Cette démonstration est laborieuse; elle comporte d'assez longs calculs, et nécessite l'examen séparé de nombreux cas particuliers; elle présente toutefois l'avantage de donner une description précise de la situation dans chaque cas, permettant de généraliser certains des résultats obtenus récemment par Kodaira [7], et qui concernent les courbes elliptiques définies sur un corps de séries à coefficients complexes.

Dans le cas des variétés abéliennes quelconques, ou plus généralement, des espaces homogènes principaux abéliens, nous ne considérons que des modèles « faiblement $\mathfrak{p}$-simples », caractérisés par le fait que tout point rationnel $\mathfrak{p}$-adique sur un tel modèle se réduit (mod. $\mathfrak{p}$) en un point $\mathfrak{p}$-simple. Nous obtenons encore deux théorèmes, l'un local, l'autre global, affirmant l'existence des modèles « faiblement $\mathfrak{p}$-simples $\mathfrak{p}$-minimaux » de ces variétés (chap. II, th. 2 et 3). Le premier de ces deux théorèmes permet de munir, d'une manière canonique, le groupe des points rationnels $\mathfrak{p}$-adiques d'une variété abélienne quelconque, définie sur k, d'une structure de *groupe proalgébrique* au sens de Serre [19], défini sur le corps résiduel k^0, et uniquement déterminé, à un k^0-isomorphisme près, par la variété de départ.

---

[1] En particulier, le présent travail a pour origine la recherche d'une démonstration de certaines propriétés des hauteurs des points rationnels d'une variété abélienne définie sur un corps global, en connexion avec un résultat annoncé dans [14].

La démonstration de ces théorèmes est préparée par une étude générale, développée dans le chapitre I[er], des propriétés des points rationnels ou entiers p-adiques sur une variété algébrique quelconque.

Il importe de remarquer que les problèmes relatifs aux divers types de modèles minimaux considérés ne sont pas particuliers aux variétés abéliennes, mais se posent aussi pour les variétés quelconques. Il y aurait lieu, à ce sujet, d'étudier le cas des courbes algébriques quelconques de genre $\geqslant 1$; la version globale du problème relatif aux modèles p-simples p-minimaux est alors voisine, en effet, du problème de l'existence des modèles minimaux sans point multiple des surfaces, au sens de la Géométrie algébrique classique, et on sait que ce dernier est complètement résolu, au moins en caractéristique 0 (voir Zariski [26]) ; il est à prévoir que la solution de ce problème apportera, en même temps, une simplification dans le cas des courbes elliptiques, car, pour les courbes de genre $\geqslant 2$, la possibilité de calculs explicites, analogues à ceux de notre chapitre III, paraît exclue ; d'autre part, on peut espérer que l'étude simultanée des modèles minimaux d'une courbe et de sa jacobienne permettra de compléter les résultats obtenus par Igusa [6] concernant les jacobiennes des « fibres dégénérées » d'une famille de courbes algébriques.

La notion de *schéma* sur un anneau commutatif, au sens de [3], interviendra fréquemment dans ce travail, d'une manière plus ou moins explicite (dans le cas local, il s'agira du schéma, sur l'anneau R de la valuation donnée du corps k, attaché à la variété donnée, ou bien du schéma, sur le corps résiduel k^0, réduit du précédent (mod. $\mathfrak{p}$)). Nous énoncerons, dans le langage des schémas, quelques-uns des principaux résultats. Cependant, faute d'être suffisamment accoutumé à ce langage, nous avons estimé plus prudent de renoncer à son emploi systématique, et d'utiliser le plus souvent un langage dérivé de celui des *Foundations* de Weil ([21], cité [F]), ou de celui de Shimura ([17], cité [R]), laissant les spécialistes se charger de la traduction.

Je tiens à exprimer ma vive reconnaissance à tous ceux qui m'ont apporté leur aide : à S. Lang et A. Weil, dont les suggestions et les encouragements m'ont été d'un grand secours, particulièrement dans la phase initiale de l'élaboration de ce travail ; aux auditeurs d'un séminaire à l'Institut des Hautes Études Scientifiques en 1961-62, consacré à ce travail, et, parmi eux, à J. Dieudonné, A. Grothendieck, J.-P. Serre ; à Michael Artin, qui a bien voulu se charger de revoir les deux premiers chapitres du manuscrit, et à qui je suis redevable de plusieurs corrections ou améliorations.

Enfin, je ne saurais omettre de souligner combien a été précieux pour moi l'accueil que j'ai reçu à l'Institut des Hautes Études Scientifiques, et je tiens à remercier très vivement cet Institut d'avoir bien voulu accepter de faire paraître ce travail dans ses Publications.

CHAPITRE PREMIER

POINTS RATIONNELS $\mathfrak{p}$-ADIQUES SUR LES VARIÉTÉS ALGÉBRIQUES

1. Préliminaires.

On désigne par k un corps muni d'une valuation *discrète* v. On désigne respectivement par R et $\mathfrak{p}$ l'anneau et l'idéal de valuation correspondants, et par k^0 le corps résiduel R/$\mathfrak{p}$. On suppose d'autre part que k^0 est *parfait*. On note $\hat{k}$ et $\hat{\mathrm{R}}$ les complétés respectifs de k et R relativement à v. On se trouve alors, comme on sait, dans l'un des deux cas suivants :

a) Les corps k et k^0 ont *même caractéristique*. Alors $\hat{\mathrm{R}}$ est isomorphe à l'anneau de *séries formelles* $k^0[[t]]$ sur k^0.

b) k est de caractéristique 0, *et* k^0 *de caractéristique* $p \neq 0$. Alors, si $v(p) = e$ est l'ordre de ramification de k relativement à v, l'anneau $\hat{\mathrm{R}}$ est isomorphe à un module libre de rang e sur l'anneau $\mathrm{W}(k^0)$ des *vecteurs de Witt* à coefficients dans k^0; si t est une uniformisante locale de R (i.e. un élément de R tel que $v(t) = 1$), ce module admet pour base $(1, t, \ldots, t^{e-1})$, et t est solution d'une équation d'Eisenstein

$$t^e + a_1 t^{e-1} + \ldots + a_e = 0$$

où les a_i sont des éléments de $\mathrm{W}(k^0)$, tels qu'on ait $v_p(a_i) \geqslant 1$ pour tout i $(1 \leqslant i \leqslant e)$, et $v_p(a_e) = 1$. En particulier, si $e = 1$ (k non ramifié relativement à v), $\hat{\mathrm{R}}$ est isomorphe à $\mathrm{W}(k^0)$.

Quant au corps $\hat{k}$, il est, dans les deux cas *a)* et *b)*, isomorphe au corps des quotients de $\hat{\mathrm{R}}$.

Le point de vue que nous avons décidé d'adopter (celui des *Foundations* de Weil [F]) comporte d'autre part l'introduction de « domaines universels » pour k et k^0. Il est commode de les choisir comme suit : on introduit d'abord un domaine universel arbitraire $\mathfrak{k}^0$ pour k^0, c'est-à-dire un corps contenant k^0, algébriquement clos, et de degré de transcendance infini sur k^0; on supposera de plus que $\mathfrak{k}^0$ possède une base de transcendance non dénombrable sur k^0 (car on aura à introduire des extensions de base de transcendance infinie dénombrable de k^0); on désigne par $\mathfrak{R}$ l'anneau déduit de $\hat{\mathrm{R}}$ « par extension de k^0 à $\mathfrak{k}^0$ », c'est-à-dire défini par $\mathfrak{R} = \mathfrak{k}^0[[t]]$ dans le cas *a)*, et $\mathfrak{R} = \hat{\mathrm{R}} \otimes_{\mathrm{W}(k^0)} \mathrm{W}(\mathfrak{k}^0)$ dans le cas *b)*; on note $\mathfrak{k}$ le corps des quotients de $\mathfrak{R}$; l'anneau $\hat{\mathrm{R}}$

s'identifie naturellement à un sous-anneau de $\mathfrak{R}$, et le corps $\hat{k}$ à un sous-corps de $\mathfrak{k}$; de plus, $\mathfrak{R}$ est un anneau de valuation de $\mathfrak{k}$; la valuation correspondante est discrète, de corps résiduel $\mathfrak{k}^0$, et on peut la normer de manière qu'elle prolonge v (on la désignera encore par v); on a $R = \mathfrak{R} \cap k$; les éléments de $\mathfrak{R}$ sont appelés les *entiers* de $\mathfrak{k}$. On introduit enfin un domaine universel arbitraire Ω pour $\mathfrak{k}$ (donc aussi *a fortiori*, pour k). Les corps k^0 et k, et les domaines universels $\mathfrak{k}^0$ et Ω sont regardés comme fixes, dans toute la suite de ce travail.

Lorsqu'on parlera d'un sous-corps k_1^0 de $\mathfrak{k}^0$, il sera entendu qu'il s'agit d'un sous-corps de $\mathfrak{k}^0$ tel que $\mathfrak{k}^0$ ait une base de transcendance non dénombrable sur k_1^0. De même, lorsqu'on parlera d'un sous-corps k_1 de Ω, il sera entendu qu'il s'agit d'un sous-corps k_1 de Ω tel que Ω soit de degré de transcendance infini sur k_1. Lorsqu'on parlera d'une variété définie sur k_1^0 (resp. k_1) il sera entendu qu'il s'agit d'une variété algébrique « abstraite » au sens de Weil ([F], chap. VII), définie sur ce corps, relativement au domaine universel $\mathfrak{k}^0$ (resp. Ω). Les conventions analogues seront valables lorsqu'on parlera d'un sous-ensemble k_1^0-fermé, k_1^0-ouvert, k_1^0-constructible (resp. k_1-fermé, k_1-ouvert, k_1-constructible), ou d'une sous-k_1^0-variété (resp. d'une sous-k_1-variété) d'une telle variété, ou encore d'un cycle sur une telle variété, rationnel sur k_1^0 (resp. sur k_1).

On adjoindra parfois aux corps $\mathfrak{k}^0$ et Ω un élément, noté ∞. Les ensembles $\mathfrak{k}^0 \cup \infty$ et $\Omega \cup \infty$ seront notés respectivement $\mathfrak{k}_\infty^0$ et Ω_∞. On mettra de même l'indice ∞ pour désigner la réunion d'un sous-corps quelconque de $\mathfrak{k}^0$ ou de Ω avec cet élément. On note ρ l'homomorphisme canonique $\mathfrak{R} \to \mathfrak{R}/\mathfrak{p} = \mathfrak{k}^0$. Il se prolonge d'une manière unique à une place k^0-valuée ρ^* de $\mathfrak{k}$; rappelons qu'une telle place est une application surjective $\rho^* : \mathfrak{k}_\infty \to \mathfrak{k}_\infty^0$, telle qu'on ait $\rho^*(a+b) = \rho^*(a) + \rho^*(b)$, et $\rho^*(a.b) = \rho^*(a).\rho^*(b)$ toutes les fois que les expressions figurant dans les deux membres de ces relations ont un sens, et lorsqu'on fait les conventions habituelles $\infty + a = \infty$, et $\infty . a = \infty$ pour $a \neq 0$. Si k_1 est un sous-corps quelconque de $\mathfrak{k}$, l'image $\rho^*(k_1)_\infty$ est de la forme $(k_1^0)_\infty$, où k_1^0 est un sous-corps de $\mathfrak{k}^0$. On a aussi $k_1^0 = \rho(R_1)$, où $R_1 = \mathfrak{R} \cap k_1$ est l'anneau des entiers de k_1. Par abus de notations, on écrira parfois $k_1^0 = \rho(k_1)$.

Pour tout sous-corps k_1^0 de $\mathfrak{k}$, on désignera par $[k_1^0]^\#$ l'anneau déduit de $\hat{R}$ par extension de k^0 à k_1^0, c'est-à-dire l'anneau de séries entières $k_1^0[[t]]$ dans le cas *a)*, ou l'anneau $\hat{R} \otimes_{W(k^0)} W(k_1^0)$ dans le cas *b)*. Le corps des quotients k_1 de l'anneau $R_1 = [k_1^0]^\#$ s'identifie à un sous-corps de $\mathfrak{k}$; il est complet relativement à la valuation induite par v; on a $R_1 = \mathfrak{R} \cap k_1$, et $k_1^0 = \rho(k_1)$. Ce corps k_1 sera désigné par la notation $(k_1^0)^\#$. En particulier $[k^0]^\#$ et $(k^0)^\#$ coïncident respectivement avec $\hat{R}$ et $\hat{k}$.

On remarquera que, pour tout sous-corps k_1^0 de $\mathfrak{k}^0$, et pour tout sous-corps k_1 de $\mathfrak{k}$, tels qu'on ait $\hat{k}_1 = (k_1^0)^\#$ (ce qui implique $k_1^0 = \rho(k_1)$), les corps $\mathfrak{k}^0$ et Ω sont des domaines universels relatifs à k_1^0 et k_1 respectivement, vérifiant les mêmes conditions que plus haut. Compte tenu de cette remarque tous les résultats qui, dans la suite, sont énoncés en prenant (pour fixer les idées) k^0 et k comme corps de référence restent valables lorsqu'on remplace k^0 et k par k_1^0 et k_1 respectivement.

2. Réduction modulo $\mathfrak{p}$.

L'image $\rho(a)$ d'un élément a de $\mathfrak{R}$ par l'homomorphisme canonique $\rho : \mathfrak{R} \to \mathfrak{k}^0$ sera appelé *élément réduit* (*mod.* $\mathfrak{p}$) de a. Si P est un polynôme à coefficients dans $\mathfrak{R}$, le polynôme à coefficients dans k^0 obtenu en appliquant ρ à chacun de ses coefficients est appelé *polynôme réduit* (mod. $\mathfrak{p}$) de P, et noté $\rho(P)$.

Si I est un idéal de l'anneau $\mathfrak{R}[X] = \mathfrak{R}[X_1, \ldots, X_n]$, l'idéal $\rho(I)$ de $\mathfrak{k}^0[X] = \mathfrak{k}^0[X_1, \ldots, X_n]$, image de I par ρ, est appelé *idéal réduit* (mod. $\mathfrak{p}$) de I. En particulier, soit S un sous-ensemble $\mathfrak{k}$-fermé de l'espace affine $\mathbf{S}_n = \Omega^n$, et prenons pour I l'idéal $\mathfrak{I}(S)$ de $\mathfrak{R}[X]$ composé des polynômes de cet anneau qui s'annulent sur S. L'ensemble des zéros de l'idéal réduit $\rho(I)$ est un sous-ensemble fermé de l'espace affine $\mathbf{S}_n^0 = (\mathfrak{k}^0)^n$, qu'on appelle *ensemble réduit* (mod. $\mathfrak{p}$) de S, et qu'on note $\rho_e(S)$. Si k_1 est un sous-corps de $\mathfrak{k}$ tel que S soit k_1-fermé, et si $k_1^0 = \rho(k_1)$, l'ensemble $\rho_e(S)$ est k_1^0-fermé.

Si V est une sous-variété de $\mathbf{S}_n$, définie sur $\mathfrak{k}$ (resp. si X est un cycle sur $\mathbf{S}_n$, rationnel sur $\mathfrak{k}$), de dimension r, on sait lui associer un cycle positif (resp. un cycle) sur $\mathbf{S}_n^0$, de dimension r, appelé *cycle réduit* (mod. $\mathfrak{p}$) de V (resp. de X), de manière que cette opération de réduction vérifie les propriétés énoncées dans ([F], X, 5); ce cycle sera désigné par $\rho(V)$ (resp. $\rho(X)$). Si k_1 est un sous-corps de $\mathfrak{k}$ tel que V soit définie sur k_1 (resp. tel que X soit rationnel sur k_1), alors $\rho(V)$ (resp. $\rho(X)$) est rationnel sur k_1^0. Le cycle $\rho(V)$ admet pour support l'ensemble réduit $\rho_e(V)$. Pour la construction du cycle $\rho(V)$, et pour l'étude de ses propriétés, nous renvoyons à Shimura [R].

3. L'anneau local $\mathfrak{o}(x^0, V)$.

Soit V une variété affine, définie sur $\mathfrak{k}$, de dimension r, et soit $V^0 = \rho(V)$ son cycle réduit (mod. $\mathfrak{p}$). Soit f une fonction rationnelle sur V, définie sur $\mathfrak{k}$, et soit x^0 un point de l'ensemble réduit $\rho_e(V) = \operatorname{supp} V^0$. Alors f est induite par un quotient P/Q de polynômes à coefficients dans $\mathfrak{R}$. Posons $P^0 = \rho(P)$ et $Q^0 = \rho(Q)$. Si, pour f et x^0 donnés, on peut choisir P et Q de manière qu'on ait $Q^0(x^0) \neq 0$, on dira que la fonction f est $\mathfrak{p}$-*morphique en* x^0; l'expression $P^0(x^0)/Q^0(x^0)$ sera dite *valeur de* f *en* x^0, et sera notée $f^0(x^0)$; il est clair que cette valeur ne dépend pas du choix des polynômes P et Q.

L'ensemble des fonctions sur V définies sur $\mathfrak{k}$ (resp. sur un sous-corps k_1 de $\mathfrak{k}$ contenant k, et tel que x^0 soit rationnel sur $k_1^0 = \rho(k_1)$) qui sont $\mathfrak{p}$-morphiques en x^0 est un anneau local, appelé *anneau local de* V *en* x^0 (resp. de V en x^0 relatif à k_1), qu'on notera $\mathfrak{o}(x^0, V)$ (resp. $\mathfrak{o}_{k_1}(x^0, V)$). Il résulte de ([R], n° 1, prop. 7) que l'anneau local $\mathfrak{o}_{k_1}(x^0, V)$ est aussi l'ensemble des fonctions sur V qui sont induites par un quotient P_1/Q_1 de polynômes *à coefficients dans l'anneau* $R_1 = \mathfrak{R} \cap k_1$ *des entiers de* k_1, tels que $Q_1^0(x^0) \neq 0$. L'idéal maximal de l'anneau $\mathfrak{o}(x^0, V)$ (resp. $\mathfrak{o}_{k_1}(x^0, V)$) est noté $\mathfrak{m}(x^0, V)$ (resp. $\mathfrak{m}_{k_1}(x^0, V)$). Il se compose des fonctions f qui *s'annulent en* x^0, c'est-à-dire telles que, pour un choix convenable de P et Q, on ait $P^0(x^0) = 0$, et $Q^0(x^0) \neq 0$.

Posons, pour simplifier, $\mathfrak{o} = \mathfrak{o}(x^0, V)$ (resp. $\mathfrak{o}_1 = \mathfrak{o}_{k_1}(x^0, V)$) et, de même $\mathfrak{m} = \mathfrak{m}(x^0, V)$ (resp. $\mathfrak{m}_1 = \mathfrak{m}_{k_1}(x^0, V)$). Le quotient $\mathfrak{o}/\mathfrak{m}$ (resp. $\mathfrak{o}_1/\mathfrak{m}_1$) est isomorphe à $\mathfrak{k}$ (resp. k_1).

Le quotient $\mathfrak{m}/\mathfrak{m}^2$ (resp. $\mathfrak{m}_1/\mathfrak{m}_1^2$) s'identifie à un espace vectoriel sur $\mathfrak{k}$ (resp. k_1), de dimension $r+1$, appelé *espace tangent de Zariski de* V *en* x^0 (resp. de V en x^0 relatif à k_1) et que nous noterons $Z(x^0, V)$ (resp. $Z_{k_1}(x^0, V)$).

Soient maintenant V et W deux variétés affines, définies sur $\mathfrak{k}$, et considérons une application rationnelle $\varphi : V \to W$, définie sur $\mathfrak{k}$. Soit x^0 un point de $\rho_e(V)$. Soient $y_j = \varphi_j(x) = \varphi_j(x_1, \ldots, x_n)$ $(1 \leqslant j \leqslant m)$ les formules définissant φ. Si chacune des fonctions φ_j (coordonnées de φ), est $\mathfrak{p}$-morphique en x^0, on dira que φ est $\mathfrak{p}$-*morphique en* x^0. Le point y^0 ayant pour coordonnées les $y_j^0 = \varphi_j^0(x^0)$ sera appelé *valeur de* φ *en* x^0, et noté $\varphi^0(x^0)$. On a $y^0 \in \rho_e(W)$. De plus, φ induit un $\mathfrak{R}$-homomorphisme de $\mathfrak{o}(y^0, W)$ dans $\mathfrak{o}(x^0, V)$; cet homomorphisme est local, c'est-à-dire applique $\mathfrak{m}(y^0, W)$ dans $\mathfrak{m}(x^0, V)$; par passage au quotient, on en déduit un homomorphisme canonique $\varphi_{x^0}^0 : Z(y^0, W) \to Z(x^0, V)$. Si V, W et φ sont définies sur un même sous-corps k_1 de $\mathfrak{k}$, contenant k, tel que x^0 soit rationnel sur $k_1^0 = \rho(k_1)$, et si $R_1 = \mathfrak{R} \cap k_1$ est l'anneau des entiers de k_1, l'application φ induit, de même, un R_1-homomorphisme local de $\mathfrak{o}_{k_1}(y^0, W)$ dans $\mathfrak{o}_{k_1}(x^0, V)$, d'où l'on déduit, par passage au quotient, un k_1^0-homomorphisme de $Z_{k_1}(y^0, W)$ dans $Z_{k_1}(x^0, V)$. Dans le cas où φ est une application birationnelle, on dira que φ est $\mathfrak{p}$-*isomorphique en* x^0 si φ^{-1} est $\mathfrak{p}$-morphique en $y^0 = \varphi^0(x^0)$ (ce qui implique $x^0 = (\varphi^{-1})^0(y^0)$). Chacun des homomorphismes que nous venons de considérer est alors un isomorphisme.

Si $\varphi : V \to W$ est un $\mathfrak{k}$-morphisme (resp. un k_1-morphisme), et si φ est $\mathfrak{p}$-morphique en tout point de $\rho_e(V)$, on dira que φ est un $\mathfrak{R}$-*morphisme* (resp. un R_1-morphisme). Si φ et φ^{-1} sont des $\mathfrak{R}$-morphismes (resp. des R_1-morphismes), on dit que φ est un $\mathfrak{R}$-isomorphisme (resp. un R_1-isomorphisme). Désignons par $\mathscr{I}(V)$ (resp. $\mathscr{I}_{R_1}(V)$) l'idéal de $\mathfrak{R}[X]$ (resp. $R_1[X]$) composé des polynômes qui s'annulent sur V, et $\mathscr{A}(V)$ (resp. $\mathscr{A}_{R_1}(V)$) l'anneau de coordonnées $\mathfrak{R}[X]/\mathscr{I}(V)$ (resp. $R_1[X]/\mathscr{I}_{R_1}(V)$); notons $\mathbf{S}_{\mathfrak{R}}(V)$, ou simplement $\mathbf{S}(V)$ (resp. $\mathbf{S}_{R_1}(V)$) et appelons *schéma* sur $\mathfrak{R}$ (resp. sur R_1) *attaché à* V le schéma affine Spec $\mathscr{A}(V)$ (resp. Spec $\mathscr{A}_{R_1}(V)$) (cf. [3], chap. I[er], § 1). La donnée d'un $\mathfrak{R}$-morphisme (resp. d'un R_1-morphisme) $V \to W$ se traduit par celle d'un $\mathfrak{R}$-morphisme $\mathbf{S}(V) \to \mathbf{S}(W)$ (resp. d'un R_1-morphisme $\mathbf{S}_{R_1}(V) \to \mathbf{S}_{R_1}(W)$); la donnée de la classe de V à un $\mathfrak{R}$-isomorphisme près (resp. à un R_1-isomorphisme près) est équivalente à celle de $\mathbf{S}(V)$ (resp. $\mathbf{S}_{R_1}(V)$).

Soit encore $\varphi : V \to W$ une application rationnelle, et supposons V, W et φ définies sur un sous-corps k_1 de $\mathfrak{k}$. Posons $k_1^0 = \rho(k_1)$. Soit X^0 une k_1^0-variété contenue dans $\rho_e(V)$, et soit x^0 un point générique de X^0 sur k_1^0. On dira que l'application φ est *génériquement* $\mathfrak{p}$-*morphique sur* X^0 si φ est $\mathfrak{p}$-morphique en x^0. Cette propriété ne dépend pas, pour X^0 donnée, du choix de k_1 et x^0. Le point $y^0 = \varphi^0(x^0)$ est générique sur k_1^0 d'une k_1^0-variété Y^0, contenue dans $\rho_e(W)$, qu'on désignera par $\varphi_g^0(X^0)$. Si X^0 est une variété (au sens absolu), il en est de même de Y^0. Il existe une et une seule application rationnelle $\varphi | X^0 : X^0 \to Y^0$, définie sur k_1^0, et telle que $y^0 = (\varphi | X^0)(x^0)$.

Cette application $\varphi | X^0$ est appelée *application rationnelle induite* par φ sur X^0.

Ces définitions s'appliquent, en particulier, au cas où W est la droite affine $\mathbf{S}_1$; φ s'identifie alors à une fonction f sur V. Si X^0 est une variété (resp. une k_1^0-variété),

l'ensemble des fonctions sur V (resp. des fonctions sur V définies sur k_1) qui sont génériquement p-morphiques sur X^0 est un anneau local, qu'on appelle *anneau local de* V *en* X^0 (resp. de V en X^0 relatif à k_1), et qu'on note $\mathfrak{o}(X^0, V)$ (resp. $\mathfrak{o}_{k_1}(X^0, V)$). Son idéal maximal, composé des fonctions qui s'annulent sur X^0, est noté $\mathfrak{m}(X^0, V)$ (resp. $\mathfrak{m}_{k_1}(X^0, V)$).

Soient à nouveau V et W deux variétés affines, et soit $\varphi : V \to W$ une application rationnelle, définies sur $\mathfrak{k}$. Soit $\Gamma = \Gamma_\varphi$ le graphe de φ. Soit E^0 un sous-ensemble quelconque de $\rho_e(V)$. L'ensemble des points $y^0 \in \rho_e(W)$ pour lesquels il existe au moins un $x^0 \in \rho_e(V)$ tel que $(x^0, y^0) \in \rho_e(\Gamma)$ est appelé *transformé ensembliste* de E^0 par φ, et noté $\varphi^0_e(E^0)$. Si E^0 est un ensemble *constructible* (intersection d'un ouvert et d'un fermé de l'espace affine), il en est de même de $\varphi^0_e(E^0)$. Si E^0 est réduit à un point x^0, l'ensemble $\varphi^0_e(x^0)$ sera aussi appelé *ensemble des valeurs* de φ en x^0. Si, en particulier, φ est p-morphique en x^0, on a $\varphi^0_e(x^0) = \{\varphi^0(x^0)\}$.

Les propositions suivantes résultent immédiatement des définitions, et des résultats de [R] :

Proposition 1. — *Soient* U, V, W *trois variétés affines, définies sur* $\mathfrak{k}$, *et soient* $\varphi : U \to V$ *et* $\psi : V \to W$ *des applications rationnelles, définies sur k. Soit* θ *l'application rationnelle composée* $\theta = \psi \circ \varphi : U \to W$. *Soit* x^0 *un point de* $\rho_e(U)$.

(i) *Si* φ *est* p*-morphique en* x^0, *on a* $\theta^0_e(x^0) = \psi^0_e(\varphi^0(x^0))$.

(ii) *Si* ψ *est* p*-morphique en un point* y^0 *de* $\varphi^0_e(x^0)$, *et si* $z^0 = \psi^0(y^0)$, *on a* $z^0 \in \theta^0_e(x^0)$.

(iii) *Si* φ *est* p*-morphique en* x^0, *et si* ψ *est* p*-morphique en* $y^0 = \varphi^0(x^0)$, θ *est* p*-morphique en* x^0, *et on a* $\theta^0(x^0) = \psi^0(\varphi^0(x^0))$.

Proposition 2. — *Soient* U, V, W *trois variétés affines, définies sur* $\mathfrak{k}$, *et soient* $\varphi : U \to V$ *et* $\psi : U \to W$ *des applications rationnelles, définies sur k. Soit* θ *l'application* $\theta = \varphi \times \psi : U \to V \times W$. *Soit* x^0 *un point de* $\rho_e(U)$. *Alors on a* $\theta^0_e(x^0) = \varphi^0_e(x^0) \times \psi^0_e(x^0)$. *Pour que* θ *soit* p*-morphique en* x^0, *il faut et il suffit que* φ *et* ψ *le soient, et on a alors* $\theta^0(x^0) = \varphi^0(x^0) \times \psi^0(x^0)$.

Proposition 3. — *Soient* U, V, W *trois variétés affines, définies sur* $\mathfrak{k}$. *Soit* $\varphi : U \to V$ *une application rationnelle, définie sur k, et soit* ψ *l'application* $U \times W \to V$ *telle qu'on ait* $\psi(x, z) = \varphi(x)$, *si* x *et* z *sont des points génériques indépendants sur k de* U *et* W *respectivement. Soient* x^0 *un point de* $\rho_e(U)$ *et* z^0 *un point de* $\rho_e(W)$. *Alors on a* $\psi^0_e(x^0, z^0) = \varphi^0_e(x^0)$. *Pour que* ψ *soit* p*-morphique en* (x^0, z^0), *il faut et il suffit que* φ *le soit en* x^0, *et on a alors* $\psi^0(x^0, z^0) = \varphi^0(x^0)$.

4. p-variétés.

Considérons une variété abstraite $V = \{V_\alpha; T_{\beta\alpha}\}$ au sens de Weil ([F], chap. VII), définie sur un sous-corps k_1 de $\mathfrak{k}$. Pour tout couple (α, β), notons $\Gamma_{\beta\alpha}$ le graphe de la transformation $T_{\beta\alpha}$. Nous dirons, avec Shimura que V est une p-*variété* si, quels que soient $x^0_\alpha \in \rho_e(V_\alpha)$ et $x^0_\beta \in \rho_e(V_\beta)$ tels que $(x^0_\alpha, x^0_\beta) \in \rho_e(\Gamma_{\beta\alpha})$ (i.e. tels que x^0_β appartienne à l'ensemble des valeurs de $T_{\beta\alpha}$ en x^0_α), l'application φ est p-isomorphique en x^0_α (chez Shimura, ([R], n° 4), les V_α sont remplacés par des $\mathfrak{k}$-ouverts $U_\alpha = V_\alpha - F_\alpha$ de variétés affines V_α, et les $\rho_e(V_\alpha)$ par des sous-ensembles de la forme $\rho_e(V_\alpha) - F^0_\alpha$, où, pour tout α, F^0_α est un sous-ensemble fermé de $\rho_e(V_\alpha)$ contenant $\rho_e(F_\alpha)$; cette différence n'est cependant

pas essentielle; on sait en effet que, si V est une variété affine définie sur $\mathfrak{k}$, F un sous-ensemble $\mathfrak{k}$-fermé de V, et F^0 un sous-ensemble fermé de $\rho_e(V)$ contenant $\rho_e(F)$, il existe un $\mathfrak{k}$-modèle affine (W, φ) de V tel que φ applique $\mathfrak{k}$-isomorphiquement $U = V - F$ sur W et applique $\mathfrak{p}$-isomorphiquement $U^0 = \rho_e(V) - F^0$ sur $\rho_e(W)$; autrement dit tel que le schéma sur $\mathfrak{R}$ induit par $\mathbf{S}(V)$ sur l'ouvert défini par le couple (U, U^0) soit $\mathfrak{R}$-isomorphe au schéma affine $\mathbf{S}(W)$).

Nous dirons qu'une $\mathfrak{p}$-variété est *non dégénérée* (*mod.* $\mathfrak{p}$) (Shimura emploie ici le terme $\mathfrak{p}$-simple, mais nous avons préféré réserver à ce dernier une autre signification) s'il existe un α tel que le cycle $V^0_\alpha = \rho(V_\alpha)$ se réduise à une variété (plus correctement, admette une composante unique, de coefficient 1). Il en est alors de même de V^0_β pour tout β. Pour tout couple (α, β), l'application $T^0_{\beta\alpha} = T_{\beta\alpha} | V^0_\alpha$ induite par $T_{\beta\alpha}$ sur V^0_α est une application birationnelle $V^0_\alpha \to V^0_\beta$. Puisque le graphe $\Gamma^0_{\beta\alpha}$ de $T^0_{\beta\alpha}$ est une composante de $\rho_e(T_{\beta\alpha})$, et d'après la définition d'une $\mathfrak{p}$-variété, $T^0_{\beta\alpha}$ est isomorphique en x^0_α de valeur x^0_β, pour tout couple (x^0_α, x^0_β) appartenant à $\Gamma^0_{\beta\alpha}$. Autrement dit le système $\{V^0_\alpha, T^0_{\beta\alpha}\}$ définit une variété abstraite V^0 dite *réduite* (*mod.* $\mathfrak{p}$) *de* V (cf. [R], n° 4), qu'on notera encore $\rho(V)$. A tout cycle Z sur V, rationnel sur $\mathfrak{k}$, on associe un cycle Z^0 sur V^0, qu'on appelle *cycle réduit* (*mod.* $\mathfrak{p}$) *de* Z, et qu'on note $\rho(Z)$; pour la définition de ce cycle, on se ramène au cas des variétés affines; l'opération de réduction, ainsi généralisée, vérifie encore les conditions de ([F], X, 5). En particulier, on sait définir le cycle $\rho(W)$ pour toute sous-variété de W, définie sur $\mathfrak{k}$.

Si V est une $\mathfrak{p}$-variété sans point multiple, nous dirons qu'elle est *strictement non dégénérée* (*mod.* $\mathfrak{p}$) si elle est non dégénérée (mod. $\mathfrak{p}$), et si $V^0 = \rho(V)$ est une variété sans point multiple. Nous conviendrons une fois pour toutes d'apporter au sens du mot $\mathfrak{p}$-variété la restriction suivante : lorsque nous parlerons d'une $\mathfrak{p}$-*variété*, il sera entendu qu'il s'agit d'une sous-$\mathfrak{p}$-variété d'une $\mathfrak{p}$-variété ambiante **V** sans point multiple, définie sur $\mathfrak{k}$, et strictement non dégénérée (mod. $\mathfrak{p}$). Ainsi, on pourra toujours parler du cycle réduit $V^0 = \rho(V)$.

Toute variété affine ou projective, définie sur $\mathfrak{k}$, est une $\mathfrak{p}$-variété. Toute sous-variété, définie sur $\mathfrak{k}$, d'une $\mathfrak{p}$-variété, tout produit de deux $\mathfrak{p}$-variétés, au sens où nous entendons désormais ce terme, est encore une $\mathfrak{p}$-variété. On peut, d'autre part, étendre d'une manière évidente la signification des symboles $\rho_e(V)$, $\mathfrak{o}(x^0, V)$, $\mathfrak{o}_{k_1}(x^0, V)$, $\mathfrak{o}(X^0, V)$, $\mathbf{S}_{\mathfrak{R}}(V)$, etc., au cas où V est une $\mathfrak{p}$-variété, et conserver la terminologie correspondante (fonction ou application rationnelle $\mathfrak{p}$-morphique en x^0, ou génériquement $\mathfrak{p}$-morphique sur X^0, etc.). Les propositions 1, 2 et 3 s'étendent immédiatement au cas où U, V, W sont des $\mathfrak{p}$-variétés.

5. $\mathfrak{p}$-spécialisations.

Soit k_1 un sous-corps de $\mathfrak{k}$; soit $R_1 = k_1 \cap \mathfrak{R}$ l'anneau des entiers de k_1; posons $k^0_1 = \rho(k_1)$, et soit ρ_1 l'application canonique $\rho_1 = \rho | R_1 : R_1 \to k^0_1$, induite par ρ. Soient $x^0 = (x^0_1, \ldots, x^0_n)$ un élément de $(\mathfrak{k}^0_\infty)^n$, et x un élément de $(\Omega_\infty)^n$. Nous dirons, avec Shimura, que x^0 est une *spécialisation de* x *sur* R_1 s'il existe une place $\mathfrak{k}^0$-valuée $\tilde{\rho}$ de Ω,

prolongeant ρ_1, telle que $x_i^0 = \tilde{\rho}(x_i)$ pour tout i; nous dirons aussi que x est une *généralisation de* x^0 *sur* R_1. De même, nous dirons que x^0 est une spécialisation de x sur $\mathfrak{R}$, ou une $\mathfrak{p}$-*spécialisation de* x s'il existe une place $\mathfrak{k}^0$-valuée $\tilde{\rho}$ de Ω, prolongeant ρ, telle que $x_i^0 = \tilde{\rho}(x_i)$ pour tout i; nous dirons aussi que x est une $\mathfrak{p}$-*généralisation de* x^0; pour que x^0 soit une $\mathfrak{p}$-spécialisation de x, il faut et il suffit que x^0 soit une spécialisation de x sur R_1 quel que soit R_1.

Nous dirons qu'une spécialisation sur R_1 (resp. une $\mathfrak{p}$-spécialisation) x^0 de x est *finie* si les x_i^0 sont distincts de ∞ i.e. si $x^0 \in \mathbf{S}_n^0$ (ce qui implique $x \in \mathbf{S}_n$). Supposons $x^0 \in \mathbf{S}_n^0$, et $x \in \mathbf{S}_n$; pour que x^0 soit une spécialisation (finie) de x sur R_1 (resp. une $\mathfrak{p}$-spécialisation (finie) de x), il faut et il suffit que, *pour tout polynôme* P *appartenant à* R[X] (resp. $\mathfrak{R}[X]$) *s'annulant en* x, *le polynôme réduit* $P^0 = \rho(P)$ *s'annule en* x^0. Nous dirons que deux spécialisations sur R_1 (resp. deux $\mathfrak{p}$-spécialisations) x^0 de x et y^0 de y sont *compatibles* si (x^0, y^0) est une spécialisation de (x, y) sur R_1 (resp. une $\mathfrak{p}$-spécialisation de (x, y)).

Si V est une variété affine, définie sur k_1 (resp. $\mathfrak{k}$), et si $\bar{x}$ est un point générique de V sur k_1 (resp. $\mathfrak{k}$), il résulte de ([R], n° 3, th. 7) que l'ensemble $\rho_e(V)$ coïncide avec celui de toutes les spécialisations finies de $\bar{x}$ sur R_1 (resp. de toutes les $\mathfrak{p}$-spécialisations finies de $\bar{x}$).

Soit maintenant $V = \{V_\alpha, T_{\beta\alpha}\}$ une $\mathfrak{p}$-variété, définie sur k_1. Soient x un point de V, et $\tilde{\rho}$ une place $\mathfrak{k}$-valuée de Ω prolongeant ρ (resp. ρ_1). Supposons qu'il existe un α tel que x soit représenté dans V_α, et que $x_\alpha^0 = \tilde{\rho}(x_\alpha)$ soit une spécialisation *finie* de x sur R_1. Alors x_α^0 représente un point x^0 de $\rho_e(V)$, qui ne dépend pas de α. Ce point est noté $x^0 = \tilde{\rho}(x)$, et est appelé une *spécialisation finie de* x *sur* R_1 (resp. une $\mathfrak{p}$-*spécialisation finie de* x). Si $\bar{x}$ est un point générique de V sur k_1 (resp. $\mathfrak{k}$), l'ensemble $\rho_e(V)$ coïncide avec celui des spécialisations finies de $\bar{x}$ sur R_1 (resp. des $\mathfrak{p}$-spécialisations finies) de $\bar{x}$.

Si $\bar{x}$ est un point générique de V sur $\mathfrak{k}$, et si $\tilde{\rho}(\bar{x})$ est défini, quelle que soit la place $\tilde{\rho}$ prolongeant ρ (i.e. si à toute place k^0-valuée $\tilde{\rho}$ de Ω prolongeant ρ correspond un point de $\rho_e(V)$), on dit que la variété V est $\mathfrak{p}$-*complète* (cf. [R], n° 4). En particulier, toute variété projective définie sur $\mathfrak{k}$ est $\mathfrak{p}$-complète; une sous-$\mathfrak{p}$-variété d'une $\mathfrak{p}$-variété $\mathfrak{p}$-complète, ou un produit de deux $\mathfrak{p}$-variétés $\mathfrak{p}$-complètes, est encore une $\mathfrak{p}$-variété $\mathfrak{p}$-complète.

Si $\varphi : V \to W$ est une application rationnelle, définie sur $\mathfrak{k}$, d'une $\mathfrak{p}$-variété V dans une $\mathfrak{p}$-variété $\mathfrak{p}$-complète W, l'ensemble $\varphi_e^0(x^0)$ des valeurs de φ en x^0 n'est jamais vide. Si f est une fonction sur une $\mathfrak{p}$-variété V, on peut la prolonger en une application rationnelle f_* de V dans la droite projective $\mathbf{P}_1$ (dont l'ensemble des points peut être identifié à $\mathfrak{k}_\infty^0$). On dira que f est *définie* en x^0 si f_* est $\mathfrak{p}$-morphique en ce point, c'est-à-dire si f ou $1/f$ est $\mathfrak{p}$-morphique en ce point. Si f est définie, mais non $\mathfrak{p}$-morphique en x^0, on a $f_*^0(x^0) = \infty$. On conviendra alors de dire que f est infinie en x^0, et d'écrire $f^0(x^0) = \infty$.

6. Rappel de quelques propriétés des vecteurs de Witt. Unification des notations des cas *(a)* et *(b)*.

Commençons par rappeler quelques-unes des propriétés de l'anneau des vecteurs de Witt $W(\mathfrak{k}^0)$, le corps $\mathfrak{k}^0$ étant supposé de caractéristique p (pour un exposé plus détaillé, nous renvoyons à [11], [20], [25]).

On sait qu'il existe un et un seul *système multiplicatif de représentants* de $\mathfrak{k}^0$ dans $W(\mathfrak{k}^0)$, c'est-à-dire une et une seule application injective $\eta : \mathfrak{k}^0 \to W(\mathfrak{k}^0)$ telle que $\rho \circ \eta : \mathfrak{k}^0 \to \mathfrak{k}^0$ soit l'identité, et telle qu'on ait $\eta(a^0 b^0) = \eta(a^0)\eta(b^0)$ pour tout couple (a^0, b^0) d'éléments de $\mathfrak{k}^0$.

L'anneau $W(k^0)$ est complet pour la topologie (dite $\mathfrak{p}$-adique) définie par les puissances de $\mathfrak{p} = (p)$; tout élément x de $W(\mathfrak{k}^0)$ peut être exprimé, d'une manière et d'une seule, sous la forme

$$x = \sum_{\mu=0}^{\infty} \eta(x^{(\mu)})^{p^{-\mu}} p^{\mu} \tag{1}$$

où les x^{μ} sont des éléments de $\mathfrak{k}^0$ qu'on appelle les *composantes* de x. Pour qu'on ait $x \equiv y \pmod{\mathfrak{p}^{\mu}}$, il faut et il suffit qu'on ait $x^{(0)} = y^{(0)}, \ldots, x^{(\mu-1)} = y^{(\mu-1)}$. L'intérêt de la représentation de x sous la forme (1) (avec l'exposant $p^{-\mu}$ pour le terme en p^{μ}) réside dans le fait que les composantes de $x+y$, $x-y$ et xy s'expriment par des polynômes en fonction de celles de x et y. Plus précisément, soient $x^{(0)}, \ldots, x^{(\mu)}, \ldots$ les composantes de x, et $y^{(0)}, \ldots, y^{(\mu)}, \ldots$ celles de y. Alors les composantes de $u = x+y$ ont pour valeurs

$$\begin{cases} u^{(0)} = x^{(0)} + y^{(0)} \\ u^{(1)} = x^{(1)} + y^{(1)} + \mathrm{P}_1^+(x^{(0)}, y^{(0)}) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ u^{(\mu)} = x^{(\mu)} + y^{(\mu)} + \mathrm{P}_{\mu}^+(x^{(0)}, y^{(0)}, \ldots, x^{(\mu-1)}, y^{(\mu-1)}) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{cases} \tag{2}$$

où les P_{μ}^+ sont des polynômes universels à coefficients dans le corps premier $\mathbf{F}_p$. En particulier, le polynôme $\mathrm{P}_1^+(\mathrm{X}, \mathrm{Y})$ est celui déduit de $\mathrm{Q}_1^+ = \frac{1}{p}((\mathrm{X}+\mathrm{Y})^p - \mathrm{X}^p - \mathrm{Y}^p)$ par réduction (mod. $\mathfrak{p}$).

Les formules donnant les composantes de $x-y$ sont analogues, et se déduisent des précédentes en remplaçant pour tout μ, la somme $x^{(\mu)} + y^{(\mu)}$ par $x^{(\mu)} - y^{(\mu)}$ et les polynômes P_{μ}^+ par des polynômes P_{μ}^-, également universels, et à coefficients dans $\mathbf{F}_p$. Celles donnant les composantes du produit $v = xy$ sont de la forme

$$\begin{cases} v^{(0)} = x^{(0)} y^{(0)} \\ v^{(1)} = (x^{(0)})^p y^{(1)} + x^{(1)} (y^{(0)})^p + \mathrm{P}_1^{\times}(x^{(0)}, y^{(0)}) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ v^{(\mu)} = \sum_{\nu=0}^{\mu} (x^{(\nu)})^{p^{\mu-\nu}} (y^{(\mu-\nu)})^{p^{\nu}} + \mathrm{P}_{\mu}^{\times}(x^{(0)}, y^{(0)}, \ldots, x^{(\mu-1)}, y^{(\mu-1)}) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{cases} \tag{3}$$

où les $\mathrm{P}_{\mu}^{\times}$ sont encore universels, et à coefficients dans $\mathbf{F}_p$.

Si on a $y^{(0)} = \rho(y) \neq 0$, i.e. si y est inversible, le quotient $z = x/y$ appartient encore à $W(\mathfrak{k}^0)$, et ses composantes s'expriment rationnellement en fonction de celles de x et y. Plus précisément, elles sont données par des formules de la forme

$$z^{(\mu)} = (y^{(0)})^{-(\mu+1)} \mathrm{Q}_{\mu}(x^{(0)}, y^{(0)}, \ldots, x^{(\mu)}, y^{(\mu)}) \quad (\mu \geqslant 0) \tag{4}$$

où, pour tout $\mu \geqslant 0$, Q_{μ} est un polynôme universel à coefficients dans $\mathbf{F}_p$, et dans lequel $x^{(\mu)}$ et $y^{(\mu)}$ interviennent linéairement.

Dans le cas où $v(x) \geqslant v(y) = \sigma$, i.e. où $x^{(0)} = y^{(0)} = \ldots = x^{(\sigma-1)} = y^{(\sigma-1)} = 0$, et $y^{(\sigma)} \neq 0$, le quotient $z = x/y$ appartient toujours à $W(\mathfrak{k}^0)$, mais ses composantes ne s'expriment plus rationnellement en fonction de celles de x et y; leur calcul comporte l'extraction d'une racine p^σ-ième; on a en effet, pour tout $\mu \geqslant 0$,

$$(5) \qquad (z^{(\mu)})^{p^\sigma} = (y^{(\sigma)})^{-(\mu+1)} Q_\mu(x^{(\sigma)}, y^{(\sigma)}, \ldots, x^{(\sigma+\mu)}, y^{(\sigma+\mu)})$$

où les Q_μ sont les mêmes polynômes que dans la formule (4) (pour déduire (5) de (4), il suffit de remarquer que, dans le cas où $y = p^\sigma$, on a $(z^{(\mu)})^{p^\sigma} = x^{(\sigma+\mu)}$ pour tout $\mu \geqslant 0$).

Revenons maintenant à l'anneau $\mathfrak{R}$ introduit au n° 1. Nous allons, pour représenter les éléments de $\mathfrak{R}$, introduire une notation qui nous permettra de traiter simultanément les deux cas *a)* et *b)* (égales ou inégales caractéristiques). Dans le cas *a)*, $\mathfrak{R}$ est isomorphe à l'anneau de séries formelles $\mathfrak{k}^0[[t]]$; tout élément x de $\mathfrak{R}$ s'écrit donc, d'une manière et d'une seule, sous la forme

$$(6) \qquad x = \Sigma_{\mu=0}^{\infty} x^{(\mu)} t^\mu$$

où les $x^{(\mu)}$ appartiennent à $\mathfrak{k}^0$.

Dans le cas *b)*, l'anneau $\mathfrak{R}$ est engendré, comme $W(\mathfrak{k}^0)$-module, par les puissances $1, t, \ldots, t^{e-1}$ d'une uniformisante locale t. Tout élément x de $\mathfrak{R}$ peut donc s'écrire, d'une manière et d'une seule, sous la forme

$$(7) \qquad x = \Sigma_{\mu=0}^{\infty} (\eta(x^{(\mu)}))^{p^{-q(\mu)}} t^{r(\mu)} p^{q(\mu)}$$

où $q(\mu)$ et $r(\mu)$ désignent respectivement le quotient et le reste de la division de μ par e, et où les $x^{(\mu)}$ sont des éléments de $\mathfrak{k}^0$. Si, en particulier, k est non ramifié relativement à v (i.e. si $e = 1$), l'anneau $\mathfrak{R}$ est isomorphe à $W(\mathfrak{k}^0)$, et les $x^{(\mu)}$ sont les composantes de x, regardé comme vecteur de Witt.

Nous dirons dans le cas *a)* (resp. *b)*) que les éléments $x^{(\mu)}$ de $\mathfrak{k}^0$ figurant dans la formule (6) (resp. (7)) sont les *coefficients* de x. La donnée de x est toujours équivalente à celle de la suite de ses coefficients. Nous écrirons, dans les deux cas

$$x = (x^{(0)}, x^{(1)}, \ldots, x^{(\mu)}, \ldots)$$

On a, dans les deux cas *a)* et *b)*, $x \in \hat{R}$ si et si seulement $x^{(\mu)} \in k^0$ pour tout μ. On remarquera, d'autre part, qu'on a, dans le cas *b)*, pour tout $\mu \geqslant 0$,

$$v(t^{r(\mu)} p^{q(\mu)}) = r(\mu) + eq(\mu) = \mu.$$

Donc, dans les deux cas *a)* et *b)*, pour qu'on ait $x \equiv y \pmod{\mathfrak{p}^\mu}$ il faut et il suffit qu'on ait $x^{(\nu)} = y^{(\nu)}$ pour tout $\nu < \mu$.

On désignera par F l'automorphisme de $\mathfrak{k}$ (pour la structure de corps valué complet), défini comme suit : dans le cas *a)*, F est l'identité et, dans le cas *b)*, F fait correspondre à l'élément $x = (x^{(0)}, \ldots, x^{(\mu)}, \ldots)$ de $\mathfrak{R}$ l'élément $\bar{x} = ((x^{(0)})^p, \ldots, (x^{(\mu)})^p, \ldots)$ de $\mathfrak{R}$ obtenu en appliquant à chaque coefficient de x l'automorphisme de Frobenius F^0 de k^0.

Pour tout polynôme P (resp. pour toute fraction rationnelle f), à coefficients dans $\mathfrak{k}$, on note $\overline{P}$ (resp. $\bar{f}$) le polynôme (resp. la fraction rationnelle) qui s'en déduit par application de F à chacun de ses coefficients.

Il résulte des propriétés des séries formelles, et de celles des vecteurs de Witt rappelées plus haut (formules (2) et (3)) que, si x et y sont deux éléments de $\mathfrak{R}$, les coefficients d'indice μ de $x+y$, $x-y$, $x.y$ s'expriment par des polynômes en fonction de ceux d'indice $\leqslant\mu$ de x et y, dans lesquels $x^{(\mu)}$ et $y^{(\mu)}$ interviennent linéairement. Dans le cas *a)* et, dans le cas *b)*, si k est non ramifié, ces polynômes sont universels, et à coefficients dans le corps premier; si dans le cas *b)*, k est ramifié, ces polynômes sont à coefficients dans k^0, et dépendent du choix de l'uniformisante t.

Énonçons d'autre part une règle (facilement déduite de la formule (5) précédente) qui concerne les expressions des coefficients du quotient de deux éléments de $\mathfrak{R}$. Soient $x=(x^{(0)}, \ldots, x^{(\mu)}, \ldots), y=(y^{(0)}, \ldots, y^{(\mu)}, \ldots)$ deux éléments de $\mathfrak{R}$ tels qu'on ait $v(x)\geqslant v(y)=\sigma$, c'est-à-dire $x^{(0)}=y^{(0)}=\ldots\ldots=x^{(\sigma-1)}=y^{(\sigma-1)}=0$ et $y^{(\sigma)}\neq 0$. Alors le quotient $z=x/y$ est entier (i.e. appartient à $\mathfrak{R}$), et ses coefficients $z^{(\mu)}$ sont donnés par des formules de la forme

$$\mathrm{F}_\sigma^0(z^{(\mu)})=(y^{(\sigma)})^{-(\mu+1)}\mathrm{Q}'_\mu(x^{(\sigma)}, y^{(\sigma)}, \ldots, x^{(\sigma+\mu)}, y^{(\sigma+\mu)}) \tag{8}$$

où Q'_μ est un polynôme à coefficients dans k^0, et où F_σ^0 désigne l'automorphisme de k^0 défini comme suit : dans le cas *a)*, F_σ^0 est l'identité; dans le cas *b)*, F_σ^0 est la puissance $q^*(\sigma)$-ième de l'automorphisme de Frobenius F^0, où $q^*(\sigma)$ est le plus petit entier $\geqslant\sigma/e$. De plus, $x^{(\sigma+\mu)}$ et $y^{(\sigma+\mu)}$ interviennent linéairement dans le polynôme Q'_μ.

On aura besoin également d'une formule analogue à la formule de Taylor, pour les fractions rationnelles à coefficients dans $\mathfrak{k}$.

Soit $x^0=(x_1^0, \ldots, x_n^0)$ un point de l'espace affine $\mathbf{S}_n^0=(\mathfrak{k}^0)^n$, et soit $f=f(\mathrm{X})$ un élément de l'anneau local $\mathfrak{o}=\mathfrak{o}(x^0, \mathbf{S}_n)$, c'est-à-dire une fraction rationnelle représentable sous la forme P/Q, où P et Q appartiennent à $\mathfrak{R}[\mathrm{X}]=\mathfrak{R}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ avec $\mathrm{Q}^0(x^0)\neq 0$. Dans le cas *a)*, l'idéal maximal $\mathfrak{m}=\mathfrak{m}(x^0, \mathbf{S}_n)$ de l'anneau $\mathfrak{o}$ admet pour générateurs $\mathrm{X}_1-x_1^0, \ldots, \mathrm{X}_n-x_n^0$ et t; le symbole de dérivation $\dfrac{\partial f}{\partial t}$ a un sens, et on a la formule

$$f(\mathrm{X})-f^0(x^0)\equiv\Sigma_{i=1}^n\left(\left(\frac{\partial f}{\partial \mathrm{X}_i}\right)^0(x^0)\right)(\mathrm{X}_i-x_i^0)+\left(\frac{\partial f}{\partial t}\right)^0(x^0)t \pmod{\mathfrak{m}^2} \tag{9}$$

Dans le cas *b)*, l'idéal $\mathfrak{m}$ admet pour générateurs $\mathrm{X}_1-\eta(x_1^0), \ldots, \mathrm{X}_n-\eta(x_n^0)$ et t; nous allons montrer qu'on a, dans ce cas, la formule

$$f(\mathrm{X})-\eta(f^0(x^0))\equiv\Sigma_{i=1}^n\left(\eta\left(\left(\frac{\partial f}{\partial \mathrm{X}_i}\right)^0(x^0)\right)(\mathrm{X}_i-\eta(x_i^0))\right)+\eta(h^0(x^0))^{1/p}t \pmod{\mathfrak{m}^2} \tag{10}$$

où h est la fraction rationnelle (qui appartient nécessairement à $\mathfrak{o}$) définie par $h(\mathrm{X})=\dfrac{1}{t}(\bar{f}(\mathrm{X}^p)-(f(\mathrm{X}))^p)$.

Vérifions d'abord cette formule dans le cas où la fonction f est une constante a. La fonction h est alors la constante $b=\frac{1}{t}(\overline{a}-a^p)$. On a de plus $\mathfrak{m}=\mathfrak{p}=(t)$, et

$$a\equiv\eta(a^{(0)})+\eta(a^{(1)})^{\varepsilon}t \pmod{\mathfrak{p}^2}$$

avec $\varepsilon=1$ ou $\frac{1}{p}$ suivant que k est ramifié ou non relativement à v. D'où, par élévation à la puissance p, $a^p\equiv\eta(a^{(0)})^p \pmod{\mathfrak{p}^2}$ et on en déduit aussitôt

$$\frac{1}{t}(a-\eta(a^0))\equiv b^{1/p} \pmod{\mathfrak{p}^2}$$

d'où, puisque $\eta(b^0)\equiv b \pmod{\mathfrak{p}}$, la relation à démontrer

$$a-\eta(a^0)\equiv(\eta(b^0))^{1/p}t \pmod{\mathfrak{p}^2} \tag{11}$$

Supposons maintenant f quelconque, et remarquons que le premier membre de (10) s'écrit :

$$f(\mathrm{X})-\eta(f^0(x^0))\equiv f(\mathrm{X})-f(\eta(x^0))+f(\eta(x^0))-\eta(f^0(x^0))$$

On a :

$$f(\mathrm{X})-f(\eta(x^0))\equiv\Sigma_i\frac{\partial f}{\partial \mathrm{X}_i}(\eta(x^0))(\mathrm{X}_i-\eta(x_i^0))\equiv\Sigma_i\eta\left(\left(\frac{\partial f}{\partial \mathrm{X}_i}\right)^0(x^0)\right)(\mathrm{X}_i-\eta(x^0)) \pmod{\mathfrak{m}^2}$$

D'autre part, en appliquant la formule (11), avec $a=f(\eta(x^0))$ et en remarquant qu'on a

$$\rho(f(\eta(x^0)))=f(\eta(x^0))^0=f^0(x^0),$$

on obtient

$$\begin{aligned}\frac{1}{t}(f(\eta(x^0))-\eta(f^0(x^0)))&\equiv h(\eta(x^0))^{1/p}\\&\equiv(\eta(h^0(x^0)))^{1/p}\end{aligned} \pmod{\mathfrak{m}}$$

La formule (10) est donc bien vérifiée. Nous poserons dans la suite $h^0(x^0)=\left(\frac{\partial f}{\partial t}\right)^0_*(x^0)$. La formule (10) prend ainsi la forme

$$f(\mathrm{X})-\eta(f^0(x^0))\equiv\Sigma_i\left(\eta\left(\frac{\partial f}{\partial \mathrm{X}_i}\right)^0(x^0)\right)(\mathrm{X}_i-\eta(x_i^0))+\eta\left(\left(\frac{\partial f}{\partial t}\right)^0_*(x^0)\right)t \pmod{\mathfrak{m}^2} \tag{12}$$

En utilisant cette formule, ou bien en se servant de l'expression de h, on vérifie que le symbole $\left(\frac{\partial}{\partial t}\right)^0_*$ possède les propriétés suivantes :

$$\left(\frac{\partial(fg)}{\partial t}\right)^0_*=f^0\left(\frac{\partial g}{\partial t}\right)^0_*+g^0\left(\frac{\partial f}{\partial t}\right)^0_* \tag{13}$$

$$\begin{cases}\left(\frac{\partial(f+g)}{\partial t}\right)^0_*=\left(\frac{\partial f}{\partial t}\right)^0_*+\left(\frac{\partial g}{\partial t}\right)^0_* & \text{si } k \text{ est ramifié}\\ \left(\frac{\partial(f+g)}{\partial t}\right)^0_*=\left(\frac{\partial f}{\partial t}\right)^0_*+\left(\frac{\partial g}{\partial t}\right)^0_*+(\mathrm{P}_1^+(f^0,g^0))^{1/p} & \text{si } k \text{ est non ramifié}\end{cases} \tag{14}$$

Pour unifier complètement les notations des cas *a)* et *b)*, on étendra la signification de la notation η en convenant que η est l'identité dans le cas *a)*, et celle de la notation $\left(\frac{\partial f}{\partial t}\right)^0_*$ en posant dans le cas *a)*, $\left(\frac{\partial f}{\partial t}\right)^0_*(x^0) = \left(\frac{\partial f}{\partial t}\right)^0(x^0)$. La formule (12) ci-dessus est alors valable dans les deux cas.

7. $\mathfrak{p}$-différentielle d'une fonction en un point.

Soit V une $\mathfrak{p}$-variété de dimension r, et soit x^0 un point de $\rho_e(V)$.

Pour toute fonction f sur V, appartenant à $\mathfrak{o} = \mathfrak{o}(x^0, V)$ (i.e. $\mathfrak{p}$-morphique en x^0), la fonction $f - \eta(f^0(x^0))$ appartient à l'idéal maximal $\mathfrak{m} = \mathfrak{m}(x^0, V)$ de $\mathfrak{o}$. Sa classe (mod. $\mathfrak{m}^2$) est un élément de l'espace tangent de Zariski $Z = Z(x^0, V)$, que nous appellerons $\mathfrak{p}$-*différentielle de* f *en* x^0, et que nous noterons $(df)^0_{x^0}$.

Si, en particulier, on prend pour V l'espace affine $\mathbf{S}_n = \Omega^n$, l'espace Z est engendré par les $\mathfrak{p}$-différentielles $(dX_i)^0_{x^0}$ des fonctions coordonnées, et par $(dt)^0_{x^0}$. On a alors, pour toute fonction $f \in \mathfrak{o}(x^0, \mathbf{S}_n)$, la formule

$$(15) \qquad (df)^0_{x^0} = \Sigma_i \left(\left(\frac{\partial f}{\partial X_i} \right)^0 (x^0) \right) (dX_i)^0_{x^0} + \left(\left(\frac{\partial f}{\partial t} \right)^0_* (x^0) \right) (dt)^0_{x^0}$$

qu'on déduit de la formule (12) du numéro précédent.

Soit maintenant V une variété affine quelconque (contenue dans $\mathbf{S}_n$), définie sur $\mathfrak{k}$; soit x^0 un point de $\rho_e(V)$, et soit f un élément de $\mathfrak{O} = \mathfrak{o}(x^0, \mathbf{S}_n)$. Alors la fonction induite $f|V$ est définie, et appartient à $\mathfrak{o}(x^0, V)$. Plus précisément, on a un homomorphisme surjectif $\alpha : \mathfrak{O} = \mathfrak{o}(x^0, \mathbf{S}_n) \to \mathfrak{o} = \mathfrak{o}(x^0, V)$, défini par $\alpha(f) = f|V$. Cet homomorphisme applique $\mathfrak{M} = \mathfrak{m}(x^0, \mathbf{S}_n)$ sur $\mathfrak{m} = \mathfrak{m}(x^0, V)$, et on en déduit, par passage au quotient, un $\mathfrak{k}^0$-homomorphisme d'espaces vectoriels $\psi^0 : Z(x^0, \mathbf{S}_n) \to Z(x^0, V)$, tel qu'on ait

$$(16) \qquad \psi^0((df)^0_{x^0}) = (d(f|V))^0_{x^0}$$

pour toute $f \in \mathfrak{O}$. De la formule (15), on déduit :

$$(17) \qquad d(f|V)^0_{x^0} = \Sigma_i \left(\left(\frac{\partial f}{\partial X_i} \right)^0 (x^0) \right) d(X_i|V)^0_{x^0} + \left(\left(\frac{\partial f}{\partial t} \right)^0_* (x^0) \right) d(t|V)^0_{x^0}$$

8. Points entiers et points rationnels $\mathfrak{p}$-adiques.

Pour toute variété (resp. pour toute variété affine) V, définie sur $\mathfrak{k}$, les points de V à coordonnées dans $\mathfrak{k}$ (resp. $\mathfrak{R}$) sont appelés les *points rationnels* (resp. *entiers*) $\mathfrak{p}$-*adiques* de V. L'ensemble de ces points est noté $V_{\mathfrak{k}}$ (resp. $V_{\mathfrak{R}}$). Pour tout sous-corps k_1 de $\mathfrak{k}$ (resp. pour tout sous-anneau R_1 de $\mathfrak{R}$), on emploiera de même la notation V_{k_1} (resp. V_{R_1}) pour désigner l'ensemble des points de V à coordonnées dans k_1 (resp. R_1).

Soient V et W deux variétés affines, définies sur $\mathfrak{k}$, et soit $\varphi : V \to W$ une application rationnelle, définie sur $\mathfrak{k}$; si φ est $\mathfrak{p}$-morphique en un point $x^0 \in \rho_e(V)$, et

si x est un point de $V_{\mathfrak{R}}$ tel que $x^0=\rho(x)$, on a $y=\varphi(x)\in W_{\mathfrak{R}}$, et $y^0=\rho(y)=\varphi^0(x^0)$.

Donc si $V=\{V_\alpha, T_{\beta\alpha}\}$ est une $\mathfrak{p}$-variété, et si, pour un point $x\in V_{\mathfrak{k}}$, il existe α tel que x soit représenté dans V_α par un point $x_\alpha\in(V_\alpha)_{\mathfrak{R}}$, on a aussi $x_\beta\in(V_\beta)_{\mathfrak{R}}$, pour tout β tel que x soit représenté dans V_β. On dit alors que x est un *point entier* $\mathfrak{p}$-*adique de* V. L'ensemble de ces points est encore noté $V_{\mathfrak{R}}$. Si k_1 est un corps de définition de V, contenu dans $\mathfrak{k}$, et si $R_1=\mathfrak{R}\cap k_1$ est l'anneau des entiers de k_1, la relation $x_\alpha\in(V_\alpha)_{R_1}$ entraîne de même $x_\beta\in(V_\beta)_{R_1}$ pour tout β tel que x soit représenté dans V_β. L'ensemble des x vérifiant cette condition est noté V_{R_1}.

Lorsque V est $\mathfrak{p}$-complète (et, en particulier, lorsque V est projective), on a $V_{\mathfrak{R}}=V_{\mathfrak{k}}$, et $V_{R_1}=V_{k_1}$, i.e. les notions de point entier et de point rationnel $\mathfrak{p}$-adique coïncident.

9. Métrique $\mathfrak{p}$-adique de $V_{\mathfrak{R}}$.

Soient $x=(x_1, \ldots, x_n)$ et $y=(y_1, \ldots, y_n)$ deux points quelconques de $(\mathbf{S}_n)_{\mathfrak{R}}=\mathfrak{R}^n$; on pose $(x,y)_{\mathfrak{p}}=\inf_i v(x_i-y_i)$, et $d_{\mathfrak{p}}(x,y)=\exp(-(x,y)_{\mathfrak{p}})$. Alors $d_{\mathfrak{p}}(x,y)$ définit une métrique sur $\mathfrak{R}^n$, dite *métrique* $\mathfrak{p}$-*adique de* $\mathfrak{R}^n$.

Soient V et W deux variétés affines, définies sur $\mathfrak{k}$, et soit $\varphi: V\to W$ une application rationnelle, définie sur $\mathfrak{k}$. Soient x et y deux points de $V_{\mathfrak{R}}$ tels que φ soit $\mathfrak{p}$-morphique en $x^0=\rho(x)$ et en $y^0=\rho(y)$. En vertu de la définition d'une application $\mathfrak{p}$-morphique, et d'après la formule de Taylor, on a $(\varphi(x), \varphi(y))_{\mathfrak{p}}\geqslant(x,y)_{\mathfrak{p}}$. Si φ est birationnelle, et $\mathfrak{p}$-isomorphique en chacun des points x^0 et y^0, on a $(\varphi(x), \varphi(y))_{\mathfrak{p}}=(x,y)_{\mathfrak{p}}$.

Donc, si $V=\{V_\alpha, T_{\beta\alpha}\}$ est une $\mathfrak{p}$-variété, et si (x,y) est un couple de points de V représentés dans une même V_α, l'entier $(x_\alpha,y_\alpha)_{\mathfrak{p}}$ ne dépend pas de α. On peut encore désigner cet entier par $(x,y)_{\mathfrak{p}}$, et poser à nouveau $d_{\mathfrak{p}}(x,y)=\exp(-(x,y)_{\mathfrak{p}})$. Si, en outre, on convient de poser $(x,y)_{\mathfrak{p}}=0$, et $d_{\mathfrak{p}}(x,y)=1$ lorsqu'il n'existe aucun α tel que x et y soient tous les deux représentés dans V_α, on voit que le symbole $d_{\mathfrak{p}}$ définit encore une métrique, dite *métrique* $\mathfrak{p}$-*adique de* $V_{\mathfrak{R}}$. Cette métrique est invariante par tout $\mathfrak{R}$-isomorphisme.

Nous introduirons d'autre part la notation suivante; soit x un point de $(\mathbf{S}_n)_{\mathfrak{R}}=\mathfrak{R}^n$, et soit E un sous-ensemble $\mathfrak{k}$-fermé quelconque de $\mathbf{S}_n$; notons $\mathfrak{I}(E)$ l'idéal de $\mathfrak{R}[X]=\mathfrak{R}[X_1, \ldots, X_n]$ composé des polynômes qui s'annulent sur E; nous poserons $(x, E)_{\mathfrak{p}}=\inf_{P\in\mathfrak{I}(E)} v(P(x))$. Il est clair que cette notation généralise la notation $(x,y)_{\mathfrak{p}}$ du cas affine introduite plus haut. Si $\{F_\alpha\}$ $(1\leqslant\alpha\leqslant q)$ est un système de générateurs de $\mathfrak{I}(E)$, on a $(x, E)_{\mathfrak{p}}=\inf_\alpha v(F_\alpha(x))$. La relation $(x, E)_{\mathfrak{p}}=\infty$ équivaut à $x\in E$.

10. $\mathfrak{p}$-simplicité.

Soit V une $\mathfrak{p}$-variété de dimension r, et soit x^0 un point de $\rho_e(V)$. On dira que V est $\mathfrak{p}$-*simple en* x^0, ou que x^0 *est* $\mathfrak{p}$-*simple sur* V, si l'anneau local $\mathfrak{o}=\mathfrak{o}(x^0, V)$ est régulier. Puisque la dimension de cet anneau local est $r+1$, il revient au même de dire que l'idéal $\mathfrak{m}=\mathfrak{m}(x^0, V)$ admet un système de $r+1$ générateurs, ou que l'espace tangent de Zariski $Z=Z(x^0, V)$ est de dimension $r+1$.

Soit k_1 un corps de définition de V, contenu dans $\mathfrak{k}$, et posons $k_1^0 = \rho(k_1)$. Si X^0 est une k_1^0-variété contenue dans $\rho_e(V) = \operatorname{supp} V^0$, on dira que X^0 est *génériquement* $\mathfrak{p}$-*simple sur* V si l'anneau local $\mathfrak{o}(X^0, V)$ est régulier. Puisque la dimension de cet anneau local est $r+1-q$ (en posant $q = \dim X^0$), il revient au même de dire que l'idéal $\mathfrak{m} = \mathfrak{m}(X^0, V)$ admet $r+1-q$ générateurs, ou que l'espace tangent de Zariski $Z(X^0, V)$ est de dimension $r+1-q$. Si x^0 est un point générique de X^0 sur k_1^0, il faut et il suffit, pour que X^0 soit génériquement p-simple sur V, que x^0 soit p-simple sur V.

Cas particulier. — Supposons que k soit un corps de fonctions algébriques d'une variable sur un corps de base k_0 algébriquement clos, c'est-à-dire un corps de la forme $k_0(u)$, où u est un point générique sur k_0 d'une courbe U, définie sur k_0 (qu'on peut supposer sans point multiple, et plongée dans un espace affine $\mathbf{S}_m$) et que v est une valuation non triviale de k s'annulant sur k_0. A cette valuation, il correspond une place de k, donc un point u^0 de U, et on a $k^0 = k_0(u^0)$. Supposons V affine, plongée dans $\mathbf{S}_n$. Soit x un point générique de V sur $k = k_0(u)$, et soit $\widetilde{V}$ la sous-variété de dimension $r+1$ de $\mathbf{S}_{n+m} = \mathbf{S}_n \times \mathbf{S}_m$, lieu de $V \times u$ sur k_0 (i.e. le lieu de (x, u) sur k_0). On a $V = \mathrm{pr}_1(\widetilde{V} \,.\, (\mathbf{S}_n \times u))$, et $V^0 = \mathrm{pr}_1(\widetilde{V} \,.\, (\mathbf{S}_n \times u^0))$. Autrement dit, on peut regarder la variété $\widetilde{V}$ comme « fibrée » par une famille de sous-variétés de dimension r de $\mathbf{S}_n$ (certaines de ces « fibres » pouvant être dégénérées), de telle façon que V et V^0 soient les fibres ayant respectivement comme paramètres u et u^0. Pour $x^0 \in \rho_e(V)$, l'anneau local $\mathfrak{o}(x^0, V)$ est alors isomorphe à l'anneau local de $\widetilde{V}$ au point (x^0, u^0). Donc, dans ce cas, *pour que le point* x^0 *soit* $\mathfrak{p}$-*simple sur* V, *il faut et il suffit que* (x^0, u^0) *soit simple sur* $\widetilde{V}$.

Proposition 4 (critère jacobien de $\mathfrak{p}$-*simplicité).* — *Soit* V *une variété affine* $(V \subset \mathbf{S}_n)$, *de dimension* r, *définie sur* $\mathfrak{k}$. *Soit* $\{F_\alpha\}$ $(1 \leqslant \alpha \leqslant q)$ *un système de générateurs de l'idéal* $\mathfrak{I}(V)$ *de* $\mathfrak{R}[X] = \mathfrak{R}[X_1, \ldots, X_n]$ *composé des polynômes qui s'annulent sur* V. *Soit* x^0 *un point de* $\rho_e(V)$. *Alors la matrice*

$$M = \begin{pmatrix} \left(\frac{\partial F_1}{\partial X_1}\right)^0(x^0) & \cdots & \left(\frac{\partial F_1}{\partial X_n}\right)^0(x^0) & \left(\frac{\partial F_1}{\partial t}\right)^0_*(x^0) \\ \cdots\cdots & \cdots & \cdots\cdots & \cdots\cdots \\ \left(\frac{\partial F_q}{\partial X_1}\right)^0(x^0) & \cdots & \left(\frac{\partial F_q}{\partial X_n}\right)^0(x^0) & \left(\frac{\partial F_q}{\partial t}\right)^0_*(x^0) \end{pmatrix}$$

est de rang $\geqslant n-r$. *Pour que* x^0 *soit* $\mathfrak{p}$-*simple sur* V, *il faut et il suffit qu'elle soit exactement de rang* $n-r$.

Démonstration. — Posons en effet

$$\mathfrak{O} = \mathfrak{o}(x^0, \mathbf{S}_n), \quad \mathfrak{M} = \mathfrak{m}(x^0, \mathbf{S}_n), \quad \mathfrak{o} = \mathfrak{o}(x^0, V), \quad \mathfrak{m} = \mathfrak{m}(x^0, V).$$

Considérons l'homomorphisme canonique $\psi^0 : Z(x^0, \mathbf{S}_n) \to Z(x^0, V)$ introduit au n° 7. Montrons que le noyau N de ψ^0 coïncide avec l'ensemble des p-différentielles $(dh)^0_{x^0}$, où h parcourt l'idéal $\mathfrak{i}(V, x^0, \mathbf{S}_n) = \mathfrak{I}(V) \cap \mathfrak{O}$ de l'anneau $\mathfrak{O}$.

En effet, si $h \in \mathfrak{i}(V, x^0, \mathbf{S}_n)$, on a $h|V = 0$, donc, d'après la formule (16) du n° 7, $\psi^0((dh)^0_{x^0}) = 0$.

Inversement, tout élément de N est de la forme $(df)^0_{x^0}$, avec $f \in \mathfrak{M}$ et $f|V \in \mathfrak{m}^2$. Puisque l'homomorphisme canonique $\alpha : \mathfrak{O} \to \mathfrak{o}$ applique $\mathfrak{M}$ sur $\mathfrak{m}$ (donc $\mathfrak{M}^2$ sur $\mathfrak{m}^2$), il existe $g \in \mathfrak{M}^2$ telle que $\alpha(f-g) = 0$, autrement dit, telle que $(f-g)|V = 0$, ou encore que $h = f-g \in \mathfrak{i}(V, x^0, \mathbf{S}_n)$. Puisqu'on a $(dg)^0_{x^0} = 0$, on a aussi $(df)^0_{x^0} = (dh)^0_{x^0}$, et notre assertion est démontrée.

Donc N est le $\mathfrak{k}^0$-espace vectoriel engendré par les $(dF_\alpha)^0_{x^0}$. Or, on a, d'après la formule (17) du n° 7, pour tout α,

$$(dF_\alpha)^0_{x^0} = \Sigma_i \left(\left(\frac{\partial F_\alpha}{\partial X_i} \right)^0 (x^0) \right) (dX_i)^0_{x^0} + \left(\left(\frac{\partial F_\alpha}{\partial t} \right)^0_* (x^0) \right) (dt)^0_{x^0}$$

Puisqu'on a $\dim Z(x^0, V) \geqslant r+1$, et $\dim Z(x^0, \mathbf{S}_n) = n+1$, on a $\dim N \geqslant n-r$, donc la matrice M est de rang $\geqslant n-r$. Pour que x^0 soit p-simple sur V, il faut et il suffit qu'on ait $\dim Z(x^0, V) = r+1$, c'est-à-dire $\dim N = n-r$, donc que la matrice M soit de rang $n-r$. C.Q.F.D.

Si X est un cycle positif sur une variété quelconque, et x un point du support de X, nous dirons que x est *simple sur* X s'il n'appartient qu'à une seule composante X_0 de X, si celle-ci est simple, i.e. a pour coefficient 1 dans X, et si, de plus, x est simple sur X_0. L'ensemble des points de supp X qui sont simples sur X est noté $\mathscr{S}(X)$. Si $\mathbf{k}$ est un corps sur lequel X est rationnel, et si Y est une $\mathbf{k}$-variété contenue dans supp X, nous dirons que Y est *génériquement simple sur* X si un point (donc tout point) générique de Y sur $\mathbf{k}$ est simple sur X.

Nous ne rappellerons pas la démonstration de la proposition suivante, qui est une forme du *lemme de Hensel.*

Proposition 5. — Soit V *une* p*-variété et posons* $V^0 = \rho(V)$. *Alors on a* $\mathscr{S}(V^0) \subset \rho(V_{\mathfrak{R}})$, *et* $\mathscr{S}_{k^0}(V^0) \subset \rho(V_{\hat{\mathfrak{R}}})$.

Autrement dit : tout point x^0 simple sur V^0 peut se relever à un point entier p-adique x sur V, et si x^0 est rationnel sur k^0, on peut prendre x à coordonnées dans $\hat{\mathfrak{R}}$.

Proposition 6. — Soit V *une* p*-variété et soit* x^0 *un point de* $\rho_e(V)$. *Alors les trois propriétés suivantes sont équivalentes :*

(i) x^0 *est simple sur* V^0 (*i.e.* $x^0 \in \mathscr{S}(V^0)$).

(ii) x^0 *est* p*-simple sur* V, *et on a* $t \notin (\mathfrak{m}(x^0, V))^2$.

(iii) x^0 *est* p*-simple sur* V, *et appartient à* $\rho(V_{\mathfrak{R}})$.

Démonstration. — La question étant locale, on peut supposer V affine, contenue dans $\mathbf{S}_n = \Omega^n$. Soit, comme dans la proposition 4, $\{F_\alpha\}$ $(1 \leqslant \alpha \leqslant q)$ un système de générateurs de l'idéal $\mathscr{I}(V)$. On sait (cf. Shimura [R], n° 3, p. 155), que, pour que x^0 soit simple sur V^0, il faut et il suffit que la matrice $\left(\left(\frac{\partial F_\alpha}{\partial X_i} \right)^0 (x^0) \right)$ soit de rang $n-r$; ceci revient à dire que la matrice M de la proposition 4 est de rang $n-r$ (i.e. que x^0 est p-simple sur V) et que $(dt)^0_{x^0}$ n'appartient pas au $\mathfrak{k}^0$-espace vectoriel N engendré par

les $(dF_\alpha)^0_{x^0}$ (i.e. d'après la démonstration de la proposition 4, que $t \notin \mathfrak{m}(x_0, V)^2$). Donc (i) équivaut à (ii).

D'autre part (i) entraîne, d'après la proposition 5 (lemme de Hensel), $x^0 \in \rho(V_{\mathfrak{R}})$; donc (i) entraîne (iii).

Inversement, supposons la condition (iii) satisfaite, et soit $x \in V_{\mathfrak{R}}$ tel que $x^0 = \rho(x)$. Puisque $x \in V$, on a $F_\alpha(x) = 0$ pour tout α. Or d'après la formule (17) du n° 7, on a

$$F_\alpha(X) \equiv \Sigma_i \left(\eta\left(\left(\frac{\partial F_\alpha}{\partial X_i} \right)^0 (x^0) \right) (X_i - \eta(x_i^0)) \right) + \eta\left(\left(\frac{\partial F_\alpha}{\partial t} \right)^0_* (x^0) \right) t \qquad (\text{mod. } \mathfrak{M}^2)$$

où l'on pose $\mathfrak{M} = \mathfrak{m}(x^0, \mathbf{S}_n)$. En substituant x à X, on obtient

$$\Sigma_i \left(\eta\left(\left(\frac{\partial F_\alpha}{\partial X_i} \right)^0 (x^0) \right) (x_i - \eta(x_i^0)) \right) + \eta\left(\left(\frac{\partial F_\alpha}{\partial t} \right)^0_* (x^0) \right) t \equiv 0 \qquad (\text{mod. } t^2)$$

Comme on a, pour tout i, $x_i - \eta(x_i^0) \equiv 0 \pmod{t}$, on en déduit, en simplifiant par t la formule précédente, puis en réduisant mod. $\mathfrak{p}$ (i.e. mod. t), que $\left(\frac{\partial F_\alpha}{\partial t} \right)^0_* (x^0)$ s'exprime par une combinaison linéaire des $\left(\frac{\partial F_\alpha}{\partial X_i} \right)^0 (x^0)$, à coefficients dans k^0, ne dépendant pas de α. Donc on a $(dt)^0_{x^0} \in N$, et la condition (ii) est satisfaite.

C.Q.F.D.

Remarque. — Dans le cas particulier considéré au début de ce numéro, la condition $t \notin \mathfrak{m}(x^0, V)^2$ signifie que la variété linéaire tangente à $\widetilde{V}$ au point (x^0, u^0) n'est pas contenue dans $\mathbf{S}_n \times u^0$.

On dira dans la suite qu'un point $x \in V_{\mathfrak{R}}$ est *simple* (*mod.* $\mathfrak{p}$) *sur* V si le point $x^0 = \rho(x)$ est $\mathfrak{p}$-simple sur V, ou ce qui est équivalent, d'après la proposition 6, si x^0 est simple sur V^0. Une $\mathfrak{p}$-variété V sans point multiple, telle que tous les points de $V_{\mathfrak{R}}$ soient simples (mod. $\mathfrak{p}$) sur V, i.e. telle qu'on ait $\rho(V_{\mathfrak{R}}) = \mathscr{S}(V^0)$, sera dite *faiblement* $\mathfrak{p}$-*simple*. Il en est ainsi en particulier lorsque tous les points de $\rho_e(V)$ sont $\mathfrak{p}$-simples; on dira alors que V est $\mathfrak{p}$-*simple*.

11. $\mathfrak{p}$-normalité.

Soient V et W deux $\mathfrak{p}$-variétés, et soit $\varphi : V \to W$ une application rationnelle, définie sur $\mathfrak{k}$. Soit x^0 un point de l'ensemble réduit $\rho_e(V)$. On dira que φ est $\mathfrak{p}$-*finie en* x^0, si l'ensemble $\varphi^0_e(x^0)$ des valeurs de φ en x^0 est fini (rappelons que cet ensemble n'est jamais vide si W est complète et, en particulier, si φ est une fonction, auquel cas W est la droite projective).

On dira qu'une $\mathfrak{p}$-variété V est $\mathfrak{p}$-*normale en un point* $x^0 \in \rho_e(V)$, ou encore que le point x^0 est $\mathfrak{p}$-*normal sur* V, si l'anneau local $\mathfrak{o}(x^0, V)$ est intégralement clos. En particulier, tout point $\mathfrak{p}$-simple sur V est aussi $\mathfrak{p}$-normal sur V ([16], chap. II, n° 5, *c)*). On dira que V est $\mathfrak{p}$-*normale* si elle est $\mathfrak{p}$-normale en tout point de $\rho_e(V)$. Soit k_1 un corps de définition de V, contenu dans $\mathfrak{k}$, et posons $k_1^0 = \rho(k_1)$; si X^0 est une k_1^0-variété, contenue dans $\rho_e(V)$,

on dira que X^0 est génériquement p-normale sur V si l'anneau local $\mathfrak{o}(X^0, V)$ est intégralement clos, ou, ce qui revient au même, si tout point générique de X^0 sur k_1^0 est p-normal sur V.

Énonçons maintenant quelques-unes des propriétés, par ailleurs bien connues, de cette notion de p-normalité.

Proposition 7 (théorème de connexion de Zariski). — *Soient* V *et* W *deux* p*-variétés et soit* $\varphi : V \to W$ *une application rationnelle définie sur* $\mathfrak{k}$. *Soit* x^0 *un point de* supp V^0 *qui est* p*-normal sur* V. *Alors*

(i) *L'ensemble* $\varphi_e^0(x^0)$ *est connexe.*

(ii) *En particulier, si l'une des composantes de* $\varphi_e^0(x^0)$ *est un point* y^0, *on a nécessairement* $\varphi_e^0(x^0) = \{y^0\}$. *Dans ce cas,* φ *est* p*-morphique en* x^0, *et on a* $y^0 = \varphi^0(x^0)$.

Comme conséquence immédiate de l'assertion (ii), si φ est p-finie en un point $x^0 \in \rho_e(V)$ p-normal sur V, φ est p-morphique en x^0.

Proposition 8. — *Soit* V *une* p*-variété* p*-normale, et posons* $V^0 = \rho(V)$. *Alors, pour qu'une composante* C^0 *de* V^0 *soit génériquement* p*-simple sur* V, *il faut et il suffit qu'elle soit génériquement* p*-normale sur* V. *Toute fonction f sur* V, *définie sur* $\mathfrak{k}$, *est génériquement* p*-morphique sur une telle composante.*

La première partie de l'énoncé est l'analogue de la proposition exprimant la simplicité de toute sous-variété de codimension 1 d'une variété normale.

La seconde partie résulte de la proposition 7. En effet, en un point générique x^0 de C^0, l'ensemble $f_e^0(x^0)$ est de dimension 0 (sinon l'ensemble algébrique réduit $\rho_e(\Gamma_f)$ du graphe de f aurait une composante de dimension $r+1$, ce qui est absurde, puisque $\dim \Gamma_f = r$). Donc f est p-finie et, par suite, p-morphique en x^0.

Proposition 9. — *Soient* V *et* W *deux* p*-variétés, et soit* $\varphi : V \to W$ *une application birationnelle, définie sur* $\mathfrak{k}$. *Soient* x^0 *un point de* $\rho_e(V)$, p*-simple sur* V, *et* y^0 *un point de* $\rho_e(W)$, p*-simple sur* W, *tels que* φ *soit* p*-morphique en* x^0, *et que* $y^0 = \varphi^0(x^0)$. *Alors pour que* φ *soit* p*-isomorphique en* x^0, *il faut et il suffit que l'homomorphisme canonique* $\varphi_{x^0}^0 : Z(x^0, W) \to Z(x^0, V)$ *soit surjectif.*

Démonstration. — Il suffit de montrer que si $\varphi_{x^0}^0$ est surjectif, φ est p-isomorphique en x^0. Pour cela, supposons que φ ne soit pas p-isomorphique en x^0. D'après la proposition 7, et puisque le point y^0 est p-simple, donc p-normal sur W, l'une des composantes X^0, contenant x^0, de l'ensemble $(\varphi^{-1})_e^0(y^0)$ n'est pas réduite à un point, i.e. est de dimension $q > 0$. Posons $r = \dim V$. Soit k_1 un corps de définition pour V, W et φ, tel que $k_1^0 = \rho(k_1)$ soit un corps de définition pour X^0, x^0 et y^0. Soit $\bar{x}^0$ un point générique de X^0 sur k_1^0. Puisque l'application φ est p-morphique en x^0, elle l'est *a fortiori* en $\bar{x}^0$, et on a $y^0 = \varphi^0(\bar{x}^0)$. Puisque x^0 est p-simple sur V, il en est de même de $\bar{x}^0$, et puisque l'homomorphisme $\varphi_{x^0}^0$ est surjectif, il en est de même *a fortiori* de l'homomorphisme $\varphi_{\bar{x}^0}^0 : Z(y^0, W) \to Z(\bar{x}^0, V)$. Or l'image de $\mathfrak{m}(y^0, W)$ par l'application canonique $\mathfrak{m}(y^0, W) \to \mathfrak{m}(\bar{x}^0, V)$ est composée de fonctions s'annulant sur X^0, i.e. est contenue dans l'idéal

$$\mathfrak{m}' = \mathfrak{i}(X^0, \bar{x}^0, V) = \mathfrak{m}(X^0, V) \cap \mathfrak{O}(\bar{x}^0, V).$$

Cet idéal $\mathfrak{m}'$ s'envoie par l'homomorphisme canonique $\mathfrak{m}(\bar{x}^0, V) \to Z(\bar{x}^0, V)$ sur un sous-espace Z' de $Z = Z(\bar{x}^0, V)$; puisque $\bar{x}^0$ est simple sur X^0, Z' est de dimension $r-q+1$. D'autre part, l'image de $\varphi^0_{\bar{x}^0}$ est contenue dans Z'. Puisque $\varphi^0_{\bar{x}^0}$ est surjectif, on a donc $Z' = Z$. Puisque $\dim Z = r+1$, ceci implique $q = 0$, d'où contradiction.

12. p-diviseur d'une fonction.

Soit V une variété (relativement au domaine universel Ω). Si f est une fonction sur V, de graphe Γ_f, et si c est une constante (élément de Ω_∞), on note, comme dans ([F], chap. VIII), $(f)_c$ le diviseur sur V défini par $(f)_c = \mathrm{pr}_1(\Gamma_f . (V \times c))$. En particulier $(f)_0$ et $(f)_\infty$ sont appelés respectivement *diviseur des zéros*, et *diviseur des pôles* de f. Le *diviseur* (f) *de* f est défini par $(f) = (f)_0 - (f)_\infty$. On sait que, pour toute sous-variété C de codimension 1 de V, simple sur V, l'anneau local de C sur V est un anneau de valuation discrète, et que le coefficient $\nu(C, f)$ de C dans (f) est égal à la valeur en f de la valuation correspondante (normée de manière que l'ensemble de ses valeurs soit $\mathbf{Z}$). Le diviseur (f) est donc aussi donné par la formule $(f) = \Sigma_C \nu(C, f) C$ où la somme est étendue à toutes les sous-variétés de codimension 1 de V, simples sur V.

Supposons maintenant que V est une $\mathfrak{p}$-variété, et soit f une fonction sur V, définie sur $\mathfrak{k}$, de graphe Γ_f. Soit C^0 une composante de $V^0 = \rho(V)$, génériquement $\mathfrak{p}$-simple sur V. L'anneau local $\mathfrak{o}(C^0, V)$ étant de dimension 1, et régulier, son idéal maximal $\mathfrak{m}(C^0, V)$ est principal. Donc $\mathfrak{o}(C^0, V)$ est un anneau de valuation discrète du corps des fonctions sur V, définies sur $\mathfrak{k}$. Nous désignerons la valeur en f de la valuation correspondante (normée de manière que l'ensemble de ses valeurs soit $\mathbf{Z}$), par $\nu(C^0, f)$. Supposons en particulier que C^0 est une composante simple (i.e. de coefficient 1) de V^0. Alors, on a $t \notin (\mathfrak{m}(C^0, V))^2$, d'après la proposition 6. Donc l'idéal $\mathfrak{m}(C^0, V)$ n'est autre que l'idéal principal (t). Dans ce cas, $\nu = \nu(C^0, f)$ est l'unique entier tel que la fonction $ft^{-\nu}$ soit un élément inversible de $\mathfrak{o}(C^0, V)$, autrement dit tel que la fonction $ft^{-\nu}$ soit génériquement $\mathfrak{p}$-morphique et non nulle sur C^0.

On appelle $\mathfrak{p}$-*diviseur de* f, et on désigne par $(f)_\mathfrak{p}$, le cycle de dimension $r = \dim V$ défini par $(f)_\mathfrak{p} = \Sigma_{C^0} \nu(C^0, f) C^0$, où la somme est étendue à toutes les composantes de V^0 qui sont génériquement $\mathfrak{p}$-simples sur V. Posant $\nu_+(C^0, f) = \sup(0, \nu(C^0, f))$, et $\nu_-(C^0, f) = \sup(0, -\nu(C^0, f))$, on appelle $\mathfrak{p}$-*diviseur des zéros*, et $\mathfrak{p}$-*diviseur des pôles* de f, les cycles positifs $(f)_{\mathfrak{p},0}$ et $(f)_{\mathfrak{p},\infty}$ respectivement définis par $(f)_{\mathfrak{p},0} = \Sigma_{C^0} \nu_+(C^0, f) C^0$ et $(f)_{\mathfrak{p},\infty} = \Sigma_{C^0} \nu_-(C^0, f) C^0$. On a ainsi $(f)_\mathfrak{p} = (f)_{\mathfrak{p},0} - (f)_{\mathfrak{p},\infty}$. Les composantes de $(f)_{\mathfrak{p},0}$ (resp. $(f)_{\mathfrak{p},\infty}$) sont aussi celles sur lesquelles f induit la constante 0 (resp. ∞).

Dans le cas particulier considéré au n° 10, on peut caractériser comme suit le $\mathfrak{p}$-diviseur $(f)_\mathfrak{p}$ de f : désignons par $\widetilde{f}$ la fonction sur $\widetilde{V}$, définie sur k_0, et obtenue par extension de f à $\widetilde{V}$, c'est-à-dire telle que $\widetilde{f}(x, u) = f(x)$, pour x générique de V sur $k = k_0(u)$; alors $(f)_\mathfrak{p} \times u^0$ est la contribution des composantes de $V^0 \times u^0 = \widetilde{V} . (\mathbf{S}_n \times u^0)$ dans le diviseur $(\widetilde{f})$ de $\widetilde{f}$.

Proposition 10. — *Soit* V *une* $\mathfrak{p}$*-variété et soit* f *une fonction sur* V, *définie sur* $\mathfrak{k}$. *Soit* x^0 *un point de* supp V^0 *tel que toutes les composantes* C_j^0 *de* V^0 *contenant* x^0 *soient génériquement* $\mathfrak{p}$*-simples sur* V. *Soit* c *un élément de* $\mathfrak{k}_\infty$, *et posons* $c^0=\rho(c)$. *Alors, pour que* c^0 *appartienne à l'ensemble* $f_e^0(x^0)$ *des valeurs de* f *en* x^0, *il faut et il suffit que l'une des deux propriétés suivantes soit satisfaite : on a* $x^0\in\rho_e(\mathrm{supp}(f)_c)$, *ou bien* f *induit la constante* c^0 *sur l'une au moins des* C_j^0.

Démonstration. — La question étant locale, on peut supposer V affine, contenue dans $\mathbf{S}_n$. Posons $r=\dim V$. Notons Γ_f le graphe de f; la propriété $c^0\in f_e^0(x^0)$ équivaut à $(x^0, c^0)\in\rho_e(\Gamma_f)$.

Montrons d'abord que la condition est suffisante. On a, en effet, $\mathrm{supp}(f)_c\times c\in\Gamma_f$, donc $x^0\in\rho_e(\mathrm{supp}(f)_c)$ entraîne bien $(x^0, c^0)\in\rho_e(\Gamma_f)$. D'autre part, si f induit c^0 sur C_j^0, on a $C_j^0\times c^0\subset\rho_e(\Gamma_f)$, donc on a bien encore $(x^0, c^0)\in\rho_e(\Gamma_f)$.

Montrons maintenant que la condition est nécessaire. Notons que, d'après la proposition 8, f est génériquement $\mathfrak{p}$-morphique sur chacune des C_j^0. Donc, si f n'induit la constante c^0 sur aucune des C_j^0, on a, pour tout j, $C_j^0\times c^0\not\subset\rho_e(\Gamma_f)$. Donc les composantes de l'intersection $(\rho_e(V)\times c^0)\cap\rho_e(\Gamma_f)$, c'est-à-dire de l'intersection $(\mathbf{S}_n^0\times c^0)\cap\rho_e(\Gamma_f)$, qui contiennent (x^0, c^0), sont de dimension $\leqslant r-1$; elles sont en fait exactement de dimension $r-1$ (d'après [F], VI, 1, th. 1, cor. 2), et ce sont des composantes propres de $(\mathbf{S}_n^0\times c^0)\cap\rho_e(\Gamma_f)$ dans le produit $\mathbf{S}_n^0\times\mathbf{P}_1^0$. D'après ([R], n° 3, th. 11) on a alors $(x^0, c^0)\in\rho_e((\mathbf{S}_n\times c)\cap\Gamma_f)$, autrement dit $(x^0, c^0)\in\rho_e((V\times c)\cap\Gamma_f)$. De plus, si $Z\times c$ est une $\mathfrak{k}$-composante de $(V\times c)\cap\Gamma_f$, telle que $(x^0, c^0)\in\rho_e(Z)$, Z est simple sur V (puisque x_0 est $\mathfrak{p}$-simple sur V). Donc on a $x^0\in\rho_e(\mathrm{supp}(f)_c)$. C.Q.F.D.

Il sera commode de poser, pour toute fonction f sur V, définie sur $\mathfrak{k}$

$$\{f\}_{\mathfrak{p},0}=(\mathrm{supp}(f)_{\mathfrak{p},0})\cup(\rho_e(\mathrm{supp}(f)_0)$$
$$\{f\}_{\mathfrak{p},\infty}=(\mathrm{supp}(f)_{\mathfrak{p},\infty})\cup(\rho_e(\mathrm{supp}(f)_\infty)$$

et
$$\{f\}_{\mathfrak{p}}=\{f\}_{\mathfrak{p},0}\cup\{f\}_{\mathfrak{p},\infty}=(\mathrm{supp}(f)_{\mathfrak{p}})\cup\rho_e(\mathrm{supp}(f)).$$

Corollaire (critère pour qu'une fonction soit $\mathfrak{p}$*-morphique en un point).* — *Soit* V *une* $\mathfrak{p}$*-variété; soit* x^0 *un point de* $\rho_e(V)$, $\mathfrak{p}$*-normal sur* V. *Soit* f *une fonction sur* V, *définie sur* $\mathfrak{k}$. *Alors, pour que* f *soit* $\mathfrak{p}$*-morphique* (resp. $\mathfrak{p}$*-morphique et non nulle*, resp. *définie*) *en* x^0, *il faut et il suffit qu'on ait* $x^0\notin\{f\}_{\mathfrak{p},\infty}$ (*resp.* $x^0\notin\{f\}_{\mathfrak{p}}$, *resp.* $x^0\notin\{f\}_{\mathfrak{p},0}\cap\{f\}_{\mathfrak{p},\infty}$).

Il suffit de vérifier le critère pour que f soit $\mathfrak{p}$-morphique. Les deux autres s'en déduisent en effet en remplaçant f par $1/f$. Puisque x^0 est $\mathfrak{p}$-normal sur V, toutes les composantes de $\rho_e(V)$ contenant x^0 sont génériquement $\mathfrak{p}$-normales, donc (n° 11, prop. 8) génériquement $\mathfrak{p}$-simples sur V; il faut et il suffit, pour que f soit $\mathfrak{p}$-morphique en x^0, que ∞ n'appartienne pas à l'ensemble $f_e^0(x^0)$ des valeurs de f en x^0, ou encore, d'après la proposition 10, qu'on ait $x^0\notin\rho_e(\mathrm{supp}(f)_\infty)$, et que f n'induise pas la constante ∞ sur l'une des composantes de V^0 qui contiennent x^0, autrement dit que $x^0\notin\mathrm{supp}(f)_{\mathfrak{p},\infty}$.

13. Différentielles sur V. Étude en un point $\mathfrak{p}$-simple.

Soit V une $\mathfrak{p}$-variété, et notons $\mathfrak{k}(V)$ le corps des fonctions sur V, définies sur $\mathfrak{k}$. Pour tout entier $q>0$, l'ensemble des différentielles de degré q du corps $\mathfrak{k}(V)$ (qu'on

appellera aussi $\mathfrak{k}$-différentielles de degré q sur V), est un espace vectoriel sur $\mathfrak{k}(V)$, que nous désignerons par $D^q(V)$. Si W est une sous-$\mathfrak{p}$-variété simple de V, les éléments de $D^q(V)$ qui sont *génériquement morphiques sur* W forment un module sur l'anneau local $\mathfrak{o}(W, V)$, que nous désignerons par $D^q(W, V)$. Nous désignerons par $D^q(W, V)_0$ le sous-module de $D^q(W, V)$ composé des différentielles qui s'annulent sur W, i.e. défini par $D^q(W, V)_0 = \mathfrak{m}(W, V).D^q(W, V)$. En particulier, si x est un point de $V_{\mathfrak{k}}$, le $\mathfrak{o}(x, V)$-module $D^q(x, V)$ (resp. $D^q(x, V)_0$) se compose des $\mathfrak{k}$-différentielles de degré q qui sont *morphiques en x* (resp. qui s'annulent en x). Pour toute différentielle $\omega \in D^q(W, V)$, on peut parler de la *différentielle induite* par ω sur W, qu'on note $\omega | W$. Pour $f \in \mathfrak{o}(W, V)$, on a $df \in D^1(W, V)$, et $df | W = d(f | W)$. Si ω s'annule sur W, on a $\omega | W = 0$, mais la réciproque n'est pas exacte (par exemple $\omega | W$ est toujours nulle si W est un point). Si k_1 est un sous-corps de $\mathfrak{k}$ sur lequel V est définie, on notera de même $k_1(V)$ le corps des fonctions sur V, définies sur k_1, et $D^q_{k_1}(V)$ l'espace vectoriel sur $k_1(V)$ des k_1-différentielles sur V. Si W est une sous-$\mathfrak{p}$-variété simple de V, définie sur k_1, les éléments de $D^q(W, V)$ (resp. $D^q(W, V)_0$) qui sont définis sur k_1 forment un module sur $\mathfrak{o}_{k_1}(W, V)$, qu'on note $D^q_{k_1}(W, V)$ (resp. $D^q_{k_1}(W, V)_0$).

Nous allons définir des notions analogues, mais faisant intervenir, au lieu d'un point ou d'une sous-variété de V, un point ou une sous-variété de l'ensemble réduit $\rho_e(V)$.

Commençons par considérer une différentielle $\omega \in D^q(\mathbf{S}_n)$ sur l'espace affine $\mathbf{S}_n$; elle s'écrit sous la forme

$$\omega = \Sigma_{(i)} g_{(i)} dX_{i_1} \wedge \ldots \wedge dX_{i_q}$$

où (i) parcourt l'ensemble des multi-indices $(i) = (i_1, \ldots, i_q)$ tels qu'on ait

$$1 \leqslant i_1 < \ldots < i_q \leqslant n,$$

et où les $g_{(i)}$ sont des fonctions sur $\mathbf{S}_n$, définies sur $\mathfrak{k}$.

Soit x^0 un point de l'espace affine réduit $\mathbf{S}^0_n$. Soit X^0 une sous-variété de $\mathbf{S}^0_n$. On dira que ω est $\mathfrak{p}$-*morphique* en x^0 (resp. *génériquement* $\mathfrak{p}$-*morphique sur* X^0) si chacune des $g_{(i)}$ est $\mathfrak{p}$-morphique en x^0 (resp. génériquement $\mathfrak{p}$-morphique sur X^0). On dira que ω *s'annule* en x^0 (resp. sur X^0) si les $g_{(i)}$ s'annulent en x^0 (resp. sur X^0). Soit k_1 un sous-corps de $\mathfrak{k}$ sur lequel V et ω sont définies, et tel que X^0 soit définie sur $k_1^0 = \rho(k_1)$; pour que ω soit génériquement $\mathfrak{p}$-morphique (resp. s'annule) sur X^0, il faut et il suffit que ω soit $\mathfrak{p}$-morphique (resp. s'annule) en un point générique $\bar{x}^0$ de X^0 sur k_1^0. L'ensemble des différentielles $\omega \in D^q(\mathbf{S}_n)$ qui sont $\mathfrak{p}$-morphiques en x^0 (resp. génériquement $\mathfrak{p}$-morphiques sur X^0) est un module sur l'anneau local $\mathfrak{o}(x^0, \mathbf{S}_n)$ (resp. $\mathfrak{o}(X^0, \mathbf{S}_n)$), que nous noterons $D^q(x^0, \mathbf{S}_n)$ (resp. $D^q(X^0, \mathbf{S}_n)$). L'ensemble de celles qui s'annulent en x^0 (resp. sur X^0) en est un sous-module, que nous noterons $D^q(x^0, \mathbf{S}_n)_0$ (resp. $D^q(X^0, \mathbf{S}_n)_0$).

Soit k_1 un sous-corps de $\mathfrak{k}$ sur lequel V est définie, et posons $k_1^0 = \rho(k)$. Si X^0 est une sous-k_1^0-variété de $\mathbf{S}^0_n$, on définit de même les sous-modules $D^q_{k_1}(X^0, \mathbf{S}_n)$ et $D^q_{k_1}(X^0, \mathbf{S}_n)_0$ du module $D^q_{k_1}(\mathbf{S}_n)$ des différentielles d'ordre q définies sur k_1.

Soit maintenant V une variété affine dans $\mathbf{S}_n$, de dimension r, définie sur $\mathfrak{k}$, et soit x^0 un point de $\rho_e(V)$, $\mathfrak{p}$-simple sur V. Notons $\mathfrak{i}(V) = \mathfrak{i}(V, x^0, \mathbf{S}_n)$ l'idéal $\mathfrak{m}(V, \mathbf{S}_n) \cap \mathfrak{o}(x^0, \mathbf{S}_n)$

de l'anneau $\mathfrak{o} = \mathfrak{o}(x^0, \mathbf{S}_n)$ (composé des fonctions sur $\mathbf{S}_n$, p-morphiques en x^0, et qui s'annulent sur V). Cet idéal $\mathfrak{i}(V)$ est contenu dans $\mathfrak{m}(x^0, \mathbf{S}_n)$. Désignons par $f_1, \ldots, f_{n-r}$ un système d'éléments de $\mathfrak{i}(V)$ tels que les p-différentielles $(df_i)_{x^0}$ soient linéairement indépendantes (i.e. un système minimal de générateurs), et posons $\theta_0 = df_1 \wedge \ldots \wedge df_{n-r}$.

Montrons que, pour tout entier $q \geqslant 0$, et pour $\omega \in D^q(V, \mathbf{S}_n)$, les relations $\omega | V = 0$, et $\omega \wedge \theta_0 \in D^{n+q-r}(V, \mathbf{S}_n)_0$ sont équivalentes. On remarque en effet qu'on peut trouver des fonctions $u_1, \ldots, u_r$ sur $\mathbf{S}_n$ telles que $(df_1, \ldots, df_{n-r}, du_1, \ldots, du_r)$ soit une base du module $D^1(x^0, \mathbf{S}_n)$ (puisque ce dernier est de dimension n). La différentielle ω est alors de la forme

$$\omega = \Sigma_{(i),(j)} g_{(i),(j)} df_{i_1} \wedge \ldots \wedge df_{i_h} \wedge du_{j_1} \wedge \ldots \wedge du_{j_l},$$

où $((i), (j))$ parcourt tous les couples de multi-indices de la forme $(i) = (i_1, \ldots, i_h)$ et $(j) = (j_1, \ldots, j_l)$, tels que $h + l = q$, et avec $g_{(i),(j)} \in \mathfrak{o}(V, \mathbf{S}_n)$. Or, on a $df_i | V = 0$ pour tout i. Donc, pour que $\omega | V = 0$, il faut et il suffit que les coefficients des produits extérieurs de la forme $du_{j_1} \wedge \ldots \wedge du_{j_q}$ dans l'expression de ω, s'annulent sur V, ou encore, qu'on ait $g_{(i),(j)} | V = 0$ pour tout couple $((i), (j))$ tel que $h = 0$ et $l = q$. Compte tenu des expressions de ω et θ_0, cette condition est bien équivalente à $\omega \wedge \theta_0 \in D^{n+q-r}(V, \mathbf{S}_n)_0$.

Nous dirons qu'une $\mathfrak{k}$-différentielle ω, de degré q, sur V, est p-*morphique en* x^0 s'il existe une différentielle $\theta \in D^{n+q-r}(x^0, \mathbf{S}_n)$ (différentielle sur $\mathbf{S}_n$, p-morphique en x^0) et une différentielle $\bar{\omega} \in D^q(V, \mathbf{S}_n)$ (différentielle sur $\mathbf{S}_n$, génériquement p-morphique sur V), telle que $\bar{\omega} | V = \omega$, vérifiant la condition

$$\theta \equiv \bar{\omega} \wedge \theta_0 \ (\text{mod. } D^{n+q-r}(V, \mathbf{S}_n)_0) \tag{18}$$

Cette condition est indépendante du choix de θ_0, c'est-à-dire du système $(f_1, \ldots, f_{n-r})$. En effet, soit $(f'_1, \ldots, f'_{n-r})$ un autre système analogue. Alors, si $\theta'_0 = df'_1 \wedge \ldots \wedge df'_{n-r}$, on a $\theta'_0 = b\theta_0$, où b est un élément inversible de $\mathfrak{o}(x^0, \mathbf{S}_n)$; il suffit de remarquer que, pour que θ et $\bar{\omega}$ vérifient la relation (18), il faut et il suffit que $\theta' = b\theta$ et $\bar{\omega}$ vérifient la relation $\theta' \equiv \bar{\omega} \wedge \theta'_0$ (mod. $D^{n+q-r}(V, \mathbf{S}_n)_0$).

D'autre part, en vertu de ce qui précède, si la relation (18) est vérifiée par θ et $\bar{\omega}$, elle l'est aussi par θ et $\bar{\omega}'$, pour toute différentielle $\bar{\omega}' \in D^r(V, \mathbf{S}_n)$ telle que $\bar{\omega}' | V = \omega$.

L'ensemble des différentielles d'ordre q sur V qui sont p-morphiques en x^0 est un module sur l'anneau local $\mathfrak{o}(x^0, V)$. On le notera $D^q(x^0, V)$. On dira que $\omega \in D^q(x^0, V)$ *s'annule* en x^0 si la différentielle θ intervenant dans la définition précédente s'annule en x^0 (cette propriété ne dépend pas, comme on le voit immédiatement, du choix de θ_0, θ et $\bar{\omega}$). Les éléments de $D^q(x^0, V)$ qui s'annulent en x^0 forment un sous-module de $D^q(x^0, V)$, qu'on note $D^q(x^0, V)_0$. Si X^0 est une variété contenue dans $\rho_e(V)$, génériquement p-simple sur V, on définit de même les modules $D^q(X^0, V)$ et $D^q(X^0, V)_0$ sur l'anneau local $\mathfrak{o}(X^0, V)$, respectivement composés des différentielles *génériquement* p-*morphiques sur* X^0, et de celles qui *s'annulent sur* X^0; on remplace, pour cela, les f_i par un système minimal de générateurs de l'idéal $\mathfrak{i}(V, X^0, \mathbf{S}_n) = \mathfrak{m}(V, \mathbf{S}_n) \cap \mathfrak{o}(X^0, \mathbf{S}_n)$ de l'anneau $\mathfrak{o}(X^0, \mathbf{S}_n)$, et la condition

$$\theta \in D^{n+q-r}(x^0, \mathbf{S}_n)$$

par $\theta \in D^{n+q-r}(X^0, \mathbf{S}_n)$; soit k_1 un sous-corps de $\mathfrak{k}$ sur lequel V et ω sont définies, et tel que X^0 soit définie sur $k_1^0 = \rho(k_1)$; pour que ω soit génériquement p-morphique (resp. s'annule) sur X^0, il faut et il suffit qu'elle soit p-morphique (resp. qu'elle s'annule) en un point générique x^0 de X^0 sur k_1^0.

Soit $k_1 \subset \mathfrak{k}$ un corps de définition de V, et posons $k_1^0 = \rho(k_1)$; si X^0 est une sous-k_1^0-variété de V^0, on définit de même les symboles $D^q_{k_1}(X^0, V)$ et $D^q_{k_1}(X^0, V)_0$.

Cas particulier. — Supposons que le point x^0 soit *simple sur* V^0. Soit C^0 la composante de $V^0 = \rho(V)$ contenant x^0. On peut trouver des fonctions $v_1, \ldots, v_r$ sur V définies sur $\mathfrak{k}$, p-morphiques en x^0, et telles que les fonctions induites $v_i | C^0$ forment un système de générateurs de l'idéal $\mathfrak{m}(x^0, C^0)$ de l'anneau local $\mathfrak{o}(x^0, C^0)$ ou, ce qui revient au même, telles que les p-différentielles $(dv_i)^0_{x^0}$ $(1 \leqslant i \leqslant r)$ soient indépendantes. De telles fonctions $v_1, \ldots, v_r$ sont appelées *paramètres uniformisants* de V en x^0. Les fonctions $v_1, \ldots, v_r$ sont algébriquement indépendantes, et on peut donc écrire ω sous la forme $\omega = \Sigma_{(i)} h_{(i)} dv_{i_1} \wedge \ldots \wedge dv_{i_q}$, où (i) parcourt l'ensemble des multi-indices $(i) = (i_1, \ldots, i_q)$ tels que $1 \leqslant i_1 < \ldots < i_q \leqslant n$, et où les $h_{(i)}$ sont des fonctions sur V définies sur $\mathfrak{k}$. Pour que ω soit p-morphique en x^0, il est alors nécessaire et suffisant que les $h_{(i)}$ soient p-morphiques en x^0. En effet, soient $\overline{v}_1, \ldots, \overline{v}_r$ des éléments de $\mathfrak{o}(x^0, \mathbf{S}_n)$ tels que $v_i = \overline{v}_i | V$ $(1 \leqslant i \leqslant r)$, et considérons à nouveau la différentielle $\theta_0 = df_1 \wedge \ldots \wedge df_{n-r}$ introduite plus haut. D'après le choix des f_j, les fonctions $\overline{v}_1, \ldots, \overline{v}_r, f_1, \ldots, f_{n-r}, t$ forment une base de l'idéal maximal $\mathfrak{m}(x^0, \mathbf{S}_n)$ de $\mathfrak{o}(x^0, \mathbf{S}_n)$; donc la différentielle $d\overline{v}_1 \wedge \ldots \wedge d\overline{v}_r \wedge df_1 \wedge \ldots \wedge df_{n-r}$ sur $\mathbf{S}_n$ est p-morphique et non nulle en x^0.

Si les $h_{(i)}$ sont p-morphiques en x^0, on peut, pour tout (i), trouver une fonction $\overline{h}_{(i)} \in \mathfrak{o}(x^0, \mathbf{S}_n)$, telle que $\overline{h}_{(i)} | V = h_{(i)}$. Posant alors $\overline{\omega} = \Sigma_{(i)} \overline{h}_{(i)} d\overline{v}_{i_1} \wedge \ldots \wedge d\overline{v}_{i_q}$, on a $\overline{\omega} | V = \omega$, et la différentielle $\theta = \overline{\omega} \wedge \theta_0$ est p-morphique en x^0; en vertu de la définition précédente, ω est également p-morphique en x^0.

Inversement, supposons que ω est p-morphique en x^0. Soient $\overline{\omega} \in D^q(V, \mathbf{S}_n)$ telle que $\overline{\omega} | V = \omega$, et $\theta \in D^{n+q-r}(x^0, \mathbf{S}_n)$, vérifiant la relation (18). On peut écrire θ sous la forme

$$\theta = \Sigma_{(i),(j)} \overline{h}^*_{(i),(j)} d\overline{v}_{i_1} \wedge \ldots \wedge dv_{i_h} \wedge df_{j_1} \wedge \ldots \wedge df_{j_l}$$

où $((i), (j))$ parcourt tous les couples de multi-indices $((i) = (i_1, \ldots, i_h), (j) = (j_1, \ldots, j_l))$ tels qu'on ait $1 \leqslant i_1 < \ldots < i_h \leqslant r$, $1 \leqslant j_1 < \ldots < j_l \leqslant n-r$, et $h + l = n + q - r$, et où les $\overline{h}^*_{(i),(j)}$ appartiennent à $\mathfrak{o}(x^0, \mathbf{S}_n)$. D'après la relation (18), tous les coefficients des termes du second membre qui ne contiennent pas en facteur $\theta_0 = df_1 \wedge \ldots \wedge df_{n-r}$ s'annulent sur V et, de plus, si $\overline{\omega} = \Sigma_{(i)} \overline{h}_{(i)} d\overline{v}_{i_1} \wedge \ldots \wedge d\overline{v}_{i_q}$, on a nécessairement, pour tout (i), $\overline{h}_{(i)} \equiv \overline{h}'_{(i)}$ (mod. $\mathfrak{m}(V, \mathbf{S}_n)$), en posant $\overline{h}'_{(i)} = \overline{h}^*_{(i),(1,\ldots,n-r)}$. On a donc $h_{(i)} = \overline{h}'_{(i)} | V$, pour tout (i), donc les $h_{(i)}$ sont bien p-morphiques en x^0.

De même, pour que ω s'annule en x^0, il faut et il suffit que chacune des $h_{(i)}$ s'annule en x^0.

Soit k_1 un corps de définition de V et de ω, contenu dans $\mathfrak{k}$, et posons $k_1^0 = \rho(k_1)$; soit X^0 une k_1^0-variété contenue dans $\rho_e(V)$, et *génériquement simple sur* $V^0 = \rho(V)$. On peut, comme plus haut, introduire un système de paramètres uniformisants $v_1, \ldots, v_r$

de V en x^0, et exprimer ω sous la forme $\omega = \Sigma_{(i)} h_{(i)} dv_1 \wedge \ldots \wedge dv_r$, où les h_i sont définies sur k_1. On trouve encore que ω est génériquement p-morphique (resp. s'annule) sur X^0, si et si seulement $h_{(i)}$ est génériquement p-morphique (resp. s'annule) sur X^0 pour tout (i). On définit alors la *différentielle induite* $\omega | X^0$ par ω sur X^0 en posant

$$\omega | X^0 = \Sigma_{(i)} (h_{(i)} | X^0) d(v_1 | X^0) \wedge \ldots \wedge d(v_q | X^0).$$

Si ω s'annule sur X^0, on a $\omega | X^0 = 0$, mais la réciproque n'est pas exacte (en particulier, $\omega | X^0$ est toujours nulle si X^0 est un point).

14. Symbole $(\omega \wedge \mathbf{dt})^0_{x^0}$.

Pour tout point $x^0 \in \mathbf{S}^0_n$, et pour toute différentielle $\theta \in D^q(x^0, \mathbf{S}_n)$, de la forme $\theta = \Sigma_{(i)} h_{(i)} dX_{i_1} \wedge \ldots \wedge dX_{i_q}$, on désignera par $\theta^0_{x^0}$ l'élément

$$\theta^0_{x^0} = \Sigma_{(i)} h^0_{(i)}(x^0) (dX_{i_1})_{x^0} \wedge \ldots \wedge (dX_{i_q})_{x^0}$$

de la puissance extérieure $\wedge^r Z(x^0, \mathbf{S}_n)$ de l'espace tangent de Zariski $Z(x^0, \mathbf{S}_n)$; pour que θ s'annule en x^0, il faut et il suffit qu'on ait $\theta^0_{x^0} = 0$.

Revenons au cas où x^0 est un point p-simple quelconque sur une sous-variété V de $\mathbf{S}_n$. Soit ω une différentielle sur V, de *degré maximum* $(q = r = \dim V)$, p-morphique en x^0. Soit encore $(f_1, \ldots, f_{n-r})$ une base de l'idéal $\mathfrak{i}(V, x^0, \mathbf{S}_n)$ de l'anneau local $\mathfrak{o}(x^0, \mathbf{S}_n)$, et posons, comme plus haut, $\theta_0 = df_1 \wedge \ldots \wedge df_{n-r}$. Soit $\overline{\omega}$ un élément de $D^r(V, \mathbf{S}_n)$ tel que $\overline{\omega} | V = \omega$. Il existe alors, par définition d'une différentielle p-morphique en un point, un élément θ de $D^n(x^0, \mathbf{S}_n)$, tel que la relation (18) soit satisfaite. D'après le choix des f_j, on a $(\theta_0)^0_{x^0} \neq 0$. Puisque l'espace tangent de Zariski $Z(x^0, \mathbf{S}_n)$ est de dimension $n+1$, on peut trouver un élément $\overline{\omega}^0_0$ de $\wedge^{r+1} Z(x^0, \mathbf{S}_n)$ tel que $\theta^0_{x^0} \wedge (dt)^0_{x^0} = \overline{\omega}^0_0 \wedge (\theta_0)^0_{x^0}$.

Soit ω^0_0 l'élément de $\wedge^{r+1} Z(x^0, V)$ image de $\overline{\omega}^0_0$ par la puissance extérieure $\wedge^{r+1} \psi^0$ de l'homomorphisme canonique $\psi^0 : Z(x^0, \mathbf{S}_n) \to Z(x^0, V)$.

Montrons que cet élément ω^0_0 ne dépend que de V, ω et x^0, mais non du choix de θ^0, θ, et $\overline{\omega}^0_0$.

En effet, on voit d'abord que, pour θ_0 fixé, ω^0_0 ne dépend pas du choix du couple $(\theta, \overline{\omega}^0_0)$; si ω'_0 correspond à un autre couple $(\theta', \overline{\omega}'^0_0)$ vérifiant les mêmes conditions, on a :

$$(\theta - \theta')^0_{x^0} \wedge (dt)^0_{x^0} = (\overline{\omega}^0_0 - \overline{\omega}'^0_0) \wedge (\theta_0)^0_{x^0}$$

et comme $\theta - \theta' \in D^n(V, \mathbf{S}_n)_0 \cap D^n(x^0, \mathbf{S}_n) \subset D^n(x^0, \mathbf{S}_n)_0$, le premier membre de cette relation est nul; donc $\overline{\omega}^0_0 - \overline{\omega}'^0_0$ est une combinaison de termes de la forme $(df_j)^0_{x^0} \wedge \omega^0_j$, où les ω^0_j sont des éléments de $\wedge^r Z(x^0, S_n)$; donc on a bien $\omega^0_0 = \omega'^0_0$. D'autre part, ω^0_0 ne dépend pas du choix de θ_0 : en effet, pour V et x^0 donnés, θ_0 est, comme on a vu, déterminée au produit près par un élément inversible de $\mathfrak{o}(x^0, \mathbf{S}_n)$; or, si b est un tel élément, toutes les conditions de la définition précédente restent satisfaites lorsqu'on remplace θ_0 par $\theta'_0 = b\theta_0$, et θ' par $\theta' = b\theta$, sans modifier $\overline{\omega}^0_0$.

Nous désignerons l'élément ω^0_0 de $\wedge^{r+1}(x^0, V)$ ainsi défini par la notation $(\omega \wedge dt)^0_{x^0}$. L'écriture $\omega \wedge dt$ est purement symbolique : le signe $\wedge$ ne représente pas

un produit extérieur, pas plus que dt ne représente la différentielle de t (non définie dans le cas d'inégales caractéristiques). On peut la justifier en remarquant qu'on a $(\omega\wedge dt)^0_{x^0}=(\omega^0_{x^0}\wedge dt)^0_{x^0}$ lorsque ω est un élément de $\mathrm{D}^n(x^0, \mathbf{S}_n)$ et que, d'autre part, dans le cas particulier considéré au n° 10, $(\omega\wedge dt)^0_{x^0}$ s'identifie à l'élément de la puissance $(r+1)$-ième de l'espace tangent de Zariski à la variété $\widetilde{\mathrm{V}}$ au point (x^0, u^0) induit en ce point par $\widetilde{\omega}\wedge dt$, où $\widetilde{\omega}$ est la différentielle sur $\widetilde{\mathrm{V}}$ transposée de ω.

On a un homomorphisme canonique :

$\delta : \mathrm{D}^r(x^0, \mathrm{V})\to\wedge^{r+1}\mathrm{Z}(x^0, \mathrm{V})$, pour la structure de $\mathfrak{o}(x^0, \mathrm{V})$-module, défini par $\delta(\omega)=(\omega\wedge dt)^0_{x^0}$. Le noyau de cet homomorphisme est $\mathrm{D}^r(x^0, \mathrm{V})_0$.

15. Transposée d'une différentielle par une application $\mathfrak{p}$-morphique.

Proposition 11. — *Soient* V *et* V^* *deux variétés affines, définies sur* k, *de même dimension* r, *et soit* $\varphi : \mathrm{V}^*\to\mathrm{V}$ *une application rationnelle, définie sur* $\mathfrak{k}$, *génériquement surjective. Soit* ω *une* $\mathfrak{k}$*-différentielle de degré* q *sur* V, *et soit* ω^* *sa transposée sur* V^*. *Soient* x^{*0} *un point de* $\mathfrak{p}_e(\mathrm{V}^*)$, $\mathfrak{p}$*-simple sur* V^*, *et* x^0 *un point de* $\mathfrak{p}_e(\mathrm{V})$, $\mathfrak{p}$*-simple sur* V, *tels que* φ *soit* $\mathfrak{p}$*-morphique en* x^{*0}, *de valeur* x^0. *Alors, si* ω *est* $\mathfrak{p}$*-morphique* (resp. *s'annule*) *en* x^0, ω^* *est* $\mathfrak{p}$*-morphique* (resp. *s'annule*) *en* x^{*0}. *De plus, si* $q=r$, $(\omega^*\wedge dt)^0_{x^{*0}}$ *coïncide avec l'image de* $(\omega\wedge dt)^0_{x^0}$ *par la puissance extérieure* $\wedge^{r+1}\varphi^0_{x^{*0}}$ *de l'homomorphisme canonique* $\varphi^0_{x^{*0}} : \mathrm{Z}(x^0, \mathrm{V})\to\mathrm{Z}(x^{*0}, \mathrm{V}^*)$.

Démonstration. — Par passage au graphe, on peut se borner à considérer le cas où l'on a $\mathrm{V}^*\subset\mathbf{S}_m$, $\mathrm{V}\subset\mathbf{S}_n$ $(m>n)$, et où φ est induite par la projection $\pi : \mathbf{S}_m\to\mathbf{S}_n$ qui, au point $(x_1, \ldots, x_m)$, fait correspondre $(x_1, \ldots, x_n)$; il suffit de vérifier la proposition dans ce cas, et de montrer de plus que si, dans ce cas, φ est $\mathfrak{p}$-isomorphique en x^{*0}, la différentielle ω^* est $\mathfrak{p}$-morphique en x^{*0} si et si seulement ω l'est en x^0.

Soit, comme au n° 13, $(f_1, \ldots, f_{n-r})$ un système d'éléments de l'idéal $\mathfrak{i}(\mathrm{V}, x^0, \mathbf{S}_n)$ de l'anneau local $\mathfrak{o}(x^0, \mathbf{S}_n)$, tels que les $(df_i)_{x^0}$ soient linéairement indépendantes. Notons $f_1^*, \ldots, f_{n-r}^*$ les fonctions sur $\mathbf{S}_m$ transposées des f_j. Ce sont là des éléments de $\mathfrak{i}^*=\mathfrak{i}(\mathrm{V}^*, x^{*0}, \mathbf{S}_m)$, tels que les $\mathfrak{p}$-différentielles $(df_i^*)_{x^{*0}}$ soient linéairement indépendantes; on peut trouver des éléments $g_1, \ldots, g_{m-n}$ de $\mathfrak{i}^*$ tels que les $\mathfrak{p}$-différentielles en x^{*0} de $f_1^*, \ldots, f_{n-r}^*, g_1, \ldots, g_{m-n}$ soient linéairement indépendantes. Posons $\theta_0=df_1\wedge\ldots\wedge df_{n-r}$, $\theta_0^*=df_0^*\wedge\ldots\wedge df_{n-r}^*$, et $\widetilde{\theta}_0^*=\theta_0^*\wedge dg_1\wedge\ldots\wedge dg_{m-n}$.

Soit $\overline{\omega}$ un élément de $\mathrm{D}^q(\mathrm{V}, \mathbf{S}_n)$ tel que $\overline{\omega}\,|\,\mathrm{V}=\omega$. Le transposé $\overline{\omega}^*$ de cet élément appartient à $\mathrm{D}^q(\mathrm{V}^*, \mathbf{S}_n)$, et on a $\overline{\omega}^*\,|\,\mathrm{V}^*=\omega^*$. Si ω est $\mathfrak{p}$-morphique en x^0, il existe $\theta\in\mathrm{D}^{n+q-r}(x^0, \mathbf{S}_n)$ telle qu'on ait $\theta\equiv\overline{\omega}\wedge\theta^0$ (mod. $\mathrm{D}^{n+q-r}(\mathrm{V}, \mathbf{S}_n)_0$). Donc, en posant $\widetilde{\theta}^*=\theta^*\wedge dg_1\wedge\ldots\wedge dg_{m-n}$, on a $\widetilde{\theta}^*\equiv\pm\overline{\omega}^*\wedge\widetilde{\theta}_0^*$ (mod. $\mathrm{D}^{m+q-r}(\mathrm{V}^*, \mathbf{S}_m)_0$). Comme $\widetilde{\theta}^*$ est $\mathfrak{p}$-morphique en x^{*0}, ω^* l'est également. Le même raisonnement montre que, si ω s'annule en x^0, alors ω^{*0} s'annule en x^{*0}.

En conservant les mêmes notations, mais avec $q=r$, posons $\omega_0^0=(\omega\wedge dt)^0_{x^0}$. Par définition de ce symbole, il existe un élément $\overline{\omega}_0^0$ de $\wedge^{r+1}\mathrm{Z}(x^0, \mathbf{S}_n)$ tel qu'on ait :

$$\theta^0_{x^0}\wedge(dt)^0_{x^0}=\overline{\omega}_0^0\wedge(\theta_0)^0_{x^0} \tag{19}$$

et $\omega_0^0 = (\wedge^r \psi^0)(\bar{\omega}_0^0)$, où ψ^0 est l'homomorphisme canonique $Z(x^0, \mathbf{S}_n) \to Z(x^0, V)$. Soit $\pi^0_{x^{*0}}$ l'homomorphisme canonique : $Z(x^0, \mathbf{S}_n) \to Z(x^{*0}, \mathbf{S}_m)$. En appliquant aux deux membres de (19) l'homomorphisme $\wedge^{r+1}\pi^0_{x^{*0}}$, on obtient la relation $(\theta^*)^0_{x^{*0}} \wedge (dt)^0_{x^{*0}} = \bar{\omega}_0^{*0} \wedge (\widetilde{\theta}_0^*)^0_{x^{*0}}$, où l'on pose

$$\bar{\omega}_0^{*0} = (\wedge^{r+1}\pi^0_{x^{*0}})(\bar{\omega}_0^0) \tag{20}$$

On en déduit $(\widetilde{\theta}^*)^0_{x^{*0}} \wedge (dt)^0_{x^{*0}} = \bar{\omega}_0^{*0}(\widetilde{\theta}_0^*)^0_{x^{*0}}$, d'où, en désignant par ψ^{*0} l'homomorphisme canonique $Z(x^{*0}, \mathbf{S}_m) \to Z(x^{*0}, V^*)$,

$$(\omega^* \wedge dt)^0_{x^{*0}} = (\wedge^{r+1}\psi^{*0})(\bar{\omega}_0^{*0}) \tag{21}$$

Comme on a $(\varphi^0_{x^{*0}}) \circ \psi^0 = \psi^{*0} \circ \pi^0_{x^{*0}}$, les relations (20) et (21) entraînent bien $(\wedge^{r+1}\varphi^0_{x^{*0}})(\omega_0^0) = (\omega^* \wedge dt)^0_{x^{*0}}$.

Il reste à vérifier que, q étant de nouveau quelconque, si φ est p-isomorphique en x^{*0}, et si ω^* est p-morphique en x^{*0}, ω est p-morphique en x^0. Soit $(\bar{x}_1, \ldots, \bar{x}_m)$ un point générique de V^* sur $\mathfrak{k}$. Puisque φ^{-1} est p-morphique en x^0, on a des relations de la forme

$$\bar{x}_{n+j} = h_{n+j}(\bar{x}_1, \ldots, \bar{x}_n) \quad (1 \leqslant j \leqslant m-n),$$

où les h_{n+j} sont des fonctions sur V, p-morphiques en x^0. On peut donc, dans ce cas, prendre $g_j = X_{n+j} - h_{n+j}$ $(1 \leqslant j \leqslant m-n)$. Puisque ω^* est p-morphique en x^{*0}, il existe $\widetilde{\theta}_1^* \in D^{m+q-r}(x^{*0}, \mathbf{S}_m)$, telle que

$$\widetilde{\theta}_1^* \equiv \bar{\omega}^* \wedge \widetilde{\theta}_0^* = \bar{\omega}^* \wedge \theta_0^* \wedge dX_{n+1} \wedge \ldots \wedge dX_m \ (\text{mod. } D^{m+q-r}(V^*, \mathbf{S}_m)_0).$$

On peut trouver $\theta_1 \in D^{n+q-r}(x^0, \mathbf{S}_n)$, telle qu'on ait

$$\widetilde{\theta}_1^* \equiv \theta_1^* \wedge dX_{n+1} \wedge \ldots \wedge dX_m \ (\text{mod. } D^{m+q-r}(V^*, \mathbf{S}_m)_0),$$

en notant θ_1^* la transposée de θ_1 sur V^*. On a alors

$$(\theta_1^* - (\bar{\omega}^* \wedge \theta_0^*)) \wedge dX_{n+1} \wedge \ldots \wedge dX_m \equiv 0 \ (\text{mod. } D^{m+q-r}(V^*, \mathbf{S}_m)_0).$$

Ceci implique $\theta_1 - (\bar{\omega} \wedge \theta_0) \equiv 0$ (mod. $D^{n+q-r}(V, \mathbf{S}_n)_0$). Donc ω est bien p-morphique en x^0.

C.Q.F.D.

Proposition 12. — *Soient* V^*, V, φ, x^{*0}, x^0, ω *et* ω^* *comme dans la proposition précédente. Supposons de plus que* φ *est birationnelle, et que* ω *est de degré maximum* $q = r$, p-*morphique et* non nulle *en* x^0. *Alors, pour que* φ *soit* p-*isomorphique en* x^{*0}, *il faut et il suffit que* ω^* *soit* non nulle *en* x^{*0}.

Démonstration. — Le fait que cette condition est nécessaire résulte de la proposition précédente.

Supposons donc que ω et ω^* sont p-morphiques et non nulles en x^0 et x^{*0} respectivement. Avec les notations de la démonstration de la proposition précédente, les différentielles θ et $\widetilde{\theta}^* = \theta^* \wedge dg_1 \wedge \ldots \wedge dg_{m-n}$ sont p-morphiques et non nulles en x^0 et x^{*0} respectivement. Ceci entraîne que la fonction

$$(dX_1 \wedge \ldots \wedge dX_m)/(dX_1 \wedge \ldots \wedge dX_n \wedge dg_1 \wedge \ldots \wedge dg_{m-n})$$

sur $\mathbf{S}_m$ est $\mathfrak{p}$-morphique et non nulle en x^{*0} (i.e. est un élément inversible de l'anneau local $\mathfrak{o}(x^{*0}, \mathbf{S}_m)$. Donc la réunion des $(dX_i)^0_{x^{*0}}$ $(1 \leqslant i \leqslant n)$ et des $(dg_j)^0_{x^{*0}}$ $(1 \leqslant j \leqslant m-n)$ est une base du $\mathfrak{k}^0$-espace vectoriel $Z(x^{*0}, \mathbf{S}_m)$. Donc les $d(X_i|V^*)^0_{x^{*0}}$ $(1 \leqslant i \leqslant n)$ forment une base du $\mathfrak{k}^0$-espace vectoriel $Z(x^{*0}, V^*)$ et, par suite, l'homomorphisme canonique $\varphi^0_{x^0} : Z(x^0, V) \to Z(x^{*0}, V^*)$ est surjectif. D'après la proposition 9 du n° 11, φ est donc $\mathfrak{p}$-isomorphique en x^{*0}. C.Q.F.D.

La proposition 11 permet d'étendre, d'une manière évidente, la signification de la notion de différentielle $\mathfrak{p}$-morphique en un point au cas où V est une $\mathfrak{p}$-variété, ainsi que celle de toutes les notations introduites ($D(x^0, V)$, $D(x^0, V)_0$, $(\omega \wedge dt)^0_{x^0}$, etc.). Les propositions 11 et 12 sont encore valables lorsque V et V^* sont des $\mathfrak{p}$-variétés.

16. $\mathfrak{p}$-diviseur d'une différentielle.

Soit à nouveau V une $\mathfrak{p}$-variété affine de dimension r. Commençons par transformer la condition, donnée comme définition au n° 13, pour qu'une $\mathfrak{k}$-différentielle ω de degré q sur V soit $\mathfrak{p}$-morphique en un point $x^0 \in \rho_e(V)$, $\mathfrak{p}$-simple sur V. Si $u_1, \ldots, u_n$ sont des fonctions sur V, telles que les du_i forment une base de $D^1(V)$, on peut exprimer ω sous la forme $\omega = \Sigma_{(i)} g_{(i)} du_{i_1} \wedge \ldots \wedge du_{i_q}$, où (i) parcourt l'ensemble des multi-indices $(i_1, \ldots, i_q)$ tels que $1 \leqslant i_1 < \ldots < i_q \leqslant r$.

Soit encore $(f_1, \ldots, f_{n-r})$ un système d'éléments de l'idéal $\mathfrak{i}(V, x^0, \mathbf{S}_n)$, tels que les $(df_i)_{x^0}$ soient indépendantes, et posons $\theta_0 = df_1 \wedge \ldots \wedge df_{n-r}$. Soit, pour tout (i), $\overline{g}_{(i)}$ un élément de $\mathfrak{o}(x^0, \mathbf{S}_n)$ tel qu'on ait $\overline{g}_{(i)}|V = g_{(i)}$; soient de même $\overline{u}_1, \ldots, \overline{u}_n$ des éléments de $\mathfrak{o}(V, \mathbf{S}_n)$ tels qu'on ait $\overline{u}_i|V = u_i$ pour tout i. La différentielle ω est induite sur V par $\overline{\omega} = \Sigma_{(i)} \overline{g}_{(i)} d\overline{u}_{i_1} \wedge \ldots \wedge d\overline{u}_{i_q}$.

Pour que ω soit $\mathfrak{p}$-morphique en x^0, il faut et il suffit, par définition, qu'il existe $\theta' \in D^{n+q-r}(x^0, \mathbf{S}_n)$ telle qu'on ait $\theta \equiv \overline{\omega} \wedge \theta_0$ (mod. $D^{n+q-r}(V, \mathbf{S}_n)_0$). On peut écrire $\overline{\omega} \wedge \theta_0$ sous la forme $\overline{\omega} \wedge \theta_0 = \Sigma_{(l)} \overline{h}_{(l)} dX_{l_1} \wedge \ldots \wedge dX_{l_{n+q-r}}$ où (l) parcourt tous les multi-indices $(l) = (l_1, \ldots, l_{n+q-r})$ tels que $1 \leqslant l_1 < \ldots < l_{n+q-r} \leqslant n$, et où, pour tout (l), on pose :

$$\overline{h}_{(l)} = \Sigma_{(i)} \overline{g}_{(i)} D(\overline{u}_{i_1}, \ldots, \overline{u}_{i_q}, f_1, \ldots, f_{n-r}) / D(X_{l_1}, \ldots, X_{l_{n+q-r}})$$

D'autre part, tout élément θ de $D^{n+q-r}(x^0, \mathbf{S}_n)$ est de la forme

$$\theta = \Sigma_{(l)} h'_{(l)} dX_{l_1} \wedge \ldots \wedge dX_{l_{n+q-r}}$$

où les $h'_{(l)}$ appartiennent à $\mathfrak{o}(x^0, \mathbf{S}_n)$. Donc, *pour que* ω *soit* $\mathfrak{p}$*-morphique en* x^0, il faut et il suffit qu'il existe, pour tout (l), un élément $h'_{(l)}$ de $\mathfrak{o}(x^0, \mathbf{S}_n)$ tel que $(h'_{(l)} - \overline{h}_{(l)})|V = 0$; en d'autres termes, si, pour tout (l), on pose $\overline{h}_{(l)}|V = h_{(l)}$, *il faut et il suffit que, pour tout* (l), *la fonction* $h_{(l)}$ *sur* V *soit* $\mathfrak{p}$*-morphique en* x^0. Le même raisonnement montre que, pour que ω s'annule en x^0, il faut et il suffit que, pour tout (l), la fonction $h_{(l)}$ s'annule en x^0.

Supposons de plus ω et V définies sur k. Les fonctions $\overline{u}_1, \ldots, \overline{u}_r, f_1, \ldots, f_{n-r}$ peuvent être choisies définies sur k. Comme les $g_{(i)}$ sont alors définies sur k, on peut aussi prendre $\overline{g}_{(i)}$ définie sur k pour tout i. La fonction $\overline{h}_{(l)}$, donc aussi $h_{(l)}$, est alors définie sur k pour tout (l). On déduit de là la proposition suivante :

Proposition 13. — *Soit* V *une* $\mathfrak{p}$*-variété, définie sur* k, *et soit* x^0 *un point de* $\rho_e(V)$, $\mathfrak{p}$*-simple sur* V. *Alors, si* $y^0 \in \rho_e(V)$ *est une généralisation de* x^0 *sur* k^0, *on a* $D_k^q(y^0, V) \subset D_k^q(x^0, V)$ (*autrement dit, si* $\omega \in D_k^q(V)$, *l'ensemble des points* $\mathfrak{p}$*-simples sur* V *en lesquels* ω *n'est pas* $\mathfrak{p}$*-morphique, est* k^0*-fermé, relativement à l'ensemble de tous les points* $\mathfrak{p}$*-simples sur* V), *et* $D_k^q(x^0, V)_0 \subset D_k^q(x^0, V) \cap D_k^q(y^0, V)_0$. *Si* $x \in V$ *est une généralisation de* x^0 *sur* R, *on a* $D^q(x^0, V) \subset D^q(x, V)$ *et* $D^q(x^0, V)_0 \subset D^q(x^0, V) \cap D^q(x, V)_0$.

Démonstration. — On se ramène en effet immédiatement au cas d'une variété affine. Il suffit alors d'utiliser le critère précédent en remarquant que, pour $\omega \in D_k^q(x^0, V)$, on peut choisir les fonctions $u_i, f_j, \bar{g}_{(i)}$ de manière qu'elles soient définies sur k; puisque les $(df_j)_{x^0}$ sont linéairement indépendantes, il en est de même des $(df_j)_{y^0}$; d'autre part les fonctions $h_{(l)}$ sont définies sur k; donc si les $h_{(l)}$ sont p-morphiques (resp. s'annulent) en x^0, elles sont $\mathfrak{p}$-morphiques (resp. s'annulent) en y^0. Ceci prouve la première assertion; la seconde se traite d'une manière analogue.

Le critère précédent se simplifie dans le cas où ω est de *degré maximum* ($q = r = \dim V$). On a alors en effet $\omega = g du_1 \wedge \ldots \wedge du_r$, et il n'y a qu'une fonction $\bar{h}$; celle-ci est définie par $\bar{h} = \bar{g}\bar{J}$, où $\bar{g}$ est une fonction sur $\mathbf{S}_n$ telle que $\bar{g}|V = g$, et où $\bar{J} = D(\bar{u}_1, \ldots, \bar{u}_r, f_1, \ldots, f_{n-r})/D(X_1, \ldots, X_n)$. Il n'y a donc qu'une fonction h, définie par $h = gJ$, en posant $J = \bar{J}|V$. Dans ce cas, *pour que* ω *soit* $\mathfrak{p}$*-morphique (resp. s'annule) en* x^0, *il faut et il suffit que* h *soit* $\mathfrak{p}$*-morphique (resp. s'annule) en* x^0. Comme J ne dépend pas de ω, on voit en même temps que ωh^{-1} est $\mathfrak{p}$-morphique et non nulle en x^0, et que, si ω et ω' sont deux $\mathfrak{k}$-différentielles d'ordre r sur V, $\mathfrak{p}$-morphiques et non nulles en x^0, leur quotient ω/ω' est une fonction $\mathfrak{p}$-morphique et non nulle en x^0.

Dans toute la suite de ce numéro, on suppose ω de degré maximum r. On dira que ω est *définie* (resp. est *infinie*) en x^0 si h est $\mathfrak{p}$-définie (resp. infinie) en x^0. D'après ce qui précède, cette propriété ne dépend que de V, ω, et x^0, mais non de la façon dont on a choisi h. De même, si k_1 est un sous-corps de $\mathfrak{k}$ sur lequel V et ω sont définies, et si, en posant $k_1^0 = \rho(k_1)$, X est une k_1^0-variété contenue dans $\rho_e(V)$, et génériquement $\mathfrak{p}$-simple sur V, pour que ω soit génériquement $\mathfrak{p}$-morphique (resp. s'annule) sur X^0, il faut et il suffit qu'il en soit de même de h; on dira que ω est définie (resp. infinie) sur X^0 s'il en est de même de h.

Dans le cas particulier où X^0 est une k_1^0-composante C^0 de l'ensemble $\rho_e(V)$ (i.e. du cycle $V^0 = \rho(V)$), génériquement $\mathfrak{p}$-simple sur V, l'entier $\nu(C^0, h)$ (cf. n° 12) ne dépend que de V, C^0 et ω, mais non de h. On le désignera par $\nu(C^0, \omega)$. Le symbole $\nu(C^0, \omega)$ possède les propriétés suivantes :

$$\nu(C^0, f\omega) = \nu(C^0, f) + \nu(C^0, \omega)$$
$$\nu(C^0, \omega_1 + \omega_2) \geqslant \inf(\nu(C^0, \omega_1), \nu(C^0, \omega_2))$$

Dans le cas particulier où C^0 est une composante simple de V^0, on a, comme on a vu, $\nu(C^0, t) = 1$, et $\nu(C^0, \omega)$ est alors l'unique entier tel que la différentielle $\omega t^{-\nu}$ soit $\mathfrak{p}$-morphique et non nulle sur C^0.

Nous appellerons $\mathfrak{p}$-*diviseur* de ω le cycle $(\omega)_\mathfrak{p}$, de dimension r, défini par $(\omega)_\mathfrak{p} = \Sigma_{C^0} \nu(C^0, \omega) C^0$ où la somme est étendue à toutes les composantes C^0 de V^0 qui sont génériquement $\mathfrak{p}$-simples sur V. Posant $\nu_+(C^0, \omega) = \sup(0, \nu(C^0, \omega))$, et $\nu_-(C^0, \omega) = \sup(0, -\nu(C^0, \omega))$, on appelle $\mathfrak{p}$-diviseur des zéros, et $\mathfrak{p}$-diviseur des pôles de ω les cycles $(\omega)_{\mathfrak{p},0}$ et $(\omega)_{\mathfrak{p},\infty}$ respectivement définis par $(\omega)_{\mathfrak{p},0} = \Sigma_{C^0} \nu_+(C^0, \omega) C^0$, et $(\omega)_{\mathfrak{p},\infty} = \Sigma_{C^0} \nu_-(C^0, \omega) C^0$. On a ainsi $(\omega)_\mathfrak{p} = (\omega)_{\mathfrak{p},0} - (\omega)_{\mathfrak{p},\infty}$. Il sera commode, d'autre part, de désigner par $\{\omega\}_{\mathfrak{p},0}$, $\{\omega\}_{\mathfrak{p},\infty}$ et $\{\omega\}_\mathfrak{p}$ les sous-ensembles de $\rho_e(V)$ respectivement définis par

$$\{\omega\}_{\mathfrak{p},0} = (\mathrm{supp}(\omega)_{\mathfrak{p},0}) \cup \rho_e(\mathrm{supp}(\omega)_0)$$
$$\{\omega\}_{\mathfrak{p},\infty} = (\mathrm{supp}(\omega)_{\mathfrak{p},\infty}) \cup \rho_e(\mathrm{supp}(\omega)_\infty)$$
$$\{\omega\}_\mathfrak{p} = \{\omega\}_{\mathfrak{p},0} \cup \{\omega\}_{\mathfrak{p},\infty} = (\mathrm{supp}(\omega)_\mathfrak{p}) \cup \rho_e(\mathrm{supp}(\omega))$$

où l'on désigne par $(\omega)_0$ (resp. $(\omega)_\infty$), (resp. (ω)) le diviseur des zéros (resp. le diviseur des pôles, resp. le diviseur) de ω au sens habituel.

Proposition 14 (critère pour qu'une différentielle de degré maximum r soit $\mathfrak{p}$*-morphique en un point).* — *Soit* V *une* $\mathfrak{p}$*-variété, de dimension r, et soit* x^0 *un point de* $\rho_e(V)$, $\mathfrak{p}$*-simple sur* V. *Soit* ω *une* $\mathfrak{k}$*-différentielle de degré r sur* V. *Alors, pour que* ω *soit* $\mathfrak{p}$*-morphique (resp.* $\mathfrak{p}$*-morphique et non nulle, resp. définie) en* x^0, *il faut et il suffit qu'on ait* $x^0 \notin \{\omega\}_{\mathfrak{p},\infty}$ (*resp.* $x^0 \notin \{\omega\}_\mathfrak{p}$, *resp.* $x^0 \notin \{\omega\}_{\mathfrak{p},0} \cap \{\omega\}_{\mathfrak{p},\infty}$).

Démonstration. — Commençons par montrer que, si ω est $\mathfrak{p}$-morphique et non nulle en x^0, on a $x^0 \notin \{\omega\}_\mathfrak{p}$.

En effet, d'après la proposition 13, ω est génériquement $\mathfrak{p}$-morphique et non nulle sur toute composante de $\rho_e(V)$ contenant x^0. On a donc $x^0 \notin \mathrm{supp}(\omega)_\mathfrak{p}$. D'autre part, toujours d'après la proposition 13, si X est une sous-$\mathfrak{k}$-variété de V telle que $x^0 \notin \rho_e(X)$, ω est morphique et non nulle sur X; donc X ne peut être une $\mathfrak{k}$-composante de (ω). Autrement dit, on a $x^0 \notin \rho_e(\mathrm{supp}(\omega))$. On a donc bien $x^0 \notin \{\omega\}_\mathfrak{p}$.

Soit maintenant ω une différentielle quelconque de degré r sur V, définie sur $\mathfrak{k}$. On a vu qu'il existe une fonction h sur V définie sur $\mathfrak{k}$, telle que $\omega_0 = \omega h^{-1}$ soit $\mathfrak{p}$-morphique et non nulle en x^0. D'après ce que nous venons de montrer, on a $x^0 \notin \{\omega_0\}_\mathfrak{p}$. Donc, les composantes de $(\omega)_{\mathfrak{p},0}$ et $(h)_{\mathfrak{p},0}$ (et, de même, celles de $(\omega)_{\mathfrak{p},\infty}$ et $(h)_{\mathfrak{p},\infty}$) qui contiennent x^0 sont les mêmes. D'autre part, comme on a vu, pour que ω soit $\mathfrak{p}$-morphique (resp. $\mathfrak{p}$-morphique et non nulle, resp. définie) en x^0, il faut et il suffit que h le soit. Donc notre proposition résulte du corollaire de la proposition 10 du n° 12.

Introduisons encore une notation. Soit x^0 un point de $\rho_e(V)$ simple sur V^0. D'après la proposition précédente, pour qu'il existe un entier ν tel que $\omega t^{-\nu}$ soit $\mathfrak{p}$-morphique et non nulle en x^0, il faut et il suffit qu'on ait $x^0 \notin \rho_e(\mathrm{supp}(\omega))$, et cet entier ν est alors égal à $\nu(C^0, \omega)$, en désignant par C^0 l'unique composante de V^0 qui contient x^0. Nous désignerons alors cet entier par $\nu(x^0, \omega)$.

Proposition 15. — *Soient* V *et* V^* *deux* $\mathfrak{p}$*-variétés de même dimension r, et soit* $\varphi : V^* \to V$ *une application rationnelle, définie sur* $\mathfrak{k}$, *génériquement surjective. Soit* ω *une* $\mathfrak{k}$*-différentielle sur* V, *et soit* ω^* *la différentielle sur* V^* *transposée de* ω. *Soient* x^0 *un point de* $\rho_e(V)$, *simple sur* $V^0 = \rho(V)$

et x^{*0} un point de $\mathfrak{p}_e(V^*)$, simple sur $V^{*0}=\mathfrak{p}(V^*)$, tels que φ soit $\mathfrak{p}$-morphique en x^{*0}, de valeur x^0. Alors, si le symbole $v(x^0, \omega)$ est défini, le symbole $v(x^{*0}, \omega^*)$ l'est également, et on a $v(x^0, \omega)\leqslant v(x^{*0}, \omega^*)$.

Démonstration. — Il suffit d'appliquer la proposition 11 à la différentielle ωt^{-v}, en posant $v=v(x^0, \omega)$.

17. Introduction des entiers $l(x, V)$, $l_0(V)$.

Pour tout point $x\in\mathfrak{R}^n$, c'est-à-dire pour tout point entier $\mathfrak{p}$-adique de $\mathbf{S}_n$, de coordonnées $x_i=(x_i^{(0)}, x_i^{(1)}, \ldots, x_i^{(\mu)}, \ldots)$ $(1\leqslant i\leqslant n)$, on notera $k^0(x)$ le corps engendré sur k^0 par tous les coefficients $x_i^{(\mu)}$ $(1\leqslant i\leqslant n, \mu\geqslant 0)$.

Soit V une variété affine $(V\subset\mathbf{S}_n)$, de dimension r, définie sur $\mathfrak{k}$. Soit à nouveau $I=\mathfrak{I}(V)$ l'idéal de l'anneau $\mathfrak{R}[X]$ composé des polynômes de cet anneau qui s'annulent sur V. Soit $\mathfrak{B}=\{F_\alpha\}$ $(1\leqslant\alpha\leqslant q)$ un système de générateurs de I.

Soit $M=M_{\mathfrak{B}}$ la matrice $\left(\frac{\partial F_\alpha}{\partial X_i}\right)$ sur l'anneau R[X]. A tout point $x\in V_{\mathfrak{R}}$, associons l'entier

$$l=\inf_D v(D(x))$$

où D parcourt tous les déterminants d'ordre $n-r$ de la matrice M.

Posons $x^0=\mathfrak{p}(x)$. Considérons l'idéal $\mathfrak{i}(V, x^0, \mathbf{S}_n)=I\mathfrak{o}(x^0, S_n)=\mathfrak{m}(V, S_n)\cap\mathfrak{o}(x^0, S_n)$ de l'anneau local $\mathfrak{o}(x^0, \mathbf{S}_n)$, composé des fonctions $\mathfrak{p}$-morphiques en x^0 qui s'annulent sur V. Si $\mathfrak{S}=(g_1, \ldots, g_{n-r})$ est un système de $n-r$ éléments de cet idéal, et si $(i)=(i_1, \ldots, i_{n-r})$ est un système de $n-r$ entiers tels que $1\leqslant i_1<\ldots<i_{n-r}\leqslant n$, le déterminant

$$D_{(i)}(\mathfrak{S}, x)=(D(g_1, \ldots, g_{n-r})/D(X_{i_1}, \ldots, X_{i_{n-r}}))(x)$$

est une combinaison linéaire, à coefficients dans $\mathfrak{R}$, des déterminants $D(x)$ précédents. On a donc

$$l=\inf_{\mathfrak{S}, (i)} v(D_{(i)}(\mathfrak{S}, x))$$

Ceci montre que l'entier l ne dépend que de V et x, mais non de $\mathfrak{B}$. Nous le désignerons par $l(x)$, ou par $l(x, V)$. D'après les critères jacobiens de simplicité, pour que $x\in V_{\mathfrak{R}}$ soit simple sur V, il faut et il suffit que $l(x)$ soit fini. Pour que $x\in V_{\mathfrak{R}}$ soit simple (mod. $\mathfrak{p}$) sur V, il faut et il suffit que $l(x)=0$.

Supposons toujours que x est un point de $V_{\mathfrak{R}}$. Considérons l'anneau $\mathfrak{o}(x, \mathbf{S}_n)$ des fonctions sur $\mathbf{S}_n$ morphiques en x, son idéal maximal $\mathfrak{m}(x, \mathbf{S}_n)$ et l'espace tangent de Zariski $Z(x, \mathbf{S}_n)$. Soit ψ l'application canonique $\mathfrak{m}(x, \mathbf{S}_n)\to Z(x, \mathbf{S}_n)$. Pour toute $f\in\mathfrak{m}(x, \mathbf{S}_n)$, l'image $\psi(f)$ est appelée différentielle de f en x, et est notée $(df)_x$. On a

$$(df)_x=\Sigma_i\frac{\partial f}{\partial X_i}(x)(dX_i)_x.$$

Considérons d'autre part l'idéal $\mathfrak{i}(x)=\mathfrak{i}(x, x^0, \mathbf{S}_n)=\mathfrak{m}(x, \mathbf{S}_n)\cap\mathfrak{o}(x^0, \mathbf{S}_n)$ de l'anneau local $\mathfrak{o}(x^0, \mathbf{S}_n)$, composé des fonctions $\mathfrak{p}$-morphiques en x^0 qui s'annulent en x. L'image de $\mathfrak{i}(x)$

par ψ est le $\mathfrak{R}$-module $\overline{\mathrm{D}}(x, \mathbf{S}_n)$, isomorphe à $\mathfrak{R}^n$, engendré par les $(d\mathrm{X}_i)_x$. L'image par ψ de l'idéal $\mathfrak{i}(\mathrm{V}) = \mathfrak{i}(\mathrm{V}, x^0, \mathbf{S}_n)$ considéré plus haut est le sous-$\mathfrak{R}$-module $\overline{\mathrm{D}}(\mathrm{V}, x, \mathbf{S}_n)$ du précédent engendré par les $(d\mathrm{F}_\alpha)_x$. La matrice des $(d\mathrm{F}_\alpha)_x$ par rapport aux $(d\mathrm{X}_i)_x$ est $M(x) = \left(\frac{\partial \mathrm{F}_\alpha}{\partial \mathrm{X}_i}\right)(x)$.

Supposons en particulier que x est simple sur V. Alors le $\mathfrak{R}$-module $\overline{\mathrm{D}}(\mathrm{V}, x, \mathbf{S}_n)$ est de dimension $n-r$. D'après les propriétés des modules sur les anneaux principaux ([1], chap. VII, § 4, th. 1), il existe une $\mathfrak{R}$-base $\mathscr{B}$ de $\overline{\mathrm{D}}(\mathrm{V}, x, \mathbf{S}_n)$ qui est de la forme $\{t^{m_\beta}\varphi_\beta\}$ $(1 \leqslant \beta \leqslant n-r)$ où les m_β sont des entiers $\geqslant 0$ (on supposera les indices ordonnés de manière qu'on ait $m_1 \leqslant \ldots \leqslant m_{n-r}$), et où les φ_β sont des éléments $\mathfrak{R}$-indépendants de $\overline{\mathrm{D}}(x, \mathbf{S}_n)$. Une telle base $\mathscr{B}$ sera appelée une *base standard* du $\mathfrak{R}$-module $\overline{\mathrm{D}}(\mathrm{V}, x, \mathbf{S}_n)$. Il existe des éléments $g_\beta \in \mathfrak{i}(\mathrm{V})$ tels qu'on ait $(dg_\beta)_x = t^{m_\beta}\varphi_\beta$. On dira que ces éléments *induisent la base standard* $\mathscr{B}$. On peut toujours prendre pour fonctions g_β des polynômes, i.e. des éléments de $\mathrm{I} = \mathscr{I}(\mathrm{V})$. On a, pour tout β, $\varphi_\beta = \Sigma_i b_{\beta i}(d\mathrm{X}_i)_x$, d'où $\frac{\partial g_\beta}{\partial \mathrm{X}_i}(x) = t^{m_\beta} b_{\beta i}$ pour tout couple (β, i), où les $b_{\beta i}$ sont des éléments de $\mathfrak{R}$ tels que, en posant $b^0_{\beta i} = \rho(b_{\beta i})$, la matrice $(b^0_{\beta i})$ soit de rang $n-r$. L'entier $l(x) = l(x, \mathrm{V})$ est alors donné par $l(x) = \Sigma_\beta m_\beta$.

Proposition 16 (invariance de $l(x, \mathrm{V})$). — *Soient* V *et* W *deux variétés affines, définies sur* $\mathfrak{k}$, *et soit* $\varphi : \mathrm{V} \to \mathrm{W}$ *une application rationnelle, définie sur* $\mathfrak{k}$. *Soit* $x \in \mathrm{V}_\mathfrak{R}$ *tel que* φ *soit* $\mathfrak{p}$*-isomorphique en* $x^0 = \rho(x)$, *et posons* $y = \varphi(x)$. *Alors on a* $y \in \mathrm{W}_\mathfrak{R}$, *et* $l(x, \mathrm{V}) = l(y, \mathrm{W})$.

Démonstration. — L'appartenance $y \in \mathrm{W}_\mathfrak{R}$ est immédiate, et on a $y^0 = \rho(y) = \varphi^0(x^0)$.

Par passage au graphe, on se ramène au cas où φ est induite par la projection $\pi : \mathbf{S}_m \to \mathbf{S}_n$ $(m > n)$ qui, au point $x = (x_1, \ldots, x_m)$ fait correspondre $y = (x_1, \ldots, x_n)$.

On a alors un $\mathfrak{R}$-monomorphisme $\pi^* : \overline{\mathrm{D}}(\mathrm{W}, y, \mathbf{S}_n) \to \overline{\mathrm{D}}(\mathrm{V}, x, \mathbf{S}_m)$ canoniquement déduit de π; le $\mathfrak{R}$-module $\overline{\mathrm{D}}(\mathrm{V}, x, \mathbf{S}_m)$ est engendré par l'image de π^*, et par $(d\mathrm{X}_{n+1})_x, \ldots, (d\mathrm{X}_m)_x$. Le résultat s'en déduit aussitôt.

D'après cette proposition, la définition de l'entier $l(x)$ s'étend d'une manière naturelle au cas où V est une $\mathfrak{p}$-variété quelconque.

Lemme 1. — *Soient* P_j $(1 \leqslant j \leqslant q)$ *des polynômes appartenant à* $\mathfrak{R}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, *et n'admettant aucun zéro commun sur* $\mathbf{S}_n$. *Alors il existe un entier a, qui ne dépend que des* P_j, *tel qu'on ait* $\inf_j v(\mathrm{P}_j(x)) \leqslant a$ *pour tout point* $x \in (\mathbf{S}_n)_\mathfrak{R} = \mathfrak{R}^n$. (*Ce lemme est un cas particulier de* ([23], chap. I^er, n° 7, th. 3).)

Démonstration. — D'après le théorème des zéros de Hilbert, il existe des polynômes Q^*_j, à coefficients dans $\mathfrak{k}$, tels qu'on ait $\Sigma_j \mathrm{P}_j \mathrm{Q}^*_j = 1$. En chassant les dénominateurs des coefficients des polynômes Q^*_j, on en déduit qu'il existe des polynômes Q_j $(1 \leqslant j \leqslant q)$ à coefficients dans $\mathfrak{R}$, et un entier a, tels qu'on ait $\Sigma_j \mathrm{P}_j \mathrm{Q}_j = t^a$. En substituant aux indéterminées les coordonnées de x, on voit qu'on a bien $\inf_j v(\mathrm{P}_j(x)) \leqslant a$.

Corollaire. — *Soient* E_α $(1 \leqslant \alpha \leqslant q)$ *des sous-ensembles* $\mathfrak{k}$*-fermés de* $\mathbf{S}_n$ *n'admettant aucun point commun. Alors il existe un entier a, qui ne dépend que des* E_α, *tel qu'on ait* $\inf_\alpha v(x, \mathrm{E}_\alpha)_\mathfrak{p} \leqslant a$, *pour tout point* $x \in (\mathbf{S}_n)_\mathfrak{R} = \mathfrak{R}^n$.

En effet, si, pour tout j, $\{P_{\alpha j}\}$ $(1 \leqslant j \leqslant h_\alpha)$ est un système de générateurs de l'idéal $\mathfrak{I}(E_\alpha)$, il suffit d'appliquer le lemme précédent à l'ensemble des polynômes $P_{\alpha j}$ obtenus pour tous les couples (α, j) possibles $(1 \leqslant \alpha \leqslant q,\ 1 \leqslant j \leqslant h_\alpha)$.

Proposition 17. — Soit V *une* p*-variété sans point multiple. Alors, pour* $x \in V_{\mathfrak{R}}$, *l'entier* $l(x, V)$ *admet une borne supérieure qui ne dépend que de* V.

Démonstration. — Soit $\{F_\alpha\}$ $(1 \leqslant \alpha \leqslant q)$ un système de générateurs de l'idéal $\mathfrak{I}(V)$. Les déterminants D_j d'ordre $n-r$ de la matrice $M = \left(\frac{\partial F_\alpha}{\partial X_i}\right)$ n'admettent aucun zéro commun sur V. Autrement dit, les polynômes F_α et D_j (obtenus pour toutes les valeurs possibles de α et de j) n'admettent aucun zéro commun sur $\mathbf{S}_n$. Il suffit de leur appliquer le lemme 1.

La borne supérieure (majorant minimum) de l'entier $l(x)$ sera désignée par $l_0(V)$.

18. Introduction des entiers $m(x, V)$, $m_0(V)$.

Pour $x \in \mathfrak{R}^n$, et pour tout entier $\mu \geqslant 0$, notons $\varphi_{\mu x}$ le $\mathfrak{k}$-automorphisme de l'espace affine $\mathbf{S}_n$ qui, au point $u = (u_1, \ldots, u_n)$, fait correspondre le point $u' = (u'_1, \ldots, u'_n)$ défini par $u'_i = t^{-(\mu+1)}(u_i - x_i)$ pour tout i. En particulier, le transformé x' de x est l'origine $(0, \ldots, 0)$.

Proposition 18. — Soit V *une variété affine* $(V \subset \mathbf{S}_n)$, *définie sur* k, *et soit* $x \in V_{\mathfrak{R}}$. *A tout entier* $\mu \geqslant 0$, *associons la variété* $V_{\mu x} = \varphi_{\mu x}(V)$, *et le cycle réduit* $V^0_{\mu x} = \rho(V_{\mu x})$.

Il existe un plus petit entier $m = m(x) = m(x, V)$ *tel que l'origine soit un point simple sur* $V^0_{\mu x}$. *On a* $m(x) \leqslant l(x)$. *De plus, pour* $\mu > m(x)$, *le cycle* $V^0_{\mu x}$ *admet une composante unique et simple, qui est une variété linéaire. Cette variété linéaire* $L_0(x)$ *ne dépend pas de* μ.

Démonstration. — Posons $r = \dim V$. Soit $\{G_\beta\}$ $(1 \leqslant \beta \leqslant n-r)$ un système de polynômes de $\mathfrak{I}(V)$ induisant une base standard du $\mathfrak{R}$-module $\overline{D}(V, x, \mathbf{S}_n)$. Pour tout $\mu \geqslant 0$, les polynômes $G'_\beta(X) = G_\beta(x + t^{\mu+1}X)$ $(1 \leqslant \beta \leqslant n-r)$, s'annulent sur $V_{\mu x}$. D'après la formule de Taylor, on a, dans l'anneau $\mathfrak{R}[X] = \mathfrak{R}[X_1, \ldots, X_n]$, la congruence

$$G'_\beta(X) \equiv t^{\mu+1} \Sigma_{i=1}^n \frac{\partial G_\beta}{\partial X_i}(x) X_i \qquad (\text{mod. } t^{2\mu+2})$$

On a donc $G'_\beta(X) \equiv t^{\mu+1+m_\beta} \Sigma_i b_{\beta i} X_i$ (mod. $t^{2\mu+2}$), avec les notations introduites au numéro précédent. Donc, si on a pris $\mu \geqslant l(x) = \Sigma_\beta m_\beta$, on a, *a fortiori*, pour tout β, $\mu + 1 > m_\beta$ d'où $\mu + 1 + m_\beta < 2\mu + 2$; pour tout β, le polynôme $G^*_\beta = G'_\beta t^{-(\mu+1+m_\beta)}$ est alors à coefficients entiers (donc appartient à l'idéal $\mathfrak{I}(V_{\mu x})$), et admet pour polynôme réduit $G^{*0}_\beta(X) = \Sigma_i b^0_{\beta i} X_i$. Comme la matrice $(b^0_{\beta i})$ est de rang $n-r$, les équations $G^{*0}_\beta(X) = 0$ $(1 \leqslant \beta \leqslant n-r)$ représentent une variété linéaire de dimension r. Comme cette variété linéaire $L_0(x)$ contient $\rho_e(V_{\mu x})$, et comme ce dernier ensemble n'est pas vide (puisqu'il contient l'origine), on a $\rho_e(V_{\mu x}) = L_0(x)$. L'indépendance linéaire des p-différentielles $(dG^*_\beta)^0_{x^0}$ implique en outre que l'origine est simple sur le cycle $V^0_{\mu x}$, donc que $L_0(x)$ est une composante simple de ce cycle.

Pour achever la démonstration, il suffit de vérifier que, si μ est un entier tel que l'origine soit simple sur $V^0_{\mu x}$, et si ν est un entier >0, le cycle $V^0_{\mu+\nu,x}$ admet pour composante unique et simple une variété linéaire (qui coïncide alors nécessairement avec $L_0(x)$). Or, ceci résulte du fait que $V_{\mu+\nu,x}$ se déduit de $V_{\mu x}$ par l'homothétie $u \to t^{-\nu}u$ de $\mathbf{S}_n$.

Remarque. — L'entier m est majoré par $m' = \sup_\beta m_\beta$. Mais il peut arriver qu'il soit strictement inférieur à m'. Par exemple, si V est la courbe $t^2X + Y^3 = 0$, et x l'origine (0, 0), on a $n - r = 1$, et $m' = m_1 = 2$, mais cependant $m = 1$.

Proposition 19 (Invariance de $m(x)$). — *Soient* V *et* W *deux variétés affines, définies sur* $\mathfrak{k}$, *et soit* φ *une application rationnelle* $\varphi : V \to W$, *définie sur* $\mathfrak{k}$. *Soit* $x \in V_{\mathfrak{R}}$, *tel que* φ *soit* $\mathfrak{p}$*-isomorphique en* $x^0 = \rho(x)$. *Alors, on a* $y \in W_{\mathfrak{R}}$ *et* $m(x, V) = m(y, W)$.

Démonstration. — Supposons $V \subset \mathbf{S}_m$, $W \subset \mathbf{S}_n$. Posons $x = (x_1, \ldots, x_m)$ et $y = (y_1, \ldots, y_n)$. On a, comme dans la proposition 16, $y \in W_{\mathfrak{R}}$, et $y^0 = \rho(y) = \varphi^0(x^0)$.

Soit $\overline{x} = (\overline{x}_1, \ldots, \overline{x}_m)$ un point générique de V sur $\mathfrak{k}$; le point $\overline{y} = \varphi(\overline{x}) = (\overline{y}_1, \ldots, \overline{y}_n)$ est alors générique de W sur $\mathfrak{k}$. Pour tout entier $\mu \geqslant 0$, posons $\overline{x}'_\mu = \varphi_{\mu x}(\overline{x})$, et $\overline{y}'_\mu = \varphi_{\mu y}(\overline{y})$. Les coordonnées de $\overline{x}$ et $\overline{y}$ vérifient des relations de la forme $\overline{y}_j - y_j = \sum_{i=1}^m g_{ji}(\overline{x})(\overline{x}_i - x_i)$ $(j = 1, \ldots, n)$ où les g_{ji} sont des fonctions sur V, $\mathfrak{p}$-morphiques en x^0. On en déduit que, pour tout μ, les coordonnées $\overline{y}_{\mu j}$ de $\overline{y}'_\mu$ s'expriment par des fonctions $\mathfrak{p}$-morphiques à l'origine au moyen de celles $\overline{x}_{\mu i}$ de $\overline{x}_\mu$. L'application $\varphi'_\mu : V_{\mu x} \to W_{\mu y}$, définie par $\varphi'_\mu = \varphi_{\mu y} \circ \varphi \circ \varphi_{\mu x}^{-1}$ est donc $\mathfrak{p}$-isomorphique à l'origine. La $\mathfrak{p}$-simplicité de l'origine est conservée par φ'_μ, d'où la proposition.

Cette proposition permet immédiatement d'étendre la définition de l'entier $m(x)$ au cas d'une $\mathfrak{p}$-variété quelconque. Puisqu'on a toujours $m(x, V) \leqslant l(x, V)$, l'entier $m(x, V)$ est majoré par $l_0(V)$. On désignera sa borne supérieure par $m_0(V)$. On a $m_0(V) \leqslant l_0(V)$.

19. Condition pour qu'un point entier $\mathfrak{p}$-adique soit congru (mod. $\mathfrak{p}^\mu$) à un point entier $\mathfrak{p}$-adique de V.

Proposition 20. — *Soit* V *une variété affine* $(V \subset \mathbf{S}_n)$, *de dimension* r, *définie sur* $\mathfrak{k}$, *sans point multiple. Il existe un plus petit entier* $s_0 = s_0(V)$ *vérifiant la condition suivante : pour tout entier* $\mu \geqslant s_0$, *et pour tout* $x \in \mathfrak{R}^n$ *tel qu'on ait* $(x, V)_\mathfrak{p} \geqslant \mu + s_0$, *il existe* $y \in V_{\mathfrak{R}}$ *tel que* $(x, y)_\mathfrak{p} \geqslant \mu$ (i.e. $y \equiv x \pmod{\mathfrak{p}^\mu}$).

Démonstration. — Posons $r = \dim V$. Soit $\{F_\alpha\}$ $(1 \leqslant \alpha \leqslant q)$ un système de générateurs de l'idéal $\mathscr{I}(V)$. Pour tout système $(\alpha) = (\alpha_1, \ldots, \alpha_{n-r})$ de $n - r$ entiers tels que $1 \leqslant \alpha_1 < \ldots < \alpha_{n-r} \leqslant q$, désignons par $S_{(\alpha)}$ l'intersection des hypersurfaces $F_{\alpha_j}(X) = 0$ $(1 \leqslant j \leqslant n - r)$, par $S^*_{(\alpha)}$ la $\mathfrak{k}$-adhérence du complémentaire de V dans $S_{(\alpha)}$; par $M_{(\alpha)}$ la matrice $\left(\frac{\partial F_{\alpha_j}}{\partial X_i}\right)$ sur l'anneau $\mathfrak{R}[X] = \mathfrak{R}[X_1, \ldots, X_n]$; par $S'_{(\alpha)}$ l'ensemble des zéros communs des déterminants $D_{(\alpha),(i)} = D(F_{\alpha_1}, \ldots, F_{\alpha_{n-r}})/D(X_{i_1}, \ldots, X_{i_{n-r}})$ d'ordre $n - r$ de $M_{(\alpha)}$; par $T_{(\alpha)}$ la réunion $S^*_{(\alpha)} \cup S'_{(\alpha)}$. Pour tout $x \in \mathfrak{R}^n$, posons $l_{(\alpha)}(x) = \inf_{(i)} v(D_{(\alpha),(i)}(x))$.

On a $(\bigcap_{(\alpha)} T_{(\alpha)}) \cap V = \emptyset$. En effet, si $x \in V$, il existe un (α) tel que $M_{(\alpha)}(x)$ soit de rang $n-r$; pour un tel α, les hypersurfaces $F_{\alpha_j}(X) = 0$ se coupent transversalement en x; par suite V est la seule composante de leur intersection contenant x, et on a $x \notin T_{(\alpha)}$.

Il existe donc, d'après le corollaire du lemme 1 du n° 17, un entier s_1 tel qu'on ait, pour tout $x \in \mathfrak{R}^n$, la relation

$$\inf_{(\alpha)}((x, T_{(\alpha)})_p, (x, V)_p) \leqslant s_1 \tag{22}$$

Nous allons montrer que la condition de l'énoncé est vérifiée par l'entier $s_1 + 1$. Pour cela, il nous suffit de prouver l'assertion suivante : pour tout triplet $(x, \mu, (\alpha))$ composé d'un point $x \in \mathfrak{R}^n$, d'un entier $\mu \geqslant s_1 + 1$, et d'un système d'indices (α) de la forme considérée plus haut, tels qu'on ait les relations

$$\inf_j v(F_{\alpha_j}(x)) \geqslant s_1 + \mu \tag{23}$$

et

$$(x, T_{(\alpha)}) \leqslant s_1, \tag{24}$$

il existe un $z \in \mathfrak{R}^n$ tel qu'on ait les relations

$$(z, x)_p \geqslant \mu \tag{25}$$

$$\inf_j v(F_{\alpha_j}(z)) \geqslant s_1 + \mu + 1. \tag{26}$$

En effet, puisqu'on a $\mu > s_1$, les relations (24) et (25) entraînent $(z, T_{(\alpha)})_p \leqslant s_1$. Donc, en supposant exacte l'assertion précédente, on peut, pour $x \in \mathfrak{R}^n$ tel que $(x, V)_p \geqslant \mu + s_1 + 1$, trouver (en tenant compte de (22)) un entier (α) tel que $(x, T_{(\alpha)})_p \leqslant s_1$, puis, par récurrence sur ν, construire une suite $(x_0 = x, x_1, \ldots, x_\nu, \ldots)$ de points de $\mathfrak{R}^n$ telle qu'on ait, pour tout $\nu \geqslant 0$, les inégalités $(x_\nu, x_{\nu+1})_p \geqslant \mu + \nu$, $\inf_j v(F_{\alpha_j}(x_\nu)) \geqslant s_1 + \mu + \nu$ et $(x_\nu, T_{(\alpha)}) \leqslant s_1$. La première de ces trois inégalités entraîne que la suite x_ν converge p-adiquement, et que, si y est sa limite, on a $(x, y)_p \geqslant \mu$; la seconde entraîne $F_{\alpha_j}(y) = 0$ pour tout j $(1 \leqslant j \leqslant n-r)$, d'où $y \in S_{(\alpha)}$: la troisième entraîne $(y, T_{(\alpha)}) \leqslant s_1$, ce qui implique $y \notin T_{(\alpha)}$; on a donc $y \notin S^*_{(\alpha)}$, d'où $y \in V$, d'où $y \in V_{\mathfrak{R}}$.

On remarque d'autre part, en faisant le changement de variable $z = x + t^\mu u$, que, pour x, μ et (α) vérifiant les conditions (23) et (24), la condition de l'existence d'un z vérifiant (25) et (26) équivaut à celle de l'existence d'un $u \in \mathfrak{R}^n$ tel qu'on ait, pour tout j $(1 \leqslant j \leqslant n-r)$

$$v(F_{\alpha_j}(x + t^\mu u)) \geqslant s_1 + \mu + 1. \tag{27}$$

Or, on peut exhiber un tel u. Il suffit de prendre pour u une solution entière ($u_i \in \mathfrak{R}$ pour tout i) du système linéaire

$$F_{\alpha_j}(x) + t^\mu \Sigma_{i=1}^n \left(\frac{\partial F_{\alpha_j}}{\partial X_i}\right)(x) X_i = 0 \qquad (1 \leqslant j \leqslant n-r) \tag{28}$$

Une telle solution existe puisqu'on a $\inf_j v(F_{\alpha_j}(x)) \geqslant s_1 + \mu$ et puisque la relation $(x, T_{(\alpha)}) \leqslant s_1$ implique $(x, S'_{(\alpha)}) \leqslant s_1$, d'où $l_{(\alpha)}(x) \leqslant s_1$; d'autre part, on a, pour tout j ($1 \leqslant j \leqslant n-r$), d'après la formule de Taylor, la congruence

$$F_{\alpha_j}(x + t^\mu X) \equiv F_{\alpha_j}(x) + t^\mu \Sigma_{i=1}^n \frac{\partial F_{\alpha_j}}{\partial X_i}(x) X_i \qquad (\text{mod. } t^{2\mu})$$

dans l'anneau $\mathfrak{R}[X]$. En prenant pour u une solution entière de (28) et en substituant u à X dans la relation ci-dessus, on obtient $v(F_{\alpha_j}(x + t^\mu u)) \geqslant 2\mu$. Cette inégalité entraîne bien (27), puisqu'on a $\mu \geqslant s_1 + 1$, d'où $2\mu \geqslant s_1 + \mu + 1$.

Donc, on a bien montré que l'entier $s_1 + 1$ vérifie la condition de l'énoncé. D'autre part, il est clair que si un entier $\geqslant 0$ vérifie cette condition, il en est de même de tout entier plus grand; donc, il existe bien un plus petit entier s_0 vérifiant cette condition.

20. Provariétés.

Nous appellerons *provariété* la limite projective X d'une suite

$$X^0 \xleftarrow[\theta^0]{} X^1 \xleftarrow[\theta^1]{} \dots \leftarrow X^\mu \xleftarrow[\theta^\mu]{} \dots$$

où les X^μ sont des variétés (relativement au domaine universel $\mathfrak{k}^0$) et les θ^μ des morphismes, que nous supposerons toujours génériquement surjectifs. Soit k_1^0 un sous-corps de $\mathfrak{k}^0$; nous dirons que X est *définie sur* k_1^0 si X^μ et θ^μ sont définis sur k_1^0 pour tout μ.

Un *point* x de X est une suite $(x^0, x^1, \dots, x^\mu, \dots)$ avec $x^\mu \in X^\mu$ et $x^\mu = \theta^\mu(x^{\mu+1})$ pour tout μ. On note $k_1^0(x)$ le corps $k_1^0(x^0, x^1, \dots, x^\mu, \dots)$. L'application $X \to X^\mu$ qui, au point x, fait correspondre x^μ, est notée ρ^μ. L'ensemble $\rho^\mu(X)$ admet pour adhérence X^μ, mais est, en général, distinct de X^μ. La variété X^μ sera également désignée par la notation $\overline{\rho}^\mu(X)$.

Une *sous-provariété* Y de X est une provariété définie par une suite

$$Y^0 \xleftarrow[\varphi^0]{} Y^1 \xleftarrow[\varphi^1]{} \dots \leftarrow Y^\mu \xleftarrow[\varphi^\mu]{} \dots$$

où, pour tout μ, Y^μ est une sous-variété de X^μ, et où le morphisme φ^μ est induit par θ^μ.

Supposons X définie sur k_1^0, et soient x et y deux points de X. On dit que y est une *spécialisation de x sur k_1^0* ou que x est une *généralisation de y sur k_1^0*, si, pour tout μ, y^μ est une spécialisation de x^μ sur k_0^1.

21. Structure des ensembles $\mathbf{V}_{\mathfrak{R}}^\mu$.

Pour tout point $x \in \mathfrak{R}^n = (\mathbf{S}_n)_{\mathfrak{R}}$, de coordonnées $x_i = (x_i^{(0)}, x_i^{(1)}, \dots, x_i^{(\mu)}, \dots)$, et pour tout entier $\mu \geqslant 0$, on notera x^μ le point de l'espace affine $\mathbf{S}^0_{n(\mu+1)}$ ayant pour coordonnées $x_1^{(0)}, \dots, x_n^{(0)}, \dots, x_1^{(\mu)}, \dots, x_n^{(\mu)}$. On notera ρ^μ l'application $\mathfrak{R}^n \to \mathbf{S}_{n(\mu+1)}$ définie par $x^\mu = \rho^\mu(x)$; en particulier ρ^0 s'identifie à ρ. On notera d'autre part ρ_*^μ l'application $\mathfrak{R}^n \to \mathfrak{R}^n$ qui, au point x, fait correspondre le point x_*^μ de coordonnées $x_{i*}^\mu = (x_i^{(0)}, \dots, x_i^{(\mu)}, 0, \dots, 0, \dots)$, c'est-à-dire le point obtenu en tronquant à l'ordre μ les suites des coefficients de chacune des coordonnées de x. On a, pour tout μ, une

application injective $\xi^\mu : \mathbf{S}^0_{n(\mu+1)} \to \mathfrak{R}^n$ telle que $\rho^\mu_* = \xi^\mu \circ \rho^\mu$, c'est-à-dire que $x^\mu_* = \rho^\mu_*(x^\mu)$. La donnée du point $x^\mu = \rho^\mu(x)$, ou celle du point $x^\mu_* = \rho^\mu_*(x) = \xi^\mu(x^\mu)$ équivaut à celle de la classe de x (mod. t^μ).

Pour tout couple d'entiers (μ, μ') tels que $0 \leqslant \mu' \leqslant \mu$, on notera $\theta^{\mu'\mu}$ la projection $\mathbf{S}^0_{n(\mu+1)} \to \mathbf{S}^0_{n(\mu'+1)}$ définie par la restriction aux $n(\mu'+1)$ premières coordonnées. La projection $\theta^{\mu,\mu+1}$ sera également notée θ^μ. On a, quels que soient μ et μ', $x^{\mu'} = \theta^{\mu'\mu}(x^\mu)$, et $x^\mu = \theta^\mu(x^{\mu+1})$.

On peut munir, d'une manière naturelle, l'ensemble $\mathfrak{R}^n$ des points entiers p-adiques de $\mathbf{S}_n$ d'une structure de provariété : celle définie par la suite

$$\mathbf{S}^0_n \xleftarrow[\theta^0]{} \mathbf{S}^0_{2n} \xleftarrow[\theta^1]{} \cdots \leftarrow \mathbf{S}^0_{n(\mu+1)} \xleftarrow[\theta^\mu]{} \cdots$$

le point $x \in \mathfrak{R}^n$ étant identifié à la suite $x^0, x^1, \ldots, x^\mu, \ldots$, où $x^\mu = \rho^\mu(x)$ pour tout μ. Cette provariété est définie sur le sous-corps premier de k^0. On remarquera que, pour $x \in \mathfrak{R}^n$, toute spécialisation de x sur k^0 est aussi une spécialisation de x sur k.

Pour toute sous-variété V de $\mathbf{S}_n$, définie sur k, on posera $\mathrm{V}^\mu_{\mathfrak{R}} = \rho^\mu(\mathrm{V}_{\mathfrak{R}})$. L'application induite par ρ^μ (resp. θ^μ, resp. $\theta^{\mu'\mu}$) sur $\mathrm{V}_{\mathfrak{R}}$ (resp. $\mathrm{V}^\mu_{\mathfrak{R}}$, resp. $\mathrm{V}^\mu_{\mathfrak{R}}$) sera notée ρ^μ_{V} (resp. θ^μ_{V}, $\theta^{\mu'\mu}_{\mathrm{V}}$).

Proposition 21. — Soit V *une variété affine, définie sur k, et soit* x^μ *un point de* $\mathrm{V}^\mu_{\mathfrak{R}}$ *vérifiant la condition suivante : il existe* $x \in \mathrm{V}_{\mathfrak{R}}$, *simple sur* V, *tel qu'on ait* $x^\mu = \rho^\mu(x)$, *et* $m(x) \leqslant \mu$. *Alors l'ensemble* $(\theta^\mu_{\mathrm{V}})^{-1}(x^\mu)$ *est une variété linéaire* $\mathrm{L}^\mu(x^\mu)$, *de dimension r, et qui est rationnelle sur* $k^0(x^\mu)$. *La condition précédente est, en particulier, vérifiée pour tout* $x^\mu \in \mathrm{V}^\mu_{\mathfrak{R}}$ *si* V *est sans point multiple, et si on a* $\mu \geqslant m_0(\mathrm{V})$.

Démonstration. — Puisqu'on a $\mu \geqslant m(x)$, et d'après la définition de $m(x)$ (cf. n° 18, prop. 18), le cycle $\mathrm{V}^0_{\mu+1,x}$, réduit (mod p) de la variété $\mathrm{V}_{\mu+1,x} = \varphi_{\mu+1,x}(\mathrm{V})$ admet pour composante unique et simple une variété linéaire $\mathrm{L}_0(x)$, passant par l'origine, et ne dépendant pas de μ. Considérons le point $y = \rho^\mu_*(x)$, obtenu en tronquant à l'ordre μ les suites de coefficients qui définissent les coordonnées de x, et remplaçons x par y. L'application $\tau = \varphi_{\mu+1,y} \circ \varphi^{-1}_{\mu+1,x} : \mathbf{S}_n \to \mathbf{S}_n$ est la translation définie par le point $\mu = (x - y)t^{-(\mu+1)}$ de $\mathfrak{R}^n$, donc est un $\mathfrak{R}$-automorphisme de $\mathbf{S}_n$. Le cycle $\mathrm{V}^0_{\mu+1,y}$ réduit (mod p) de $\mathrm{V}_{\mu+1,y} = \rho_{\mu+1,y}(\mathrm{V})$ admet encore pour composante unique et simple une variété linéaire $\mathrm{L}^\mu_0(x^\mu)$, déterminée par x^μ, et définie sur $k^0(y) = k^0(x^\mu)$. Or si z et z' sont deux points de $\mathfrak{R}^n$ tels qu'on ait $z' = \varphi_{\mu+1,y}(z)$, les relations $z \in (\rho^\mu_{\mathrm{V}})^{-1}(x^\mu)$, et $z' \in (\mathrm{V}_{\mu+1,y})_{\mathfrak{R}}$ sont équivalentes; de plus, lorsque ces relations sont satisfaites, on a, pour tout i, $z_i^{(\mu+1)} = (\mathrm{F}^0)^{\mu+1}(z'^0)$. Or, l'automorphisme F^0 laisse invariante la variété $\mathrm{L}^\mu_0(x^\mu)$. Donc l'ensemble $(\theta^\mu_{\mathrm{V}})^{-1}(x^\mu)$ est la variété linéaire $\mathrm{L}^\mu(x^\mu) = x^{(\mu)} \times \mathrm{L}^\mu_0(x^\mu)$ dans l'espace affine $\mathbf{S}_{n(\mu+2)} = \mathbf{S}_{n(\mu+1)} \times \mathbf{S}_n$. Puisque $\mathrm{L}^\mu_0(x^\mu)$ est définie sur $k^0(x^\mu)$, il en est de même de $\mathrm{L}^\mu(x^\mu)$.

Pour tout entier $\nu \geqslant 0$, on désignera par $\mathscr{F}_\nu(\mathrm{V})$ l'ensemble des points $x \in \mathfrak{R}^n$, tels qu'on ait $(x, \mathrm{V})_{\mathfrak{p}} \geqslant \nu$, c'est-à-dire tels qu'on ait $v(\mathrm{P}(x)) \geqslant \nu$ pour tout $\mathrm{P} \in \mathscr{I}(\mathrm{V})$. L'ensemble $\mathrm{V}_{\mathfrak{R}} = \mathrm{V} \cap \mathfrak{R}^n$ coïncide avec l'intersection $\bigcap_\nu \mathscr{F}_\nu(\mathrm{V})$. Pour tout couple (μ, ν) d'entiers positifs, on posera $\mathscr{F}^\mu_\nu = \mathscr{F}^\mu_\nu(\mathrm{V}) = \rho^\mu(\mathscr{F}_\nu(\mathrm{V}))$.

Proposition 22. — *Soit* V *une sous-variété de* $\mathbf{S}_n$, *définie sur* k. *Alors :*

(i) *pour tout couple d'entiers positifs* (μ, ν), $\mathscr{F}_\nu^\mu(V)$ *est un sous-ensemble* k^0*-constructible de l'espace affine* $\mathbf{S}^0_{n(\mu+1)}$; *de plus, pour* $\mu \geqslant \nu$, *ce sous-ensemble est* k^0*-fermé.*

(ii) *Pour tout entier positif* μ, $V_\mathfrak{R}^\mu$ *est un sous-ensemble constructible de* $\mathbf{S}^0_{n(\mu+1)}$.

Démonstration. — Notons $\mathscr{I}_R(V)$ l'idéal de l'anneau $R[X_1, \ldots, X_n]$ composé des polynômes de cet anneau qui s'annulent sur V. Soit $\{F_\alpha\}(1 \leqslant \alpha \leqslant q)$ une base de cet idéal $\mathscr{I}_R(V)$ (donc aussi de $\mathscr{I}(V)$). Pour $x \in \mathfrak{R}^n$, la relation $x \in \mathscr{F}_\nu(V)$ équivaut à : $v(F_\alpha(x)) \geqslant \nu$ pour tout α. Or si $x_i = (x_i^{(0)}, \ldots, x_i^{(\nu)}, \ldots)$ sont les coordonnées de x $(1 \leqslant i \leqslant n)$, cette relation équivaut elle-même à un nombre fini de relations algébriques, à coefficients dans k^0, entre les $x_i^{(\nu')}$ $(0 \leqslant \nu' \leqslant \nu,\ 1 \leqslant i \leqslant n)$, c'est-à-dire entre les coordonnées du point x^ν. Donc, pour $\mu \geqslant \nu$, l'ensemble $\mathscr{F}_\nu^\mu = \rho^\mu(\mathscr{F}_\nu(V))$ est un sous-ensemble k^0-fermé de $\mathbf{S}^0_{n(\mu+1)}$. De plus, $\mathscr{F}_\nu^\mu$ est un sous-ensemble k^0-constructible de $\mathbf{S}^0_{n(\mu+1)}$, pour tout couple (μ, ν) (puisqu'on a, pour $\mu' \leqslant \mu$, $\mathscr{F}_\nu^{\mu'} = \theta^{\mu'\mu}(\mathscr{F}_\nu^\mu)$).

D'autre part, pour $\mu \geqslant s_0 = s_0(V)$ (cf. n° 19), on a $V_\mathfrak{R}^\mu = \mathscr{F}^\mu_{\mu+s_0}(V)$. En effet, l'inclusion $V_\mathfrak{R}^\mu \subset \mathscr{F}^\mu_{\mu+s_0}(V)$ est triviale, tandis que l'inclusion $\mathscr{F}^\mu_{\mu+s_0}(V) \subset V_\mathfrak{R}^\mu$ est une traduction de l'énoncé de la proposition 20 du n° 19. Donc $V_\mathfrak{R}^\mu$ est bien un sous-ensemble constructible de $\mathbf{S}^0_{n(\mu+1)}$). Il en est de même de $V_\mathfrak{R}^{\mu'}$ pour $\mu' \leqslant s_0$, puisqu'on a, pour $\mu' \leqslant \mu$, $V_\mathfrak{R}^{\mu'} = \theta^{\mu'\mu}(V_\mathfrak{R}^\mu)$. C.Q.F.D.

Remarque. — Il serait souhaitable de s'affranchir de l'hypothèse (probablement superflue) que V est sans point multiple, dans la dernière partie de l'énoncé.

22. (V, p)-provariétés.

Soit toujours V une sous-variété de $\mathbf{S}_n$, définie sur k, de dimension r. Soit k_1^0 un sous-corps de $\mathfrak{k}^0$, contenant k^0. On appellera (V, p)-*provariété* définie sur k_1^0 (resp. (V, p, k_1^0)-*provariété*) toute sous-provariété X, définie sur k_1^0 (resp. toute sous-k_1^0-provariété X) de la provariété $\mathfrak{R}^n$, vérifiant les deux conditions suivantes :

(*) Tout point générique x de X sur k_1^0 appartient à V, et est simple sur V.

(**) Si x est un point générique de V sur k_1^0, il existe un voisinage p-adique de x dans $V_\mathfrak{R}$ qui est contenu dans X.

Remarques. — *a)* Toute spécialisation sur k^0 d'un point de $V_\mathfrak{R}$ est un point de $V_\mathfrak{R}$; donc, on a $X \subset V$. Mais on n'a pas nécessairement $X^\mu = \overline{\rho}^\mu(X) \subset V_\mathfrak{R}^\mu$.

b) D'après leur définition, les entiers $l(x)$ et $m(x)$ ne dépendent que de X. Nous les désignerons respectivement par $l(X) = l(X, V)$ et $m(X) = m(X, V)$.

c) La condition (**) équivaut à l'existence d'une boule p-adique de $V_\mathfrak{R}$, de centre x, contenue dans X. Autrement dit, cette condition équivaut à l'existence d'un entier μ_0 tel que, en posant $x^{\mu_0} = \rho^{\mu_0}(x)$, on ait $(\rho_V^{\mu_0})^{-1}(x^{\mu_0}) \subset X$.

Si μ_0 est un tel entier, et si, de plus, on a $\mu_0 \geqslant m(X)$, on dira que X est d'*indice* μ_0 (noter que, si X est d'indice μ_0, X est aussi d'indice μ_0', pour tout $\mu_0' \geqslant \mu_0$).

Il résulte des définitions que X est la limite projective de la suite

$$X^0 \leftarrow X^1 \leftarrow \ldots \leftarrow X^\mu \leftarrow \ldots$$

où, pour tout μ, $X^\mu = \overline{\rho}^\mu(X)$ est la variété, définie sur k_1^0 (resp. la k_1^0-variété) lieu du point $x^\mu = \rho^\mu(x)$ sur k_1^0, et où les flèches représentent les morphismes induits par les projections θ^μ.

La condition (**) signifie encore que, si $x_i = (x_i^{(0)}, \ldots, x_i^{(\mu)}, \ldots)$ $(1 \leqslant i \leqslant n)$ sont les coordonnées de x, les coefficients $x_i^{(\mu)}$ obtenus pour tous les couples d'indices (i, μ) possibles $(1 \leqslant i \leqslant n, \mu \geqslant 0)$ ne sont liés que par un nombre fini de relations algébriques à coefficients dans k_1^0, outre celles exprimant l'appartenance $x \in V$ (à savoir les relations exprimant l'appartenance $x^{\mu_0} \in X^{\mu_0}$).

d) La condition (**) implique la suivante :

(***) Il existe un entier μ_0 tel que, pour tout $\mu \geqslant \mu_0$, et pour x^μ générique de X^μ sur k_1^0, on ait $(\theta_V^\mu)^{-1}(x^\mu) \subset X^{\mu+1}$.

On peut, en effet, prendre pour μ_0 le même entier que dans *c)*. En particulier, si X est d'indice μ_0, la variété linéaire $L^\mu(x^\mu)$ est contenue dans $X^{\mu+1}$, pour tout $\mu \geqslant \mu_0$. On en déduit que, pour qu'un point $x^{\mu+1}$ soit générique de $X^{\mu+1}$ sur k_1^0, il faut et il suffit que le point $x^\mu = \theta^\mu(x^{\mu+1})$ soit générique de X^μ sur k_1^0 et que $x^{\mu+1}$ soit générique de $L^\mu(x^\mu)$ sur $k_1^0(x^\mu)$. Donc $X^{\mu+1}$ est déterminée par X^μ; par récurrence sur μ, on en déduit que X est déterminée par X^μ.

Nous montrerons, au numéro suivant (prop. 23) qu'on peut inversement « relever » une sous-k_1^0-variété X^μ de $\mathbf{S}_{n(\mu+1)}$, génériquement contenue dans $V_{\mathfrak{R}}^\mu$, à une $(V, \mathfrak{p}, k^0)$-provariété, pourvu que le symbole $L^\mu(x^\mu)$ soit défini en un point générique x^μ de X^μ sur k_1^0. Nous montrerons, en même temps, qu'on peut substituer la condition (***) à la condition (**) dans la définition précédente.

e) Tout point générique sur k_1^0 d'une $(V, \mathfrak{p}, k_1^0)$-provariété X est aussi un point générique de V sur $k_1 = (k_1^0)^\#$. En effet, supposons X d'indice μ_0 et soit μ un entier $\geqslant \mu_0$. On peut trouver deux points génériques x et y de X sur k_1^0, tels que $x^\mu = y^\mu$, et que $y^{\mu+1}$ soit un point générique de la variété linéaire $L^\mu(x^\mu)$ sur $k'^0 = k_1^0(x)$. Considérons le point $z = \varphi_{\mu x}(y)$, où $\varphi_{\mu x}$ est la transformation de $\mathbf{S}_n$ introduite au n° 18. On a $z \in V_{\mathfrak{R}}$, et $z^0 = \rho(z)$ est générique sur k'^0 d'une variété linéaire de dimension r. Donc le degré de transcendance de $k'^0(z^0)$ sur k'^0 est r. Donc, si on pose $k' = (k'^0)^\#$ le degré de transcendance de $k'(z) = k'(y)$ sur k' est $\geqslant r$ (donc est égal à r). Donc y est générique de V sur k' et, *a fortiori*, sur k_1. Ceci prouve notre assertion, compte tenu de la remarque *a)*.

Nous dirons qu'une $(V, \mathfrak{p}, k_1^0)$-provariété X est *simple* lorsqu'un point (donc tout point) générique x de X sur k_1^0 est simple (mod. $\mathfrak{p}$) sur V ou, ce qui revient au même, lorsque la k_1^0-variété réduite $X^0 = \overline{\rho}(X)$ est génériquement simple sur $V^0 = \rho(V)$. Pour que X soit simple, il faut et il suffit qu'on ait $l(X) = 0$, ou encore qu'on ait $m(X) = 0$.

23. (V, $\mathfrak{p}$)-ensembles.

Soient encore V une variété affine $(\subset \mathbf{S}_n)$, définie sur k, de dimension r, et k_1^0 un sous-corps de $\mathfrak{k}^0$, contenant k^0. Nous appellerons $(V, \mathfrak{p})$-*ensemble* (resp. $(V, \mathfrak{p}, k_1^0)$-*ensemble*) tout sous-ensemble S de $V_{\mathfrak{R}}$ de la forme $S = (\rho_V^{\mu_0})^{-1}(S^{\mu_0})$ où S^{μ_0} est un sous-ensemble

constructible (resp. k_1^0-constructible) quelconque de l'espace affine $\mathbf{S}^0_{n(\mu+1)}$. Nous dirons de plus que S est d'*indice* μ_0, et que S est le (V, p)-ensemble (resp. le (V, p, k_1^0)-ensemble) *obtenu en relevant* S^{μ_0}. Nous poserons $S=(S^{\mu_0})^{\#}$. Il est clair que tout (V, p)-ensemble d'indice μ_0 est aussi d'indice μ_0', pour tout entier $\mu_0' \geqslant \mu_0$.

Une autre forme de la définition d'un (V, p, k^0)-ensemble est la suivante : un tel ensemble est l'ensemble des points $x \in V_{\mathfrak{R}}$, de coordonnées $x_i=(x_i^{(0)}, \ldots, x_i^{(\mu)}, \ldots)$ $(1 \leqslant i \leqslant n)$, tels que les $x_i^{(\mu)}$ obtenus pour toutes les valeurs possibles du couple (i, μ) $(1 \leqslant i \leqslant n, \mu \geqslant 0)$ vérifient un nombre fini de relations de l'une des formes $P_\alpha(\ldots)=0$ ou $Q_\beta(\ldots) \neq 0$, où les P_α et les Q_β sont des polynômes à coefficients dans k_1^0.

Dans le cas particulier où V est sans point multiple, on a montré (n° 20, prop. 22) que, pour tout $\mu \geqslant 0$, l'ensemble $V^\mu_{\mathfrak{R}}=\rho^\mu(V_{\mathfrak{R}})$ est constructible. Soit $S=(\rho_V^{\mu_0})^{-1}(S^{\mu_0})$ un (V, p)-ensemble. Alors, *pour tout* $\mu \geqslant 0$ *l'ensemble* $S^\mu=\rho^\mu(S)$ *est constructible.* En effet, on a, pour $\mu \leqslant \mu_0$, $S^\mu=\theta^{\mu\mu_0}(S^{\mu_0} \cap V^{\mu_0}_{\mathfrak{R}})$, et, pour $\mu \geqslant \mu_0$, $S^\mu=((\theta^{\mu_0\mu})^{-1}(S^{\mu_0} \cap V^{\mu_0}_{\mathfrak{R}})) \cap V^\mu_{\mathfrak{R}}$.

On dira qu'un (V, p)-ensemble (resp. un (V, p, k^0)-ensemble) est *irréductible* (resp. *k^0-irréductible*) si, pour tout $\mu \geqslant 0$, S^μ est un ensemble constructible irréductible (resp. k^0-irréductible), c'est-à-dire si S^μ est un ouvert (resp. un k^0-ouvert) d'une sous-variété (resp. d'une sous-k_1^0-variété) X^μ de l'espace $\mathbf{S}^0_{n(\mu+1)}$. Dans ce cas, la suite (X^μ) définit une provariété (resp. une k^0-provariété) X, qu'on appellera *adhérence* de S, et qu'on notera adh S.

En vue de l'énoncé qui suit, introduisons encore une notation. Soit x^μ un point de $V^\mu_{\mathfrak{R}}=\rho^\mu(V_{\mathfrak{R}})$ vérifiant la condition de la proposition 21, i.e. un point de la forme $\rho^\mu(x)$, avec $x \in V_{\mathfrak{R}}$, simple sur V, et $m(x) \leqslant \mu$; alors, pour tout autre point $x' \in V_{\mathfrak{R}}$ tel que $x^\mu=\rho^\mu(x')$, le point $\rho_{\mu+1,x}(x')$ est entier, et simple (mod. p); donc x' est simple sur V, et on a $m(x')=m(x)$. L'entier $m(x)$ ne dépend donc que de x^μ. Nous le désignerons par $m^\mu(x^\mu)$.

Proposition 23. — Soit V *une variété affine, définie sur k, et soit* μ *un entier* $\geqslant 0$. *Soit* X^μ *une sous-k^0-variété de* $\mathbf{S}_{n(\mu+1)}$, *génériquement contenue dans* $V^\mu_{\mathfrak{R}}$, *i.e. telle qu'un point générique* x^μ *de* X^μ *sur* k^0 *appartienne à* $V^\mu_{\mathfrak{R}}$. *Supposons que le symbole* $m^\mu(x^\mu)$ *est défini (ceci est toujours le cas, en particulier, si* V *est sans point multiple, et si on a pris* $\mu \geqslant m_0(V)$). *Alors :*

(i) *Il existe une et une seule* (V, p, k^0)*-provariété* X *d'indice* μ, *telle que* $X^\mu=\bar{\rho}^\mu(X)$. *On a* $m(X)=m=m^\mu(x^\mu)$.

(ii) *Il existe un k^0-ouvert* S^μ *de* X^μ, *contenu dans* $V^\mu_{\mathfrak{R}}$, *tel que le* (V, p, k^0)*-ensemble* $S=(S^\mu)^{\#}$ *soit irréductible, d'adhérence* X, *contenu dans l'ensemble* $\mathscr{S}(V)$ *des points simples sur* V, *et tel qu'on ait* $m(u) \leqslant \mu$ *pour tout* $u \in S$.

Démonstration. — D'après la proposition 21, l'ensemble $L^\mu(x^\mu)=(\theta_V^\mu)^{-1}(x^\mu)$ est une variété linéaire, de dimension $r=\dim V$, définie sur $k^0(x^\mu)$. Si $x^{\mu+1}$ est un point générique de $L^\mu(x^\mu)$ sur $k^0(x^\mu)$, ce point appartient à $V^{\mu+1}_{\mathfrak{R}}$; on a $x^\mu=\theta^\mu(x^{\mu+1})$, et $m^\mu(x^\mu)=m^{\mu+1}(x^{\mu+1})$. Par récurrence sur ν $(\nu \geqslant \mu)$, on peut donc construire une suite $(x^\mu, x^{\mu+1}, \ldots, x^\nu, \ldots)$, avec $x^\nu \in V^\nu_{\mathfrak{R}}$, de façon que, pour tout $\nu \geqslant \mu$, le point $x^{\nu+1}$ soit générique sur $k^0(x^\nu)$ de la variété linéaire $L^\nu(x^\nu)$. Pour $\mu' \leqslant \mu$, posons d'autre part $x^{\mu'}=\theta^{\mu'\mu}(x^\mu)$, et notons X la sous-$k^0$-provariété de $\mathfrak{R}^n$ lieu sur k^0 du point x défini par la suite $x^0, \ldots, x^\nu, \ldots$ Toute (V, p, k^0)-provariété qui vérifie la condition (i)

de la proposition coïncide nécessairement avec X, d'après la remarque *d)* du n° 22.

Il nous suffit de montrer l'existence d'un k^0-ouvert S^μ de X^μ tel que $S=(S^\mu)^\#$ ait pour adhérence X, et vérifie les conditions énumérées dans (ii). Ceci entraînera en même temps que X vérifie la condition (**) du n° 22, donc que X est une (V, $\mathfrak{p}$)-provariété.

On a, d'après l'hypothèse, $\mu \geqslant m(x)$. Donc l'origine est un point simple sur le cycle $V^0_{\mu x}$ réduit (mod. $\mathfrak{p}$) de la variété $V_{\mu x}=\varphi_{\mu x}(V)$. Considérons le point $y=\rho^\mu_*(x)$, obtenu en tronquant à l'ordre μ les suites de coefficients qui définissent chacune des coordonnées de x. L'application $\varphi_{\mu x}\circ\varphi_{\mu y}^{-1}$ étant une translation à coordonnées dans $\mathfrak{R}$, donc un $\mathfrak{R}$-isomorphisme de $\mathbf{S}_n$, l'origine est aussi un point simple sur le cycle réduit (mod. $\mathfrak{p}$) de $V_{\mu y}=\varphi_{\mu y}(V)$. De plus la variété $V_{\mu y}$ est définie sur $k(y)$.

On peut trouver des polynômes G_j $(1\leqslant j\leqslant n-r)$, à coefficients dans l'anneau $R_y=\mathfrak{R}\cap k(y)$ des entiers de $k(y)$, qui s'annulent sur $V_{\mu y}$, et tels que les $\mathfrak{p}$-différentielles à l'origine $(dG_1)^0_0, \ldots, (dG_{n-r})^0_0, (dt)^0_0$ soient linéairement indépendantes. Écrivons ces polynômes sous la forme

$$G_j(X)=a_{j0}+\Sigma_{i=1}^n a_{ji}X_i+\Sigma_{h=1}^m a'_{jh}M_{jh} \qquad (1\leqslant j\leqslant n-r)$$

où les M_{jh} sont des monômes de degré $\geqslant 2$, et où les a_{ji} $(0\leqslant i\leqslant n)$, a'_{jh} $(1\leqslant h\leqslant m)$ appartiennent à R_y. Si, pour tout couple (i,j), on pose $a^0_{ji}=\rho(a_{ji})$, on a alors $a^0_{j0}=0$ pour tout j, et la matrice (a^0_{ji}) est de rang $(n-r)$.

Puisque les a_{ji}, a'_{jh} appartiennent à R_y, ils sont de la forme $a_{ji}=P_{ji}(y)/Q(y)$ et $a'_{jh}=P'_{jh}(y)/Q(y)$, où P_{ji}, P'_{jh}, Q sont des polynômes à coefficients dans R, tels que, en posant $v(Q(y))=\sigma$, on ait $v(P_{ji}(y))\geqslant\sigma$, et $v(P'_{jh}(y))\geqslant\sigma$ quels que soient i, j, h. De plus, l'un des déterminants $D(y)$ de la matrice $(a_{ji})=(P_{ji}(y)/Q(y))$ est un élément inversible de R (i.e. tel que $v(D(y))=0$).

Or les coordonnées de y sont $y_i=(x_i^{(0)}, \ldots, x_i^{(\mu)}, 0, \ldots, 0, \ldots)$. Les coefficients de chacun des éléments $Q(y)$, $P_{ji}(y)$, $P'_{jh}(y)$ de $\mathfrak{R}$ s'expriment (cf. n° 6) par des polynômes à coefficients dans k^0 en fonction des $x_i^{(\mu')}$ $(1\leqslant i\leqslant n,\ 0\leqslant\mu'\leqslant\mu)$ i.e. en fonction des coordonnées de x^μ. On peut donc trouver un ouvert S^μ de X^μ, tel que, pour tout point $w^\mu\in S^\mu$, et en désignant par z le point correspondant $z=\xi^\mu(w^\mu)$ de $\mathfrak{R}^n$, on ait encore $v(Q(z))=\sigma$, et $v(D(z))=0$. Puisque z est une spécialisation de y sur k^0, on a, d'autre part, $v(P_{ji}(z))\geqslant\sigma$, et $v(P'_{jh}(z))\geqslant\sigma$ quels que soient i, j, h.

Donc les éléments $b_{ji}=P_{ji}(z)/Q(z)$, et $b'_{jh}=P'_{jh}(z)/Q(z)$ du corps $k(z)$ appartiennent à l'anneau $R_z=\mathfrak{R}\cap k(z)$ des entiers de ce corps. Les polynômes

$$H_j(X)=b_{j0}+\Sigma_i b_{ji}X_i+\Sigma_h b'_{jh}M_h$$

s'annulent sur $V_{\mu z}=\varphi_{\mu z}(V)$, et sont tels que les $\mathfrak{p}$-différentielles à l'origine $(dH_1)^0_0, \ldots, (dH_{n-r})^0_0, (dt)^0_0$ soient linéairement indépendantes : en posant

$$b^0_{ji}=\rho(b_{ji}) \quad (0\leqslant i\leqslant n,\ 1\leqslant j\leqslant n-r),$$

on a, en effet, $b^0_{j0}=0$ pour tout j, et la matrice (b^0_{ji}) est de rang $n-r$. Donc l'origine est un point simple sur $V^0_{\mu z}=\rho(V_{\mu z})$; donc on a $w^\mu\in V^\mu_{\mathfrak{R}}$, et $m^\mu(w^\mu)\leqslant\mu$.

Si on pose $S=(S^{\mu})^{\sharp}$, on a de plus $S\subset\mathscr{S}(V)$, et $m(u)\leqslant\mu$ pour tout $u\in S$. Nous allons montrer, par récurrence sur μ', que, pour tout entier $\mu'\geqslant\mu$, $S^{\mu'}=\rho^{\mu'}(S)$ est un ouvert de $X^{\mu'}$.

Cette propriété est vraie pour $\mu'=\mu$; supposons-la vérifiée pour μ', et montrons qu'elle l'est pour $\mu'+1$. Soit en effet $w^{\mu'}$ un point de $S^{\mu'}$ tel que $\theta^{\mu\mu'}(w^{\mu'})=w^{\mu}$, où w^{μ} est le point de S^{μ} considéré plus haut. Posons $z'=\xi^{\mu'}(w^{\mu'})$. D'après l'hypothèse de récurrence, on a $w^{\mu'}\in X^{\mu'}=\overline{\rho}^{\mu'}(X)$. Puisqu'on a $w^{\mu'}\in V^{\mu'}_{\mathfrak{R}}$, et $\mu'\geqslant\mu\geqslant m(x)$, le cycle réduit $V^{0}_{\mu'+1,z'}$ de la variété $\varphi_{\mu'+1,z'}(V)$ est une variété linéaire. Si $\overline{z}'$ est le point de $\mathfrak{R}^n$ tel qu'on ait $z'=z+t^{\mu+1}\overline{z}'$, les polynômes $\overline{H}'_j(X)=H_j(\overline{z}'+t^{\mu'-\mu}X)$ s'annulent sur $V_{\mu'+1,z'}$. Soit ν le plus grand entier tel que le polynôme $\overline{H}_j(X)=\overline{H}'_j(X)t^{-\nu}$ soit à coefficients dans $\mathfrak{R}$. Le polynôme réduit $\overline{H}^0_j=\rho(\overline{H}_j)$ s'annule sur $V^0_{\mu'+1,z'}$. On ne peut avoir $\nu<\mu'-\mu$, car, dans ce cas, $\overline{H}^0_j$ serait une constante non nulle. On a donc $v(H_j(\overline{z}'))\geqslant\mu'-\mu$. Puisque la matrice (b^0_{ji}) est de rang $n-r$, on a donc $\nu=\mu'-\mu$, et $\overline{H}^0_j(X)=\overline{b}^0_{j0}+\Sigma_{i=1}^n b^0_{ji}X_i$, où l'on note $\overline{b}^0_{j0}$ l'élément de $\mathfrak{k}^0$ réduit (mod. $\mathfrak{p}$) de $\overline{b}_{j0}=H_j(\overline{z}')t^{\mu-\mu'}$.

Donc la variété linéaire $V^0_{\mu'+1,z'}=L^{\mu'}_0(w^{\mu'})$ est définie par le système d'équations

$$\overline{b}^0_{j0}+\Sigma_{i=1}^n b^0_{ji}X_i=0 \qquad (1\leqslant j\leqslant n-r)$$

De même, si on pose $y'=\rho^{\mu'}_*(x)=\xi^{\mu'}(x^{\mu'})$, et si $\overline{y}'$ est le point de $\mathfrak{R}^n$ défini par $y'=y+t^{\mu+1}\overline{y}'$, on a, pour tout j, $\overline{a}_{j0}=G_j(y')t^{\mu'-\mu}\in\mathfrak{R}^n$, et, en posant $\overline{a}^0_{j0}=\rho(\overline{a}_{j0})$, la variété linéaire $L^{\mu'}_0(x^{\mu'})$ est définie par le système d'équations

$$\overline{a}^0_{j0}+\Sigma_{i=1}^n a^0_{ji}X_i=0 \qquad (1\leqslant j\leqslant n-r)$$

En comparant les expressions des coefficients $\overline{b}_{j0}$, b_{ji} $(1\leqslant i\leqslant n)$ à celles de $\overline{a}_{j0}$, a_{ji} respectivement, on en déduit que la variété linéaire $L^{\mu'}(w^{\mu'})$ est l'unique spécialisation de la variété $L^{\mu'}(x^{\mu'})$ compatible avec la spécialisation $w^{\mu'}$ de $x^{\mu'}$. Autrement dit $L^{\mu'}(w^{\mu'})=(\theta^{\mu'}_V)^{-1}(w^{\mu'})$ coïncide avec l'image inverse de $w^{\mu'}$ par le morphisme $\theta^{\mu'}\,|\,X^{\mu'+1}$ induit par $\theta^{\mu'}$. Puisque $S^{\mu'}$ est un ouvert de $X^{\mu'}$, $S^{\mu'+1}=(\rho^{\mu'}_V)^{-1}(S^{\mu'})$ est un ouvert de $X^{\mu'+1}$. C.Q.F.D.

On dira que la $(V, \mathfrak{p}, k^0)$-provariété X vérifiant la condition (i) de la proposition est la $(V, \mathfrak{p}, k^0)$-*provariété obtenue en relevant génériquement* X^{μ}; on la désignera par $(X^{\mu})^{\sharp}_g$.

Remarques. — *a)* Soit X une sous-k^0_1-provariété de $\mathfrak{R}^n$, vérifiant les conditions (*) et (***) (cf. n° 22, remarque *d)*). D'après la construction utilisée dans la démonstration précédente, on a, pour $\mu_1\geqslant\sup(\mu_0, m(X))$, $X=(X^{\mu_1})^{\sharp}_g$, et, par suite, X est une $(V, \mathfrak{p}, k^0_1)$-provariété d'indice μ_1. On peut donc bien, comme on l'a annoncé, substituer (***) à (**) dans la définition des $(V, \mathfrak{p})$-provariétés.

b) Soit X une $(V, \mathfrak{p}, k^0)$-provariété, et exprimons-la sous la forme $X=(X^{\mu})^{\sharp}_g$. Soient $X^{(\mu)}_i$ les composantes irréductibles (au sens absolu) de X^{μ}. Alors X est la réunion des $(V, \mathfrak{p})$-provariétés $X_i=(X^{(\mu)}_i)^{\sharp}_g$. Ces provariétés ne dépendent pas du choix de μ, et sont mutuellement conjuguées sur k^0. On les appellera les *composantes* de X.

c) Dans le cas particulier où $\lambda=\mu=0$, c'est-à-dire où X^0 est une sous-variété

de $\rho_e(V)$, génériquement simple sur V^0, le raisonnement précédent montre qu'on peut prendre pour S^0 n'importe quel ouvert de X^0 contenu dans l'ensemble $\mathscr{S}(V^0)$ des points simples sur V^0.

24. Image d'une (V, p)-provariété, ou d'un (V, p)-ensemble, par un f-morphisme.

Pour tout entier $\sigma \geqslant 0$, rappelons qu'on a désigné, au n° 6, par F_σ^0 l'automorphisme de k^0 ainsi défini : F_σ^0 est l'identité dans le cas d'égales caractéristiques, et est la puissance $q^*(\sigma)$-ième de l'automorphisme de Frobenius de k^0 (où $q^*(\sigma)$ est le plus petit entier $\geqslant \sigma/e$) dans le cas d'inégales caractéristiques.

Proposition 24. — *Soient* V *et* W *deux variétés affines, définies sur* k ($V \subset \mathbf{S}_m$, $W \subset \mathbf{S}_n$), *et soit* $\varphi : V \to W$ *une application rationnelle, définie sur* k. *Soit* X *une* $(V, \mathfrak{p}, k^0)$*-provariété d'indice* μ_0 *et soit* x *un point générique de* X *sur* k^0. *Soient* P_j $(1 \leqslant j \leqslant n)$ *et* Q *des éléments de* $R[X_1, \ldots . X_m]$ *tels que les coordonnées* φ_j *de* φ *soient induites respectivement par les quotients* P_j/Q, *et qu'on ait* $Q(x) \neq 0$. *Posons* $v(Q(x)) = \sigma$. *Supposons que le point* $y = \varphi(x)$ *appartient à* $W_{\mathfrak{R}}$. *Soit* Y *la sous-*k^0*-provariété de* $\mathfrak{R}^n$ *lieu de* y *sur* k^0. *Alors*

(i) *Pour tout* $\nu \geqslant 0$, *le point* $y^\nu = \rho^\nu(y)$ *est uniquement déterminé par le point* $x^{\sigma+\nu} = \rho^{\sigma+\nu}(x)$, *et le point* $\widetilde{y}^\nu = F_\sigma^0(y^\nu)$ *est rationnel sur* $k^0(x^{\sigma+\nu})$ (*on a donc le diagramme commutatif suivant d'applications rationnelles, définies sur* k^0, *génériquement surjectives* :

$$\begin{array}{ccccccc} X^\sigma & \leftarrow & X^{\sigma+1} & \leftarrow \ \ldots \ \leftarrow & X^{\sigma+\nu} & \leftarrow & \ldots \\ \downarrow \varphi^{0\sigma} & & \downarrow \varphi^{1,\sigma+1} & & \downarrow \varphi^{\nu,\sigma+\nu} & & \\ Y^0 & \leftarrow & Y^1 & \leftarrow \ \ldots \ \leftarrow & Y^\nu & \leftarrow & \ldots \end{array}$$

où, pour tout $\nu \geqslant 0$, *on note* Y^ν *le lieu de* y^ν *sur* k^0, *et* $\varphi^{\nu,\sigma+\nu}$ *l'application rationnelle* $X^{\sigma+\nu} \to Y^\nu$ *telle que* $\widetilde{y}^\nu = \varphi^{\nu,\sigma+\nu}(x^{\sigma+\nu})$.

(ii) *Il existe un* $(V, \mathfrak{p}, k^0)$*-ensemble* S, *irréductible, d'adhérence* X, *contenu dans* $\mathscr{S}(V)$, *d'indice* $\mu_1 = \sup(\mu_0, \sigma)$, *tel que* φ *soit morphique en tout point de* S, *et que, pour tout* $\nu \geqslant 0$, $\varphi^{\nu,\sigma+\nu}$ *soit morphique en tout point de l'ouvert* $S^{\sigma+\nu} = \rho^{\sigma+\nu}(S)$ *de* $X^{\sigma+\nu}$ (*on a donc un diagramme commutatif de* morphismes, *définis sur* k^0, *déduit du précédent en remplaçant* $X^{\sigma+\nu}$ *par* $S^{\sigma+\nu}$ *et* $\varphi^{\nu,\sigma+\nu}$ *par sa restriction à* $S^{\sigma+\nu}$; *on a aussi, pour tout* $u \in S$, *la relation* $\varphi^{\nu,\sigma+\nu}(\rho^{\sigma+\nu}(\mu)) = F_\sigma^0(\rho^\nu(\varphi(\mu)))$.

Démonstration. — On a $y_j = P_j(x)/Q(x)$, avec $v(Q(x)) = \sigma$. Puisqu'on suppose $y \in W_{\mathfrak{R}}$, on a, pour tout j, $v(P_j(x)) \geqslant \sigma$. Si on pose

$$Q(x) = (w^{(0)}, \ldots, w^{(\nu)}, \ldots)$$
$$P_j(x) = (v_j^{(0)}, \ldots, v_j^{(\nu)}, \ldots) \qquad (1 \leqslant j \leqslant n),$$

on a donc $v_j^{(\nu')} = w^{(\nu')} = 0$ pour tout $\nu' \leqslant \sigma$, et $w^{(\sigma)} \neq 0$. D'après la formule 8 du n° 6, on a donc, pour tout $\nu \geqslant 0$, une relation de la forme

$$F_\sigma^0(y_j^{(\nu)}) = \widetilde{y}_j^{(\nu)} = (w^{(\sigma)})^{-(\nu+1)} \overline{Q}_\nu(v_j^{(\sigma)}, w^{(\sigma)}, \ldots, v_j^{(\sigma+\nu)}, w^{(\sigma+\nu)}),$$

où $\overline{Q}_\nu$ est un polynôme à coefficients dans k^0.

D'autre part, $w^{(\sigma+\nu)}$, et les $v_j^{(\sigma+\nu)}$ $(1 \leqslant j \leqslant n)$ s'expriment en fonction des coordonnées de $x^{\sigma+\nu}$ par des polynômes à coefficients dans k^0. Donc, on a, pour tout $\nu \geqslant 0$,

$$\widetilde{y}_j^{(\nu)} = (R_0(x^\sigma))^{-(\nu+1)} R_j^{(\nu)}(x^{(\sigma+\nu)}) \qquad (1 \leqslant j \leqslant n) \tag{29}$$

où R_0 et les $R_j^{(\nu)}$ sont des polynômes à coefficients dans k^0. L'assertion (i) est donc démontrée.

De plus, d'après la formule (29), pour $\nu \geqslant 0$, l'application $\varphi^{\nu,\sigma+\nu}$ est morphique en tout point de $X^{\sigma+\nu}$ qui appartient au k^0-ouvert $U^{\sigma+\nu}$ de $X^{\sigma+\nu}$ défini par $R_0(\theta^{\sigma,\sigma+\nu}(x^{\sigma+\nu})) \neq 0$. Donc, si on pose $\mu_1 = \sup(\mu_0, \sigma)$, on peut, d'après la proposition 23, et puisqu'on a $\mu_1 \geqslant \mu_0 \geqslant m(X)$, trouver un k^0-ouvert S^{μ_1} de X^{μ_1}, contenu dans $V_{\mathfrak{R}}^{\mu_1} \cap U^{\mu_1}$, tel que le $(V, \mathfrak{p}, k^0)$-ensemble $S = (S^{\mu_1})^{\#}$ soit irréductible, d'adhérence X, contenu dans $\mathscr{S}(V)$. L'application φ est bien alors morphique en tout point de S; de plus, on a, pour tout $\nu \geqslant 0$, $S^{\sigma+\nu} = \rho^{\sigma+\nu}(S) \subset U^{\sigma+\nu}$, et $\varphi^{\nu,\sigma+\nu}$ est donc bien morphique en tout point de $S^{\sigma+\nu}$.

Toutes les fois qu'un entier σ, une application $\varphi : V \to W$ et une $(V, \mathfrak{p})$-provariété X (resp. un $(V, \mathfrak{p}, k^0)$-ensemble irréductible S) vérifient les propriétés énoncées dans la proposition précédente, nous dirons que φ est *génériquement promorphique d'indice* σ *sur* X (resp. *promorphique d'indice* σ *sur* S). La sous-provariété Y de $\mathfrak{R}^n$ sera notée $Y = \varphi_g(X)$.

Dans le cas où φ est génériquement $\mathfrak{p}$-morphique sur $X^0 = \overline{\rho}(X)$ (i.e. $\mathfrak{p}$-morphique en $x^0 = \rho(x)$), on peut prendre $\sigma = 0$. L'application $\varphi^{\nu\nu} : X^\nu \to Y^\nu$ est alors $\mathfrak{p}$-morphique en tout point $u^\nu \in X^\nu$ tel que φ soit $\mathfrak{p}$-morphique en $u^0 = \theta^{0\nu}(u^\nu)$. Lorsque φ est un $\mathfrak{R}$-morphisme, $\varphi^{\nu\nu}$ est un morphisme pour tout ν. Si, de plus, φ est génériquement $\mathfrak{p}$-isomorphique sur X^0, il résulte de la proposition précédente que la provariété $Y = \varphi_g(X)$ est une $(W, \mathfrak{p}, k^0)$-provariété, de même indice que X : on le voit en effet en remarquant que, pour x générique de X sur k^0, et pour $x' \in V_{\mathfrak{R}}$ quelconque, on a $(\varphi(x), \varphi(x'))_{\mathfrak{p}} = (x, x')_{\mathfrak{p}}$.

De même, si, avec les notations de la proposition 24, φ est $\mathfrak{p}$-morphique en tout point de l'ensemble $S^0 = \rho(S)$, l'application $\varphi^{\mu\mu}$ est un morphisme pour tout $\mu \geqslant 0$. Si, de plus, φ est $\mathfrak{p}$-isomorphique en tout point de S^0, l'application $\varphi^{\mu\mu}$ est un isomorphisme pour tout μ, et l'image $T = \varphi(S)$ est un $(W, \mathfrak{p}, k^0)$-ensemble de même indice que S.

Ces propriétés seront généralisées un peu plus loin (th. 1 et 2); elles sont suffisantes pour permettre dès maintenant d'étendre aux p-variétés quelconques les résultats déjà obtenus et la terminologie relatifs au cas des variétés affines.

Soit $V = \{V_\alpha, T_{\beta\alpha}\}$ une p-variété abstraite quelconque, définie sur k, et, pour l'un des indices α, considérons une $(V_\alpha, \mathfrak{p})$-provariété X_α, définie sur un sous-corps k_1^0 de $\mathfrak{k}^0$ contenant k^0. Soit x_α un point générique de X sur k_1^0, et soit x le point de $V_{\mathfrak{R}}$ représenté par x_α. Comme x_α est un point générique de V_α sur k (cf. n° 22, remarque *e)*), x est représenté dans V_β pour tout β, et on a $x_\beta = T_{\beta\alpha}(x_\alpha)$. D'après ce qui précède, $T_{\beta\alpha}$ induit, pour tout $\mu \geqslant 0$, une application birationnelle $T_{\beta\alpha}^{\mu\mu} : X_\alpha^\mu \to X_\beta^\mu$, définie sur k_1^0, et, pour tout couple $(u_\alpha^\mu, u_\beta^\mu)$ appartenant à son graphe, cette application est isomorphique en u_α^μ, de valeur u_β^μ. Donc l'ensemble $\{X_\alpha^\mu, T_{\beta\alpha}^\mu\}$ définit, pour tout μ, une variété X^μ, sur le

corps k_1^0. On peut étendre les k_1^0-morphismes $\theta_\alpha^\mu : X_\alpha^{\mu+1} \to X_\alpha^\mu$ à des k_1^0-morphismes $\theta^\mu : X^{\mu+1} \to X^\mu$ génériquement surjectifs. On a ainsi une suite :

$$X^0 \underset{\theta^0}{\leftarrow} X^1 \underset{\theta^1}{\leftarrow} \dots \leftarrow X^\mu \underset{\theta^\mu}{\leftarrow} \dots$$

à laquelle est associée une provariété X. Nous dirons que X est une (V, p)-*provariété*, et, plus précisément, que X est la (V, p)-provariété *représentée par les* X_α. Nous dirons aussi que X est la (V, p)-provariété *lieu de x sur* k_1^0, et que x est un *point générique de* X *sur* k_1^0. On peut de même, plus généralement, définir la notion de (V, p, k_1^0)-provariété. Toute (V, p, k_1^0)-provariété est une sous-k_1^0-provariété de $\mathbf{V}_\mathfrak{R}$, où $\mathbf{V}$ est la variété strictement non dégénérée (mod. p) dans laquelle on a plongé V (cf. les conventions adoptées au n° 4, et la remarque *c)* du n° 23).

La terminologie et les notations relatives au cas des variétés affines, introduites dans ce numéro et dans les deux précédents ((V, p)-ensemble, symbole φ_g, application promorphique d'indice σ, etc.) s'étendent d'une manière naturelle au cas des p-variétés abstraites; les propositions 23 et 24 sont encore valables pour de telles variétés (on pourrait également utiliser ici les résultats récemment obtenus par Greenberg [5], qui a traité de façon systématique les problèmes analogues relatifs à des préschémas sur l'anneau R d'un type plus général).

Remarque. — Les coordonnées $x_i^{(\sigma+\nu)}$ d'indice supérieur maximum du point $x^{\sigma+\nu}$ interviennent linéairement dans le second membre de la formule (29) de la démonstration précédente. Plus précisément, les termes qui les contiennent sont de la forme $g_i^{(\nu)}(x^\sigma)x_i^{(\sigma+\nu)}$, où les $g^{(\nu)}$ sont des fractions rationnelles à coefficients dans k^0. Donc, si $\sigma+\nu \geqslant \mu_1$, pour $u^{\sigma+\nu} \in S^{\sigma+\nu}$, et en posant $v^\nu = \varphi^{\nu,\sigma+\nu}(u^{\sigma+\nu})$, l'application $\varphi^{\nu+1,\sigma+\nu+1}$ induit une application linéaire affine $\psi^{\nu,\sigma+\nu}$: $L^{\sigma+\nu}(u^{\sigma+\nu}) \to L^\nu(v^\nu)$; cette application linéaire est déterminée, à une translation près, par le point $u^\sigma = \theta^{\sigma,\sigma+\nu}(u^{\sigma+\nu})$; en particulier, son rang ne dépend que de u^σ.

Théorème 1. — *Soient* V *et* W *deux* p*-variétés, et soit* $\varphi : V \to W$ *une application rationnelle, définie sur* k*, génériquement surjective et séparable. Soit* X *une* (V, p, k^0)*-provariété, et soit* x *un point générique de* X *sur* k^0*. Supposons que* φ *est définie en* x*, et que* $y = \varphi(x)$ *appartient à* $W_\mathfrak{R}$*. Alors* $Y = \varphi_g(X)$ *est une* (W, p, k^0)*-provariété. Supposons de plus que* X *et* Y *sont d'indices respectifs* μ *et* ν*, et que* φ *est génériquement promorphique d'indice* σ *sur* X*; posons* $\mu_1 = \sup(\mu, \sigma+\nu)$ *et* $\nu_1 = \mu_1 - \sigma = \sup(\mu - \sigma, \nu)$*. Alors il existe un* (V, p, k^0)*-ensemble irréductible* S *d'adhérence* X*, contenu dans* $\mathscr{S}(V)$*, d'indice* μ_1*, tel que* φ *soit promorphique d'indice* σ *sur* S*, et que* $T = \varphi(S)$ *soit un* (W, p, k^0)*-ensemble irréductible, d'adhérence* X*, d'indice* ν_1*, contenu dans* $\mathscr{S}(W)$.

Démonstration. — Nous allons commencer par démontrer l'existence d'un (V, p)-ensemble S_0, d'adhérence X, tel que $T_0 = \varphi(S_0)$ soit un (W, p)-ensemble.

On se ramène immédiatement au cas où V et W sont deux variétés affines, définies sur k. Supposons $V \subset \mathbf{S}_m$, et $W \subset \mathbf{S}_n$. Posons $r = \dim V$, $s = \dim W$. Soient $F_1, \dots, F_{m-r}$ des polynômes de l'anneau R[X], s'annulant sur V, et tels que les hypersurfaces $F_\alpha(X) = 0$ se coupent transversalement suivant V, i.e. tels que l'un des déterminants d'ordre $m-r$

de la matrice $M=\left(\frac{\partial F_\alpha}{\partial X_i}\right)$, par exemple $D=D(F_1, \ldots, F_{m-r})/D(X_1, \ldots, X_{m-r})$ ne s'annule pas sur V. Soient, de même, $G_1, \ldots, G_{n-s}$ des polynômes de l'anneau R[Y], s'annulant sur W, et tels que le déterminant $E=D(G_1, \ldots, G_{n-s})/D(Y_1, \ldots, Y_{n-s})$ ne s'annule pas sur W. Si, alors, on désigne par $f_j=P_j/Q$ des fonctions sur S_n induisant sur V les coordonnées φ_j de φ, la matrice $M'=\left(\frac{\partial F_\alpha}{\partial X_i}, \frac{\partial f_j}{\partial X_i}\right)$ est de rang $m-r+s$. On peut supposer, par exemple, que le déterminant

$$D'=D(F_1, \ldots, F_{m-r}, f_1, \ldots, f_s)/D(X_1, \ldots, X_{m-r+s})$$

ne s'annule pas sur V.

On désignera par V' l'intersection des hypersurfaces $F_\alpha(X)=0$ $(1\leqslant\alpha\leqslant m-r)$ et par V* la $\mathfrak{k}$-adhérence du complémentaire de V relativement à V'. De même, on désignera par W' l'intersection des hypersurfaces $G_\beta(Y)=0$ $(1\leqslant\beta\leqslant n-s)$ et par W* la $\mathfrak{k}$-adhérence du complémentaire de W relativement à W'.

A tout point $\widetilde{x}\in\mathfrak{R}^m$, associons les entiers (plus précisément, les éléments de $\mathbf{N}_\infty=\mathbf{N}\cup\infty$) $a(\widetilde{x})=v(D(\widetilde{x}))$, $a^*(\widetilde{x})=(\widetilde{x}, V^*)_\mathfrak{p}$, et $a'(\widetilde{x})=v(D'(\widetilde{x}))$. De même, à tout point $\widetilde{y}\in\mathfrak{R}^n$, associons les entiers $b(\widetilde{y})=v(E(\widetilde{y}))$ et $b^*(\widetilde{y})=(\widetilde{y}, W^*)_\mathfrak{p}$. Posons $a_0(\widetilde{x})=\sup(a(\widetilde{x}), a^*(\widetilde{x}), a'(\widetilde{x}))$ et $b_0(\widetilde{y})=\sup(b(\widetilde{y}), b^*(\widetilde{y}))$.

Soit x un point générique de X sur k^0. Alors (cf. n° 22, remarque *e)*), x est aussi un point générique de V sur k. Son image $y=\varphi(x)$, qui est un point générique de Y sur k^0, est aussi un point générique de W sur k. Donc $a(x)$, $a^*(x)$, $a'(x)$, $b(y)$, $b^*(y)$ sont finis. Désignons ces entiers respectivement par a, a^*, a', b, b^*; posons $a_0=a_0(x)=\sup(a, a^*, a')$ et $b_0=\sup(b, b^*)$. Supposons que X est d'indice μ_0' et que φ est génériquement promorphique d'indice σ sur X. Posons $\mu_0=\sup(\mu_0', a_0, b_0+\sigma)$ et $\nu_0=\mu_0-\sigma=\sup(\mu_0'-\sigma, a_0-\sigma, b_0)$. Considérons les points $x^{\mu_0}=\rho^{\mu_0}(x)$, et $y^{\nu_0}=\rho^{\nu_0}(y)$; ces points sont génériques sur k^0 des variétés $X^{\mu_0}=\overline{\rho}^{\mu_0}(X)$ et $Y^0=\overline{\rho}^{\mu_0}(Y)$ respectivement. D'après la proposition 24, le point $\widetilde{y}_{\nu_0}=F_\sigma^0(y^{\nu_0})$ est rationnel sur $k^0(x^{\mu_0})$; notons encore $\varphi^{\nu_0\mu_0}$ l'application rationnelle, définie sur k^0, telle que $\widetilde{y}^{\nu_0}=\varphi^{\nu_0\mu_0}(x^{\mu_0})$. Considérons le point $x_*^{\mu_0}=\rho_*^{\mu_0}(x)=\xi^{\mu_0}(x^{\mu_0})$ (resp. $y_*^{\nu_0}=\rho_*^{\nu_0}(y)=\xi^{\nu_0}(y^{\nu_0})$) obtenu en tronquant à l'ordre μ_0 (resp. ν_0) les suites de coefficients définissant les coordonnées de x (resp. y). D'après le choix de μ_0, on a $a_0(x_*^{\mu_0})=a_0(x)=a_0$, et $b_0(x_*^{\mu_0})=b_0(x)=b_0$. On peut trouver un k^0-ouvert $S_0^{\mu_0}$ de X^{μ_0}, contenu dans $V_\mathfrak{R}^{\mu_0}$, tel que, pour tout $u^0\in S_0^{\mu_0}$, et en posant $u_*^{\mu_0}=\xi^{\mu_0}(u^{\mu_0})$, on ait encore $a_0(u_*^{\mu_0})=a_0$. De même, on peut trouver un k^0-ouvert $T_0^{\nu_0}$ de Y^{ν_0} tel que, pour $v^{\nu_0}\in T_0^{\nu_0}$, et en posant $v_*^{\nu_0}=\xi^{\nu_0}(v^{\nu_0})$, on ait encore $b_0(v_*^{\nu_0})=b_0$; en outre, on peut choisir ces ouverts de manière que $S_0^{\mu_0}$ soit k^0-irréductible, d'adhérence X, que $\varphi^{\nu_0\mu_0}$ soit p-morphique en tout point de $S_0^{\mu_0}$, et que $\varphi^{\nu_0\mu_0}(S^{\mu_0})=F_\sigma^0(T^{\nu_0})$.

Posons $S_0=(S_0^{\mu_0})^\#$, et $T_0=(T_0^{\nu_0})^\#$. D'après le choix de $S_0^{\mu_0}$ et $T_0^{\nu_0}$, on a $a_0(u_0)=a_0$ pour tout $u_0\in S_0$ et, de même, $b_0(v_0)=b_0$ pour tout $v_0\in T_0$. Ceci implique, en particulier $S_0\subset\mathscr{S}(V)$ et $T_0\subset\mathscr{S}(W)$. D'autre part, il est clair qu'on a $\varphi(S_0)\subset T_0$. Nous allons montrer qu'on a, en fait, $\varphi(S_0)=T_0$, autrement dit que, pour tout point $\overline{y}=(\overline{y}_1, \ldots, \overline{y}_n)$ de T_0, il existe un point $\overline{x}=(\overline{x}_1, \ldots, \overline{x}_m)$ de S_0, tel que $\overline{y}=\varphi(\overline{x})$.

Nous allons commencer par montrer qu'il nous suffit de prouver l'assertion A) suivante :

A) Pour tout couple (μ, x'), composé d'un entier $\mu \geqslant \mu_0 + 1$ et d'un point $x' = (x'_1, \ldots, x'_m)$ de $\mathfrak{R}^m$, tels qu'on ait $\rho^\mu(x') \in S_0^\mu$, vérifiant les inégalités

$$v(F_\alpha(x')) \geqslant \mu_0 + \mu \qquad (1 \leqslant \alpha \leqslant m-r) \tag{30}$$

$$v(f_j(x') - \overline{y}_j) \geqslant \mu_0 + \mu \qquad (n-s+1 \leqslant j \leqslant n) \tag{31}$$

il existe un $x'' \in \mathfrak{R}^m$ tel qu'on ait $x''^\mu = \rho^\mu(x'') \in S_0^\mu$, et tel qu'on ait les inégalités

$$v(F_\alpha(x'')) \geqslant \mu_0 + \mu + 1 \qquad (1 \leqslant \alpha \leqslant m-r) \tag{32}$$

$$v(f_j(x'') - \overline{y}_j) \geqslant \mu_0 + \mu + 1 \qquad (n-s+1 \leqslant j \leqslant n) \tag{33}$$

$$(x'', x')_p \geqslant \mu \tag{34}$$

En effet, supposons exacte l'assertion A). Soit $x_0^{\mu_0}$ un point de $S_0^{\mu_0}$, tel qu'on ait $\varphi^{\nu_0\mu_0}(x_0^{\mu_0}) = F_\sigma^0(\overline{y}^{\nu_0})$, et soit x_0 un point de S_0, tel que $x_0^{\mu_0} = \rho^{\mu_0}(x_0)$. On voit immédiatement, par récurrence sur ν, qu'on peut, en partant de x_0, construire une suite $(x_0, x_1, \ldots, x_\nu, \ldots)$ de points de $\mathfrak{R}^m$, tels qu'on ait, pour tout $\nu \geqslant 0$, les inégalités

$$v(F_\alpha(x_\nu)) \geqslant \mu_0 + \mu + \nu \qquad (1 \leqslant \alpha \leqslant m-r) \tag{35}$$

$$v(f_j(x_\nu) - \overline{y}_j) \geqslant \mu_0 + \mu + \nu \qquad (n-s+1 \leqslant j \leqslant n) \tag{36}$$

$$(x_\nu, x_{\nu+1})_p \geqslant \mu + \nu \tag{37}$$

Cette dernière inégalité entraîne que la suite x_ν converge p-adiquement, et que sa limite est un point $\overline{x} \in \mathfrak{R}^m$ tel qu'on ait $(x_0, \overline{x})_p \geqslant \mu$. Les inégalités (35) entraînent $F_\alpha(\overline{x}) = 0$ $(1 \leqslant \alpha \leqslant m-r)$ d'où $\overline{x} \in V'$. Les relations $a_0(x_0) = a_0 \leqslant \mu_0 < \mu$, et $(x_0, \overline{x})_p \geqslant \mu$ entraînent $a_0(\overline{x}) = a_0$. En particulier, on a $a_*(\overline{x}) \leqslant a_0$, ce qui implique $\overline{x} \notin V^*$, d'où $\overline{x} \in V$, d'où $\overline{x} \in V_{\mathfrak{R}}$. Comme on a $x_0^\mu = \overline{x}^\mu$, on a $\overline{x} \in S_0$.

Soit $\overline{y}' = (\overline{y}'_1, \ldots, \overline{y}'_n)$ le point $\overline{y}' = \varphi(\overline{x})$. Les inégalités (36) entraînent

$$f_j(\overline{x}) = \overline{y}_j = \overline{y}'_j$$

pour $n-s+1 \leqslant j \leqslant n$. De plus, puisqu'on a $x \in S_0$, on a $\overline{y}' \in T_0$ et, puisque $(x_0, \overline{x}) > \mu_0$, on a $(\overline{y}, \overline{y}') > \nu_0$. Nous allons montrer qu'on a $\overline{y}' = \overline{y}$. Supposons, en effet, $\overline{y}' \neq \overline{y}$, et posons $(\overline{y}, \overline{y}')_p = \nu'$; on a alors $\overline{y}' = \overline{y} + t^{\nu'}\overline{z}$, où $\overline{z} = (z_1, \ldots, z_{n-s}, 0, \ldots, 0)$ est un point de $\mathbf{S}_n$ tel que le point réduit $\overline{z}^0 = \rho(\overline{z}) = (z_1^0, \ldots, z_{n-s}^0, 0, \ldots, 0)$ soit distinct de l'origine. Puisque $\overline{y}' \in W$, on a $G_\beta(\overline{y}') = G_\beta(\overline{y} + t^{\nu'}\overline{z}) = 0$ $(1 \leqslant \beta \leqslant n)$. D'après la formule de Taylor, on en déduit $\Sigma_{j=1}^{n-s} \frac{\partial G_\beta}{\partial X_j}(\overline{y})\overline{z}_j \equiv 0 \pmod{t^{\nu'}}$ $(1 \leqslant \beta \leqslant n-s)$. On en déduit, pour $1 \leqslant j \leqslant n-s$, $v(z_j) \leqslant \nu' - b(\overline{y})$; comme on a, d'autre part, $b(\overline{y}) = b \geqslant \nu_0$, et $\nu' > \nu_0 \geqslant b$, on a $v(z_j) > 0$, d'où $z_j^0 = 0$ pour tout j $(1 \leqslant j \leqslant n)$, ce qui est contradictoire. On a donc bien $\overline{y} = \overline{y}' = \varphi(\overline{x})$.

Démontrons maintenant l'assertion A). En faisant le changement de variable

$x'' = x' + t^{\mu}u$, on voit que la condition de l'existence d'un x'' vérifiant (32), (33) et (34) est équivalente à celle de l'existence d'un $u \in \mathfrak{R}^m$ tel qu'on ait les inégalités

$$(38) \qquad \begin{cases} v(\mathrm{F}_{\alpha}(x' + t^{\mu}u)) \geqslant \mu_0 + \mu + 1 & (1 \leqslant \alpha \leqslant m - r) \\ v(f_j(x' + t^{\mu}u) - \overline{y}) \geqslant \mu_0 + \mu + 1 & (n - s + 1 \leqslant j \leqslant n) \end{cases}$$

Or, on peut exhiber un tel u. Il suffit de prendre pour u une solution entière du système linéaire

$$(39) \qquad \begin{cases} \mathrm{F}_{\alpha}(x') + \Sigma_{i=1}^{n} \dfrac{\partial \mathrm{F}_{\alpha}}{\partial \mathrm{X}_i}(x')\mathrm{X}_i = 0 & (1 \leqslant \alpha \leqslant m - r) \\ f_j(x') + \Sigma_{i=1}^{n} \dfrac{\partial f_j}{\partial \mathrm{X}_i}(x')\mathrm{X}_i = 0 & (n - s + 1 \leqslant j \leqslant n) \end{cases}$$

Une telle solution u existe, d'après les relations (30) et (31), et puisqu'on a $\mu > \mu_0 \geqslant a_0(x') \geqslant a'(x')$; en appliquant la formule de Taylor, on voit qu'on a, pour un tel u :

$$\begin{cases} v(\mathrm{F}_{\alpha}(x' + t^{\mu}u)) \geqslant 2\mu & (1 \leqslant \alpha \leqslant m - r) \\ v(f_j(x' + t^{\mu}u) - \overline{y}) \geqslant 2\mu & (n - s + 1 \leqslant j \leqslant n) \end{cases}$$

d'où résultent *a fortiori* les relations (38), puisqu'on a pris $\mu \geqslant \mu_0 + 1$.

On a donc bien montré que $\mathrm{T}_0 = \varphi(\mathrm{S}_0)$. Ceci entraîne, en particulier, $(\rho_{\mathrm{W}}^{\mu})^{-1}(y^0) \subset \mathrm{Y}$; autrement dit Y vérifie la condition (**) relativement à W et, par suite, Y est une (W, $\mathfrak{p}$, k^0)-provariété. On peut trouver, d'après la proposition 24, un (V, $\mathfrak{p}$, k^0)-ensemble irréductible S_0', d'indice μ_0, d'adhérence X, contenu dans S_0, tel que φ soit promorphique d'indice σ sur S_0'. Posons $\mathrm{T}_0' = \varphi(\mathrm{S}_0')$. D'après ce qui précède, T_0' est encore un (W, $\mathfrak{p}$)-ensemble d'indice ν_0. On peut trouver un sous-ensemble k^0-constructible irréductible T^{ν_0} de $(\mathrm{T}_0')^{\nu_0} = \rho^{\nu_0}(\mathrm{T}')$ tel que $\mathrm{T} = (\mathrm{T}^{\nu_0})^{\sharp}$ soit un sous-(W, $\mathfrak{p}$, k^0)-ensemble k^0-irréductible de T_0', d'adhérence Y ; si alors on pose $\mathrm{S}^{\mu_0} = (\varphi^{\nu_0 \mu_0})^{-1}(\mathrm{T}^{\nu_0})$, et $\mathrm{S} = (\mathrm{S}^{\mu_0})^{\sharp}$, S est encore un (V, $\mathfrak{p}$, k^0)-ensemble irréductible d'adhérence X, et on a $\mathrm{T} = \varphi(\mathrm{S})$; puisqu'on a $\mathrm{S}_0 \subset \mathscr{S}(\mathrm{V})$ et $\mathrm{T}_0 \subset \mathscr{S}(\mathrm{W})$, on a aussi *a fortiori* $\mathrm{S} \subset \mathscr{S}(\mathrm{V})$ et $\mathrm{T} \subset \mathscr{S}(\mathrm{W})$; ceci termine la démonstration du théorème 1.

Remarque. — Dans le cas particulier où φ est birationnelle (ce cas est d'ailleurs le seul dont nous aurons besoin dans la suite), la démonstration précédente se simplifie considérablement. On voit alors directement que Y est une (W, $\mathfrak{p}$, k^0)-provariété en remarquant que, si x est un point générique de X sur k^0, et si $y = \varphi(x)$, φ est bicontinue en (x, y) pour la topologie $\mathfrak{p}$-adique. Il suffit ensuite d'appliquer la proposition 24 aux deux applications φ et φ^{-1} simultanément.

On remarquera que la condition $y \in \mathrm{W}_{\mathfrak{R}}$ de la proposition 24 et du théorème 1 est toujours vérifiée lorsque W est $\mathfrak{p}$-*complète*, et on en déduit le corollaire suivant du théorème 1, exprimant le caractère *intrinsèque* de la notion de (V, $\mathfrak{p}$)-provariété, lorsque V est $\mathfrak{p}$-complète, relativement aux isomorphismes sur $\mathfrak{k}$ (et pas seulement sur $\mathfrak{R}$).

Corollaire. — *Soient* V *et* W *deux* $\mathfrak{p}$-*variétés* $\mathfrak{p}$-*complètes, définies sur k, et soit* $\varphi : \mathrm{V} \to \mathrm{W}$ *un k-isomorphisme. Alors* φ_g *est une bijection de l'ensemble des* (V, $\mathfrak{p}$)-*provariétés (resp. des* (V, $\mathfrak{p}$, k^0)-*provariétés) sur celui des* (W, $\mathfrak{p}$)-*provariétés (resp. des* (W, $\mathfrak{p}$, k^0)-*provariétés).*

Il importe de remarquer que l'application φ_g ne respecte pas l'inclusion. Par exemple, prenons pour V la droite projective $\mathbf{P}_1$ et pour φ l'application $V \to V$ qui, au point (x, y) ait correspondre (x, ty). Prenons pour X la provariété obtenue en relevant le point (0, 1), et pour Y la provariété maximale $V_{\mathfrak{R}} = V_{\mathfrak{k}}$, composée de tous les points rationnels $\mathfrak{p}$-adiques de V. Alors on a $\varphi_g(X) = Y$ tandis que $\varphi_g(Y)$ est la $(V, \mathfrak{p})$-provariété obtenue en relevant le point (1, 0). On a donc $X \subset Y$, tandis que $\varphi_g(X) \supset \varphi_g(Y)$ (et ces deux inclusions sont strictes !).

Lemme 2. — Soit V *une variété définie sur un corps* $\mathbf{k}$. *Soit* S *un sous-ensemble* $\mathbf{k}$*-constructible de* V, *et supposons qu'à toute sous-*$\mathbf{k}$*-variété* X *de* V, *génériquement contenue dans* S, *on ait associé un* $\mathbf{k}$*-ouvert non vide* $\mathscr{U}(X)$ *de* X, *contenu dans* S. *Alors il existe une partition finie de* S, *composée d'ensembles de la forme* $\mathscr{U}(X_\alpha)$.

Démonstration. — On peut, par récurrence sur α, construire une suite $X_1, \ldots, X_\alpha, \ldots$ de sous-$\mathbf{k}$-variétés de V, génériquement contenues dans S, telles que les $\mathscr{U}(X_\alpha)$ soient disjoints, et vérifiant en outre les conditions suivantes : si X'_α est l'adhérence du complémentaire, relativement à S, de la réunion $\bigcup_{\beta \leqslant \alpha} \mathscr{U}(X_\beta)$, la suite (X'_α) est décroissante et, de plus, $X'_{\alpha+1}$ est strictement contenue dans X'_α, à moins que X'_α ne soit vide. Il suffit en effet, pour tout α, de prendre pour X_α l'une des $\mathbf{k}$-composantes de $X'_{\alpha-1}$. L'ensemble $\mathbf{k}$-fermé X'_α est alors vide à partir d'un certain α, d'où le lemme.

Théorème 2. — Soient V *et* W *deux* $\mathfrak{p}$*-variétés sans point multiple, définies sur* k, *et soit* $\varphi : V \to W$ *un* k*-morphisme génériquement surjectif et séparable, défini sur* k. *Soit* S *un* $(V, \mathfrak{p}, k^0)$*-ensemble, tel que* $T = \varphi(S)$ *soit contenu dans* $W_{\mathfrak{R}}$. *Alors* $T = \varphi(S)$ *est un* $(W, \mathfrak{p}, k^0)$*-ensemble. De plus, il existe un entier* $\sigma_0 = \sigma_0(V, W, \varphi)$, *qui ne dépend pas de* S, *et une partition finie* $\{S_\alpha\}$ $(1 \leqslant \alpha \leqslant h)$ *de* S, *composée de* $(V, \mathfrak{p}, k^0)$*-ensembles irréductibles* S_α, *tel que* φ *soit promorphique d'indice* σ_0 *sur chacun des* S_α, *et que, pour tout* α, $T_\alpha = \varphi(S_\alpha)$ *soit un* $(W, \mathfrak{p}, k^0)$*-ensemble irréductible.*

Démonstration. — Il résulte de la proposition 24 que, si la propriété de l'énoncé est vraie pour un $(V, \mathfrak{p}, k^0)$-ensemble S, elle l'est aussi pour tout sous-$(V, \mathfrak{p}, k^0)$-ensemble de S, et que si elle l'est pour deux $(V, \mathfrak{p}, k^0)$-ensembles S et T, elle l'est aussi pour leur réunion.

Ceci permet de se ramener au cas où V est une variété affine $(V \subset \mathbf{S}_m)$. Commençons par examiner le cas où W est aussi une variété affine $(W \subset \mathbf{S}_n)$. D'après ([F], VII, 2, th. 2, cor. 2), il existe des polynômes P_j $(1 \leqslant j \leqslant n)$ appartenant à l'anneau $k[X_1, \ldots, X_m]$ tels que, pour tout j, la j-ième coordonnée φ_j de φ soit induite par P_j. Soit σ_0 un entier tel que tous les polynômes $t^{\sigma_0} P_j$ soient à coefficients dans R. Soit μ un entier $\geqslant \sup(m_0(V), m_0(W) + \sigma_0)$, et posons $S^\mu = \rho^\mu(S)$. A toute sous-k^0-variété X^μ de $\mathbf{S}^0_{n(\mu+1)}$ génériquement contenue dans S^μ, on peut, d'après le théorème 1, faire correspondre un ouvert $U^\mu = \mathscr{U}(X^\mu)$ de X^μ, tel que le $(V, \mathfrak{p}, k^0)$-ensemble $U = (U^\mu)^\#$ soit k^0-irréductible, que φ soit promorphique d'indice σ_0 sur U, et que l'image $\varphi(U)$ soit un $(W, \mathfrak{p}, k^0)$-ensemble k^0-irréductible. Il suffit alors d'appliquer le lemme 2 au sous-ensemble k^0-constructible S^μ de $\mathbf{S}^0_{n(\mu+1)}$, et à la famille des ensembles $\mathscr{U}(X^\mu)$ (μ fixe, X^μ variable).

Examinons maintenant le cas général, où $W = (W_\alpha, T_{\beta\alpha})$ $(1 \leqslant \alpha \leqslant h,\ 1 \leqslant \beta \leqslant h)$ est une $\mathfrak{p}$-variété quelconque. Supposons qu'on a, pour tout α, $W_\alpha \subset \mathbf{S}_{n_\alpha}$, et soit φ_α l'application rationnelle $\varphi_\alpha : V \to W_\alpha$ qui représente φ. On se ramène immédiatement au cas

suivant : pour tout α, il existe des polynômes $P_{\alpha i}$ $(1 \leqslant i \leqslant n_\alpha)$, et Q_α, tels que les coordonnées $\varphi_{\alpha i}$ de φ_α soient respectivement induites par les $P_{\alpha i}/Q_\alpha$. Raisonnons par récurrence sur h : le résultat a été prouvé pour $h=1$; supposons-le vrai pour $h-1$, et montrons qu'il l'est pour h.

Les polynômes Q_α $(1 \leqslant \alpha \leqslant h)$ n'ont pas de zéro commun. D'après le lemme 1 du n° 17, il existe un entier σ tel qu'on ait $\inf_\alpha v(Q_\alpha(x)) \leqslant \sigma$ pour tout point $x \in V_\mathfrak{R}$. Pour tout α, notons T_α le $(V, \mathfrak{p}, k^0)$-ensemble, d'indice σ, défini par $v(Q_\alpha(x)) \leqslant \sigma$. Puisque les T_α recouvrent $V_\mathfrak{R}$, les $S_\alpha = S \cap T_\alpha$ recouvrent S. Il suffit donc de prouver que la propriété de l'énoncé est vérifiée par l'un quelconque des $(V, \mathfrak{p}, k^0)$-ensembles S_α.

Pour tout α, notons S'_α le sous-ensemble de S_α composé des $x \in S_\alpha$ tels qu'on ait $\inf_i v(P_{\alpha i}(x)) \geqslant v(Q_\alpha(x))$ (i.e. $\varphi_\alpha(x) \in (W_\alpha)_\mathfrak{R}$). Ce sous-ensemble S'_α est en fait un sous-$(V, \mathfrak{p}, k^0)$-ensemble de S_α. Pour tout α, notons U_α l'ouvert de définition de φ_α (défini par $x \in U_\alpha$ si et seulement si φ_α est morphique en x). On a $S'_\alpha \subset S_\alpha \subset U_\alpha$, et $\varphi_\alpha(S'_\alpha) \subset V_\mathfrak{R}$. D'après le résultat de la première partie de la démonstration, appliqué au morphisme $U_\alpha \to W_\alpha$ induit par φ_α, la propriété de l'énoncé est vérifiée par le $(V, \mathfrak{p}, k^0)$-ensemble S'_α.

Considérons maintenant le complémentaire $\overline{S}'_\alpha$ de S'_α relativement à S_α. Posons $U'_\alpha = \bigcup_{\beta \neq \alpha} U_\beta$, et notons W'_α l'ouvert de W composé des points qui sont représentés dans l'un au moins des W_β $(\beta \neq \alpha)$. Pour $x \in \overline{S}'_\alpha$, on a $\varphi_\alpha(x) \notin (W_\alpha)_\mathfrak{R}$; donc, puisque $\varphi_\alpha(S) \subset W_\mathfrak{R}$, il existe un $\beta \neq \alpha$ tel que φ_β soit morphique en x, et tel qu'on ait $\varphi_\beta(x) \in (W_\beta)_\mathfrak{R}$. Autrement dit, on a $\overline{S}'_\alpha \subset U'_\alpha$, et $\varphi(\overline{S}'_\alpha) \subset (W'_\alpha)_\mathfrak{R}$. D'après l'hypothèse de récurrence, appliquée au morphisme $\varphi'_\alpha : U'_\alpha \to W'_\alpha$ induit par φ, la propriété de l'énoncé est vérifiée par $\overline{S}'_\alpha$. Elle l'est donc bien aussi par $S_\alpha = S'_\alpha \cup \overline{S}'_\alpha$.

Dans le cas particulier où W est $\mathfrak{p}$-complète et sans point multiple, la condition $T \subset W_\mathfrak{R}$ imposée dans l'énoncé est toujours vérifiée. On en déduit le corollaire suivant du théorème 2, exprimant le caractère *intrinsèque* de la notion de $(V, \mathfrak{p})$-ensemble, au même sens que plus haut, lorsque V est $\mathfrak{p}$-complète et sans point multiple.

Corollaire. — *Soient* V *et* W *deux* $\mathfrak{p}$*-variétés* $\mathfrak{p}$*-complètes, sans point multiple, définies sur* k*, et soit* $\varphi : V \to W$ *un* k*-isomorphisme. Alors* φ *induit une bijection de l'ensemble des* $(V, \mathfrak{p})$*-ensembles (resp. des* $(V, \mathfrak{p}, k^0)$*-ensembles) sur celui des* $(W, \mathfrak{p})$*-ensembles (resp. des* $(W, \mathfrak{p}, k^0)$*-ensembles).*

Remarque. — Il résulte de la démonstration que, si $\varphi : V \to W$ est un morphisme d'une $\mathfrak{p}$-variété quelconque V dans une $\mathfrak{p}$-variété W, l'application $\varphi | V_\mathfrak{R}$ induite par φ sur $V_\mathfrak{R}$ est *uniformément continue pour la topologie* $\mathfrak{p}$*-adique*. Plus précisément, il existe un entier σ_0 possédant la propriété suivante : pour tout couple (x, x') d'éléments de $V_\mathfrak{R}$ tels qu'on ait $(x, x')_\mathfrak{p} \geqslant \sigma_0 + \mu$ et tels que les points $y = \varphi(x)$, $y' = \varphi(x')$ appartiennent à $W_\mathfrak{R}$, on a $(y, y')_\mathfrak{p} \geqslant \mu$.

25. Transformations $\mathfrak{p}$-monoïdales.

Fixons-nous un entier $n > 0$. Pour tout entier $s \geqslant 0$, nous noterons L_s l'espace vectoriel sur k composé des polynômes homogènes et de degré s de l'anneau $R[X_0, \ldots, X_n]$, et M_s le R-module composé des éléments de L_s qui sont à coefficients entiers (c'est-à-dire dans R).

Considérons d'abord un sous-R-module J de M_s. Pour tout système de générateurs $\mathscr{B}=\{P_0, \ldots, P_m\}$ de J, notons $\eta^*=\eta_s^*(\mathscr{B}, J)$ l'application rationnelle $\eta^*: \mathbf{P}_n \to \mathbf{P}_m$, définie sur k, qui, à tout point générique $\overline{x}$ de $\mathbf{P}_n$ sur $\mathfrak{k}$, fait correspondre le point $\overline{y}^*=(\overline{y}_0^*, \ldots, \overline{y}_m^*)$ de $\mathbf{P}_m$ ayant pour coordonnées les $\overline{y}_j^*=P_j(\overline{x})$. Désignons par $\mathbf{W}^*$ la sous-variété de $\mathbf{P}_m$ lieu de $\overline{y}^*$ sur k, et par $\xi^*=\xi_s^*(\mathscr{B}, J)$ l'application réduite $\xi^*: \mathbf{P}_n \to \mathbf{W}^*$ de η^*. Notons d'autre part η l'application rationnelle $\eta: \mathbf{P}_n \to \mathbf{P}_n \times \mathbf{P}_m$, définie sur k, telle qu'on ait $\eta(\overline{x})=\overline{x}\times\overline{y}^*=\overline{x}\times\eta^*(\overline{x})$; notons $\mathbf{W}$ la sous-variété de $\mathbf{P}_n\times\mathbf{P}_m$ lieu de $\overline{y}=\eta(\overline{x})$ sur k (i.e. le graphe de η^*) et $\xi=\xi_s(\mathscr{B}, J)$ l'application réduite $\xi: \mathbf{P}_n \to \mathbf{W}$ de η. On remarquera que l'application inverse ξ^{-1} est toujours un R-morphisme et, de plus, que ξ^* et ξ sont déterminés, à un R-isomorphisme près, par la donnée de J. L'ensemble des transformations $\xi^*=\xi_s^*(\mathscr{B}, J)$ (resp. $\xi=\xi_s(\mathscr{B}, J)$) ainsi associées (pour J fixe et $\mathscr{B}$ variable) au sous-R-module J de M_s sera désigné par $\mathscr{M}_s^*(J, \mathbf{P}_n)$ (resp. $\mathscr{M}_s(J, \mathbf{P}_n)$).

Soit maintenant I un idéal homogène de l'anneau $R[X_0, \ldots, X_n]$. Supposons que l'ensemble $\mathscr{Z}(I)$ des zéros de I dans $\mathbf{P}_n$ est vide, et notons $\mathscr{Z}^0(I)$ l'ensemble de ses zéros dans l'espace réduit $\mathbf{P}_n^0$, i.e. l'ensemble des points $x^0\in\mathbf{P}_n^0$ tels qu'on ait $P^0(x^0)=0$, en posant $P^0=\rho(P)$, pour tout $P\in I$. Pour tout entier $s\geqslant 0$, l'ensemble $I_s=I\cap M_s$ est un sous-R-module de M_s. Il existe un entier $s_0=s_0(I)$ tel que I soit engendré, comme R-module, par les $I_{s'}(s'\leqslant s_0)$. Pour $s\geqslant s_0$, les éléments de I_s n'admettent alors aucun zéro commun dans $\mathbf{P}_n$, et leurs seuls zéros communs dans $\mathbf{P}_n^0$ sont alors les points de $\mathscr{Z}^0(I)$. Donc, pour un tel s, tout élément ξ de $\mathscr{M}_s(I_s, \mathbf{P}_n)$ est un k-isomorphisme.

D'autre part, toujours pour $s\geqslant s_0$, l'application ξ est déterminée, à un R-isomorphisme près, par la seule donnée de I. Nous dirons que ξ est une *transformation* $\mathfrak{p}$-*monoïdale de* $\mathbf{P}_n$ *attachée à l'idéal* I. L'ensemble de ces transformations (i.e. la réunion des $\mathscr{M}_s(I_s, \mathbf{P}_n)$, obtenus pour s variable $\geqslant s_0$) sera désigné par $\mathscr{M}(I, \mathbf{P}_n)$.

Soit en particulier S^0 un sous-ensemble k^0-fermé quelconque de l'espace projectif $\mathbf{P}_n^0$, et considérons l'idéal $I=\mathscr{I}_R(S^0)$, composé des polynômes homogènes $P\in R[X_0, \ldots, X_n]$ tels que $P^0=\rho(P)$ s'annule sur X^0. Cet idéal I vérifie la condition $\mathscr{Z}(I)=\emptyset$ imposée plus haut. Nous écrirons $\mathscr{M}(S^0, \mathbf{P}_n)$ au lieu de $\mathscr{M}(\mathscr{I}_R(S^0), \mathbf{P}_n)$, et les éléments de cet ensemble seront appelés *transformations* $\mathfrak{p}$-*monoïdales de centre* S^0.

26. Cas d'un corps global.

Nous appellerons *corps global* un corps K qui est, ou bien

a) Un corps de nombres algébriques, de degré fini sur le corps des rationnels $\mathbf{Q}$,

ou bien

b) Un corps de fonctions algébriques d'une variable sur un corps de base parfait K_0.

On note $\mathfrak{S}=\mathfrak{S}(K)$ l'ensemble de tous les $\mathfrak{p}$ respectivement associés, dans le cas *a)*, aux valuations non triviales de K et, dans le cas *b)*, aux valuations non triviales de K s'annulant sur K_0.

Dans le cas *a)*, les éléments de $\mathfrak{S}$ correspondent biunivoquement aux idéaux premiers de l'anneau $\mathscr{R}$ des entiers de K. Dans le cas *b)*, K est de la forme $K_0(u)$, où u est un point générique, sur K_0, d'une courbe U complète, sans point multiple, définie

sur K_0; les éléments de $\mathfrak{S}$ correspondent biunivoquement aux diviseurs sur U qui sont rationnels et premiers sur K_0.

On suppose maintenant, dans la suite de ce numéro, et tout en conservant les notations introduites au n° 1, que k est un corps global, et que $\mathfrak{p}$ appartient à $\mathfrak{S}=\mathfrak{S}(k)$. Pour tout $\mathfrak{q}\in\mathfrak{S}$, on notera $v_\mathfrak{q}$ la valuation, et $R_\mathfrak{q}$ l'anneau de valuation correspondant. On a, en particulier, $v=v_\mathfrak{p}$, et $R=R_\mathfrak{p}$.

Proposition 25. — Supposons que k est un corps global, et que $\mathfrak{p}\in\mathfrak{S}=\mathfrak{S}(k)$. *Soit* I *un idéal homogène de l'anneau* $R[X_0, \ldots, X_n]$, *tel qu'on ait* $\mathfrak{Z}(I)=\emptyset$. *Alors, il existe une transformation* $\mathfrak{p}$*-monoïdale* $\xi : \mathbf{P}_n \to \mathbf{W}$ *attachée à* I (*i.e. appartenant à* $\mathfrak{M}(I, \mathbf{P}_n)$), *et qui est un* $R_\mathfrak{q}$*-isomorphisme pour tout* $\mathfrak{q}\in\mathfrak{S}$ *distinct de* $\mathfrak{p}$.

(On dira alors que ξ est une transformation *strictement* $\mathfrak{p}$*-monoïdale* de $\mathbf{P}_n$ attachée à I.)

Démonstration. — On peut, d'après le théorème des zéros de Hilbert, trouver deux entiers h et s ($s\geqslant s_0=s_0(I)$), tels qu'on ait $\mathfrak{p}^h X_i^s \subset I$, d'où $\mathfrak{p}^h X_i^s \subset I_s = I\cap M_s$ pour tout i ($1\leqslant i\leqslant n$).

Dans le cas *a)*, introduisons l'anneau $\mathfrak{R}$ des entiers (au sens absolu) de k. Le $\mathfrak{R}$-module $J_s=I_s\cap\mathfrak{R}[X]$ est de type fini, puisque $\mathfrak{R}[X]$ est noethérien. On a $I_s=RJ_s$; en effet, il est clair qu'on a $RJ_s\subset I_s$; inversement pour $P\in I_s$, il existe $a\in\mathfrak{R}$ tel que $v(a)=v_\mathfrak{p}(a)=0$, et $aP\in\mathfrak{R}[X]$, d'où $aP\in J_s$, d'où $P\in a^{-1}J_s\subset RJ_s$. D'autre part, pour tout $\mathfrak{q}\in\mathfrak{S}$ distinct de $\mathfrak{p}$, les éléments de $R_\mathfrak{q}J_s$ n'admettent aucun zéro commun dans l'espace $(\mathbf{P}_n)_\mathfrak{q}^0$ réduit de $\mathbf{P}_n$ (mod. $\mathfrak{q}$); en effet, il suffit de montrer que les X_i^s appartiennent à $R_\mathfrak{q}J_s$; or, on peut trouver un élément u de $\mathfrak{R}$ tel que $v(u)=v_\mathfrak{p}(u)=h$, et tel que $v_\mathfrak{q}(u)=0$; on a alors $uX_i^s\in I_s$, d'où $uX_i^s\in J_s$ pour tout i, d'où $X_i^s\in u^{-1}J_s\subset R_\mathfrak{q}J_s$. Donc, si $\mathfrak{B}$ est un système de générateurs du $\mathfrak{R}$-module J_s, les polynômes réduits (mod. $\mathfrak{q}$) des éléments de $\mathfrak{B}$ n'admettent aucun zéro commun, pour $\mathfrak{q}\in\mathfrak{S}$ distinct de $\mathfrak{p}$. L'application $\xi=\xi_s(\mathfrak{B}, J_s) : \mathbf{P}_n\to\mathbf{W}$ vérifie alors les conditions de la proposition.

Dans le cas *b)*, le corps k est de la forme $k_0(u)$, où k_0 est un corps parfait, et où u est un point générique, sur k_0, d'une courbe U, complète et sans point multiple, définie sur k_0. A tout $\mathfrak{q}\in\mathfrak{S}$ correspond un diviseur $a_\mathfrak{q}$ sur U, rationnel et premier sur k_0. Introduisons un nombre fini d'éléments t_ν ($1\leqslant\nu\leqslant\nu_0$) de k, tels qu'on ait $\inf_\nu v_\mathfrak{p}(t_\nu)=h$, et $\inf_\nu v_\mathfrak{q}(t_\nu)\leqslant 0$ pour tout $\mathfrak{q}\in\mathfrak{S}$ distinct de $\mathfrak{p}$. Posons de plus, pour $\mathfrak{q}\neq\mathfrak{p}$, $m_\mathfrak{q}=-\inf_\nu v_\mathfrak{q}(t_\nu)$, et désignons par $\mathfrak{m}$ le diviseur positif $\Sigma_\mathfrak{q} m_\mathfrak{q} a_\mathfrak{q}$ de U, où la somme est étendue à tous les $\mathfrak{q}\in S-\{\mathfrak{p}\}$. On a aussi $\mathfrak{m}=-\inf_\nu(0, t_\nu))$, où (t_ν) est le diviseur de t_ν, et où le signe inf est relatif à la relation d'ordre habituelle sur le groupe des diviseurs sur U.

Soit $\mathfrak{R}$ le sous-anneau de k composé des fonctions f sur U définies sur k, et dont tous les pôles appartiennent à $\mathrm{supp}(\mathfrak{m})$. Pour tout entier $l\geqslant 0$, désignons par $\mathfrak{R}_l$ l'espace vectoriel sur k_0 composé des $f\in\mathfrak{R}$ telles que $(f)\succ -l\mathfrak{m}$. Ce k_0-espace vectoriel $\mathfrak{R}_l$ est, pour tout $l\geqslant 0$, de dimension finie, et on a $\mathfrak{R}=\bigcup_l\mathfrak{R}_l$. Le $\mathfrak{R}$-module $J_s=I_s\cap\mathfrak{R}[X]$ est de type fini. En effet, $\mathfrak{R}$ est noethérien, donc aussi $\mathfrak{R}[X]$, et J_s est contenu dans le $\mathfrak{R}$-module de type fini $M_s\cap\mathfrak{R}[X]$. Il existe donc un entier l_0 tel que J_s soit engendré, comme $\mathfrak{R}$-module, par $J_{sl_0}=I_s\cap\mathfrak{R}_{l_0}[X]$. De plus J_{sl_0} est un k_0-espace vectoriel de

dimension finie : en effet, il est contenu dans $M_{sl_0} = M_s \cap \mathscr{R}_{l_0}[X]$, et comme $\mathscr{R}_{l_0}$ est un k_0-espace vectoriel de dimension finie, il en est de même de M_{sl_0}.

On a $RJ_{sl_0} = I_s$. En effet, il est clair qu'on a $RJ_{sl_0} \subset I_s$. D'autre part, pour $P \in I_s$, il existe $f \in k$ tel que $v_\mathfrak{p}(f) = 0$, et $fP \in \mathscr{R}[X]$. On a donc $fP \in I_s \cap \mathscr{R}[X] = J_s = \mathscr{R}J_{sl_0}$, d'où $P \in f^{-1}\mathscr{R}J_{sl_0} \subset RJ_{sl_0}$.

D'autre part, pour $\mathfrak{q} \in \mathfrak{S}$ distinct de $\mathfrak{p}$, on peut trouver un entier $\nu = \nu_\mathfrak{q}$ $(1 \leqslant \nu \leqslant \nu_0)$, tel que $v_\mathfrak{q}(t_\nu) = -m_\mathfrak{q}$. Pour ν ainsi choisi, on a $t_\nu^{-l_0} J_{sl_0} \subset R_\mathfrak{q}[X]$. Montrons que les polynômes de $t_\nu^{-l_0} J_{sl_0}$ n'admettent aucun zéro commun dans l'espace projectif réduit $(\mathbf{P}_n)_\mathfrak{q}^0$. Il suffit, pour cela, de montrer qu'on a $t_\nu^{l_0} X_i^s \in J_{sl_0}$ pour tout i. Or, on a $l_0 \geqslant 1$, et $v_\mathfrak{p}(t_\nu) \geqslant h$; on a donc $t_\nu^{l_0} X_i^s \in I_s$. On a, d'autre part, $t_\nu^{l_0} \in \mathscr{R}_{l_0}$, d'où $t_\nu^{l_0} X_i^s \in \mathscr{R}_{l_0}[X]$. Donc on a bien $t_\nu^{l_0} X_i^s \in J_{sl_0}$.

Donc tout système de générateurs $\mathscr{B}$ du k_0-espace vectoriel J_{sl_0} est aussi un système de générateurs du R-module I_s, et est tel que, pour tout $\mathfrak{q} \in \mathfrak{S}$ distinct de $\mathfrak{p}$, l'ensemble $t_{\nu_\mathfrak{q}}^{-l_0} \mathscr{B}$ se compose de polynômes n'ayant aucun zéro commun dans $(\mathbf{P}_n)_\mathfrak{q}^0$. L'application $\xi = \xi_s(\mathscr{B}, J_{sl_0}) : \mathbf{P}_n \to \mathbf{W}$ vérifie les conditions de la proposition.

27. Désingularisation et éclatement d'une (V, p)-provariété.

Soit V une p-variété définie sur k. Par *k-modèle* de V, on entendra toujours un couple (W, φ), composé d'une variété W définie sur k, et d'un k-isomorphisme $\varphi : V \to W$.

Théorème 3 (désingularisation d'une (V, p)*-provariété).* — *Soit* V *une variété projective, définie sur k, de dimension r, et soit* X *une* (V, p, k^0)*-provariété. Posons* $\lambda = l(X, V)$. *Alors, il existe un k-modèle projectif* (W, φ) *de* V *vérifiant les conditions suivantes*

(i) φ^{-1} *est un* R*-morphisme.*

(ii) φ *est* p*-isomorphique en tout point de l'ensemble réduit* $\rho_e(V)$ *qui n'appartient pas à* $X^0 = \overline{\rho}(X)$.

(iii) *La* (W, p, k^0)*-provariété* $Y = \varphi_g(X)$ *est* simple.

(iv) φ *est génériquement promorphique d'indice* λ *sur* X.

Par récurrence sur λ, il nous suffira de démontrer le théorème suivant :

Théorème 3.* — *Soient* V $(\subset \mathbf{P}_n)$, X, X^0 *et* λ *comme dans le théorème 3. Supposons de plus* $\lambda > 0$. *Alors toute transformation* p*-monoïdale* ξ *de centre* X^0 *de l'espace projectif* $\mathbf{P}_n$ *induit un k-isomorphisme* $\varphi : V \to W$ *vérifiant les propriétés suivantes*

(iii*) *Si* $Y = \varphi_g(X)$, *on a* $l(Y) = l(Y, W) < \lambda$.

(iv*) φ *est génériquement promorphique d'indice 1 sur* X.

En effet, les conditions (i) et (ii) sont automatiquement vérifiées par un tel modèle, d'après les propriétés des transformations p-monoïdales.

Il résultera en même temps du théorème 3* que *la désingularisation de* X *est réalisable par le produit d'un nombre fini* $(\leqslant \lambda)$ *de transformations* p*-monoïdales.*

Démonstration du théorème 3.* — Posons en effet $I = \mathscr{I}_R(X^0)$. La transformation p-monoïdale ξ est de la forme $\xi = \xi_s(\mathscr{B}, I_s)$, où s est un entier $\geqslant s_0(I)$, où I_s est le R-module $I \cap M_s$, et où $\mathscr{B} = (P_0, \ldots, P_m)$ est un système de générateurs de I_s. (Cf. les notations du n° 25.)

Soit $u=(u_0, \ldots, u_n)$ un point générique de X sur k^0. On peut supposer qu'on a $u_i \in R$ pour tout i, et $\inf_i v(u_i)=0$, soit, par exemple, $v(u_0)=0$. Le point réduit $u^0=\rho(u)$, générique de X^0 sur k^0, a pour système de coordonnées $(u_0^0, \ldots, u_n^0)$, où $u_i^0=\rho(u_i)$ pour tout i, avec $u_0^0 \neq 0$.

Soit $\bar{u}$ un point générique de V sur $\mathfrak{k}$. La variété $W=\xi(V)$ est, par définition de ξ, le lieu sur k du point $\bar{v}=\bar{u}\times\bar{w}$, où $\bar{w}$ est le point de $\mathbf{P}_m$ ayant pour coordonnées les $\bar{w}_j=P_j(\bar{u})$ $(1 \leqslant j \leqslant m)$. Puisqu'on a $u^0 \in X^0$, on a $v(P_j(u))>0$ pour tout j. Puisque ${}^tM_s \subset I_s$, on a $\inf_j v(P_j(u))=1$. On peut supposer qu'on a, par exemple, $v(P_0(u))=1$.

La variété V admet pour représentant affine au point u la sous-variété V_0 de $\mathbf{S}_n$ lieu du point $\bar{x}$ ayant pour coordonnées les $\bar{x}_i=\bar{u}_i/\bar{u}_0$ $(1 \leqslant i \leqslant n)$. Soit X_0 la $(V_0, \mathfrak{p}, k^0)$-provariété qui représente X dans V_0, c'est-à-dire le lieu sur k^0 du point x de $\mathfrak{R}_n$ ayant pour coordonnées les $x_i=u_i/u_0$. Notons, pour tout j $(0 \leqslant j \leqslant m)$, Q_j le polynôme défini par $Q_j(U_1, \ldots, U_n)=P_j(1, U_1, \ldots, U_n)$. Posons $X_0^0=\bar{\rho}(X_0)$.

Puisque les P_j forment un système de générateurs de I, les Q_j forment un système de générateurs de l'idéal maximal $\mathfrak{m}=\mathfrak{m}(X_0^0, \mathbf{S}_n)$ de l'anneau local $\mathfrak{o}=\mathfrak{o}(X_0^0, \mathbf{S}_n)$. La dimension de $\mathfrak{o}$ est $n-q+1$, en posant $q=\dim X_0^0=\dim X^0$. On peut supposer qu'on a mis les indices de façon que $Q_0, \ldots, Q_{n-q}$ forment un système *minimal* de générateurs de $\mathfrak{m}$.

Soient $\bar{z}$ et z les points de $\mathbf{S}_{n-q}$ ayant respectivement pour coordonnées les $\bar{z}_j=Q_j(\bar{x})/Q_0(\bar{x})$, et les $z_j=Q_j(x)/Q_0(x)$ $(1 \leqslant j \leqslant n-q)$; posons $z^0=\rho(z)$. Soit W_0 la variété lieu sur k du point $\bar{y}=\bar{x}\times\bar{z}$, dans l'espace affine $\mathbf{S}_{2n-q}=\mathbf{S}_n\times\mathbf{S}_{n-q}$, et soit φ_0 l'application rationnelle $\varphi_0 : V_0 \to W_0$, définie sur k, telle que $\bar{y}=\varphi_0(\bar{x})$. Notons y le point $y=\varphi_0(x)=x\times z$ de $(W_0)_{\mathfrak{R}}$; d'après le théorème 1, $Y_0=\mathrm{loc}_{k^0} y=(\varphi_0)_g(X_0)$ est une $(W_0, \mathfrak{p}, k_0)$-provariété; cette provariété Y_0 est celle qui représente Y dans W_0.

Puisque $Q_0, \ldots, Q_{n-q}$ forment un système de générateurs de $\mathfrak{m}$, l'application $\theta : W_0 \to W$, telle que $\theta(\bar{y})=\bar{v}$ est p-isomorphique au point $y^0=\rho(y)=(x^0, z^0)$. Ceci nous permet de remplacer W par W_0. Il nous suffit de montrer que les conditions (iii*) et (iv*) sont vérifiées par le k-modèle affine (W_0, φ_0) de V_0, relativement à la $(V_0, \mathfrak{p}, k^0)$-provariété X_0. Or, la relation $v(P_0(u))=1$ entraîne $v(Q_0(x))=1$, et (iv*) s'en déduit aussitôt. Il reste à démontrer (iii*).

Introduisons pour cela un système de polynômes $G_\beta(X)$ appartenant à $\mathfrak{I}(V_0)$, tels que les $(dG_\beta)_x$ forment une base standard du $\mathfrak{R}$-module $\bar{D}(V_0, x, \mathbf{S}_n)$ (cf. n° 17). Il existe donc des entiers m_β tels que $\Sigma_\beta m_\beta=\lambda$, et que les $\varphi_\beta=t^{-m_\beta}(dG_\beta)_x$ soient des éléments linéairement indépendants du $\mathfrak{R}$-module $D(x, \mathbf{S}_n)$. Pour tout β, notons d'autre part s_β la « p-multiplicité » de X_0^0 sur l'hypersurface $G_\beta(X)=0$ de $\mathbf{S}_n$, c'est-à-dire le plus petit entier qui vérifie la condition $G_\beta \in \mathfrak{m}^{s_\beta}$. Remarquons que, pour tout β tel que $m_\beta \geqslant 1$, on a aussi $s_\beta \geqslant 2$; en effet, pour un tel β, le point x^0 est multiple sur l'hypersurface réduite $G_\beta^0(X)=0$; donc, d'après la proposition 6 du n° 10, x^0 est p-multiple sur l'hypersurface $G_\beta(X)=0$.

Considérons l'idéal $\mathfrak{I}(W_0)$ de l'anneau $\mathfrak{R}[X, Z]=\mathfrak{R}[X_1, \ldots, X_n, Z_1, \ldots, Z_{n-q}]$. Cet idéal contient les polynômes G_β $(1 \leqslant \beta \leqslant n-r)$ et $Q_j'=Q_0Z_j-Q_j$ $(1 \leqslant j \leqslant n-q)$.

D'autre part, G_β appartient à la puissance s_β-ième de $\mathfrak{m} = (Q_0, \ldots, Q_{n-q})$. On a donc, pour tout β, dans l'anneau $\mathfrak{R}[X, Z]$, une congruence de la forme

$$H_\beta G_\beta \equiv Q_0^{s_\beta} G'_\beta \qquad (\text{mod. } Q'_1, \ldots, Q'_{n-1}),$$

où les G'_β sont des éléments de $\mathscr{I}(W)$, et où les H_β sont des éléments de $\mathfrak{R}[X_1, \ldots, X_n]$, tels que $v(H_\beta(x)) = 0$ $(1 \leqslant \beta \leqslant n-r)$.

Le $\mathfrak{R}$-module $\overline{D}(W_0, y, \mathbf{S}_{2n-q})$ est un sous-module libre, de rang $2n-r-q$, du $\mathfrak{R}$-module $M = D^1(y, \mathbf{S}_{2n-q})$ (puisque y est simple sur W). Ce module M contient les $(dQ'_j)_y$ et les $(dG'_\beta)_x$ (en convenant d'identifier canoniquement $D^1(x, \mathbf{S}_n)$ à un sous-$\mathfrak{R}$-module de $M = D^1(y, \mathbf{S}_{2n-q})$). On déduit des relations précédentes

$$(40) \qquad \begin{cases} (dQ'_j)_y = Q_0(x)(dZ_j)_y - (dQ_j)_x & (1 \leqslant j \leqslant n-q) \\ (dG'_\beta)_x \equiv (Q_0(x))^{-s_\beta} H_\beta(x)(dG_\beta)_x \quad (\text{mod. } M') & (1 \leqslant \beta \leqslant n-r) \end{cases}$$

où M' est le sous-$\mathfrak{R}$-module de M engendré par les $(dQ'_j)_y$. Puisque les

$$\varphi_\beta = t^{-m_\beta}(dG_\beta)_x \qquad (1 \leqslant \beta \leqslant n-r)$$

sont des éléments indépendants du $\mathfrak{R}$-module $D^1(x, \mathbf{S}_n)$, et puisqu'il en est de même des $(dQ_j)_x$, (les $(dQ_j)^0_{x^0}$ étant k^0-indépendants), on peut trouver une $\mathfrak{R}$-base $\mathscr{B}_0$ de $D^1(x, \mathbf{S}_n)$ contenant les φ_β $(1 \leqslant \beta \leqslant n-r)$, et $r-q$ éléments pris parmi les $(dQ_j)_x$. La réunion $\mathscr{B}'_0$ de $\mathscr{B}_0$ et des $(dZ_j)_y$ est alors une $\mathfrak{R}$-base de M. D'après les relations (40), l'un des déterminants d'ordre $2n-r-q$ de la matrice des éléments $(dQ'_j)_y$, $(dG'_\beta)_x$ de M relativement à la base $\mathscr{B}'_0$ a pour valeur

$$\Delta = \varepsilon t^{-a}(Q_0(x))^b \prod\nolimits_\beta H_\beta(x)$$

avec $\varepsilon = \pm 1$, $a = \Sigma_\beta m_\beta = \lambda$, et $b = n-r-\Sigma_\beta s_\beta$. Comme on a $v(Q_0(x)) = 1$, et $v(H_\beta(x)) = 0$ pour tout β, on a

$$v(\Delta) = \lambda + n - r - \Sigma_\beta s_\beta = \lambda + \Sigma_\beta(1 - s_\beta).$$

Comme on a supposé $\lambda = \Sigma_\beta m_\beta > 0$, l'un au moins des m_β est >0. Donc, d'après la remarque précédente, l'un au moins des entiers positifs $s_\beta - 1$ est >0. Donc on a $v(\Delta) < \lambda$, d'où $l(Y_0, W) = l(y, W) < \lambda$, ce qui montre bien que notre modèle (W_0, φ_0) vérifie la condition (iii*). C.Q.F.D.

Théorème 4. — Soit V *une variété projective définie sur k, et soit* X *une* (V, p, k^0)*-provariété. Alors il existe un k-modèle projectif* (W, φ) *de* V *vérifiant les conditions* (i), (ii) *et* (iii) *du théorème 3, et, de plus, la condition suivante*

(iv') *La k^0-variété* $Y^0 = \overline{\rho}(Y)$ *réduite de* $Y = \varphi_g(X)$ *est de dimension* $r = \dim V$ (*i.e. est une composante du cycle* $W^0 = \rho(W)$).

On se ramène, d'après le théorème 3, au cas où X est simple. Il suffit alors de démontrer le théorème suivant :

Théorème 4. — Soit* V *une variété projective* ($V \subset \mathbf{P}_n$), *définie sur k, de dimension r, et soit* X *une* (V, p, k^0)*-provariété simple, d'indice* μ. *Posons* $X^0 = \overline{\rho}(X)$, *et* $q = \dim X^0$. *Supposons de plus* $q < r$. *Soit* ξ^* *une transformation* p*-monoïdale de centre* X^0 *de* $\mathbf{P}_n$, *et soit* $\varphi : V \to W$

le k-isomorphisme induit par ξ^*. *Alors la* $(W, \mathfrak{p}, k^0)$*-provariété* $Y = \varphi_g(X)$ *est simple, d'indice* μ, *et, si on pose* $X^\mu = \bar{\rho}^\mu(X)$, $Y^\mu = \bar{\rho}^\mu(Y)$, *on a* $\dim Y^\mu > \dim X^\mu$.

En effet, le théorème 4 en résultera immédiatement, par récurrence sur l'entier $\dim X^\mu$.

Nous dirons qu'un modèle (W, φ) de V vérifiant les conditions du théorème 4 est *obtenu en faisant éclater* X. Il résultera du théorème 4* qu'un tel modèle peut encore être obtenu en appliquant à V le produit d'un nombre fini de transformations $\mathfrak{p}$-monoïdales.

*Démonstration du théorème 4**. — On peut reprendre toutes les notations de la démonstration du théorème 3 et, en particulier, considérer à nouveau les variétés affines V_0 et W_0, ainsi que les provariétés X_0 et Y_0. Si on pose $X_0^\mu = \bar{\rho}^\mu(X_0)$, et $Y_0^\mu = \bar{\rho}^\mu(Y_0)$, il nous suffit de montrer qu'on a $\dim Y_0^\mu > \dim X_0^\mu$.

Or φ est génériquement promorphique d'indice 1 sur X, et on a donc une application rationnelle $\varphi^{\mu-1,\mu} : X^\mu \to Y^{\mu-1}$, canoniquement déduite de φ, qui induit une application linéaire affine $\psi^\mu : L^\mu(x^\mu) \to L^{\mu-1}(y^{\mu-1})$ (cf. n° 24, remarque faisant suite à la proposition 24). D'autre part, on a vu que la variété linéaire $L^\mu(x^\mu)$ (resp. $L^\mu(y^\mu)$) est, pour tout $\mu \geqslant 0$, de la forme $x^\mu \times L_0^\mu(x^\mu)$ (resp. $y^\mu \times L_0^\mu(y^\mu)$) où $L_0^\mu(x^\mu)$ (resp. $L_0^\mu(y^\mu)$) est une sous-variété linéaire de dimension r de $\mathbf{S}_n^0$ (resp. de $\mathbf{S}_{2n-q}^0$) déduite de $L_0(x)$ (resp. $L_0(y)$) par une translation rationnelle sur $k_0(x^\mu)$ (cf. n° 21, démonstration de la proposition 21). Comme on a $m(x) = m(y) = 0$, les variétés $L_0(x)$ et $L_0(y)$ coïncident respectivement avec les variétés linéaires tangentes (réduites à l'origine) à V_0^0 en x^0 et à W_0^0 en y^0. En appliquant la formule de Taylor aux expressions des coordonnées de y, on trouve que l'application $\psi_0 : L_0(x) \to L_0(y)$, transposée de ψ^μ, est celle qui, au point $(dX_1, \ldots, dX_n)$, fait correspondre le point $(dX_1, \ldots, dX_n, dZ_1, \ldots, dZ_{n-q})$ défini par $dZ_j = \Sigma_i \left(\left(\frac{\partial f_j}{\partial X_i} \right)^0 (x^0) \right) dX_i$, où l'on pose $f_j = tQ_j/Q_0 \; (1 \leqslant j \leqslant n-q)$. Or $f_0 = t, f_1, \ldots, f_{n-q}$ sont des générateurs de $\mathfrak{m} = \mathfrak{m}(X^0, V)$. Il en résulte que le noyau de ψ_0 est la variété linéaire tangente (réduite à l'origine) à X^0 en x^0. Ce noyau est donc de dimension $q = \dim X^0$. Donc, les applications linéaires ψ_0 et ψ^μ sont de rang $r - q$. Comme on a $k^0(x^\mu) \subset k^0(y^\mu) \subset k^0(x^{\mu+1})$, le degré de transcendance de $k^0(x^{\mu+1})$ sur $k^0(y^\mu)$ est égal à q. Or celui de $k^0(x^{\mu+1})$ sur $k^0(x^\mu)$ est égal à r. Donc celui de $k^0(y^\mu)$ sur $k^0(x^\mu)$ est $r - q$. Autrement dit, on a :

$$\dim Y^\mu = \dim X^\mu + r - q \tag{41}$$

d'où $\dim Y^\mu > \dim X^\mu$. C.Q.F.D.

Remarques. — *a)* Les théorèmes 3 et 4 sont applicables aussi à toute sous-variété d'une variété projective et, en particulier, à toute variété affine. Ils restent valables pour une $\mathfrak{p}$-variété quelconque lorsqu'on supprime, dans chacun d'eux, la condition (iii).

b) Dans le cas particulier où X est simple, d'indice 0, la relation (41) devient $\dim Y^0 = \dim X^0 + r - q$, autrement dit $\dim Y^0 = r$. Donc, on obtient le modèle (W, φ) du théorème 4 au moyen d'une seule transformation $\mathfrak{p}$-monoïdale, de centre X^0.

c) On peut trouver un modèle de V vérifiant les conditions de l'un quelconque des deux théorèmes 3 ou 4, et qui, de plus, est $\mathfrak{R}$-*normal*, c'est-à-dire tel que les anneaux locaux de tous les points de V et de $\rho_e(V)$ soient intégralement clos. Il suffit, en effet, de « p-normaliser » le modèle (W, φ) de V, de la manière habituelle. Nous n'aurons pas à utiliser cette remarque dans la suite.

Corollaire. — *Soit* V *une variété projective, définie sur k, et soient* X_i $(1 \leqslant i \leqslant h)$ *des* (V, p, k^0)*-provariétés en nombre fini h. Alors il existe un k-modèle* (W, φ) *de* V, *vérifiant, pour chacune des* X_i, *les conditions* (i), (ii) et (iv') *du théorème 4, et vérifiant en outre la condition suivante :*

(iii') φ *est* p*-isomorphique en tout point de* supp V^0 *n'appartenant pas à la réunion des* $X_i^0 = \bar{\rho}(X_i)$.

Ce corollaire s'obtient par récurrence sur *h*. Considérons en effet un *k*-modèle (W_{h-1}, φ_{h-1}) de V vérifiant les conditions précédentes relativement aux provariétés $X_1, \ldots, X_{h-1}$. Posons, pour $1 \leqslant i \leqslant h$, $Y_i = (\varphi_{h-1})_g(X_i)$, et $Y_i^0 = \bar{\rho}(Y_i)$. On peut construire un *k*-modèle (W_h, ψ_h) de W_{h-1} vérifiant les conditions du théorème 4, relativement à la $(W_{h-1}, \mathfrak{p})$-provariété Y_h. Posons $\varphi_h = \psi_h \circ \varphi_{h-1}$, et montrons que le *k*-modèle (W_h, φ_h) vérifie les conditions voulues relativement à $X_1, \ldots, X_h$. En effet, la condition (i) est satisfaite, ainsi que les conditions (ii) et (iv') relatives à X_h. On peut supposer que Y_h n'est pas simple, ou bien qu'elle est simple, mais telle que $\dim Y^0 < r = \dim V$. Dans ces conditions, Y_h^0 ne peut contenir aucune des Y_i^0 $(1 \leqslant i \leqslant h-1)$ et, puisque le modèle (W_h, ψ_h) vérifie (iii), ψ_h est génériquement p-isomorphique sur $Y_1, \ldots, Y_{h-1}$. Donc le modèle (W_h, φ_h) vérifie les conditions (ii) et (iv') relativement à $X_1, \ldots, X_{h-1}$. Enfin, soit x^0 un point de supp V^0 n'appartenant à aucune des variétés $X_i^0 = \rho(X_i)$. Alors, puisque le modèle (W_{h-1}, φ_{h-1}) de V vérifie (iii') relativement à $X_1, \ldots, X_{h-1}$, φ_{h-1} est p-isomorphique en x^0; comme $x^0 \notin X_h^0$, le point $y^0 = \varphi_{h-1}^0(x^0)$ n'appartient pas à l'image $(\varphi_{h-1})_e^0(X_h^0)$. Donc on a $y^0 \notin Y_h^0$. Donc ψ_h est p-isomorphique en y^0, donc $\varphi_h = \psi_h \circ \varphi_{h-1}$ est p-isomorphique en x^0. Donc, le modèle (W_h, φ_h) vérifie (iii'). C.Q.F.D.

Théorème 5. — *Supposons que k est un corps global, et que* $\mathfrak{p} \in \mathfrak{S}(k)$. *Les modèles* (W, φ) *de* V *construits dans les théorèmes 3 et 4, et dans le corollaire au théorème 4, peuvent être choisis tels que* φ *soit un* $R_\mathfrak{q}$*-isomorphisme pour tout* $\mathfrak{q} \in \mathfrak{S}$ *distinct de* p.

Démonstration. — La construction du modèle (W, φ) s'effectue, dans chaque cas, au moyen d'un nombre fini de transformations p-monoïdales. A chaque étape de la construction (cf. théorèmes 3* et 4*), la transformation peut être choisie arbitrairement parmi toutes celles de centre X^0; il suffit de choisir une transformation *strictement* p-monoïdale (ce qui est possible, d'après la proposition 25).

Théorème 6. — *Soit* V *une variété projective sans point multiple, de dimension r, définie sur k. Alors, il existe un ensemble fini de k-modèles* (W_i, φ_i) *de* V *et pour tout i, un* (V, p, k^0)*-ensemble* S_i, *tels que les conditions suivantes soient satisfaites :*

(i) *Les* S_i *recouvrent* $V_\mathfrak{R} = V_\mathfrak{I}$.

(ii) *Les* $(W_i, \mathfrak{p})$*-ensembles* $T_i = \varphi_i(S_i)$ *ne contiennent que des points simples* (mod. p).

Démonstration. — Supposons $V \subset \mathbf{P}_n$. Soit μ un entier $\geqslant l_0(V)$. Commençons par considérer une sous-k^0-variété arbitraire X^μ de $(\mathbf{P}_n)^\mu_{\mathfrak{R}} = \rho^\mu(\mathbf{P}_n)$, génériquement contenue dans $V^\mu_{\mathfrak{R}} = \rho^\mu(V_{\mathfrak{R}})$, et la $(V, \mathfrak{p}, k^0)$-provariété $X = (X^\mu)^\#_g$ obtenue en relevant génériquement X^μ. On peut associer à X^μ un modèle (W, φ) vérifiant, relativement à V et X, les conditions du théorème 3. Alors $Y = \varphi_g(X)$ est une $(W, \mathfrak{p}, k^0)$-provariété simple, et φ est génériquement promorphique d'indice μ sur S. On peut, d'après la proposition 24 du n° 24, trouver un k^0-ouvert $S^\mu = \mathscr{U}(X^\mu)$ de X^μ, tel que $S = (S^\mu)^\#$ soit un $(V, \mathfrak{p}, k^0)$-ensemble k^0-irréductible, d'adhérence X, et que φ soit promorphique d'indice μ sur S. L'application rationnelle $\varphi^{0\mu} : X^\mu \to Y^0$, canoniquement déduite de φ, est alors, en particulier, morphique en tout point de S^μ. Comme Y^0 est génériquement simple sur $W^0 = \rho(W)$, on peut, en remplaçant éventuellement S^μ par un ouvert plus petit de X^μ, supposer que $\varphi^{0\mu}(S^\mu) = T^0$ est contenu dans l'ensemble $\mathscr{S}(W^0)$ des points simples sur W^0. Le $(W, \mathfrak{p}, k^0)$-ensemble $T = \varphi(S)$ ne contient alors que des points simples (mod. $\mathfrak{p}$). Il suffit, pour obtenir le théorème, d'appliquer le lemme 2 du n° 24 au sous-ensemble k^0-constructible $V^\mu_{\mathfrak{R}}$ de $(\mathbf{P}_n)^\mu_{\mathfrak{R}}$, et à la famille $\mathscr{U}(X^\mu)$.

Remarque. — Le théorème 6 est valable également pour les sous-variétés des variétés projectives, et, en particulier, pour les variétés affines.

28. Symbole $\nu(X, \omega)$.

Soit V une $\mathfrak{p}$-variété de dimension r, définie sur k, et considérons une k-différentielle ω de degré r sur V. Soit k_1^0 un sous-corps de $\mathfrak{k}^0$, contenant k^0, et posons $k_1 = (k_1^0)^\#$; soit X une $(V, \mathfrak{p}, k_1^0)$-provariété. D'après le théorème 4, il existe un k_1-modèle (W, φ) de V tel que la $(W, \mathfrak{p}, k_1^0)$-provariété $Y = \varphi_g(X)$ soit simple, et que $Y^0 = \overline{\rho}(Y)$ soit une composante (nécessairement simple) de W^0. Considérons alors l'entier $\nu(Y^0, \omega)$ (cf. n° 16). Cet entier ne dépend pas du choix du modèle (W, φ), mais seulement de V, X, et ω. En effet, soit (W', φ') un autre modèle vérifiant les mêmes conditions. Soit x un point générique de X sur k_1^0, et considérons les points $y = \varphi(x)$ et $y' = \varphi'(x)$; ces points sont génériques sur k_1^0 de $Y = \varphi_g(X)$ et $Y' = \varphi'_g(X)$ respectivement. Posons $x^0 = \rho(x)$, $y^0 = \rho(y)$, et $y'^0 = \rho(y')$. Considérons l'application rationnelle, définie sur k_1 : $\psi = \varphi' \circ \varphi^{-1} : W \to W'$. Puisque le couple (y, y') appartient au graphe Γ_ψ de ψ, le couple (y^0, y'^0) appartient à $\rho_e(\Gamma_\psi)$, i.e. on a $y'^0 \in \psi^0_e(y^0)$. D'autre part, y^0 (resp. y'^0) est, par construction, générique sur k_1^0 d'une composante simple Y^0 (resp. Y'^0) de $W^0 = \rho(W)$ (resp. $W'^0 = \rho(W')$). D'après la proposition 8 du n° 11, ψ est donc $\mathfrak{p}$-isomorphique en y^0, de valeur y'^0. On a donc, d'après la proposition 15 du n° 16, $\nu(Y^0, \omega) = \nu(Y'^0, \omega)$. Autrement dit, l'entier $\nu(Y^0, \omega)$ ne dépend que de V, ω et X. Nous le désignerons par $\nu(X, \omega)$, ou $\nu(X, \omega, V)$.

D'après cette définition, si $\varphi : V \to V'$ est un k-isomorphisme, et si $X' = \varphi_g(X)$, on a $\nu(X, \omega) = \nu(X', \omega)$. On remarquera aussi qu'on a $\nu(X, \omega) = \nu(X_i, \omega)$ si X_i est l'une quelconque des composantes absolument irréductibles de X.

Proposition 26. — *Soit* V *une* $\mathfrak{p}$*-variété, définie sur* k*, de dimension* r*, et soit* ω *une* k*-différentielle de degré* r *sur* V. *Soit* X *une* $(V, \mathfrak{p}, k^0)$*-provariété simple, et soit* C^0 *la composante*

simple de V^0 *qui contient* $X^0=\overline{\rho}(X)$. *Supposons que* X^0 *n'est pas contenue dans* $\rho_e((\omega)_\infty)$. *Alors, en posant* $q=\dim X^0$, *on a* $\nu(X,\omega)\geqslant\nu(C^0,\omega)+r-q$.

Démonstration. — En effet, soit (W,φ) un k-modèle de V qui vérifie, relativement à V et X, les conditions du théorème 4. Soit x un point générique de X sur k^0. Posons $y=\varphi(x)$, et $Y=\varphi_g(X)=\mathrm{loc}_{k^0}y$. Les points $x^0=\rho(x)$ et $y^0=\rho(y)$ sont génériques sur k^0 de $X^0=\overline{\rho}(X)$ et $Y^0=\overline{\rho}(Y)$ respectivement, et on a, par construction, $\dim Y^0=r$. Puisque φ^{-1} est un R-morphisme, φ^{-1} induit un k^0-morphisme $\psi^0: Y^0\to X^0$, tel qu'on ait $x^0=\psi^0(y^0)$. Soient $(u_1,\ldots,u_r)$ (resp. $(v_1,\ldots,v_r)$) des fonctions sur V (resp. W) définies sur k^0, induisant des paramètres uniformisants de C^0 en x^0 (resp. de Y^0 en y^0). Puisqu'on a $\dim Y^0=r$, et $\dim X^0=q$, la matrice $\left(\left(\frac{\partial u_i}{\partial v_j}\right)^0(y^0)\right)$ est de rang q.

Donc le déterminant $D=D(u_1,\ldots,u_r)/D(v_1,\ldots,v_r)$, regardé comme fonction sur W, est tel que

$$v(D(y))\geqslant r-q \tag{42}$$

Notons ω^* la différentielle sur W transposée de ω par φ et soient f et g des fonctions sur V et W respectivement, telles qu'on ait $\omega=f du_1\wedge\ldots\wedge du_r$, et $\omega^*=g dv_1\wedge\ldots\wedge dv_r$. Alors on a

$$g(y)=f(x)D(y) \tag{43}$$

Or on a $\nu=\nu(C^0,\omega)=\nu(C^0,f)$. Puisque $x^0\notin\rho_e((\omega)_\infty)$ on a aussi $x^0\notin\rho_e((f)_\infty)$, d'après la proposition 14 du n° 16, et, en posant $f'=ft^{-\nu}$, on a $x^0\notin\{f'\}_{\mathfrak{p},\infty}$, donc f' est $\mathfrak{p}$-morphique en x^0. Donc on a $v(f(x))\geqslant\nu$. D'autre part, puisque y^0 est générique, sur k^0, de la k^0-composante Y^0 de $W^0=\rho(W)$, on a $\nu(Y^0,\omega)=\nu(Y^0,g)=v(g(y))$. D'après les relations (42) et (43), on a donc bien

$$\nu(Y^0,\omega)\geqslant\nu(C^0,\omega)+r-q$$

29. Provariétés ω-maximales.

Théorème 7. — *Soit* V *une* $\mathfrak{p}$*-variété de dimension* r, *sans point multiple, définie sur* k, *et soit* ω *une* k*-différentielle de degré* r *sur* V, *telle que* $(\omega)_\infty=0$, *c'est-à-dire n'admettant aucun pôle. A tout* $\mathfrak{k}$*-modèle* (W,φ) *de* V, *et à toute composante simple* C^0 *de* $W^0=\rho(W)$, *associons l'entier* $\nu(C^0,\omega,W)$. *Cet entier admet une borne inférieure* $\nu_0=\nu_0(\omega,V)$, *qui ne dépend que de* V *et* ω, *mais non du modèle* (W,φ), *ni de la composante* C^0.

Pour V *et* ω *fixées, associons d'autre part à toute* $(V,\mathfrak{p})$*-provariété* X *l'entier* $\nu(X,\omega,V)$. *Cet entier admet également pour borne inférieure* ν_0.

Démonstration. — Considérons un recouvrement fini de $V_{\mathfrak{R}}$ par des $(V,\mathfrak{p},k^0)$-ensembles S_i, et, pour tout i, un k-modèle (W_i,φ_i), tels que les conditions du théorème 6 soient satisfaites. Appelons ν_0 le plus petit des entiers $\nu(C_{ij}^0,\omega,W_i)$ obtenus pour tous les couples (i,j) possibles, en notant, pour chaque i, C_{ij}^0 $(1\leqslant j\leqslant m_i)$ les composantes simples de $W_i^0=\rho(W_i)$.

Montrons d'abord que l'entier $\nu(X,\omega)=\nu(X,\omega,V)$ admet ν_0 comme borne

inférieure. En effet, soit k_1^0 un corps sur lequel X est définie, et soit x un point générique de X sur k_1^0. Le point x appartient à l'un des S_i, et le point $y_i = \varphi_i(x)$ de $(W_i)_{\mathfrak{R}}$ est simple (mod. p). Donc la (W_i, p)-provariété $Y_i = (\varphi_i)_g(X) = \mathrm{loc}_{k_1^0} y_i$ est simple. Si C_{ij}^0 est la composante de $W_i^0 = \rho(W_i)$ contenant $Y_i^0 = \overline{\rho}(Y_i)$, on a donc, d'après la proposition 26, $\nu(X, \omega, V) = \nu(Y_i, \omega, W_i) \geqslant \nu(C_{ij}^0, \omega, W_i)$. On a donc bien $\nu(X, \omega, V) \geqslant \nu_0$. Ce minorant ν_0 est atteint si on prend pour X la provariété obtenue en relevant l'une des composantes C_i^0 pour lesquelles on a $\nu(C_{ij}^0, \omega, W_i) = \nu_0$.

La première partie de l'énoncé en résulte aussitôt, puisqu'on a $\nu(C^0, \omega, W) = \nu(Y, \omega)$, où Y est la (W, p)-provariété obtenue en relevant C^0.

Soit V une variété définie sur k, de dimension r, et soit ω une k-différentielle sur V, dépourvue de pôles. Soit k_1^0 un sous-corps de $\mathfrak{k}^0$ contenant k^0, et soit C^0 une k_1^0-composante de V^0. On dira que C^0 est *ω-maximale* si on a $\nu(C^0, \omega, V) = \nu_0(\omega, V)$. Soit x^0 un point de $\rho_e(V)$, simple sur $V^0 = \rho(V)$, et n'appartenant pas à $\rho_e((\omega)) = \rho_e((\omega)_0)$; on dira que x^0 est *ω-maximal* si l'unique composante C^0 de V^0 contenant x^0 est ω-maximale ou, ce qui est équivalent, si on a $\nu(x^0, \omega) = \nu_0$, où $\nu(x^0, \omega)$ est le symbole introduit au n° 16. Si un k-isomorphisme $\varphi : V \to W$ est génériquement p-isomorphique sur C^0 (resp. p-isomorphique en x^0), la composante $\varphi_g^0(C^0)$ de W^0 (resp. le point $y^0 = \varphi^0(x^0)$) est encore ω-maximale (resp. ω-maximal). Pour que C^0 soit ω-maximale, il faut et il suffit que chacune de ses composantes irréductibles (au sens absolu) soit ω-maximale. Un point $x \in V_{\mathfrak{R}}$ simple (mod. p), et n'appartenant pas à $\mathrm{supp}(\omega) = \mathrm{supp}(\omega)_0$ sera dit *ω-maximal* (mod. p) si le point $x^0 = \rho(x)$ est ω-maximal.

Proposition 27. — Soit V *une* p*-variété, définie sur* k*, de dimension* r*, sans point multiple, et soit* ω *une* k*-différentielle de degré* r *sur* V*, dépourvue de pôles. Soit* k_1^0 *un sous-corps de* $\mathfrak{k}^0$ *contenant* k^0*. Soit* X *une* (V, p, k_1^0)*-provariété simple, maximale au sens de l'inclusion (i.e. de la forme* $(X^0)_g^{\sharp}$*, où* X^0 *est une* k_1^0*-composante simple de* $V^0 = \rho(V)$*), et telle, de plus, qu'on ait* $\nu(X, \omega, V) = \nu_0(\omega, V)$*. Soit* (W, φ) *un* k*-modèle de* V *tel que la* (W, p, k_1^0)*-provariété* $Y = \varphi_g(X)$ *soit simple. Alors* Y *est également maximale au sens de l'inclusion, et* φ *est génériquement* p*-isomorphique sur* $X^0 = \overline{\rho}(X)$*, de valeur* $Y^0 = \overline{\rho}(Y)$.

Démonstration. — En effet, d'après la proposition 26, et la définition du symbole $\nu(Y, \omega)$, on a nécessairement $\dim Y^0 = r$. De plus, soient x un point générique de X sur k_1^0, et y un point générique de Y sur k_1^0, tels qu'on ait $y = \varphi(x)$. Les points $x^0 = \rho(x)$ et $y^0 = \rho(y)$ sont génériques sur k^0 de X^0 et Y^0 respectivement. D'après la proposition 8 du n° 11, φ est donc p-isomorphique en x^0, de valeur y^0. Puisqu'on a $X = (X^0)_g^{\sharp}$, on a aussi $Y = (Y^0)_g^{\sharp}$. C.Q.F.D.

Soient encore V une p-variété, définie sur k, de dimension r, sans point multiple, et ω une k-différentielle de degré r sur V, dépourvue de pôles. On dit qu'une (V, p)-provariété X est *ω-maximale* si on a $\nu(X, \omega, V) = \nu_0(\omega, V)$, et s'il existe un k-modèle (W, φ) de V tel que $Y = \varphi_g(X)$ soit simple, et soit maximale au sens de l'inclusion. D'après la proposition précédente, il en est de même pour tout autre modèle (W', φ') de V tel que $Y' = \varphi'_g(X)$ soit simple.

On remarquera que, pour qu'une k_1^0-composante simple C^0 de $V^0 = \rho(V)$ soit ω-maximale, il faut et il suffit que la $(V, \mathfrak{p}, k_1^0)$-provariété $(C^0)_g^\#$ soit ω-maximale.

Théorème 8. — Soit V *une variété projective, définie sur k, de dimension r, sans point multiple, et soit* ω *une k-différentielle de degré r sur* V, *dépourvue de pôles. Alors il n'existe qu'un nombre fini de* $(V, \mathfrak{p})$*-provariétés* ω*-maximales.*

Démonstration. — Considérons à nouveau un recouvrement de $V_{\mathfrak{R}} = V_{\mathfrak{k}}$ par des $(V, \mathfrak{p})$-ensembles S_i, et, pour tout i, un k-modèle (W_i, φ_i), tels que les conditions du théorème 6 soient satisfaites. Soit X une $(V, \mathfrak{p})$-provariété ω-maximale. Alors X est génériquement contenue dans l'un des S_i, et la $(W_i, \mathfrak{p})$-provariété $Y_i = (\varphi_i)_g(X)$ est simple. D'après la proposition 27 elle est maximale au sens de l'inclusion, i.e. coïncide avec la $(W_i, \mathfrak{p})$-provariété obtenue en relevant génériquement l'une des composantes de $W_i^0 = \rho(W_i)$, d'où le théorème.

Théorème 9. — Soit V *une variété projective, définie sur k, de dimension r, sans point multiple, et soit* ω *une k-différentielle de degré r sur* V, *dépourvue de pôles. Alors, il existe un k-modèle projectif* (W, φ) *de* V *tel que toutes les* $(V, \mathfrak{p})$*-provariétés* ω*-maximales soient simples (ces provariétés sont alors toutes celles de la forme* $(C_i^0)_g^\#$, *où les* C_i^0 *sont les composantes simples* ω*-maximales de* $V^0 = \rho(V)$).

Démonstration. — Il suffit en effet d'appliquer le corollaire du théorème 4 à l'ensemble (fini, d'après le théorème 8) des $(V, \mathfrak{p}, k^0)$-provariétés ω-maximales.

En outre, dans le cas particulier où k est un corps global, et où $\mathfrak{p} \in \mathfrak{S}(k)$, on peut choisir ce modèle de manière que φ soit un $R_\mathfrak{q}$-isomorphisme pour tout $\mathfrak{q} \in \mathfrak{S}(k)$ distinct de $\mathfrak{p}$. On en déduit :

Théorème 10. — Soit V *une variété projective, de dimension r, sans point multiple, définie sur un corps global* K, *et soit* ω *une* K*-différentielle de degré r sur* V, *dépourvue de pôles. Alors, il existe un* K*-modèle* (W, φ) *de* V *qui vérifie la condition du théorème précédent pour tout* $\mathfrak{p} \in \mathfrak{S} = \mathfrak{S}(K)$.

Démonstration. — En effet, on sait qu'il existe un sous-ensemble fini $\mathfrak{S}_0$ de $\mathfrak{S}$ tel que V soit strictement non dégénérée (mod. $\mathfrak{p}$) pour tout $\mathfrak{p} \notin \mathfrak{S}_0$. Pour un tel $\mathfrak{p}$, la condition du théorème est satisfaite : en effet, d'après la proposition 26, V n'admet qu'une seule provariété ω-maximale, celle obtenue en relevant la variété réduite $V_\mathfrak{p}^0$, et qui coïncide avec l'ensemble $V_{\mathfrak{R}_\mathfrak{p}} = V_{K_\mathfrak{p}}$ de tous les points rationnels $\mathfrak{p}$-adiques de V. Soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ les éléments de $\mathfrak{S}_0$. On peut trouver, d'après ce qui précède, des K-modèles (V_i, φ_i) de V $(1 \leqslant i \leqslant m)$ tels que, pour tout i, V_i soit $R_\mathfrak{q}$-isomorphe à V_{i-1} pour $\mathfrak{q} \in \mathfrak{S}$ distinct de $\mathfrak{p}_i$, et que la condition du théorème soit vérifiée par le couple $(V_i, \mathfrak{p}_i)$. Le dernier modèle (V_m, φ_m) de la suite ainsi construite vérifie alors cette condition pour tout $\mathfrak{p} \in \mathfrak{S}$.

CHAPITRE II

MODÈLES FAIBLEMENT p-SIMPLES p-MINIMAUX DES ESPACES HOMOGÈNES PRINCIPAUX ABÉLIENS

1. Espaces homogènes principaux.

Il paraît commode, à certains égards, d'introduire la notion *d'espace homogène principal* indépendamment de la donnée *a priori* d'un groupe structural.

Nous appellerons espace homogène principal (commutatif) un ensemble H muni d'une loi ternaire $\gamma = \gamma_H : H \times H \times H \to H$ vérifiant les axiomes suivants :

(EHP 1). Si $y_2 = \gamma(y_1, x_1, x_2)$, on a aussi

$$y_1 = \gamma(x_1, x_2, y_2) \quad \text{(fig. 1)}$$

(EHP 2) (commutativité)

$$\gamma(y_1, x_1, x_2) = \gamma(x_2, x_1, y_1)$$

(EHP 3) (axiome du « prisme »)

$$\gamma(y_1, x_1, x_2) = \gamma(y_1, z_1, \gamma(z_1, x_1, x_2)) \quad \text{(fig. 2)}$$

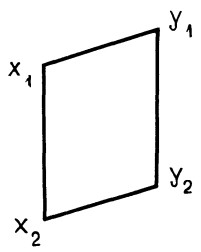


FIG. 1

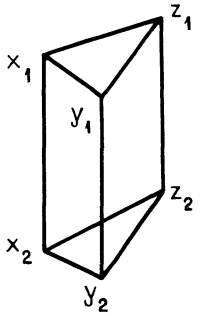


FIG. 2

Comme conséquence de (EHP 1) et (EHP 3), on a $\gamma(x_1, x_2, x_2) = \gamma(x_2, x_2, x_1) = x_1$.

Soit, d'autre part, $\Gamma = \Gamma_H$ le graphe de γ, dans le produit $H \times H \times H \times H$. Notons φ_{ij} la permutation de ce produit qui, à un élément quelconque, fait correspondre celui obtenu en échangeant ses composantes de rang i et j ($1 \leqslant i \leqslant 4$, $1 \leqslant j \leqslant 4$). On voit immédia-

tement qu'on peut remplacer, dans la définition précédente, le couple d'axiomes (EHP 1) et (EHP 2) par

(EHP'1). Γ est invariant par le groupe (commutatif) de permutations, à huit éléments, engendré par φ_{13} et $\varphi_{12}\circ\varphi_{34}$.

Soient x_1 et x_2 deux éléments de H. La permutation $\tau=\tau_{x_1,x_2}: H\to H$ définie par $\tau(x)=\gamma_H(x, x_1, x_2)$ est appelée une *translation* sur H. On écrira fréquemment x_τ, E_τ (E étant un sous-ensemble de H) au lieu de $\tau(x)$, $\tau(E)$. Il résulte des axiomes précédents que les translations sur H forment un *groupe commutatif* H_0. Ce groupe opère transitivement sur H, par la loi $(x,\tau)\to x_\tau$, et de façon que $x_\tau=x$ entraîne $\tau=0$. On retrouve ainsi la définition habituelle, avec H_0 comme *groupe structural.*

On remarquera que tout groupe commutatif admet une structure naturelle d'espace homogène principal, obtenue en prenant $\gamma(y_1, x_1, x_2)=y_1-x_1+x_2$. Inversement, si H est un espace homogène principal, et si x_0 est un élément arbitraire de H, on définit sur H une structure de groupe commutatif, avec x_0 pour origine, en munissant H de la loi γ_{H,x_0} définie par $\gamma_{H,x_0}(x, y)=\gamma_H(x, x_0, y)$.

Soient $m_1, \ldots, m_r, n_1, \ldots, n_s$ des entiers, et soient $x_1, \ldots, x_r, y_1, \ldots, y_s$ des éléments de H. Si on a $\Sigma_i m_i=\Sigma_j n_j$ la relation

$$\Sigma_i m_i x_i=\Sigma_j n_j y_j \tag{1}$$

au sens de la loi de groupe γ_{H,x_0}, a une signification indépendante de l'origine x_0 choisie. On conviendra d'employer l'écriture (1) sans préciser cette origine. On pourra, par exemple, avec cette convention, écrire, dans tous les cas, $\gamma_H(y_1, x_1, x_2)=y_1-x_1+x_2$.

Si H est une variété algébrique complète, définie sur un corps $\mathbf{k}$, et si γ_H est un $\mathbf{k}$-morphisme, nous dirons que H est un *espace homogène principal abélien*, défini sur $\mathbf{k}$. Pour tout point $x_0\in H$, la loi γ_{H,x_0} définit alors sur H une structure de variété abélienne, définie sur $\mathbf{k}(x_0)$ (ce qui montre en même temps que H est sans point multiple). Une translation $\tau=\tau_{x_1,x_2}$ est toujours un $\mathbf{k}(x_1, x_2)$-automorphisme de H. En utilisant les méthodes usuelles de descente du corps de base ([24], ou [10], chap. I^{er}, § 3), on voit qu'on peut mettre sur H_0 une structure de *variété abélienne, définie sur* $\mathbf{k}$, et que H est un espace homogène principal sur H_0, au sens habituel (cf. [18], chap. V, § 4, n° 21).

Dans le cas où H est une réunion finie de sous-variétés algébriques disjointes (qu'on appelle *composantes* de H) d'une variété ambiante V_0, et, où, pour tout triplet (H'_1, H_1, H_2) de telles composantes, γ_H induit un morphisme : $H'_1\times H_1\times H_2\to H'_2$ (H'_2 étant encore une composante de H), nous dirons que H est un *espace homogène principal algébrique.* Si, en outre, V_0 est définie sur $\mathbf{k}$, si H est un sous-$\mathbf{k}$-ensemble algébrique de V_0, et si γ_H induit une $\mathbf{k}$-application rationnelle sur toute $\mathbf{k}$-composante de $H\times H\times H$, nous dirons que l'espace homogène principal algébrique H est *défini sur* $\mathbf{k}$. Pour tout point $x_0\in H$, la loi γ_{H,x_0} définit alors sur H une structure de groupe algébrique, défini sur $\mathbf{k}(x_0)$. Une translation $\tau=\tau_{x_1,x_2}$ est encore un $\mathbf{k}(x_1, x_2)$-automorphisme de H, et on peut définir sur H_0 une structure de *groupe algébrique* défini sur $\mathbf{k}$; ceci permet de retrouver la définition habituelle d'un espace homogène principal sur un groupe algébrique ([15], ou [18], *loc. cit.*).

2. Espaces homogènes principaux abéliens. Notations et conventions.

Reprenons maintenant les notations introduites dans le chapitre Ier (k, k^0, R, v, $\mathfrak{p}$, $\mathfrak{k}^0$, $\mathfrak{k}$, $\mathfrak{R}$, Ω).

Nous désignerons par A une variété abélienne ou, plus généralement, un espace homogène principal abélien, défini sur k. Par *k-modèle* de A, nous désignons un couple (B, φ) composé d'un espace homogène principal abélien B, et d'un k-isomorphisme $\varphi : A \to B$, pour la structure d'espace homogène principal abélien (il suffit d'ailleurs que ce soit un isomorphisme pour la structure de variété algébrique ; il suffit même que ce soit une application birationnelle (cf. [22], III, n° 20, th. 9)). Nous convenons, d'autre part, une fois pour toutes, de ne considérer que des espaces homogènes principaux abéliens *projectifs*. Ceci ne restreindra pas la portée des résultats de ce chapitre, puisqu'on sait que tout espace homogène principal abélien défini sur k peut être plongé k-isomorphiquement dans un espace projectif [2].

Les translations sur A qui sont définies sur $\mathfrak{k}$ forment un groupe (isomorphe au groupe $(A_0)_{\mathfrak{k}}$ des points du groupe structural A_0 qui sont rationnels sur $\mathfrak{k}$). Ce groupe sera noté $\mathscr{T}(A)$. Les éléments de $\mathscr{T}(A)$ qui sont rationnels sur un sous-corps k_1 de $\mathfrak{k}$, contenant k, forment un sous-groupe de $\mathscr{T}(A)$ qu'on note $\mathscr{T}(A)_{k_1}$. Pour tout cycle X sur A, et pour $\tau \in \mathscr{T}(A)$, le cycle translaté de X par τ est noté X_τ.

On désignera par ω une k-différentielle sur A, définie sur k, de degré $r = \dim A$, et invariante par translation. On sait que ω existe, et est unique, au produit près par une constante non nulle (i.e. par un élément de k^*). On sait aussi qu'on a $(\omega) = 0$, c'est-à-dire que ω n'admet ni zéros, ni pôles. Ceci permettra, en particulier, d'utiliser les théorèmes 7, 8 et 9 du chapitre Ier. Les notions de (A, $\mathfrak{p}$, k^0)-provariété ω-maximale, celle de point simple ω-maximal sur $A^0 = \mathfrak{p}(A)$, celle de composante simple ω-maximale de A^0, ont ici une signification intrinsèque, en ce sens qu'elles ne dépendent pas en fait de la façon dont on a normé ω.

On dira que A est *pseudo-$\mathfrak{p}$-simple* si toutes les (A, $\mathfrak{p}$)-provariétés ω-maximales (en nombre fini d'après le théorème 8 du chap. Ier) sont simples. Ces provariétés sont alors celles obtenues en relevant génériquement les composantes simples ω-maximales de A^0. En vertu du théorème 9 du chap. Ier, tout espace homogène principal abélien défini sur k possède un k-modèle pseudo-$\mathfrak{p}$-simple.

3. L'espace homogène principal fini commutatif $\Gamma(A)$.

Proposition 1. — Soit A *un espace homogène principal abélien (*resp. *une variété abélienne) défini sur k. Soient* Y_1, X_1, X_2 *trois* (A, $\mathfrak{p}$)*-provariétés ω-maximales, définies sur* k^0. *Alors* $Y_2 = (\gamma_A)_g(Y_1, X_1, X_2)$ *est une* (A, $\mathfrak{p}$)*-provariété ω-maximale. Si* x_1 *et* x_2 *sont deux points génériques indépendants de* X_1 *et* X_2 *respectivement sur* k^0, *et si on pose* $\tau = \tau_{x_1, x_2}$, *on a aussi* $Y_2 = \tau_g(X_1)$. *L'ensemble* $\Gamma(A)$ *des* (A, $\mathfrak{p}$)*-provariétés ω-maximales, muni de la loi* $(\gamma_A)_g$ (resp. $(\gamma_{A,0})_g$) *est un espace homogène principal (*resp. *un groupe) fini commutatif.*

Démonstration. — On peut, d'après les résultats du chapitre Ier (corollaire du th. 2, et th. 9), se ramener au cas où A est pseudo-p-simple. Soient y_1, x_1, x_2 trois points génériques indépendants, sur k^0, de Y_1, X_1 et X_2 respectivement. Par définition du symbole $(\gamma_A)_g$, Y_2 est le lieu sur k^0 du point $y_2=\gamma_A(y_1, x_1, x_2)$ de A_t. Or, on a auss $y_2=\tau(y_1)$, en posant $\tau=\tau_{x_1,x_2}$. Si on pose $k'=(k'^0)^\sharp$, la translation τ est un k'-automorphisme de A. Donc $Y'_2=\mathrm{loc}_{k'}y_2=\tau_g(Y_1)$ est une (A, p)-provariété ω-maximale. Puisque A est pseudo-p-simple, Y'_2 est maximale au sens de l'inclusion (chap. Ier, n° 29, prop. 27). Comme on a $Y_2\supset Y'_2$, on a donc $Y_2=Y'_2$, donc Y_2 est bien une (A, p)-provariété ω-maximale, définie sur k^0.

De plus, nous venons de montrer que y_2 est générique de Y_2 sur $k'^0=k^0(x_1, x_2)$, donc que x_1, x_2, et y_2 sont des points génériques indépendants de X_1, X_2 et Y_2 respectivement sur k^0. Comme on a $y_1=\gamma_A(x_1, x_2, y_2)$, on voit, en échangeant les rôles des quatre points, qu'on a aussi $Y_1=(\gamma_A)_g(X_1, X_2, Y_2)$. La loi $(\gamma_A)_g$ sur l'ensemble $\Gamma(A)$ vérifie donc l'axiome (EHP 1). Elle vérifie aussi les deux autres axiomes, comme on le voit en appliquant les propriétés de γ_A à des points génériques indépendants des provariétés qui interviennent dans les relations correspondantes. C.Q.F.D.

A étant à nouveau un espace homogène principal abélien quelconque, défini sur k, considérons une (A, p)-provariété X, et un élément arbitraire τ de $\mathscr{T}(A)$. Puisque τ est un t-automorphisme de A, $Y=\tau_g(X)$ est encore une (A, p)-provariété, et si X est ω-maximale, il en est de même de Y. On a, d'autre part $(\tau_1+\tau_2)_g(X)=(\tau_1)_g((\tau_2)_g(X))$. Donc, par la loi $(\tau, x)\to\tau_g(x)$, le groupe $\mathscr{T}(A)$ *opère* sur $\Gamma(A)$. De plus, ce groupe opère *transitivement* sur $\Gamma(A)$: en effet, soient X et Y deux (A, p)-provariétés ω-maximales; soit k^0_* un corps de définition pour X et Y, contenant k^0; soient x et y deux points génériques indépendants de X et Y respectivement sur k^0_*, et posons $\tau=\tau_{xy}$; alors, d'après la proposition 1, on a $\tau_g(X)=\gamma_A(X, X, Y)$, d'où $\tau_g(X)=Y$. Enfin, on a, quels que soient X et $Y\in\Gamma(A)$, et $\tau\in\mathscr{T}(A)$, la formule

$$\tau_g(Y)=\gamma_A(\tau_g(X), X, Y) \tag{2}$$

En effet, soit k^0_* un corps de définition de X, Y et τ, contenant k^0. Soient x, y et x' trois points génériques indépendants de X, Y et $\tau_g(X)$ respectivement sur k^0_*; la (A, p)-provariété $\gamma_A(\tau_g(X), X, Y)$ est le lieu, sur k^0_*, du point $y'=\gamma_A(x', x, y)$; d'autre part, $\bar{x}=\tau(x)$ et $\bar{y}=\tau(y)$ sont des points génériques indépendants, sur k^0_*, des (A, p)-provariétés $\tau_g(X)$ et $\tau_g(Y)$ respectivement; puisqu'on a $k^0_*(x, y)=k^0_*(\bar{x}, \bar{y})$, le point x' est générique de X' sur $k^0_*(\bar{x}, \bar{x})$; or, on a $y'=\gamma_A(x', \bar{x}, \bar{y})$; donc le lieu de y' sur k^0_* coïncide avec la (A, p)-provariété $(\gamma_A)_g(\tau_g(X), \tau_g(X), \tau_g(Y))=\tau_g(Y)$, ce qui démontre la formule (2).

Il résulte de là que l'ensemble des éléments de $\mathscr{T}(A)$ qui laissent invariante une (A, p)-provariété ω-maximale X est un sous-groupe de $\mathscr{T}(A)$, qui ne dépend pas de X. Nous désignerons ce sous-groupe par $\mathscr{T}_0(A)$. Le groupe quotient $\Gamma_0(A)=\mathscr{T}(A)/\mathscr{T}_0(A)$ est un groupe abélien fini, canoniquement isomorphe au groupe structural de $\Gamma(A)$.

Corollaire. — *Soit* A *un espace homogène principal abélien défini sur k, pseudo-*$\mathfrak{p}$*-simple, et soient* Y_1^0, X_1^0, X_2^0 *trois composantes simples* ω*-maximales de* $A^0 = \rho(A)$, *définies sur* k^0. *Soient* y_1^0, x_1^0, x_2^0 *des points génériques indépendants sur* k^0 *de* Y_1^0, X_1^0, X_2^0 *respectivement. Alors* γ_A *est* $\mathfrak{p}$*-morphique en* (y_1^0, x_1^0, x_2^0).

Si, de plus, y_2^0 *est simple sur* A^0, *il est générique sur* k^0 *d'une composante simple* ω*-maximale* Y_2^0 *de* A^0, *et on a* $k^0(y_1^0, x_1^0, x_2^0) = k^0(x_1^0, x_2^0, y_2^0) = k^0(x_2^0, y_2^0, y_1^0) = k^0(y_2^0, y_1^0, x_1^0)$; *cette condition est, en particulier, toujours vérifiée dans les deux cas suivants*

a) A *est pseudo-*$\mathfrak{p}$*-simple.*

b) $X_2^0 = X_1^0$; *dans ce dernier cas on a aussi* $Y_2^0 = Y_1^0$.

En effet, le point (y_2^0, x_1^0, x_2^0) est générique sur k^0 d'une composante simple de $A^0 \times A^0 \times A^0$; donc γ_A est bien $\mathfrak{p}$-morphique en ce point, d'après la proposition 8 du n° 11 du chapitre I^er^. Considérons les (A, $\mathfrak{p}$)-provariétés $Y_1 = (Y_1^0)_g^\#$, $X_1 = (X_1^0)_g^\#$, et $X_2 = (X_2^0)_g^\#$ obtenues en relevant génériquement Y_1^0, X_1^0 et X_2^0 respectivement. D'après la proposition 1, $Y_2 = (\gamma_A)_g(Y_1, X_1, X_2)$ est une (A, $\mathfrak{p}$)-provariété ω-maximale. On peut trouver des points y_1, x_1, x_2, génériques indépendants sur k^0 des (A, $\mathfrak{p}$)-provariétés Y_1, X_1 et X_2 respectivement, et tels qu'on ait $y_1^0 = \rho(y_1)$, $x_1^0 = \rho(x_1)$ et $x_2^0 = \rho(x_2)$. Le point $y_2 = \gamma_A(y_1, x_1, x_2)$ est alors générique de Y_2 sur k^0; on a d'autre part $y_2^0 = \rho(y_2)$.

Pour que la provariété Y_2 soit simple, il faut et il suffit que y_2^0 soit simple sur A^0; dans ce cas $Y_2^0 = \overline{\rho}(Y_2) = \mathrm{loc}_{k^0} y_2$ est une composante simple ω-maximale de A^0; d'autre part, il résulte de la démonstration précédente que x_1, y_1, y_2 sont des points génériques indépendants sur k^0 de X_1, Y_1, Y_2 respectivement; donc x_1^0, y_1^0, y_2^0 sont génériques indépendants sur k^0 de X_1^0, Y_1^0, Y_2^0 respectivement. On en déduit $y_1^0 = (\gamma_A)^0(x_1^0, y_1^0, y_2^0)$, d'où $k^0(y_1^0, x_1^0, x_2^0) = k^0(x_1^0, x_2^0, y_2^0)$, et les autres relations analogues, par permutation circulaire.

Dans chacun des deux cas *a)* et *b)*, Y_2 est simple (par définition d'un modèle pseudo-$\mathfrak{p}$-simple, dans le cas *a)*, et puisqu'on a $Y_2 = Y_1$ (d'où $Y_2^0 = Y_1^0$), d'après la proposition 1, dans le cas *b)*), donc la condition « y_2^0 simple sur A^0 » est bien satisfaite.

Proposition 2. — *Soit* A *un espace homogène principal abélien, défini sur k, et soient* X^0 *et* Y^0 *deux composantes simples* ω*-maximales de* $A^0 = \rho(A)$, *définies sur* k^0. *Soient* x^0 *et* y^0 *des points génériques (non nécessairement indépendants) sur* k^0 *de* X^0 *et* Y^0 *respectivement. Alors* γ_A *est* $\mathfrak{p}$*-morphique en* (x^0, x^0, y^0), *de valeur* y^0.

Démonstration. — Supposons d'abord que x^0 et y^0 sont des points génériques *indépendants* de X^0 et Y^0 respectivement sur k^0. Soit x_1^0 un point générique de X^0 sur $k^0(x^0, y^0)$. D'après le corollaire de la proposition 1 (cas *b)*), γ_A est $\mathfrak{p}$-morphique en (x_1^0, x^0, y^0) et le point $y_1^0 = \gamma_A^0(x_1^0, x^0, y^0)$ est générique de Y^0 sur k^0; de plus, on a $k^0(x_1^0, x^0, y^0) = k^0(x^0, x_1^0, y_1^0)$, ce qui implique que γ_A est $\mathfrak{p}$-morphique en (x^0, x_1^0, y_1^0), de valeur y^0. Donc, d'après l'axiome du prisme (EHP 3), et d'après les propositions 1, 2 et 3 du n° 3 du chapitre I^er^, γ_A est $\mathfrak{p}$-morphique en (x^0, x^0, y^0) et on a

$$\gamma_A^0(x^0, x^0, y^0) = \gamma_A^0(x^0, x_1^0, \gamma_A^0(x_1^0, x^0, y^0)),$$

ce qui donne bien $\gamma_A^0(x^0, x^0, y^0) = y^0$.

Supposons maintenant que x^0 et y^0 sont des points génériques quelconques (non

nécessairement indépendants) de X^0 et Y^0 respectivement sur k^0. Soit z^0 un point générique, sur $k^0(x^0, y^0)$, d'une composante simple ω-maximale Z^0 de A^0 (on peut, par exemple, prendre $Z^0 = X^0$, ou $Z^0 = Y^0$). D'après la première partie de la démonstration, γ_A est $\mathfrak{p}$-morphique en (y^0, z^0, z^0) et en (z^0, x^0, x^0) et prend respectivement en ces points les valeurs y^0 et z^0. Donc, toujours en appliquant l'axiome au prisme (EHP 3), et les propositions 1, 2 et 3 du n° 3 du chapitre I[er], on voit que γ_A est $\mathfrak{p}$-morphique en (x^0, x^0, y^0) et que $\gamma_A^0(x^0, x^0, y^0) = \gamma_A^0(y^0, x^0, x^0) = \gamma_A^0(y^0, z^0, \gamma_A^0(z^0, x^0, x^0))$, ce qui donne bien encore $\gamma_A^0(x^0, x^0, y^0) = y^0$.

4. Une propriété essentielle des points simples ω-maximaux sur A^0.

Le résultat qui suit s'apparente à la propriété fondamentale bien connue des variétés abéliennes, d'après laquelle toute application rationnelle $V \to A$ d'une variété quelconque V dans une variété abélienne est morphique en tout point simple de V (cf. [22], § 11, th. 6).

Théorème 1. — *Soit* A *un espace homogène principal abélien, défini sur* k; *soit* V *une* $\mathfrak{p}$-*variété* quelconque, *définie sur* k, *et soit* $\varphi : V \to A$ *une application rationnelle, définie sur* k. *Posons* $A^0 = \rho(A)$, *et* $V^0 = \rho(V)$. *Soit* (z^0, x^0) *un couple composé d'un point* $z^0 \in \rho_e(V) = \operatorname{supp} V^0$, *simple sur* V^0, *et d'un point* $x^0 \in \rho_e(A) = \operatorname{supp} A^0$, *simple et* ω-*maximal sur* A^0, *tels que* x^0 *appartienne à l'ensemble* $\varphi_e^0(z^0)$ *des valeurs de* φ *en* z^0. *Alors* φ *est* $\mathfrak{p}$-*morphique en* z^0 (*et on a donc* $x^0 = \varphi^0(z^0)$).

Démonstration. — On peut supposer que A est pseudo-$\mathfrak{p}$-simple; sinon, en effet, on remarque qu'il existe (d'après le corollaire au th. 3, et le th. 9 du chap. I[er]), un k-modèle pseudo-$\mathfrak{p}$-simple (B, ψ) de A, tel que ψ soit $\mathfrak{p}$-isomorphique en x^0. Il suffit alors de remplacer A par B.

Soit k_1^0 un sous-corps de $\mathfrak{k}^0$, contenant $k^0(z^0, x^0)$, et sur lequel toutes les composantes de V^0 et de A^0 sont définies. Soit Y une $(A, \mathfrak{p})$-provariété ω-maximale quelconque. Alors Y est définie sur k_1^0. Soient y et y' deux points génériques indépendants de Y sur k_1^0. Considérons la translation $\tau = \tau_{y,y'}$ sur A, et l'application rationnelle $\overline{\varphi} = \tau \circ \varphi : V \to A$.

Soit, d'autre part, z un point générique sur $k_1^0(y, y')$ de la $(V, \mathfrak{p})$-provariété $(z^0)_g^\sharp$ obtenue en relevant génériquement le point z^0. D'après le n° 20 du chapitre I[er] (remarque *e)*), z est un point générique de V sur $k_1(y, y')$, en posant $k_1 = (k_1^0)^\sharp$. Donc φ et $\overline{\varphi}$ sont morphiques en z. Posons $x_* = \varphi(z)$, et $\overline{x} = \overline{\varphi}(z) = \tau(x_*) = \gamma_A(x_*, y, y')$. D'après le choix de z, les points y et y' sont génériques indépendants de Y sur $k_1^0(z)$, donc aussi sur $k_1^0(x_*)$. Le point $\overline{x}$ est donc générique sur k_1^0 d'une $(A, \mathfrak{p})$-provariété ω-maximale, à savoir la provariété $(\tau_*)_g(Y)$, où l'on pose $\tau_* = \tau_{yx_*}$ (on le voit en procédant comme dans la démonstration de la proposition 1). Donc le point $\overline{x}^0 = \rho(\overline{x})$ est générique sur k_1^0 d'une composante simple ω-maximale de A^0. De plus, puisque $\overline{x} = \overline{\varphi}(z)$, ce point $\overline{x}^0$ appartient à l'ensemble $\overline{\varphi}_e^0(z^0)$ des valeurs de $\overline{\varphi}$ en z^0.

Nous allons montrer, en utilisant les propositions 1 et 2 précédentes, par une

méthode analogue à celle qu'emploie Weil dans [22] pour la démonstration du théorème cité plus haut, que $\overline{\varphi}$ est p-morphique en z^0 (donc de valeur $\overline{x}^0$).

Soient z_1 et z_2 deux points génériques indépendants de V sur $\mathfrak{k}$, et considérons l'application rationnelle $\overline{\psi} : V \times V \to A$, définie sur $k(\overline{x})$, telle que

$$\overline{\psi}(z_1, z_2) = \gamma_A(\overline{x}, \overline{\varphi}(z_1), \overline{\varphi}(z_2)) \tag{3}$$

D'après la proposition 2, γ_A est p-morphique en $(\overline{x}^0, \overline{x}^0, \overline{x}^0)$, de valeur $\overline{x}^0$. Puisque $\overline{x}^0 \in \overline{\varphi}_e^0(z^0)$, et d'après les propositions 1 à 3 du n° 3 du chapitre I^er, on a donc $\overline{x}^0 \in \overline{\psi}_e^0(z^0, z^0)$.

Soit d'autre part Z^0 la composante simple de A^0 contenant z^0, et soit z' un point générique sur k_1^0 de la (V, p)-provariété $Z = (Z^0)_g^\#$, obtenue en relevant génériquement Z^0, sur $k_1^0(y, y')$. Posons $x'_* = \varphi(z')$, et $\overline{x}' = \overline{\varphi}(z') = \tau(x'_*) = \gamma_A(x'_*, y, y')$. Le point $\overline{x}'$ est encore générique sur k_1^0 d'une (A, p)-provariété ω-maximale. Donc $\overline{x}'^0$ est générique sur k_1^0 d'une composante simple ω-maximale de A^0. D'autre part, le point $z'^0 = \rho(z')$ est générique de Z^0 sur $k_1^0(y, y')$. Donc, d'après la proposition 8 du n° 11 du chapitre I^er, $\overline{\varphi}$ est p-morphique en z'^0. Puisqu'on a $\overline{x}' = \overline{\varphi}(z')$, on a aussi $\overline{x}'^0 = \overline{\varphi}^0(z'^0)$. D'après la proposition 2, γ_A est p-morphique en $(\overline{x}^0, \overline{x}^0, \overline{x}'^0)$, de valeur $\overline{x}'^0$. D'après la formule (3) définissant ψ, et d'après les propositions 1 à 3 du chapitre I^er, on a donc $\overline{x}'^0 \in \overline{\psi}_e^0(z^0, z'^0)$.

Supposons que $\overline{\varphi}$ ne soit pas p-morphique en z^0, et montrons que $\overline{\psi}$ n'est pas p-morphique en (z^0, z^0). En effet, si $\overline{\psi}$ était p-morphique en (z^0, z^0), $\overline{\psi}$ serait, *a fortiori*, p-morphique en z^0, z'^0, et on aurait donc $\overline{x}'^0 = \overline{\psi}^0(z^0, z'^0)$. Or, d'après la proposition 2, γ_A est p-morphique en $(\overline{x}^0, \overline{x}'^0, \overline{x}'^0)$, de valeur $\overline{x}^0$; d'autre part, d'après la formule (1), et les propriétés de γ_A, on a :

$$\overline{\varphi}(z_1) = \gamma_A(\overline{x}, \overline{\psi}(z_1, z_2), \overline{\varphi}(z_2)).$$

En appliquant à nouveau les propositions 1 à 3 du chapitre I^er, on en déduirait que $\overline{\varphi}$ est p-morphique en z^0, contrairement à ce qu'on a supposé.

Soient maintenant $\overline{y}_i = \overline{\psi}_i(z_1, z_2)$ les coordonnées du point $\overline{y} = \overline{\psi}(z_1, z_2)$ relativement à un modèle affine U d'un ouvert de A contenant $\overline{x}^0$. En supposant toujours que φ n'est pas p-morphique en $\overline{x}^0$, l'une au moins des fonctions $\overline{\psi}_i$ n'est pas p-morphique en (z^0, z^0). D'autre part, d'après la relation (1) et la proposition 2, $\overline{\psi}$ est p-morphique en (z'^0, z'^0), de valeur $\overline{x}^0$. Donc $\overline{\psi}_i$ est génériquement p-morphique sur $Z^0 \times Z^0$. Or, (z^0, z^0) est p-simple sur $V \times V$, et $Z^0 \times Z^0$ est l'unique composante de $V^0 \times V^0 = \rho(V \times V)$ qui le contient. Donc, d'après le corollaire de la proposition 10 du n° 12, on a $(z^0, z^0) \in \rho_e(\mathrm{supp}(\overline{\psi}_i)_\infty)$. Donc il existe une $\mathfrak{k}$-composante T de $(\overline{\psi}_i)_\infty$ telle que $(z^0, z^0) \in \rho_e(T)$. Comme $\overline{\psi}$ est p-morphique en (z'^0, z'^0), on a $(z'^0, z'^0) \notin \rho_e(T)$. Donc, puisque T est de codimension 1 dans $V \times V$, toute composante de $\rho_e(T)$ contenant (z^0, z^0) coupe proprement la diagonale Δ_{Z^0} dans le produit $Z^0 \times Z^0$. D'après ([R], n° 3, th. 11), il existe une $\mathfrak{k}$-composante X, de dimension $r-1$ (si $r = \dim V$), de l'intersection $\Delta_V \cap T$, telle qu'on ait $(z^0, z^0) \in \rho_e(X)$. Cette composante X est nécessairement de la forme $X = \Delta_W$,

où W est une sous-$\mathfrak{k}$-variété de codimension 1 de V, simple sur V, telle que $z^0 \in \rho_e(W)$. Soit w un point générique de W sur $\mathfrak{k}$. On a $(w, w) \in T$, donc, puisque T est une $\mathfrak{k}$-composante de $(\overline{\psi}_i)_\infty$, $\overline{\psi}$ n'est pas morphique en (w, w). Ceci est contradictoire, puisque (w, w) est simple sur $V \times V$.

On a donc bien démontré que $\overline{\varphi}$ est $\mathfrak{p}$-morphique en z^0, de valeur $\overline{x}^0$. Puisque, par hypothèse, on a $x^0 \in \varphi_e^0(z^0)$, on a aussi, d'après la proposition 1 du n° 3 du chapitre Ier, $\overline{x}^0 \in \tau_0^e(x^0)$. D'autre part, en appliquant ce qui précède au cas particulier où φ est l'application identique $A \to A$, on voit que τ est $\mathfrak{p}$-morphique en x^0 de valeur $\overline{x}^0$. Puisque x^0 et $\overline{x}^0$ sont tous les deux simples et ω-maximaux, la différentielle $\omega t^{-\nu_0}$ (où $\nu_0 = \nu_0(\omega, V)$) ne s'annule en aucun de ces deux points. Donc, d'après la proposition 12 du n° 15 du chapitre Ier, τ est $\mathfrak{p}$-isomorphique en x^0. Donc $\varphi = \tau^{-1} \circ \overline{\varphi}$ est $\mathfrak{p}$-morphique en z^0.

C.Q.F.D.

Corollaire 1. — *Soit* A *un espace homogène principal abélien, défini sur k, et soient* $x_1^0, x_2^0, y_1^0, y_2^0$ *quatre points de* $\rho_e(A)$, *simples sur* A^0, *tels que* y_2^0 *soit* ω*-maximal, et appartienne à l'ensemble* $\gamma_e^0(y_1^0, x_1^0, x_2^0)$. *Alors* γ_A *est* $\mathfrak{p}$*-morphique en* (y_1^0, x_1^0, x_2^0) *(et on a donc* $y_2^0 = \gamma_A^0(y_1^0, x_1^0, x_2^0)$*). En particulier, si* x^0 *est un point simple, et* y^0 *un point simple* ω*-maximal, sur* A^0, γ_A *est* $\mathfrak{p}$*-morphique en* (y^0, x^0, x^0), *de valeur* y^0.

Ce corollaire est une amélioration de la proposition 2 précédente (dans laquelle n'intervenaient que des points génériques). Il s'obtient en appliquant le théorème à $\gamma_A : A \times A \times A \to A$, et en remarquant que (y_1^0, x_1^0, x_2^0) est simple sur

$$A^0 \times A^0 \times A^0 = \rho(A \times A \times A)$$

Corollaire 2. — *Soit* A *un espace homogène principal abélien, défini sur k, strictement non dégénéré* (mod. $\mathfrak{p}$) *(c'est-à-dire tel que* $A^0 = \rho(A)$ *soit une variété sans point multiple). Alors* γ_A *est* $\mathfrak{p}$*-morphique en tout triplet* (y_1^0, x_1^0, x_2^0) *de points de* A^0, *et la loi réduite* γ_A^0 *définit sur* A^0 *une structure d'espace homogène principal abélien, défini sur* k^0.

En effet, puisque A^0 n'a qu'une composante, et puisque celle-ci est simple, $(A^0)^\sharp = A_{\mathfrak{R}} = A_{\mathfrak{k}}$ est l'unique $(A, \mathfrak{p})$-provariété ω-maximale, d'après la proposition 25 du n° 28 du chapitre Ier. Donc A^0 est ω-maximale, donc tous les points de A^0 sont ω-maximaux, et il suffit d'appliquer le corollaire précédent.

En particulier, si A est une variété abélienne, strictement non dégénérée (mod. $\mathfrak{p}$) (*without defect for* $\mathfrak{p}$, avec la terminologie de [8] et [9]), A^0 est aussi une variété abélienne pour la loi réduite. On retrouve là un résultat de Koizumi ([8], th. 3).

5. Recouvrement de $A_{\mathfrak{k}}$ par des translatés de $(V, \mathfrak{p})$-ensembles simples et ω-maximaux (mod. $\mathfrak{p}$).

Proposition 3. — *Soit* A *un espace homogène principal abélien, pseudo-*$\mathfrak{p}$*-simple, défini sur k. Alors on peut recouvrir* $A_{\mathfrak{k}}$ *par un nombre fini de* $(V, \mathfrak{p})$*-ensembles* S_α *vérifiant la condition suivante : pour tout* α, *il existe une translation* $\tau_\alpha \in \mathscr{T}_0(A)$ *telle que les* $(V, \mathfrak{p})$*-ensembles* $T_\alpha = (S_\alpha)_{\tau_\alpha}$, *et* $T'_\alpha = (S_\alpha)_{-\tau_\alpha}$ *ne contiennent que des points simples et* ω*-maximaux* (mod. $\mathfrak{p}$).

Démonstration. — On peut se borner à considérer au lieu de $A_{\mathfrak{k}}$, un (A, $\mathfrak{p}$)-ensemble S vérifiant la condition suivante :

(*) il existe un $\mathfrak{k}$-modèle (B, φ) de A, tel que le (B, $\mathfrak{p}$)-ensemble $T=\varphi(S)$ ne contienne que des points simples (mod. $\mathfrak{p}$).

Il nous suffit de montrer qu'un tel ensemble S peut être recouvert par un nombre fini de (A, $\mathfrak{p}$)-ensembles vérifiant la condition de l'énoncé : en effet, d'après le théorème 6 du n° 27 du chapitre I^er, l'ensemble $A_{\mathfrak{k}}$ peut lui-même être recouvert par un nombre fini de (A, $\mathfrak{p}$)-ensembles S_i vérifiant la condition (*). On peut en outre supposer (en agrandissant S et T, s'il y a lieu) que T est de la forme $\rho^{-1}(T^0)=(T^0)^{\sharp}$, où T^0 est un ouvert d'une composante Y^0 de $B^0=\rho(B)$.

Considérons d'abord un point quelconque z de T, et associons-lui le point $x=\varphi^{-1}(z)$ de $A_{\mathfrak{k}}$. On peut trouver une translation $\tau\in\mathscr{T}_0(A)$ telle que les deux points $y=x_\tau$ et $y'=x_{-\tau}$ soient simples et ω-maximaux (mod. $\mathfrak{p}$). Il suffit, par exemple, si k_1^0 est un corps de définition pour toutes les composantes simples de A^0, de prendre τ de la forme $\tau_{uu'}$, où u et u' sont deux points génériques indépendants, sur k_1^0, d'une même (A, $\mathfrak{p}$)-provariété ω-maximale X, car alors y et y' sont deux points génériques (non nécessairement indépendants) sur k_1^0 de la (A, $\mathfrak{p}$)-provariété ω-maximale $Y=(\tau_{ux})_g(X)=(\tau_{u'x})_g(X)$.

La variété $Y^0=\rho(Y)$ est alors une composante simple ω-maximale de A^0, admettant $y^0=\rho(y)$ et $y'^0=\rho(y')$ comme points génériques (non nécessairement indépendants) sur k_1^0. D'après la proposition 13 du n° 16 du chapitre I^er, on peut trouver un k_1^0-ouvert $\overline{U}^0$ de Y^0, dont tous les points sont simples et ω-maximaux sur A^0. Considérons le k-isomorphisme $\psi=\tau\circ\varphi^{-1}$ (resp. $\psi'=(-\tau)\circ\varphi^{-1}$) : $B\to A$. On a $y=\psi(z)$ (resp. $y'=\psi(z')$), donc y^0 (resp. y'^0) appartient à l'ensemble des valeurs de ψ (resp. ψ') en z^0. Puisque $z\in T$, le point z^0 est simple sur B^0. Donc, d'après le théorème 1, ψ (resp. ψ') est $\mathfrak{p}$-morphique en z^0, de valeur y^0 (resp. y'^0). Soit Z^0 la composante simple de B^0 qui contient z^0. On peut trouver un ouvert $U^0=\mathscr{U}^0(z)$ de Z^0, contenant z^0, contenu dans T^0, tel que ψ et ψ' soient $\mathfrak{p}$-morphiques en tout point de U^0, et tel que les images $\psi^0(U^0)$ et $\psi'^0(U^0)$ soient contenues dans $\overline{U}^0$. Si alors on pose $U=(U^0)^{\sharp}$, $\overline{S}=\varphi^{-1}(U)$, $\overline{U}=(\overline{U}^0)^{\sharp}$, les (A, $\mathfrak{p}$)-ensembles $\overline{S}_\tau=\psi(U)$ et $\overline{S}_{-\tau}=\psi'(U)$ sont contenus dans $\overline{U}$, donc ne contiennent que des points simples et ω-maximaux (mod. $\mathfrak{p}$).

Notre assertion concernant l'existence d'un recouvrement fini de S s'obtient alors en remarquant qu'il existe un recouvrement fini de T^0 par des ouverts de la forme $\mathscr{U}^0(z)$.

6. Le groupe $\mathscr{D}'_l(A)$.

Soit A un espace homogène principal abélien, défini sur k (plus généralement, les définitions qui suivent pourraient s'appliquer au cas d'une variété V sans point multiple, de dimension r, munie d'une différentielle ω de degré r, telle que $(\omega)_\infty=0$).

Nous noterons $\mathscr{D}(A)$ le groupe des diviseurs sur A qui sont rationnels sur $\mathfrak{k}$, et $\mathscr{D}_l(A)$ le sous-groupe des éléments linéairement équivalents à zéro de $\mathscr{D}(A)$. Si k_1 est un sous-corps de $\mathfrak{k}$ sur lequel A est définie, le sous-groupe des éléments rationnels sur k_1

de $\mathscr{D}(A)$ (resp. $\mathscr{D}_l(A)$) est noté $\mathscr{D}(A)_{k_1}$ (resp. $\mathscr{D}_l(A)_{k_1}$). D'après ([F], chap. IX-4, th. 8, cor. 2), on sait que si $D\in\mathscr{D}_l(A)$ (resp. si $D\in\mathscr{D}_l(A)_{k_1}$), il existe une fonction f sur V, définie sur $\mathfrak{k}$ (resp. k_1), telle qu'on ait $(f)=D$.

D'autre part, on sait que si $D\in\mathscr{D}_l(A)$, et si τ et τ' sont deux éléments de $\mathscr{T}(A)$, on a $D_{\tau+\tau'}-D_\tau-D_{\tau'}+D\in\mathscr{D}_l(A)$.

Supposons maintenant que A est pseudo-p-simple. Considérons les diviseurs $D\in\mathscr{D}_l(A)$ qui vérifient la condition supplémentaire suivante :

(*) Il existe une fonction f sur A, définie sur $\mathfrak{k}$, telle que $(f)=D$, qui est génériquement p-morphique et non nulle sur toutes les composantes simples ω-maximales de A^0.

Il revient au même de dire qu'il existe une fonction f' sur A, définie sur $\mathfrak{k}$, telle que l'entier $\nu(C_i^0,f')$ prenne une valeur constante ν sur toutes les composantes simples ω-maximales C_i^0 de A^0 (en effet on peut alors prendre $f=f't^{-\nu}$).

L'ensemble des diviseurs $D\in\mathscr{D}_l(A)$ qui vérifient la condition (*) est un sous-groupe de $\mathscr{D}_l(A)$, que nous noterons $\mathscr{D}'_l(A)$. Le sous-groupe des éléments rationnels sur k_1 de $\mathscr{D}'_l(A)$ sera noté $\mathscr{D}'_l(A)_{k_1}$.

Si (B,φ) est un k-modèle pseudo-p-simple de A, et si $D\in\mathscr{D}'_l(A)$, l'image $\varphi(D)$ de D sur B appartient à $\mathscr{D}'_l(B)$. En effet, φ est génériquement p-isomorphique sur toute composante simple ω-maximale de A^0 (chap. I^{er}, n^o 29, prop. 27). Donc le groupe $\mathscr{D}'_l(A)$ ne dépend, pour A pseudo-p-simple, que de la classe de A à un k-isomorphisme près.

Proposition 4. — *Pour* $D\in\mathscr{D}_l(A)$, *et* $\tau\in\mathscr{T}_0(A)$, *on a* $D_\tau-D\in\mathscr{D}'_l(A)$.

Démonstration. — Puisque $D\in\mathscr{D}_l(A)$, il existe, en effet, une fonction f sur A, définie sur $\mathfrak{k}$, telle que $(f)=D$. Soit X^0 une composante simple ω-maximale de A^0. Soit k_1^0 un corps de définition de X^0 contenant k^0, et soit x^0 un point générique de X^0 sur k_1^0. Puisque l'application τ appartient à $\mathscr{T}_0(A)$, elle laisse invariante la (A, p)-provariété ω-maximale $X=(X^0)_g^\sharp$. Donc τ est génériquement p-isomorphique sur X^0, et on a $\tau_g^0(X^0)=X^0$. Donc, on a, en posant $f'=f\circ\tau^{-1}$, la relation $\nu(X^0,f)=\nu(X^0,f')$ d'où $\nu(X^0,f'/f)=0$, quelle que soit X^0. Or on a $(f')=D_\tau$, d'où $(f'/f)=D_\tau-D$. On a donc bien $D_\tau-D\in\mathscr{D}'_l(A)$.

Proposition 5. — *Pour* $D\in\mathscr{D}(A)$, $\tau_0\in\mathscr{T}_0(A)$ *et* $\tau\in\mathscr{T}(A)$ *on a*

$$D_{\tau_0+\tau}-D_{\tau_0}-D_\tau+D\in\mathscr{D}'_l(A).$$

Démonstration. — τ étant regardé comme fixe, posons, pour $\sigma\in\mathscr{T}_0(A)$,

$$E(\sigma)=D_{\sigma+\tau}-D_\sigma-D_\tau+D,$$

et commençons par montrer que la classe du diviseur $E(\sigma)$ (mod. $\mathscr{D}'_l(A)$) dépend linéairement de σ. On a, en effet, $E(\sigma)\in\mathscr{D}_l(A)$, d'après ([18], VIII, n^o 57, th. 30, cor. 2). Donc, d'après la proposition précédente, pour $\sigma'\in\mathscr{T}_0(A)$, on a $(E(\sigma))_{\sigma'}-E(\sigma)\in\mathscr{D}'_l(A)$, d'où l'on tire $E(\sigma+\sigma')-E(\sigma)-E(\sigma')\in\mathscr{D}'_l(A)$, ce qui prouve notre assertion.

Soit maintenant k_1^0 un corps de définition, contenant k^0, de toutes les composantes simples ω-maximales de A^0, tel que les translations τ_0 et τ soient définies sur $k_1=(k_1^0)^\sharp$.

Soit X une (A, $\mathfrak{p}$)-provariété ω-maximale quelconque, et soient x et x' deux points génériques indépendants de X sur k_1^0. Alors x et $x''=x'_\tau$ sont également deux points génériques indépendants de X sur k_1^0. Il existe un k_1^0-automorphisme α^0 de $\mathfrak{k}^0$ tel que, si α est le k_1-automorphisme de $\mathfrak{k}$ obtenu « en relevant α^0 » (i.e. le k_1-automorphisme qui, à $x\in\mathfrak{k}$, fait correspondre l'élément x^α de $\mathfrak{k}$ déduit de x par application de α^0 à chacun de ses coefficients), on ait $x^\alpha=x$, et $(x')^\alpha=x''$. Posons $\tau'_0=\tau_{xx'}$ et $\tau''_0=\tau_{xx''}$. D'après ([22], VIII, n° 57, th. 30, cor. 2) on peut trouver une fonction f sur A, rationnelle sur $\mathfrak{k}$, telle qu'on ait $(f)=\mathrm{E}(\tau'_0)$. On a alors $(f^\alpha)=\mathrm{E}(\tau''_0)$. Si, de plus, Y^0 est une composante simple ω-maximale quelconque de A^0, on a $(\mathrm{Y}^0)^{\alpha^0}=\mathrm{Y}^0$, puisque Y^0 est rationnelle sur k_1^0. On a donc $\nu(\mathrm{Y}^0, f)=\nu((\mathrm{Y}^0)^{\alpha^0}, f^\alpha)=\nu(\mathrm{Y}^0, f^\alpha)$, d'où $\nu(\mathrm{Y}^0, (f^\alpha/f))=0$, d'où $(f^\alpha/f)=\mathrm{E}(\tau''_0)-\mathrm{E}(\tau'_0)\in\mathscr{D}'_l(\mathrm{A})$. Or τ'_0 et τ''_0 sont des éléments de $\mathscr{T}_0(\mathrm{A})$, et on a $\tau''_0=\tau_0+\tau'_0$. On a donc $\mathrm{E}(\tau_0)\equiv\mathrm{E}(\tau''_0)-\mathrm{E}(\tau'_0)(\mathrm{mod.}\ \mathscr{D}'_l(\mathrm{A}))$, d'après la première partie de la démonstration, d'où $\mathrm{E}(\tau_0)\in\mathscr{D}'_l(\mathrm{A})$.

7. Espaces homogènes principaux abéliens faiblement $\mathfrak{p}$-simples $\mathfrak{p}$-minimaux.

Rappelons (chap. I[er], n° 10), qu'une $\mathfrak{p}$-variété V, sans point multiple, est dite *faiblement* $\mathfrak{p}$-*simple* si tout point de $\mathrm{V}_\mathfrak{R}$ est simple (mod. $\mathfrak{p}$) sur V ou encore, ce qui est équivalent, si on a $\rho(\mathrm{V}_\mathfrak{R})=\mathscr{S}(\mathrm{V}^0)$; si, en particulier V est $\mathfrak{p}$-*simple*, c'est-à-dire si tous les points de $\rho_e(\mathrm{V})=\mathrm{supp}\ \mathrm{V}^0$ sont $\mathfrak{p}$-simples sur V, elle est *a fortiori* faiblement $\mathfrak{p}$-simple, mais la réciproque est inexacte.

Exemple. — Prenons pour V la courbe plane affine d'équation $\mathrm{Y}^2=\mathrm{X}^3+t^5$. Le point (o, o) est le seul point de $\rho_e(\mathrm{V})$ qui est $\mathfrak{p}$-multiple sur V, mais on voit facilement qu'il n'appartient pas à $\mathrm{V}^0_\mathfrak{R}=\rho(\mathrm{V}_\mathfrak{R})$; donc V est faiblement $\mathfrak{p}$-simple, mais n'est pas $\mathfrak{p}$-simple.

Il résulte des définitions que tout espace homogène principal abélien faiblement $\mathfrak{p}$-simple est aussi pseudo-$\mathfrak{p}$-simple.

Nous dirons qu'une $\mathfrak{p}$-variété est *faiblement* $\mathfrak{p}$-*simple* $\mathfrak{p}$-*minimale* si V est faiblement $\mathfrak{p}$-simple et si, pour toute $\mathfrak{p}$-variété W et tout $\mathfrak{k}$-isomorphisme $\varphi : \mathrm{W}\to\mathrm{V}$, φ est $\mathfrak{p}$-morphique en tout point de $\mathscr{S}(\mathrm{W}^0)$.

Si V est une $\mathfrak{p}$-variété sans point multiple, l'existence d'un $\mathfrak{k}$-modèle faiblement $\mathfrak{p}$-simple $\mathfrak{p}$-minimal (V_*, θ) de V implique pour ce dernier certaines propriétés d'unicité. En effet, si $(\overline{\mathrm{V}}_*, \overline{\theta})$ est un autre $\mathfrak{k}$-modèle faiblement $\mathfrak{p}$-simple $\mathfrak{p}$-minimal de V, le $\mathfrak{k}$-isomorphisme $\psi : \overline{\theta}\circ\theta^{-1} : \mathrm{V}_*\to\overline{\mathrm{V}}_*$ est $\mathfrak{p}$-isomorphique en tout point de $\mathscr{S}(\mathrm{V}^0_*)$. En particulier, $\mathscr{S}(\mathrm{V}^0_*)$ et $\mathscr{S}(\overline{\mathrm{V}}^0_*)$ ont le même nombre de composantes, et on peut associer biunivoquement les composantes de $\mathscr{S}(\overline{\mathrm{V}}^0_*)$ et celles de $\mathscr{S}(\mathrm{V}^0_*)$, de manière que, si $\overline{\mathrm{C}}^0_i$ est associée à C^0_i, φ induise, pour tout i, un isomorphisme $\mathrm{C}^0_i\to\overline{\mathrm{C}}^0_i$.

On peut aussi exprimer ceci d'une manière simple avec le langage des schémas. Pour toute $\mathfrak{p}$-variété V, notons $\mathbf{S}'(\mathrm{V})$ le *schéma simple* sur $\mathfrak{R}$ déduit de $\mathbf{S}(\mathrm{V})$ par restriction au couple $(\mathrm{V}, \mathscr{S}(\mathrm{V}^0))$ (cf. chap. I[er], n° 4); soit $\mathbf{S}_\mathfrak{k}(\mathrm{V})=\mathbf{S}(\mathrm{V})\otimes_\mathfrak{R}\mathfrak{k}$ le *schéma sur* $\mathfrak{k}$ attaché à V. La propriété précédente se traduit par l'existence d'un $\mathfrak{R}$-isomorphisme canonique

$\mathbf{S}'(V_*) \to \mathbf{S}'(\overline{V}_*)$. Autrement dit, *le schéma* $\mathbf{S}'(V_*)$ *est uniquement déterminé, à un* $\mathfrak{R}$*-isomorphisme près,* par la donnée de V; plus précisément, $\mathbf{S}'(V_*)$ est déterminé, à un $\mathfrak{R}$-isomorphisme près, par la donnée de V à un $\mathfrak{k}$-isomorphisme près, i.e. par la donnée de $\mathbf{S}_{\mathfrak{k}}(V)$. Si, de plus, V et θ sont définis sur k, le schéma $\mathbf{S}'_R(V_*)$ déduit de $\mathbf{S}'(V_*)$ par restriction de $\mathfrak{R}$ à R, est déterminé à un R-isomorphisme près, par la donnée du schéma $\mathbf{S}_k(V)$.

Il existe des p-variétés n'admettant pas de modèle faiblement p-simple p-minimal. En particulier :

Proposition 6. — L'espace affine $\mathbf{S}_n$*, et l'espace projectif* $\mathbf{P}_n$ $(n \geqslant 1)$ *n'admettent pas de modèle faiblement* p*-simple* p*-minimal.*

Démonstration. — Supposons en effet qu'il existe un $\mathfrak{k}$-isomorphisme $\varphi : \mathbf{S}_n \to V$ (resp. $\mathbf{P}_n \to V$), où V est faiblement p-simple p-minimale. Soit Y^0 une composante simple de $V^0 = \rho(V^0)$. Soit k_1^0 un corps de définition de Y^0, et soit y un point générique sur k_1^0 de la (V, p)-provariété $Y = (Y^0)_g^{\#}$ obtenue en relevant génériquement Y^0. Posons $x = \varphi^{-1}(y)$, et soit $(x_1, \ldots, x_n)$ (resp. $(x_0, x_1, \ldots, x_n)$ avec $x_0 \neq 0$) un système de coordonnées (resp. de coordonnées homogènes) de x. Il existe un entier h tel que les $t^h x_i$ (resp. les $t^h x_i/x_0$) soient entiers. Notons ψ_{h+1} l'homothétie $x \to t^{h+1}x$ de $\mathbf{S}_n$ (resp. le $\mathfrak{k}$-automorphisme de $\mathbf{P}_n$ qui, au point $x = (x_0, x_1, \ldots, x_n)$ fait correspondre $(x_0, t^{h+1}x_1, \ldots, t^{h+1}x_n)$). Alors l'application $\varphi' = \varphi \circ \psi_{h+1}^{-1} : \mathbf{S}_n \to V$ (resp. $\mathbf{P}_n \to V$) est un $\mathfrak{k}$-isomorphisme. Si on pose $x' = \psi_{h+1}(x) = (\varphi')^{-1}(y)$, le point réduit $x'^0 = \rho(x')$ est l'origine $(0, \ldots, 0)$ de $\mathbf{S}_n^0$ (resp. le point $(1, 0, \ldots, 0)$ de $\mathbf{P}_n^0$). L'ensemble $(\varphi')_e^0(x'^0)$ des valeurs de φ' en x'^0 contient le lieu Y^0 du point $y^0 = \rho(y)$ sur k_1^0. Ce lieu étant de dimension $\geqslant 1$, l'application φ' n'est pas p-morphique en x'^0. Compte tenu de la p-minimalité de V, ceci conduit à une contradiction.

Proposition 7. — Soit A *un espace homogène principal abélien faiblement* p*-simple, défini sur* $\mathfrak{k}$*, et posons* $A^0 = \rho(A)$. *Les quatre propriétés suivantes sont équivalentes :*

(i) A *est* p*-minimal.*

(ii) *Pour toute application rationnelle* $\varphi : V \to A$, *définie sur k, d'une* p*-variété* quelconque V *dans* A, *et en posant* $V^0 = \rho(V)$, φ *est* p*-morphique en tout point* x^0 *de* $\mathscr{S}(V^0)$ *(et on a alors* $\varphi^0(x^0) \in \mathscr{S}(A^0)$*).*

(iii) *Tous les points de* $\rho(A_{\mathfrak{k}}) = \mathscr{S}(A^0)$ *sont* ω*-maximaux.*

(iv) *La métrique* p*-adique de* $A_{\mathfrak{k}}$ *est invariante par toute translation* $\tau \in \mathscr{T}(A)$.

Démonstration :

(ii) entraîne trivialement (i).

(iii) entraîne (ii). En effet, soit $x^0 \in \mathscr{S}(V^0)$. D'après le lemme de Hensel, il existe $x \in V_{\mathfrak{k}}$ tel que $x^0 = \rho(x)$. On a alors $y = \varphi(x) \in A_{\mathfrak{k}}$. Le point $y^0 = \rho(y)$ est simple sur A^0, puisque A est faiblement p-simple. Il est donc ω-maximal, d'après l'hypothèse. Donc, d'après le théorème 1, φ est p-morphique en x^0, de valeur y^0.

(i) entraîne (iv). En effet, soit $\tau \in \mathscr{T}(A)$, et soient x et y deux points de $A_{\mathfrak{k}}$. En appliquant (i) aux deux translations τ et $-\tau$, on voit que τ est p-isomorphique en $x^0 = \rho(x)$, de valeur $y^0 = \rho(y)$. Donc on a $(x, y)_{\mathfrak{p}} = (\tau(x), \tau(y))_{\mathfrak{p}}$.

(iv) entraîne (iii). En effet, on peut supposer $A_{\mathfrak{k}}$ non vide. Il existe au moins un

point y^0 de $\mathscr{S}(A^0)$ qui est ω-maximal, car A, étant faiblement $\mathfrak{p}$-simple, est pseudo-$\mathfrak{p}$-simple. Soit x^0 un point quelconque de $\mathscr{S}(A^0)$. D'après le lemme de Hensel, il existe des points x et y de $A_\mathfrak{f}$ tels qu'on ait $x^0=\rho(x)$ et $y^0=\rho(y)$. La translation $\tau=\tau_{xy}$ sur A est $\mathfrak{p}$-morphique en x^0, de valeur y^0, d'après le théorème 1.

D'après la proposition 11 du n° 15 du chapitre I[er], il nous suffit de montrer que τ est $\mathfrak{p}$-isomorphique en x^0. Or, s'il n'en était pas ainsi, l'ensemble $(-\tau)^0_e(y^0)$, ne pouvant admettre x^0 comme composant isolé (d'après la prop. 8 du n° 11 du chap. I[er]), contiendrait un point x'^0, distinct de x^0, et simple sur A^0.

D'après le lemme de Hensel, il existerait $x'\in A_\mathfrak{f}$ tel que $x'^0=\rho(x')$. D'après le théorème 1, τ serait $\mathfrak{p}$-morphique en x'^0, de valeur y^0. Donc, en posant $y'=\tau(x')$, on aurait $(x,y)_\mathfrak{p}>0$, tandis que $(x',y')_\mathfrak{p}=0$, ce qui contredit (iv).

Remarque. — L'implication (i) $\Rightarrow$ (iii), d'où l'équivalence des conditions (i), (ii) et (iii), se démontre plus rapidement, sans passer par (iv), en utilisant la translation τ_{xy} précédente.

Supposons toujours que A est un espace homogène principal abélien faiblement $\mathfrak{p}$-simple $\mathfrak{p}$-minimal, défini sur k; nous pouvons maintenant préciser la structure de l'espace homogène principal $A_\mathfrak{R}=A_\mathfrak{f}$ des points rationnels $\mathfrak{p}$-adiques de A.

D'après (ii), la loi γ_A est $\mathfrak{p}$-morphique en tout triplet y_1^0, x_1^0, x_2^0 composé de points de $A_\mathfrak{f}^0=\mathscr{S}(A^0)$, et sa valeur $y_2^0=\gamma_A^0(y_1^0, x_1^0, x_2^0)$ est encore un point de $\mathscr{S}(A^0)$. On voit immédiatement que la loi γ_A^0 ainsi définie sur $\mathscr{S}(A^0)$ vérifie les axiomes des espaces homogènes principaux. Pour tout triplet (Y_1^0, X_1^0, X_2^0) de composantes simples de A^0, la loi γ_A induit d'autre part une application rationnelle $\psi^0 : Y_1^0\times X_1^0\times X_2^0\to Y_2^0$, où Y_2^0 est une composante simple de A^0. Si, de plus, on désigne par S_i^0, T_i^0 $(i=1, 2)$ les ouverts $S_i^0=X_i^0\cap\mathscr{S}(A^0)$ et $T_i^0=Y_i^0\cap\mathscr{S}(A^0)$ de X_i^0 et Y_i^0 respectivement, cette application ψ^0 est, d'après ce qui précède, morphique en tout point de $T_1^0\times S_1^0\times S_2^0$. Enfin, comme γ_A induit une application k^0-rationnelle sur toute k^0-composante simple de $A^0\times A^0\times A^0$, on voit que la loi γ_A^0 définit sur $\mathscr{S}(A^0)=A_\mathfrak{f}^0$ une structure d'espace homogène principal algébrique, défini sur k^0.

Plus généralement nous allons définir pour tout $\mu\geqslant 0$, une structure analogue sur l'ensemble $A_\mathfrak{f}^\mu=\rho^\mu(A_\mathfrak{f})$.

Remarquons d'abord que, si S^0 est une composante quelconque de $\mathscr{S}(A^0)$, d'adhérence X^0, le (A, $\mathfrak{p}$)-ensemble $S=(S^0)^\#$ est irréductible (chap. I[er], n° 23, remarque *c)*) et, de plus, coïncide avec la (A, $\mathfrak{p}$)-provariété ω-maximale $X=\operatorname{adh} S=(X^0)^\#_g$. En effet, on a $S\subset X$; inversement, si $x\in X$, on a aussi $x\in A_\mathfrak{f}$, donc x est simple (mod. $\mathfrak{p}$) sur A, puisque A est faiblement $\mathfrak{p}$-simple, et le point réduit $x^0=\rho(x)$ appartient à $\mathscr{S}(A)\cap X^0=S^0$, ce qui implique $x\in S$; on a donc $X\subset S$, d'où $X=S$. On en déduit, en même temps, que les (A, $\mathfrak{p}$)-provariétés ω-maximales sont deux à deux disjointes, et que $A_\mathfrak{f}$ est leur réunion. Nous les appellerons aussi les *composantes* de $A_\mathfrak{f}$. Pour tout entier $\mu\geqslant 0$, on peut, à toute composante X de $A_\mathfrak{f}$, faire correspondre le sous-ensemble $S^\mu=\rho^\mu(X)$ de $A_\mathfrak{f}^\mu$; ce sous-ensemble est un ouvert de la variété $X^\mu=\overline{\rho}^\mu(X)$; on a, inversement, $X=(S^\mu)^\#=(X^\mu)^\#_g$, et l'application qui, pour μ fixé, fait correspondre à la composante X

de $A_\mathfrak{t}$ le sous-ensemble S^μ de $A_\mathfrak{t}^\mu$ est bijective. Pour μ fixé, les S^μ sont deux à deux disjoints, et leur réunion est $A_\mathfrak{t}^\mu$; nous dirons que ce sont les *composantes* de $A_\mathfrak{t}^\mu$.

Pour tout triplet (Y_1, X_1, X_2) de (A, p)-provariétés ω-maximales (i.e., dans le cas particulier considéré, de composantes de $A_\mathfrak{t}$), on a vu (prop. 1 du n° 3) que $Y_2 = (\gamma_A)_g(Y_1, X_1, X_2)$ est encore une (A, p)-provariété ω-maximale. De plus (chap. I[er], n° 24, prop. 24 et remarque *a)*), φ est promorphique (et non pas seulement « génériquement promorphique ») d'indice o sur (Y_1, X_1, X_2). Autrement dit, si pour tout $\mu \geqslant 0$, on pose $S_i^\mu = \rho^\mu(X_i)$ et $T_i^\mu = \rho^\mu(Y_i)$ $(i = 1, 2)$, on a, pour tout μ, un morphisme $\psi^\mu : T_1^\mu \times S_1^\mu \times S_2^\mu \to T_2^\mu$ tel qu'on ait :

$$\psi^\mu(\rho^\mu(y_1) \cdot \rho^\mu(x_1) \cdot \rho^\mu(x_2)) = \rho^\mu(\gamma_A(y_1, x_1, x_2)) \tag{4}$$

quels que soient $x_1 \in X_1$, $x_2 \in X_2$ et $y_1 \in Y_1$. En réunissant les applications ψ^μ respectivement associées aux différents triplets (Y_1, X_1, X_2), on définit une loi ternaire γ_A^μ sur l'ensemble $A_\mathfrak{t}^\mu$; tenant compte de la relation (4), on voit que cette loi vérifie les axiomes des espaces homogènes principaux. Enfin, on remarque que γ_A induit une application k^0-rationnelle sur toute k^0-composante de $A_\mathfrak{t}^\mu \times A_\mathfrak{t}^\mu \times A_\mathfrak{t}^\mu$. Donc la loi γ_A^μ définit sur $A_\mathfrak{t}^\mu$ une structure d'espace homogène principal algébrique, défini sur k^0.

L'espace homogène principal $A_\mathfrak{t}$ est la limite projective de la suite

$$A_\mathfrak{t}^0 \leftarrow A_\mathfrak{t}^1 \leftarrow \ldots \leftarrow A_\mathfrak{t}^\mu \leftarrow \ldots \tag{5}$$

où les flèches (induites par les morphismes θ^μ), sont des homomorphismes surjectifs, pour la structure d'espace homogène principal algébrique. Nous traduirons cette propriété en disant que $A_\mathfrak{t}$ est un *espace homogène principal proalgébrique*, défini sur k^0.

Si, en particulier, A est une variété abélienne, définie sur k^0, la loi de groupe $\gamma_{A,0}$ induit sur chacun des $A_\mathfrak{t}^\mu$ une structure de groupe algébrique, défini sur k^0. Le groupe $A_\mathfrak{t}$, limite projective de la suite (4), est alors un *groupe proalgébrique* au sens de Serre [19] ([1]). La proposition 21 du chapitre I[er] entraîne que, pour tout μ, $A_\mathfrak{t}^{\mu+1}$ est une extension de $A_\mathfrak{t}^\mu$ par $(\mathfrak{k}^0)^r$ (puissance r-ième du groupe additif sur $\mathfrak{k}^0$).

8. Existence d'un k-modèle faiblement p-simple p-minimal de A.

Théorème 2. — Tout espace homogène principal abélien A, *défini sur k, admet un k-modèle* (A_*, θ) *faiblement* p*-simple* p*-minimal.*

Nous allons, plus précisément, donner plus loin, dans le théorème 2*, un procédé de construction d'un tel modèle, en supposant que A est pseudo-p-simple (on a vu, par ailleurs, que tout espace homogène principal abélien défini sur k admet un k-modèle pseudo-p-simple).

Introduisons au préalable quelques notations. Comme au n° 25 du chapitre I[er], désignons, pour tout entier $s \geqslant 0$, par M_s le R-module composé des polynômes homogènes

([1]) Voir aussi [4], où est utilisée également l'expression de $A_\mathfrak{t}$ comme limite de la suite (5), dans le cas particulier d'une réduction strictement non dégénérée. Pour une étude locale de $A_\mathfrak{t}$ dans le cas d'un modèle quelconque, voir [12] et [13].

et de degré s de l'anneau $R[X]$; désignons de même par $\mathfrak{M}_s$ le $\mathfrak{R}$-module composé des polynômes homogènes et de degré s de l'anneau $\mathfrak{R}[X]$. Considérons une variété projective quelconque V, définie sur k ($V \subset \mathbf{P}_n$). Soit X^0 un cycle de la forme $\Sigma_\gamma \mu_\gamma C^0_\gamma$, où les C^0_γ sont des composantes de $V^0 = \rho(V)$, et les μ_γ des entiers >0. On peut trouver un entier s tel qu'il existe un polynôme $P_0 \in M_s$ ne s'annulant sur aucune des variétés C^0_γ. A tout polynôme $P \in \mathfrak{M}_s$, associons alors la fonction f sur V induite par P/P_0. Nous désignerons par $J_s(X^0)$ (resp. $\mathfrak{J}_s(X^0)$) le sous-R-module de M_s (resp. le sous-$\mathfrak{R}$-module de $\mathfrak{M}_s$) composé des polynômes P tels qu'on ait $X^0 \prec (f)_\mathfrak{p}$, où $(f)_\mathfrak{p}$ est le $\mathfrak{p}$-diviseur de f (ou, ce qui revient au même, tels que, pour tout γ, la fonction $ft^{-\mu_\gamma}$, induite sur V par $t^{-\mu_\gamma} P/P_0$, soit génériquement $\mathfrak{p}$-morphique sur C^0_γ).

Proposition 8. — *Le $\mathfrak{R}$-module $\mathfrak{J}_s(X^0)$ est engendré par $J_s(X^0)$ (donc $\mathfrak{J}_s(X^0)$ est isomorphe à $J_s(X^0) \otimes_R \mathfrak{R}$).*

Démonstration. — Soit $P \in \mathfrak{J}_s(X^0)$; exprimons-le sous la forme $P = \Sigma_\alpha a_\alpha M_\alpha(X)$, où les M_α sont des monômes distincts de degré s, et où les a_α appartiennent à $\mathfrak{R}$.

Soit μ un entier $\geqslant 0$. On peut (comme il résulte, par exemple, d'un raisonnement par récurrence très simple) trouver un nombre fini d'éléments b_i ($1 \leqslant i \leqslant h$) de $\mathfrak{R}$ (dépendant de μ), tels que les $b_i^0 = \rho(b_i)$ soient linéairement indépendants sur k^0, et tels qu'on ait, pour tout α, dans l'anneau $\mathfrak{R}$, une congruence de la forme

$$a_\alpha \equiv \Sigma_i c_{\alpha i} b_i \qquad (\text{mod. } t^\mu),$$

où les $c_{\alpha i}$ appartiennent à R.

Posons, comme plus haut, $X^0 = \Sigma_\gamma \mu_\gamma C^0_\gamma$, et appliquons la propriété précédente, en prenant $\mu = \sup_\gamma \mu_\gamma$. On obtient, dans l'anneau $\mathfrak{R}[X]$, la congruence

$$P \equiv \Sigma_i b_i P_i \qquad (\text{mod. } t^\mu),$$

en posant, pour $1 \leqslant i \leqslant h$,

$$P_i = \Sigma_\alpha c_{\alpha i} M_\alpha.$$

Or, d'après ([F], II-4, prop. 19), on peut trouver des k^0-automorphismes $\sigma_1^0, \ldots, \sigma$ de $\mathfrak{k}^0$, en nombre h, tels que le déterminant D^0 de la matrice $(\sigma_j^0(b_i^0))$ soit non nul. Pour tout j, notons σ_j le $\hat{R}$-automorphisme de $\mathfrak{R}$ obtenu en relevant σ_j^0, c'est-à-dire l'automorphisme qui fait correspondre à l'élément $x = (x^{(0)}, \ldots, x^{(\nu)}, \ldots)$ de $\mathfrak{R}$ celui obtenu par application de σ_j^0 à chacun des $x^{(\nu)}$; notons $\overline{P}_j$ le polynôme déduit de P par application de σ_j à chacun de ses coefficients. On a, pour tout j,

$$\overline{P}_j \equiv \Sigma_i \sigma_j(b_i) P_i \qquad (\text{mod. } t^\mu).$$

On en déduit une relation de la forme

$$DP_i \equiv \Sigma_j e_{ij} \overline{P}_j \qquad (\text{mod. } t^\mu), \tag{6}$$

où D est le déterminant $\det(\sigma_j(b_i))$, et où les e_{ij} sont des éléments de $\mathfrak{R}$. Or D est un élément inversible de $\mathfrak{R}$, puisqu'on a $D^0 = \rho(D) \neq 0$. Puisque P appartient à $\mathfrak{J}_s(X^0)$, il en est de même de chacun des $\overline{P}_j$. Compte tenu du choix de μ, et d'après la relation (6), il en

est de même également de chacun des P_i. Comme on a $P_i \in R[X]$, on a aussi $P_i \in J_s(X^0)$, pour tout i; donc P appartient bien au $\mathfrak{R}$-module engendré par $J_s(X^0)$.

Théorème 2.* — *Soit* A *un espace homogène principal abélien pseudo-*p*-simple, contenu dans l'espace projectif* $\mathbf{P}_n$, *et notons* X^0 *le cycle* $\Sigma_\gamma C^0_\gamma$, *somme de toutes les composantes simples* ω*-maximales* C^0_γ *de* $A^0 = \rho(A)$. *On peut trouver deux entiers positifs* s *et* μ, *tels que toute transformation* $\xi \in \mathscr{M}^*_s(J_s(\mu X^0), \mathbf{P}_n)$ *induise un* k*-isomorphisme* $\theta : A \to A_*$, *où* A_* *est un espace homogène principal abélien faiblement* p*-simple* p*-minimal.*

Démonstration. — Pour tout entier $u \geqslant 0$, notons L_u le système linéaire des sections de A par les hypersurfaces de degré u. On peut trouver un entier positif s_0 vérifiant les conditions suivantes :

(i) Il existe un polynôme $Q_0 \in M_{s_0}$ ne s'annulant sur aucune des composantes simples ω-maximales C^0_γ.

(ii) En posant $s = 2s_0$, le système linéaire L_s est complet.

Soit alors $\mathscr{L}_0$ l'espace vectoriel sur $\mathfrak{k}$ composé des fonctions sur A induites par les quotients de la forme Q/Q_0, où $Q \in \mathfrak{k}[X_0, \ldots, X_n]$ est homogène et de degré s_0. Choisissons des polynômes $Q_i \in \mathfrak{M}_{s_0}$ $(1 \leqslant i \leqslant r)$ de façon que les fonctions φ_i sur A respectivement induites par les Q_i/Q_0 forment un système de générateurs de $\mathscr{L}_0$, et que les polynômes réduits $Q^0_i = \rho(Q_i)$ n'admettent aucun zéro commun non trivial. Notons D_0 le diviseur positif section de A par l'hypersurface $Q_0(X) = 0$. Le système linéaire L_{s_0} se compose des diviseurs de la forme $D_0 + (f)$, avec $f \in \mathscr{L}_0$; en particulier, pour tout i, nous noterons D_i l'élément de L_{s_0} défini par $D_i = D_0 + (\varphi_i)$. Comme le système L_{s_0} est ample, l'application rationnelle $\mathbf{P}_n \to \mathbf{P}_r$ admettant pour coordonnées homogènes les fonctions $\varphi_0 = 1, \varphi_1, \ldots, \varphi_r$ induit un $\mathfrak{k}$-isomorphisme $\varphi : A \to A'$ de A sur une sous-variété A′ de $\mathbf{P}_r$.

Introduisons maintenant un recouvrement fini $\{S_\alpha\}$ $(1 \leqslant \alpha \leqslant q)$ de A, et, pour tout α, une translation τ_α sur A, rationnelle sur $\mathfrak{k}$, tels que les conditions de la proposition 3 soient satisfaites. Pour tout triplet d'entiers (i, j, α) $(0 \leqslant i \leqslant r,\ 0 \leqslant j \leqslant r,\ 1 \leqslant \alpha \leqslant q)$, le diviseur $D'_{ij\alpha} = (D_i)_{\tau_\alpha} + (D_j)_{-\tau_\alpha} - D_i - D_j$ appartient au groupe $\mathscr{D}'_1(A)$, d'après les propositions 4 et 5 du n° 6; il existe donc une fonction $\psi'_{ij\alpha}$ sur A, définie sur $\mathfrak{k}$, telle que $(\psi'_{ij\alpha}) = D'_{ij\alpha}$, et qui est génériquement p-morphique et non nulle sur chacune des composantes simples ω-maximales C^0_γ de A^0. La fonction $\psi_{ij\alpha}$ sur A définie par $\psi_{ij\alpha} = \psi'_{ij\alpha}\varphi_i\varphi_j$ est donc génériquement p-morphique sur chacune des C^0_γ. Or on a $(\psi_{ij\alpha}) = (D_i)_{\tau_\alpha} + (D_j)_{-\tau_\alpha} - 2D_0$. Comme le système linéaire L_s est complet, il existe un polynôme $Q_{ij\alpha}$, appartenant à $\mathfrak{k}[X_0, \ldots, X_n]$, homogène et de degré s, tel que $\psi_{ij\alpha}$ soit induite sur A par $Q_{ij\alpha}/Q_0^2$. Nous allons prendre pour μ un entier tel que tous les polynômes $\overline{Q}_{ij\alpha} = Q_{ij\alpha}t^\mu$ soient à coefficients dans $\mathfrak{R}$. Ces polynômes sont alors des éléments de $\mathfrak{J}_s(\mu X^0)$.

Les entiers s et μ étant ainsi choisis, soit $\mathscr{B} = \{P_0, \ldots, P_m\}$ un système de générateurs arbitraire du R-module $J_s(\mu X^0)$. D'après la proposition 8, c'est aussi un système de générateurs du $\mathfrak{R}$-module $\mathfrak{J}_s(\mu X^0)$. Considérons la transformation $\xi \in \mathscr{M}^*_s(J_s(\mu X^0), \mathbf{P}_n)$ attachée à ce système, et le k-isomorphisme $\theta : A \to A_*$ induit par ξ. Soit $\overline{x}$ un point générique de A sur k, de coordonnées homogènes $\overline{x}_0, \ldots, \overline{x}_n$. Par construction, la

variété A_* est le lieu sur k du point $\overline{x}_* = \xi(\overline{x}) = \theta(\overline{x})$, ayant pour coordonnées homogènes les $\overline{x}_{*h} = P_h(\overline{x})$ $(o \leqslant h \leqslant m)$.

Il nous suffit de démontrer que A_* vérifie la condition (ii) de la proposition 7 du n° 7, autrement dit que si x_* est un point quelconque de $(A_*)_{\mathfrak{k}}$, le point réduit $x_*^0 = \rho(x_*)$ est simple ω-maximal sur A^0. Pour un tel point x_*, considérons le point $x = \theta^{-1}(x_*)$ de $A_{\mathfrak{k}}$. Il existe un α tel que les deux points $y = x_{-\tau_\alpha}$ et $y' = x_{\tau_\alpha}$ soient simples et ω-maximaux (mod. $\mathfrak{p}$). Notons $\widetilde{\theta}_\alpha$ le $\mathfrak{k}$-isomorphisme $\widetilde{\theta}_\alpha = \theta \circ \tau_\alpha : A \to A_*$. Comme on a $x_* = \widetilde{\theta}_\alpha(y)$, le point $x_*^0 = \rho(x_*)$ appartient à l'ensemble des valeurs de $\widetilde{\theta}_\alpha$ en $y^0 = \rho(y)$. Comme y^0 est simple ω-maximal sur A^0, il nous suffit de montrer que $\widetilde{\theta}_\alpha$ est $\mathfrak{p}$-isomorphique en y^0.

Pour $o \leqslant h \leqslant m$, notons θ_h la fonction induite sur A par $t^{-\mu} P_h / Q_0^2$. Choisissons un i_0 tel que $Q_{i_0}^0(y^0) \neq o$, d'où $y^0 \notin \rho_e(D_{i_0})$, et un j_0 tel que $Q_{j_0}^0(y'^0) \neq o$, d'où $y'^0 \notin \rho_e(D_{j_0})$; posons $\eta_{h\alpha} = \theta_h / \psi_{i_0 j_0 \alpha}$. Les $\eta_{h\alpha}(\overline{x})$ constituent (pour α fixé, et pour $o \leqslant h \leqslant m$) un système de coordonnées homogènes du point $\overline{x}_*$. Posons, quels que soient h et α, $\widetilde{\eta}_{h\alpha} = \eta_{h\alpha} \circ \tau_\alpha$, de sorte que $\widetilde{\eta}_{h\alpha}(\overline{x}) = \eta_{h\alpha}(\overline{x}_{\tau_\alpha})$. Le diviseur de la fonction $\eta_{h\alpha}$ est de la forme $D'_h - (D_{i_0})_{\tau_\alpha} - (D_{j_0})_{-\tau_\alpha}$, où D'_h est un diviseur positif de A, rationnel sur $\mathfrak{k}$. Celui de la fonction $\widetilde{\eta}_{h\alpha}$ est donc $(D'_h)_{-\tau_\alpha} - D_{i_0} - (D_{j_0})_{-2\tau_\alpha}$. D'après le théorème 1, la translation $-2\tau_\alpha$ est $\mathfrak{p}$-isomorphique en y^0, de valeur y'^0. Puisqu'on a $y'^0 \notin \rho_e(D_{j_0})$, on a aussi $y^0 \notin \rho_e(D_{j_0})_{-2\tau_\alpha}$. Comme on a, d'autre part, $y^0 \notin \rho_e(D_{i_0})$, on a $y^0 \notin \{\widetilde{\eta}_{h\alpha}\}_{\mathfrak{p},\infty}$. Donc, d'après le corollaire de la proposition 10 du n° 12 du chapitre I^er, $\widetilde{\eta}_{h\alpha}$ est $\mathfrak{p}$-morphique en y^0. De plus, $\eta_{h\alpha}$ est induite sur A par le quotient $P_h / \overline{Q}_{i_0 j_0 \alpha}$. Puisque $\overline{Q}_{i_0 j_0 \alpha} \in \mathfrak{J}_s(\mu X^0)$, le $\mathfrak{R}$-module engendré (pour α fixé) par les $\eta_{h\alpha}$ contient 1. Il en est donc de même de celui engendré par les $\widetilde{\eta}_{h\alpha}$. Donc les $\widetilde{\eta}_{h\alpha}$ ne s'annulent pas toutes en y^0. Donc $\widetilde{\theta}_\alpha$ est $\mathfrak{p}$-morphique en y^0 (et nécessairement de valeur x_*^0).

Posons maintenant, pour $o \leqslant i \leqslant r$, $\lambda_{i\alpha} = \psi_{ij_0\alpha} / \psi_{i_0 j_0 \alpha}$, puis $\widetilde{\lambda}_{i\alpha} = \lambda_{i\alpha} \circ \tau_\alpha$, et remarquons qu'on a $(\widetilde{\lambda}_{i\alpha}) = D_i - D_{i_0}$; on a donc des relations de la forme $\widetilde{\lambda}_{i\alpha} = a_{i\alpha} \varphi_i / \varphi_{i_0}$, où les $a_{i\alpha}$ sont des constantes (i.e. des éléments de k). D'après le choix des $\psi_{ij\alpha}$, les $a_{i\alpha}$ sont de plus des éléments inversibles de $\mathfrak{R}$. D'autre part, on a, pour tout i, $\overline{Q}_{ij_0\alpha} \in \mathfrak{J}_s(\mu X^0)$; donc $\lambda_{i\alpha}$ appartient au $\mathfrak{R}$-module engendré par les $\eta_{h\alpha}$ et, par suite, $\widetilde{\lambda}_{i\alpha}$ appartient au $\mathfrak{R}$-module engendré par les $\widetilde{\eta}_{h\alpha}$; autrement dit, on a des relations de la forme $\widetilde{\lambda}_{i\alpha} = \sum_{h=0}^m b_{ih} \widetilde{\eta}_{h\alpha}$, où les b_{ih} sont des éléments de $\mathfrak{R}$. En faisant $i = i_0$, on obtient, en particulier, $1 = \sum_{h=0}^m b_{i_0 h} \widetilde{\eta}_{h\alpha}$. Or les $\overline{x}_{*h} = \widetilde{\eta}_{h\alpha}(\overline{y})$ (resp. les $x_{*h}^0 = \widetilde{\eta}_{h\alpha}^0(y^0)$) forment un système de coordonnées homogènes du point $\overline{x}_*$ (resp. x_*^0); les relations précédentes entraînent $a_{i\alpha} \varphi_i(\overline{y}) / \varphi_{i_0}(\overline{y}) = (\sum_h b_{ih} \overline{x}_{*h}) / (\sum_h b_{i_0 h} \overline{x}_{*h})$ $(o \leqslant i \leqslant r)$ et $\sum_h b_{i_0 h}^0 x_{*h}^0 = 1$. Donc les fonctions $(\varphi_i / \varphi_{i_0}) \circ \theta_\alpha^{-1}$ sur A_* sont $\mathfrak{p}$-morphiques en x_*^0. Les $\varphi_i(\overline{y}) / \varphi_{i_0}(\overline{y})$ sont, d'autre part, un système de coordonnées homogènes du point $\overline{y}' = \varphi(y)$ de A', où (A', φ) est le $\mathfrak{k}$-modèle de A considéré au début de la démonstration. L'application $\varphi'_\alpha = \varphi \circ \widetilde{\theta}_\alpha^{-1} : A_* \to A'$ est donc $\mathfrak{p}$-morphique en x^0. Comme $\varphi : A \to A'$ est un $\mathfrak{R}$-isomorphisme, il en résulte aussitôt, par application de la proposition 1 du chapitre I^er, que $\theta_\alpha^{-1} = \varphi^{-1} \circ \varphi'_\alpha$ est $\mathfrak{p}$-morphique en x_*^0 (et nécessairement de valeur y^0). C.Q.F.D.

9. Propriétés fonctorielles des modèles faiblement p-simples p-minimaux.

Soient A et B deux espaces homogènes principaux abéliens (resp. deux variétés abéliennes), définis sur k, et soit $\varphi : A \to B$ un k-morphisme. Soient (A_*, α) et (B_*, β) des k-modèles faiblement p-simples p-minimaux de A et B respectivement. Alors, d'après le théorème 1, l'application $\varphi_* = \beta \circ \varphi \circ \alpha^{-1} : A_* \to B_*$ est p-morphique en tout point de $\mathscr{S}(A_*^0) = (A_*)_{\mathfrak{k}}^0$. On déduit de φ_*, par réduction (mod. p), une application $\varphi_*^0 : (A_*)_{\mathfrak{k}}^0 \to (B_*)_{\mathfrak{k}}^0$, qui est nécessairement un k^0-morphisme pour la structure d'espace homogène principal algébrique (resp. de groupe algébrique) introduite au n° 7. De plus, φ est promorphique d'indice o sur chaque composante de $(A_*)_{\mathfrak{k}}$. On en déduit, compte tenu de la proposition 24 du chapitre I^er^, qu'on a, pour tout $\mu \geqslant o$, une application $\varphi_*^\mu : (A_*)_{\mathfrak{k}}^\mu \to (B_*)_{\mathfrak{k}}^\mu$ qui est encore un k^0-morphisme pour la même structure que plus haut, telle qu'on ait $\varphi_*^\mu(\rho^\mu(x_*)) = \rho^\mu(\varphi_*^\mu(x_*))$ pour tout $x_* \in (A_*)_{\mathfrak{k}}$. On a le diagramme commutatif

$$\begin{array}{ccccccccc}
(A_*)_{\mathfrak{k}}^0 & \longleftarrow & (A_*)_{\mathfrak{k}}^1 & \longleftarrow & \dots & \longleftarrow & (A_*)_{\mathfrak{k}}^\mu & \longleftarrow & \dots \\
\downarrow{\scriptstyle \varphi_*^0} & & \downarrow{\scriptstyle \varphi_*^1} & & & & \downarrow{\scriptstyle \varphi_*^\mu} & & \\
(B_*)_{\mathfrak{k}}^0 & \longleftarrow & (B_*)_{\mathfrak{k}}^1 & \longleftarrow & \dots & \longleftarrow & (B_*)_{\mathfrak{k}}^\mu & \longleftarrow & \dots
\end{array}$$

L'application $(\varphi_*)_{\mathfrak{k}} : (A_*)_{\mathfrak{k}} \to (B_*)_{\mathfrak{k}}$ induite par φ (et qui est évidemment un homomorphisme pour la structure d'espace homogène principal (resp. de groupe)) peut donc être qualifiée de *k^0-morphisme* pour la structure d'espace homogène principal proalgébrique (resp. de groupe proalgébrique) considérée au n° 7.

En particulier, si $\varphi : A \to B$ est un k-isomorphisme, les k^0-morphismes $\varphi_*^0, \dots, \varphi_*^\mu, \dots$, et $(\varphi_*)_{\mathfrak{k}}$ sont des k^0-isomorphismes. Autrement dit, les espaces homogènes principaux algébriques (resp. les groupes algébriques) $(A_*)_{\mathfrak{k}}^0, \dots, (A_*)_{\mathfrak{k}}^\mu, \dots$, et leur limite projective $(A_*)_{\mathfrak{k}}$ sont *uniquement déterminés, à un k^0-isomorphisme près*, par la donnée de A, et, plus précisément, par celle du schéma $\mathbf{S}_k(A)$; ils sont même déterminés *par la donnée du corps $k(A)$ des fonctions sur* A rationnelles sur k, puisqu'on sait que toute application birationnelle $A \to B$, définie sur k (où A et B sont des espaces homogènes principaux abéliens) est nécessairement un k-isomorphisme. Nous désignerons parfois l'espace homogène principal algébrique (resp. le groupe algébrique) $(A_*)_{\mathfrak{k}}^0 = \mathscr{S}(A_*^0)$ par $\mathscr{G}_{\mathfrak{p}}(A)$. Dans le cas où A est une variété abélienne, la composante de l'origine de $\mathscr{G}_{\mathfrak{p}}(A)$ sera désignée par $\mathscr{G}_{\mathfrak{p}0}(A)$; le groupe quotient $\mathscr{G}_{\mathfrak{p}}(A)/\mathscr{G}_{\mathfrak{p}0}(A)$ est isomorphe au groupe $\Gamma(A)$ introduit au n° 3.

On remarquera que si A, B, C sont trois espaces homogènes principaux abéliens, si $\varphi : A \to B$ et $\psi : B \to C$ sont des k-morphismes, et si (A_*, α), (B_*, β) et (C_*, γ) sont trois modèles faiblement p-simples p-minimaux de A, B et C respectivement, on a les formules $(\psi \circ \varphi)_*^\mu = \psi_*^\mu \circ \varphi_*^\mu$ $(\mu \geqslant o)$ et $((\psi \circ \varphi)_*)_{\mathfrak{k}} = (\psi_*)_{\mathfrak{k}} \circ (\varphi_*)_{\mathfrak{k}}$.

D'autre part, si $C = A \times B$, et si (A_*, α) et (B_*, β) sont des modèles faiblement p-simples p-minimaux de A et B respectivement, le couple (C_*, γ), composé de $C_* = A_* \times B_*$,

et du k-isomorphisme $\gamma : C \to C^*$, défini par $\gamma(x, y) = \alpha(x) \times \beta(y)$, est un modèle faiblement $\mathfrak{p}$-simple $\mathfrak{p}$-minimal de C.

Il peut arriver (et ceci quelles que soient les caractéristiques de k et de k^0) que le k-morphisme $\varphi : A \to B$ soit *surjectif* sans qu'il en soit de même de $(\varphi_*)_{\mathfrak{k}} : (A_*)_{\mathfrak{k}} \to (B_*)_{\mathfrak{k}}$ (c'est-à-dire de $\varphi_{\mathfrak{k}} : A_{\mathfrak{k}} \to B_{\mathfrak{k}}$) ni de $\varphi^0_* = (A_*)^0_{\mathfrak{k}} \to (B_*)^0_{\mathfrak{k}}$.

On verra par exemple, au chapitre III, que si A est la courbe plane elliptique ayant pour équation $Y^2Z + \lambda XYZ = X^3 + \alpha X^2Z + \gamma Z^3$, dans le plan projectif $\mathbf{P}_2$, où λ, α, γ sont des éléments de R tels qu'on ait $v(\lambda^2 + 4\alpha) = 0$, et $v(\gamma) = -m$ $(m > 0)$, le groupe $\mathscr{G}_{\mathfrak{p}}(A) = (A_*)^0_{\mathfrak{k}} = \mathscr{S}(A^0_*)$ est une extension du groupe multiplicatif sur k^0 par un groupe cyclique fini d'ordre m. Considérons l'application $\varphi : A \to A$, définie par $\varphi(x) = mx$. L'image de l'application φ^0_* correspondante est la composante de l'origine de $\mathscr{S}(A^0_*)$. Si $m > 1$, elle est donc distincte de $\mathscr{S}(A^0)$, et les k^0-morphismes φ^0_* et $(\varphi_*)_{\mathfrak{k}}$ ne sont pas surjectifs.

Il existe cependant un cas où ces morphismes sont toujours surjectifs : celui où A est strictement non dégénérée (mod. $\mathfrak{p}$) (without defect for $\mathfrak{p}$). En effet, φ est nécessairement partout $\mathfrak{p}$-morphique, et applique $\mathscr{S}(A^0_*)$ sur $\mathscr{S}(B^0_*)$, d'après le théorème 1. Ceci implique de plus que $\mathscr{S}(B^0_*)$ est une variété abélienne. En particulier, $\mathscr{S}(B^0_*)$ est une variété complète, i.e. est une composante de B^0_*, donc ne rencontre pas les autres composantes de B^0_*. Puisque $\rho_e(B_*) = \operatorname{supp} B^0_*$ est connexe, $\mathscr{S}(B^0_*)$ est l'unique composante de B^0_*. Donc B_* est non dégénérée (mod. $\mathfrak{p}$); on retrouve là un résultat de Koizumi et Shimura ([9], § 6, th. 4).

Si $\varphi : B \to A$ est *injectif*, le k^0-morphisme $(\varphi_*)_{\mathfrak{k}} : (B_*)_{\mathfrak{k}} \to (A_*)_{\mathfrak{k}}$ est injectif. Nous allons montrer que, si k^0 est de caractéristique nulle, les k^0-morphismes φ^μ_* $(\mu \geqslant 0)$ sont aussi injectifs. Nous allons, pour cela, démontrer préalablement deux lemmes.

Lemme 1. — *Soient* U *et* V *deux variétés algébriques sans point multiple, et soit* $f : U \to V$ *un morphisme surjectif. Soient* U′ *une sous-variété de* U *sans point multiple, et supposons que le morphisme* $f' : U' \to V$, *obtenu par restriction de* f *à* U′, *est surjectif. Soit* X *une sous-variété de* V *telle que le symbole* $(f')^{-1}(X)$ (*au sens de* [F], VIII-4) *soit défini. Alors le symbole* $f^{-1}(X)$ *l'est également et on a* $(f')^{-1}(X) = (f^{-1}(X)) . U'$.

Démonstration. — En effet, soit Γ le graphe de f. Puisque f est un morphisme, l'intersection $\Gamma \cap (U' \times V)$ admet une composante unique Γ', nécessairement simple sur $U' \times V$, et qui est le graphe de f'. Par définition du symbole $(f')^{-1}(X)$, on a

$$Y' = (f')^{-1}(X) = \mathrm{pr}_U Z',$$

avec $Z' = \{\Gamma' . (U' \times X)\}_{U' \times V}$. L'intersection $\Gamma \cap (U' \times X) = \Gamma \cap (U \times X) \cap (U' \times V)$ n'ayant que des composantes propres dans $U \times V$, il en est de même de $\Gamma \cap (U \times X)$ ([F], VI-2, th. 5). Par suite, le produit d'intersection $Z = \Gamma . (U \times X)$ est défini. Donc le cycle $Y = f^{-1}(X)$ est défini, et on a $Y = f^{-1}(X) = \mathrm{pr}_U Z$.

D'après ([F], VIII-4, th. 10), on a $Z' = \{\Gamma' . (U' \times X)\}_{U' \times V} = \{\Gamma' . (U \times X)\}_{U \times V}$. D'après l'associativité des produits d'intersection ([F], VI-2, th. 5), on a donc, dans le produit $U \times V$, $Z' = (\Gamma . (U' \times V)) . (U \times X) = (\Gamma . (U \times X)) . (U' \times V) = Z . (U' \times V)$. La

projection sur U induit un isomorphisme $\Gamma \to U$, puisque φ est un morphisme. Puisque U est sans point multiple, il en est donc de même de Γ. En appliquant à nouveau ([F], VIII-4, th. 10) on obtient $Z' = \{Z.(U' \times V)\}_{U \times V} = \{Z.\Gamma'\}_\Gamma$, d'où, en projetant sur U, $Y' = \{Y.U'\}_U$. C.Q.F.D.

Avant d'énoncer le second lemme, introduisons encore une notation. Si H est un espace homogène principal, a un élément de H, et m un entier, nous désignerons par $\Theta(a, m, H)$ l'application $H \to H$ qui, à $x \in H$, fait correspondre $y \in H$ défini par $y - a = m(x - a)$. Si $H = A$ est un espace homogène principal abélien, une telle application est toujours un homomorphisme. Nous conviendrons, d'autre part, toutes les fois que C est une composante d'un cycle X, de noter $\mu(C, X)$ le coefficient de C dans X.

Lemme 2. — *Soit* A *un espace homogène principal abélien, faiblement* $\mathfrak{p}$*-simple* $\mathfrak{p}$*-minimal, défini sur k. Soient a et b deux points de* $A_\mathfrak{k}$, *et soit m un entier* > 0, *non multiple de la caractéristique de* k^0; *posons* $\theta = \Theta(a, m, A)$. *Posons d'autre part* $a^0 = \rho(a)$, $b^0 = \rho(b)$, *et* $\overline{\theta}^0 = \Theta(a^0, m, \mathscr{S}(A^0))$. *Considérons le cycle positif, de dimension* 0, $\mathfrak{a} = \theta^{-1}(b)$, *et le cycle réduit* $\mathfrak{a}^0 = \rho(\mathfrak{a})$. *Pour qu'un point* $x^0 \in \mathscr{S}(A^0)$ *soit un composant du cycle* $\mathfrak{a}^0$, *il faut et il suffit qu'on ait* $\overline{\theta}^0(x^0) = b^0$; *le point* x^0 *est alors un composant simple de* $\mathfrak{a}^0$, *et il existe un composant x de* $\mathfrak{a}$ *(nécessairement unique) appartenant à* $A_\mathfrak{k}$, *tel que* $x^0 = \rho(x)$.

Démonstration. — En effet, $\overline{\theta}^0$ est l'application induite par θ sur $A^0_\mathfrak{k} = \mathscr{S}(A^0)$. Donc, si x^0 est un composant de $\mathfrak{a}^0$, on a $\overline{\theta}^0(x^0) = b^0$. Inversement, soit x^0 un point de $\mathscr{S}(A^0)$, tel que $\overline{\theta}^0(x^0) = b^0$. Puisque m est premier avec la caractéristique de k^0, et d'après une propriété connue des groupes algébriques, le cycle $(\overline{\theta}^0)^{-1}(b^0)$ est de dimension 0, et tous ses composants, parmi lesquels x^0, ont pour coefficient 1.

Soit Γ le graphe de θ, et posons $\Gamma^0 = \rho(\Gamma)$. Soit X^0 la composante de A^0 contenant x^0, et soit ζ^0 l'application induite $\theta | X^0 = \overline{\theta}^0 | X^0$. Soit k^0_1 un corps de définition de X^0 contenant k^0, et soit $\overline{x}^0$ un point générique de X^0 sur k^0_1. Posons $\overline{y}^0 = \zeta^0(\overline{x}^0) = \theta^0(\overline{x}^0)$, et soit Y^0 la composante de A^0 qui contient $\overline{y}^0$ (nécessairement celle qui contient b^0). Le graphe Γ_{ζ^0} est la seule composante de Γ^0 contenant le point $\overline{x}^0 \times \overline{y}^0$. Montrons que cette composante a pour coefficient 1. En effet, le point $\overline{x}^0 \times \overline{y}^0$ est une composante propre, de coefficient 1, de l'intersection $\Gamma_{\zeta^0} \cap (X^0 \times \overline{y}^0)$ dans $X^0 \times Y^0$. Soit $\overline{x}$ un point générique de A sur $\mathfrak{k}$, et posons $\overline{y} = \theta(\overline{x})$. D'après le théorème sur la réduction d'un produit d'intersection ([R], n° 3, th. 11), on a la relation

$$\mu(\Gamma_{\zeta^0}, \Gamma^0)\, i((\overline{x}^0 \times \overline{y}^0), \Gamma_{\zeta^0}.(\overline{x}^0 \times Y^0); (X^0 \times Y^0)) = i((\overline{x} \times \overline{y}), \Gamma.(\overline{x} \times A); (A \times A)),$$

où le symbole i représente la multiplicité d'intersection, au sens de ([F], chap. VI). Le second membre étant égal à 1, chacun des deux facteurs du premier membre est égal à 1. En particulier, on a $\mu(\Gamma_{\zeta^0}, \Gamma^0) = 1$, ce qui prouve notre assertion.

Le point (x^0, b^0) est un composant propre, de multiplicité 1, du cycle $\Gamma_{\zeta^0}.(X^0 \times b^0)$ dans $X^0 \times Y^0$. Appliquant à nouveau ([R], n° 3, th. 11), on voit qu'il existe un et un seul composant (x, b) de $\Gamma.(A \times b) = \mathfrak{a} \times b$, tel que x^0 soit une $\mathfrak{p}$-spécialisation de x. D'après le lemme de Hensel, x est rationnel sur $\mathfrak{k}$.

Théorème 3. — *Soit* A *une variété abélienne définie sur* $\mathfrak{k}$, *faiblement* $\mathfrak{p}$*-simple* $\mathfrak{p}$*-minimale, et soit* B *une sous-variété abélienne de* A, *définie sur* $\mathfrak{k}$. *Supposons qu'il existe une sous-variété* D *de* A, *telle que* $D \cap B$ *soit de dimension* o, *et que le degré m du cycle* D.B *ne soit pas multiple de la caractéristique de* k^0. *Alors* B *est faiblement* $\mathfrak{p}$*-simple* $\mathfrak{p}$*-minimale. On a, de plus* $B^0_{\mathfrak{k}} = \rho_e(B) \cap A^0_{\mathfrak{k}}$. *Si* A *est strictement non dégénérée* (mod. $\mathfrak{p}$) (*without defect for* $\mathfrak{p}$) *il en est de même de* B.

Démonstration. — Nous allons d'abord démontrer la relation $B^0_{\mathfrak{k}} = \rho_e(B) \cap A^0_{\mathfrak{k}}$. L'inclusion $B^0_{\mathfrak{k}} \subset \rho_e(B) \cap A^0_{\mathfrak{k}}$ est évidente. Inversement, soit a^0 un point de $\rho_e(B) \cap A^0_{\mathfrak{k}}$; nous allons montrer qu'il appartient à $B^0_{\mathfrak{k}}$.

D'après ([22], VII, prop. 25), et compte tenu de notre hypothèse concernant D, on peut trouver un k-morphisme $\psi : A \to A$, admettant pour image B, et induisant sur B un $\mathfrak{k}$-morphisme de la forme $\beta = \Theta(b_*, m, B)$, avec $b_* \in B_{\mathfrak{k}}$. Soit $a \in A_{\mathfrak{k}}$, tel que $a^0 = \rho(a)$. Posons $b = \psi(a)$, $b^0 = \rho(b)$, et $b^0_* = \rho(b_*)$. Considérons les cycles $C = \psi^{-1}(b)$ et $\mathfrak{c} = \beta^{-1}(b)$. D'après le lemme 1, on a $\mathfrak{c} = C.B$. D'autre part, $\mathfrak{c}$ est un cycle positif de dimension o sur B, dont tous les composants ont pour multiplicité 1 (d'après [22], IX, n° 65, th. 33, cor. 1).

Montrons que l'ensemble $E^0 = \rho_e(B) \cap \rho_e(C) \cap A^0_{\mathfrak{k}}$ est fini. En effet, soit $c^0 \in E^0$. Puisque A est faiblement $\mathfrak{p}$-simple $\mathfrak{p}$-minimale, et puisque $c^0 \in A^0_{\mathfrak{k}} = \mathscr{S}(A^0)$, ψ est $\mathfrak{p}$-morphique en c^0. Puisqu'on a $c^0 \in \rho_e(C)$, on a $b^0 \in \psi^0_e(c^0)$, d'où $b^0 = \psi^0(c^0)$. D'autre part, posons $\alpha = \Theta(b_*, m, A)$. Les deux k-morphismes α et ψ prennent la même valeur en tout point de B. Or α et ψ sont $\mathfrak{p}$-morphiques en c^0; puisque $c^0 \in \rho_e(B)$, on a $\alpha^0(c^0) = \psi^0(c^0)$. Si on pose $\overline{\alpha}^0 = \Theta(b^0_*, m, \mathscr{S}(A^0))$, on a aussi $\alpha^0(c^0) = \overline{\alpha}^0(c^0)$. On en déduit $b^0 = \overline{\alpha}^0(c^0)$. On a donc $E^0 \subset (\overline{\alpha}^0)^{-1}(b^0)$. Ce dernier ensemble étant fini, comme on l'a déjà remarqué dans le lemme 2, il en est de même de E^0.

Le point A est donc un composant, et par suite, un composant propre (de la bonne dimension) de $\rho_e(B) \cap \rho_e(C)$ sur la composante X^0 de A^0 contenant a^0. Donc, si on pose $\mathfrak{c}^0 = \rho(\mathfrak{c})$, on a, d'après le théorème déjà cité de [R], relatif à la réduction d'un produit d'intersection :

$$\mu(a^0, \mathfrak{c}^0) = \Sigma_{i,j} \mu(B^0_i, B^0) \mu(C^0_j, C^0) i(a^0, B^0_i, C^0_j; X^0) \tag{6}$$

où la somme est étendue à toutes les composantes B^0_i (resp. C^0_j) de $\rho_e(B)$ (resp. $\rho_e(C)$) contenant a^0. Comme, d'autre part, on a $\mathfrak{c} \prec \mathfrak{a}$, o na aussi $\mathfrak{c}^0 \prec \mathfrak{a}^0 = \rho(\mathfrak{a})$. Comme on a $\mu(a^0, \mathfrak{a}^0) = 1$, d'après le lemme 2, on a aussi $\mu(a^0, \mathfrak{c}^0) = 1$.

D'après la relation (6), ceci entraîne, en particulier, qu'il passe par A^0 une et une seule composante de $\rho_e(B)$, et que a^0 est simple sur cette composante. Autrement dit, a^0 est simple sur B^0. Donc, d'après le lemme de Hensel, il appartient à $\rho(B_{\mathfrak{k}}) = B^0_{\mathfrak{k}}$, comme on l'a annoncé.

Il en résulte, en même temps, que tout point de $\rho(B_{\mathfrak{k}})$ est simple sur B^0, c'est-à-dire que B est faiblement $\mathfrak{p}$-simple. De plus puisque A vérifie (ii) de la proposition 7 du n° 7, il en est de même de B. Donc B est $\mathfrak{p}$-minimale.

Enfin, supposons que A soit strictement non dégénérée (mod. $\mathfrak{p}$). Alors (n° 4, cor. 2 du th. 1), $\rho(A_{\mathfrak{k}}) = A^0_{\mathfrak{k}} = A^0$ est une variété abélienne définie sur k^0; donc on a

$\rho_e(B) = B_{\mathfrak{k}}^0$. De plus, $\rho_e(B)$ est connexe, et $B_{\mathfrak{k}}^0$ est un sous-groupe de $A_{\mathfrak{k}}^0$. Donc $\rho_e(B)$ est une sous-variété abélienne B_*^0 de A^0. Le cycle $B^0 = \rho(B)$ est donc un multiple de B_*^0. Puisque tout point de B_*^0 est simple sur B^0, on a nécessairement $B^0 = B_*^0$.

C.Q.F.D.

Le résultat du cas strictement non dégénéré (mod. $\mathfrak{p}$) (dernière assertion du théorème) est dû à Koizumi et Shimura ([9], § 6, remarque, p. 204).

Corollaire. — *Soient* A *et* B *deux variétés abéliennes, définies sur k, et soit* $\varphi : B \to A$ *un k-morphisme. Soient* (A_*, α) *et* (B_*, β) *des k-modèles faiblement* $\mathfrak{p}$*-simples* $\mathfrak{p}$*-minimaux de* A *et* B *respectivement. Alors si* k^0 *est de caractéristique nulle, et si* φ *est* injectif, *les* k^0*-morphismes canoniques* $\varphi_*^\mu = (B_*)_{\mathfrak{k}}^\mu \to (A_*)_{\mathfrak{k}}^\mu$ *sont* injectifs.

En effet, l'application $\varphi_* = \alpha \circ \varphi \circ \beta^{-1} : B_* \to A_*$ est injective. D'après le théorème précédent, son image est une variété abélienne faiblement $\mathfrak{p}$-simple $\mathfrak{p}$-minimale B'_*. Donc l'application réduite $B_* \to B'_*$ est un R-isomorphisme, et le résultat s'en déduit aussitôt.

Un exemple, donné par Koizumi et Shimura (*loc. cit.*, p. 205), relatif au cas strictement non dégénéré (mod. $\mathfrak{p}$), montre que ce corollaire n'est pas valable si k^0 est de caractéristique non nulle.

Remarque. — Il est indifférent de prendre pour A et B, dans l'énoncé du théorème 3, des variétés abéliennes ou des espaces homogènes principaux abéliens. En effet, dans le cas des espaces homogènes principaux, on peut supposer $B_{\mathfrak{k}}^0$ non vide (sinon l'énoncé est trivial) et se ramener au cas des variétés abéliennes en prenant un point de $B_{\mathfrak{k}}^0$ comme origine.

10. Cas d'un corps global.

Théorème 4. — *Soit* K *un corps global, et soit* A *un espace homogène principal abélien, défini sur* K. *Alors il existe un* K*-modèle* (A_*, α) *de* A *qui est faiblement* $\mathfrak{p}$*-simple* $\mathfrak{p}$*-minimal pour tout* $\mathfrak{p} \in \mathfrak{S} = \mathfrak{S}(K)$.

Démonstration. — En confrontant le théorème 2*, et la proposition 25 du n° 26 du chapitre Ier, on voit qu'il existe, pour tout $\mathfrak{p} \in \mathfrak{S}$, et pour tout espace homogène principal abélien B défini sur K, un K-modèle (B_*, β) de B tel que B_* soit faiblement $\mathfrak{p}$-simple $\mathfrak{p}$-minimal et que, pour tout $\mathfrak{q} \in \mathfrak{S}$ distinct de $\mathfrak{p}$, l'application β soit un $R_{\mathfrak{q}}$-isomorphisme.

D'autre part, on sait qu'il existe un sous-ensemble fini $\mathfrak{S}_0$ de $\mathfrak{S}$ tel que, pour tout $\mathfrak{p} \in \mathfrak{S} - \mathfrak{S}_0$, A soit strictement non dégénéré (mod. $\mathfrak{p}$) ; pour un tel $\mathfrak{p}$, $\rho_{\mathfrak{p}}(A) = A_{\mathfrak{p}}^0$ est une variété sans point multiple (et, par conséquent, un espace homogène principal abélien, d'après le cor. 2 du th. 1), donc A est faiblement $\mathfrak{p}$-simple $\mathfrak{p}$-minimal.

Soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ les éléments de $\mathfrak{S}_0$. On peut, d'après ce qui précède, construire, par récurrence sur i $(1 \leqslant i \leqslant m)$ une suite de K-modèles (A_i, φ_i) de A tels que, pour tout i, A_i soit $R_{\mathfrak{q}}$-isomorphe à A_{i-1} si $\mathfrak{q} \neq \mathfrak{p}_i$, et soit faiblement $\mathfrak{p}_i$-simple $\mathfrak{p}_i$-minimal. Le dernier modèle $(B, \varphi) = (A_m, \varphi_m)$ de la suite est alors faiblement $\mathfrak{p}$-simple $\mathfrak{p}$-minimal pour tout $\mathfrak{p} \in \mathfrak{S}$.

CHAPITRE III

MODÈLES p-SIMPLES p-MINIMAUX DES COURBES ELLIPTIQUES

1. Énoncé des résultats essentiels.

Soit V une p-variété p-simple, c'est-à-dire (chap. I[er], n° 10) telle que tous les points de l'ensemble réduit $\rho_e(V)$ soient p-simples sur V. Nous dirons que V est p-*simple* p-*minimale* si, pour toute p-variété W, et pour tout $\mathfrak{k}$-isomorphisme $\varphi : W \to V$, φ est p-morphique en tout point de $\rho_e(W)$ qui est p-simple sur W.

Si (V_*, θ) et $(\overline{V}_*, \overline{\theta})$ sont deux k-modèles p-simples p-minimaux d'une même p-variété V, l'application $\overline{\theta} \circ \theta^{-1} : V_* \to \overline{V}_*$ est nécessairement un $\mathfrak{R}$-isomorphisme. Autrement dit, si V possède un $\mathfrak{k}$-modèle p-simple p-minimal, le schéma $\mathbf{S}(V_*) = \mathbf{S}_{\mathfrak{R}}(V_*)$ sur l'anneau $\mathfrak{R}$ est uniquement déterminé, à un $\mathfrak{R}$-isomorphisme près, par la donnée de V. Plus précisément, il est uniquement déterminé par la donnée de V à un $\mathfrak{k}$-isomorphisme près, i.e. par la donnée du schéma $\mathbf{S}_{\mathfrak{k}}(V) = \mathbf{S}(V) \otimes_{\mathfrak{R}} \mathfrak{k}$ sur $\mathfrak{k}$ associé à V. Si, de plus, V est définie *sur* k, et si (V_*, θ) est un k-modèle de V, le schéma $\mathbf{S}_R(V_*)$ *sur* R est, de même, déterminé, à un R-isomorphisme près, par la donnée du schéma $\mathbf{S}_k(V)$.

Il est clair que toute p-variété, définie sur k, qui est p-simple et p-minimale, est aussi faiblement p-simple p-minimale.

L'exemple de l'espace affine $\mathbf{S}_n$, et celui de l'espace projectif $\mathbf{P}_n$ (chap. II, n° 7, prop. 6) montrent qu'il existe des variétés définies sur k, et n'admettant pas de modèle p-simple p-minimal. L'objet essentiel de ce chapitre est de démontrer le théorème suivant :

Théorème 1. — *Soit* A *une courbe elliptique, définie sur k, et possédant un point rationnel sur k (ou, ce qui est équivalent, une variété abélienne de dimension 1, définie sur k). Alors il existe un k-modèle* (A_*, θ) p-*simple* p-*minimal de* A.

Comme on sait que toute application birationnelle $A \to A'$, définie sur k, est un k-isomorphisme, il en résultera que le schéma $\mathbf{S}_R(A_*)$ sur R associé à A est déterminé, à un R-isomorphisme près, par la seule donnée du corps $k(A)$ des fonctions sur A, définies sur k. Il y a également unicité du schéma sur le corps résiduel k^0 déduit du précédent par réduction (mod. p); ceci entraîne, en particulier, que le nombre des composantes du cycle $A_*^0 = \rho(A_*)$, leurs coefficients respectifs dans ce cycle, et leurs multiplicités d'intersection deux à deux sont déterminés par la donnée du corps $k(A)$.

On démontrera d'autre part le théorème suivant, relatif au cas d'un *corps global.*

Théorème 2. — Soit K *un corps global et soit* A *une courbe elliptique, définie sur* K, *et possédant un point rationnel sur* K. *Alors il existe un* K*-modèle* (A_*, θ) *de* A *qui est* $\mathfrak{p}$*-simple* $\mathfrak{p}$*-minimal pour tout* $\mathfrak{p} \in \mathfrak{S}(K)$.

Il en résultera que, si K est un corps de nombres (resp. un corps de fonctions d'une variable sur un corps parfait K_0), le schéma sur l'anneau $\mathscr{R}$ des entiers de K (resp. le schéma sur K_0) associé à A_* est déterminé par la connaissance du corps de fonctions K(A).

On peut, dans le second cas, celui où K est un corps de fonctions d'une variable sur K_0, et en supposant K_0 algébriquement clos, donner une interprétation « géométrique » simple de ce résultat.

Supposons A projective, plongée dans $\mathbf{P}_n$, et introduisons la surface $\widetilde{A}$, déjà considérée dans le cas particulier étudié au n° 10 du chapitre Ier.

Rappelons qu'on peut écrire K sous la forme $K_0(u)$, où u est un point générique sur K_0 d'une courbe U non singulière, définie sur K_0, et que si x est un point générique de A sur $K = K_0(u)$, on a pris pour $\widetilde{A}$ la surface lieu du point (x, u) sur K_0, dans le produit $\mathbf{P}_n \times U$. Cette surface $\widetilde{A}$ peut être regardée comme « fibrée » par une famille de courbes paramétrée par U, la fibre générique étant $A \times u$, et celle associée au point $u_\mathfrak{p} = \rho_\mathfrak{p}(u)$ étant $A_\mathfrak{p} \times u_\mathfrak{p}$, avec $A_\mathfrak{p} = \rho_\mathfrak{p}(A)$.

Notons $\widetilde{A}_*$ la surface analogue, construite à partir de A_*, et considérons l'application rationnelle $\widetilde{\theta} : \widetilde{A} \to \widetilde{A}_*$, définie sur K_0, telle qu'on ait $\widetilde{\theta}(x, u) = (\theta(x), u)$. Alors la condition pour A_* d'être $\mathfrak{p}$-simple pour tout $\mathfrak{p}$ équivaut, d'après ce qu'on a vu au n° 10 du chapitre Ier, à celle pour la surface $\widetilde{A}_*$ d'être *sans point multiple*; la condition de $\mathfrak{p}$-minimalité pour tout $\mathfrak{p}$ entraîne que, pour tout modèle analogue (A'_*, θ') de A vérifiant la condition précédente ($\widetilde{A}'_*$ sans point multiple), l'application $\widetilde{\theta} \circ (\widetilde{\theta}')^{-1} : \widetilde{A}'_* \to \widetilde{A}$ est un morphisme.

Cette propriété est analogue à celle caractérisant les modèles minimaux non singuliers des surfaces, au sens 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 compatibles avec la fibration. On peut montrer, par des exemples simples, que $\widetilde{A}_*$ n'est pas toujours un modèle minimal de $\widetilde{A}$ au sens classique; il peut arriver, en particulier, que $\widetilde{A}$ soit une surface rationnelle (birationnellement équivalente au plan), auquel cas il n'existe pas de modèle minimal de $\widetilde{A}$ au sens classique.

2. Critère de $\mathfrak{p}$-minimalité.

Proposition 1. — Soit V *une courbe projective, sans point multiple, définie sur* k, $\mathfrak{p}$*-simple. Supposons qu'il existe une* k*-différentielle* ω *sur* V, *dépourvue de pôles, et telle qu'on ait* $(\omega)_\mathfrak{p} = 0$, (i.e. $\nu(C^0, \omega) = 0$ *pour toute composante* C^0 *de* $V^0 = \rho(V)$). *Alors* V *est* $\mathfrak{p}$*-simple* $\mathfrak{p}$*-minimale.*

La méthode que nous emploierons pour démontrer le théorème 1 consistera à construire, pour toute courbe elliptique A définie sur k, un k-modèle $\mathfrak{p}$-simple de A auquel ce critère soit applicable, ω étant la différentielle invariante sur A, convenablement

normée. On obtiendra donc, dans le cas particulier des courbes elliptiques, la réciproque suivante de la proposition 1 :

Proposition 1'. — Si A *est une courbe elliptique* p*-simple* p*-minimale, définie sur k, on peut normer la différentielle invariante* ω *sur* A *de manière qu'elle soit définie sur k, et qu'on ait* $(\omega)_p = 0$.

Démonstration de la proposition 1. — Soit $\varphi : W \to V$ un k-isomorphisme. Soit k_1^0 un corps de définition de toutes les composantes de $W^0 = \rho(W)$ et de $V^0 = \rho(V)$. Commençons par considérer une composante D^0 de W^0, génériquement p-simple sur W, et un point $\overline{y}^0$ générique de D^0 sur k_1^0. Ce point $\overline{y}^0$ est p-simple sur W, et φ est p-morphique en $\overline{y}^0$, d'après la proposition 8 du n° 11 du chapitre I^er. Posons $\overline{x}^0 = \varphi^0(\overline{y}^0)$. D'après l'hypothèse, ω est p-morphique en $\overline{x}^0$. Donc, d'après la proposition 11 du n° 15 du chapitre I^er, la différentielle ω^* sur W transposée de ω par φ est p-morphique en $\overline{y}^0$. Donc, on a $\overline{y}^0 \notin \{\omega^*\}_{p,\infty}$. Donc D^0 n'est pas une composante du p-diviseur $(\omega^*)_{p,\infty}$ des pôles de ω^*.

Soit maintenant y^0 un point quelconque de $\rho_e(W)$, p-simple sur W. Toutes les composantes de W^0 contenant y^0 sont alors génériquement p-simples sur W, donc, d'après ce qui précède, ne sont pas des composantes de $(\omega^*)_{p,\infty}$; donc, on a $y^0 \notin \{\omega^*\}_{p,\infty}$. Donc, d'après la proposition 14 du n° 16 du chapitre I^er, ω^* est p-morphique en y^0.

Supposons que φ ne soit pas p-morphique en y^0. Alors, l'ensemble $\varphi_e^0(y^0)$, qui est connexe, et non réduit à un point (chap. I^er, prop. 7), contient au moins une composante C^0 de V^0. Soit x^0 un point générique de C^0 sur k_1^0. D'après la proposition 8 du n° 11 du chapitre I^er, l'application $\varphi^{-1} : V \to W$ est p-morphique en x^0, de valeur y^0. D'autre part, ω est p-morphique et non nulle en x^0, d'après l'hypothèse. Donc, d'après la proposition 11 du n° 15 du chapitre I^er, ω^* ne s'annule pas en y^0. Donc, d'après la proposition 12 du n° 15 du chapitre I^er, φ^{-1} est p-isomorphique en x^0, de valeur y^0, ce qui contredit notre hypothèse.

3. Courbes elliptiques planes.

Considérons, dans le plan projectif $\mathbf{P}_2$, une courbe elliptique B sans point multiple, donc de degré 3, définie sur un corps $\mathbf{k}$ (n'admettant pas nécessairement de point rationnel sur $\mathbf{k}$). Pour tout couple (x, y) de points de B, il existe un et un seul point z de B tel que le cycle $(x) + (y) + (z)$ soit le produit d'intersection de B avec une droite; on a $z = \beta_B(x, y)$, où $\beta_B : B \times B \to B$ est un morphisme défini sur $\mathbf{k}$, déterminé par B. La courbe B admet, comme on sait, une structure d'espace homogène principal abélien, défini sur $\mathbf{k}$, la loi γ_B étant définie par la formule $\gamma_B(x, y, z) = \beta_B(\beta_B(x, y), z)$.

Supposons, en particulier $\mathbf{k} = k$, et posons $B^0 = \rho(B)$. On a alors le lemme suivant :

Lemme 1. — Soient x^0, y^0, z^0 *trois points de* $\rho_e(B)$. *Supposons que* x^0 *et* y^0 *sont simples sur* $B^0 = \rho(B)$, *et que le cycle* $(x^0) + (y^0) + (z^0)$ *est le produit d'intersection de* B^0 *avec une droite* D^0, *dans le plan* $\mathbf{P}_2^0$. *Alors* β_B *est* p*-morphique en* (x^0, y^0), *de valeur* z^0, *et* z^0 *est simple sur* B^0.

En effet, z^0 est simple sur B^0, car, sinon, on aurait $z^0 \neq x^0$, et $z^0 \neq y^0$; comme z^0 figurerait avec un coefficient $\geqslant 2$ dans $D^0 . B^0$, le degré de ce cycle serait $\geqslant 4$, ce qui est absurde.

Puisque le point (x^0, y^0) est simple sur $B^0 \times B^0$, il nous suffit de montrer que z^0 est la seule valeur de β_B en (x^0, y^0). Soit, en effet, z'^0 une autre valeur de β_B en (x^0, y^0). Soient x et y deux points génériques indépendants de B sur $\mathfrak{k}$. Posons $z = \gamma_B(x, y)$, et soit D la droite telle que $B.D = (x) + (y) + (z)$. Alors (x^0, y^0, z'^0) est une $\mathfrak{p}$-spécialisation de (x, y, z) sur k^0. On peut l'étendre à une $\mathfrak{p}$-spécialisation $D \to D'^0$, où D'^0 est une droite de $\mathbf{P}_2^0$. Cette droite ne peut être une composante de B^0. En effet, dans ce cas, elle serait distincte de D^0, et x^0 serait un composant simple de $D^0.B^0$; on aurait donc $y^0 \neq x^0$; donc les deux droites D^0 et D'^0, qui contiennent x^0 et y^0, coïncideraient, ce qui est contradictoire. Donc le produit d'intersection $B^0.D'^0$ est défini, et d'après les propriétés de la réduction d'une intersection de cycles, on a $B^0.D'^0 = (x^0) + (y^0) + (z'^0)$. Ceci entraîne $D'^0 = D^0$ (car D^0 et D'^0 coïncident avec la droite qui joint les points x^0 et y^0 si ceux-ci sont distincts, ou bien avec la tangente en x^0 à B^0 s'ils sont confondus), d'où $z'^0 = z^0$.

Corollaire. — *Supposons* B^0 *irréductible (dans ce cas* B^0 *est une courbe admettant au plus un point double). Alors* γ_B *est* $\mathfrak{p}$*-morphique en tout triplet* (x^0, y^0, z^0) *composé de points simples sur* B^0, *et le point* $w^0 = \gamma_B^0(x^0, y^0, z^0)$ *est également simple sur* B^0. *La loi* γ_B^0 *définit sur l'ensemble* $\mathcal{S}(B^0)$ *des points simples sur* B^0 *une structure d'espace homogène principal algébrique, défini sur* k^0.

Il suffit en effet d'appliquer le lemme, en remarquant que le cycle $D^0.B^0$ est défini pour toute droite D^0 de $\mathbf{P}_2^0$.

Proposition 2. — *Soit* B *une courbe elliptique plane, définie sur k, et soit* ω *la k-différentielle sur* B, *invariante par translation. Alors, on peut normer* ω *de manière que son* $\mathfrak{p}$*-diviseur soit nul (i.e. de manière que* ω *soit* $\mathfrak{p}$*-morphique et non nulle en tout point de* $\rho_e(B)$ $\mathfrak{p}$*-simple sur* B).

Démonstration. — Soit en effet $F(X, Y, Z) = 0$ l'équation de B, où F est un polynôme homogène de degré 3 de l'anneau $R[X, Y, Z]$, irréductible dans cet anneau. On peut alors prendre pour ω la différentielle induite sur B par l'une quelconque des trois différentielles de degré 1

$$\omega_X = (Y dZ - Z dY)/(\partial F/\partial X),\ \omega_Y = (Z dX - X dZ)/(\partial F/\partial Y),\ \text{et}\ \omega_Z = (X dY - Y dX)/(\partial F/\partial Z)$$

sur le plan projectif $\mathbf{P}_2$ (en effet, on voit sans peine que ω_X, ω_Y et ω_Z induisent la même différentielle sur B, et que celle-ci est dépourvue de pôles et de zéros, donc coïncide avec la différentielle invariante sur B). Soit $u^0 = (x^0, y^0, z^0)$ un point de $\rho_e(B)$, simple sur B^0, et supposons $z^0 \neq 0$. Alors, si on note f la fonction F/Z^3 sur $\mathbf{P}_2$, on trouve que la différentielle $\theta = df \wedge \omega_Z$ sur $\mathbf{P}_2$ est $\mathfrak{p}$-morphique et non nulle en u^0 et, plus précisément, qu'on a $\theta^0_{u^0} = (d(X/Z) \wedge d(Y/Z))^0_{u^0}$. D'après les définitions du n° 13 du chapitre I[er], ω est bien $\mathfrak{p}$-morphique et non nulle en u^0.

Corollaire. — *Toute courbe elliptique plane* $\mathfrak{p}$*-simple est* $\mathfrak{p}$*-minimale.*

4. Choix d'un k-modèle de A.

On sait que toute courbe elliptique, définie sur un corps $\mathbf{k}$, et possédant un point rationnel sur $\mathbf{k}$, est $\mathbf{k}$-isomorphe à une courbe projective plane A de degré 3, ayant une équation de la forme :

$$Y^2Z + \lambda XYZ + \mu YZ^2 = X^3 + \alpha X^2Z + \beta XZ^2 + \gamma Z^3, \tag{1}$$

où les coefficients λ, μ, α, β, γ appartiennent à $\mathbf{k}$; si la caractéristique de $\mathbf{k}$ est différente de 2, on peut trouver un tel modèle pour lequel, de plus, on a $\lambda = \mu = 0$; si la caractéristique de $\mathbf{k}$ est différente de 2 et 3, on peut trouver un tel modèle pour lequel $\lambda = \mu = \alpha = 0$, c'est-à-dire un *modèle de Weierstrass* de A. La courbe définie par (1) passe, dans tous les cas, par le point $b = (0, 1, 0)$; plus précisément, b est un point d'inflexion de A, admettant pour tangente la droite $Z = 0$.

En particulier, on peut supposer, dans le théorème 1, que la courbe donnée A est une courbe plane projective définie par une équation de la forme (1); on peut supposer de plus que les coefficients λ, μ, α, β, γ, sont entiers (appartiennent à R).

Le cycle A^0 réduit (mod. $\mathfrak{p}$) de A a alors pour équation

$$Y^2Z + \lambda^0XYZ + \mu^0YZ^2 = X^3 + \alpha^0X^2Z + \beta^0XZ^2 + \gamma^0Z^3 \tag{2}$$

où λ^0, μ^0, α^0, β^0, γ^0 sont les éléments de k^0 réduits (mod. $\mathfrak{p}$) de λ, μ, α, β, γ respectivement. Ce cycle est toujours irréductible, i.e. admet une composante unique et simple; celle-ci est une courbe de degré 3, admettant au plus un point double. On le voit, par exemple, en remarquant que le point $b^0 = (0, 1, 0)$ de $\mathbf{P}_2^0$ est simple sur A^0, et que A^0 admet, en ce point, la droite $Z = 0$ comme tangente d'inflexion.

5. Le groupe algébrique $\mathscr{S}(A^0)$.

Convenons d'identifier l'ouvert $Z \neq 0$ de $\mathbf{P}_2$ (resp. $\mathbf{P}_2^0$) à l'espace affine $\mathbf{S}_2$ (resp. $\mathbf{S}_2^0$) par l'isomorphisme qui, au point (x, y, z), fait correspondre $(x/z, y/z)$. Pour tout triplet q, r, s, d'éléments de $\mathfrak{R}$, nous noterons $\psi_{q,r,s}$ le $\mathfrak{R}$-automorphisme de $\mathbf{P}_2$ qui, au point (x, y, z), fait correspondre $(x + qz, y + sx + rz, z)$. Le plus souvent, q, r et s seront des éléments de R; l'ensemble des $\psi_{q,r,s}$ pour lesquels q, r et s appartiennent à R est un sous-groupe du groupe $\mathrm{Aut}_R\mathbf{P}_2$ des R-automorphismes de $\mathbf{P}_2$; nous le désignerons par H. Si $\psi \in H$, toute équation de la forme (1), à coefficients dans R, est transformée par ψ en une équation de la même forme, également à coefficients dans R. Le sous-ensemble de H composé des éléments de la forme $\varphi_{q,r} = \psi_{q,r,0}$ est un sous-groupe de H, que nous noterons H_0. Les éléments de H_0 sont aussi les éléments de $\mathrm{Aut}_R\mathbf{P}_2$ qui induisent sur $\mathbf{S}_2$ les translations à coordonnées dans R. Nous appellerons *groupe additif* (resp. *groupe multiplicatif*) sur k^0 le groupe algébrique, défini sur k^0, admettant comme variété sous-jacente la droite affine (resp. la droite affine privée de l'origine), la loi étant l'addition (resp. la multiplication). Ce groupe sera noté $\mathbf{G}_a$ (resp. $\mathbf{G}_m$).

Revenons à la courbe elliptique A définie par l'équation (1), à coefficients dans R. Cette courbe admet une et une seule structure de variété abélienne admettant pour origine le point $b = (0, 1, 0)$, la loi de groupe étant définie par $\alpha_A(x, y) = \gamma_A(x, b, y)$. Il résulte du corollaire du lemme 1 que α_A est $\mathfrak{p}$-morphique en tout couple (x^0, y^0) de points de $\mathscr{S}(A^0)$, et que α_A^0 définit sur $\mathscr{S}(A^0)$ une structure de *groupe algébrique*.

Nous allons déterminer la structure de ce groupe $\mathscr{S}(A^0)$, en distinguant les trois cas suivants :

a) A^0 est sans point multiple.

b) A^0 a un point double à tangentes distinctes.

c) A^0 a un point de rebroussement.

Dans les deux cas *b)* et *c)*, le point double de A^0 est rationnel sur k^0, puisque k^0 est parfait. On peut, en transformant A par un élément $\varphi_{q,r}$ du groupe H_0, se ramener au cas où ce point double est le point $c^0=(0, 0, 1)$ de $\mathbf{P}_2^0$; on a alors $\mu^0=\beta^0=\gamma^0$. De plus, dans le cas *c)*, la tangente à A^0 en b^0 est également rationnelle sur k^0. On peut, en transformant A par un élément ψ_{qrs} de H, se ramener au cas où cette tangente est la droite $Y=0$; on a alors $\lambda^0=\mu^0=\alpha^0=\beta^0=\gamma^0=0$. On a, dans ces conditions, la proposition suivante :

Proposition 3. — Le groupe $\mathscr{S}(A^0)$ *est* k^0*-isomorphe* : dans le cas *a)*, *à la* variété abélienne *admettant pour variété sous-jacente* A^0, *et pour origine* $b^0=\rho(b)$; dans le cas *b)*, *au groupe algébrique* $\mathbf{H}_Q$ *des* k^0*-automorphismes de la droite projective* $\mathbf{P}_1^0$ *qui laissent invariants chacun des deux points en lesquels s'annule la forme quadratique* $Q(X, Y)=Y^2+\lambda^0XY-\alpha^0X^2$ *(ceci implique, en particulier, que* $\mathscr{S}(A^0)$ *est isomorphe au* groupe multiplicatif $\mathbf{G}_m$ *sur l'extension (quadratique au plus)* k'^0 *de* k^0 *engendrée par les racines* ν^0 *et* $\bar{\nu}^0$ *de l'équation* $U^2+\lambda^0U-\alpha^0=0$) ; dans le cas *c)*, *au* groupe additif $\mathbf{G}_a$.

Démonstration. — Le résultat du cas *a)* se déduit immédiatement du corollaire du lemme 1 du n° 2.

Dans les cas *b)* et *c)*, notons ψ l'application $\mathscr{S}(A^0)\to\mathbf{P}_1^0$ qui, à tout point (x, y, z) de $\mathscr{S}(A^0)$, fait correspondre le point (x, y). Dans les deux cas, ψ est un k^0-isomorphisme de $\mathscr{S}(A^0)$ sur un ouvert U^0 de $\mathbf{P}_1^0$.

Dans le cas *b)*, U^0 est le complémentaire du couple de points défini par l'équation $Q(X, Y)=0$. Un calcul élémentaire permet de vérifier que l'image par ψ du groupe des translations sur $\mathscr{S}(A^0)$ est bien le groupe $\mathbf{H}_Q$ défini dans l'énoncé. L'assertion relative à ce cas s'en déduit aussitôt.

Dans le cas *c)*, U^0 est le complémentaire du point $(1, 0)$, donc est isomorphe (pour la structure de groupe algébrique transportée de celle de $\mathscr{S}(A^0)$) au groupe additif $\mathbf{G}_a$.

6. L'invariant de A.

Rappelons qu'on appelle *invariant* d'une courbe elliptique A, définie sur k, un certain élément $j(A)$ du corps k qui ne dépend que de la classe de A modulo les transformations birationnelles; rappelons que cet invariant a pour valeur, dans le cas d'une courbe de Weierstrass $(\lambda=\mu=\alpha=0)$,

$$j(A)=2^6 3^3\frac{4\beta^3}{4\beta^3+27\gamma^2} \tag{3}$$

et, plus généralement, dans le cas d'une courbe définie par une équation quelconque de la forme (1)

$$j(A)=\frac{(24\bar{\beta}-\bar{\alpha}^2)^3}{8\bar{\beta}^3+27\bar{\gamma}^2-9\bar{\alpha}\bar{\beta}\bar{\gamma}+\bar{\alpha}^2\bar{\delta}} \tag{4}$$

où l'on pose :

$$\overline{\alpha} = 4\alpha + \lambda^2$$
$$\overline{\beta} = 2\beta + \lambda\mu$$
$$\overline{\gamma} = 4\gamma + \mu^2$$
$$\overline{\delta} = -\beta^2 + 4\alpha\gamma + \mu^2\alpha - \lambda\mu\beta - \lambda^2\gamma$$

(si la caractéristique de k est $\neq 2$, on a $\overline{\delta} = \frac{1}{4}(\overline{\beta}^2 - \overline{\alpha\gamma})$).

En particulier, si k est de caractéristique 2, on a

$$j(A) = \frac{\lambda^{12}}{\mu^4 + \lambda^3\mu^3 + \lambda^4\beta^2 + \lambda^4\mu^2\alpha + \lambda^5\mu\beta + \lambda^6\gamma}. \tag{5}$$

Si k est de caractéristique 3, on a

$$j(A) = \frac{(\alpha + \lambda^2)^6}{(-\beta + \lambda\mu)^3 + (\alpha + \lambda^2)^2(\beta^2 - \alpha\gamma - \mu^2\alpha + \lambda\mu\beta + \lambda^2\gamma)}. \tag{6}$$

7. Subdivision du problème. Modèles p-standard.

Lemme 2. — Soit A *une courbe elliptique plane, définie par une équation de la forme* (1), *à coefficients dans* R. *Alors, il existe un entier* m_0, *qui ne dépend que de* A, *tel que, pour tout* R*-automorphisme* $\psi \in H$ *de* $\mathbf{P}_2$, *les coefficients de l'équation* $Y^2Z + \lambda'XYZ + \mu'YZ^2 = X^3 + \alpha'X^2Z + \beta'XZ^2 + \gamma'Z^3$ *de la courbe* $A' = \psi(A)$ *vérifient l'inégalité*

$$\inf(v(\mu'), v(\beta'), v(\gamma')) \leqslant m_0. \tag{7}$$

Démonstration. — Notons F(X, Y) le polynôme

$$F(X, Y) = -Y^2 - \lambda XY - \mu Y + X^3 + \alpha X^2 + \beta X + \gamma.$$

Si $\psi = \psi_{qrs}$, on a les relations $\mu' = (\partial F/\partial Y)(-q, -r')$, $\beta' - s\mu' = (\partial F/\partial X)(-q, -r')$ et $\gamma' = F(-q, -r')$, en posant $r' = r - qs$.

Or les polynômes F, $\partial F/\partial X$ et $\partial F/\partial Y$ n'admettent aucun zéro commun, puisque A est sans point multiple. D'après le lemme 2 du n° 17 du chapitre I^er^, il existe un entier m_0, indépendant de q, r et s, tel qu'on ait

$$\inf(v(\mu'), v(\beta' - s\mu'), v(\gamma')) \leqslant m_0$$

d'où résulte l'inégalité (7).

Désignons par δ le k-automorphisme du plan projectif $\mathbf{P}_2$ qui, au point (x, y, z), fait correspondre le point (t^2x, t^3y, z). Observons que la transformée $A_h = \delta^h(A)$ de A par une puissance arbitraire δ^h de δ a encore une équation de la forme (1), dont les coefficients appartiennent à k pour tout h, et à R pour $h \geqslant 0$.

Proposition 4. — Pour toute courbe elliptique plane A, *définie par* (1), *il existe un entier* $h \geqslant 0$, *et un* R*-automorphisme* $\psi \in H$ *de* $\mathbf{P}_2$ *tels que les propriétés suivantes soient satisfaites :*

(i) *Les coefficients de l'équation* $Y^2Z + \lambda'XYZ + \mu'YZ^2 = X^3 + \alpha'X^2Z + \beta'XZ^2 + \gamma'Z^3$ *de la courbe* A' *transformée de* A *par le k-automorphisme* $\delta^{-h}\psi$ *sont entiers.*

(ii) *La courbe* A′ *vérifie les conditions de l'un des cas* a) *ou* b), *ou sinon* (*c'est-à-dire si* A′ *vérifie les conditions du cas* c)) *les coefficients* λ', μ', α', β', γ' *appartiennent à* $\mathfrak{p}$ (*i.e. sont de valuation* $\geqslant 1$), *et vérifient l'une des huit conditions suivantes* :

(c 1)	$v(\gamma')=1$				
(c 2)	$v(\beta')=1$	$v(\gamma')\geqslant 2$			
(c 3)	$v(\beta')\geqslant 2$	$v(\gamma')\geqslant 2$	$v(\overline{\gamma}')=2$		
(c 4)	$v(\mu')\geqslant 2$	$v(\beta')\geqslant 2$	$v(\gamma')\geqslant 3$	$v(\Delta')=6$	
(c 5)	$v(\mu')\geqslant 2$	$v(\alpha')=1$	$v(\beta')\geqslant 3$	$v(\gamma')\geqslant 4$	
(c 6)	$v(\mu')\geqslant 2$	$v(\alpha')\geqslant 2$	$v(\beta')\geqslant 3$	$v(\gamma')\geqslant 4$	$v(\overline{\gamma}')=4$
(c 7)	$v(\mu')\geqslant 3$	$v(\alpha')\geqslant 2$	$v(\beta')=3$	$v(\gamma')\geqslant 5$	
(c 8)	$v(\mu')\geqslant 3$	$v(\alpha')\geqslant 2$	$v(\beta')\geqslant 4$	$v(\gamma')=5$	

où l'on pose $\overline{\gamma}'=\mu'^2+4\gamma'$

et
$$\Delta'=4\beta'^3+27\gamma'^2+4\alpha'^3\gamma'-18\alpha'\beta'\gamma'-\alpha'^2\beta'^2$$

($\overline{\gamma}'$ *et* Δ' *sont les discriminants respectifs des polynômes* $Y^2+\mu'Y-\gamma'$ *et* $X^3+\alpha'X^2+\beta'X+\gamma'$).

Remarque. — Il résultera de la propriété d'unicité du modèle $\mathfrak{p}$-simple $\mathfrak{p}$-minimal de A que les cas a), b), (c 1), ..., (c 8) s'excluent mutuellement; en d'autres termes, pour A donnée, quels que soient h et ψ, la courbe A′ ne peut vérifier les conditions que d'un seul de ces dix cas. Au n° 8, nous donnerons, dans l'hypothèse où la caractéristique de k^0 est différente de 2 et 3, une démonstration directe de cette propriété d'exclusion mutuelle, résultant d'une caractérisation très simple des cas a), b), (c 1), ..., (c 8).

Démonstration. — Supposons que la proposition n'est pas vérifiée par A. Montrons qu'on peut alors trouver un R-automorphisme $\psi_1\in H$ de $\mathbf{P}_2$ tel que les coefficients de l'équation de la courbe $A'_1=\psi_1(A)$ vérifient les inégalités

$$(8)\qquad v(\lambda'_1)\geqslant 1,\qquad v(\mu'_1)\geqslant 3,\qquad v(\alpha'_1)\geqslant 2,\qquad v(\beta'_1)\geqslant 4,\qquad v(\gamma'_1)\geqslant 6.$$

En effet, notre hypothèse implique que A ne vérifie les conditions d'aucun des deux cas *a)* ou *b)*. Donc A vérifie les conditions du cas *c)*, et on peut, comme on a vu, se ramener au cas où les coefficients λ, μ, α, β, γ sont de valuation $\geqslant 1$. Comme A ne vérifie, par hypothèse, aucune des conditions (c 1), (c 2) et (c 3), on a nécessairement $v(\beta)\geqslant 2$, $v(\gamma)\geqslant 2$ et, de plus, en posant $\mu_1=\mu t^{-1}$, $\gamma_2=\gamma t^{-2}$, puis $\mu_1^0=\rho(\mu)$, et $\gamma_2^0=\rho(\gamma)$, l'équation $Y^2+\mu_1^0Y-\gamma_2^0$ a une racine double η_1^0. Celle-ci est nécessairement rationnelle sur k^0. Soit η_1 un élément de R tel que $\eta_1^0=\rho(\eta_1)$. En transformant A par le R-automorphisme $\varphi_{0,t\eta_1}$ de $\mathbf{P}_2$, on se ramène au cas où $\eta_1^0=0$, c'est-à-dire où l'on a $v(\mu)\geqslant 2$, et $v(\gamma)\geqslant 3$.

D'autre part, A ne vérifie pas (c 4). Donc, si on pose $\alpha_1=\alpha t^{-1}$, $\beta_2=\beta t^{-2}$, $\gamma_3=\gamma t^{-3}$, et si on note α_1^0, β_2^0, γ_3^0 les éléments de k^0 réduits (mod. $\mathfrak{p}$) de α_1, β_2, γ_3 respectivement, l'équation $X^3+\alpha_1^0X^2+\beta_2^0X+\gamma_3^0$ ne peut admettre trois racines distinctes. L'une de ces racines ξ_1^0 est au moins double; celle-ci est nécessairement rationnelle sur k^0; soit ξ_1 un élément de k tel que $\xi_1^0=\rho(\xi_1)$. En transformant A par le R-automor-

phisme $\varphi_{t\xi_{1,0}}$ de $\mathbf{P}_2$, on se ramène au cas où $\xi_1^0=0$, c'est-à-dire où $v(\beta)\geqslant 3$ et $v(\gamma)\geqslant 4$.

Comme A ne vérifie pas (c 5), on a alors aussi $v(\alpha)\geqslant 2$. D'autre part A ne vérifie pas (c 6); donc, si on pose $\mu_2=\mu t^{-2}$, $\gamma_4=\gamma t^{-4}$, et si on note μ_2^0, γ_4^0 les éléments de k^0 réduits (mod. p) de μ_2 et γ_4 respectivement, l'équation $Y^2+\mu_2^0Y-\gamma_4^0$ a une racine double η_2^0, qui est rationnelle sur k^0. Soit η_2 un élément de R tel que $\eta_2^0=\rho(\eta_2)$. En transformant A par le R-automorphisme $\varphi_{0,t^2\eta_2}$ de $\mathbf{P}_2$, on se ramène au cas où $\eta_2^0=0$; ce qui implique $v(\mu)\geqslant 3$, $v(\alpha)\geqslant 2$, $v(\beta)\geqslant 3$ et $v(\gamma)\geqslant 5$.

Comme A ne vérifie aucune des conditions (c 7) et (c 8), on a alors, en fait, $v(\beta)\geqslant 4$ et $v(\gamma)\geqslant 6$; notre assertion est donc démontrée.

La transformée $A_1=\delta^{-1}(A_1')$ est alors une courbe de $\mathbf{P}_2$ ayant une équation de la forme (1), à coefficients entiers.

En supposant toujours que A ne vérifie pas la proposition, montrons maintenant qu'il existe, pour tout entier $h\geqslant 0$, un élément ψ_h de H tel que la courbe $A_h=\delta^{-h}\psi_h(A)$ de $\mathbf{P}_2$ ait une équation de la forme (1), à coefficients entiers.

Raisonnons en effet par récurrence sur h. Le résultat vient d'être établi pour $h=1$. Soit $\psi_{h-1}\in H$ tel que la courbe $A_{h-1}=\delta^{-(h-1)}\psi_{h-1}(A)$ ait une équation de la forme (1), à coefficients entiers. Puisque A ne vérifie pas la proposition, A_{h-1} ne la vérifie pas non plus. D'après la première partie de la démonstration, il existe un élément ψ_h' de H tel que les coefficients de $A_h'=\psi_h'(A_{h-1})$ vérifient les inégalités (8). La courbe $A_h=\delta^{-1}(A_h')=\delta^{-1}\psi_h'(A_{h-1})=\delta^{-1}\psi_h'\delta^{-(h-1)}\psi_{h-1}(A)$ a alors une équation de la forme (1), à coefficients entiers. Or si $\psi=\psi_{qrs}$ est un élément quelconque de H, on a $\delta\psi=\psi'\delta$, avec $\psi'=\psi_{q'r's'}$, en posant $q'=t^2q$, $r'=t^3r$, et $s'=ts$. Donc on a $\delta H\delta^{-1}\subset H$, ou encore $H\delta^{-1}\subset\delta^{-1}H$. Donc on a bien $A_h=\delta^{-h}\psi_h(A)$, avec $\psi_h\in H$.

La courbe $A_h''=\psi_h(A)=\delta^h(A_h)$ a alors une équation de la forme

$$Y^2Z+\lambda_h'XYZ+\mu_h'YZ^2=X^3+\alpha_h'X^2Z+\beta_h'XZ^2+\gamma_h'Z^3,$$

avec $v(\lambda_h')\geqslant h$, $v(\mu_h')\geqslant 3h$, $v(\alpha_h')\geqslant 2h$, $v(\beta_h')\geqslant 4h$, $v(\gamma_h')\geqslant 6h$.

D'après le lemme 2, les inégalités vérifiées par $v(\mu_h')$, $v(\beta_h')$ et $v(\gamma_h')$ entraînent, pour h assez grand, une contradiction.

Proposition 5. — Supposons que A *vérifie les conditions du cas* b), *i.e. que* A^0 *possède un point double à tangentes distinctes. Alors on a* $v(j(A))=-m<0$. *Pour tout entier* l, *on peut trouver un* R*-automorphisme* $\varphi\in H_0$ *de* $\mathbf{P}_2$ *tel que l'équation de la courbe* $A'=\varphi(A)$ *soit de la forme*

$$Y^2Z+\lambda XYZ+\mu'YZ^2=X^3+\alpha X^2Z+\beta'XZ^2+\gamma'Z^3,$$

où tous les coefficients sont entiers, et avec $v(\mu')\geqslant l$, $v(\beta')\geqslant l$.

Si on a pris $l>\frac{m}{2}$, *on a alors* $v(\gamma')=m$ (*on dira alors que* A' *vérifie la condition* (b_m)).

Démonstration. — On peut, comme dans la proposition 3 du n° 5, supposer qu'on a $\mu^0=\beta^0=\gamma^0$ (i.e. que μ, β et γ sont de valuation $\geqslant 1$). On a alors $\overline{\alpha}^0=(\lambda^0)^2+4\alpha^0\neq 0$.

Montrons qu'on peut trouver deux éléments q_0, r_0 de $\hat{R}$, appartenant à une même

extension k' de k de degré $\leqslant 2$, et tels que la courbe $A'_0 = \varphi_0(A)$ transformée de A par le $\mathfrak{R}$-automorphisme $\varphi_0 = \varphi_{q_0 r_0}$ de $\mathbf{P}_2$ ait une équation de la forme

$$Y^2Z + \lambda'_0 XYZ = X^3 + \alpha'_0 X^2Z + \gamma'_0 Z^3$$

(μ'_0 et β'_0 nuls). En effet, si la caractéristique de k^0 est $\neq 2$, l'équation de A'_0 est bien de la forme voulue, pourvu que q_0 soit l'une des racines du polynôme $P(U) = 6U^2 - (\lambda^2 + 4\alpha)U + \lambda\mu - 2\beta$, et qu'on ait $r_0 = \frac{1}{2}(\mu - a_0)$.

Or le polynôme réduit (mod. p) de P(U) est $P^0(U) = 6U^2 - \delta^0 U$. Puisqu'on a $\delta^0 \neq 0$, le polynôme P admet au moins une racine dans $\hat{R}$, d'après le lemme de Hensel. Il suffit de prendre pour q_0 cette racine.

Si la caractéristique de k^0 est 2, on a $\lambda^0 \neq 0$; il suffit de prendre $q_0 = -\mu/\lambda$, et $r_0 = (q_0^2 + \beta)/\lambda$ (et on a alors $k' = k$). Notre assertion est donc bien démontrée dans tous les cas.

Puisque q_0 et r_0 appartiennent à $\hat{R}$, on peut trouver des éléments q et r de R aussi voisins qu'on veut de q_0 et r_0 respectivement pour la topologie p-adique. Comme les coefficients de l'équation de la courbe $A' = \varphi_{qr}(A)$ dépendent continûment de q et r pour cette topologie, on peut choisir q et r de manière que μ' et β' soient aussi voisins qu'on veut de 0 et, en particulier, tels que $v(\beta') \geqslant l$ et $v(\mu') \geqslant l$.

La relation $v(j(A)) < 0$ résulte des formules (4), (5) et (6), donnant l'expression de j. D'après ces mêmes formules, appliquées à la courbe A', les relations

$$v(j(A)) = v(j(A')) = -m, \quad v(\beta') > \frac{m}{2} \quad \text{et} \quad v(\mu') > \frac{m}{2} \quad \text{entraînent} \quad v(\gamma') = m.$$

Proposition 6. — Supposons que la courbe elliptique A, *d'équation* (1), *vérifie la condition* (c 5) *de la proposition 4* ($v(\mu) \geqslant 1$, $v(\alpha) = 1$, $v(\beta) \geqslant 3$, $v(\gamma) \geqslant 4$).

Alors il existe un entier $m \geqslant 1$ *et un* R-*automorphisme* $\varphi \in H_0$ *de* $\mathbf{P}_2$, *tels que les coefficients de l'équation*

$$Y^2Z + \lambda XYZ + \mu' YZ^2 = X^3 + \alpha X^2Z + \beta' XZ^2 + \gamma' Z^3$$

de la courbe $A' = \varphi(A)$ *vérifient la condition suivante*

$$(c\,5_m) \quad \begin{cases} \textit{si} \quad m = 2n - 1, \\ v(\mu') \geqslant n+1 \qquad v(\beta') \geqslant n+2 \qquad v(\gamma') \geqslant 2n+2 \qquad v(\overline{\gamma}') = 2n+2 \\ \textit{si} \quad m = 2n, \\ v(\mu') \geqslant n+2 \qquad v(\beta') \geqslant n+2 \qquad v(\gamma') \geqslant 2n+3 \qquad v(\widetilde{\delta}') = 2n+4 \end{cases}$$

où l'on pose $\overline{\gamma}' = \mu'^2 + 4\gamma'$ *et* $\widetilde{\delta}' = \beta'^2 - 4\alpha'\gamma'$.

Remarque. — Il résultera de la propriété d'unicité du théorème 1 (ou des résultats du n° 8, dans le cas où la caractéristique de k^0 est différente de 2 et 3) que l'entier m est uniquement déterminé par la donnée de A.

Démonstration. — Appelons (c 5_m^*) la condition obtenue en remplaçant, dans (c 5_m), les égalités $v(\overline{\gamma}')=2n+2$ et $v(\widetilde{\delta}')=2n+4$ par les inégalités strictes $v(\gamma')>2n+2$ et $v(\widetilde{\delta}')>2n+4$.

Supposons que A ne vérifie pas la proposition, et montrons qu'il existe, pour tout entier $m\geqslant 1$, un R-automorphisme $\varphi_m\in H_0$ de $\mathbf{P}_2$ tel que la courbe $A_m=\varphi_m(A)$ vérifie (c 5_m^*).

Raisonnons en effet par récurrence sur m. Le résultat est évident pour $m=1$, car il suffit alors de prendre $A_1=A$. Soit φ_{m-1} un élément de H_0 tel que la courbe $A_{m-1}=\varphi_{m-1}(A)$ vérifie (c 5_{m-1}^*), et notons

$$Y^2Z+\lambda XYZ+\mu'YZ^2=X^3+\alpha XZ^2+\beta'X^2Z+\gamma'Z^3$$

l'équation de A_{m-1}.

Pour $m=2n$ (d'où $m-1=2n-1$), les éléments

$$\mu'_{n+1}=\mu' t^{-(n+1)} \text{ et } \gamma'_{2n+2}=\gamma' t^{-(2n+2)}$$

de k appartiennent à R, et, si on pose $\mu'^0_{n+1}=\rho(\mu'_{n+1})$ et $\gamma'^0_{2n+2}=\rho(\gamma'_{2n+2})$, le polynôme $Y^2+\mu'^0_{n+1}Y-\gamma'^0_{2n+2}$ a une racine double η^0. Celle-ci est rationnelle sur k^0. Soit $\eta\in R$ tel que $\eta^0=\rho(\eta)$, et soit

$$Y^2Z+\lambda XYZ+\mu''YZ^2=X^3+\alpha XZ^2+\beta''X^2Z+\gamma''Z^3 \tag{9}$$

l'équation de la courbe A_m transformée de A_{m-1} par l'élément $\varphi_{0,\eta t^{n+1}}$ de H_0. Cette courbe A_m vérifie encore la condition (c 5_{m-1}^*), mais, cette fois, la racine double du polynôme $Y^2+\mu''^0_{n+1}Y-\gamma''^0_{2n+2}$ est nulle. Autrement dit, on a

$$v(\mu'')\geqslant n+2, \text{ et } v(\gamma'')\geqslant 2n+3;$$

on a aussi $v(\beta'')\geqslant n+2$, puisque $\beta''=\beta'$. Puisque A ne vérifie pas la proposition, la courbe A_m ne vérifie pas (c 5_m). Donc, elle vérifie (c 5_m^*).

Pour $m=2n-1$ (d'où $m-1=2n-2$), les éléments $\alpha_1=\alpha t^{-1}$, $\beta'_{n+1}=\beta' t^{-(n+1)}$ et $\gamma'_{2n+1}=\gamma' t^{-(2n+1)}$ de k appartiennent à R et, si on pose $\alpha_1^0=\rho(\alpha_1)$, $\beta'^0_{n+1}=\rho(\beta'_{n+1})$ et $\gamma'^0_{2n+1}=\rho(\gamma'_{2n+1})$, le polynôme $\alpha_1^0X^2+\beta'^0_{n+1}X+\gamma'^0_{2n+1}$ a une racine double ξ^0. Celle-ci est rationnelle sur k^0. Soit ξ un élément de R tel que $\xi^0=\rho(\xi)$; l'équation de la courbe A_m, transformée de A_{m-1} par l'élément $\varphi_{\xi t^n,0}$ de H_0, est encore de la forme (9), et cette courbe A_m vérifie encore la condition (c 5_{m-1}^*), mais, cette fois, la racine double du polynôme $\alpha_1^0X^2+\beta''^0_{n+1}X+\gamma''^0_{2n+1}$ est nulle. Autrement dit, on a $v(\beta'')\geqslant n+2$, et $v(\gamma'')\geqslant 2n+2$; puisque $\mu''=\mu'$, on a aussi $v(\mu'')\geqslant n+1$. Comme la courbe A_m ne vérifie pas (c 5_m), elle vérifie (c 5_m^*).

Notre assertion concernant l'existence de A_m pour tout m est donc démontrée. Elle conduit à une contradiction, compte tenu du lemme 2. C.Q.F.D.

Nous dirons qu'une courbe elliptique plane, définie sur k, est p-*standard* si elle est représentée par une équation de la forme (1), à coefficients dans R, et si elle vérifie l'une des conditions a), b_m), (c 1), (c 2), (c 3), (c 4), (c 5_m), (c 6), (c 7) ou (c 8). Il résulte des propositions 4, 5 et 6 que toute courbe elliptique définie sur k, et possédant un point rationnel sur k, admet un k-modèle p-standard.

8. Interprétation de la classification précédente lorsque la caractéristique de $\mathbf{k}^0$ est différente de 2 et 3.

Considérons deux courbes elliptiques planes A et A′, définies sur un même corps $\mathbf{k}$ de caractéristique $\neq 2$, et représentées respectivement par les équations de Weierstrass :

$$Y^2Z = X^3 + \beta XZ^2 + \gamma Z^3 \tag{10}$$

$$Y^2Z = X^3 + \beta' XZ^2 + \gamma' Z^3 \tag{11}$$

On sait que, pour que ces deux courbes soient $\mathbf{k}$-isomorphes, il faut et il suffit qu'il existe un élément τ de $\mathbf{k}$ tel qu'on ait $\beta' = \tau^4\beta$, $\gamma' = \tau^6\gamma$; A′ est alors transformée de A par le $\mathbf{k}$-automorphisme de $\mathbf{P}_2$ qui, au point (x, y, z), fait correspondre $(\tau^2 x, \tau^3 y, z)$.

Soient j et j' les invariants respectifs de A et A′. Puisque A et A′ sont des courbes elliptiques, les discriminants $\Delta = 4\beta^3 + 27\gamma^2$ et $\Delta' = 4\beta'^3 + 27\gamma'^2$ sont $\neq 0$. Notons $\mathbf{k}^*$ le groupe multiplicatif de $\mathbf{k}$. Compte tenu des expressions de j et j' la condition d'isomorphisme précédente est équivalente à la suivante :

(*) $j = j'$, et Δ/Δ' est la puissance douzième d'un élément de $\mathbf{k}$.

Autrement dit, la donnée de la classe de A à un $\mathbf{k}$-isomorphisme près équivaut à celle des deux invariants suivants de A : $j = j(\mathrm{A})$, et l'image de Δ par l'homomorphisme canonique $\mathbf{k}^* \to \mathbf{k}^*/(\mathbf{k}^*)^{12}$.

Dans le cas où on a $\beta \neq 0$ et $\gamma \neq 0$ (c'est-à-dire $j \neq 0$, et $j \neq 2^6 3^3$), la condition (*) est équivalente à

(**) $j = j'$, et γ/γ' est le carré d'un élément de $\mathbf{k}^*$.

La donnée de la classe de A à un $\mathbf{k}$-isomorphisme près équivaut alors à celle des deux invariants suivants : $j = j(\mathrm{A})$, et l'image de Δ par l'homomorphisme $\mathbf{k}^* \to \mathbf{k}^*/(\mathbf{k}^*)^2$.

Revenons maintenant à la courbe A, définie sur k, du théorème 1, et supposons la caractéristique de k^0 différente de 2 et 3. On peut alors supposer que A est définie par une équation de Weierstrass de la forme (10), avec β et γ entiers.

Nous allons démontrer, comme il a été annoncé, que les différents cas considérés dans chacune des propositions 4 et 6 s'excluent mutuellement, et donner une caractérisation simple de chacun d'eux au moyen des invariants que nous venons d'introduire,

Soit en effet (A′, ψ) un k-modèle de A vérifiant les conditions de la proposition 4, et reprenons les notations introduites dans cette dernière. Le R-automorphisme $\psi_1 \in \mathrm{H}$ de $\mathbf{P}_2$ défini par $\psi_1 = \psi_{q_1 r_1 s_1}$, avec $q_1 = \frac{1}{3}\left(\alpha' + \frac{\lambda'^2}{4}\right)$, $r_1 = \frac{\mu'}{2}$ et $s_1 = \frac{\lambda'}{2}$, transforme A′ en la courbe de Weierstrass A_1 d'équation

$$Y^2Z = X^3 + \beta_1 X^2 Z + \gamma_1 Z^3$$

où β_1 et γ_1 sont les éléments de R définis par

$$\begin{cases} \beta_1 = \beta' + \dfrac{\lambda'\mu'}{2} - \dfrac{1}{3}\left(\alpha' + \dfrac{\lambda'^2}{4}\right)^2 \\ \gamma_1 = \gamma' + \dfrac{\mu'^2}{4} - \dfrac{1}{3}\left(\alpha' + \dfrac{\lambda'^2}{4}\right)^2\left(\beta' + \dfrac{\lambda'\mu'}{2}\right) + \dfrac{2}{27}\left(\alpha' + \dfrac{\lambda'^2}{4}\right)^3 \end{cases} \tag{12}$$

Si A′ vérifie la condition b), on déduit des relations (12) que β_1 et γ_1 sont des éléments inversibles de R. D'après la propriété (**) précédente, l'entier $v(\gamma)$ est *pair*. D'autre part, on a vu, dans la proposition 5, qu'on a $v(j)<0$, c'est-à-dire $j\notin R$.

Si A′ vérifie la condition (c 5), les relations (12) entraînent que β_1 et γ_1 sont $\neq 0$, et qu'on a $v(\beta_1)=2$, et $v(\gamma_1)=3$. D'après (**), l'entier $v(\gamma)$ est *impair*. D'autre part, la formule (4) du n° 6, appliquée à A′, permet de vérifier qu'on a $v(j)<0$, et plus précisément que si A′ vérifie la condition (c 5_m), on a $v(j)=-m$.

Dans le cas où A′ vérifie l'une des conditions a), (c 1), (c 2), (c 3), (c 4), (c 6), (c 7) ou (c 8), on déduit des relations (12) que A_1 vérifie aussi cette condition. Or, si on pose $\Delta_1=4\beta_1^3+27\gamma_1^2$, les conditions a), (c 1), (c 2), (c 3), (c 4), (c 6), (c 7) et (c 8) entraînent respectivement $v(\Delta_1)\equiv 0, 2, 3, 4, 6, 8, 9$ et 10 (mod. 12), d'où l'on déduit respectivement, compte tenu de (*), $v(\Delta)\equiv 0, 2, 3, 4, 6, 8, 9$ et 10 (mod. 12). Chacune de ces conditions entraîne d'autre part $v(j)\geqslant 0$ (c'est-à-dire $j\in R$).

Les propriétés obtenues pour A dans chaque cas sont récapitulées dans le tableau suivant. Ces propriétés s'excluent mutuellement, autrement dit chacune d'elles caractérise le cas auquel elle correspond.

Cas (b_m)	$v(j)=-m$	$v(\gamma)$ pair
Cas (c 5_m)	$v(j)=-m$	$v(\gamma)$ impair
Cas (a)	$v(j)\geqslant 0$	$v(\Delta)\equiv 0$ (mod. 12)
Cas (c 1)	—	$v(\Delta)\equiv 2$ —
Cas (c 2)	—	$v(\Delta)\equiv 3$ —
Cas (c 3)	—	$v(\Delta)\equiv 4$ —
Cas (c 4)	—	$v(\Delta)\equiv 6$ —
Cas (c 6)	—	$v(\Delta)\equiv 8$ —
Cas (c 7)	—	$v(\Delta)\equiv 9$ —
Cas (c 8)	—	$v(\Delta)\equiv 10$ —

Remarque. — On peut remplacer les propriétés $v(\gamma)$ pair et $v(\gamma)$ impair des cas b) et (c 5) par $v(j\Delta)\equiv 0$ (mod. 12), et $v(j\Delta)\equiv 6$ (mod. 12) respectivement.

D'après les propositions 5 et 6 du n° 7, et d'après les formules (4), (5) et (6) du n° 6 donnant l'expression de $j(A)$, on peut trouver des exemples montrant que la condition

$v(j)<0$ caractérisant le cas (b) ou (c 5)) n'est plus valable si k^0 est de caractéristique 2 ou 3.

En revanche, d'après la proposition 4, la relation $v(j) = -m$ a toujours lieu dans le cas b_m), quelle que soit la caractéristique de k^0.

9. Indications générales concernant la démonstration du théorème 1.

Le corps k^0 est supposé à nouveau de caractéristique quelconque. Nous allons maintenant aborder la démonstration du théorème 1. Il nous suffit, d'après ce qui précède, de supposer que A est une courbe elliptique plane p-standard, définie sur k; plus précisément, on peut supposer que A est représentée par une équation de la forme (1), et qu'elle vérifie l'une des conditions b_m), (c 1), (c 2), (c 3), (c 4), (c 5_m), (c 6), (c 7) ou (c 8); en effet, le résultat est évident dans le cas a), puisque A est alors elle-même p-simple p-minimale. Commençons par donner quelques indications générales concernant la méthode, le mode d'exposition, les notations utilisées.

La construction du k-modèle p-simple p-minimal de A sera toujours réalisée à partir d'un nombre fini de k-modèles plans (A_i, φ_i) $(1 \leqslant i \leqslant h)$ de A, tels que toutes les composantes de $A_i^0 = \rho(A_i)$ soient génériquement p-simples sur A_i; le nombre h de ces modèles dépendra du cas considéré. On prendra pour (A_*, θ) le *joint* de ces modèles (A_i, φ_i); autrement dit, en désignant par u un point générique de A sur k, et, pour tout i, par u_i le point générique correspondant $u_i = \varphi_i(u)$ de A_i sur k, on prendra pour A_* le lieu sur k du point $u_* = \theta(u) = u_1 \times \ldots \times u_h$ du produit de h facteurs $\mathbf{P}_2 \times \ldots \times \mathbf{P}_2$. Nous donnerons, *a priori*, dans chaque cas, la liste des modèles (A_i, φ_i). Nous ne chercherons pas à justifier le choix de ces modèles autrement que par la vérification, *a posteriori*, de la p-simplicité et (grâce aux propositions 1 et 2 précédentes) de la p-minimalité de A_*. Bornons-nous à indiquer que la méthode utilisée pour les obtenir a consisté à construire, dans chaque cas, une suite de k-modèles (B_i, ψ_i) de A tels que chacun d'eux s'obtienne en faisant « éclater » l'un au moins des points p-multiples du modèle précédent, par une transformation p-monoïdale (ou R-équivalente à une transformation p-monoïdale) du type introduit au n° 25 du chapitre I[er].

On désignera toujours par π_i la projection sur le i-ième facteur, dans le produit $\mathbf{P}_2 \times \ldots \times \mathbf{P}_2$, et par ψ_i le k-isomorphisme $A_* \to A_i$ induit par ψ_i. On a ainsi, pour tout i, $\psi_i = \varphi_i \circ \theta^{-1}$. On commencera par déterminer toutes les composantes du cycle $A_*^0 = \rho(A_*)$. Si C^0 est une telle composante, il existe un i tel que $\pi_i^0(C^0)$ soit de dimension 1, et, par conséquent, soit l'une des composantes C_i^0 de A_i^0. Soit alors u_i^0 un point générique de C_i^0 sur l'un de ses corps de définition k_i^0 contenant k^0. D'après le choix des A_i, le point u_i^0 est p-simple sur A_i. L'application $\psi_i^{-1} : A_i \to A_*$ est p-morphique en u_i^0, d'après la proposition 8 du n° 11 du chapitre I[er], donc est p-isomorphique en ce point, et a pour valeur un point générique u^0 de C^0 sur k^0. Donc on a montré que toutes les composantes de A_*^0 sont toujours génériquement p-simples sur A_*, et obtenu en même temps un procédé permettant de déterminer un point générique de chacune d'elles. De plus, ceci donne le coefficient de C^0 dans A_*^0 (égal à celui de C_i^0 dans A_i^0). Dans tous les cas où $h \geqslant 2$,

on donnera, dans un tableau, la liste de ces points génériques, chacun d'eux étant défini par ses projections sur les différents facteurs du produit $\mathbf{P}_2 \times \ldots \times \mathbf{P}_2$.

On appellera *sommet* du cycle A_*^0 tout point commun à plusieurs composantes de A_*^0 (on verra que, si l'on excepte le cas (c 3), il passe par tout sommet exactement deux composantes de A_*^0, dont ce sommet est l'unique point commun). Dans chaque cas, les sommets pourront être déterminés par simple lecture du tableau donnant les points génériques des composantes.

Pour vérifier la p-simplicité de A_*, on appliquera fréquemment les deux remarques suivantes :

Remarque 1. — Si la projection $u_i^0 = \psi_i^0(u^0)$ d'un point $u^0 \in A_*^0$ est un point p-simple sur A_i (resp. simple sur A_i^0), et si ψ_i^{-1} est p-finie en u_i^0, alors u^0 est p-simple sur A_* (resp. simple sur A_*^0); en effet ψ_i^{-1} est p-isomorphique en u_i^0, d'après la proposition 7 du chapitre I^er^.

Remarque 2. — Notons, pour tout couple (i, j), A_{ij} le lieu sur k du point $u_i \times u_j$, dans le produit $\mathbf{P}_2 \times \mathbf{P}_2$, et ψ_{ij} le k-isomorphisme $A_* \to A_{ij}$ induit par $\pi_i \times \pi_j$; si, de même, la projection $u_i^0 \times u_j^0 = \psi_{ij}^0(u^0)$ d'un point $u^0 \in A_*^0$ est un point p-simple sur A_{ij}, et, si ψ_{ij}^{-1} est p-finie en $u_i^0 \times u_j^0$, le point u^0 est p-simple sur A_*^0. La condition de p-finitude en $u_i^0 \times u_j^0$ est, en particulier, toujours satisfaite lorsque u^0 est un sommet, par lequel passent exactement deux composantes C_i^0, C_j^0 de A_*^0, telles que les projections $\pi_i^0(C_i^0)$ et $\pi_j^0(C_j^0)$ soient de dimension 1 (donc soient des composantes de A_i^0 et A_j^0 respectivement); sinon, en effet, il passerait par u^0 une troisième composante de A_*^0.

Pour vérifier la p-simplicité du point $u_i^0 \times u_j^0$ sur A_{ij}, on introduira alors des coordonnées locales $\overline{\xi}_i$, $\overline{\eta}_i$ (resp. $\overline{\xi}_j$, $\overline{\eta}_j$) de $\mathbf{P}_2$ en u_i^0 (resp. u_j^0), et les fonctions ξ_i, η_i (resp. ξ_j, η_j) qu'elles induisent sur A_{ij}. L'idéal maximal $\mathfrak{m}_{ij} = \mathfrak{m}(u_i^0 \times u_j^0, A_{ij})$ de l'anneau local $\mathfrak{o}_{ij} = \mathfrak{o}(u_i^0 \times u_j^0, A_{ij})$ admet pour générateurs ξ_i, η_i, ξ_j, η_j, t. On explicitera, dans chaque cas, les relations existant entre ces générateurs (déduites des équations de A_i et A_j, et des formules de passage des coordonnées de u_i à celles de u_j); on vérifiera que le nombre des générateurs de $\mathfrak{m}_{ij}$ peut être réduit à deux.

On vérifiera la p-minimalité de A_* en utilisant la proposition 1 du n° 2 ou la proposition 2 du n° 5. On prendra pour ω la différentielle induite sur A par l'une quelconque des différentielles $\omega_X = (Y dZ - Z dY)/(\partial F/\partial X)$, $\omega_Y = (Z dX - X dZ)/(\partial F/\partial Y)$ et $\omega_Z = (X dY - Y dX)/(\partial F/\partial Z)$ (cf. démonstration de la prop. 2), où F est le polynôme $Y^2Z + \lambda XYZ + \mu Y^2Z - (X^3 + \alpha X^2Z + \beta XZ^2 + \gamma Z^3)$. La différentielle sur A_i (resp. A_*) transposée de ω sera désignée par ω_i (resp. ω_*).

Dans tous les cas où certaines des composantes du cycle A_*^0 sont multiples, on emploiera, pour les désigner, une notation telle que ${}_qC^0$, ou ${}_qC_j^0$, l'indice de gauche étant le coefficient de la composante considérée dans le cycle; on pourra donc écrire $A_*^0 = \Sigma_{q,j}\, q\, {}_qC_j^0$; dans les mêmes conditions, un sommet qui est l'intersection de deux composantes de coefficients q et r sera représenté par une notation telle que ${}_{qr}s^0$, ou ${}_{qr}s_j^0$.

λ, μ, α, β, γ étant les coefficients de l'équation (1) définissant A, il sera commode de poser, pour tout entier j, $\lambda_j = \lambda t^{-j}$, $\mu_j = \mu t^{-j}$, $\alpha_j = \alpha t^{-j}$, $\beta_j = \beta t^{-j}$, $\gamma_j = \gamma t^{-j}$ et, lorsque

ces éléments sont entiers (i.e. appartiennent à R), de désigner par λ_j^0, μ_j^0, α_j^0, β_j^0, γ_j^0 les éléments de k^0 réduits (mod. $\mathfrak{p}$) de λ_j, μ_j, α_j, β_j, γ_j respectivement.

Les points (1, 0, 0), (0, 1, 0) et (0, 0, 1) de $\mathbf{P}_2^0$ sont notés respectivement a^0, b^0, c^0. Le k-automorphisme de $\mathbf{P}_2$ qui, au point (x, y, z), fait correspondre (x, y, tz) est noté σ.

10. Démonstration du théorème 1 (cas ($\mathbf{b}_m$)).

$$\left(v(\alpha)=0, \qquad v(\mu)>\frac{m}{2}, \qquad v(\beta)>\frac{m}{2}, \qquad v(\gamma)=m\right)$$

Rappelons que le point $c^0=(0, 0, 1)$ est l'unique point multiple (double, à tangentes distinctes) de A^0. Pour $m=1$, comme on a $(\partial F/\partial t)_*^0(c^0)\neq 0$, c^0 est $\mathfrak{p}$-simple sur A.

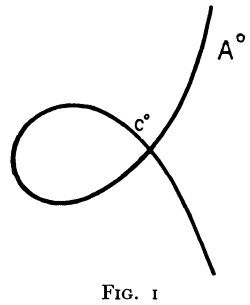


FIG. 1

Donc A est $\mathfrak{p}$-simple; donc A est $\mathfrak{p}$-minimale, d'après le corollaire de la proposition 2.

Supposons maintenant $m\geqslant 2$. Posons $m=2h$, ou $m=2h+1$ suivant que m est pair ou impair. Pour tout entier i ($1\leqslant i\leqslant h$), la puissance i-ième σ^i du k-automorphisme σ de $\mathbf{P}_2$ induit un k-isomorphisme $\varphi_i : A\to A_i$ de A sur la courbe A_i ayant pour équation

$$Y^2Z+\lambda XYZ+\mu_i YZ^2=t^iX^3+\alpha X^2Z+\beta_i XZ^2+\gamma_{2i}Z^3$$

On prend alors pour (A_*, θ) le joint des modèles (A_i, φ_i) de A ($1\leqslant i\leqslant h$).

Pour $i<\frac{m}{2}$, le cycle réduit A_i^0 a pour équation

$$Y^2Z+\lambda^0XYZ=\alpha^0X^2Z$$

Il admet pour composantes les droites $Z=0$, $Y=\nu^0X$, $Y=\bar{\nu}^0X$, où ν^0 et $\bar{\nu}^0$ sont les racines (distinctes) du polynôme $U^2+\lambda^0U-\alpha^0$, déjà considérées au n° 5. Le triangle formé par ces trois droites a pour sommets les points $c^0=(0, 0, 1)$, $a_1^0=(1, \nu^0, 0)$ et $\bar{a}_1^0=(1, \bar{\nu}^0, 0)$.

Pour $i=\frac{m}{2}$ (ce qui implique $i=h$, et $m=2h$), le cycle réduit $A_i^0=A_h^0$ a pour équation

$$Y^2Z+\lambda XYZ=\alpha^0X^2Z+\gamma_{2h}^0Z^3$$

Il admet pour composantes la droite $Z=0$, et une conique non dégénérée $\tilde{C}^0$. Les points communs (distincts) à ces deux composantes sont a_1^0 et $\bar{a}_1^0$.

Le tableau suivant donne les composantes de A_*^0, chacune d'elles étant déterminée par un point générique, comme il a été indiqué plus haut. On note respectivement w^0, v^0, $\overline{v}^0$ et $\widetilde{v}^0$ des points génériques, sur $k'^0 = k^0(\nu^0)$, des droites $Z = 0$, $Y = \nu^0 X$, $Y = \overline{\nu}^0 X$, et de la conique $\widetilde{C}^0$.

Composantes		Points génériques
	C_0^0	$w^0 \times w^0 \times w^0 \times \ldots \ldots \ldots \ldots \ldots \ldots \times w^0$
	C_1^0	$v^0 \times a_1^0 \times a_1^0 \times \ldots \ldots \ldots \ldots \ldots \ldots \times a_1^0$
	C_{m-1}^0	$v^0 \times \overline{a}_1^0 \times \overline{a}_1^0 \ldots \ldots \ldots \ldots \ldots \ldots \times \overline{a}_1^0$
	C_i^0	$c^0 \times c^0 \times \ldots \times c^0 \times v^0 \times a_1^0 \times \ldots \ldots \times a_1^0 \times a_1^0$
	C_{m-i}^0	$c^0 \times c^0 \times \ldots \times c^0 \times \overline{v}^0 \times \overline{a}_1^0 \times \ldots \ldots \times \overline{a}_1^0 \times \overline{a}_1^0$ ($i-1$ facteurs égaux à c^0)
	C_{h-1}^0	$c^0 \times c^0 \times \ldots \ldots \ldots \ldots \ldots \ldots \times c^0 \times v^0 \times a_1^0$
	C_{m-h+1}^0	$c^0 \times c^0 \times \ldots \ldots \ldots \ldots \ldots \ldots \times c^0 \times \overline{v}^0 \times \overline{a}_1^0$
(si $m = 2h+1$)	C_h^0	$c^0 \times c^0 \times \ldots \ldots \ldots \ldots \ldots \ldots \times c^0 \times v^0$
(si $m = 2h+1$)	C_{h+1}^0	$c^0 \times c^0 \times \ldots \ldots \ldots \ldots \ldots \ldots \times c^0 \times \overline{v}^0$
(si $m = 2h$)	C_h^0	$c^0 \times c^0 \times \ldots \ldots \ldots \ldots \ldots \ldots \times c^0 \times \widetilde{v}^0$

Les sommets sont les m points suivants :

$$s_1^0 = a_1^0 \times a_1^0 \times \ldots \ldots \ldots \ldots \times a_1^0$$
$$s_m^0 = \overline{a}_1^0 \times \overline{a}_1^0 \times \ldots \ldots \ldots \ldots \times \overline{a}_1^0$$
$$\ldots \ldots \ldots \ldots \ldots \ldots$$
$$s_i^0 = c^0 \times c^0 \times \ldots \times c^0 \times a_1^0 \times \ldots \times a_1^0$$
$$s_{m-i+1}^0 = c^0 \times c^0 \times \ldots \times c^0 \times \overline{a}_1^0 \times \ldots \times \overline{a}_1^0$$

($2 \leqslant i \leqslant h$) ($i-1$ facteurs égaux à c^0)

et, si $m = 2h+1$,

$$s_{h+1}^0 = c^0 \times c^0 \times \ldots \ldots \ldots \ldots \times c^0$$

Chaque sommet appartient à deux composantes, et chaque composante contient deux sommets; les composantes sont connectées à la façon des côtés d'un polygone (fig. 2).

Tout point de A_*^0 autre qu'un sommet se projette sur l'un des facteurs en un point simple sur le cycle réduit correspondant; d'après la remarque 1 du n° 9, un tel point est donc simple sur A_*^0. De même, les sommets s_1^0, s_m^0 et (si $m = 2h+1$) s_{h+1}^0 sont p-simples sur A_*; en effet, les points c_1^0, $\overline{c}_1^0$ sont p-simples sur A_1, et, si $m = 2h+1$, le point c^0 est p-simple sur A_h.

Il reste à montrer que l'un quelconque des autres sommets, par exemple s_i^0 ($2 \leqslant i \leqslant h$) est p-simple sur A_*. Pour cela, il suffit, d'après la remarque 2 du n° 9, de montrer que

le point $c^0 \times a_1^0$ est p-simple sur la courbe $A_{i-1,i} = \pi_{i-1,i}(A_*)$. L'idéal maximal $\mathfrak{m}_i$ de l'anneau local $\mathfrak{o}_i = \mathfrak{o}(c^0 \times a_1^0, A_{i-1,i})$ est engendré par les fonctions $\xi_{i-1}, \eta_{i-1}, \eta_i, \zeta_i, t$, où ξ_{i-1}, η_{i-1} sont induites respectivement par les fonctions X_{i-1}/Z_{i-1} et Y_{i-1}/Z_{i-1} sur le $(i-1)$-ième facteur, et où ξ_i, ζ_i sont induites respectivement par les fonctions $Y_i/X_i - \nu$ et Z_i/X_i sur le i-ième facteur, ν étant un élément de R tel que $\rho(\nu) = \nu^0$.

De la relation $u_i = \sigma(u_{i-1})$, on tire $\eta_{i-1} = \xi_{i-1}(\eta_i + \nu)$ et $t = \xi_{i-1}\zeta_i$. En portant ces expressions dans l'équation de A_{i-1}, on obtient une relation de la forme

$$(2\nu + \lambda)\eta_i \equiv r_i \xi_{i-1} + s_i \zeta_i \qquad (\text{mod. } \mathfrak{m}_i^2),$$

où r_i et s_i sont des éléments de R. Comme on a $2\nu^0 + \lambda^0 \neq 0$, quelle que soit la caractéristique de k^0, on en déduit que $\mathfrak{m}_i$ est engendré par ξ_{i-1} et ζ_i. Donc $\mathfrak{o}_i$ est régulier,

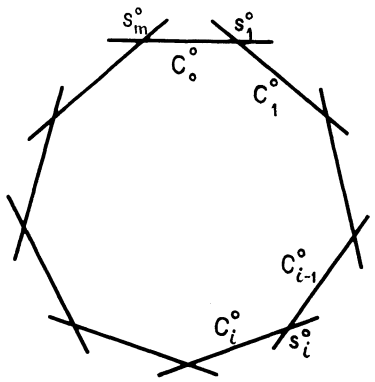


FIG. 2

i.e. $c^0 \times a_1^0$ est p-simple sur $A_{i-1,i}$. On a donc complètement démontré que A_* est p-simple.

D'autre part, d'après la proposition 2 du n° 3, appliquée à A_i, l'entier $\nu(C_{ij}^0, \omega_i, A_i)$ s'annule sur toutes les composantes C_{ij}^0 de A_i^0. En remontant à A_*, on en déduit que l'entier $\nu(C_i^0, \omega_*, A_*)$ s'annule pour tout i. D'après la proposition 1 du n° 2, A_* est donc p-minimale.

Déterminons maintenant la structure du groupe $\mathscr{G}_\mathfrak{p}(A)$. D'après la proposition 3 du n° 5, l'ensemble $\mathscr{S}(A^0)$, muni de la loi α_A^0 réduite (mod. $\mathfrak{p}$) de α_A, possède une structure de groupe algébrique, et ce groupe est isomorphe (sur l'extension k'^0 de k^0) au groupe multiplicatif $\mathbf{G}_m$. Or le k-isomorphisme $\theta : A \to A_*$ applique p-isomorphiquement $\mathscr{S}(A^0)$ sur la composante de l'élément neutre de $\mathscr{S}(A_*^0)$ (i.e. la composante C_0^0, privée des sommets s_1^0 et s_m^0). Donc cette dernière est isomorphe à $\mathbf{G}_m$, pour la loi $\alpha_{A_*}^0$ réduite (mod. $\mathfrak{p}$) de α_{A_*}. Donc la composante de l'origine $\mathscr{G}_{\mathfrak{p}0}(A)$ de $\mathscr{G}_\mathfrak{p}(A)$ est isomorphe à $\mathbf{G}_m$. La symétrie $x \to -x$ fait correspondre C_i à C_{m-i} $(1 \leqslant i \leqslant m-1)$. Il en résulte que toute translation $\tau \in \mathscr{T}(A)$ qui applique C_0^0 sur C_1^0 applique également C_{m-1}^0 sur C_0^0. Comme la translation τ permute les composantes de A_*^0, et respecte la connexion de ces composantes deux à deux, elle les permute circulairement. Donc le groupe $\Gamma(A) = \mathscr{G}_\mathfrak{p}(A)/\mathscr{G}_{\mathfrak{p}0}(A)$ est *cyclique* d'ordre m.

11. Démonstration du théorème 1 (cas (c 1), (c 2), (c 3), (c 4)).

Cas (c 1) $(v(\gamma)=1)$. — L'unique point multiple $c^0=(0,0,1)$ de A^0 est p-simple sur A puisqu'on a $(\partial F/\partial t)^0_*(c^0)\neq 0$. Donc A est p-simple. Donc A est p-minimale, d'après le corollaire à la proposition 2 du n° 3. D'après la proposition 3 du n° 5, le groupe $\mathscr{G}_p(A)$ est k^0-isomorphe à $\mathbf{G}_a$.

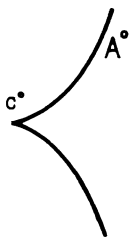


FIG. 3

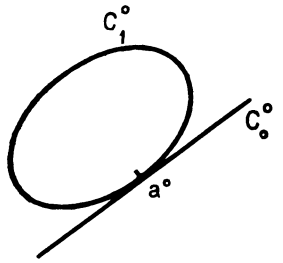


FIG. 4

Cas (c 2) $(v(\beta)=1,\ v(\gamma)\geqslant 2)$. — On prend pour A_* la courbe $A_1=\sigma(A)$, et pour θ le k-isomorphisme $A\to A_*$ induit par σ. L'équation de $A_*=A_1$ est :

$$Y^2Z+t\lambda_1XYZ+\mu_1YZ^2=X^3+t\alpha_1X^2Z+\beta_1XZ^2+\gamma_2Z^3 \tag{13}$$

L'équation du cycle réduit A_1^0 est $Z(Y^2+\mu_1^0YZ-\beta_1^0X^2-\gamma_2^0Z^2)=0$.

Ce cycle est décomposé en la droite C_0^0 $(Z=0)$ et une conique non dégénérée (puisque $\beta_1^0\neq 0$). Ces deux composantes sont tangentes au point $a^0=(1,0,0)$ (fig. 4). D'après l'équation (13), a^0 est p-simple sur A_1. Donc A_* est p-simple. Donc A_* est p-minimale, d'après le corollaire à la proposition 2 du n° 3.

L'ensemble $\mathscr{S}(A^0)$, muni de la loi α_A^0 réduite (mod. p) de α_A est encore isomorphe à $\mathbf{G}_a$ sur le corps k^0. Or le k-isomorphisme $\varphi : A\to A_1$ applique p-isomorphiquement $\mathscr{S}(A^0)$ sur la composante de l'origine de $\mathscr{S}(A_1^0)$ (la droite C_0^0, privée du point a^0). Donc $\mathscr{G}_{p0}(A)$ est k^0-isomorphe à $\mathbf{G}_a$. Le groupe $\Gamma(A)=\mathscr{G}_p(A)/\mathscr{G}_{p0}(A)$ est d'ordre 2.

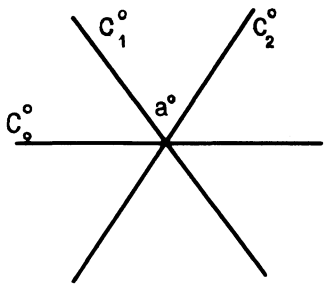


FIG. 5

Cas (c 3) $(v(\beta)\geqslant 2,\ v(\gamma)\geqslant 2,\ v(\overline{\gamma})=2)$. — On prend encore $A_*=A_1$. On a alors $\beta_1^0=0$, et $(\mu_1^0)^2+4\gamma_2^0\neq 0$. Donc $A_*^0=A_1^0$ est décomposée en trois droites distinctes C_0^0 $(Z=0)$, C_1^0, C_2^0 concourantes en a^0. D'après l'équation (13), le point a^0 est encore

p-simple sur A_1. Donc $A_1 = A_*$ est p-simple. Donc A_* est p-minimale, d'après le corollaire à la proposition 2 du n° 3.

Le groupe $\Gamma(A)$ est d'ordre 3 et, comme dans le cas précédent, $\mathscr{G}_{p0}(A)$ est isomorphe à $\mathbf{G}_a$ sur k^0.

Cas (c 4) $(v(\mu) \geqslant 2,\ v(\beta) \geqslant 2,\ v(\gamma) \geqslant 3,\ v(\Delta) = 6)$. — Notons ε le k-automorphisme du plan projectif $\mathbf{P}_2$ qui, au point (x, y, z), fait correspondre (tx, y, tz). Les k-automorphismes ε et $\sigma\varepsilon$ de $\mathbf{P}_2$ induisent des k-isomorphismes $\varphi_1 : A \to A_1$ et $\varphi_2 : A \to A_2$ de A sur les courbes planes A_1 et A_2 respectivement définies par les équations

$$A_1 \mid\ Y^2Z + t\lambda_1XYZ + t\mu_2YZ^2 = tX^3 + t\alpha_1X^2Z + t\beta_2XZ^2 + t\gamma_3Z^3$$
$$A_2 \mid\ tY^2Z + t\lambda_1XYZ + t\mu_2YZ^2 = X^3 + \alpha_1X^2Z + \beta_2XZ^2 + \gamma_3Z^3$$

On prend pour (A_*, θ) le joint de ces deux modèles (A_1, φ_1) et (A_2, φ_2).

Le cycle réduit A_1^0 a pour équation $Y^2Z = 0$. Il est décomposé en les droites $Y = 0$ (double) et $Z = 0$. Les seuls points p-multiples sont les points $a_i^0 = (\xi_{i0}^0, 0, 1)$, $(i = 1, 2, 3)$ où les ξ_{i0}^0 sont les trois racines (distinctes, puisque $v(\Delta) = 6$) du polynôme $X^3 + \alpha_1^0X^2 + \beta_2^0X + \gamma_3^0 = 0$.

Le cycle réduit A_2^0 a pour équation

$$X^3 + \alpha_1^0X^2Z + \beta_2^0XZ^2 + \gamma_3^0Z^3 = 0.$$

Il se compose des trois droites, distinctes et concourantes D_i^0 $(i = 1, 2, 3)$ respectivement définies par les équations $X - \xi_{i0}^0Z = 0$.

Les composantes de A_*^0 sont données par le tableau ci-dessous :

Composantes	Points génériques
${}_1C_0^0$	$w^0 \times b^0$
${}_1C_i^0$ $(i = 1, 2, 3)$	$a_i^0 \times u_i^0$
${}_2C^0$	$v^0 \times b^0$

où v^0 et w^0 sont des points génériques sur k^0 des droites $Y = 0$ et $Z = 0$ respectivement, et où u_i^0 est un point générique de D_i^0 sur $k_i^0 = k^0(\xi_i^0)$ $(i = 1, 2, 3)$. De plus, les composantes ${}_1C_i^0$ $(i = 1, 2, 3)$ sont simples, tandis que ${}_2C^0$ est double.

Le cycle A_*^0 admet quatre sommets, qui sont les points :

$$s_0^0 = {}_{12}s_0^0 = a^0 \times b^0$$
$$s_i^0 = {}_{12}s_i^0 = a_i^0 \times b^0 \qquad (i = 1, 2, 3)$$

En appliquant la remarque 1 du n° 9, on voit que tout point de $\rho_e(A_*) = \operatorname{supp} A_*^0$ autre qu'un sommet est p-simple sur A_*; de même, comme a^0 est p-simple sur A_1, le sommet s_0^0 est p-simple sur A_*.

Il reste à montrer que l'un quelconque des trois sommets s_i^0 $(i = 1, 2, 3)$ est p-simple,

ou encore que l'anneau local $\mathfrak{o}_i = \mathfrak{o}(s_i^0, A_*)$ est régulier. Or l'idéal maximal $\mathfrak{m}_i$ de cet anneau est engendré par $\xi_{i1}, \eta_1, \xi_2, \zeta_2, t$, où $\xi_{i1}, \eta_1, \xi_2, \zeta_2$ sont les fonctions sur A_* respectivement induites par $(X_1/Z_1) - \xi_{i0}$, Y_1/Z_1, X_2/Y_2, Z_2/Y_2, en désignant par ξ_{i0} un élément quelconque de $\mathfrak{R}$ tel que $\xi_{i0}^0 = \rho(\xi_{i0})$. Compte tenu de $A_2 = \sigma(A_1)$, on a les relations $\xi_2 = \zeta_2(\xi_{i0} + \xi_{i1})$, et $t = \eta_1\zeta_2$. En portant dans l'équation de A_1, on voit qu'on a $\eta_1 \in \mathfrak{m}_i^2$, donc que $\mathfrak{m}_i$ est engendré par ξ_{i1} et ζ_2. Donc $\mathfrak{o}_i$ est bien régulier. Donc A_* est $\mathfrak{p}$-simple.

La $\mathfrak{p}$-minimalité de A_* s'obtient immédiatement au moyen de la proposition 2 du n° 3, appliquée à A_1 et A_2, et du critère de $\mathfrak{p}$-minimalité (n° 2, prop. 1).

Le k-isomorphisme $\theta : A \to A_*$ applique encore $\mathfrak{p}$-isomorphiquement $\mathscr{S}(A^0)$ sur la composante de l'origine de $\mathscr{S}(A_*^0)$ ($_1C_0^0$, privée du point s_0^0). Le groupe $\mathscr{G}_{\mathfrak{p}0}(A)$

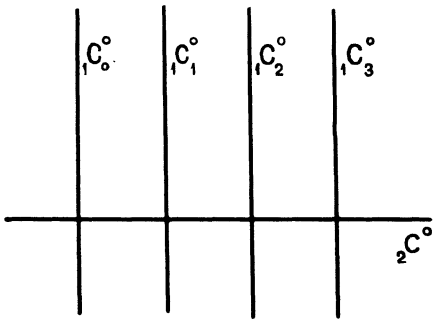


FIG. 6

est donc isomorphe à $\mathbf{G}_a$. D'autre part, $\Gamma = \Gamma(A)$ est *fini d'ordre 4*. Si on pose $_1\mathscr{S}_i^0 = \mathscr{S}(A_*^0) \cap {}_1C_i^0$ $(i = 1, 2, 3)$ on voit, en appliquant à la courbe A_2 le lemme 1 du n° 3, que le k-morphisme $\beta_* : A_* \times A_* \to A_*$ défini par $\beta_*(x, y) = -(x + y)$ applique $_1\mathscr{S}_1^0 \times {}_1\mathscr{S}_2^0$ sur $_1\mathscr{S}_3^0$. Donc les éléments de Γ respectivement représentés par les trois composantes $_1\mathscr{S}_i^0$ $(i = 1, 2, 3)$ de $\mathscr{S}(A_*^0)$, i.e. les trois éléments non nuls de Γ, ont pour somme 0. Donc Γ est *non cyclique*.

12. Démonstration du théorème 1 (cas (c 5_m)).

Pour tout entier $j \geqslant 0$, on note $\bar{\sigma}_j$ le k-automorphisme du plan projectif $\mathbf{P}_2$ défini par $\bar{\sigma}_j = \sigma^i$ pour $j = 2i - 1$, et $\bar{\sigma}_j = \varepsilon\sigma^i$ pour $j = 2i$. Si $u = (x, y, z)$ est un point générique de A sur k, le point $u_j = \bar{\sigma}_j(x)$ admet donc pour coordonnées $(x, y, t^i z)$ ou $(tx, y, t^i z)$ suivant qu'on a $j = 2i - 1$ ou $j = 2i$.

On pose $h = m + 2$. On note $A_1, \ldots, A_h$ les transformées de A par $\bar{\sigma}_1, \ldots, \bar{\sigma}_h$ respectivement, et on considère les k-isomorphismes $\varphi_1 : A \to A_1, \ldots, \varphi_h : A \to A_h$ respectivement induits par $\bar{\sigma}_1, \ldots, \bar{\sigma}_h$. On prend pour (A_*, θ) le joint des modèles $(A_1, \varphi_1), \ldots, (A_h, \varphi_h)$.

Les courbes A_{2i-1} et A_{2i} sont respectivement définies par les équations suivantes, à coefficients dans R :

$$A_{2i-1} \mid Y^2Z + t\lambda_1XYZ + \mu_iYZ^2 = t^iX^3 + t\alpha_1X^2Z + \beta_iXZ^2 + \gamma_{2i}Z^3$$
$$A_{2i} \mid tY^2Z + t\lambda_1XYZ + \mu_iYZ^2 = t^{i-1}X^3 + \alpha_1X^2Z + \beta_{i-1}XZ^2 + \gamma_{2i+1}Z^3$$

L'équation du cycle réduit A^0_{2i-1} est toujours $Y^2Z=0$, sauf pour $i=n+1$, si $m=2n-1$, auquel cas cette équation est $Y^2Z+\mu^0_{n+1}YZ^2=\gamma^0_{2n+2}Z^3$. Le cycle $A^0_{2i-1}=A^0_{2n+1}=A^0_h$ est alors décomposé en trois droites distinctes, concourantes en $a^0=(1,0,0)$, à savoir celles respectivement définies par les équations $Z=0$, $Y=\eta^0_*Z$ et $Y=\overline{\eta}^0_*Z$, où η^0_* et $\overline{\eta}^0_*$ sont les racines (distinctes, d'après (c 5_m)) du polynôme $Q^0_n=Y^2+\mu^0_{n+1}Y+\gamma^0_{2n+2}$.

L'équation du cycle A^0_2 est $X^2(X+\alpha^0_1Z)=0$. Pour $i\geqslant 2$, l'équation du cycle A^0_{2i} est toujours $Y^2Z=0$, sauf pour $i=n+1$, si $m=2n$, auquel cas cette équation est $Z(\alpha^0_1X^2+\beta^0_{n+2}XZ+\gamma^0_{2n+3}Z^2)=0$. Le cycle $A^0_{2i}=A^0_{2n+2}=A^0_h$ est alors décomposé en trois droites distinctes, concourantes en $b^0=(0,1,0)$, à savoir celles respectivement définies par les équations $Z=0$, $X=\xi^0_*Z$ et $X=\overline{\xi}^0_*Z$, où ξ^0_* et $\overline{\xi}^0_*$ sont les racines (distinctes d'après (c 5_m)) du polynôme $P^0_n=\alpha^0_1X^2+\beta^0_{n+2}X+\gamma^0_{2n+3}$.

Pour m impair ($m=2n+1$), les composantes de A^0_* sont données par le tableau ci-dessous :

Composantes	Points génériques
${}_1C^0_0$	$w^0\times b^0\times w^0\times b^0\times\ldots\ldots\ldots\ldots\times w^0\times b^0\times w^0$
${}_1C^0_1$	$\widetilde{c}^0_1\times\widetilde{u}^0_1\times a^0\times w^0\times\ldots\ldots\ldots\ldots\times a^0\times w^0\times a^0$
${}_2C^0_1$	$v^0\times b^0\times a^0\times b^0\times\ldots\ldots\ldots\ldots\times a^0\times b^0\times a^0$
${}_2C^0_2$	$c^0\times u^0\times a^0\times b^0\times\ldots\ldots\ldots\ldots\times a^0\times b^0\times a^0$
. . . . .	. . . . .
${}_2C^0_{2i-1}$	($2i-2$ facteurs égaux à c^0) $c^0\times c^0\times\ldots\times c^0\times v^0\times b^0\times a^0\times\ldots\ldots\ldots\times b^0\times a^0$
${}_2C^0_{2i}$	$c^0\times c^0\times\ldots\times c^0\times c^0\times u^0\times a^0\times\ldots\ldots\ldots\times b^0\times a^0$ ($2i-1$ facteurs égaux à c^0)
. . . . .	. . . . .
${}_2C^0_{2n-1}$	$c^0\times c^0\times\ldots\ldots\ldots\ldots\ldots\times c^0\times v^0\times b^0\times a^0$
${}_2C^0_{2n}$	$c^0\times c^0\times\ldots\ldots\ldots\ldots\ldots\times c^0\times c^0\times u^0\times a^0$
${}_1C^0_2$	$c^0\times c^0\times\ldots\ldots\ldots\ldots\ldots\times c^0\times c^0\times b^0_*\times v^0_*$
${}_1C^0_3$	$c^0\times c^0\times\ldots\ldots\ldots\ldots\ldots\times c^0\times c^0\times\overline{b}^0_*\times\overline{v}^0_*$

dans lequel on désigne respectivement par a^0, b^0, c^0, $\widetilde{c}^0_1$, b^0_*, $\overline{b}^0_*$ les points (1, 0, 0), (0, 1, 0), (0, 0, 1), $(-\alpha^0_1, 0, 1)$, $(0, \eta^0_*, 1)$, $(0, \overline{\eta}^0_*, 1)$ de $\mathbf{P}_2$; par u^0, v^0, w^0 des points génériques sur k^0

des droites $X=0$, $Y=0$ et $Z=0$ respectivement; par $\widetilde{u}_1^0$ le point (générique sur k^0) de la droite $X+\alpha_1^0 Z=0$, défini comme intersection de cette dernière avec celle joignant c^0 et w^0; par v_*^0 et $\overline{v}_*^0$ des points génériques sur le corps $k^0(\eta_*^0)$, des droites $Y=\eta_*^0 Z$, et $Y=\overline{\eta}_*^0 Z$ respectivement.

En supposant toujours $m=2n-1$, les sommets de A_*^0 sont les points

$$s_0^0={}_{12}s_0^0={}_1C_0^0\cap{}_2C_1^0 \quad =a^0\times b^0\times a^0\times b^0\times\ldots\ldots\times a^0\times b^0\times a^0$$
$$s_1^0={}_{12}s_1^0={}_1C_1^0\cap{}_2C_1^0 \quad =\widetilde{c}^0\times b^0\times a^0\times b^0\times\ldots\ldots\times a^0\times b^0\times a^0$$
$$s_2^0={}_{12}s_2^0={}_1C_2^0\cap{}_2C_{m+1}^0=c^0\times c^0\times c^0\times\ldots\ldots\ldots\times c^0\times b_*^0\times a^0$$
$$s_3^0={}_{12}s_3^0={}_1C_3^0\cap{}_2C_{m+1}^0=c^0\times c^0\times c^0\times\ldots\ldots\ldots\times c^0\times \overline{b}_*^0\times a^0$$

et, pour tout i tel que $1\leqslant i\leqslant n-1$,

$$\overline{s}_{2i-1}^0={}_{22}s_{2i-1}^0={}_2C_{2i-1}^0\cap{}_2C_{2i}^0=c^0\times c^0\times\ldots\times c^0\times b^0\times a^0\times b^0\times\ldots\times a^0\times b^0\times a^0$$
($2i-1$ facteurs égaux à c^0)

$$\overline{s}_{2i}^0 \quad ={}_{22}s_{2i}^0 \quad ={}_2C_{2i}^0\cap{}_2C_{2i+1}^0=c^0\times c^0\times\ldots\times c^0\times c^0\times a^0\times b^0\times\ldots\times a^0\times b^0\times a^0$$
($2i$ facteurs égaux à c^0)

Pour *m pair* ($m=2n$), les composantes de A_*^0 sont données par le tableau ci-dessous :

Composantes	Points génériques
${}_1C_0^0$	$w^0\times b^0\times w^0\times b^0\times w^0\times\ldots\ldots\times b^0\times w^0\times b^0$
${}_1C_1^0$	$\widetilde{c}^0\times\widetilde{u}_1^0\times a^0\times w^0\times a^0\times\ldots\ldots\times w^0\times a^0\times w^0$
${}_2C_1^0$	$v^0\times b^0\times a^0\times b^0\times a^0\times\ldots\ldots\ldots\times b^0\times a^0\times b^0$
${}_2C_2^0$	$c^0\times u^0\times a^0\times b^0\times a^0\times\ldots\ldots\ldots\times b^0\times a^0\times b^0$
. . . . .	. . . . .
	($2i-2$ facteurs égaux à c^0)
${}_2C_{2i-1}^0$	$c^0\times c^0\times\ldots\times c^0\times v^0\times b^0\times a^0\times\ldots\times b^0\times a^0\times b^0$
${}_2C_{2i}^0$	$c^0\times c^0\times\ldots\times c^0\times c^0\times u^0\times a^0\times\ldots\times b^0\times a^0\times b^0$
	($2i-1$ facteurs égaux à c^0)
. . . . .	. . . . .
${}_2C_{2n}^0$	$c^0\times c^0\times\ldots\ldots\ldots\ldots\ldots\times c^0\times u^0\times a^0\times b^0$
${}_2C_{2n+1}^0$	$c^0\times c^0\times\ldots\ldots\ldots\ldots\ldots\times c^0\times c^0\times v^0\times b^0$
${}_1C_2^0$	$c^0\times c^0\times\ldots\ldots\ldots\ldots\ldots\times c^0\times c^0\times a_*^0\times u_*^0$
${}_1C_3^0$	$c^0\times c^0\times\ldots\ldots\ldots\ldots\ldots\times c^0\times c^0\times \overline{a}_*^0\times u_*^0$

où les notations $a^0, b^0, c^0, \widetilde{c}_1^0, u^0, v^0, w^0, \widetilde{u}_1^0$ ont la même signification que précédemment; où, de plus, on désigne respectivement par a_*^0 et $\overline{a}_*^0$ les points $(\xi_*^0, 0, 1)$ et $(\overline{\xi}_*^0, 0, 1)$; par u_*^0 et $\overline{u}_*^0$ des points génériques, sur le corps $k^0(\xi_*^0)$ des droites $X = \xi_*^0 Z$ et $X = \overline{\xi}_*^0 Z$ respectivement.

Les sommets de A_*^0 sont alors les points :

$$s_0^0 = {}_{12}s_0^0 = {}_1C_0^0 \cap {}_2C_1^0 \quad = a^0 \times b^0 \times a^0 \times b^0 \times \ldots\ldots\ldots \times b^0 \times a^0 \times b^0$$
$$s_1^0 = {}_{12}s_1^0 = {}_1C_1^0 \cap {}_2C_1^0 \quad = \widetilde{c}_1^0 \times b^0 \times a^0 \times b^0 \times \ldots\ldots\ldots \times b^0 \times a^0 \times b^0$$
$$s_2^0 = {}_{12}s_2^0 = {}_1C_2^0 \cap {}_2C_{m+1}^0 = c^0 \times c^0 \times c^0 \times \ldots\ldots\ldots\ldots\ldots \times c^0 \times a^0 \times b^0$$
$$s_3^0 = {}_{12}s_3^0 = {}_1C_3^0 \cap {}_2C_{m+1}^0 = c^0 \times c^0 \times c^0 \times \ldots\ldots\ldots\ldots\ldots \times c^0 \times \overline{a}_*^0 \times b^0$$

et, pour tout i tel que $1 \leqslant i \leqslant n$

$$\overline{s}_{2i-1}^0 = {}_{22}s_{2i-1}^0 = {}_2C_{2i-1}^0 \cap {}_2C_{2i}^0 = c^0 \times c^0 \times \ldots \times c^0 \times b^0 \times a^0 \times b^0 \times \ldots \times b^0 \times a^0 \times b^0$$
$$\overline{s}_{2i}^0 \quad = {}_{22}s_{2i}^0 \quad = {}_2C_{2i}^0 \cap {}_2C_{2i+1}^0 = c^0 \times c^0 \times \ldots \times c^0 \times c^0 \times a^0 \times b^0 \times \ldots \times b^0 \times a^0 \times b^0$$

Quelle que soit la parité de m, les composantes de A_*^0 sont connectées comme l'indique la figure suivante :

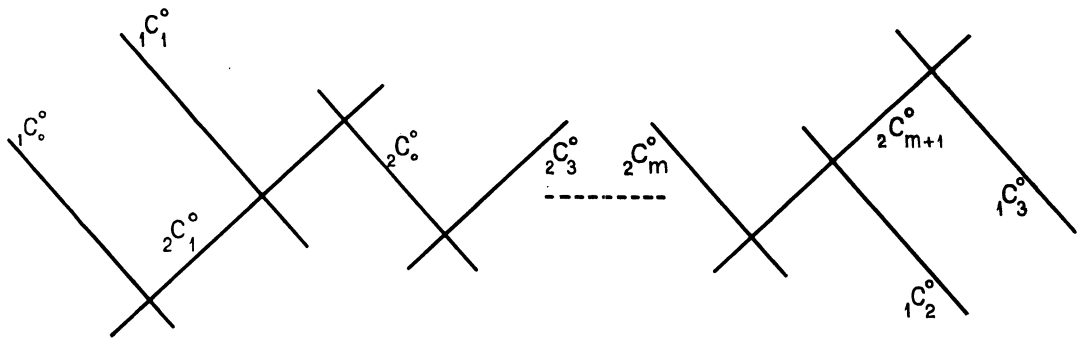


FIG. 7

Les composantes ${}_1C_i^0$ $(i = 0, 1, 2, 3)$ sont simples, tandis que les ${}_2C_j^0$ $(1 \leqslant j \leqslant m+1)$ sont doubles. La remarque 1 du n° 9 permet de vérifier que tout point de A_*^0 autre qu'un sommet est p-simple sur A_*; de même, le sommet s_0^0 est p-simple sur A_*, puisque a^0 est p-simple sur A_1.

Vérifions la p-simplicité des autres sommets.

p-simplicité de s_1^0. — Il suffit de montrer, d'après la remarque 2 du n° 9, que l'anneau local $\mathfrak{o}_1 = \mathfrak{o}(\widetilde{c}_1^0 \times b^0, A_{12})$ est régulier. Or l'idéal maximal $\mathfrak{m}_1$ de cet anneau est engendré par ξ_1, η_1, ξ_2, ζ_2 et t, où ξ_1, η_1, ξ_2, ζ_2 sont les fonctions sur A_{12} respectivement induites par $(X_1/Z_1) - \alpha_1$, Y_1/Z_1, X_2/Y_2, Z_2/Y_2. Ces générateurs sont liés par les relations $\xi_2 = \zeta_2(\alpha_1 + \xi_1)$ et $t = \eta_1\zeta_2$. En portant dans l'équation de A_1, on obtient $\eta_1 \equiv \xi_1\zeta_2$ (mod. $\mathfrak{m}_1^3$). L'idéal $\mathfrak{m}_1$ est donc bien engendré par deux éléments : ξ_1 et ζ_2.

p-simplicité de s_2^0 *et* s_3^0. — Montrons par exemple que s_2^0 est p-simple sur A_*^0. Pour m impair $(m = 2n-1)$, il suffit de montrer que l'anneau local $\mathfrak{o}_2 = \mathfrak{o}(b_*^0 \times a^0, A_{m+1,m+2})$ est régulier. L'idéal maximal $\mathfrak{m}_2$ de cet anneau est engendré par $\xi_{m+1}, \eta_{m+1}, \eta_{m+2}, \zeta_{m+2}$ et t, où $\xi_{m+1}, \eta_{m+1}, \eta_{m+2}$ et ζ_{m+2} sont induites respectivement par X_{m+1}/Z_{m+1}, $(Y_{m+1}/Z_{m+1}) - \eta_*$,

Y_{m+2}/X_{m+2} et Z_{m+2}/X_{m+2} (η_* étant un élément de $\mathfrak{R}$ tel que $\eta_*^0 = \rho(\eta_*)$). On a les relations $\eta_{m+2} = \xi_{m+2}(\eta_* + \eta_{m+1})$ et $t = \xi_{m+1}\zeta_{m+2}$. En portant dans l'équation de A_{m+2}, on obtient $\alpha_1\xi_{m+1} \equiv (2\eta_* + \mu_n)\eta_{m+1}\xi_{m+2}$ (mod. $\mathfrak{m}_2^3$). Comme on a $2\eta_*^0 + \mu_n^0 \neq 0$, l'idéal $\mathfrak{m}_2$ admet pour générateurs η_{m+1} et ξ_{m+2}.

Pour m pair ($m = 2n$), il suffit de montrer que l'anneau local $\mathfrak{o}_2' = \mathfrak{o}(a_*^0 \times b^0, A_{m+1,m+2})$ est régulier. L'idéal maximal $\mathfrak{m}_2'$ de cet anneau est engendré par ξ'_{m+1}, η'_{m+1}, ξ'_{m+2}, ζ'_{m+2} et t, où les quatre premières fonctions sont induites respectivement par $(X_{m+1}/Z_{m+1}) - \xi_*$, Y_{m+1}/Z_{m+1}, X_{m+2}/Y_{m+2} et Z_{m+2}/Y_{m+2} (ξ_* étant un élément de $\mathfrak{R}$ tel que $\xi_*^0 = \rho(\xi_*)$). On a les relations $\xi'_{m+2} = (\xi_* + \xi'_{m+1})\zeta'_{m+2}$, et $t = \eta'_{m+1}\zeta'_{m+2}$. En portant dans l'équation de A_{m+2}, on obtient $\eta'_{m+1} \equiv (2\alpha_1\xi_* + \beta_{n+2})\xi'_{m+1}\zeta'_{m+2}$ (mod. $\mathfrak{m}_2'^3$). Donc $\mathfrak{m}_2'$ est engendré par ξ'_{m+1} et ζ'_{m+2}.

p-*simplicité de* $\bar{s}_{2i-1}^0$. — Il suffit de vérifier que l'anneau local $\bar{\mathfrak{o}}_{2i-1} = \mathfrak{o}(c^0 \times b^0, A_{2i-1,2i})$ est régulier. Or l'idéal maximal $\overline{\mathfrak{m}}_{2i-1}$ de cet anneau est engendré par t, et par les fonctions ξ_{2i-1}, η_{2i-1}, ξ_{2i}, ζ_{2i} respectivement induites par X_{2i-1}/Z_{2i-1}, Y_{2i-1}/Z_{2i-1}, X_{2i}/Y_{2i} et Z_{2i}/Y_{2i}. Ces fonctions sont liées par les relations $\xi_{2i} = \xi_{2i-1}\zeta_{2i}$, et $t = \eta_{2i-1}\zeta_{2i}$. En portant dans l'équation de A_{2i-1}, on obtient $\eta_{2i-1} \equiv \zeta_{2i}\xi_{2i-1}^2$ (mod. $\overline{\mathfrak{m}}_{2i-1}^4$). Donc $\overline{\mathfrak{m}}_{2i-1}$ est engendré par ξ_{2i-1} et ζ_{2i}.

p-*simplicité de* $\bar{s}_{2i}^0$. — Il suffit de vérifier que l'anneau local $\bar{\mathfrak{o}}_{2i} = \mathfrak{o}(c^0 \times a^0, A_{2i,2i+1})$ est régulier. Or l'idéal maximal $\overline{\mathfrak{m}}_{2i}$ de cet anneau est engendré par t, et par les fonctions ξ'_{2i}, η_{2i}, η_{2i+1}, ζ_{2i+1} respectivement induites par X_{2i}/Z_{2i}, Y_{2i}/Z_{2i}, Y_{2i+1}/X_{2i+1} et Z_{2i+1}/X_{2i+1}. On a les relations $\eta_{2i+1} = \eta_{2i}\zeta_{2i+1}$ et $t = \xi'_{2i}\zeta_{2i+1}$. En portant dans l'équation de A_{2i}, on obtient $\alpha_1\xi'_{2i} \equiv \eta_{2i}^2\zeta_{2i+1}$ (mod. $\overline{\mathfrak{m}}_{2i}^4$). Donc $\overline{\mathfrak{m}}_{2i}$ est engendré par η_{2i} et ζ_{2i+1}.

On a donc complètement démontré que A_* est p-simple. En appliquant la proposition 2 du n° 3 à chacune des courbes A_j, on voit que l'entier $\nu(C_{jl}^0, \omega_j, A_j)$ s'annule pour toute composante C_{jl}^0 de A_j^0. En remontant aux composantes correspondantes de A_*^0, on en déduit, compte tenu de la proposition 15 du n° 16, que l'entier ν s'annule sur toutes les composantes de A_*^0. Donc, d'après la proposition 1 du n° 2, A_* est p-minimale.

Comme dans le cas (c 4), le groupe $\mathscr{G}_{p0}(A)$ est k^0-isomorphe à $\mathbf{G}_a$, et le groupe fini $\Gamma = \Gamma(A)$ est *d'ordre 4*. Si on pose ${}_1\mathscr{S}_i^0 = \mathscr{S}(A_*^0) \cap {}_1C_i^0$ ($i = 0, 1, 2, 3$), on voit, en appliquant à la courbe $A_h = A_{m+2}$, le lemme 1 du n° 3, que le k-morphisme $\beta_* : A_* \times A_* \to A_*$, défini par $\beta_*(x, y) = -(x + y)$ applique ${}_1\mathscr{S}_1^0 \times {}_1\mathscr{S}_2^0$ sur ${}_1\mathscr{S}_3^0$ ou sur ${}_1\mathscr{S}_0^0$ suivant que m est pair ou impair. Pour *m pair*, les trois éléments non nuls de Γ ont pour somme 0, donc Γ est *non cyclique*. Pour *m impair*, il existe deux éléments non nuls distincts de Γ ayant pour somme 0, donc Γ est *cyclique*.

13. Démonstration du théorème 1 (cas (c 6)).

$$(v(\mu) \geqslant 2 \qquad v(\alpha) \geqslant 2 \qquad v(\beta) \geqslant 3 \qquad v(\gamma) \geqslant 4 \qquad v(\overline{\gamma}) = 4)$$

On note, comme dans le cas précédent, A_1, A_2 et A_3 les transformées de A par σ_1, $\overline{\sigma}_2$, $\overline{\sigma}_3$, et φ_1, φ_2, φ_3 les k-isomorphismes $A \to A_1$, $A \to A_2$, $A \to A_3$ induits respectivement par $\overline{\sigma}_1$, $\overline{\sigma}_2$, $\overline{\sigma}_3$. Les images $u_j = \varphi_j(u)$ ($j = 1, 2, 3$) d'un point générique u de A sur k sont donc

$u_1=(x, y, tz)$, $u_2=(tx, y, t^2z)$ et $u_3=(x, y, t^2z)$. On considère, d'autre part, la courbe A_4 lieu sur k du point $u_4=(x^2, tyz, t^3z^2)$. On prend pour (A_*, θ) le joint des quatre modèles (A_1, φ_1), (A_2, φ_2), (A_3, φ_3), (A_4, φ_4). Les équations respectives de A_1, A_2, A_3, A_4 sont :

$$\begin{aligned}
A_1|\ & Y^2Z+t\lambda_1XYZ+t\mu_2YZ^2 &&= tX^3+t^2\alpha_2X^2Z+t^2\beta_3XZ^2+t^2\gamma_4Z^3\\
A_2|\ & tY^2Z+t\lambda_1XYZ+t\mu_2YZ^2 &&= X^3+t\alpha_2X^2Z+t\beta_3XZ^2+t\gamma_4Z^3\\
A_3|\ & Y^2Z+t\lambda_1XYZ+\mu_2YZ^2 &&= t^2X^3+t^2\alpha_2X^2Z+t\beta_3XZ^2+\gamma_4Z^3\\
A_4|\ & (Y^2+\mu_2YZ-t\alpha_2XZ-\gamma_4Z^2)^2 &&= tX^2Z(-\lambda_1Y+X+\beta_3Z)
\end{aligned}$$

Les cycles réduits A_1^0 et A_2^0 ont respectivement pour équations $Y^2Z=0$ et $X^3=0$. Le cycle réduit A_3^0 a pour équation $Z(Y^2+\mu_2^0YZ+\gamma_4^0Z^2)=0$. Il se décompose en les trois droites $Z=0$, $Y=\eta_0^0Z$, et $Y=\overline{\eta}_0^0Z$, où η_0^0 et $\overline{\eta}_0^0$ sont les racines (distinctes, puisque $v(\delta')=4$) du polynôme $Y^2+\mu_2^0Y-\gamma_4^0=0$. Le cycle réduit A_4^0 a pour équation $(Y^2+\mu_2^0YZ-\gamma_4^0Z^2)^2=0$. Il se décompose en les deux droites (doubles) $Y=\eta_0^0Z$, et $Y=\overline{\eta}_0^0Z$. Le tableau suivant donne les composantes de A_*^0.

Composantes	Points génériques
${}_1C_0^0$	$w^0\times b^0\times w^0\times a^0$
${}_2C_0^0$	$v^0\times b^0\times a^0\times a^0$
${}_1C_1^0$	$c^0\times b_1^0\times v_1^0\times b_1^0$
${}_2C_1^0$	$c^0\times b_1^0\times a^0\times v_1^0$
${}_1C_2^0$	$c^0\times \overline{b}_1^0\times \overline{v}_1^0\times \overline{b}_1^0$
${}_2C_2^0$	$c^0\times \overline{b}_1^0\times a^0\times \overline{v}_1^0$
${}_3C^0$	$c^0\times u^0\times a^0\times a^0$

où a^0, b^0, c^0, b_1^0, $\overline{b}_1^0$ désignent respectivement les points $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, $(0, \eta_0^0, 1)$, $(0, \overline{\eta}_0^0, 1)$; u^0, v^0, w^0 des points génériques sur k^0 des droites $X=0$, $Y=0$, $Z=0$ respectivement; v_1^0 et $\overline{v}_1^0$ des points génériques sur $k^0(\eta_0^0)$ des droites $Y=\eta_0^0Z$ et $Y=\overline{\eta}_0^0Z$ respectivement.

Les sommets sont les points :

$$\begin{aligned}
s_0^0 &= {}_{12}s_0^0 = {}_1C_0^0\cap{}_2C_0^0 = a^0\times b^0\times a^0\times a^0\\
s_1^0 &= {}_{12}s_1^0 = {}_1C_1^0\cap{}_2C_1^0 = c^0\times b_1^0\times a^0\times b_1^0\\
s_2^0 &= {}_{12}s_2^0 = {}_1C_2^0\cap{}_2C_2^0 = c^0\times \overline{b}_1^0\times a^0\times \overline{b}_1^0\\
s_0'^0 &= {}_{23}s_0^0 = {}_2C_0^0\cap{}_3C^0 = c^0\times b^0\times a^0\times a^0\\
s_1'^0 &= {}_{23}s_1^0 = {}_2C_1^0\cap{}_3C^0 = c^0\times b_1^0\times a^0\times a^0\\
s_2'^0 &= {}_{23}s_2^0 = {}_2C_2^0\cap{}_3C^0 = c^0\times \overline{b}_1^0\times a^0\times a^0
\end{aligned}$$

Les composantes de A_*^0 sont connectées comme l'indique la figure 8. Conformément aux conventions du n° 9, chacune d'elles est notée avec un indice de gauche égal à son coefficient dans A_*^0. D'après la remarque 1 du n° 9, tout point de l'une des composantes ${}_1C_i^0$ $(i=0, 1, 2)$, ${}_2C_0^0$, ${}_3C^0$ autre qu'un sommet de A_*^0 est p-simple sur A_*; de même, puisque a^0 est p-simple sur A_1, le point s_0^0 est p-simple sur A_*.

Montrons qu'un point de l'une des composantes ${}_2C_1^0$, ${}_2C_2^0$ autre qu'un sommet est p-simple sur A_* (la remarque 1 du n° 9 ne suffit plus car A_4^0 possède, en général, des points p-multiples sur A_4 autres que a^0, b_1^0 ou $\bar{b}_1^0$). Soit u_0^0 un tel point. Supposons, par exemple, qu'on ait $u_0^0 \in {}_2C_1^0$. Ce point est de la forme $u_0^0 = c^0 \times b_1^0 \times a^0 \times v_0^0$, où $v_0^0 \in \mathbf{P}_2^0$ et

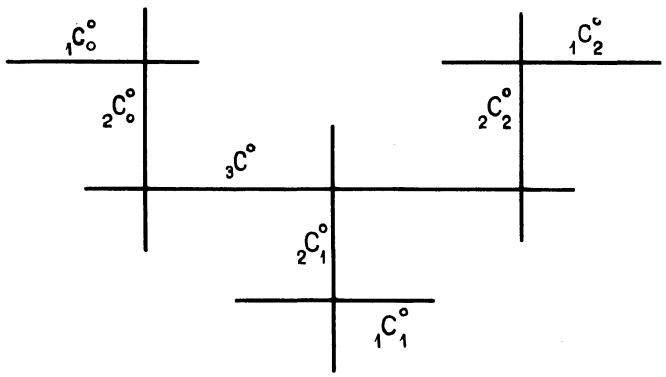


FIG. 8

on a $v_0^0 = (\xi_0^0, \eta_0^0, 1)$ avec $\xi_0^0 \neq 0$. Soient ξ_0 et η_0 des éléments de $\mathfrak{R}$ tels que $\xi_0^0 = \rho(\xi_0)$ et $\eta_0^0 = \rho(\eta_0)$. Il suffit (n° 9, remarque 2) de vérifier que l'anneau local $\mathfrak{o}_0 = \mathfrak{o}(a^0 \times v_0^0, A_{34})$ est régulier. Or son idéal maximal $\mathfrak{m}_0$ est engendré par t, et par les fonctions η_3, ζ_3, ξ_4, η_4 respectivement induites par Y_3/X_3, Z_3/X_3, $(X_4/Z_4) - \xi_0$, $(Y_4/Z_4) - \eta_0$. Ces générateurs sont liés par les relations $\eta_3 = \zeta_3(\eta_0 + \eta_4)$ et $t = \zeta_3^2(\xi_0 + \xi_4)$. En portant dans l'équation de A_3, on obtient une relation de la forme $(2\eta_0 + \mu_2)\eta_4 \equiv a\xi_4 + b\zeta_3 \pmod{\mathfrak{m}_0^2}$, avec a et $b \in \mathfrak{R}$. Comme on a $2\eta_0^0 + \mu_2^0 \neq 0$, l'idéal $\mathfrak{m}_0$ admet pour générateurs ξ_4 et ζ_3. Donc $\mathfrak{o}_0$ est bien régulier.

Il reste à prouver la p-simplicité des points s_1^0, s_2^0, $s_0'^0$, $s_1'^0$, $s_2'^0$.

p-simplicité de s_1^0 et s_2^0. — Pour montrer, par exemple que s_1^0 est p-simple sur A_*, il suffit de vérifier la régularité de l'anneau local $\mathfrak{o}_1 = \mathfrak{o}(a^0 \times b_1^0, A_{34})$. L'idéal maximal $\mathfrak{m}_1$ de cet anneau est engendré par t, et par les fonctions η_3, ζ_3, ξ_4, η_4 induites respectivement par Y_3/X_3, Z_3/X_3, X_4/Z_4 et $(Y_4/Z_4) - \eta_0$. Ces générateurs sont liés par les relations $\eta_3 = \zeta_3(\eta_0 + \eta_4)$ et $t = \zeta_3^2\xi_4$. En portant dans l'équation de A_3, on trouve $(2\eta_0 + \mu_2)\eta_4 \equiv \zeta_3\xi_4 \pmod{\mathfrak{m}^3}$. Comme on a $2\eta_0^0 + \mu_2^0 \neq 0$, l'idéal $\mathfrak{m}_1$ est engendré par ζ_3 et ξ_4.

p-simplicité de $s_0'^0$. — Il suffit de vérifier la régularité de l'anneau local $\mathfrak{o}_0' = \mathfrak{o}(c^0 \times b^0, A_{12})$. L'idéal maximal $\mathfrak{m}_0'$ de cet anneau est engendré par t, et par les fonctions ξ_1, η_1, ξ_2, ζ_2 respectivement induites par X_1/Z_1, Y_1/Z_1, X_2/Y_2 et Z_2/Y_2. On a $\xi_2 = \xi_1\zeta_2$, et $t = \eta_1\zeta_2$. En portant dans l'équation de A_1, on trouve $\eta_1 \equiv \zeta_2\xi_1^3 \pmod{\mathfrak{m}_0'^5}$. Donc $\mathfrak{m}_0'$ est engendré par ξ_1 et ζ_2.

p-simplicité de $s_1'^0$ et $s_2'^0$. — Pour montrer, par exemple, que $s_1'^0$ est p-simple sur A_*, il suffit de vérifier la régularité de l'anneau local $\mathfrak{o}_1' = \mathfrak{o}(b_1^0 \times a^0, A_{24})$. L'idéal maximal $\mathfrak{m}_1'$ de cet anneau est engendré par t et par les fonctions ξ_2', η_2, η_4', ζ_4 respectivement induites par X_2/Z_2, $(Y_2/Z_2) - \eta_0$, Y_4/X_4 et Z_4/X_4. On a les relations $\eta_4' = \zeta_4(\eta_0 + \eta_2)$ et $t = \zeta_4 \xi_2'^2$. En portant dans l'équation de A_4, on obtient $\xi_2' \equiv (2\eta_0 + \mu_2)\zeta_4 \eta_2 \pmod{\mathfrak{m}_1'^3}$. Donc $\mathfrak{m}_1'$ est engendré par η_2 et ζ_4.

On a donc démontré la p-simplicité de A_*. D'après la proposition 2 du n° 3, et compte tenu de l'expression de la différentielle invariante ω, on voit que ω_* ne s'annule sur aucune des composantes ${}_1C_i^0$ $(i = 0, 1, 2)$, ${}_2C_0^0$ et ${}_3C^0$ de A_*^0. Il reste à vérifier que ω_* ne s'annule sur aucune des autres composantes. Montrons, par exemple, que ω_* ne s'annule pas en s_1^0 (ni, par conséquent, *a fortiori*, sur ${}_1C_0^0$). Cela revient à montrer que la différentielle ω_{34} sur A_{34} transposée de ω ne s'annule pas en $a^0 \times b_1^0$. Utilisons les mêmes paramètres η_3, ζ_3, ξ_4, η_4 que dans la démonstration de la p-simplicité de s_1^0, respectivement induits par $\overline{\eta}_3 = Y_3/X_3$, $\overline{\zeta}_3 = Z_3/X_3$, $\overline{\xi}_4 = X_4/Z_4$, $\overline{\eta}_4 = (Y_4/Z_4) - \eta_0$. Notons $\overline{\mathfrak{m}}_1$ l'idéal maximal de l'anneau local $\overline{\mathfrak{o}}_1 = \mathfrak{o}(a^0 \times b_1^0, \mathbf{P}_2 \times \mathbf{P}_2)$. D'après les calculs précédents, parmi les éléments de $\overline{\mathfrak{o}}_1$ qui s'annulent sur A_{34} figurent $f_1 = t - \overline{\zeta}_3^2 \overline{\xi}_4$, $f_2 = \overline{\eta}_3 - (\eta_0 + \overline{\eta}_4)\overline{\zeta}_3$, et une fonction de la forme $f_3 = (2\eta_0 + \mu_2)\overline{\eta}_4 - \overline{\zeta}_3 \overline{\xi}_4 + g_3$, avec $g_3 \in \overline{\mathfrak{m}}_1^3$. Les p-différentielles de f_1, f_2, f_3 en $a^0 \times b_1^0$ sont linéairement indépendantes. D'autre part, ω_{34} est induite par la différentielle $\overline{\omega}_{34} = -d\overline{\zeta}_3/(2\overline{\eta}_3\overline{\zeta}_3 + t\lambda_1\overline{\zeta}_3 + \mu_2\overline{\zeta}_3^2)$ sur $\mathbf{P}_2 \times \mathbf{P}_2$. La différentielle

$$\theta_{34} = \overline{\omega}_{34} \wedge df_1 \wedge df_2 \wedge df_3$$

est de la forme $d\overline{\zeta}_3 \wedge d\overline{\xi}_4 \wedge d\overline{\eta}_3 \wedge d\overline{\eta}_4(1 + g)$, avec $g \in \overline{\mathfrak{m}}_1$, donc θ_{34} est p-morphique et non nulle en $a^0 \times b_1^0$; il en est donc de même de ω_{34}, d'après les définitions du n° 13 du chapitre I^er^. On a donc bien démontré la p-minimalité de A_*.

Le groupe $\mathscr{G}_{p0}(A)$ est encore isomorphe à $\mathbf{G}_a$ sur le corps k^0 et le groupe fini $\Gamma = \Gamma(A)$ est d'ordre 3.

14. Démonstration du théorème 1 (cas (c 7)).

$$(v(\mu) \geqslant 3, \qquad v(\alpha) \geqslant 2, \qquad v(\beta) = 3, \qquad v(\gamma) \geqslant 5)$$

On note respectivement φ_1, φ_2, φ_3, φ_4 les k-isomorphismes $\varphi_1 : A \to A_1$, $\varphi_2 : A \to A_2$, $\varphi_3 : A \to A_3$, $\varphi_4 : A \to A_4$ induits respectivement par $\overline{\sigma}_1$, $\overline{\sigma}_2$, $\overline{\sigma}_3$, $\overline{\sigma}_4$. Les images $u_j = \varphi_j(u)$ $(j = 1, 2, 3, 4)$ d'un point générique u de A sur k sont donc $u_1 = (x, y, tz)$, $u_2 = (tx, y, t^2 z)$, $u_3 = (x, y, t^2 z)$, $u_4 = (tx, y, t^3 z)$. On considère d'autre part la courbe A_5 lieu sur k du point $u_5 = \varphi_5(u) = (t^3 x^2 z, y^2 x, t^4 z^2 y)$. On prend pour (A_*, θ) le joint des modèles $(A_1, \varphi_1), \ldots, (A_5, \varphi_5)$. Les équations respectives des courbes A_1, A_2, A_3, A_4, A_5 sont

$$\begin{aligned}
A_1 &| \; Y^2Z + t\lambda_1 XYZ + t^2\mu_3 YZ^2 = tX^3 + t^2\alpha_2 X^2 Z + t^2\beta_3 XZ^2 + t^3\gamma_5 Z^3 \\
A_2 &| \; tY^2Z + t\lambda_1 XYZ + t^2\mu_3 YZ^2 = X^3 + t\alpha_2 X^2 Z + t\beta_3 XZ^2 + t^2\gamma_5 Z^3 \\
A_3 &| \; Y^2Z + t\lambda_1 XYZ + t\mu_3 YZ^2 = t^2 X^3 + t^2\alpha_2 X^2 Z + t\beta_3 XZ^2 + t\gamma_5 Z^3 \\
A_4 &| \; tY^2Z + t\lambda_1 XYZ + t\mu_3 YZ^2 = tX^3 + t\alpha_2 X^2 Z + \beta_3 XZ^2 + \gamma_5 Z^3 \\
A_5 &| \; Y(\beta_3 X - Y)^3 Z^4 + tX^2(XY + \gamma_5 Z^2 - \lambda YZ)^3 + t^2 XY^2 Z^2(\alpha_2 X - \mu_3 Z)^3 - \\
&\qquad - 6tXYZ^2(\alpha_2 X - \mu_3 Z)(\beta_3 X - Y)(X^2 + \gamma_5 Z^2 - \lambda_1 YZ) = 0
\end{aligned}$$

Les cycles réduits A_1^0, A_2^0, A_3^0, A_4^0 et A_5^0 ont respectivement pour équations $Y^2Z=0$, $X^3=0$, $Y^2Z=0$, $Z^2(\beta_3^0X+\gamma_5^0Z)=0$ et $Y(\beta_3^0X-Y)^3Z^4=0$.

Les composantes de A_* sont données par le tableau suivant.

Composantes	Points génériques
${}_1C_0^0$	$w^0\times b^0\times w^0\times b^0\times b^0$
${}_2C_0^0$	$v^0\times b^0\times a^0\times b^0\times b^0$
${}_3C_0^0$	$c^0\times u^0\times a^0\times b^0\times b^0$
${}_4C^0$	$c^0\times c^0\times a^0\times b^0\times w^0$
${}_2C^0$	$c^0\times c^0\times a^0\times w^0\times a^0$
${}_3C_1^0$	$c^0\times c^0\times a^0\times b^0\times\widetilde{w}^0$
${}_2C_1^0$	$c^0\times c^0\times v^0\times b^0\times c^0$
${}_1C_1^0$	$c^0\times c^0\times\widetilde{a}^0\times\widetilde{u}^0\times v^0$

où l'on désigne respectivement par a^0, b^0, c^0, $\widetilde{a}^0$, les points (1, 0, 0) (0, 1, 0), (0, 0, 1), $(-\gamma_5^0, 0, \beta_3^0)$; par u^0, v^0, w^0 et $\widetilde{w}^0$ des points génériques sur k^0 des droites $X=0$, $Y=0$, $Z=0$, et $\beta_3^0X-Y=0$ respectivement, et, en notant $(x^0, 0, z^0)$ les coordonnées de v^0, par $\widetilde{u}^0$ le point (générique sur k^0) de la droite $\beta_3^0X+\gamma_5^0Z=0$ ayant pour coordonnées $-\beta_3^0\gamma_5^0x^0$, $(\gamma_5^0)^2z^0$, $(\beta_3^0)^2x^0$.

Les sommets sont les points :

$$
\begin{aligned}
{}_{12}s_0^0 &= {}_1C_0^0\cap{}_2C_0^0 = a^0\times b^0\times a^0\times b^0\times b^0\\
{}_{23}s_0^0 &= {}_2C_0^0\cap{}_3C_0^0 = c^0\times b^0\times a^0\times b^0\times b^0\\
{}_{34}s_0^0 &= {}_3C_0^0\cap{}_4C^0 = c^0\times c^0\times a^0\times b^0\times b^0\\
{}_{24}s_0^0 &= {}_2C^0\cap{}_4C^0 = c^0\times c^0\times a^0\times b^0\times a^0\\
{}_{34}s_1^0 &= {}_3C_1^0\cap{}_4C^0 = c^0\times c^0\times a^0\times b^0\times\widetilde{c}^0\\
{}_{23}s_1^0 &= {}_2C_1^0\cap{}_3C_1^0 = c^0\times c^0\times a^0\times b^0\times c^0\\
{}_{12}s_1^0 &= {}_1C_1^0\cap{}_2C_1^0 = c^0\times c^0\times\widetilde{a}^0\times b^0\times c^0
\end{aligned}
$$

où $\widetilde{c}^0$ est le point $(1, \beta_3^0, 0)$.

Les composantes de A_*^0 sont connectées comme l'indique la figure ci-contre (fig. 9).

La remarque 1 du n° 9 permet de voir que tout point de l'une des composantes ${}_1C_0^0$, ${}_2C_0^0$, ${}_3C_0^0$, ${}_4C^0$, ${}_2C^0$, ${}_2C_1^0$, ${}_1C_1^0$, autre qu'un sommet est p-simple sur A_*; elle permet de voir également que les points ${}_{12}s_0^0$, ${}_{34}s^0$ sont p-simples sur A_*.

Montrons que tout point de ${}_3C_1^0$ autre que l'un des sommets ${}_{34}s_1^0$, ${}_{23}s_1^0$ est simple sur A_* (la remarque 1 ne suffit plus, car la composante $\beta_3^0 X = Y$ de A_5^0 peut posséder des points p-multiples sur A_5, autres que c^0). Un tel point est de la forme $c^0 \times c^0 \times a^0 \times b^0 \times w_0^0$, où w_0^0 est un point de $\mathbf{P}_2^0$ qui est lui-même de la forme $w_0^0 = (1, \beta_3^0, \zeta_0^0)$, avec $\zeta_0^0 \neq 0$. Soit $\zeta_0 \in \mathfrak{R}$, tel que $\zeta_0^0 = \rho(\zeta_0)$. Il suffit, d'après la remarque 2 du n° 9, de vérifier la régularité de l'anneau local $\mathfrak{o}_0 = \mathfrak{o}(v^0 \times w_0^0, A_{45})$. Or, l'idéal maximal $\mathfrak{m}_0$ de cet anneau est engendré par t, et par les fonctions ξ_4, ζ_4, η_5, ζ_5', induites respectivement par X_4/Y_4, Z_4/Y_4, $(Y_5/X_5) - \beta_3$ et $(Z_5/X_5) - \zeta_0$. Ces générateurs sont liés par les relations $\zeta_4 = \xi_4^2(\zeta_0 + \zeta_5')$, et $t = \xi_4\zeta_4(\beta_3 + \eta_5)$. On en déduit, en portant dans l'équation de A_4, $\beta_3\xi_4 \equiv \zeta_0\eta_5 \pmod{\mathfrak{m}_0^2}$ ce qui montre que $\mathfrak{m}_0$ est engendré par deux éléments : ξ_4 (ou η_5) et ζ_5'.

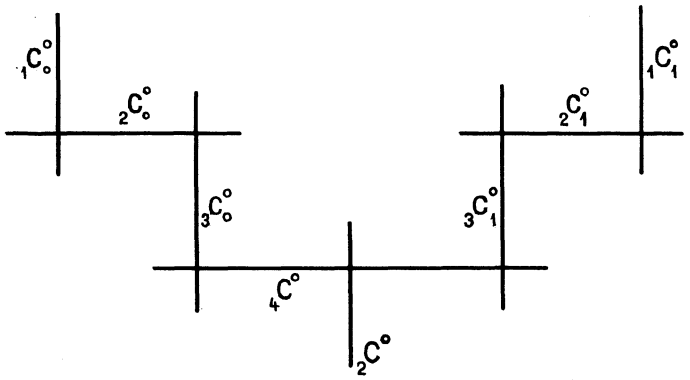


FIG. 9

Le calcul fait dans le cas (c 6) pour établir la p-simplicité du point ${}_{23}s_0^0$ est encore valable. Il reste à vérifier la p-simplicité des points ${}_{34}s_0^0$, ${}_{24}s^0$, ${}_{23}s_1^0$ et ${}_{12}s_1^0$.

p-simplicité de ${}_{34}s_0^0$. — Il suffit de vérifier la régularité de l'anneau local ${}_{34}\mathfrak{o}_0 = \mathfrak{o}(c^0 \times b^0, A_{25})$. L'idéal maximal ${}_{34}\mathfrak{m}_0$ de cet anneau est engendré par t, et par les fonctions ξ_2, η_2, ξ_5, ζ_5, respectivement induites par X_2/Z_2, Y_2/Z_2, X_5/Y_5, Z_5/Y_5. On a les relations $\xi_2 = \xi_5\eta_2^2$, et $t = \eta_2\xi_2\zeta_5$. En portant dans l'équation de A_2, on obtient $\zeta_5 \equiv \xi_5^2\eta_2 \pmod{{}_{34}\mathfrak{m}_0^4}$. L'idéal ${}_{34}\mathfrak{m}_0$ est donc engendré par ξ_5 et η_2.

p-simplicité de ${}_{24}s^0$. — Il suffit de vérifier la régularité de l'anneau local ${}_{24}\mathfrak{o} = \mathfrak{o}(b^0 \times a^0, A_{45})$. L'idéal maximal ${}_{24}\mathfrak{m}$ de cet anneau est engendré par t, et par les fonctions ξ_4, ζ_4, η_5', ζ_5, respectivement induites par X_4/Y_4, Z_4/Y_4, Y_5/X_5, Z_5/X_5. On a les relations $\zeta_4 = \xi_4^2\zeta_5$, et $t = \xi_4^3\eta_5'\zeta_5$. En portant dans l'équation de A_4, on obtient $\beta_3\zeta_5 \equiv \xi_4\eta_5' \pmod{{}_{24}\mathfrak{m}^2}$. Comme on a $\beta_3^0 \neq 0$ (d'après (c 7)) l'idéal ${}_{24}\mathfrak{m}$ est engendré par ξ_4 et η_5'.

p-simplicité de ${}_{23}s_1^0$. — Il suffit de vérifier la régularité de ${}_{23}\mathfrak{o}_1 = \mathfrak{o}(a^0 \times c^0, A_{35})$. L'idéal maximal ${}_{23}\mathfrak{m}_1$ de cet anneau est engendré par t, et par les fonctions η_3, ζ_3, ξ_5, η_5'', respectivement induites par Y_3/X_3, Z_3/X_3, X_5/Z_5, Y_5/Z_5. On a $\eta_3 = \zeta_3^2\eta_5''$, et $t = \eta_3\zeta_3\xi_5$. En portant dans l'équation de A_3, on obtient $\eta_5'' \equiv \beta_3\xi_5 \pmod{{}_{23}\mathfrak{m}_1^2}$, d'où l'on déduit que ${}_{23}\mathfrak{m}_1$ est engendré par ζ_3 et ξ_5.

p-simplicité de ${}_{12}s_1^0$. — Il suffit de vérifier la régularité de ${}_{12}\mathfrak{o}_1 = \mathfrak{o}(\widetilde{a}^0 \times b^0, A_{34})$. L'idéal maximal ${}_{12}\mathfrak{m}_1$ de cet anneau est engendré par t, et par les fonctions ξ_3, η_3', ξ_4, ζ_4 induites respectivement par $(X_3/Z_3) - \widetilde{\xi}_0$ (en posant $\widetilde{\xi}_0 = -\gamma_5/\beta_3$), Y_3/Z_3, X_4/Y_4, Z_4/Y_4. On a $\xi_4 = \zeta_4(\widetilde{\xi}_0 + \xi_3)$ et $t = \eta_3'\zeta_4$. En portant dans l'équation de A_3, on obtient $\eta_3' = \beta_3\xi_3\zeta_4 \pmod{{}_{12}\mathfrak{m}_1^3}$. Donc l'idéal ${}_{12}\mathfrak{m}_1$ est engendré par ξ_3 et ζ_4.

On a donc terminé la démonstration de la p-simplicité de A_*. D'après la proposition 2 du n° 3, et compte tenu de l'expression de la différentielle ω, on voit que ω_* ne s'annule sur aucune des composantes ${}_1C_0^0$, ${}_2C_0^0$, ${}_3C_0^0$, ${}_2C^0$, ${}_2C_1^0$, ${}_1C_1^0$ de A_*^0. Pour montrer que ω_* ne s'annule sur aucune des deux autres composantes, il nous suffit de vérifier que ω_* ne s'annule pas en ${}_{34}s_1^0$, i.e. que la différentielle ω_5 sur A_5 transposée de ω est p-morphique et non nulle au point $\widetilde{c}^0$ $(1, \beta_3^0, 0)$.

Or, en posant $\overline{\eta}_5 = (Y_5/X_5) - \beta_3$, $\overline{\zeta}_5 = Z_5/X_5$, et $\overline{\mathfrak{m}}_5 = \mathfrak{m}(\widetilde{c}^0, \mathbf{P}_2)$, on trouve que ω_5 est induite par $\overline{\omega}_5 = \overline{\omega}_5'/\overline{\eta}_5^3\overline{\zeta}_5^4$, où $\overline{\omega}_5'$ est un élément de $D^1(\widetilde{c}^0, \mathbf{P}_2)$ (i.e. une différentielle sur $\mathbf{P}_2$, p-morphique en $\widetilde{c}^0$), tel qu'on ait $\omega_5' \equiv \beta_3^2(\overline{\eta}_5 d\overline{\xi}_5 - \overline{\zeta}_5 d\overline{\eta}_5) \pmod{\overline{\mathfrak{m}}_5^2 D^1(\widetilde{c}^0, \mathbf{P}_2)}$. D'après l'équation de A_5, il existe, d'autre part, une fonction f sur $\mathbf{P}_2$, p-morphique en $\widetilde{c}^0$ s'annulant sur A_5 de la forme $f = \beta_3^2 t - \overline{\eta}_5^3\overline{\zeta}_5^4(1+g)$, avec $g \in \overline{\mathfrak{m}}_5$. On en tire $\overline{\omega}_5 \wedge df = -\beta_3^2 d\overline{\eta}_5 \wedge d\overline{\zeta}_5(1+h)$, avec $h \in \overline{\mathfrak{m}}_5$. Donc $\theta_5 = \overline{\omega}_5 \wedge df$ est p-morphique et non nulle en $\widetilde{c}^0$. Comme, d'autre part, la p-différentielle de f en $\widetilde{c}^0$ n'est pas nulle, ω_5 est p-morphique et non nulle en $\widetilde{c}^0$.

Donc, notre modèle (A_*, θ) est bien p-simple p-minimal. Le groupe $\mathscr{G}_{p0}(A)$ est encore isomorphe à $\mathbf{G}_a$ sur le corps k^0, et le groupe fini $\Gamma = \Gamma(A)$ est d'ordre 2.

15. Démonstration du théorème 1 (cas (c 8)).

$$(v(\mu) \geqslant 3, \qquad v(\alpha) \geqslant 2, \qquad v(\beta) \geqslant 4, \qquad v(\gamma) = 5)$$

On considère les mêmes modèles $(A_1, \varphi_1), \ldots, (A_5, \varphi_5)$ de A que dans le cas (c 7), respectivement obtenus en prenant pour $u_j = \varphi_j(u)$ $(j = 1, 2, 3, 4, 5)$ les points $u_1 = (x, y, tz)$, $u_2 = (tx, y, t^2z)$, $u_3 = (x, y, t^2z)$, $u_4 = (tx, y, t^3z)$, $u_5 = (t^3x^2z, y^2x, t^4z^2y)$. On considère d'autre part le k-modèle (A_6, φ_6) de A obtenu en prenant pour $\varphi_6(u)$ le point $u_6 = (t^4x^3z, y^3x, t^4y^2z^2)$. Les équations respectives de A_1, A_2, A_3, A_4, A_5 sont :

$$A_1 \mid\ Y^2Z + t\lambda_1XYZ + t^2\mu_3YZ^2 = tX^3 + t^2\alpha_2X^2Z + t^3\beta_4XZ^2 + t^3\gamma_5Z^3$$
$$A_2 \mid\ tY^2Z + t\lambda_1XYZ + t^2\mu_3YZ^2 = X^3 + t\alpha_2X^2Z + t^2\beta_4XZ^2 + t^2\gamma_5Z^3$$
$$A_3 \mid\ Y^2Z + t\lambda_1XYZ + t\mu_3YZ^2 = t^2X^3 + t^2\alpha_2X^2Z + t^3\beta_4XZ^2 + t\gamma_5Z^3$$
$$A_4 \mid\ tY^2Z + t\lambda_1XYZ + t\mu_3YZ^2 = tX^3 + t\alpha_2X^2Z + t\beta_4XZ^2 + \gamma_5Z^3$$
$$A_5 \mid\ Y(t\beta_4X - Y)^3Z^4 + tX^2(XY + \gamma_5Z^2 - \lambda YZ)^3 + t^2XY^2Z^2(\alpha_2X - \mu_3Z)^3 - $$
$$- 6tXYZ^2(\alpha_2X - \mu_3Z)(t\beta_4X - Y)(X^2 + \gamma_5Z^2 - \lambda_1YZ) = 0$$

On trouve d'autre part que celle de A_6 est obtenue en annulant un polynôme P, homogène et de degré 11, de la forme

$$P(X, Y, Z) = Y^6(X - Z)^5 + t\gamma_5^5X^2Z^9 + tYP_1 + t^2P_2$$

où P_1 et P_2 appartiennent à $R[X, Y, Z]$. (On voit immédiatement, sous cette forme, que P est irréductible dans $R[X, Y, Z]$).

Les cycles réduits A_1^0, A_2^0, A_3^0, A_4^0, A_5^0, A_6^0 ont respectivement pour équations $Y^2Z = 0$, $X^3 = 0$, $Y^2Z = 0$, $Z^3 = 0$, $Y^4Z^4 = 0$, et $Y^6(X-Z)^5 = 0$.

Le tableau des composantes de A_*^0 est le suivant :

Composantes	Points génériques
${}_1C_0^0$	$w^0 \times b^0 \times w^0 \times b^0 \times b^0 \times b^0$
${}_2C_0^0$	$v^0 \times b^0 \times a^0 \times b^0 \times b^0 \times b^0$
${}_3C_0^0$	$c^0 \times u^0 \times a^0 \times b^0 \times b^0 \times b^0$
${}_4C^0$	$c^0 \times c^0 \times a^0 \times b^0 \times w^0 \times b^0$
${}_5C^0$	$c^0 \times c^0 \times a^0 \times b^0 \times a^0 \times u_1^0$
${}_6C^0$	$c^0 \times c^0 \times a^0 \times b^0 \times a^0 \times v^0$
${}_3C^0$	$c^0 \times c^0 \times a^0 \times w^0 \times a^0 \times a^0$
${}_4C_1^0$	$c^0 \times c^0 \times a^0 \times b^0 \times v^0 \times c^0$
${}_2C_1^0$	$c^0 \times c^0 \times v^0 \times b^0 \times c^0 \times c^0$

où l'on désigne respectivement par a^0, b^0, c^0 les points (1, 0, 0), (0, 1, 0), (0, 0, 1) et par u^0, v^0, w^0, u_1^0 des points génériques sur k^0 des droites $X = 0$, $Y = 0$, $Z = 0$ et $X = Z$.

Les sommets sont les points :

$$
\begin{aligned}
{}_{12}s^0 &= {}_1C_0^0 \cap {}_2C_0^0 = a^0 \times b^0 \times a^0 \times b^0 \times b^0 \times b^0 \\
{}_{23}s^0 &= {}_2C_0^0 \cap {}_3C_0^0 = c^0 \times b^0 \times a^0 \times b^0 \times b^0 \times b^0 \\
{}_{34}s^0 &= {}_3C_0^0 \cap {}_4C^0 = c^0 \times c^0 \times a^0 \times b^0 \times b^0 \times b^0 \\
{}_{45}s^0 &= {}_4C^0 \cap {}_5C^0 = c^0 \times c^0 \times a^0 \times b^0 \times a^0 \times b^0 \\
{}_{56}s^0 &= {}_5C^0 \cap {}_6C^0 = c^0 \times c^0 \times a^0 \times b^0 \times a^0 \times c_1^0 \\
{}_{36}s^0 &= {}_3C^0 \cap {}_6C^0 = c^0 \times c^0 \times a^0 \times b^0 \times a^0 \times a^0 \\
{}_{46}s^0 &= {}_4C_1^0 \cap {}_6C^0 = c^0 \times c^0 \times a^0 \times b^0 \times a^0 \times c^0 \\
{}_{24}s^0 &= {}_2C_1^0 \cap {}_4C_1^0 = c^0 \times c^0 \times a^0 \times b^0 \times c^0 \times c^0
\end{aligned}
$$

où c_1^0 est le point (1, 0, 1) de $\mathbf{P}_2$.

Les composantes de A_*^0 sont connectées comme l'indique la figure ci-après.

La remarque 1 du n° 9 permet de voir que tout point de l'une quelconque des

composantes ${}_1C_0^0$, ${}_2C_0^0$, ${}_3C_0^0$, ${}_3C^0$, ${}_2C_1^0$ autre qu'un sommet est p-simple sur A_*; elle permet de voir également que ${}_{12}s^0$ et ${}_{56}s^0$ sont p-simples.

Considérons un point de ${}_4C_0^0$ (resp. ${}_4C_1^0$) autre qu'un sommet. Un tel point est de la forme $c^0\times c^0\times a^0\times b^0\times w_0^0\times c^0$ (resp. $c^0\times c^0\times a^0\times b^0\times v_0^0\times c^0$), avec $w_0^0=(1,\eta_0^0,0)$ (resp. $v_0^0=(1,0,\zeta_0^0)$, où η_0^0 (resp. ζ_0^0) est un élément non nul de $\mathfrak{k}^0$. Soit η_0 (resp. ζ_0) un élément de $\mathfrak{R}$ tel que $\eta_0^0=\rho(\eta_0)$ (resp. $\zeta_0^0=\rho(\zeta_0)$). D'après la remarque 2 du n° 9, il suffit de montrer que le point $b^0\times w_0^0$ (resp. $b^0\times v^0$) est p-simple sur A_{45}. L'idéal maximal ${}_4\mathfrak{m}_0$ (resp. ${}_4\mathfrak{m}_1^0$) de l'anneau local de ce point sur A_{45} est engendré par t, ξ_4, ζ_4, η_5 (resp. η_5'), ζ_5' (resp. ζ_5), où ξ_4, ζ_4, η_5, η_5', ζ_5, ζ_5' sont les fonctions sur A_{45} induites respectivement par

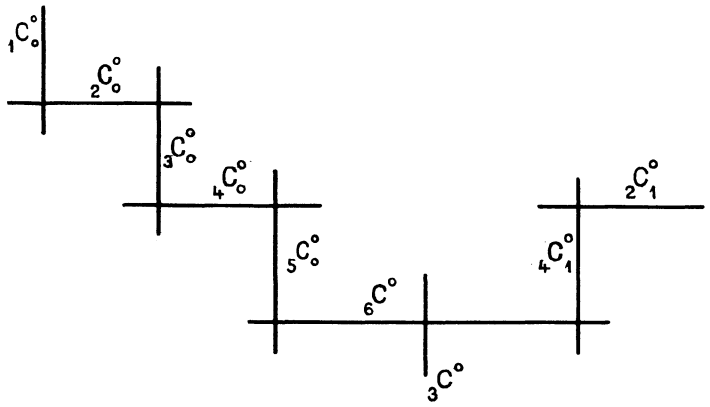


FIG. 10

X_4/Y_4, Z_4/Y_4, Y_5/X_5, $(Y_5/X_5)-\eta_0$, Z_5/X_5, $(Z_5/X_5)-\zeta_0$. Or on a les relations $\zeta_4=\xi_4^2\zeta_5$, et $t=\xi_4\zeta_4\eta_5=\xi_4^3\eta_5\zeta_5$. En portant dans l'équation de A_4, on en tire $\eta_5\equiv\gamma_5\zeta_0\xi_4$ (mod. ${}_4\mathfrak{m}_0^2$) (resp. $\zeta_5\equiv\xi_4$ (mod. ${}_4\mathfrak{m}_1^2$). Donc l'idéal ${}_4\mathfrak{m}_0$ (resp. ${}_4\mathfrak{m}_1$) est engendré par ξ_4 et ζ_5' (resp. ξ_4 et η_5').

Considérons de même un point de ${}_5C^0$ (resp. ${}_6C^0$) autre qu'un sommet. Ce point est de la forme $c^0\times c^0\times a^0\times b^0\times a^0\times u_{10}^0$ (resp. $c^0\times c^0\times a^0\times b^0\times a^0\times v_0^0$), avec $u_{10}^0=(1,\eta_{10},1)$ (resp. $v_0^0=(1,0,\zeta_0^0)$), où η_{10}^0 (resp. ζ_0^0) est un élément $\neq 0$ (resp. $\neq 0$ et 1) de $\mathfrak{k}^0$. Pour montrer que ce point est p-simple sur A_*, il suffit de vérifier la régularité de l'anneau local ${}_5\mathfrak{o}=\mathfrak{o}(b^0\times u_{10}^0, A_{46})$ (resp. ${}_6\mathfrak{o}=\mathfrak{o}(b^0\times v_0^0, A_{46})$). Soit η_{10} (resp. ζ_0) un élément de $\mathfrak{R}$ tel qu'on ait $\eta_{10}^0=\rho(\eta_{10})$ (resp. $\zeta_0^0=\rho(\zeta_0)$). L'idéal maximal ${}_5\mathfrak{m}$ (resp. ${}_6\mathfrak{m}$) de ${}_5\mathfrak{o}$ (resp. ${}_6\mathfrak{o}$) est engendré par t, ξ_4, ζ_4, η_6' (resp. η_6), et ζ_6 (resp. ζ_6') où ξ_4, ζ_4, η_6, η_6', ζ_6, ζ_6' sont les fonctions sur A_{46} respectivement induites par X_4/Y_4, Z_4/Y_4, Y_6/X_6, $(Y_6/X_6)-\eta_{10}$, $(Z_6/X_6)-1$, $(Z_6/X_6)-\zeta_0$. On a les relations $\zeta_4=\xi_4^3(1+\zeta_6)$, $t=\xi_4^2\zeta_4\eta_6$. En portant dans l'équation de A_4, on obtient une relation de la forme $\eta_{10}\zeta_6\equiv\xi_4$ (mod. ${}_5\mathfrak{m}^2$) (resp. $\eta_6\zeta_0(\zeta_0-1)\equiv\xi_4$ (mod. ${}_6\mathfrak{m}^2$)). Donc l'anneau local ${}_5\mathfrak{m}$ (resp. ${}_6\mathfrak{m}$) est engendré par ξ_4 et η_6' (resp. ξ_4 et ζ_6').

La p-simplicité de ${}_{23}s^0$ et ${}_{34}s^0$ résulte des calculs déjà faits dans le cas (c 7). Il reste à vérifier la p-simplicité des sommets ${}_{45}s^0$, ${}_{36}s^0$, ${}_{46}s^0$ et ${}_{24}s^0$.

p-simplicité de ${}_{45}s^0$. — Il suffit de vérifier la régularité de l'anneau local ${}_{45}\mathfrak{o} = \mathfrak{o}(a^0 \times b^0, A_{56})$. L'idéal maximal ${}_{45}\mathfrak{m}$ de cet anneau admet pour générateurs t, et les fonctions $\eta_5, \zeta_5, \xi_6, \zeta_6$, respectivement induites sur A_{56} par Y_5/X_5, Z_5/X_5, X_6/Y_6 et Z_6/Y_6. On a les relations $\zeta_5 = \eta_5\zeta_6$ et $t = \eta_5^5\xi_6^3\zeta_6$. On en déduit, en portant dans l'équation de A_5, $\zeta_6 \equiv \xi_6 \pmod{{}_{45}\mathfrak{m}^2}$. Donc l'idéal ${}_{45}\mathfrak{m}$ est engendré par ξ_6 et η_5.

p-simplicité de ${}_{36}s^0$. — Il suffit de vérifier la régularité de l'anneau local ${}_{36}\mathfrak{o} = \mathfrak{o}(b^0 \times a^0, A_{46})$. L'idéal maximal ${}_{36}\mathfrak{m}$ de cet anneau est engendré par t, et par les fonctions $\xi_4, \zeta_4, \eta_6, \zeta'_6$, respectivement induites sur A_{46} par X_4/Y_4, Z_4/Y_4, Y_6/X_6, Z_6/X_6. On a $\zeta_4 = \xi_4^3\zeta'_6$ et $t = \xi_4^5\eta_6\zeta'_6$. En portant dans l'équation de A_4, on trouve $\eta_6 \equiv -\gamma_5\xi_4\zeta'^2_6 \pmod{{}_{36}\mathfrak{m}^4}$. Donc ${}_{36}\mathfrak{m}$ est engendré par ξ_4 et ζ'_6.

p-simplicité de ${}_{46}s^0$. — Il suffit de vérifier la régularité de l'anneau local ${}_{46}\mathfrak{o} = \mathfrak{o}(a^0 \times c^0, A_{56})$. L'idéal maximal ${}_{46}\mathfrak{o}$ de cet anneau est engendré par t, et par les fonctions $\eta_5, \zeta_5, \xi'_6, \eta_6$ respectivement induites sur A_{56} par Y_5/X_5, Z_5/X_5, X_6/Z_6, Y_6/Z_6. On a $\eta_5 = \zeta_5\eta_6$, et $t = \eta_5\xi'^3_6\zeta_5^4 = \eta_6\xi'^3_6\zeta_5^5$. En portant dans l'équation de A_5, on trouve $\eta_6 \equiv \gamma_5\xi'_6\zeta_5 \pmod{{}_{46}\mathfrak{m}^3}$. Donc ${}_{46}\mathfrak{m}$ est engendré par ξ'_6 et ζ_5.

p-simplicité de ${}_{24}s^0$. — Il suffit de vérifier la régularité de ${}_{24}\mathfrak{o} = \mathfrak{o}(a^0 \times c^0, A_{35})$. L'idéal maximal ${}_{24}\mathfrak{m}$ de cet anneau est engendré par t, et par les fonctions $\eta_3, \zeta_3, \xi_5, \eta'_5$ respectivement induites sur A_{35} par Y_3/X_3, Z_3/X_3, X_5/Z_5, Y_5/Z_5. On a les relations $\eta_3 = \xi_3^2\eta'_5$, et $t = \zeta_3^3\xi_5\eta'_5$. En portant dans l'équation de A_3, on obtient $\eta'_5 \equiv \gamma_5\zeta_3\xi_5 \pmod{{}_{24}\mathfrak{m}^3}$. Donc ${}_{24}\mathfrak{m}$ est engendré par ζ_3 et ξ_5.

On a donc complètement démontré que A_* est p-simple. D'après la proposition 2 du n° 3, et compte tenu de l'expression de ω, on voit immédiatement que ω_* ne s'annule sur aucune des composantes ${}_1C_0^0$, ${}_2C_0^0$, ${}_3C_0^0$, ${}_3C^0$, ${}_2C_1^0$. Pour vérifier que ω_* ne s'annule pas non plus sur les quatre autres composantes, il nous suffit de vérifier que ω_* ne s'annule en aucun des deux points ${}_{45}s^0$, ${}_{46}s^0$, ou encore que la différentielle ω_{56} transposée de ω sur A_{56} ne s'annule en aucun des deux points $a^0 \times b^0$ et $a^0 \times c^0$.

Utilisons les mêmes paramètres $\eta_5, \zeta_5, \xi_6, \zeta_6, \xi'_6, \eta'_6$ que dans la démonstration de la p-simplicité de ces deux points; ces paramètres sont induits respectivement par $\overline{\eta}_5 = Y_5/X_5$, $\overline{\zeta}_5 = Z_5/X_5$, $\overline{\xi}_6 = X_6/Y_6$, $\overline{\zeta}_6 = Z_6/Y_6$, $\overline{\xi}'_6 = X_6/Z_6$, $\overline{\eta}'_6 = Y_6/Z_6$. Introduisons les anneaux locaux ${}_{45}\overline{\mathfrak{o}} = \mathfrak{o}(a^0 \times b^0, \mathbf{P}_2 \times \mathbf{P}_2)$ et ${}_{46}\overline{\mathfrak{o}} = \mathfrak{o}(a^0 \times c^0, \mathbf{P}_2 \times \mathbf{P}_2)$; soient respectivement ${}_{45}\overline{\mathfrak{m}}$ et ${}_{46}\overline{\mathfrak{m}}$ leurs idéaux maximaux.

Parmi les éléments de l'anneau ${}_{45}\overline{\mathfrak{o}}$ qui s'annulent sur A_{56} figurent $f_1 = \overline{\zeta}_5 - \overline{\eta}_5\overline{\zeta}_6$ et des fonctions de la forme $f_2 = \overline{\zeta}_6 - \overline{\xi}_6(1 + g_2)$ et $f_3 = t - \overline{\eta}_5^5\overline{\xi}_6^4(1 + g_3)$, avec $g_2 \in {}_{45}\overline{\mathfrak{m}}^2$ et $g_3 \in {}_{45}\overline{\mathfrak{m}}$. D'autre part ω_{56} est induite par une différentielle de la forme $\overline{\omega}_{56} = -d(\overline{\eta}_5\overline{\xi}_6)/\overline{\eta}_5^5\overline{\xi}_6^4(1 + g)$, avec $g \in {}_{45}\overline{\mathfrak{m}}$. La différentielle $\theta_{56} = \overline{\omega} \wedge df_1 \wedge df_2 \wedge df_3$ sur $\mathbf{P}_2 \times \mathbf{P}_2$ s'exprime sous la forme $d\overline{\xi}_6 \wedge d\overline{\eta}_5 \wedge d\overline{\zeta}_5 \wedge d\overline{\zeta}_6(1 + h)$ avec $h \in {}_{45}\overline{\mathfrak{m}}$. Donc θ_{56} est p-morphique et non nulle en $a^0 \times b^0$. Donc, puisque les p-différentielles de f_1, f_2, f_3 en ce point sont linéairement indépendantes, et, d'après les définitions du n° 13 du chapitre I^er^, ω_{56} est p-morphique et non nulle en $a^0 \times b^0$.

Parmi les éléments de l'anneau local ${}_{46}\overline{\mathfrak{o}}$ qui s'annulent sur A_{56} figurent la fonction $f'_1 = \overline{\eta}_5 - \overline{\zeta}_5\overline{\eta}'_6$, et deux fonctions f'_2, f'_3 qui sont respectivement de la

forme $f_2' = \overline{\eta}_6' - \gamma_5 \overline{\xi}_6' \overline{\zeta}_5 (1 + g_2')$ et $f_3' = t - \gamma_5 \overline{\xi}_6'^4 \overline{\zeta}_5^6 (1 + \overline{\xi}_6' + g_3')$, avec $g_2' \in_{46} \overline{\mathfrak{m}}$, et $g_3' \in_{46} \overline{\mathfrak{m}}^2$. D'autre part, ω_{56}' est induite par une différentielle $\overline{\omega}_{56}'$ sur $\mathbf{P}_2 \times \mathbf{P}_2$ de la forme $\overline{\omega}_{56}' = d(\overline{\xi}_6' \overline{\zeta}_5)/(\gamma_5 \overline{\xi}_6'^4 \overline{\zeta}_5^6 (2 - \overline{\xi}_6' + g'))$, avec $g' \in_{46} \overline{\mathfrak{m}}^2$. La différentielle $\theta_{56}' = \overline{\omega}_{56}' \wedge df_1' \wedge df_2' \wedge df_3'$ s'exprime sous la forme $\theta_{56}' = -d\overline{\zeta}_5 \wedge d\overline{\xi}_6' \wedge d\overline{\eta}_5 \wedge d\overline{\eta}_6' (1 + h')$, avec $h' \in_{46} \overline{\mathfrak{m}}$ (remarque : pour le calcul de θ_{56}', on doit examiner à part le cas où k^0 est de caractéristique 2; ceci est lié au fait que chacune des deux composantes de A_*^0 passant par le point ${}_{46}s^0$ a un coefficient pair dans A_*^0). Donc θ_{56}' est p-morphique et non nulle en $a^0 \times c^0$. Puisque les p-différentielles de f_1', f_2', f_3' en $a^0 \times c^0$ sont linéairement indépendantes sur k^0, et d'après les définitions du n° 13 du chapitre I^er, ω_{56} est p-morphique et non nulle en $a^0 \times c^0$.

Donc notre modèle (A_*, θ) est bien p-simple p-minimal. Puisque ${}_1C_0^0$ est la seule composante simple de A_*^0, le groupe $\mathscr{G}_\mathfrak{p}(A)$ est isomorphe à $\mathbf{G}_a$ sur k^0, tandis que le groupe $\Gamma(A)$ est réduit à un seul élément.

16. Démonstration du théorème 2 (cas d'un corps global).

Nous avons démontré que si A est une courbe elliptique plane, définie sur k, p-standard (au sens introduit au n° 7), il existe un k-modèle p-simple p-minimal (A_*, θ) de A, tel que $\theta^{-1} : A_* \to A$ soit un R-morphisme. De plus, ce modèle a été obtenu à partir de A, à un R-isomorphisme près, au moyen d'un nombre fini de transformations p-monoïdales : ceci résulte immédiatement, en effet, des formules qui définissent ce modèle, dans chacun des cas a), b_m), (c 1), (c 2), (c 3), (c 4) et (c 5_m); pour voir qu'il en est de même dans les cas (c 6), (c 7), (c 8), on peut, par exemple, remarquer que (A_*, θ) ne diffère que par un R-isomorphisme du modèle (A_*', θ') de A obtenu en remplaçant, dans le cas (c 6), le point $u_4 = (x^2, tyz, t^3z^2)$ de $\mathbf{P}_2$ par le point $u_4' = (x^2, tyz, t^3z^2, y^2)$ de $\mathbf{P}_3$ et, dans chacun des cas (c 7) et (c 8), les points $u_5 = (t^3x^2z, y^2x, t^4z^2y)$ et $u_6 = (t^4x^3z, y^3x, t^4y^2z^2)$ respectivement par les points

$$u_5' = (t^3x^2z, y^2x, t^4z^2y, t^3x^3, ty^3, t^6z^3) \quad \text{et} \quad u_6' = (t^4x^3z, y^3x, t^4y^2z^2, t^3x^4, y^4, t^{10}z^4)$$

de $\mathbf{P}_5$.

Soit maintenant K un corps global, et soit A une courbe elliptique définie sur K. Il existe, comme on sait, un sous-ensemble fini $\mathfrak{S}_0$ de $\mathfrak{S} = \mathfrak{S}(K)$ tel que A soit strictement non dégénérée (mod. p) (donc tel que $A_\mathfrak{p}^0 = \rho_\mathfrak{p}(A)$ soit une courbe elliptique sans point multiple), pour tout $\mathfrak{p} \in \mathfrak{S} - \mathfrak{S}_0$.

D'autre part, pour tout sous-ensemble fini $\mathfrak{S}'$ de $\mathfrak{S}$, on peut trouver un K-modèle plan de A qui est p-standard pour tout $\mathfrak{p} \in \mathfrak{S}'$. Il existe, en particulier, un K-modèle plan (A_0, φ_0) de A qui est p-standard pour tout $\mathfrak{p} \in \mathfrak{S}_0$.

Soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ les éléments de $\mathfrak{S}_0$. D'après ce qui précède, et d'après la proposition 25 du n° 26 du chapitre I^er, on peut, pour tout i $(1 \leqslant i \leqslant m)$, trouver un K-modèle (A_i, θ_i) de A_0 qui est $\mathfrak{p}_i$-simple $\mathfrak{p}_i$-minimal, tel que θ_i^{-1} soit un $R_{\mathfrak{p}_i}$-morphisme, et tel que θ_i soit un $R_\mathfrak{q}$-isomorphisme pour tout $\mathfrak{q} \in \mathfrak{S}$ distinct de $\mathfrak{p}_i$.

Le joint des K-modèles (A_i, θ_i) est alors un K-modèle (A', φ) de A_0 qui est $\mathfrak{p}_i$-simple $\mathfrak{p}_i$-minimal pour tout i $(1 \leqslant i \leqslant m)$.

Soit maintenant $\mathfrak{S}'_0$ un sous-ensemble fini de $\mathfrak{S}-\mathfrak{S}_0$ tel que $\rho_\mathfrak{p}(A')=A'^0_\mathfrak{p}$ soit strictement non dégénérée (mod. $\mathfrak{p}$) pour tout $\mathfrak{p}\in\mathfrak{S}-\mathfrak{S}_0-\mathfrak{S}'_0$. D'après le théorème 2* du chapitre II, et d'après la proposition 25 du n° 26 du chapitre I^er, il existe un K-modèle (A_*, ψ) de A' qui est faiblement $\mathfrak{p}$-simple $\mathfrak{p}$-minimal pour tout $\mathfrak{p}\in\mathfrak{S}'_0$, et tel que ψ soit un $R_\mathfrak{q}$-isomorphisme pour tout $\mathfrak{q}\in\mathfrak{S}-\mathfrak{S}'_0$.

Montrons que A_* est $\mathfrak{p}$-simple $\mathfrak{p}$-minimale pour tout $\mathfrak{p}\in\mathfrak{S}$. En effet, pour $\mathfrak{p}\in\mathfrak{S}_0$, A' est $\mathfrak{p}$-simple $\mathfrak{p}$-minimale, et ψ est un $R_\mathfrak{p}$-isomorphisme. D'autre part, pour $\mathfrak{p}\in\mathfrak{S}-\mathfrak{S}_0$, A_* est faiblement $\mathfrak{p}$-simple $\mathfrak{p}$-minimale (soit par construction de A_*, si $\mathfrak{p}\in\mathfrak{S}'_0$, soit parce que A' est strictement non dégénérée (mod. $\mathfrak{p}$), si $\mathfrak{p}\in\mathfrak{S}-\mathfrak{S}_0-\mathfrak{S}'_0$). Or, pour $\mathfrak{p}\in\mathfrak{S}-\mathfrak{S}_0$, A est strictement non dégénérée (mod. $\mathfrak{p}$), et le groupe $\mathscr{G}_\mathfrak{p}(A)$ est isomorphe à $A^0=\rho(A)$, regardée comme une variété abélienne de dimension 1. Si on pose $A^0_*=\rho(A_*)$, le groupe $\mathscr{S}(A^0_*)$ est également isomorphe à $\mathscr{G}_\mathfrak{p}(A)$. Ceci implique, en particulier que $\mathscr{S}(A^0_*)$ est une variété complète. Donc $\mathscr{S}(A^0_*)$ coïncide avec l'une des composantes de A^0_*. Par définition du symbole $\mathscr{S}$, elle ne peut rencontrer les autres composantes de A^0_*. Comme $\rho_e(A_*)=\operatorname{supp} A^0_*$ est connexe, $\mathscr{S}(A^0_*)$ est donc l'unique composante de A^0_*. Donc A_* est strictement non dégénérée (mod. $\mathfrak{p}$). Donc A_* est bien encore $\mathfrak{p}$-simple $\mathfrak{p}$-minimale.

Remarque. — La démonstration précédente peut être simplifiée dans le cas où le corps global considéré K est un corps de nombres algébriques. Dans ce cas, en effet, on peut choisir le modèle plan (A_0, φ_0) de manière qu'il soit $\mathfrak{p}$-standard pour tout $\mathfrak{p}\in\mathfrak{S}$. Si alors (A', φ) est le joint des k-modèles (A_i, θ_i) de A_0, construits comme précédemment, A' est automatiquement $\mathfrak{p}$-simple $\mathfrak{p}$-minimal pour tout $\mathfrak{p}\in\mathfrak{S}$, et la dernière partie de la construction devient inutile.

17. Tableau récapitulatif.

Nous résumons dans le tableau ci-après les résultats de la discussion intervenant dans la démonstration du théorème 1.

Dans la colonne 1 sont énumérés les différents cas rencontrés dans cette discussion, et qui donnent lieu à une réduction dégénérée de A_*. Dans la colonne 2, on reproduit les relations qui caractérisent une courbe elliptique plane $\mathfrak{p}$-standard (n° 7, prop. 4, 5 et 6) dans chacun de ces cas. Rappelons qu'une telle courbe est définie par une équation de la forme

$$Y^2Z+\lambda XYZ+\mu YZ^2=X^3+\alpha XZ+\beta XZ^2+\gamma Z^3 \tag{1}$$

où λ, μ, α, β, γ sont des éléments de R; rappelons aussi que dans le cas b) (resp. c)), les coefficients μ, β, γ (resp. λ, μ, α, β, γ) sont de valuation $\geqslant 1$, i.e. appartiennent à $\mathfrak{p}$; comme dans les n^os 6 et 7, on pose $\overline{\alpha}=\lambda^2+4\alpha$, $\overline{\gamma}=\mu^2+4\gamma$, $\widetilde{\delta}=\beta^2-4\alpha\gamma$, et on note Δ le discriminant du polynôme $X^3+\alpha X^2+\beta X+\gamma$.

Dans la colonne 3, on indique la caractérisation de chacun des cas considérés lorsque la caractéristique de k^0 est différente de 2 et 3, pour une courbe elliptique plane

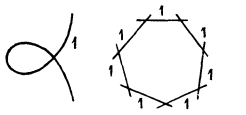
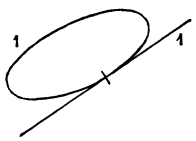
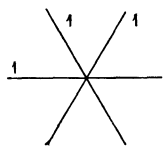
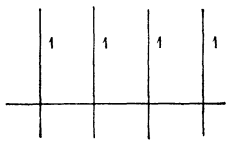
quelconque A (non nécessairement p-standard) représentée par une équation de Weierstrass

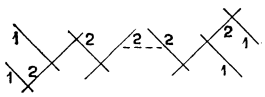
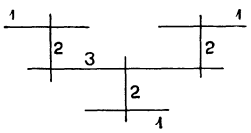
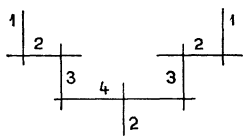
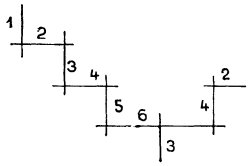
$$Y^2Z = X^3 + \beta XZ^2 + \gamma Z^3 \tag{10}$$

(cf. n° 8). On pose alors $\Delta = 4\beta^3 + 27\gamma^2$, et on note j l'invariant de A.

Dans la colonne 4, on reproduit la figure représentant la connection des composantes (et, éventuellement, les points multiples) du cycle A^0_*; les chiffres représentent les coefficients de ces différentes composantes).

Dans les colonnes 5 et 6 sont indiquées respectivement la structure du groupe $\mathscr{G}_{p0}(A)$ (composante de l'origine de $\mathscr{G}_p(A)$), et celle du groupe fini commutatif $\Gamma(A) = \mathscr{G}_p(A)/\mathscr{G}_{p0}(A)$.

	Caractéristique quelconque	Caractéristique $\neq 2$ et 3	Cycle A^0_*	Structure de $\mathscr{G}_{p0}(A)$	Ordre et structure de $\Gamma(A)$
Cas (b_m)	$v(\alpha) = 0$ $v(\mu) > \frac{m}{2}$ $\quad v(\beta) > \frac{m}{2}$ $v(\gamma) = m$	$v(j) = -m$ $v(\gamma)$ pair	$m = 1$ $\quad m$ quelconque  (m composantes)	$\mathbf{G}_m$	m (cyclique)
Cas (c 1)	$v(\gamma) = 1$	$v(j) \geqslant 0$ $v(\Delta) \equiv 2$ (mod. 12)		$\mathbf{G}_a$	1
Cas (c 2)	$v(\beta) = 1$ $\quad v(\gamma) \geqslant 2$	$v(j) \geqslant 0$ $v(\Delta) \equiv 3$ (mod. 12)		$\mathbf{G}_a$	2
Cas (c 3)	$v(\beta) \geqslant 2$ $\quad v(\gamma) \geqslant 2$ $v(\overline{\gamma}) = 2$	$v(j) \geqslant 0$ $v(\Delta) \equiv 4$ (mod. 12)		$\mathbf{G}_a$	3
Cas (c 4)	$v(\mu) \geqslant 2$ $\quad v(\beta) \geqslant 2$ $v(\gamma) \geqslant 3$ $\quad v(\Delta) = 6$	$v(j) \geqslant 0$ $v(\Delta) \equiv 6$ (mod. 12)		$\mathbf{G}_a$	4 (non cyclique)

	Caractéristique quelconque	Caractéristique $\neq 2$ et 3	Cycle A^0_*	Structure de $\mathcal{G}_{po}(A)$	Ordre et structure de $\Gamma(A)$
Cas (c 5_m)	$v(\alpha) = 1$; si $m = 2n-1$, $v(\mu) \geqslant n+1$ $v(\beta) \geqslant n+2$ $v(\gamma) \geqslant 2n+2$ $v(\bar{\gamma}) = 2n+2$ si $m = 2n$, $v(\mu) \geqslant n+2$ $v(\beta) \geqslant n+2$ $v(\gamma) \geqslant 2n+3$ $v(\tilde{\delta}) = 2n+4$	$v(j) = -m$ $v(\gamma)$ impair	 ($m+1$ composantes doubles)	$\mathbf{G}_a$	4 (cyclique pour m impair, non cyclique pour m pair)
Cas (c 6)	$v(\mu) \geqslant 2$ $v(\alpha) \geqslant 2$ $v(\beta) \geqslant 3$ $v(\gamma) \geqslant 4$ $v(\bar{\gamma}) = 4$	$v(j) \geqslant 0$ $v(\Delta) \equiv 8$ (mod. 12)		$\mathbf{G}_a$	3
Cas (c 7)	$v(\mu) \geqslant 3$ $v(\alpha) \geqslant 2$ $v(\beta) = 3$ $v(\gamma) \geqslant 5$	$v(j) \geqslant 0$ $v(\Delta) \equiv 9$ (mod. 12)		$\mathbf{G}_a$	2
Cas (c 8)	$v(\mu) \geqslant 3$ $v(\alpha) \geqslant 2$ $v(\beta) \geqslant 4$ $v(\Delta) = 5$	$v(j) \geqslant 0$ $v(\Delta) \equiv 10$ (mod. 12)		$\mathbf{G}_a$	1

BIBLIOGRAPHIE

[1] N. Bourbaki, *Éléments de mathématique*, liv. II *(Algèbre)*, chap. VII, Actualités sc. et indust., n° 1179, Paris, Hermann, 1952.

[2] W. L. Chow, Projective embedding of homogeneous spaces, *Lefschetz Conference Volume*, Princeton University Press, 1957.

[3] J. Dieudonné et A. Grothendieck, Éléments de géométrie algébrique, I, *Publ. Math. Inst. Htes Ét. scientifiques*, Paris, *4*, 1960.

[4] M. Greenberg, *Pro-algebraic structure on the rational subgroup of a p-adic abelian variety*, Thesis, Princeton Univ., 1959.

[5] M. Greenberg, Schemata over local rings, *Ann. Math.*, 73 (1961), pp. 624-648.

[6] J. Igusa, Fibre systems of jacobian varieties, *Amer. J. Math.*, vol. 78 (1956), pp. 171-199 et 745-760.

[7] K. Kodaira, On compact analytic surfaces, *Princeton Math. Series*, 24, pp. 121-135.

[8] S. Koizumi, On specialization of the Albanese and Picard varieties, *Mem. Coll. Sci. Univ. Kyoto*, 32 (1960), pp. 371-382.

[9] S. Koizumi and G. Shimura, On specialization of abelian varieties, *Scientific Papers of the College of General Education University of Tokyo*, 9 (1959), pp. 187-211.

[10] S. Lang, *Abelian varieties*, Interscience Tracts, New York, 1959.

[11] M. Lazard, Bemerkungen zur Theorie der bewerteten Körper und Ringe, *Math. Nach*, 12 (1954), pp. 67-73.

[12] E. Lutz, Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps p-adiques, *J. Crelle*, 177 (1937), pp. 238-247.

[13] A. Mattuck, Abelian varieties over p-adic fields, *Ann. Math.*, 62 (1955), pp. 92-119.

[14] A. Néron, Valeur asymptotique du nombre des points de hauteur bornée sur une courbe elliptique, *International Congress of Math.*, Edinburgh, 1958.

[15] M. Rosenlicht, Some basic theorems on algebraic groups, *Amer. J. Math.*, 78, 1956, pp. 401-443.

[16] P. Samuel, Algèbre locale, *Mém. Sci. Math.*, n° 123, Paris, Gauthier-Villars, 1953.

[17] G. Shimura (cité [R]), Reduction of algebraic varieties with respect to a discrete valuation of the basic field, *Amer. J. Math.*, 77 (1955), pp. 134-176.

[18] J.-P. Serre, *Groupes algébriques et corps de classes*, Act. sc. et indust., n° 1264, Paris, Hermann, 1959.

[19] J.-P. Serre, Groupes proalgébriques, *Publ. Math. Inst. Htes Ét. scientifiques*, Paris, 7, 1962.

[20] J.-P. Serre, *Corps locaux*, Act. sc. et indust., n° 1296, Paris, Hermann, 1962.

[21] A. Weil (cité [F]), *Foundations of Algebraic Geometry*, Amer. Math. Soc. Colloquium Publ., vol. 29, New York, 1946, 2e éd.

[22] A. Weil, *Variétés abéliennes et courbes algébriques*, Act. sc. et indust., n° 1064, Paris, Hermann, 1948.

[23] A. Weil, Arithmetic on algebraic varieties, *Ann. Math.* (2), 53 (1951), pp. 412-444.

[24] A. Weil, The field of definition of a variety, *Amer. J. Math.*, 78, n° 3 (1956), pp. 509-524.

[25] E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grade p^n, *J. Crelle*, 176 (1936), pp. 126-140.

[26] O. Zariski, The problem of minimal models in the theory of algebraic surfaces, *Amer. J. Math.*, 80, n° 1, (1958), pp. 146-184.

TABLE DES MATIÈRES

Reçu le 15 janvier 1963.
Révisé le 15 octobre 1963.

1964. — Imprimerie des Presses Universitaires de France. — Vendôme (France)
ÉDIT. N° 27 917 IMPRIMÉ EN FRANCE IMP. N° 18 425