Séminaire Dubreil.
Algèbre et théorie
des nombres

Paul Dubreil

Variétés algébriques, III

Séminaire Dubreil. Algèbre et théorie des nombres, tome 2-3 (1948-1950), exp. n° 3, p. 1-20

<http://www.numdam.org/item?id=SD_1948-1950__2-3__A3_0>

Faculté des Sciences de Paris
-:-:-:-
Séminaire A. CHÂTELET et P. DUBREIL
(ALGÈBRE et THÉORIE DES NOMBRES)
Années 1948-1950
-:-:-:-

VARIÉTÉS ALGÉBRIQUES, III,

par Paul DUBREIL

C. DÉFINITION ET PROPRIÉTÉS FONDAMENTALES DES VARIÉTÉS (S).

1. Points abstraits, variétés (S).

K désignant un corps commutatif, et n un entier positif, nous considérons sous le nom de points abstraits les systèmes $(x_1, \dots, x_n)$ de n éléments x_ν appartenant à K ou à telle ou telle extension finie K' de K. Le mot "abstrait", introduit par ZARISKI et qui pourra être sous-entendu, est destiné à rappeler que les x_ν n'appartiennent pas nécessairement à K lui-même ; les points dont les coordonnées sont dans K constituent l'espace cartésien C_K^n.

Nous désignerons par $X_1, \dots, X_n$, n variables indépendantes sur K, par $A = K[X_1, \dots, X_n] = K[X]$ l'anneau des polynômes en $X_1, \dots, X_n$ à coefficients dans K. Un système d'équations algébriques sur K est un système de la forme

$$(1) \qquad \begin{cases} F_1(X_1, \dots, X_n) = 0 \\ \dots \\ F_r(X_1, \dots, X_n) = 0 \end{cases} \qquad \text{où} \quad F_\nu \in A$$

Un point-solution du système (1) est un point abstrait $(x_1, \dots, x_n)$ tel que $F_\nu(x_1, \dots, x_n) = 0$ $(\nu = 1, \dots, r)$. Les points ayant cette propriété constituent, par définition, la variété algébrique définie sur K par le système (1) : une variété définie par ce procédé, c'est-à-dire au moyen des solutions d'un système, sera dite variété (S).

Cas remarquables.

a. le système (1) est incompatible (par exemple $1 = 0$). On dira qu'il définit encore une variété, et que celle-ci est la variété vide, $\emptyset$.

b. le système (2) se réduit à des identités $(0 = 0)$. On dira qu'il définit la variété à n dimensions, ou variété ambiante S^n : celle-ci joue, comme nous le verrons, le rôle d'un espace dans lequel tout est plongé.

c. Tout idéal $\mathfrak{m}$ de l'anneau A possède, d'après le théorème de Hilbert, une base finie :

$$\mathfrak{m} = (F_1 , \dots , F_r)$$

Les équations $F_\lambda = 0$ définissent sur K une variété S . Si $(G_1 , \dots , G_s)$ est une autre base de $\mathfrak{m}$, toute solution du système $F_\lambda = 0$ est une solution du système $G_\mu = 0$ et inversement, puisque

$$F_\lambda = \sum_\rho P_{\lambda\rho} G_\rho \quad \text{et} \quad G_\mu = \sum_\tau Q_{\mu\tau} F_\tau$$

où $P_{\lambda\rho}\ Q_{\mu\tau} \in A$.

On a ici un exemple de systemes équivalents au sens strict, et la variété S ainsi définie, qui ne dépend que de l'idéal $\mathfrak{m}$, sera appelée variété de $\mathfrak{m}$ et désignée par $\mathcal{S}(\mathfrak{m})$. Pour qu'un point $(x_1 , \dots , x_n)$ appartienne à $\mathcal{S}(\mathfrak{m})$, il faut et il suffit que l'on ait $F(x_1 , \dots , x_n) = 0$ pour tout $F \in \mathfrak{m}$.

Il est clair que des idéaux distincts peuvent avoir même variété (19), par exemple

$$(x_1^2 , x_2) , \quad (x_1 , x_2^2) , \quad (x_1 , x_2)$$

ou encore $\mathfrak{m}$ et $\mathfrak{m}^\alpha$.

Toute variété définie sur K comme solution d'un système (1) peut être regardée comme la variété d'un idéal $\mathfrak{m}$ de A : à savoir $\mathfrak{m} = (F_1 , \dots , F_r)$.

Parmi les idéaux $\mathfrak{m}$ dont la variété est une variété S donnée, il y en a un qui est maximum. En effet, l'ensemble $\mathfrak{J}(S)$ de tous les polynômes de A nuls en tout point abstrait appartenant à S , contient n'importe quel idéal $\mathfrak{m}$ ayant S pour variété. $\mathfrak{J}(S)$ est lui-même un idéal. En fin, les premiers membres F_λ des équations (1) définissant S appartiennent à $\mathfrak{J}(S)$: donc un point non situé sur S , c'est-à-dire en lequel un au moins des F_λ n'est pas nul, n'appartient pas à la variété de $\mathfrak{J}(S)$. Celle-ci coïncide donc avec S (qu'elle contient évidemment) : $\mathcal{S}(\mathfrak{J}(S)) = S$. L'idéal $\mathfrak{J}(S')$ est appelé idéal associé (ou attaché) à la variété S . Un tel idéal n'est pas

(19) Nous supposons connues les règles élémentaires du calcul des idéaux. Voir par exemple VAN DER WAERDEN [5], paragraphes 19 et 20, p. 59-65, [6], paragraphes 90, 91 et 92, p. 18-30, ou DUBREIL [2], chapitre IV, p. 179-219.

quelconque : si $F^{\alpha} \in \mathfrak{J}(S)$, F lui-même est nul en tout point de S , donc $F \in \mathfrak{J}(S)$ de sorte que $\mathfrak{J}(S)$ coïncide avec son radical [20]. Par conséquent si S est défini par le système (1), $\mathfrak{J}(S)$ peut très bien être distinct de l'idéal $(F_1 , \dots , F_r)$.

(Exemple : $F_\lambda = (\Phi_\lambda)^{\alpha}$ où α est un entier >0 : on a

$$(F_1 , \dots , F_r) \subset (\Phi_1 , \dots , \Phi_r) \subseteq \mathfrak{J}(S) .$$

Soit $\mathfrak{m}$ un idéal, $\mathfrak{S}(\mathfrak{m})$ sa variété, $\mathfrak{J}(\mathfrak{S}(\mathfrak{m}))$ l'idéal attaché à celle-ci, on a

$$\mathfrak{m} \subseteq \mathfrak{J}(\mathfrak{S}(\mathfrak{m})) .$$

Soit F un polynôme de $\mathfrak{r}(\mathfrak{m})$, radical de $\mathfrak{m}$: $F^{\rho} \in \mathfrak{m}$, donc $F^{\rho} = 0$ en tout point de $S(\mathfrak{m})$, donc aussi $F = 0$, d'où $F \in \mathfrak{J}(\mathfrak{S}(\mathfrak{m}))$ et par conséquent

$$(\mathfrak{m} \subseteq)\ \mathfrak{r}(\mathfrak{m}) \subseteq \mathfrak{J}(\mathfrak{S}(\mathfrak{m}))$$

Nous verrons plus loin (paragraphe 4) comme application du théorème des zéros de Hilbert, qu'on a en fait l'égalité

$$\mathfrak{r}(\mathfrak{m}) = \mathfrak{J}(\mathfrak{S}(\mathfrak{m}))$$

ce qui, en prenant pour $\mathfrak{m}$ un idéal premier $\mathfrak{p}$, $\mathfrak{p} = \mathfrak{r}(\mathfrak{p})$, donnera

$$\mathfrak{p} = \mathfrak{J}(\mathfrak{S}(\mathfrak{p})) .$$

Plus généralement, soit E un ensemble de points abstraits : l'ensemble $\mathfrak{J}(E)$ des polynômes de l'anneau A nuls en tout point de E est un idéal. La variété S de $\mathfrak{J}(E)$ contient E . Soit S' une variété algébrique, définie sur K , contenant E : S' est définie par un système d'équations $G_1 = 0 , \dots , G_s = 0$ vérifié par tout point de E . Donc $G_\mu \in \mathfrak{J}(E)$, $(G_1 , \dots , G_s) \subseteq \mathfrak{J}(E)$ et par conséquent $S' \supseteq S$: $S = \mathfrak{S}\,\mathfrak{J}(E)$ est la plus petite variété algébrique définie sur K et contenant l'ensemble E .

d. Regardons K comme sous-corps d'un domaine universel Δ : à une variété L lieu d'un point $P = (x)$ sur K correspond l'idéal $\mathfrak{R}(x)/K = (F_1 , \dots , F_r)$ avec $F_\lambda \in A$. Les équations $F_\lambda = 0$ définissent sur K une variété S . Un point $(y) = (y_1 , \dots , y_n)$ au sens de Weil (les y_n sont des quantités, c'est-à-dire des éléments de Δ) est aussi un point abstrait puisque

---

[20] L'ensemble des éléments d'un anneau A dont une puissance appartient à à un idéal $\mathfrak{m}$, est lui-même un idéal, appelé radical de $\mathfrak{m}$ et désigné par $\mathfrak{r}(\mathfrak{m})$. Un idéal qui coïncide avec son radical est dit parfois semi-premier.

$K(y_1, \dots, y_n)$ est une extension finie de K, et nous savons qu'une condition nécessaire et suffisante pour qu'un tel point (y) appartienne à L est qu'il vérifie les équations $F_\lambda = 0$, c'est-à-dire qu'en tant que point abstrait il appartienne à S : à toute variété L correspond ainsi une variété S. De plus l'idéal $\mathfrak{R}(x)/K$ est l'idéal $\mathfrak{J}(S)$ associé à S. Soit en effet $\Phi \in \mathfrak{J}(S)$ un polynôme nul en un point de S ; il est nul en particulier au point générique (x) de L, donc $\Phi \in \mathfrak{R}(x)/K$ et $\mathfrak{J}(S) \subseteq \mathfrak{R}(x)/K$. L'inclusion opposée étant évidente, puisque $F_\lambda \in \mathfrak{J}(S)$, nous avons bien

$$\mathfrak{J}(S) = \mathfrak{R}(x)/K \tag{3}$$

2. Inclusion des variétés. Intersection et réunion. Variétés réductibles et irréductibles.

Soient S et S' deux variétés définies sur le même corps K, respectivement par les systèmes (1) et

$$\left\{\begin{array}{l} G_1 = 0 \\ \dots \\ G_s = 0 \end{array}\right. \tag{1'}$$

Si tout point de S est un point de S', c'est-à-dire si tout solution de (1), dans une extension finie K' de K, est une solution de (1'), on dit que S est contenue dans S', ou en est une sous-variété :

$$S \subseteq S'.$$

S est véritable sous-variété de S', $S \subset S'$, si S est contenue dans S' sans être vide, ni coïncider avec S', au moins un point abstrait de S' n'est pas un point de S.

Si l'on a $S \subseteq S'$ et $S' \subseteq S$, S et S' coïncident, c'est-à-dire sont une seule et même variété : on écrira $S = S'$.

On a $\emptyset \subseteq S \subseteq S^n$ quelle que soit la variété S.

La relation $S \subseteq S'$ entraîne $\mathfrak{J}(S) \supseteq \mathfrak{J}(S')$, l'égalité entre les idéaux n'ayant lieu que si $S = S'$.

La relation $m_1 \subseteq m_2$ entraîne $\mathcal{S}(m_1) \supseteq \mathcal{S}(m_2)$ puisqu'un point abstrait annulant tout polynôme de m_2 annule en particulier tout polynôme de m_1.

Si V et W sont deux variétés (L), lieux respectivement de (x) et de (y) sur K, et si $V \subseteq W$ au sens de l'inclusion des variétés (L), tout polynôme de $\mathfrak{R}(y)/K$ est nul au point (x) de W, donc on a

$$(4) \qquad \mathfrak{P}(x)/K \supseteq \mathfrak{P}(y)/K$$

Appelons S et T les variétés (S) correspondant à V et W : (4) s'écrit d'après (3)

$$\mathfrak{J}(S) \supseteq \mathfrak{J}(T)$$

d'où, en prenant les variétés des deux membres

$$S \subseteq T$$

Une inclusion entre variétés (L) entraîne donc la même inclusion entre les variétés (S) correspondantes.

Soient S_1 et S_2 deux variétés définies sur K par les systèmes (1) : $F_\lambda = 0$, et (1') : $G_\mu = 0$. Le système formé par (1) et (1') définit sur K une <u>variété algébrique</u> I, appelée <u>intersection</u> de S_1 et de S_2 :

$$I = S_1 \cap S_2$$

On a évidemment $I \subseteq S_1$, $I \subseteq S_2$ et toute variété I' contenue dans S_1 et S_2 est contenue dans I puisque tout point de I' vérifie (1) et (1'). Si $S_1 \subseteq S_2$, on a $I = S_1$. On définit de proche en proche l'intersection d'un nombre fini quelconque de variétés algébriques.

Considérons dans l'anneau A, deux idéaux quelconques

$$\mathfrak{m}_1 = (F_1, \ldots, F_r), \quad \mathfrak{m}_2 = (G_1, \ldots, G_s).$$

Comme $\mathfrak{m}_1 + \mathfrak{m}_2 = (F_1, \ldots, F_r, G_1, \ldots, G_s)$, nous avons

$$\mathfrak{S}(\mathfrak{m}_1 + \mathfrak{m}_2) = \mathfrak{S}(\mathfrak{m}_1) \cap \mathfrak{S}(\mathfrak{m}_2)$$

En particulier, S_1 et S_2 étant 2 variétés, la variété de $\mathfrak{J}(S_1) + \mathfrak{J}(S_2)$ est $S_1 \cap S_2$, d'où $\mathfrak{J}(S_1) + \mathfrak{J}(S_2) \subseteq \mathfrak{J}(S_1 \cap S_2)$.

<u>Il est essentiel de remarquer qu'on peut très bien ne pas avoir l'égalité</u>. <u>Exemple</u> :

$$n = 2 \qquad S_1 : x = 0 \qquad S_2 : y^2 - x = 0 .$$

Nous avons

$$S_1 \cap S_2 = (0, 0) \qquad (S_1, S_2) = (x, y)$$

tandis que

$$\mathfrak{J}(S_1) + \mathfrak{J}(S_2) = (x) + (y^2 - x) = (x, y^2).$$

A partir des équations (1) et (1') définissant S_1 et S_2 formons maintenant le système

$$F_\lambda G_\mu = 0 \qquad (\lambda = 1, \dots, r ; \mu = 1, \dots, s)$$

Nous définissons ainsi, sur K, une variété algébrique R, contenant S_1 et S_2. Inversement, si un point (x) de R n'appartient pas à S_1, par exemple, on a $F_\lambda(x) \neq 0$ pour au moins une valeur de λ, donc, $G_\mu(x) = 0$ pour $\mu = 1, \dots, s$ et (x) est un point de S_2. Les points de R étant ceux de S_1 et ceux de S_2, et ceux-là seulement, R est appelée <u>réunion</u> de S_1 et de S_2 :

$$R = S_1 \cup S_2$$

Toute variété algébrique contenant S_1 et S_2 contient R ; si $S_1 \subseteq S_2$ on a $R = S_2$. On définit aisément la réunion d'un nombre quelconque de variétés algébriques ; les règles du calcul habituel des intersections et réunions sont valables, par exemple

$$S \cap (S_1 \cup S_2) = (S \cap S_1) \cup (S \cap S_2)$$

(tout point de la variété qui est au premier membre est un point de celle qui est au second membre, et inversement ; on peut aussi établir cette égalité au moyen d'un système d'équations).

Avec les mêmes notations que plus haut, nous avons

$$\mathfrak{m}_1 \cdot \mathfrak{m}_2 = (F_1 G_1, \dots, F_\lambda G_\mu, \dots, F_r G_s)$$

donc

$$S(\mathfrak{m}_1 \cdot \mathfrak{m}_2) = S(\mathfrak{m}_1) \cup S(\mathfrak{m}_2) .$$

Or nous avons

$$(\mathfrak{m}_1 \cap \mathfrak{m}_2)^2 \subseteq \mathfrak{m}_1 \cdot \mathfrak{m}_2 \subseteq \mathfrak{m}_1 \cap \mathfrak{m}_2$$

donc

$$S(\mathfrak{m}_1 \cap \mathfrak{m}_2) = S(\mathfrak{m}_1 \cdot \mathfrak{m}_2) = S(\mathfrak{m}_1) \cup S(\mathfrak{m}_2) .$$

En particulier, la variété de $\mathfrak{J}(S_1) \cap \mathfrak{J}(S_2)$ est $S_1 \cup S_2$, d'où

$$\mathfrak{J}(S_1) \cap \mathfrak{J}(S_2) \subseteq \mathfrak{J}(S_1 \cup S_2)$$

Mais $\mathfrak{J}(S_1 \cup S_2)$, contenu dans $\mathfrak{J}(S_1)$ et dans $\mathfrak{J}(S_2)$ l'est dans leur intersection, donc :

$$\mathfrak{J}(S_1 \cup S_2) = \mathfrak{J}(S_1) \cap \mathfrak{J}(S_2) .$$

Une variété S définie sur K, est réductible ou décomposée sur K si elle est, au moins d'une façon, la réunion de deux véritables sous-variétés définies sur K

$$S = S_1 \cup S_2 \quad \text{avec} \quad \begin{cases} \emptyset \subset S_1 \subset S \\ \emptyset \subset S_2 \subsetneq S \end{cases}$$

Dans le cas contraire, S est irréductible sur K.

LEMME 9. - Si une variété S, irréductible sur K, est contenue dans la réunion de deux variétés S_1, S_2 elle est contenue au moins dans l'une d'elles.

L'hypothèse $S \subseteq S_1 \cup S_2$ entraîne

$$S = S \cap (S_1 \cup S_2) = (S \cap S_1) \cup (S \cap S_2) \tag{5}$$

Si l'on avait par exemple $S \cap S_1 = \emptyset$, il viendrait $S = S \cap S_2$ donc $S \subseteq S_2$, la proposition serait établie. Supposons donc $S \cap S_1 \neq \emptyset$ et $S \cap S_2 \neq \emptyset$. Si S n'était contenue ni dans S_1 ni dans S_2, $S \cap S_1$ et $S \cap S_2$ seraient de véritables sous-variétés de S, qui, d'après (5) serait décomposée sur K.

REMARQUE. - La proposition s'étend immédiatement à la réunion d'un nombre fini quelconque de variétés.

THÉORÈME 10. - Pour qu'une variété S définie sur K, soit irréductible sur K, il faut et il suffit que l'idéal associé $\mathfrak{J}(S)$ soit premier dans l'anneau $A = K[X_1, \dots, X_n]$.

1° Supposons V irréductible sur K. Si $F_1 \in A$, $F_2 \in A$ et $F_1 F_2 \in \mathfrak{J}(S)$, S est contenue dans la réunion des variétés $F_1 = 0$, $F_2 = 0$, donc, d'après le lemme 9, dans une au moins de ces variétés : l'un au moins des polynômes F_1, F_2 appartient donc à l'idéal $\mathfrak{J}(S)$, et celui-ci est premier.

2° Supposons S réductible sur K. $S = S_1 \cup S_2$ avec $\emptyset \subset S_1 \subset S$ et $\emptyset \subset S_2 \subset S$. On a $\mathfrak{J}(S_1) \supset \mathfrak{J}(S)$ et $\mathfrak{J}(S_2) \supset \mathfrak{J}(S)$, (l'égalité étant exclue). Soient F_1, F_2 deux polynômes de A tels que

$$F_i \in \mathfrak{J}(S_i) \qquad F_i \notin \mathfrak{J}(S) \qquad (i = 1, 2).$$

On a

$$F_1 F_2 \in \mathfrak{J}(S_1) \cap \mathfrak{J}(S_2) = \mathfrak{J}(S_1 \cup S_2) = \mathfrak{J}(S)$$

donc $\mathfrak{J}(S)$ n'est pas premier.

CONSÉQUENCE. - Considérons une variété L *lieu de* (x) *sur* K , et la variété S correspondante : on a $\mathfrak{J}(S) = \mathfrak{P}(x)/K'$ où l'idéal $\mathfrak{P}(x)/K$ est *premier* ; S *est donc irréductible sur* K .

REMARQUE. - Si $\mathfrak{p}$ est un idéal premier quelconque de A , il ne résulte pas du théorème 10 que la variété $\mathcal{S}(\mathfrak{p})$ est irréductible sur K : cela résultera de ce théorème et de l'égalité $\mathfrak{p} = \mathfrak{J}(\mathcal{S}(\mathfrak{p}))$, qui sera établie aux paragraphes 4 et 5, et exprime que $\mathfrak{p}$ *est l'idéal associé à sa propre variété*.

3. Décomposition d'une variété en variétés irréductibles.

Sans utiliser d'autres moyens que les définitions fondamentales et le théorème de la base finie, on peut établir l'importante proposition suivante ([21]) :

THÉORÈME 11 (*Théorème de décomposition*). - *Toute variété algébrique* S , *définie par un système d'équations sur un corps* K , *est la réunion d'un nombre fini de variétés irréductibles*.

Si S n'est pas la réunion d'un nombre fini de variétés irréductibles sur K , elle n'est pas elle-même irréductible, et nous avons

$$S = S_1 \cup S_1'$$

où S_1 , S_1' sont deux variables sous-variétés dont une, au moins, n'est pas la réunion d'un nombre fini de variétés irréductibles, donc

$$S_1 = S_2 \cup S_2'$$

et une au moins des deux sous-variétés véritables S_2 , S_2' de S_1 n'est pas la réunion d'un nombre fini de variétés irréductibles, etc. On aurait donc au moins une chaîne strictement décroissante, et infinie, de variétés

$$S \supset S_1 \supset S_2 \supset \dots$$

circonstance qui est impossible d'après le lemme suivant.

LEMME 10. - *Dans toute une chaîne décroissante de variétés*

$$V_1 \supseteq V_2 \supseteq \dots \supseteq V_n \supseteq V_{n+1} \supseteq \dots$$

toutes les variétés coïncident à partir d'un certain rang.

([21]) Cf. [7], paragraphe 1, p. 360, ou [8], paragraphe 28, p. 107.

C'est ce lemme qui se démontre au moyen du théorème de la base finie, que nous énoncerons ici de la façon suivante : dans tout sous-ensemble M non vide de $A = K[X_1, \ldots, X_n]$ il existe des polynômes $F_1, \ldots, F_n$ ($\in M$) tels que tout polynôme $F \in M$ soit de la forme ([22])

$$F = P_1 F_1 + \ldots + P_h F_h \quad \text{où} \quad P_\lambda \in A$$

Soit M l'ensemble des polynômes premiers membres des équations définissant les différentes variétés V_i : les polynômes de M s'expriment tous au moyen d'un nombre fini d'entre eux, $F_1, \ldots, F_h$. Soit V la variété définie par $F_1 = \ldots = F_h = 0$. Quel que soit n, on a $V \subseteq V_n$. Si d'autre part, n_i est la plus petite valeur de n telle que $F_i = 0$ soit une des équations définissant V_n, V_{n_i} et par conséquent V_m pour $m \geq n_i$ sont contenues dans la variété définie par l'unique équation $F_i = 0$. Si $N = \mathrm{Max}(n_1, \ldots, n_h)$, V_m, pour $m \geq N$, est contenue dans chacune des variétés $F_1 = 0, \ldots, F_h = 0$, donc dans leur intersection, qui est V : nous avons donc $V = V_m$, pour $m \geq N$,

C. Q. F. D.

REMARQUE. - D'une façon complètement différente et moins élémentaire le théorème précédent peut aussi se déduire de la décomposition d'un idéal en idéaux primaires et du fait que la variété d'un idéal premier, donc d'un idéal primaire, est irréductible.

THÉORÈME 12 (Théorème d'unicité). - Soient

$$S = I_1 \cup I_2 \cup \ldots \cup I_r = J_1 \cup J_2 \cup \ldots \cup J_s$$

deux décompositions réduites de S en variétés irréductibles (c'est-à-dire telles qu'aucune variété irréductible y figurant ne soit contenue dans la réunion des autres variétés figurant dans le même membre). On a $r = s$, et avec

---

([22]) En fait, cet énoncé est celui de HILBERT. Il se ramène à l'énoncé maintenant classique "tout idéal $\mathfrak{m}$ de A possède une base finie" en introduisant précisément l'idéal $\mathfrak{m}$ engendré par M. Tout F de M est un élément de $\mathfrak{m}$, or $\mathfrak{m}$ possède une base finie, $\mathfrak{m} = (G_1, \ldots, G_R)$, où chaque G_μ, d'après la définition de $\mathfrak{m}$, est une combinaison : $\sum_i P_{i\mu} F_{i\mu}$ d'un nombre fini de polynômes de M. Par suite, tout polynôme $F \in M$ est bien une combinaison des polynômes $F_{i\mu}$, qui sont en nombre fini.

des notations convenables $I_\lambda = J_\lambda$.

D'après le lemme 9, I_1, contenue dans la réunion des variétés irréductibles $J_1, \ldots, J_s$ est contenue au moins dans l'une d'elles : par exemple, $I_1 \subseteq J_1$. Mais J_1 est de même contenue dans une des variétés figurant au premier membre $J_1 \subseteq I_\lambda$. Si λ était différent de 1, I_1 serait superflue, c'est-à-dire contenue dans $I_2 \cup \ldots \cup I_\lambda \cup \ldots \cup I_r$. Nous avons donc $I_1 = J_1$. A chaque variété I correspond donc une variété J qui lui est égale, et inversement ; le théorème en résulte.

4. Idéaux premiers et variétés irréductibles, théorème des zéros de Hilbert, applications.

Nous avons établi plus haut la relation

$$\mathfrak{r}(\mathfrak{m}) \subseteq \mathfrak{Z}(S(\mathfrak{m}))$$

pour tout idéal $\mathfrak{m}$ de l'anneau $A = K[X_1, \ldots, X_n]$; le théorème des zéros de Hilbert permet de montrer que l'on a l'égalité entre les deux idéaux $\mathfrak{r}(\mathfrak{m})$ (radical de $\mathfrak{m}$) et $\mathfrak{Z}(S(\mathfrak{m}))$ (idéal associé à la variété de $\mathfrak{m}$). Mais le théorème des zéros de Hilbert se rattache aussi à un autre ordre d'idées : L étant un sur-corps de K, nous avons vu qu'une variété (S) définie sur K n'est pas, en général, déterminée par l'ensemble $\{S\}_L$ de ses points situés dans l'espace cartésien C_L^n : elle l'est cependant quand L est la fermeture algébrique $\overline{K}$ de K. Ce fait, que l'étude directe de quelques cas simples permet de constater facilement, résulte du théorème de Hilbert.

Désignons, pour simplifier, par $\overline{T} = \{S(\mathfrak{m})\}_{\overline{K}}$ la trace de la variété $S(\mathfrak{m})$ sur l'espace $C_{\overline{K}}^n$, dont l'ensemble des points $S(\mathfrak{m})$ dont les coordonnées sont dans $\overline{K}$. L'ensemble $\mathfrak{Z}(\overline{T})$ des polynômes de A nuls en tout point de $\overline{T}$ est un idéal contenant $\mathfrak{Z}(S(\mathfrak{m}))$:

$$\mathfrak{Z}(S(\mathfrak{m})) \subseteq \mathfrak{Z}(\overline{T})$$

Or le théorème des zéros de Hilbert exprime que

$$\mathfrak{Z}(\overline{T}) \subseteq \mathfrak{r}(\mathfrak{m})$$

puisqu'il s'énonce :

THÉORÈME 13 (*Théorème de Hilbert*). - *Si un polynôme* F *s'annule en tout point de la trace* $\overline{T}$ *de* $S(\mathfrak{m})$, *une puissance de* F *appartient à* $\mathfrak{m}$. On voit que ce théorème entraîne les conséquences suivantes.

1° *On a l'égalité*

$$\mathfrak{r}(\mathfrak{m}) = \mathfrak{J}(S(\mathfrak{m}))$$

2° Soient S_1, S_2 deux variétés définies sur K, que nous pouvons regarder comme les variétés d'idéaux $\mathfrak{m}_1$, $\mathfrak{m}_2$ de l'anneau A. Si S_1 et S_2 ont la même trace sur l'espace $S^n_{\overline{K}}$, $\overline{T}_1 = \overline{T}_2$, on a $S_1 = S_2$. En effet, la relation $\overline{T}_1 \subseteq \overline{T}_2$, par exemple, entraîne que tout polynôme de $\mathfrak{m}_2$ est nul sur $\overline{T}_1$, donc d'après le théorème, a une puissance contenue dans $\mathfrak{m}_1$. Il en résulte, en considérant une base de $\mathfrak{m}_2$, qu'une puissance $\mathfrak{m}_2^\alpha$ de $\mathfrak{m}_2$ est contenue dans $\mathfrak{m}_1$, d'où $S_2 = S(\mathfrak{m}_2^\alpha) \supseteq S_1$. *Une variété* S *définie sur* K *est déterminée par sa trace sur l'espace* $C^n_{\overline{K}}$.

DÉMONSTRATION *du théorème des zéros de Hilbert*. - La démonstration de Hilbert ([3]) était fort compliquée. VAN DER WAERDEN a donné deux démonstrations (paragraphe 85, p. 6 et paragraphe 101, p. 60, ainsi que p. 55 et p. 49). La première utilise une élégante remarque de A. RABINOVITSCH ([4]) d'après laquelle le cas général se ramène à celui où $\overline{T}$ est *vide* (voir ci-dessous) mais ce dernier cas est traité par l'élimination, ce qui est encore bien compliqué. Nous laisserons de côté la deuxième démonstration donnée par VAN DER WAERDEN, parce qu'elle se rattache à une théorie des variétés algébriques présentée dans un ordre entièrement différent de celui que nous suivons ici, et dans laquelle le théorème des zéros de Hilbert joue un rôle moins important.

R. BRAUER a donné récemment ([1]) une démonstration directe extrêmement élémentaire. ZARISKI, peu de temps avant, en avait donné deux ([9]). Nous reproduirons la première démonstration de ZARISKI parce que, tout en restant élémentaire, elle est particulièrement instructive. Elle se décompose en trois étapes.

1° LEMME de Rabinovitsch. - Il suffit de montrer que $\overline{T} = \emptyset$ *entraîne* $\mathfrak{m} = A$.

Supposons en effet ce point établi, et soit $F \in \mathfrak{J}(\overline{T})$. Si F est le polynôme 0, n'importe quelle puissance de F appartient à l'idéal donné $\mathfrak{m} = (F_1, \dots, F_r)$. Soit donc $F(X_1, \dots, X_n) \neq 0$. Adjoignons une variable Z : les polynômes $F_1, \dots, F_r$, $1 - ZF$ de l'anneau $K[X_1, \dots, X_n, Z]$ n'ont aucun zéro commun à coordonnées dans $\overline{K}$: nous avons donc, d'après l'hypothèse faite,

$$(F_1 , \ldots , F_r , 1 - ZF) = K[X_1 , \ldots , X_n , Z] = A'$$

d'où en particulier

$$1 = P_1 F_1 + \ldots + P_r F_r + Q(1 - ZF) \quad \text{où} \quad P_\lambda , Q \in A' .$$

Remplaçons l'indéterminée Z, qui ne figure pas dans $F_1 , \ldots , F_r$, par $\frac{1}{F(X_1, \ldots, X_n)}$ et rendons l'équation entière en multipliant par une puissance convenable de F : il vient

$$F^\rho = A_1 F_1 + \ldots + A_r F_r \qquad \text{avec} \qquad A_\lambda \in A$$

C. Q. F. D.

2° Pour montrer que $\overline{T} = \emptyset$ entraîne $m = A$, il suffit d'établir le

LEMME de Zariski. - Si un domaine d'intégrité $R_n = K[\xi_1 , \ldots , \xi_n]$ fini sur K est un corps, ce corps est une extension algébrique de K.

Supposons en effet le lemme de Zariski établi, et montrons que, si m est un idéal différent de $A = (1)$, on a $\overline{T} \neq \emptyset$.

Dans l'ensemble des idéaux distincts de A et contenant m, il y a au moins un idéal $\mathfrak{p}$ maximal (ou sans diviseurs) (23) ; l'anneau quotient $R_n = A/\mathfrak{p}$ est un corps, et c'est aussi un anneau d'intégrité fini sur K : $R_n = K[\xi_1 , \ldots , \xi_n]$, où ξ_ν désigne la classe module $\mathfrak{p}$ à laquelle appartient X_ν. Ce corps étant, d'après le lemme de Zariski, une extension algébrique de K, les ξ_ν sont algébriques sur K et $\xi = (\xi_1 , \ldots , \xi_n)$ est un point à coordonnées dans $\overline{K}$ en lequel tout polynôme de $\mathfrak{p}$, donc a fortiori tout polynôme de m, est nul : $\xi \in \overline{T} \neq \emptyset$.

3° Démonstration du lemme de Zariski. - La proposition est immédiate si $n = 1$: $K[\xi_1]$ étant un corps, $\frac{1}{\xi_1} \in K[\xi_1]$ donc $\frac{1}{\xi_1} = f(\xi_1)$, $f(X_1)$ étant un polynôme à coefficients dans K, ξ_1 est donc racine de l'équation $Xf(X) - 1 = 0$, par conséquent est algébrique sur K. Supposons donc la proposition vraie pour un domaine d'intégrité de rang $n - 1$ sur un corps K', et soit $R_n = K[\xi_1 , \ldots , \xi_n]$ un domaine d'intégrité de rang n sur K, dont nous supposons qu'il est un corps. Nous pouvons écrire $R_n = K(\xi_1)[\xi_2 , \ldots , \xi_n]$ et par conséquent R_n, de rang $n - 1$ sur $K(\xi_1)$, est une extension algébrique

---

(23) L'existence de cet idéal maximal $\mathfrak{p}$ résulte de l'application du théorème de Zorn au principe de l'ensemble maximal.

de $K(\xi_1)$: <u>le lemme sera établi si nous montrons que</u> ξ_1 <u>est algébrique sur</u> K.

L'élément ξ_i $(i = 1, \dots, n)$ est racine d'une équation $f_i(X) = 0$ de degré m_i à coefficients dans $K[\xi_1]$: soit b_i $(i = 2, \dots, n)$ le coefficient du terme de plus haut degré dans $f_i(X)$. Pour tout élément ω de R_n, il existe un entier ρ tel que le produit $\omega(b_2 b_3 \dots b_n)^\rho$ soit une combinaison linéaire, à coefficients dans $K[\xi_1]$, des $m_2 m_3 \dots m_n$ monômes $\xi_2^{j_2} \dots \xi_n^{j_n}$ vérifiant $0 \leq j_i \leq m_i - 1$.

Soit ν le degré du corps $R_n = K[\xi_1, \dots, \xi_n] = K(\xi_1, \dots, \xi_n)$ sur son sous-corps $K(\xi_1)$ et soit $\omega_1 = 1, \omega_2, \dots, \omega_\nu$ une base linéaire de R_n sur $K(\xi_1)$ formée d'éléments linéairement indépendants. On peut trouver dans $K[\xi_1]$ un élément $b_1 \neq 0$ tel que dans l'expression de chacun des éléments $b_1\, \xi_2^{j_2} \dots \xi_n^{j_n}$: sous forme de combinaison linéaire de $\omega_1, \dots, \omega_\nu$ avec coefficients dans $K(\xi_1)$, le coefficient de ω_1 $(= 1)$ soit dans $K[\xi_1]$. Posons

$$b = b_1\, b_2 \dots b_n \qquad (b \neq 0,\ \ b \in K[\xi_1])$$

Pour tout élément $\omega \in R_n$, on a

$$\omega\, b^\rho = a_1 + a_2\, \omega_2 + \dots + a_\nu\, \omega_\nu$$

où $a_1 \in K[\xi_1]$ et $a_i \in K(\xi_1)$ $(i = 2, \dots, \nu)$ puisque $\omega(b_2 \dots b_n)^\rho$ est une combinaison linéaire à coefficients dans $K[\xi_1]$, des monômes $\xi_2^{j_2} \dots \xi_n^{j_n}$ $(0 \leq j_i \leq m_i - 1)$ dont le produit par b_1, a fortiori par b_1^ρ, a la propriété précédente.

Soit alors ζ un élément <u>non nul</u> quelconque de $K[\xi_1]$; prenons $\omega = \frac{1}{\zeta}$. Puisque $b^\rho \omega = \frac{b^\rho}{\zeta} \in K(\xi_1)$, nous avons nécessairement $a_2 = \dots = a_\nu = 0$, car autrement $1 = \omega_1, \omega_2, \dots, \omega_\nu$ ne seraient pas linéairement indépendants sur $K(\xi_1)$. Nous avons donc $b^\rho = a_1 \zeta$ de sorte que <u>tout élément</u> ζ <u>non nul de</u> $K[\xi_1]$ <u>divise une puissance</u> d'un élément fixe $b \in K[\xi_1]$. Il est par suite impossible que $K[\xi_1]$ soit un anneau de polynômes à une indéterminée sur K, et ξ_1 est algébrique sur K,

C. Q. F. D.

5. Idéaux premiers, point général, point générique ; dimensions.

Soit $\mathfrak{p}$ un idéal premier de l'anneau $A = K[X_1, \dots, X_n]$; nous supposons $\mathfrak{p} \neq A$ et nous formons l'anneau des classes résiduelles modulo $\mathfrak{p}$, que nous désignons par $R[\mathfrak{p}]$ ou $R[S]$. Appelons ξ_λ la classe contenant le polynôme X_λ, ξ_λ est l'image de X_λ dans l'homomorphisme

$$(\sigma) : A \longrightarrow A/\mathfrak{p} = R[S]$$

et un polynôme quelconque $F(X_1, \dots, X_n) \in A$ a pour image l'élément $F(\xi_1, \dots, \xi_n)$ de $A/\mathfrak{p}$, de sorte que nous avons

$$A/\mathfrak{p} = K[\xi_1, \dots, \xi_n]$$

Comme $\mathfrak{p}$ constitue la classe zéro, les relations

$$F(X_1, \dots, X_n) \in \mathfrak{p} \quad \text{et} \quad F(\xi_1, \dots, \xi_n) = 0$$

sont équivalentes.

Or, dans l'homomorphisme (σ), deux éléments distincts de K, regardés comme éléments de A, ont des images distinctes dans $A/\mathfrak{p}$ (autrement, on dirait $\mathfrak{p} = A$). Donc K est contenu dans le domaine d'intégrité $A/\mathfrak{p}$ et par conséquent dans son corps des quotients $\Sigma = K(\xi_1, \dots, \xi_n)$. Les ξ_ν appartiennent donc à une extension finie, Σ, de K : $(\xi_1, \dots, \xi_n)$ est un point abstrait, μ, et nous avons obtenu le théorème suivant.

THÉORÈME 14 (VAN DER WAERDEN). - Pour qu'un polynôme $F(X_1, \dots, X_n)$ appartienne à l'idéal premier $\mathfrak{p}$ il faut et il suffit que F s'annule au point $\mu = (\xi_1, \dots, \xi_n)$, que nous appellerons point général de l'idéal $\mathfrak{p}$, ou de la variété $S(\mathfrak{p})$.

REMARQUE. - La construction précédente du point général (ou zéro général) de l'idéal $\mathfrak{p}$ n'est qu'une généralisation du procédé de l'adjonction symbolique pour la construction des nombres algébriques.

Le théorème 14 exprime que l'idéal $\mathfrak{J}(\mu)$, ensemble des polynômes nuls au point μ, est l'idéal $\mathfrak{p}$:

$$\mathfrak{J}(\mu) = \mathfrak{p}$$

Comme $\mu \in S(\mathfrak{p})$, nous avons $\mathfrak{J}(\mu) \supseteq \mathfrak{J}(S(\mathfrak{p}))$ c'est-à-dire $\mathfrak{p} \supseteq \mathfrak{J}(S(\mathfrak{p}))$. Or nous savons (paragraphe 1), que $\mathfrak{p} \subseteq \mathfrak{J}(S(\mathfrak{p}))$: nous retrouvons donc, indépendamment du théorème des zéros de Hilbert, l'égalité fondamentale

$$\mathfrak{p} = \mathfrak{J}(S(\mathfrak{p}))$$

et, en posant $S = S(\mathfrak{p})$, nous avons l'égalité

$$\mathfrak{J}(\mu) = \mathfrak{J}(S) \quad (= \mathfrak{p})$$

D'une façon générale, cherchons maintenant à quelle condition il existe un point abstrait $M = (x_1 , \dots , x_n)$ tel que l'on ait

$$\mathfrak{J}(M) = \mathfrak{J}(S)$$

S désignant une variété définie sur un corps K , et a priori quelconque. Or l'égalité précédente équivaut aux deux inclusions

a. $\mathfrak{J}(M) \supseteq \mathfrak{J}(S)$, c'est-à-dire M est un point de S

b. $\mathfrak{J}(M) \supseteq \mathfrak{J}(S)$, c'est-à-dire : un polynôme nul en M est nul en tout point M' de S .

Un point M ayant les deux propriétés précédentes sera appelé point générique de la variété S . (On n'impose pas ici la condition supplémentaire que $K(x_1 , \dots , x_n)$ soit une extension régulière de K , qui intervenait dans la théorie de WEIL).

L'idéal $\mathfrak{J}(M)$ étant, visiblement, premier, $\mathfrak{J}(S)$ ne peut lui être égal que s'il est lui-même premier, et alors S est irréductible sur K : une variété S qui possède un point générique est irréductible.

THÉORÈME 15 (théorème d'unicité (24)). - Si $M = (x)$ et $M' = (x')$ sont deux points génériques d'une variété S définie sur K , les corps $K(x)$ et $K(x')$ sont isomorphes sur K .

On a en effet $\mathfrak{J}(M) = \mathfrak{J}(M')$: c'est-à-dire que M' est spécialisation générique de M sur K , et il suffit d'appliquer lemme 3 (dans lequel la régularité de $K(x)$ n'intervient pas).

Enfin, si nous nous donnons un point abstrait $M = (x_1 , \dots , x_n)$ dont les coordonnées appartiennent à une certaine extension de K , mais sans supposer nécessairement que $K(x)$ est une extension régulière de K (de sorte qu'on aura des résultats moins précis que ceux de WEIL), l'idéal $\mathfrak{J}(M)$ dans $A[X_1 , \dots , X_n]$ est un idéal premier $\mathfrak{p}$, qui a une certaine variété $S = S(\mathfrak{p})$. Nous avons

---

(22) Cf. B.L. VAN DER WAERDEN paragraphe 24, p. 111.

$$\mathfrak{J}(M) = \mathfrak{p} = \mathfrak{J}(S(\mathfrak{p}))$$

donc S est irréductible sur K et M en est un point générique. Nous dirons encore que S est le lieu de M. A cette variété S correspond une variété (L) au sens de Weil si en outre $K(x)$ est une extension régulière de K. Alors, si (ξ) désigne le point général de S, $K(\xi)$ est aussi une extension régulière de K, puisque $K(\xi)$ et $K(x)$ sont isomorphes sur K : il en est ainsi toutes les fois que K est algébriquement fermé.

La dimension d d'un idéal premier $\mathfrak{p}$ de l'anneau A ou de la variété S, irréductible sur K, correspondante, est le degré de transcendance du corps $K(x_1, \dots, x_n)$ où $M = (x_1, \dots, x_n)$ est un point générique quelconque de S. On a évidemment $0 \leq d \leq n$.

THÉORÈME 16 ([8], p. 113). - Soient $\mathfrak{p}$, $\mathfrak{p}'$, deux idéaux premiers de A, de dimensions d et d', dont les variétés sont S et S'. Si $\mathfrak{p} \subseteq \mathfrak{p}'$, ou, ce qui revient au même, $S \supseteq S'$, on a $d \geqslant d'$ et l'égalité $d = d'$ n'a lieu que si $\mathfrak{p} = \mathfrak{p}'$.

Soient $M = (x_1, \dots, x_d, \dots, x_n)$, $M' = (x'_1, \dots, x'_{d'}, \dots, x'_n)$ des points génériques de S et S', les notations étant telles que $x'_1, \dots, x'_{d'}$ soient algébriquement indépendants sur K. Alors $x_1, \dots, x_{d'}$ le sont aussi car $\varphi(x_1, \dots, x_{d'}) = 0$, où $\varphi(X_1, \dots, X_{d'}) \in K[X_1, \dots, X_{d'}]$ et $\neq 0$, entraînerait $\varphi(X_1, \dots, X_{d'}) \in \mathfrak{p} \subseteq \mathfrak{p}'$, donc $\varphi(x'_1, \dots, x'_{d'}) = 0$ ce qui est absurde. Les d' éléments $x_1, \dots, x_{d'}$ étant algébriquement indépendants sur K, nous avons bien $d \geqslant d'$. Nous pouvons d'ailleurs supposer les notations telles que $x_1, \dots, x_d$ soient algébriquement indépendants sur K, et le corps $\sum = K(x_1, \dots, x_n)$ est une extension algébrique de $K(x_1, \dots, x_n)$ est une extension algébrique de $K(x_1, \dots, x_d)$.

Si $d = d'$, et si nous avions $\mathfrak{p} \subset \mathfrak{p}'$ (strictement), il existerait au moins un polynôme $G(X_1, \dots, X_n) \in \mathfrak{p}'$ et n'appartenant pas à $\mathfrak{p}$, donc tel que $g' = G(x'_1, \dots, x'_n)$ et $g = G(x_1, \dots, x_n) \neq 0$. Or $g \in \sum$ vérifie une équation algébrique de la forme

$$p_0 g^r + \dots + p_r = 0$$

où $p_\lambda = P_\lambda(x_1, \dots, x_d)$ avec $P_\lambda \in K[X_1, \dots, X_d]$ et nous pouvons supposer $p_r \neq 0$. Le polynôme $P_0 G^r + \dots + P_r$ appartient à $\mathfrak{p}$, donc à $\mathfrak{p}'$, d'où, puisque $g' = 0$, $P_r(x'_1, \dots, x'_d) + 0$ ce qui contredit l'indépendance de $x'_1, \dots, x'_{d'}$ sur K.

COROLLAIRE. - Tout point Q de S a une dimension $d' \leq d$ sur K, et, si $d' = d$, Q est un point générique de S. Il suffit de remarquer que la variété S' lieu de Q est contenue dans S.

Cas particuliers.

1° La variété ambiante S^n, dont l'idéal $\mathfrak{Z}(S^n)$ est l'idéal (0), et dont le point général est le point $(X_1, \dots, X_n)$ dont toutes les coordonnées sont des indéterminées, a la dimension n.

2° Tout idéal premier principal $\mathfrak{p} = (F) \neq A$ et $\neq (0)$ a la dimension $n - 1$, car on a une équation unique entre les coordonnées du point général, cette équation n'est pas une identité et une au moins des coordonnées y figure effectivement.

Inversement, soit $\mathfrak{p} = (F_1, \dots, F_h)$ un idéal premier de A, de dimension $n - 1$. Si F_1 n'est irréductible sur K, au moins un facteur irréductible F_1^* de F_1 appartient à $\mathfrak{p}$ (25). En posant $F_1 = F_1^* \Phi_1$, nous avons

$$\mathfrak{p} = (F_1^* \Phi_1, F_2, \dots, F_h) \subseteq (F_1^*, F_2, \dots, F_h) \subseteq \mathfrak{p}$$

donc

$$\mathfrak{p} = (F_1^*, F_2, \dots, F_h) \supseteq (F_1^*) .$$

Or (F_1^*) est un idéal premier de dimension $n - 1$, comme $\mathfrak{p}$: on a donc l'égalité $\mathfrak{p} = (F_1^*)$.

3° L'idéal premier $\mathfrak{Z}(a)$ associé à un point $a = (a_1, \dots, a_n)$ dont les coordonnées appartiennent à K, a la dimension 0. Le point a est en effet définie par les équations

$$X_\lambda - a_\lambda = 0 \qquad (\lambda = 1, \dots, n)$$

Il est point générique de cette variété qui ne comprend pas d'autre point ; or on a $K(a_1, \dots, a_n) = K$, donc $d = 0$.

Inversement, si K est algébriquement fermé, un idéal premier de dimension 0, dans $A = K[X_1, \dots, X_n]$ a une variété $S(\mathfrak{p})$ réduite à un point dont les coordonnées appartiennent à K. Les coordonnées $(\xi_1, \dots, \xi_n)$ du point général μ de $\mathfrak{p}$ sont algébriques sur K puisque $d = 0$, donc appartiennent à $K = \overline{K}$. Comme $\mathfrak{p} = \mathfrak{Z}(\mu)$, la variété de $\mathfrak{p}$ se réduit au point μ.

---

(25) L'existence d'un tel facteur résulte des propositions classiques sur la factorisation dans les anneaux de polynômes ; voir par exemple DUBREIL [2] chapitre VI, n° 1, 2 et 5.

Si K n'est pas algébriquement fermé, tout point M de $S(\mathfrak{p})$ a ses coordonnées dans $\overline{K}$, car un tel point a sur K une dimension au plus égale à d, et $d = 0$. M est donc point générique de S, d'après le corollaire du théorème 16. Il peut y avoir plusieurs tels points, mais alors, ils engendrent, d'après le théorème 15, des corps isomorphes sur K : ce sont des points conjugués sur K. Par conséquent, toute variété irréductible sur K et de dimension 0, est un système de points de l'espace $C^n_{\overline{K}}$, conjugués par rapport à K.

EXEMPLE. - Prenons $n = 1$, $K = \Gamma$, corps des nombres rationnels, $\mathfrak{p} = (X^2 - 2)$. Nous avons $A/\mathfrak{p} = \Gamma(\sqrt{2})$. L'idéal $\mathfrak{p}$ est premier sur $K = \Gamma$, puisque $X^2 - 2$ est irréductible sur Γ ; la variété $S(\mathfrak{p})$, irréductible sur Γ, est de dimension 0 et se compose des deux points $x = \sqrt{2}$ et $x = -\sqrt{2}$ dans $\overline{K}$.

6. Extension du corps fondamental.

Considérons une variété S définie sur un corps K par des équations $F_\lambda = 0$ $(\lambda = 1, \dots, r)$ où $F_\lambda \in K[X_1, \dots, X_n]$. Si L désigne un surcorps de K, les mêmes équations $F_\lambda = 0$ définissent sur L une variété que nous désignerons par S_L. L'exemple ci-dessus montre que, S étant irréductible, S_L peut se décomposer (sur L). Si, S étant irréductible, S_L l'est aussi quel que soit $L \supseteq K$, S est dite absolument irréductible. On a à ce sujet le théorème suivant.

THÉORÈME 17. - Si S est une variété irréductible sur K, de dimension d la variété S_L, où L est un sur-corps de K, est la réunion de variétés irréductibles, toutes de dimension d, conjuguées par rapport à K. Il suffit d'effectuer une extension algébrique finie, convenable, Λ, de K, pour obtenir une variété S_Λ qui soit réunion de variétés absolument irréductibles. (Cf. [8], paragraphe 31, en particulier Satz 5 p. 123. La démonstration donnée par VAN DER WAERDEN repose sur la théorie de l'élimination).

Ce théorème entraîne visiblement l'important corollaire suivant.

COROLLAIRE. - Pour qu'une variété S définie et irréductible sur K soit absolument irréductible, il faut et il suffit que $S_{\overline{K}}$ soit irréductible sur $\overline{K}$. En particulier, toute variété S définie et irréductible sur un corps algébriquement fermé, est absolument irréductible.

En fait, cette proposition se rattache immédiatement à la théorie de Weil. La condition du corollaire étant évidemment nécessaire, supposons S irréductible sur K et $S_{\overline{K}}$ irréductible sur $\overline{K}$.

Soit $\bar{\mu} = (\bar{\xi}_1 , \dots , \bar{\xi}_n)$ le point général de $S_{\bar{K}}$: $\bar{K}$ étant algébriquement fermé, $\bar{K}(\bar{\xi})$ est une extension régulière de $\bar{K}$ et le lieu $S_{\bar{K}}$ de $\bar{\mu}$ sur $\bar{K}$ est une variété-lieu au sens de Weil, $S_{\bar{K}} = V$. L'idéal

$$\mathfrak{P}(\bar{\xi})/\bar{K} = \mathfrak{J}(S_{\bar{K}})$$

a même base que $\mathfrak{J}(S)$, donc a une base dans $K[X_1 , \dots , X_n]$: K <u>est un corps de définition de</u> V . (Cf. théorème 8).

S est par suite <u>absolument irréductible</u>. Soit en effet L un sur-corps de K . C'est aussi un corps de définition pour V et on peut trouver un point (x) qui soit point générique de V sur L et sur K (théorème 7). Nous avons

$$\mathfrak{J}(S) = \mathfrak{P}(x)/K \qquad \mathfrak{J}(S_L) = \mathfrak{P}(x)/L$$

or l'idéal $\mathfrak{P}(x)/L$ est premier, quel que soit L ; S_L est donc irréductibble et S est absolument irréductible.

Dans l'exemple placé à la fin du paragraphe 5, nous avons une variété irréductible sur Γ qui n'est pas absolument irréductible. Le corps $K(\xi) = \Gamma(\sqrt{2})$ n'est pas ici une extension régulière de Γ , <u>parce que</u> Γ n'est pas algébriquement fermé dans $\Gamma(\sqrt{2})$.

Donnons maintenant un <u>exemple</u> montrant que d'autres accidents peuvent se produire dans l'extension du théorème fondamental, quand le corps $K(\xi)$ engendré par le point général n'est pas une extension régulière de K .

Un champ de Galois étant un corps parfait et toute extension algébrique d'un corps parfait étant séparable prenons, pour obtenir un exemple d'extension inséparable une extension transcendante simple $k(u)$ du corps <u>premier</u> k de caractéristique p ($\neq 0$). L'élément $v = \sqrt[p]{u}$ est algébrique sur $k(u) = K$, et <u>aucun des éléments</u> v^m , pour $m = 1 , \dots , p-1$ <u>n'appartient à</u> K . En effet une relation de la forme

$$v^m = \frac{a_0 u^r + \dots}{b_0 u^s + \dots} \qquad (r \geq 0 , \quad s \geq 0) \quad a_0 , \dots , b_0 , \dots , \in k$$

entraînerait, en élevant le puissance p :

$$u^m(b_0^p u^{ps} + \dots) = a_0^p u^{pr} + \dots$$

ce qui exigerait $m + ps = pr$; or, p étant premier ceci est impossible pour les valeurs de m considérées.

Le polynôme

$$X^p - u = X^p - v^p = (X - v)^p \in k[X] \ .$$

se décompose en facteurs linéaires sur le corps $L = K(v)$, donc ne pourrait avoir comme facteurs irréductibles sur K que des polynômes de la forme $(X - v)^m$ $(m = 1 , \dots , p - 1)$: comme le terme constant $\pm v^m$ n'appartient pas à K , $X^p - u = 0$ définit sur K une variété irréductible S . Sur $L = K(v)$, cette équation s'écrit $(X - v)^p = 0$: S_L se réduit au point $x = v$, et est encore une variété irréductible. Mais alors que $\mathfrak{J}(X)$ a pour base $(X^p - u)$, $\mathfrak{J}(S_L)$ a pour base $(X - v)$ (On rapprochera d'ailleurs cette circonstance du théorème 6)

BIBLIOGRAPHIE

[1] BRAUER (Richard). - A note on Hilbert's Nullstellensatz, Bull. Amer. math. Soc., t. 54, 1948, p. 894-896.

[2] DUBREIL (Paul). - Algèbre, Tome I. - Paris, Gauthier-Villars, 1954 (Cahiers scientifiques, 20).

[3] HILBERT (David). - Über die Theorie der algebraischen Formen, Math. Annalen, t. 36, 1890, p. 473-534.

[4] RABINOVITCH (J.L.). - Zum Hilbertschen Nullstellensatz, Math. Annalen, t. 102, 1929, p. 520.

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

[6] VAN DER WAERDEN (B.L.). - Algebra, II., 3e éd. - Berlin, Springer, 1955 (Die Grundlehren der mathematischen Wissenschaften, 34).

[7] VAN DER WAERDEN (B.L.). - Zur algebraischen Geometrie, XIII : Vereinfachte Grundlagen des algebraischen Geometrie, Math. Annalen, t. 115, 1937, p. 359-378.

[8] VAN DER WAERDEN (B.L.). - Einführung in die algebraische Geometrie. - Berlin, Springer, 1939 (Die Grundlehren der mathematischen Wissenschaften, 51).

[9] ZARISKI (O.). - A new proof of Hilbert's Nullstellensatz, Bull. Amer. math. Soc., t. 53, 1947, p. 362-368.