Paul Dubreil

Variétés algébriques, II

Séminaire Dubreil. Algèbre et théorie des nombres, tome 2-3 (1948-1950), exp. nº 2, p. 1-17
<http://www.numdam.org/item?id=SD_1948-1950__2-3__A2_0>

VARIÉTÉS ALGÉBRIQUES, II.,

par Paul DUBREIL

4. Changement du corps de définition : préliminaires algébriques.

Après avoir vu une condition nécessaire et suffisante pour que deux points P et P' engendrent le même lieu sur un corps k donné, et montré que deux tels points génériques d'une même variété ont la même dimension sur k (voir exposé précédent, paragraphe 3 : théorème 2, lemme 3 et remarque), nous allons étudier le changement du corps de définition k : cela nous conduira à une condition nécessaire et suffisante pour qu'un corps k soit corps de définition de V, à une condition nécessaire et suffisante pour que deux variétés définies par les couples (k , P) et (k' , P') coïncident, et au caractère intrinsèque de la dimension.

Le problème de base est le suivant. Soient deux corps k et K, avec $k \leqslant K \ (\leqslant \Delta)$. Si un point $P = (x)$ a un lieu v sur k, a-t-il un lieu V sur K, et a-t-on $V = v$? Inversement, si un point $P = (x)$ a un lieu V sur K, a-t-il un lieu v sur k et a-t-on $v = V$?

Il est clair que ce problème se décompose en deux :

(a) un problème de théorie des corps : $k(x)$ étant une extension régulière de k, le corps $K(x)$ est-il extension régulière de k ?

Dans l'autre sens, $K(x)$ étant extension régulière de K, $k(x)$ est-il une extension régulière de k ? On répondra affirmativement à ces questions, à condition, bien entendu, de faire des hypothèses convenables sur les corps k, K, $k(x)$, $K(x)$.

(b) un problème de spécialisation, c'est-à-dire de théorie des idéaux, comparaison des variétés v, et V, dont (a) aura permis d'affirmer l'existence simultanée.

La résolution du problème (a), dans le sens de k vers K, fait intervenir à peu près les mêmes moyens algébriques que la démonstration de l'équivalence de la première et de la deuxième définition des extensions régulières.

La première étape consiste à introduire une propriété plus faible que la disjonction linéaire : non seulement la nouvelle propriété permet d'exprimer sous leur forme la plus large les hypothèses qui doivent être faites, mais elle joue un rôle essentiel dans certains raisonnements. On l'obtient en remplaçant dans la disjonction linéaire les mots "linéairement indépendants" par les mots "algébriquement indépendants".

Soient donc L_1, L_2 deux corps contenant k comme sous-corps. Si les quantités $x_1, \dots, x_r \in L_1$, algébriquement indépendantes sur k, le sont toujours aussi sur L_2, de même les quantités $y_1, \dots, y_s \in L_2$ algébriquement indépendantes sur k le sont aussi sur L_1 : deux corps L_1 et L_2 possédant cette propriété symétrique sont dits algébriquement indépendants ou libres sur k.

On peut à la fois établir et expliquer l'existence de cette propriété et de la disjonction linéaire, en considérant d'une façon très générale, dans un ensemble Δ (qui est ici le domaine universel), une propriété d'indépendance $\mathfrak{J}_{L_2}^{L_1}$ et une propriété de dépendance $\mathfrak{D}_{L_2}^{L_1}$, négations l'une de l'autre, portant sur les éléments d'un sous-ensemble L_1 et relatives à un autre sous-ensemble L_2 (11). Soit k un sous-ensemble de L_1 et de L_2. Nous dirons que L_1 est disjoint de L_2 sur k si

$$\mathfrak{J}_k^{L_1}(x_1, \dots, x_p) \quad \text{entraîne} \quad \mathfrak{J}_{L_2}^{L_1}(x_1, \dots, x_p)$$

$(x_\rho \in L_1)$. Cette propriété de disjonction est symétrique toutes les fois que

$$(6) \qquad \mathfrak{D}_{L_1}^{L_2}(y_1, \dots, y_q) \quad \text{et} \quad \mathfrak{J}_k^{L_2}(y_1, \dots, y_q)$$

$(y_\mu \in L_2)$ entraîne l'existence de $x_1, \dots, x_p \in L_1$ tels que

$$(7) \qquad \mathfrak{D}_{L_2}^{L_1}(x_1, \dots, x_p) \quad \text{et} \quad \mathfrak{J}_k^{L_1}(x_1, \dots, x_p)$$

En effet, si L_2 n'était pas disjoint de L_1 sur k, on aurait au moins un ensemble $\{y_1, \dots, y_q\}$ vérifiant (6), donc un ensemble $\{x_1, \dots, x_p\}$ vérifiant (7), ce qui est absurde, puisque, par hypothèse, L_1 est disjoint de L_2.

---

(11) On trouvera une étude systématique des propriétés de dépendance ou d'indépendance, ainsi envisagées, dans un mémoire de HAUPT, NÖBELING et PAUC [2].

Il suffit donc, pour chaque type de dépendance, de vérifier que (6) entraîne (7). Dans le cas de la dépendance linéaire, c'est à peu de choses près, la démonstration donnée au paragraphe 2 : les relations (6) signifient $\sum_{\mu} u_{\mu} y_{\mu} = 0$ où les u_{μ}, éléments de L_1, n'appartiennent pas tous à k. En désignant par x_{ρ} $(= v_{\rho})$ un système maximal d'éléments linéairement indépendants sur k parmi les u_{μ}, on a $u_{\mu} = \sum_{\rho} c_{\mu\rho} x_{\rho}$ avec $c_{\mu\rho} \in k$, d'où $\sum_{\rho} z_{\rho} x_{\rho} = 0$ avec $z_{\rho} = \sum_{\mu} c_{\mu\rho} y_{\mu} \in L_2$, c'est-à-dire (7).

Dans le cas de l'<u>indépendance algébrique</u>, l'hypothèse (6) signifie que $y_1 , \dots , y_q$ algébriquement indépendants sur k, annulent au moins un polynôme $F(Y_1 , \dots , Y_q)$ à coefficients dans L_1. Soit $x_1 , \dots , x_p$ un système maximal d'éléments algébriquement indépendants sur k parmi ces coefficients : les coefficients de F appartiennent tous à une extension algébrique $\sum'$, d'ailleurs finie, du corps $\sum = k(x_1 , \dots , x_p)$; les y, algébriquement dépendants sur $\sum'$, le sont aussi sur $\sum$ VAN DER WAERDEN [3], paragraphe 64, Grundsatz 3, p. 210, donc annulent un polynôme $G(Y_1 , \dots , Y_q)$ à coefficients dans $\sum$ et il suffit de multiplier par le dénominateur commun éventuel pour obtenir une relation

$$P(x_1 , \dots , x_p , y_1 , \dots , y_q) = 0 \quad \text{où} \quad P \in k[X_1 , \dots , X_p , Y_1 , \dots , Y_q]$$

de sorte que les x, algébriquement indépendants sur k, sont algébriquement dépendants sur $k(y_1 , \dots , y_q)$, donc sur L_2.

C. Q. F. D.

EXEMPLE. - La fermeture algébrique $\bar{k}$ de k et un corps K quelconque sont algébriquement indépendants sur k. En effet, tout ensemble d'éléments de $\bar{k}$ algébriquement indépendants sur k est <u>vide</u>, il n'existe donc pas de tel système dont les éléments soient algébriquement dépendants sur K (on peut remarquer aussi que des éléments (de K) algébriquement dépendants sur $\bar{k}$ le sont aussi sur k.

<u>Deux extensions</u> L_1, L_2 <u>de</u> k, <u>linéairement disjointes sur</u> k, <u>sont algébriquement indépendantes sur</u> k. ([4], proposition 4, p. 4).

Soit en effet un ensemble d'éléments $y_1 , \dots , y_q \in L_2$, algébriquement dépendants sur L_1. Nous avons

(8) $\qquad F(y_1 , \dots , y_q) = 0$ où $F(Y_1 , \dots , y_q) \in L_1[X]$ et $\neq 0$

Si les coefficients u_μ de F appartiennent tous à k, les y sont algébriquement dépendants sur k (C. Q. F. D.). Sinon, les u_μ ($\in L_1$) s'expriment linéairement au moyen d'un ensemble maximal d'éléments x_ρ linéairement indépendants sur k :

$$u_\mu = \sum_\rho c_{\mu\rho} x_\rho \qquad c_{\mu\rho} \in k\ , \ x_\rho \in L_1$$

et (σ) s'écrit

$$\sum_\rho x_\rho P_\rho(y) = 0 \quad \text{où} \quad P_\rho(y) \in k[Y] \quad \text{donc} \quad P_\rho(y) \in k(y) \subseteq L_2 \, .$$

Or, L_1 et L_2 étant linéairement disjoints sur k, les x_ρ sont aussi linéairement indépendants sur L_2, ce qui entraîne $P_\rho(y) = 0$: comme un au moins des $P_\rho(Y)$ n'est pas nul, puisque $F(Y) = \sum_\rho x_\rho P_\rho(Y) \neq 0$, les y sont encore algébriquement dépendants sur k

C. Q. F. D.

Il est naturel de se demander si, en imposant une condition convenable à certains des corps k, L_1, L_2, on peut passer inversement de l'indépendance algébrique de L_1 et L_2 sur k à leur disjonction linéaire. Le théorème suivant répond à cette question, tout en résolvant la première partie du problème (a).

THÉORÈME 3. - Soit $P = (x_1, \dots, x_n) = (x)$ un point tel que $k(x) = L_1$ soit extension régulière de k. Si K ($= L_2$) et $k(x)$ sont algébriquement indépendants sur k, il sont linéairement disjoints sur k, et $K(x)$ est extension régulière de K (P a donc un lieu sur K comme il en a un sur k) [12].

L'ensemble des éléments de K algébriques et séparables sur k est un corps k' (car les propriétés "algébrique" et "séparable" se conservent dans les opérations rationnelles, voir par exemple VAN DER WAERDEN [3] paragraphe 38, p. 118-119 et paragraphe 41, p. 136) ; on établit d'abord que : $k(x)$, dans lequel k est algébriquement fermé, et k' (regardé comme une extension algébrique séparable quelconque de k) sont linéairement disjoints sur k. Soient en effet $\alpha_1, \dots, \alpha_r$ des éléments de k' linéairement indépendants sur k ; $k(\alpha_1, \dots, \alpha_r)$; étant séparable sur k, est une extension simple

---

[12] [4], chapitre IV, paragraphe 1, théorème 1, p. 70 et chapitre I, paragraphe 7, théorème 5, p. 18. Ce théorème repose sur une série de lemmes dont il serait trop long de reproduire les démonstrations : nous nous bornerons à indiquer l'enchaînement des idées.

$k(\theta)$ de k ("théorème de l'élément primitif, [3], paragraphe 43, p. 138), et il suffit de montrer que $k(\theta)$ *et* $k(x)$ *sont linéairement disjoints sur* k. On l'établit ([4], chapitre I, proposition 7, p. 6) en s'appuyant sur le lemme suivant ([4], proposition 6, p. 5 ; on pourra se reporter aussi à VAN DER WAERDEN, [3], paragraphe 35, p. 106, et paragraphe 38, p. 118).

LEMME 4. - *Soit* $(\xi_1, \dots, \xi_s) = (\xi)$ *un ensemble d'éléments algébriques sur un corps* k, *et* L *un sur-corps de* k. *On a*

$$[L(\xi) : L] \leqslant [k(\xi) : k]$$

avec l'égalité si et seulement si L *et* $k(\xi)$ *sont linéairement disjoints sur* k.

Ce lemme permet de montrer que $k(\theta)$ et $k(x)$, dans lequel k est algébriquement fermé, sont linéairement disjoints sur k : les $\alpha_i \in k(\theta) \leqslant k'$ sont donc bien linéairement indépendants sur $k(x)$.

On sait donc, d'après la symétrie de la disjonction linéaire, que des éléments de $k(x)$ linéairement indépendants sur k le sont sur k' : *pour établir que* $k(x)$ *et* K *sont linéairement disjoints sur* k, *il suffit de montrer que* $k'(x) \geqslant k(x)$ *et* K *sont linéairement disjoints sur* k'.

Or, cette dernière propriété résulte du lemme suivant, dont la démonstration ([4], chapitre I, proposition 18, p. 17) repose sur la théorie des dérivations abstraites ([4], paragraphe 5, en particulier proposition 15 et théorème 1, p. 13).

LEMME 5. - *On suppose l'extension* $k(x)$ *séparablement engendrée sur* k. *Alors,* K, *algébriquement indépendant de* $k(x)$ *sur* k, *et* $k'(x)$ *sont linéairement disjoints sur* k' (k' désigne toujours l'ensemble des éléments de K qui sont algébriques et séparables sur k).

Pour achever la démonstration du théorème 3, il reste à montrer que $K(x)$ est une extension régulière de K. Comme $k(x)$ et K sont par hypothèse algébriquement indépendants sur k, $k(x)$ et $\overline{K}$, fermeture algébrique de K, le sont aussi (car des éléments de $k(x)$ algébriquement dépendants sur $\overline{K}$ sont algébriquement dépendants sur K, ([2]), donc finalement sur k). Donc d'après la première partie du théorème 3, $k(x)$ et $\overline{K}$ sont linéairement disjoints sur k : par conséquent, *des éléments de* $k(x)$ (= [illegible]) *linéairement indépendants sur* K $(= \Sigma)$, *donc sur* k, *le sont sur* $\overline{K}$ $(= \Sigma' \geqslant \Sigma)$: *d'après le lemme*

<u>suivant,</u> $\Sigma' = \bar{K}$ <u>et le corps composé</u> [13] $\mathfrak{P}_1$ <u>de</u> $\mathfrak{P}$ <u>et de</u> Σ , <u>c'est-à-dire ici</u> $K(x)$, <u>sont linéairement disjoints sur</u> $\Sigma = K$ <u>et</u> $K(x)$ <u>est bien une extension régulière de</u> K .

LEMME 6. - Soient $\Sigma \leq \Sigma'$ et $\mathfrak{P}$, trois corps $(\leq \Delta)$, et $\mathfrak{P}_1$ <u>le corps composé de</u> $\mathfrak{P}$ <u>et de</u> Σ <u>. Si tout ensemble d'éléments de</u> $\mathfrak{P}$ linéairement indépendants sur Σ est un ensemble d'éléments linéairement indépendants sur Σ', Σ et $\mathfrak{P}_1$ sont linéairement disjoints sur Σ ([4], chapitre I, proposition 5, p. 5).

Soit $\{\ldots , w_\mu , \ldots\}$ un ensemble fini d'éléments de Σ' linéairement indépendants sur Σ, et soit une relation

$$(9) \qquad \sum_\mu u'_\mu \, w_\mu = 0 \qquad \text{avec} \qquad u'_\mu \in \mathfrak{P}_1$$

Or, les u'_μ sont des quotients de sommes $\sum_\nu x_\nu y_\nu$ où $x_\nu \in \Sigma$, $y_\nu \in \mathfrak{P}$; donc, en les multipliant par un multiple commun $c \neq 0$ $(c \in \mathfrak{P}_1)$ des dénominateurs, on obtient les éléments

$$(10) \qquad u_\mu = cu'_\mu = \sum_\nu x_{\mu\nu} y_{\mu\nu} \begin{cases} c \neq 0 \\ x_{\mu\nu} \in \Sigma \\ y_{\mu\nu} \in \mathfrak{P} \end{cases}$$

Soit $\{\ldots , z_\lambda , \ldots\}$ un ensemble <u>maximal</u> d'éléments linéaires indépendants sur Σ, extraits de l'ensemble des $y_{\mu\nu}$: on a

$$y_{\mu\nu} = \sum_\lambda a_{\mu\nu\lambda} \, z_\lambda \qquad a_{\mu\nu\lambda} \in \Sigma , \quad z_\lambda \in \mathfrak{P}$$

d'où

$$u_\mu = \sum_\lambda b_{\mu\lambda} z_\lambda \qquad \text{avec} \qquad b_{\mu\lambda} = \sum_\nu a_{\mu\nu\lambda} \, x_{\mu\nu} \in \Sigma \leq \Sigma'$$

(9) entraîne

$$\sum_\mu u_\mu \, w_\mu = 0 \qquad \text{c'est-à-dire} \qquad \sum_\lambda c_\lambda \, z_\lambda = 0$$

où $c_\lambda = \sum_\mu w_\mu \, b_{\mu\lambda} \in \Sigma'$. Or, par hypothèse, les z_λ, éléments de $\mathfrak{P}$ linéairement indépendants sur Σ , sont linéairement indépendants sur Σ'. Donc $c_\lambda = 0$, et, puisque les w_μ sont indépendants sur Σ, $b_{\mu\lambda} = 0$, $u_\mu = 0$, $u' = 0$,

C. Q. F. D.

---

[13] Le corps composé $\mathfrak{P}_1$ de $\mathfrak{P}$ et de Σ, tous deux contenus dans Δ , est le plus petit sous-corps de Δ contenant $\mathfrak{P}$ et Σ . Les éléments de $\mathfrak{P}_1$ sont des quotients de sommes $\sum x_\nu y_\nu$ où $x_\nu \in \Sigma$, $y_\nu \in \mathfrak{P}$.

a. Le problème est ainsi résolu par le théorème 3, pour le passage d'un corps k à un sur-corps K. Considérons maintenant le passage inverse, d'ailleurs beaucoup plus facile.

THÉORÈME 4. - $K(x_1, \ldots, x_n) = K(x)$ étant une extension régulière de K, et k désignant un sous-corps de K, si K et $k(x)$ sont linéairement disjoints (donc algébriquement indépendants) sur k, $k(x)$ est également une extension régulière de k.

Des éléments de $k(x)$ linéairement indépendants sur k, le sont aussi sur K, donc sur $\overline{K}$ (puisque $\overline{K}$ et $K(x)$ sont linéairement disjoints sur K d'après la première définition des extensions régulières), et a fortiori sur $\overline{k}$, sous-corps de $\overline{K}$: $k(x)$ est donc bien extension régulière de k.

b. Nous supposons maintenant les corps k et K, $k \leq K$ et le point $P = (x)$, tels que K et $k(x)$ soient algébriquement indépendants sur k, et $k(x)$ une extension régulière de k. D'après (a), $K(x)$ est extension régulière de K, et K et $k(x)$ sont linéairement disjoints sur k.

THÉORÈME 5. - Avec les hypothèses précédentes, le lieu v de P sur k et le lieu V de P sur K coïncident, en d'autres termes on a la relation d'équivalence

$$(k, P) \equiv (K, P)$$

ou encore : toute spécialisation finie (y) de P sur k est une spécialisation (Y) de P sur K, et inversement ([4], chapitre IV, théorème 1, p. 70, et chapitre II, théorème 4, p. 29).

En particulier, si $P = (x)$ a un lieu V sur k, il a le même lieu V sur la fermeture algébrique $\overline{k}$ de k, puisque $\overline{k}$ et tout corps K (en particulier $K = k(x)$) sont algébriquement indépendants sur k.

Les points de v, spécialisations (y) de P sur k, sont les systèmes de n quantités annulant les polynômes d'une base de l'idéal $\mathfrak{P}(x)/k$. Les points de V, spécialisations (Y) de P sur K, sont les systèmes de n quantités annulant les polynômes d'une base de l'idéal $\mathfrak{P}(x)/K$. Le théorème sera évident si l'idéal $\mathfrak{P}(x)/K$ possède une base dans l'anneau $k[X]$ et si, de plus, cette base est une base de l'idéal $\mathfrak{P}(x)/k$. Il en est bien ainsi d'après le théorème suivant ([4], chapitre I, théorème 3 et lemme 1, p. 15 ; le lemme 1 est donné ci-dessous).

THÉORÈME 6. - <u>Soit</u> K <u>sur un sur-corps de</u> k . <u>L'idéal</u> $\mathfrak{P}(x)/K$ <u>a une base dans</u> $k[X]$ <u>si et seulement si</u> K <u>et</u> $k(x)$ <u>sont linéairement disjoints sur</u> k ; <u>quand il en est ainsi, cette base est également une base pour</u> $\mathfrak{P}(x)/k$.

Non seulement cet important théorème permet de démontrer le précédent, mais il apporte une <u>condition nécessaire et suffisante pour que</u> $k(x)$ <u>soit une extension régulière de</u> k (c'est-à-dire pour que $k(x)$ et $\bar{k}$ soient linéairement disjoints sur k) : <u>cette condition est que l'idéal</u> $\mathfrak{P}(x)/\bar{k}$ <u>ait une base dans</u> $k[X]$. Signalons en outre que cette condition intervient dans la démonstration de l'équivalence de la première et de la deuxième définition des extensions régulières. Enfin, le théorème 6 interviendra encore dans la recherche d'une condition nécessaire et suffisante pour qu'un corps soit corps de définition d'une variété donnée.

Le théorème 6 repose sur le lemme suivant, souvent utilisé (sous une forme ou sous une autre) dans la théorie des idéaux de polynômes.

LEMME 7. - <u>Soit</u> $\mathfrak{a}$ <u>un idéal de l'anneau</u> $K[X_1, \dots, X_n] = K[X]$. <u>On suppose que</u> $\mathfrak{a}$ <u>admet une base</u> $(\dots, F_\nu, \dots)$ <u>dans</u> $k[X]$, k <u>désignant un sous-corps de</u> K .

1° <u>Tout polynôme</u> $\Phi(X) \in \mathfrak{a}$ <u>est combinaison linéaire, à coefficients dans</u> K , <u>de polynôme de l'idéal</u> $\mathfrak{a}_0$ <u>engendré par la base</u> $(\dots, F_\nu, \dots)$ <u>dans</u> $k[X]$:

$$\Phi(X) = \sum_\mu \alpha_\mu \Psi_\mu(X) \qquad \alpha_\mu \in K , \ \Psi_\mu(X) \in \mathfrak{a}_0$$

En effet, Φ peut être écrit sous forme de combinaison linéaire à coefficients dans K , de polynômes de la forme

$$X_1^{e_1} \dots X_n^{e_n} F_\nu(X)$$

lesquels appartiennent à $\mathfrak{a}_0$.

2° Si

$$\Phi(X) = \sum_{\lambda=1}^{r} \beta_\lambda P_\lambda(X) \qquad P_\lambda(X) \in k[X] \tag{11}$$

<u>et où les</u> $\beta_\lambda \in K$ <u>sont linéairement indépendants sur</u> k , <u>on a</u>

$$P_\lambda(X) \in \mathfrak{a}_0$$

<u>En particulier</u> $\mathfrak{a} \cap k[X] = \mathfrak{a}_0$.

Soit $\{\ldots , G_\rho(X) , \ldots\}$, $(\rho = 1 , \ldots , m)$, un ensemble minimal de polynômes de $\mathfrak{a}_0$ tel que $\Phi(X)$ puisse s'exprimer sous la forme $\sum_\rho \gamma_\rho G_\rho$ où $\gamma_\rho \in K$; les G_ρ sont donc linéairement indépendants sur k. La relation (11) entraîne

$$(12) \qquad \sum_\rho \gamma_\rho G_\rho = \sum_\lambda \beta_\lambda P_\lambda$$

En identifiant, on obtient les relations linéaires de la forme

$$(12') \qquad L_\sigma(\gamma) = M_\sigma(\beta)$$

où les $L_\sigma(U)$, $M_\sigma(V)$ sont des formes linéaires sur k. Il ne peut y avoir plus de m formes L linéairement indépendantes (puisque ce sont des formes à m variables et il y en a exactement m , car, dans le cas contraire, les équations $L_\sigma(\gamma) = 0$ auraient au moins un système de solutions $c_\rho \in k$ non toutes nulles, et nous aurions $\sum_\rho c_\rho G_\rho = 0$ ce qui est impossible. Par conséquent, les relations (12'), compatibles puisqu'elles proviennent de (12), peuvent être résolues par rapport aux γ , ce qui donne

$$\gamma_\rho = \sum_{\lambda=1}^{r} b_{\rho\lambda} \beta_\lambda \quad \text{où} \qquad b_{\rho\lambda} \in k$$

(12) s'écrit donc

$$\sum_{\lambda=1}^{r} \beta_\lambda (P_\lambda - \sum_\rho b_{\rho\lambda} G_\rho) = 0$$

Les β étant linéairement indépendants sur k , et les polynômes $P_\lambda - \sum_\rho b_{\rho\lambda} G_\rho$ appartenant à l'anneau $k[X]$, ces polynômes doivent être identiquement nuls, d'où $P_\lambda \in \mathfrak{a}_0$. En particulier, on voit, en prenant $r = 1$, $\beta_1 = 1$, qu'un polynôme de $\mathfrak{a} \cap k[X]$ appartient à $\mathfrak{a}_0$; or, on a évidemment $\mathfrak{a}_0 \subseteq \mathfrak{a} \cap k[X]$, d'où l'égalité.

DÉMONSTRATION du théorème 6.

1° Supposons que l'idéal $\mathfrak{P}(x)/K$ ait une base dans $k[X]$. Soient β_λ des éléments de K linéairement indépendants sur k ; une relation $\sum_\lambda \beta_\lambda p_\lambda = 0$ où $p_\lambda \in k(x)$ se ramène à la forme

$$\sum_\lambda \beta_\lambda P_\lambda(x) = 0 \quad \text{où} \quad P_\lambda(X) \in k[X]$$

donc à la forme

$$\sum_\lambda \beta_\lambda P_\lambda(X) = \Phi(X) \in \mathfrak{P}(x)/K = \mathfrak{a}$$

ce qui entraîne d'après le lemme 1, $P_\lambda(X) \in \mathfrak{a}_0$, et par conséquent $P_\lambda(x) = 0$, $p_\lambda = 0$; les β_λ sont donc aussi linéairement indépendants sur

$k(x)$, et K et $k(x)$ sont linéairement disjoints sur k.

2° Inversement, supposons K et $k(x)$ linéairement disjoints sur k. Soit $\Phi(X) \in K[X]$; prenons parmi les coefficients de $\Phi(X)$ un ensemble maximal d'éléments β_λ ($\in K$) linéairement indépendants sur k. En exprimant les autres coefficients au moyen des β, nous obtenons $\Phi(X) = \sum_\lambda \beta_\lambda P_\lambda(X)$, où $P_\lambda(X) \in k[X]$. Si alors nous avons

$$\Phi \in \mathfrak{R}(x)/K = \mathfrak{a} \quad \text{c'est-à-dire} \qquad \Phi(x) = 0$$

il vient $\sum_\lambda \beta_\lambda P_\lambda(x) = 0$, d'où $P_\lambda(x) = 0$ puisque les β_λ sont aussi linéairement indépendants sur $k(x)$, c'est-à-dire

$$P_\lambda(x) \in \mathfrak{R}(x)/k = \mathfrak{a}$$

Tout polynôme de $\mathfrak{a}$ est donc une combinaison linéaire, à coefficients dans K, de polynômes de $\mathfrak{a}$; on a d'autre part, $\mathfrak{a} = \mathfrak{a} \cap k[X]$, donc $\mathfrak{a} \subseteq \mathfrak{a}$. Par conséquent, toute base de $\mathfrak{a}$ dans $k[X]$ est une base de $\mathfrak{a}$ (14)

C. Q. F. D.

Dans le même ordre d'idées, on a encore cette importante proposition.

LEMME 8. – Soit $\mathfrak{a}$ un idéal de l'anneau $K[X] = K[X_1, \ldots, X_n]$. Parmi tous les sous-corps k de K tels que $\mathfrak{a}$ ait une base dans $K[X]$, il y en a un, k_0, qui est contenu dans tous les autres. Pour que $\mathfrak{a}$ soit invariant dans un automorphisme σ de K, il faut et il suffit que σ laisse invariant tout élément de k_0 (15).

Nous renvoyons à [4] (chapitre I, lemme 2 p. 19) pour la démonstration dont le principe consiste à ordonner les modules en $X_1, \ldots, X_n$.

---

(14) On déduit immédiatement du théorème 6 le lemme 2, établi directement ci-dessus. Si $X_1, \ldots, X_n$ sont des variables indépendantes sur un sur-corps K de k, K et $k(X_1, \ldots, X_n)$ sont linéairement disjoints sur k. En effet, l'idéal $\mathfrak{R}(X)/K$ est l'idéal (0), qui a une base dans $k[X]$. Signalons encore, dans cet ordre d'idées, une proposition susceptible d'applications fréquentes. Soit $(\ldots, F_\nu(X), \ldots)$ une base pour l'idéal $\mathfrak{R}(x)/k$; $(u_1, \ldots, u_r)$ étant un ensemble de variables indépendantes sur $k(x)$, les F constituent une base pour l'idéal $\mathfrak{R}(x, u)/k$ ([4], chapitre I, corollaire du théorème 4, p. 16).

(15) On ne manquera pas de noter tout l'intérêt que présente cet énoncé en lui même ; si par exemple un idéal $\mathfrak{a}$ possède une base dans $k_1[X]$ et une base dans $k_2[X]$, il en possède une dans $k[X]$ où $k = k_1 \cap k_2$. En combinant le lemme 8 et le théorème 6 où K est regardé comme un corps fixe, on voit que si des corps k ($\subseteq K$) sont tels que K et $k(x)$ soient linéairement disjoints sur k, leur intersection a la même propriété ; (k_0 est d'ailleurs l'intersection de tous les sous-corps k ayant cette propriété).

La première partie de l'énoncé peut d'ailleurs, d'après une remarque de Henri CARTAN, se déduire aisément d'un théorème analogue sur les espaces vectoriels (BOURBAKI [1], chapitre II, paragraphe 5, n° 5, p. 67). Un sous-espace V d'un espace vectoriel E, de base (a_i) sur un corps K peut être engendré par ses éléments primordiaux (par rapport à cette base) ; et s'il est engendré par des éléments dont les composantes appartiennent à un sous-corps k de K, les éléments primordiaux ont eux-mêmes leurs composantes dans k ([4], proposition 8, p. 67). Le plus petit sous-corps de K contenant les composantes des éléments primordiaux est donc le plus petit sous-corps k_0 de K tel que V soit engendré par l'ensemble des éléments de V dont les composantes appartiennent à k_0.

Considérons alors l'idéal $\mathfrak{a}$ (lemme 8) comme un sous-espace V de l'espace vectoriel $E = K[X]$ engendré sur K par les monômes M_i en $X_1, \dots, X_n$. Comme on le voit immédiatement, <u>pour que $\mathfrak{a}$ ait une base à coefficients dans</u> k_0, $k_0 \subsetneq K$, <u>il faut et il suffit que le sous-espace vectoriel</u> $V = \mathfrak{a}$ <u>soit engendré par l'ensemble des polynômes de</u> $\mathfrak{a}$ <u>dont les "composantes", c'est-à-dire ici les coefficients, appartiennent tous à</u> k_0, <u>c'est-à-dire par les polynômes de</u> $\mathfrak{a} \cap k_0[X]$. C'est nécessaire parce que, si $\mathfrak{a} = (\dots, F_\mu, \dots)$ où $F_\mu \in k_0[X]$, la relation $F = \sum_\mu P_\mu F_\mu$ où $P_\mu = \sum_\nu \alpha_{\mu\nu} M_{\mu\nu} \in K[X]$, $\alpha_{\mu\nu} \in k$, entraîne $F_\mu = \sum_\nu \alpha_{\mu\nu} Q_{\mu\nu}$ où $Q_{\mu\nu} = M_{\mu\nu} F_\mu \in \mathfrak{a} \cap k_0[X]$; c'est suffisant, parce que $\mathfrak{a} \cap k_0[X]$, idéal dans $k_0[X]$, a, en tant qu'idéal, une base finie $(\dots, G_\mu, \dots)$; comme on suppose pour tout $F \subset \mathfrak{a}$, $F = \sum_\rho \beta_\rho H_\rho$ avec $\beta_\rho \in K$, $H_\rho \in \mathfrak{a} \cap k_0[X]$, donc $H_\rho = \sum_\mu R_{\rho\mu} G_\mu$, où $R_{\rho\mu} \in k_0[X]$, il vient

$$F = \sum_\mu \left(\sum_\rho \beta_\rho R_{\rho\mu}\right) G_\mu \quad \text{où} \quad Q_\mu = \sum_\rho \beta_\rho R_{\rho\mu} \in K[X] \;;$$

$(\dots, G_\mu, \dots)$ est bien une base pour $\mathfrak{a}$.

Dans ces conditions, d'après les propriétés rappelées ci-dessus, il existe bien un corps <u>minimum</u> k_0 tel que $\mathfrak{a}$ ait une base dans $k_0[X]$.

En prenant l'idéal $\mathfrak{R}(x)/k$ comme idéal $\mathfrak{a}$ et en tenant compte du théorème 6, on obtient la condition nécessaire et suffisante suivante.

COROLLAIRE. - <u>Pour que</u> K <u>et</u> $k(x)$ <u>soient linéairement disjoints sur</u> k, $(k \subseteq K)$, <u>il faut et il suffit que</u> k <u>contienne</u> k_0, <u>corps minimum dans lequel</u> $\mathfrak{R}(x)/K$ <u>possède une base</u>.

5. Changement du corps de définition ; théorèmes fondamentaux.

Pour aller plus loin, nous devons faire intervenir la dimension r du point générique $P = (x)$ sur le corps de définition k correspondant. Supposons, avec des notations convenables, $x_1, \dots, x_2$, algébriquement indépendants sur k, $x_{r+1}, \dots, x_n$ algébriques sur $k(x_1, \dots, x_r)$. Si K est un sur-corps de k, P n'a plus forcément la dimension r sur K, mais une dimension $r' \leqslant r$, car $x_1, \dots, x_r$ peuvent ne plus être indépendants sur K (par exemple, K peut contenir certains d'entre eux). Mais, si nous introduisons r quantités $x'_1, \dots, x'_r$ $(\in \Delta)$ algébriquement indépendantes sur K, elles le sont a fortiori sur k, et nous avons l'isomorphisme

$$\sigma : k(x_1, \dots, x_r \xrightarrow[(k)]{\sim} k(x'_1, \dots, x'_r)$$

(puisque ces deux corps sont des extensions purement transcendantes de k, de même dimension). Les fermetures algébriques de ces deux corps sont isomorphes dans un isomorphisme σ_1 prolongeant σ [16].

Posons

$$x'_{r+h} = \sigma_1 x_{r+h} \qquad (h = 1, \dots, n-r)$$

Ces quantités sont algébriques sur $k(x'_1, \dots, x'_r)$, donc a fortiori sur $K(x'_1, \dots, x'_r)$ de sorte que $K(x'_1, \dots, x'_n)$ a le degré de transcendance r sur K : le point (x') a la dimension r sur K. Or, ce point est une spécialisation générique de (x) sur k, d'après le lemme 3, paragraphe 3, puisque σ_1 induit un isomorphisme entre $k(x_1, \dots, x_n)$ et $k(x'_1, \dots, x'_n)$ appliquant x_ν sur x'_ν. Nous pouvons énoncer :

THÉORÈME 7. - Si r est la dimension du point $P = (x)$ sur k, et si K est un sur-corps quelconque de k, il y a une spécialisation générique $P' = (x')$ de P sur k, qui a la dimension r sur K ([4], chapitre II, théorème 2, p. 28 ; chapitre I, proposition 9, p. 7).

COMPLÉMENTS. - Supposons en outre que P ait un lieu V sur k, P' a aussi un lieu V sur k (théorème 2, paragraphe 3). Le théorème 7 permet d'affirmer

---

[16] C'est un théorème connu (VAN DER WAERDEN [3], paragraphe 62, p. 205, le démontre quand il s'agit de deux fermetures algébriques d'un même corps : σ est alors l'identité. Le raisonnement est susceptible de s'étendre).

que K et $k(x')$ sont algébriquement indépendants sur k ; [17]. Ils sont donc linéairement disjoints sur k, puisque $k(x')$ est une extension régulière de k, et alors $K(x')$ est aussi une extension régulière de K (théorème 3). P' a donc un lieu sur K, qui coïncide avec son lieu V sur k (théorème 5).

THÉORÈME 8. - Soit k un corps de définition pour une variété V, lieu de $P = (x)$ sur k.

1° Tout corps K contenant k est un corps de définition pour V ; tout point générique $\overline{P} = (\overline{x})$ de V sur K est un point générique de V sur k ; K et $k(\overline{x})$ sont linéairement disjoints sur k.

2° Soit k_0 le plus petit corps tel que $\mathfrak{P}(x)_k$ ait une base à coefficients dans k_0 [18] : k_0 est un corps de définition de V, et, pour qu'un corps K soit corps de définition de V, il faut et il suffit qu'il contienne k_0 ([4] chapitre IV, corollaires 2 et 3, p. 71).

1° Soit, d'après le théorème 7, P' une spécialisation générique de P sur K, ayant même dimension r sur K que P sur K. D'après les compléments au théorème 7 P' a V pour lieu sur K comme sur k. K est donc bien corps de définition pour V. Un point générique $\overline{P} = (\overline{x})$ quelconque de V sur K est une spécialisation générique de P' sur K, donc a fortiori sur k. C'est bien un point générique de V sur k. $\overline{P}$ a, comme P', la dimension r sur K et sur k (remarque paragraphe 3 ; nous voyons ici que $\dim_k P = \dim_K \overline{P}$ lorsque $k \leq K$; le cas tout à fait général sera examiné plus loin). Il en résulte que $k(\overline{P})$ et K sont algébriquement indépendants sur k, donc aussi linéairement disjoints.

2° L'idéal $\mathfrak{P}(x)_k$ ayant par hypothèse une base dans $k_0[X]$, k et $k_0(x)$ sont linéairement disjoints sur k_0 (théorème 6), donc $k_0(x)$ est une extension régulière de k_0 (théorème 4) et le lieu de $P = (x)$ sur k_0 coïncide avec V : k_0 est un corps de définition pour V. C'est le plus petit sous-corps de k ayant cette propriété. Si en effet $k' \subseteq k$ en est un autre, nous pouvons construire un point $O' = (x')$, point générique de V sur k comme sur k' ;

---

[17] Dans le cas contraire, ρ quantités $u_1, \dots, u_\rho$ de $k(P')$, algébriquement indépendantes sur k, (d'où $\rho \leq r$), seraient algébriquement dépendantes sur K. P' étant la dimension r sur k, soient $v_{\rho+1}, \dots, v_r$ des quantités de $k(P')$ telles que $u_1, \dots, u_\rho, v_{\rho+1}, \dots, v_r$ soient algébriquement indépendantes sur k : tout élément de $k(P')$, en particulier tout x', dépend algébriquement des u et des v sur k, donc aussi (a fortiori) sur K : comme les u sont algébriquement dépendants sur K, on voit que le degré de transcendance de $K(x')$ sur K serait inférieur à r.

[18] Cf. lemme 8 ci-dessus. WEIL désigne ce corps de définition minimum de V par $k_0 = \mathrm{def}(V)$.

$k(x')$ et k' sont linéairement disjoints sur k' (théorème 7 et compléments). Par conséquent, $\mathfrak{N}(x)_k$ a une base dans $k'[X]$, (théorème 6), ce qui entraîne que k' contient k_0 (lemme 8).

Soit enfin K un corps de définition de V, non contenu dans k. Formons le corps K_0 de K et de k_0. Contenant K, K_0 est aussi corps de définition pour V. Parmi les corps de définition contenus dans K_0, il y en a un, k_0', qui est <u>minimum</u> : nous avons donc

$$(13) \qquad k_0' \subseteq k_0 \qquad \text{et} \qquad k_0' \subseteq K$$

puisque k_0 et K sont des corps de définition contenus dans K_0. Mais, d'après (13), k_0' est un corps de définition contenu dans k, et comme k_0 est le plus petit, nous avons nécessairement

$$k_0 = k_0' \subseteq K$$

C. Q. F. D.

Indiquons enfin trois résultats importants concernant la <u>dimension</u>, les <u>pseudo-points</u>, et les <u>équations</u> d'une variété.

<u>Dimensions</u>. - Nous avons vu que, lorsqu'un corps de définition K en contient un autre k, on a : $\dim_K \overline{P} = \dim_k P$, $\overline{P}$ étant un point générique sur K, P un point générique sur k. Remplaçons k par k_0 : nous voyons, en tenant compte de la seconde partie du théorème 8, qu'un point générique quelconque de V sur un corps de définition K quelconque a, sur K, la même dimension r qu'un point générique P_0 sur k_0. <u>La dimension</u> r <u>d'une variété est donc un élément géométrique attaché à cette variété</u>, c'est-à-dire invariant dans les changements de corps de définition et de points génériques. On écrit $V = V^r$, ou $r = \dim V$ pour indiquer que la dimension de V est r.

<u>Pseudo-points</u>. - Si une variété V est le lieu de P sur k, et d'autre part de P' sur k', <u>les spécialisations infinies de</u> P <u>sur</u> k <u>sont aussi les mêmes que celles de</u> P' <u>sur</u> k' (pour les spécialisations finies, cela résulte de la définition même d'une variété); P et P' sont aussi points génériques de V sur $k_0 = \mathrm{def}(V)$ ils sont donc spécialisations génériques l'un de l'autre sur k_0 (théorème 2, paragraphe 3) : c'est-à-dire qu'ils ont mêmes spécialisations sur k_0. D'autre part, les spécialisations finies de P sur k sont les mêmes que celles de P sur k_0 (théorèmes 5 et 8) et, par réciprocité cela s'étend aux spécialisations infinies. De même, les spécialisations de P' sur

k' sont les mêmes que celles de P' sur k_0, donc finalement, les mêmes que celles de P sur k. L'ensemble de points et de pseudo-points qui sont spécialisations sur un corps de définitions quelconque k, d'un point générique sur k quelconque, constituent ce que WEIL appelle l'ensemble attaché à V.

Equations. - THÉORÈME 9. - Soit $F_\mu(X) = 0$ un système d'équations pour une variété V définie sur k.

1° Tout corps k' contenant les coefficients des polynômes $F_\mu(X)$ est un corps de définition pour V

2° $F_\mu(X) = 0$ est un système d'équations pour V sur k' ([4], chapitre IV, corollaire 5, p. 71).

1° Soit π le sous-corps premier de k, $a_{\mu\nu}$ les coefficients des $F_\mu(X)$: $\mathfrak{P}(x)_k$ a une base, $(\ldots, F_\mu, \ldots)$ dans le corps $\pi(\ldots, a_{\mu\nu}, \ldots) \subseteq k'$

2° $k_1 = k \cap k'$ contient k_0 : k_1 est donc un corps de définition pour V. Soit (x) un point générique de V sur un corps K contenant k et k' : c'est aussi un point générique sur k, k' et k_1 (théorème 8, 1°). Soient $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}_1$ les idéaux déterminés par ce point (x) sur k, k' et k_1. La base $(\ldots, F_\mu, \ldots)$ de $\mathfrak{P}$ est une base de $\mathfrak{P}_1$ puisque nous avons $F_\mu \in k_1[X]$ et $\mathfrak{P}_1 = \mathfrak{P} \cap k_1[X]$ d'après le théorème 8 (qui s'applique puisque k et $k_1(x)$ sont linéairement disjoints sur k_1). $\mathfrak{P}$ a aussi une base dans $k_1[X]$, formée de polynômes de $\mathfrak{P}_1$: ceux-ci s'expriment au moyen des F_μ, et comme les F_μ appartiennent évidemment à $\mathfrak{P}'$, les F_μ constituent bien une base de $\mathfrak{P}'$.

COROLLAIRE. - Coïncidence de deux variétés définies respectivement par les couples (k, P) et (k', P').

Soient $P = (x)$ un point ayant un lieu V sur un corps k, et $P' = (x')$ un point ayant un lieu V' sur un corps k'. On a $V = V'$ si et seulement si les idéaux $\mathfrak{P}(x)/k$ et $\mathfrak{P}(x')/k'$ ont une base commune. ([4], chapitre IV, corollaire 6, p. 72).

Posons $k_1 = k \cap k'$. Si $V = V'$, k_1, intersection de deux corps de définition contient le corps de définition minimum, donc est un corps de définition. Toute base de l'idéal définissant V sur k_1, est, d'après le théorème précédent, une base commune.

Inversement, si $\mathfrak{P}(x)/k$ et $\mathfrak{P}(x')/k'$ ont une base commune $(\ldots , F_\mu , \ldots)$, celle-ci appartient à $k_1[X]$ et k_1 est corps de définition pour V et V' (théorème 9), qui sont définies sur k_1 par les mêmes équations $F_\mu = 0$ (voir paragraphe 3) et par conséquent, coïncident.

D'après le théorème 9, on peut parler d'un <u>système d'équations</u> pour une variété sans préciser le corps de définition : celui-ci sera n'importe quel corps contenant les coefficients de ces équations. (Bien entendu, cela ne veut pas dire que n'importe quel système d'équations définit une variété-lieu sur un corps contenant les coefficients : voir les remarques 1 et 2, à la fin du paragraphe 3). Nous voyons ainsi que les variétés-lieux sont un cas particulier des variétés-S , définies à partir d'un système d'équations comme nous l'avons indiqué sommairement dans l'introduction (b).

Nous allons donc maintenant étudier directement les propriétés les plus fondamentales des variétés-S , ce qui nous donnera en particulier de nouvelles propriétés des variétés-L , par exemple celle-ci : <u>si une variété-L</u> , V , <u>est contenue dans une autre,</u> V' , <u>on a</u> $\dim V \leq \dim V'$, <u>avec l'égalité seulement</u> si $V = V'$. Les démonstrations de telles propriétés pour les variétés-L se trouvent dans [4] ; nous ne les donnons pas pour éviter les répétitions. Nous renvoyons également à [4] pour la construction des variétés-S plus générales que les variétés-L , à partir de celles-ci, au moyen de la <u>réunion</u>: ce sont les unions ou "bouquets" de variétés (bunchs of varieties).

N.B. - Bien que nous ayons donné un certain nombre de démonstrations pour montrer la nature des méthodes, l'exposé précédent ne doit pas être regardé comme ayant un caractère déductif. En particulier, les lemmes que nous avons volontairement rapprochés des théorèmes qui semblent les avoir suggérés, devraient, dans une exposition systématique et rigoureuse, être reportés plus en avant de façon à précéder toutes leurs applications. Pour plusieurs d'entre eux, l'une de ces applications est précisément la démonstration de l'équivalence des deux définitions des extensions régulières, que nous avons laissée de côté pour simplifier.

BIBLIOGRAPHIE

[1] BOURBAKI (Nicolas). - Algèbre, Chapitre II : Algèbre linéaire, 2e éd. - Paris, Hermann, 1955 (Act. scient. et ind., 1032-1236 ; Eléments de Mathématique, 6).

[2] HAUPT (O.), NÖBELING (G.) und PAUC (C.). - Über Abhängigkeitsräume, J. für die reine und ang. Math., t. 181, 1939, p. 193-217.

[3] VAN DER WAERDEN (B.L.). - Moderne Algebra, I., 3e éd. - Berlin, Springer, 1950 (Die Grundlehren der mathematischen Wissenschaften, 33).

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