BULLETIN DE LA S. M. F.

FRANÇOIS CHÂTELET

Essais de géométrie galoisienne

Bulletin de la S. M. F., tome 74 (1946), p. 69-86

<http://www.numdam.org/item?id=BSMF_1946__74__69_0>

ESSAIS DE GÉOMÉTRIE GALOISIENNE;

PAR M. FRANÇOIS CHÂTELET.

Dans un précédent Mémoire (1), j'ai exposé les éléments d'une géométrie dans un corps abstrait quelconque en définissant les êtres géométriques : points, transformations, idéaux, variétés, correspondances, . . . à coefficients dans ce corps et en établissant leur propriétés les plus simples. Ce premier Mémoire était destiné à préparer une question plus difficile, dont je vais m'occuper maintenant et qui peut être appelée *étude de la géométrie algébrique à la manière de Galois*, ou plus brièvement géométrie galoisienne.

On sait les importants travaux faits par E. Galois sur le sujet suivant : chercher la façon la plus simple d'obtenir un nombre défini par une relation algébrique. C'est une étude analogue pour les êtres géométriques et non plus numériques que j'aborde ici.

Le premier problème d'une telle étude peut être énoncé de la façon suivante : reconnaître si un élément géométrique défini dans une extension finie d'un corps quelconque ρ peut être aussi défini dans le corps de base ρ. L'intérêt de ce problème est que certains êtres géométriques de ρ possèdent, dans une extension convenable de ρ, des propriétés de nature *algébrique* plus simples que les propriétés *arithmétiques* de cet être dans ρ, et qu'il est plus facile de remonter des propriétés algébriques aux propriétés arithmétiques que d'aborder directement les secondes. C'est le passage des premières aux secondes que permet la solution du problème galoisien énoncé plus haut.

Le premier chapitre du Mémoire présent est consacré à ce problème galoisien. Dans un second chapitre, j'utilise les résultats obtenus pour former les *équations d'équivalence*, qui m'ont

(1) *Annales de l'Université de Lyon*, année 1945.

permis, dans mon mémoire de thèse ([2]), de résoudre d'importants problèmes diophantiens.

L'intérêt de la géométrie galoisienne semble bien ne pas se limiter aux considérations suivantes et j'espère avoir l'occasion d'y revenir ultérieurement.

I. — CRITÈRES DE GALOIS.

Aprés un bref rappel des propriétés classiques des extensions finies et séparables d'un corps ρ ([3]), j'aborde la comparaison des êtres géométriques du corps ρ avec les êtres géométriques de ses extensions finies et séparables; ce qui me conduit aux critères de Galois pour les êtres géométriques, généralisations de propriétés classiques des nombres algébriques.

1. Les extensions finies et séparables. — Une *extension* ([4]), ou un sur-corps, du corps de base ρ est un corps k qui contient tous les éléments de ρ. L'extension est *algébrique*, par rapport à ρ, si chacun de ses éléments est zéro d'un polynome *irréductible* d'une seule variable $F(x)$, $G(x)$, ... à coefficients dans ρ défini à un facteur près de proportionnalité. L'extension est finie, par rapport à ρ, si elle peut être engendrée par des êtres (ou des symboles) en nombre fini α, β, ...; chaque être de l'extension s'exprime en fonction rationnelle, à coefficients dans ρ, des êtres de base α, β, ... Toute extension finie de ρ est algébrique.

Il existe une extension Ω de ρ, *l'extension algébriquement fermée*, définie à une isomorphie près par les propriétés suivantes : Ω est une extension algébrique de ρ; il n'existe pas d'extension algébrique de Ω autre que Ω elle-même, c'est-à-dire que tout poly-

---

([2]) *Ann. École Norm. sup.*, année 1944.

([3]) Dans les deux mémoires cités le corps de base est désigné par la lettre grecque majuscule P.

([4]) La notion d'extension, conçue d'un point de vue arithmétique, a été exposée en France, suivant les idées de Kronecker, par MM. Borel et Drach, d'après des leçons de J. Tannery (*Introduction à la théorie des nombres et à l'algèbre supérieure*). En plus de son intérêt philosophique, cette conception a l'avantage de s'appliquer à tout corps ρ (même fini) et notamment aux domaines de Galois qui font l'objet d'une importante étude dans les leçons de Tannery. Pour les résultats plus récents, je renvoie encore à l'*Encyclopédie*, édition française (I.10) et à la *Moderne Algebra* de Van der Waerden.

nome $F(x)$ d'une seule variable et à coefficients dans Ω a au moins un zéro, ou racine, dans Ω. Une isomorphie entre deux corps est une correspondance biunivoque entre les éléments de ces corps qui respecte la somme et le produit; elle respecte la « structure » d'un corps, donc le transforme en un corps qui n'en diffère que par l'aspect et qu'il n'y a aucun inconvénient théorique à assimiler au corps primitif. Dans l'extension algébriquement fermée Ω de ρ, on peut trouver un sous-corps isomorphe à une extension finie arbitrairement choisie de ρ.

Une extension finie k de ρ est *séparable*, si aucun des polynomes irréductibles $F(x), G(x), \ldots$ annulés par ses éléments n'a de racine multiple dans k. Une extension finie et séparable de ρ peut être engendrée par adjonction à ρ d'un être *unique* θ qui est appelé *élément primitif* de l'extension (théorème de Galois) ([5]). Inversement, si un polynome à coefficients dans ρ est irréductible et sans racine multiple, un « symbole » annulant ce polynome définit une extension finie et séparable de ρ.

Le degré n d'un polynome $F(x)$ caractérisant un élément primitif θ est le *degré* de k; les n symboles distincts, zéros de ce polynome, sont les *conjugués, par rapport à* ρ, de θ. Je les désigne par

$$\theta^{(i)} = \theta_i \qquad \begin{cases} i = 1, 2, \ldots, n, \\ \theta_n \text{ étant égal à } \theta. \end{cases}$$

Le corps k est *normal*, si tous les conjugués d'un élément primitif et, par suite, de tout élément de ce corps sont dans k. J'envisage, en même temps que k, *son corps normal* K, obtenu par adjonction à ρ des n symboles θ_i; il est confondu avec k si ce corps est normal. Si k est séparable, K l'est aussi et peut être engendré par un élément primitif Θ, dont chaque θ_i est alors une fonction rationnelle à coefficients dans ρ. Les conjugués Θ_i de Θ par rapport à ρ sont dans K, donc sont des fonctions rationnelles à

([5]) Si ρ est de caractéristique nulle, c'est-à-dire si les multiples $m.\varepsilon$ de son unité ε sont tous différents de o, toute extension finie de ρ est nécessairement séparable; si ρ est de caractéristique p (nombre premier, c'est-à-dire s'il contient un corps isomorphe au corps des restes d'entiers rationnels, module p), une extension non séparable de ρ contient au moins un élément qui est zéro d'un polynome en x^p. Voir à ce sujet la *Moderne Algebra* de Van der Waerden, tome I, chapitre V.

coefficients dans ρ de Θ et chacun est primitif. Ils définissent le groupe de Galois Γ de k formé par les substitutions

$$\sigma = \text{substitution transformant } \Theta \text{ en } \Theta_1.$$

L'application d'une substitution σ à un élément α de K est obtenue en exprimant α en fonction rationnelle à coefficients dans ρ de Θ, puis en remplaçant, dans cette fonction, Θ par Θ_1, enfin en exprimant Θ_1 en fonction rationnelle, à coefficients dans ρ, de Θ. On obtient ainsi une fonction rationnelle, à coefficients dans ρ, de Θ; donc un élément de K que l'on désigne par $\sigma(\alpha)$, *transformé de* α *par* σ.

Les substitutions σ qui laissent inchangé θ forment un sous-groupe γ de Γ. On peut répartir les éléments de Γ en classes à droite $S^{(i)}$ par rapport à γ; la classe $S^{(i)}$ est alors constituée par celles des substitutions σ qui transforment θ en son conjugué θ_i. Toutes les substitutions de la classe $S^{(i)}$ font correspondre, à un élément α de k, un même élément de K qui est le *$i^{ième}$ conjugué de α par rapport à* ρ et que je désigne par $\alpha^{(i)}$. Les $i^{èmes}$ conjugués des éléments de k sont les éléments du corps $k^{(i)}$, contenu dans K, engendré par adjonction de θ_i à ρ.

Plus généralement, si une extension k' de ρ, contenue dans k, est engendrée par un élément θ' de k, les substitutions σ de Γ, qui laissent inchangé θ', forment un sous-groupe Γ' de Γ contenant γ; le sous-groupe Γ' est *associé* à l'extension k'. Inversement à un tel sous-groupe Γ' de Γ contenant γ, *correspond* une extension unique k' (finie et séparable) de ρ contenue dans k. Les substitutions d'une classe à droite de Γ par rapport à Γ' transforment un élément α de k' en un même élément de K, en particulier les substitutions de Γ' laissent inchangé tous les éléments de k' et ceux-là seuls. Le groupe Γ' est d'ailleurs isomorphe au groupe de Galois de k par rapport à k'.

2. Critère de Galois pour les êtres algébriques. — Je rappelle le théorème fondamental connu sous le nom de « critère de Galois » :

(G, 1). *La condition nécessaire et suffisante pour qu'un élément de k soit dans ρ est que ses n conjugués par rapport à ρ soient égaux entre eux* (et en particulier à l'élément lui-même).

Ce critère permet encore de démontrer la propriété suivante qui en est une généralisation :

(G. 1 *bis*). *La condition nécessaire et suffisante pour qu'un élément de k soit dans k' est que ses transformés par les substitutions du groupe* Γ' *soient tous égaux entre eux.*

Ces critères s'étendent aux êtres algébriques de k, obtenus par des calculs rationnels effectués sur des éléments de k et éventuellement sur des indéterminées : matrices, polynomes, idéaux.

Pour cela, il faut définir les conjugués par rapport à ρ de ces éléments algébriques.

L'application d'un élément σ du groupe de Galois Γ à un être algébrique de K se fait en remplaçant les éléments qui définissent cet être :

termes d'une matrice,
coefficients d'un polynome,
polynomes de base d'un idéal,

par leur transformé par σ; on obtient ainsi un nouvel être algébrique de K qui est le transformé du premier par σ. Il y a lieu de remarquer que la définition du transformé d'un idéal est indépendante du choix de la base utilisée pour former ce transformé; le transformé d'un idéal de K par σ est encore l'ensemble des transformés par σ de ses éléments.

Si une matrice ou un polynome est dans k, tous les éléments d'une classe $S^{(i)}$ ont même effet sur cette matrice ou ce polynome; la matrice et le polynome ainsi obtenus sont les *$i^{\text{ièmes}}$ conjugués* des êtres primitifs. On peut encore dire que :

Les $i^{\text{ièmes}}$ conjugués, par rapport à ρ, *d'une matrice* A *de k ou d'un polynome* $f(x_0, x_1, \ldots, x_r)$ *de k*, sont obtenus en remplaçant les termes de A ou les coefficients de f par leurs $i^{\text{ièmes}}$ conjugués respectifs, sans modifier aucune des indéterminées. Ce $i^{\text{ième}}$ conjugué est une matrice, ou un polynome, de $k^{(i)}$ que je désigne encore par $A^{(i)}$, ou $f^{(i)}(x_0, x_1, \ldots, x_r)$.

Pour étendre la première des deux définitions précédentes à un idéal de k, il faut préciser en quel sens il est aussi un idéal de K. Je conviens de dire (et l'on verra que cette convention s'étend aux

êtres géométriques) que les idéaux de k et de K, qui ont une même base, sont le même idéal considéré, le premier dans k, l'autre dans K. Tout idéal de k peut ainsi être défini dans K, mais il existe des idéaux de K qui ne sont pas susceptibles d'être définis dans k.

Avec cette convention, tous les éléments d'une classe à droite $S^{(i)}$ ont même effet sur un idéal de k; l'idéal ainsi obtenu est dans K et aussi dans $k^{(i)}$, c'est le *$i^{ième}$ conjugué*, par rapport à ρ, de l'idéal primitif. On peut encore dire que :

Le $i^{ième}$ conjugué, par rapport à ρ, *d'un idéal (f) sur $S_r(k)$* est l'idéal $(f)^{(i)}$ sur $S_r[k^{(i)}]$ (6) obtenu en remplaçant les termes d'une base de (f) par leurs $i^{èmes}$ conjugués.

Mais il ne faut pas oublier que l'idéal conjugué est défini sur $S_r[k^{(i)}]$ et non sur $S_r(k)$. Je désigne cet idéal indifféremment par l'une des deux notations $(f)^{(i)}$ ou $[f^{(i)}]$.

Les définitions et remarques précédentes subsistent encore si l'on remplace les classes à droite par rapport à γ par les classes à droite par rapport au groupe Γ'.

Enfin les critères de Galois (G, 1) et (G, 1 *bis*) se généralisent de la façon suivante :

(G, 2). *La condition nécessaire et suffisante pour qu'un être numérique ou algébrique de k soit dans* ρ (ou dans l'extension k') *est que ses n conjugués par rapport à* ρ (ou ses transformés par les éléments du groupe Γ') *soient tous égaux entre eux.*

Il est encore important de noter que :

Toute relation rationnelle, à coefficients dans ρ, *vérifiée par des êtres numériques ou algébriques de k reste vraie quand on remplace chacun de ces êtres par son $i^{ième}$ conjugué par rapport à* ρ.

3. **Conjugués des êtres géométriques.** — Dans une extension k (finie ou non) de ρ, on peut définir des êtres géométriques : point M,

---

(6) $S_r(k)$, est le système de référence, ensemble des polynomes homogènes à $r+1$ variables et à coefficients dans k. [*Voir* Mémoire cité, note (1)].

transformation $\mathfrak{C}$, variété (F), correspondance ($\mathfrak{C}$), comme dans le corps de base ρ.

Je dis qu'*un tel être géométrique de k est dans* ρ, s'il admet un système algébrique de définition (système de coordonnées, d'équation ou de formules) formé uniquement d'éléments numériques ou algébriques de ρ. Je fais remarquer que, pour une correspondance entre deux variétés, cette condition implique que ces variétés sont elles-mêmes dans ρ.

Si un être de k est situé dans ρ, tous ceux de ses systèmes de définition dont les termes sont dans ρ définissent un même être géométrique de ρ. Ces deux êtres ne sont pas identiques : l'être de k admet des systèmes de définition contenant des êtres numériques ou algébriques qui ne sont pas dans ρ; l'être de ρ admet seulement les systèmes de définition du premier dont tous les termes sont dans ρ. Mais tout système de définition du second est aussi un système de définition du premier; c'est pourquoi on peut pratiquement les confondre. De façon précise, ces deux êtres sont le même être géométrique CONSIDÉRÉ SOIT DANS ρ, SOIT DANS k.

Ce sont ces définitions qui me permettront dans un Mémoire ultérieur d'étendre à un corps quelconque les notions de correspondance de Poincaré, de variété unicursale et de variété de Brauer, lorsque je les aurai définies dans un corps algébriquement fermé.

D'autre part, si k est une extension finie de ρ, je puis définir *l'application d'un élément* σ *du groupe de Galois* Γ *de* k *par rapport à* ρ *à un être géométrique* ($\mathfrak{E}$) *du corps normal* K *de* k : je choisis un système de définition de ($\mathfrak{E}$) et je remplace les éléments numériques ou algébriques de ce système par leurs transformés par σ; ce nouveau système définit un être $\sigma(\mathfrak{E})$ de K indépendant du choix du système de définition de ($\mathfrak{E}$) utilisé; $\sigma(\mathfrak{E})$ est LE TRANSFORMÉ PAR σ DE ($\mathfrak{E}$). Il y a lieu de remarquer que le transformé par σ de la correspondance

($\mathfrak{C}$) : variété (F) $\rightarrow$ variété (G)

est une correspondance entre les variétés transformées

$\sigma(\mathfrak{C})$: variété σ(F) $\rightarrow$ variété σ(G)

et non une correspondance entre (F) et (G).

Pour former, dans K, le transformé par σ d'un être géométrique $(\mathfrak{E})$ de k, je puis choisir un système de définition de $(\mathfrak{E})$ formé uniquement d'éléments numériques ou algébriques de k : je constate ainsi que ce transformé est le même pour tous les éléments σ d'une même classe $S^{(i)}$. J'appelle *$i^{ième}$* CONJUGUÉ, PAR RAPPORT A ρ, DE $(\mathfrak{E})$, l'être $\sigma(\mathfrak{E})$ ainsi formé; c'est un être du corps conjugué $k^{(i)}$ et non de k. Je le désigne par la notation

$M^{(i)}$ si $(\mathfrak{E})$ est un point M,
$\mathfrak{C}^{(i)}$ si $(\mathfrak{E})$ est la transformation $\mathfrak{C}$,
$(F)^{(i)}$ ou $(F^{(i)})$ si $(\mathfrak{E})$ est la variété (F),
$(\mathfrak{C})^{(i)}$ ou $(\mathfrak{C}^{(i)})$ si $(\mathfrak{E})$ est la correspondance $(\mathfrak{C})$.

Le $i^{ième}$ conjugué d'un être géométrique $(\mathfrak{E})$ de k est encore l'être de $k^{(i)}$ déterminé par un système de définition obtenu en remplaçant les termes numériques ou algébriques d'un système de définition de $(\mathfrak{E})$ dans k par leurs $i^{èmes}$ conjugués respectifs.

Toutes les relations algébriques ou géométriques à coefficients dans ρ vérifiées par des êtres numériques, algébriques et géométriques de k sont encore vérifiées si l'on remplace chacun de ces êtres par son $i^{ième}$ conjugué par rapport à ρ.

Enfin pour former, dans k, le $i^{ième}$ conjugué par rapport à ρ d'un être géométrique $(\mathfrak{E})$ de ρ, je puis définir cet être par un système formé d'êtres numériques ou algébriques de ρ. Le $i^{ième}$ conjugué d'un tel système lui est identique, donc le $i^{ième}$ conjugué de $(\mathfrak{E})$ est identique à $(\mathfrak{E})$. Si l'on choisit ensuite un système de définition de $(\mathfrak{E})$ contenant des êtres numériques ou algébriques de k, le $i^{ième}$ conjugué de ce second système ne lui est pas identique, mais est un autre système de définition du même être $(\mathfrak{E})$.

Ces définitions et raisonnements restent d'ailleurs valables en prenant au lieu de ρ une extension k' de ρ contenue dans k et au lieu des conjugués par rapport à ρ les transformés par les substitutions du sous-groupe associé Γ' de Γ.

J'obtiens ainsi le théorème :

Pour qu'un être géométrique de k soit dans ρ (ou dans l'extension k') *il est nécessaire que ses n conjugués par rapport à ρ* (ou ses transformés par les substitutions du groupe Γ') *soient identiques entre eux.*

4. Critère de Galois pour les êtres géométriques. — Le théorème précédent admet une réciproque qui constitue, avec lui-même, l'extension du critère de Galois aux êtres géométriques :

(G. 3). *La condition nécessaire et suffisante pour qu'un être géométrique de k soit dans* ρ (ou dans l'extension k') *est que ses conjugués par rapport à* ρ (ou ses transformés par les substitutions du groupe Γ') *soient tous identiques entre eux.*

Je vais donner quelques indications sur la démonstration de ce théorème particulièrement important pour la suite.

Je considère d'abord le cas d'un point A sur $S_r(k)$ de coordonnées $a_0, a_1, \ldots, a_r$. L'identité de A et de son $i^{\text{ième}}$ conjugué est exprimée par des égalités

$$a_0^{(i)} = \lambda_i a_0, \qquad a_1^{(i)} = \lambda_i a_1, \qquad \ldots, \qquad a_r^{(i)} = \lambda_i a_r,$$

où λ_i est un élément de K. Je forme les sommes

$$\sum_i a_0^{(i)} = a_0 \sum_i \lambda_i, \qquad \sum_i a_1^{(i)} = a_1 \sum_i \lambda_i, \qquad \ldots, \qquad \sum_i a_r^{(i)} = a_r \sum_i \lambda_i$$

(i de 1 à n).

D'une part, la forme des premiers membres montre que ces sommes sont des éléments de ρ, d'après le critère de Galois (G, 1) relatif aux éléments numériques de k. D'autre part, la forme des seconds membres montre que ces sommes forment un système de coordonnées de A qui est donc dans ρ.

Cette démonstration vaut évidemment pour les transformations de k à condition de remplacer les coordonnées de A par les polynomes qui définissent une telle transformation. Le critère de Galois, déjà indiqué, pour les idéaux pourrait aussi être démontré d'une manière analogue.

Pour les variétés, la question est un peu plus complexe. Si une variété (F) de k est définie par l'idéal (f), l'identité de (F) et de $(F)^{(i)}$ peut être exprimée par la condition que $(f)^{(i)}$ est une conséquence de (f) et inversement que (f) est une conséquence de $(f)^{(i)}$. Elle entraîne donc que l'idéal (f'), plus grand commun diviseur des idéaux $(f)^{(1)}, (f)^{(2)}, \ldots, (f)^{(n)}$ est une conséquence de (f); inversement, (f) est une conséquence de (f') et même est

contenue dans (f') puisqu'il est identique à $(f)^{(n)}$. Donc l'idéal (f') définit la même variété (F) que (f); mais, d'après le critère de Galois pour les idéaux, (f') est un idéal de ρ. Donc la variété (F) est dans ρ.

Enfin pour le cas d'une correspondance de k

$$(\mathfrak{T}) : \qquad \text{variété (F)} \dashrightarrow \text{variété (G)},$$

il y a lieu de préciser que l'identité de $(\mathfrak{T})^{(i)}$ et de $(\mathfrak{T})$ exige d'abord l'identité de $(F)^{(i)}$ et de (F), ainsi que celle de $(G)^{(i)}$ et de (G); donc les variétés (F) et (G) sont dans ρ. Je puis, par suite, définir (F) par un idéal (f) de ρ; si la correspondance $(\mathfrak{T})$ est définie par la transformation $\mathfrak{T}$, l'identité de $(\mathfrak{T})^{(i)}$ et de $(\mathfrak{T})$ est alors exprimée par la condition que $\mathfrak{T}^{(i)}$ et $\mathfrak{T}$ sont congrus suivant l'idéal des conséquences de (f). Je choisis un système de formules

$$\frac{y_0}{\xi_0(x_0, \ldots, x_r)} = \frac{y_1}{\xi_1(x_0, \ldots, x_r)} = \ldots = \frac{y_r}{\xi_r(x_0, \ldots, x_r)}$$

définissant $\mathfrak{T}$ et je forme les sommes

$$\sum_i \xi_0^{(i)}(x_0, \ldots, x_r), \quad \sum_i \xi_0^{(i)}(x_0, \ldots, x_r), \quad \ldots, \quad \sum_i \xi_0^{(i)}(x_0, \ldots, x_r)$$

(i de 1 à n).

Ces polynomes sont d'après le critère de Galois (G, 2) des polynomes de ρ. Ils définissent une transformation congrue à $\mathfrak{T}$ suivant l'idéal des conséquences de (f), donc définissent la correspondance $(\mathfrak{T})$ elle-même. Cette correspondance est donc dans ρ.

Tous ces raisonnements sont encore valables en considérant l'extension k' au lieu du corps ρ et les transformés par les substitutions du groupe Γ' au lieu des conjugués par rapport à ρ.

5. **Application aux correspondances birationnelles.** — Je termine ce chapitre en donnant une application des résultats précédents aux correspondances birationnelles :

Si, entre deux variétés de ρ, existent des correspondances, inverses l'une de l'autre dans une extension séparable k de ρ, il suffit que l'une de ces correspondances soit dans ρ pour que l'autre y soit aussi.

Je suppose la propriété vérifiée par une correspondance entre (F′) et (F) de ρ

$(\mathcal{R})$: variété (F′) → variété (F);

$(\mathcal{R})$ est dans ρ, non dégénéré et a un inverse dans k

$(\mathcal{R}')$ variété (F) → variété (F′).

Puisque les relations géométriques vérifiées par des êtres géométriques de k sont aussi vérifiées par leurs $i^{\text{ièmes}}$ conjugués, chacune des correspondances $(\mathcal{R}')^{(i)}$ est aussi un inverse de $(\mathcal{R})$. En vertu de l'univocité de la correspondance inverse, ces n conjuguées sont donc identiques entre elles; d'après le critère de Galois (G, 3), il en résulte que $(\mathcal{R}')$, ou $(\mathcal{R})^{-1}$, est une correspondance de ρ.

Je puis donc dire d'une correspondance qu'elle est birationnelle, sans préciser dans quel corps je la considère. De plus, pour reconnaître si une correspondance birationnelle, définie dans une extension du corps de base, est dans le corps de base lui-même, il suffit d'appliquer le critère de Galois (G, 3) à cette correspondance dans l'un des deux sens sans se préocuper de l'inverse.

II. — LES ÉQUATIONS D'ÉQUIVALENCE.

Ce chapitre est consacré au problème suivant :

Comment reconnaître si deux variétés de ρ sont équivalentes dans ρ (au sens homographique, ou au sens birationnel, ou au sens de Poincaré, ...) *lorsqu'on sait qu'elles sont équivalentes dans l'extension algébriquement fermée* (1) Ω *de* ρ.

C'est la résolution de ce problème, pour les variétés de Brauer et l'équivalence au sens de Poincaré, qui m'a permis dans mon

---

(1) L'extension algébriquement fermée Ω de ρ est le corps formé par l'ensemble de tous les éléments algébriques par rapport à ρ, c'est-à-dire annulant au moins un polynome à coefficients dans ρ. Dire que deux variétés de ρ sont équivalentes dans Ω revient à dire qu'il existe des extensions finies de ρ dans lesquelles ces variétés sont équivalentes.

Mémoire de Thèse de résoudre les problèmes diophantiens sur les variétés de Brauer.

La recherche de l'équivalence dans l'extension algébriquement fermée Ω de ρ est un problème de nature algébrique; on peut dire qu'il consiste à reconnaître si un système d'équations algébriques est compatible. La recherche de l'équivalence dans ρ est au contraire un problème arithmétique; il consiste à chercher si, parmi les solutions du problème précédent, il en est qui peuvent être obtenues uniquement à l'aide des quatre opérations arithmétiques effectuées dans ρ. En utilisant la théorie de Galois développée au chapitre précédent, je vais exposer une méthode pour passer de ce problème algébrique au problème arithmétique. L'étude algébrique de l'équivalence est pourtant loin d'être terminée. Bien plus, la méthode précédente ne suffit pas nécessairement pour résoudre le problème arithmétique, même si la partie algébrique en est résolue; il faut encore utiliser les particularités obtenues dans l'étude algébrique préalable. Pourtant il m'a semblé intéressant de dégager cette méthode générale qui peut sans doute avoir d'autres applications que celle exposée dans ma Thèse.

1. Système d'équivalence entre deux variétés. — Je considère deux variétés (F) et (F') d'un corps ρ, équivalentes entre elles dans l'extension algébriquement fermée Ω de ρ. Je choisis, parmi les variétés de la classe d'équivalence dans Ω qui contient (F) et (F'), une *variété de comparaison* (A) ou *variété réduite*. On peut choisir, pour variété de comparaison, une des variétés (F) ou (F') elles-mêmes; mais il y a intérêt à leur préférer une variété à proprement parler réduite, c'est-à-dire telle que le groupe d'équivalence $(G.E_\rho A)$ dans ρ sur (A) soit défini de façon aussi simple que possible ([8]). Le choix de cette variété (A) se fait d'après les propriétés algébriques de (F) et (F') et peut être pour beaucoup dans le succès de l'utilisation des équations d'équivalence. Dans le cas des variétés de Brauer et de l'équivalence au sens de Poincaré, j'ai choisi pour (A) un espace de référence.

Je forme ensuite, dans Ω, deux correspondances [de l'ensemble

([8]) Mémoire cité, note ([1]), Chap. III, § III.

(E) qui définit la notion d'équivalence envisagée] « de comparaison » entre la variété (A) d'une part, et les variétés (F) et (F′) d'autre part

$(\mathcal{F})$: variété (A) $\rightarrow$ variété(F),

$(\mathcal{F}')$: variété (A) $\rightarrow$ variété(F′);

et je choisis un système de formules pour chacune de ces correspondances. Les coefficients de ces deux systèmes de formules sont des éléments, en nombre fini, algébriques par rapport à ρ; leur ensemble engendre une extension de ρ qui est finie. Je suppose avoir pu former $(\mathcal{F})$ et $(\mathcal{F}')$ de manière que cette extension soit *séparable par rapport à* ρ, et j'en choisis une extension finie et séparable k qui peut être ce corps lui-même ou un sur-corps quelconque suivant les besoins du raisonnement. Le corps k est une extension finie et séparable de ρ dont je désigne le degré par n; je l'appelle le *corps de comparaison* utilisé. Je reprends les notations et conventions du chapitre I; je choisis un élément primitif θ de k, je forme le corps normal K de k et je désigne les conjugués de θ et d'un être numérique, algébrique ou géométrique quelconque $(\mathcal{E})$ de k par les notations

$$\theta^{(i)} = \theta_i \qquad \begin{cases} i \text{ de } 1 \text{ à } n, \\ \theta_n = \theta, \end{cases}$$

$(\mathcal{E})^{(i)}$ déduit de $(\mathcal{E})$ par les substitutions σ de la classe $S^{(i)}$.

La propriété fondamentale est la suivante :

(E) : *Les correspondances* [de l'ensemble (E)] *de* ρ *entre* (F′) *et* (F)

$(\mathcal{R})$: variété (F′) $\rightarrow$ variété (F)

sont déterminées biunivoquement par des correspondances $(\mathcal{L})$ *de* (G. E$_k$A) *d'après la formule*

$$(E, 1) \qquad (\mathcal{R}) = (\mathcal{F}')^{-1} \times (\mathcal{L}) \times (\mathcal{F});$$

dans cette formule, la correspondance $(\mathcal{L})$ *est un élément arbitraire de* (G. E.$_k$A) *vérifiant les relations*

$$(E, 2) \qquad (\mathcal{L})^{(i)} \times (\mathcal{Q}_i) = (\mathcal{Q}'_i) \times (\mathcal{L}) \qquad (i = 1, 2, \ldots, n).$$

Les $(\mathcal{A}_i)$ et les $(\mathcal{A}'_i)$ sont les éléments de $(\text{G. E.}_k\text{A})$ définis par

$$(\mathcal{A}_i)=(\mathcal{F})^{(i)}\times(\mathcal{F})^{-1},\qquad (\mathcal{A}'_i)=(\mathcal{F}')^{(i)}\times(\mathcal{F}')^{-1}$$

En particulier :

POUR QUE (F) ET (F') SOIENT ÉQUIVALENTES DANS ρ, IL FAUT ET IL SUFFIT QUE LES RELATIONS (E, 2) SOIENT VÉRIFIÉES PAR AU MOINS UN ÉLÉMENT $(\mathcal{L})$ DE $(\text{G. E.}_k\text{A})$.

Le système (E, 2) est le SYSTÈME D'ÉQUIVALENCE ENTRE (F') ET (F) par abréviation de *système des équations d'équivalence dans* ρ *entre* (F') *et* (F), *déduit des éléments de comparaison* : *variété* (A), *correspondances* $(\mathcal{F})$ *et* $(\mathcal{F}')$, *corps* k.

Démonstration : Un produit

$$(\mathcal{R})=(\mathcal{F}')^{-1}\times(\mathcal{L})\times(\mathcal{F}),$$

où $(\mathcal{L})$ est un élément arbitraire de $(\text{G. E.}_k\text{A})$ est une correspondance [de (E)] entre (F') et (F) dans k; inversement, une telle correspondance $(\mathcal{R})$ est un produit de cette forme, puisque la correspondance

$$(\mathcal{F}')\times(\mathcal{R})\times(\mathcal{F})^{-1}$$

est une correspondance [de (E)] sur (A) dans k. Ceci utilise et complète les résultats du Chapitre III, (§ III), propriété 3 du Mémoire cité note (1), qui concernent le cas particulier où (A) est confondue avec (F') et où $(\mathcal{F}')$ est la correspondance identique sur (A).

Pour chercher, parmi ces produits, ceux qui sont dans ρ, j'applique le critère de Galois (G, 3); j'obtiens la condition nécessaire et suffisante

$$[\mathcal{F}'^{(i)}]^{-1}\times(\mathcal{L})^{(i)}\times(\mathcal{F})^{(i)}=(\mathcal{F}')^{-1}\times(\mathcal{L})\times(\mathcal{F}),$$

équivalente au système (E, 2). De plus les produits :

$$(\mathcal{A}_i)=(\mathcal{F})^{(i)}\times(\mathcal{F})^{-1}\qquad (\mathcal{A}'_i)=(\mathcal{F}')^{(i)}\times(\mathcal{F}')^{-1}$$

sont bien des correspondances [de (E)] sur (A) dans K, donc des éléments de $(\text{G. E.}_k\text{A})$.

Je puis notamment former un système d'équivalence entre la la variété (F) et elle-même; il est indiqué, dans ce cas, de choisir

les correspondances $(\mathcal{F})$ et $(\mathcal{F}')$ identiques entre elles. Les correspondances $(\mathcal{A}_i)$ et $(\mathcal{A}'_i)$ sont alors respectivement identiques deux à deux. Le système d'équivalence ainsi formé a au moins une solution : la correspondance identique sur (A); cette correspondance détermine d'ailleurs, d'après la formule (E, 1), la correspondance identique sur (F). Les solutions du système d'équivalence forment de plus un *groupe multiplicatif*, qui est isomorphe au groupe $(G.\ E,_{\rho}\ F)$.

2. Effet d'un changement des éléments de comparaison. — Si l'on change le choix des éléments de comparaison, on obtient un autre système d'équivalence entre (F) et (F'); il est important de savoir comment il peut être déduit du premier. Toutefois je ne m'occupe pas du changement de la variété de comparaison (A), changement assez complexe et de moins grande utilité que les autres. J'étudie seulement le cas où l'on remplace le corps k par une de ses extensions finies et séparables et celui où l'on remplace la correspondance $(\mathcal{F})$ par une autre correspondance de k entre (A) et (F). Le changement le plus général des correspondances $(\mathcal{F})$ et $(\mathcal{F}')$ et du corps k s'obtient en combinant convenablement les deux cas précédents.

a. Changement du corps de comparaison. — Je cherche donc le système d'équivalence dans ρ entre (F) et (F'), pour les mêmes éléments de comparaison (A), $(\mathcal{F})$, $(\mathcal{F}')$, mais pour un corps de comparaison k' extension finie et séparable de k. Je dois grouper les substitutions σ' du groupe de Galois Γ' de k' par rapport à ρ en classes $S'^{(i')}$ de substitutions ayant même effet sur un élément primitif θ' de k' et chercher l'effet $(\mathcal{F})^{(i')}$ d'une telle classe sur la correspondance $(\mathcal{F})$. Or, pour obtenir l'effet d'une telle classe sur un être numérique, algébrique ou géométrique de k, il me suffit de connaître son effet sur un élément primitif de ce corps, c'est-à-dire le conjugué $\theta_j = \sigma'(\theta)$; la classe $S'^{(i')}$ de Γ' a même effet sur $(\mathcal{F})$ que la classe $S^{(j)}$ du groupe de Galois Γ de k par rapport à ρ. En particulier

$$(\mathcal{F})^{(i')} = (\mathcal{L})^{(j)}$$

et par suite

$$(\mathcal{B}_{i'}) = (\mathcal{A}_j).$$

Je fais remarquer que plusieurs i' différents correspondent au même j : des classes S' ayant des effets différents sur l'élément θ' de k' ont même effet sur l'élément θ de k.

Ainsi le nouveau système est composé des mêmes équations que le système primitif, avec une correspondance convenable d'indices : $j \to i'$, une équation de l'ancien système étant répétée plusieurs fois dans le nouveau.

b. Changement d'une correspondance de comparaison. — Dans les éléments de comparaison, je change seulement la correspondance $(\mathcal{F})$ dans k entre (A) et (F). D'après la propriété 3 du (§ III), Chapitre III du Mémoire cité note (1), la nouvelle correspondance $(\mathcal{G})$ doit être identique à un produit $(\mathcal{L}) \times (\mathcal{F})$ d'un élément $(\mathcal{L})$ de (G. E.$_k$A) et de $(\mathcal{F})$. Et il est facile d'obtenir les coefficients $(\mathcal{B}_i)$ du nouveau système d'équivalence

$$(\mathcal{B}_i) = (\mathcal{G})^{(i)} \times (\mathcal{G})^{-1} = (\mathcal{L})^{(i)} \times (\mathcal{F})^{(i)} \times (\mathcal{F})^{-1} \times (\mathcal{L})^{-1}$$
$$= (\mathcal{L})^{(i)} \times (\mathcal{A}_i) \times (\mathcal{L})^{-1}.$$

3. Relations de compatibilité du système d'équivalence. — Il est encore important de remarquer qu'il existe entre les coefficients $(\mathcal{A}_i)$ [ou les coefficients $(\mathcal{A}'_i)$] du système d'équivalence des relations qui jouent un rôle important dans les applications de ce système. Ce sont les relations

$$\text{(E, 3)} \qquad \sigma(\mathcal{A}_i) = (\mathcal{A}_k) \times (\mathcal{A}_j)^{-1}, \qquad \text{si} \begin{cases} \sigma(\theta) = \theta_j, \\ \sigma(\theta_i) = \theta_k; \end{cases}$$

je les appelle RELATIONS DE COMPATIBILITÉ du système (E, 2). Elles sont vraies pour tout indice i de 1 à n et pour tout élément σ du groupe de Galois Γ de k par rapport à ρ.

La vérification en est aisée

$$\sigma(\mathcal{A}_i) = \sigma(\mathcal{F})^{(i)} \times \sigma(\mathcal{F})^{-1} = (\mathcal{F})^{(k)} \times \mathcal{F}^{(j)})^{-1}$$
$$= (\mathcal{F})^{(k)} \times (\mathcal{F})^{-1} \times [(\mathcal{F})^{(j)} \times (\mathcal{F})^{-1}]^{-1} = (\mathcal{A}_k) \times (\mathcal{A}_j)^{-1}.$$

Elles montrent que toute solution du système (E, 2) vérifie aussi les équations conjuguées par rapport à ρ de chaque équation de ce système. En effet, la substitution σ de Γ transforme la $i^{\text{ième}}$ équation de ce système en l'équation

$$(\mathcal{L})^{(k)} \times \sigma(\mathcal{A}_i) = \sigma(\mathcal{A}'_i) \times (\mathcal{L})^{(j)}$$

ou encore, en tenant compte des relations de compatibilité (E, 3),

$$(\mathcal{L})^{(k)} \times (\mathcal{A}_k) \times (\mathcal{A}_j)^{-1} = (\mathcal{A}'_k) \times (\mathcal{A}'_j)^{-1} \times (\mathcal{L})^{(j)}.$$

Cette dernière relation est une combinaison simple des relations de rang k et j du système (E, 2)

$$(\mathcal{L})^{(k)} \times (\mathcal{A}_k) = (\mathcal{A}'_k) \times (\mathcal{L}),$$
$$(\mathcal{L})^{(j)} \times (\mathcal{A}_j) = (\mathcal{A}'_j) \times (\mathcal{L}).$$

4. Système étendu d'équivalence. — On peut enfin étendre aux correspondances (simplement rationnelles) entre (F') et (F) la propriété (E) du paragraphe 1 de ce chapitre :

(E') *Si une correspondance* (simplement rationnelles) *de* ρ

$$(\mathcal{C}) \qquad \text{variété (F')} \rightarrow \text{variété (F)}$$

transforme (F') *en une sous-variété simple de* (F), *elle peut être déterminée biunivoquement par un élément* $(\mathcal{X})$ *de* (E. C.$_k$A) [ensemble des correspondances sur (A) dans k] *d'après la formule*

$$(E', 1) \qquad (\mathcal{C}) = (\mathcal{F}')^{-1} \times (\mathcal{X}) \times (\mathcal{F});$$

dans cette formule, $(\mathcal{X})$ *est un élément de* (E. C.$_k$ A) *assujetti seulement à vérifier les relations*

$$(E', 2) \qquad (\mathcal{X})^{(i)} \times (\mathcal{A}_i) = (\mathcal{A}'_i) \times (\mathcal{X}) \qquad (i = 1, 2, \ldots, n).$$

Les correspondances $(\mathcal{F})$, $(\mathcal{F}')$, $(\mathcal{A}_i)$, $(\mathcal{A}'_i)$ sont les mêmes correspondances *birationnelles* que celles qui interviennent, avec cette notation, dans la propriété (E).

Le système (E', 2) est le système étendu d'équivalence dans ρ entre (F') et (F), déduit des éléments de comparaison : (A), $(\mathcal{F})$, $(\mathcal{F}')$, k.

La démonstration du paragraphe 1 reste valable. Le produit

$$(\mathcal{C}) = (\mathcal{F}')^{-1} \times (\mathcal{X}) \times (\mathcal{F}),$$

où $(\mathcal{X})$ est un élément quelconque de (E. C.$_k$ A), est une correspondance dans k entre (F') et (F) qui peut être singulière. Inversement, si $(\mathcal{C})$ est une correspondance de k entre (F') et (F), le produit

$$(\mathcal{X}) = (\mathcal{F}') \times (\mathcal{C}) \times (\mathcal{F})^{-1},$$

est un élément de (E. C.$_k$ A); ce n'est pas une correspondance singulière si ($\mathfrak{T}$) transforme (F') en une sous-variété simple de (F); dans ce cas, le produit du second membre est associatif et cette relation est équivalente à la relation (E', 1). Le critère de Galois (G, 3) appliqué à ce produit conduit enfin au système (E', 2).

L'existence d'une solution du système (E', 2) n'entraîne pas l'équivalence de (F) et (F'), comme l'existence d'une solution du système d'équivalence proprement dit. Mais les solutions du système (E', 2) peuvent présenter d'autres intérêts.

En particulier, les correspondances dégénérées de ρ entre (F') et (F) qui transforment (F') en une sous-variété simple (G) de (F) sont déterminées par les solutions dégénérées ($\mathfrak{T}$) du système (E', 2). La détermination n'est pas biunivoque, une telle correspondance dégénérée définissant en outre une correspondance entre (F') et (G). Si (G) est réduite à un point (simple) de (F), la solution ($\mathfrak{T}$) correspondante transforme (A) en un point. Inversement, un point simple M de (F), défini par le système de coordonnées $a_0, a_1, \ldots, a_s$, détermine la correspondance ($\mathfrak{T}$) admettant le système de formules

$$\frac{y_0}{a_0} = \frac{y_1}{a_1} = \cdots = \frac{y_s}{a_s};$$

la correspondance ($\mathfrak{T}$) transforme (F') en la variété (M) réduite au point M. La correspondance ($\mathfrak{T}$) est dans ρ si et seulement si M est dans ρ.

Ainsi, *la recherche des points simples de* (F) *dans* ρ *peut être remplacée par celle des solutions de* (E', 2) *qui transforment la variété de comparaison* (A) *en un point.*

Ce qui montre l'intérêt, pour les problèmes diophantiens, du système étendu (E', 2).

(Manuscrit reçu le 1er novembre 1945.)