ANNALES SCIENTIFIQUES DE L'É.N.S.

FRANÇOIS CHÂTELET

Variations sur un thème de H. Poincaré

Annales scientifiques de l'É.N.S. 3e série, tome 61 (1944), p. 249-300
<http://www.numdam.org/item?id=ASENS_1944_3_61__249_0>

VARIATIONS

SUR

UN THÈME DE H. POINCARÉ

PAR M. FRANÇOIS CHÂTELET.

INTRODUCTION.

On appelle *problème diophantien* tout problème équivalent à la recherche des solutions en nombres entiers d'un système d'équations algébriques à coefficients entiers. H. Poincaré a consacré un mémoire (¹) à l'un de ses problèmes : la recherche des « points rationnels » (à coordonnées rationnelles) sur une courbe rationnelle (c'est-à-dire sur une courbe définie par un système d'équations algébriques à coefficients rationnels). Il propose de ramener un tel problème au même problème sur une courbe aussi simple que possible. Pour cela, il répartit les courbes rationnelles en *classes de courbes équivalentes entre elles :* deux courbes rationnelles sont dites équivalentes s'il existe entre elles une correspondance birationnelle à coefficients rationnels. On peut déduire les points rationnels simples (²) situés sur une courbe de ceux qui sont situés sur une courbe équivalente. Il suffit alors de chercher les points rationnels sur la courbe la plus simple de chaque classe.

La méthode réussit particulièrement bien pour les courbes unicursales (ou de genre zéro). Poincaré a démontré à leur sujet deux théorèmes, dont l'essentiel avait déjà été obtenu, dans un autre langage, par Nœther, et qui ont été précisés par Hilbert et Hurwitz (³) :

Pour qu'une courbe unicursale et rationnelle, contienne des points rationnels simples, il faut et il suffit qu'elle soit équivalente à une droite (rationnelle).

(¹) *Journal de Liouville*, 5ᵉ série, t. 7, 1901, p. 161-233.

(²) Les points multiples échappent à ces considérations; mais ce n'est guère important : sur une courbe, il n'y a qu'un nombre fini de points multiples qu'on peut obtenir et étudier séparément. *Voir* à ce sujet ma Note aux *Comptes rendus de l'Académie des Sciences* du 18 janvier 1943.

(³) M. NŒTHER, *Rationale Ausführung der Operationen in der Theorie der algebraischen Funktionen* (*Math. Ann.*, Bd. 23, S. 311). — HILBERT et HURWITZ, *Über die diophantischen Gleichungen von Geschlecht Null* (*Acta mathematica*, Bd. 14, 1890-1891, S. 217-224).

Toute courbe unicursale et rationnelle est équivalente, soit à une droite, soit à une conique (rationnelle).

On peut préciser que la droite, ou la conique, du second théorème peut être obtenue, à partir de l'équation de la courbe donnée, par des opérations rationnelles en nombre fini.

Le second théorème ramène la classification des courbes unicursales à celle des coniques rationnelles. Or, des critères de Lagrange et de Gauss permettent de reconnaître si une conique rationnelle contient ou non des points rationnels. De plus, le premier théorème résout les problèmes diophantiens sur les courbes unicursales, puisqu'il est facile d'obtenir les points rationnels sur une droite rationnelle : ce sont ceux dont l'abscisse est rationnelle.

Le présent mémoire est consacré à une généralisation de cette théorie de Lagrange, Gauss, Nœther et Poincaré : on peut étendre, à certaines variétés que j'appelle *variétés de Brauer* ([4]), l'essentiel des théorèmes de Nœther-Poincaré et donner des critères analogues à ceux de Lagrange-Gauss. Mais les méthodes que j'emploie sont essentiellement différentes de celles de Poincaré; elles ramènent les problèmes d'équivalence à des problèmes classiques de la théorie des Algèbres normales et simples ou *Algèbres de Brauer* ([5]). Pour cela, je mets en équation les problèmes d'équivalence suivant un *procédé galoisien*, c'est-à-dire en utilisant la notion de *conjugués* d'un nombre algébrique, convenablement adaptée aux êtres géométriques, et les *critères de Galois*, qui permettent de reconnaître si un nombre, ou un être géométrique, obtenu dans un corps de nombres algébriques, est rationnel ou non.

H. Hasse ([6]) a montré, dans un cas particulier, la corrélation entre certains problèmes d'équivalence et la théorie des Algèbres; mais il n'a pas atteint le cas général envisagé ici et ne semble avoir signalé qu'une corrélation formelle. D'autre part, je n'ai pas épuisé ici les possibilités de la méthode *galoisienne* au sujet de laquelle je prépare d'autres mémoires ([7]).

Pour éclaircir l'exposé des méthodes générales, j'en donne, dans un premier chapitre, l'application aux théorèmes classiques de Nœther-Poincaré. Cette application, relativement simple, ne comporte guère de difficultés arithmétiques (qui sont comprises dans les critères de Lagrange-Gauss); c'est pourquoi la démonstration peut en être faite sans le secours de la théorie des Algèbres.

([4]) Cette locution est une abréviation commode de « *variété associée à une Algèbre de Brauer* ».

([5]) L'expression *Algèbre de Brauer* n'est pas consacrée par les auteurs qui ont étudié cette notion; ils emploient la locution *Algèbre normale et simple*. Mais ils désignent sous le nom de *Groupe de Brauer sur un corps* le groupe formé par les Algèbres normales et simples sur ce corps. L'expression que j'emploie est donc une abréviation de *Algèbre contenue dans le groupe de Brauer sur le corps de base*. Toutes ces notions sont définies au paragraphe I du Chapitre III.

([6]) *Elementar Beweis des Hauptsatzes über ternäre quadratische Formen* (*Journal de Crelle*, Bd. 172, 1935, S. 129-132).

([7]) Voir mes Notes aux *Comptes rendus*, t. 206, 1938, p. 1532; 212, 1941, p. 320.

CHAPITRE I.

LES THÉORÈMES DE NŒTHER-POINCARÉ.

Une courbe algébrique plane (F) de genre zéro (ou unicursale), définie par une équation à coefficients rationnels, admet des *représentations* unicursales propres à coefficients algébriques. Je ne me préoccupe pas ici de la manière dont on peut déterminer une telle représentation. J'utilise les coordonnées homogènes x, y, z du plan et je représente le paramètre par le quotient de deux variables homogènes u et v. Une représentation propre $(\mathcal{F})$ de (F) est définie par un système de relations

$$\frac{x}{\xi_1(u, v)} = \frac{y}{\xi_2(u, v)} = \frac{z}{\xi_3(u, v)}; \qquad \frac{u}{\eta_1(x, y, z)} = \frac{v}{\eta_2(x, y, z)};$$

ξ_1, ξ_2, ξ_3 sont trois polynomes homogènes en u et v de même degré et premiers entre eux; η_1 et η_2 sont deux polynomes homogènes en x, y, z de même degré et premiers entre eux; tous ces polynomes ont leurs coefficients algébriques. Ces relations définissent aussi une *correspondance birationnelle*, que je désigne par le même symbole $(\mathcal{F})$, entre le point de coordonnées homogènes x, y, z sur (F) et le point de coordonnées homogènes o, u, v sur Oy. L'énoncé du second théorème de Nœther-Poincaré est ainsi équivalent à :

S'il existe une correspondance birationnelle à coefficients algébriques entre une courbe (F) (définie par une équation algébrique irréductible à coefficients rationnels) *et l'axe* Oy, *il existe une correspondance birationnelle à coefficients rationnels entre* (F) *et, soit une droite, soit une conique* (définie par une équation à coefficients rationnels).

En outre, le premier théorème de Nœther-Poincaré, précise que :

S'il existe une correspondance birationnelle, à coefficients rationnels, entre (F) *et* Oy, *il existe une infinité de points rationnels sur* (F); *pour qu'il existe une telle correspondance, il suffit qu'il y ait un point rationnel simple sur* (F).

I. — Système d'équivalence entre deux courbes unicursales.

Je considère deux courbes (F) et (F′) unicursales et rationnelles et je détermine pour chacune d'elles une représentation propre à coefficients algébriques que je désigne par les symboles

$$(\mathcal{F}) : \qquad (o,\ u,\ v) \text{ sur } Oy \ \rightarrow\ (x,\ y,\ z) \text{ sur } (F),$$
$$(\mathcal{F}') : \qquad (o,\ u',\ v') \text{ sur } Oy \ \rightarrow\ (x',\ y',\ z') \text{ sur } (F').$$

J'utilise un *corps normal* K de nombres algébriques, contenant les coefficients de $(\mathcal{F})$ et ceux de $(\mathcal{F}')$; je choisis un élément primitif Θ dans K et je désigne par

$$\Theta_1, \quad \Theta_2, \quad \ldots, \quad \Theta_{N-1}, \quad \Theta_N = \Theta,$$

les conjugués (absolus) de Θ; N est le degré du corps K. Je puis exprimer un nombre a de K en fonction rationnelle, à coefficients rationnels, de Θ; suivant les conventions habituelles, j'appelle $i^{\text{ième}}$ conjugué de a et je désigne par $a^{(i)}$ le nombre de K obtenu en remplaçant Θ par Θ_i dans cette fonction. Plus généralement, si un système quelconque $(\mathfrak{T})$ de polynomes [par exemple le système qui définit $(\mathcal{F})$: $\xi_1, \xi_2, \xi_3, \eta_1, \eta_2$] a ses coefficients dans K, j'appelle $i^{\text{ième}}$ conjugué et je désigne par $(\mathfrak{T})^{(i)}$ le système obtenu en remplaçant chaque coefficient par son $i^{\text{ième}}$ conjugué sans modifier aucune des inconnues (x, y, z, u, v dans l'exemple cité).

Ces conventions étant acquises, je vais démontrer la proposition fondamentale suivante :

(E). *Les correspondances birationnelles, à coefficients rationnels, entre* (F′) *et* (F)

$$(\mathcal{R}) : \qquad (x', y', z') \text{ sur } (\text{F}') \rightarrow (x, y, z) \text{ sur } (\text{F}),$$

peuvent être obtenues au moyen de la formule

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

Dans cette formule, $(\mathcal{L})$ *est une homographie sur* Oy *à coefficients dans* K, *non dégénérée, vérifiant le système d'équations en* $(\mathcal{L})$

$$(\text{E}, 2) \qquad (\mathcal{L})^{(i)} \times (\mathfrak{A}_i) = (\mathfrak{A}'_i) \times (\mathcal{L}) \qquad (i = 1, 2, \ldots, \text{N}),$$

où les coefficients $(\mathfrak{A}_i)$ *et* $(\mathfrak{A}'_i)$ *sont les homographies non dégénérées sur* Oy, *à coefficients dans* K, *définies par les relations*

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

La formule (E, 1) *établit une correspondance biunivoque entre les correspondances* $(\mathcal{R})$ *et les solutions* $(\mathcal{L})$ *du système* (E, 2).

En particulier : **pour que (F) et (F′) soient équivalentes entre elles, il faut et il suffit qu'il existe au moins une homographie sur Oy, non dégénérée, à coefficients dans K, vérifiant le système (E, 2) d'équations en $(\mathcal{L})$.**

S'il existe entre (F′) et (F) une correspondance birationnelle

$$(\mathcal{R}) : \qquad (x', y', z') \text{ sur } (\text{F}') \rightarrow (x, y, z) \text{ sur } (\text{F}),$$

on peut en déduire une correspondance birationnelle $(\mathcal{L})$ sur Oy

$$(\mathcal{L}) = (\mathcal{F}') \times (\mathcal{R}) \times (\mathcal{F})^{-1} : \quad (0, u', v') \text{ sur } Oy \rightarrow (0, u, v) \text{ sur } Oy.$$

Une telle correspondance est une homographie non dégénérée sur Oy. Réciproquement, à partir d'une homographie $(\mathcal{L})$ non dégénérée sur Oy, la formule (E, 1) (équivalente à la précédente) définit une correspondance $(\mathcal{R})$ qui est birationnelle, car

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

Si les coefficients de $(\mathcal{R})$ sont rationnels, ceux de $(\mathcal{L})$ sont dans K; si les coefficients de $(\mathcal{L})$ sont dans K, ceux de $(\mathcal{R})$ et ceux de $(\mathcal{R})^{-1}$ y sont aussi. Reste donc à chercher la condition pour qu'une telle correspondance $(\mathcal{R})$, définie par des relations à coefficients dans K, puisse aussi être définie par des relations à coefficients rationnels.

Pour cela, je remarque que, (F) et (F$'$) ayant leurs coefficients rationnels, les conjugués d'une correspondance birationnelle (à coefficients dans K) entre (F$'$) et (F) sont aussi des correspondances birationnelles entre les mêmes courbes. Et j'utilise la propriété :

(G). *Pour qu'une correspondance* $(\mathcal{R})$ (à coefficients dans K) *entre* (F$'$) *et* (F) *puisse être définie par des formules à coefficients rationnels, il faut et il suffit que ses* N *conjuguées soient des correspondances entre* (F$'$) *et* (F) *identiques à* $(\mathcal{R})$

$$(\mathcal{R})^{(i)} = (\mathcal{R}) \qquad (i = 1, 2, \ldots, N).$$

La condition est manifestement nécessaire; il est aisé de montrer qu'elle est suffisante. Je n'insiste pas sur ce point; j'en ai donné une exposition détaillée et générale dans le chapitre sur les critères de Galois, dans un mémoire sur la **Géométrie galoisienne.**

Cette condition (G), appliquée au produit (E, 1), donne :

$$(\mathcal{F}')^{-1} \times (\mathcal{L}) \times (\mathcal{F}) = (\mathcal{F}'^{(i)})^{-1} \times (\mathcal{L})^{(i)} \times (\mathcal{F})^{(i)} \qquad (i = 1, 2, \ldots, N);$$

ce qui est équivalent au système (E, 2). Enfin les produits

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

sont des correspondances birationnelles sur Oy, donc des homographies *non dégénérées* sur cet axe.

Le système (E, 2) est appelé, par la suite, **système d'équivalence entre** (F$'$) **et** (F), par abréviation de « système des équations d'équivalence entre (F$'$) et (F) déduit des représentations propres $(\mathcal{F}')$ et $(\mathcal{F})$ dans le corps K ».

Il est utile de former les conjuguées de chaque équation du système (E, 2) : ces nouvelles équations doivent être des conséquences de ce système. En précisant le $j^{\text{ième}}$ conjugué de Θ_i (qui est aussi un conjugué de Θ et correspond à un produit dans le groupe de Galois de K), je puis calculer les $j^{\text{ièmes}}$ conjuguées des correspondances $(\mathcal{A}_i)$ et $(\mathcal{A}'_i)$; j'obtiens :

$$(\mathcal{A}_i)^{(j)} = (\mathcal{A}_k) \times (\mathcal{A}_j)^{-1}, \qquad \text{si} \quad \Theta_i^{(j)} = \Theta_k. \tag{E, 3}$$

En effet,

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

La $j^{\text{ième}}$ conjuguée de la $i^{\text{ième}}$ équation du système (E, 2) est donc

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

c'est une combinaison simple des équations de rang k et j du système (E, 2).

De ce calcul, je retiens les relations (E, 3) qui montrent que l'ensemble des produits $(\mathcal{A}_i)$ n'est pas un ensemble quelconque de N homographies sur Oy; elles jouent d'ailleurs un rôle important dans la suite. Je les désigne sous le nom de *relations de compatibilité du système* (E, 2).

II. — Points rationnels et homographies dégénérées.

J'ai introduit, au paragraphe précédent, les systèmes d'équivalence pour obtenir les correspondances birationnelles entre deux courbes (F') et (F) (unicursales et rationnelles); je montre maintenant qu'un tel système permet aussi la recherche des points rationnels sur une de ces courbes (F).

Un raisonnement analogue à celui du paragraphe précédent permet de généraliser la propriété (E) aux correspondances simplement rationnelles :

(E'). *Les correspondances simplement rationnelles, à coefficients rationnels, entre* (F') *et* (F)

$$(\mathfrak{C}) : \qquad (x', y', z') \text{ sur } (\mathrm{F}') \;\to\; (x, y, z) \text{ sur } (\mathrm{F}),$$

peuvent être obtenues au moyen de la formule

$$(\mathrm{E}', 1) \qquad (\mathfrak{C}) = (\mathcal{F}')^{-1} \times (\mathcal{Q}) \times (\mathcal{F}),$$

à l'exception peut-être de certaines correspondances dont chacune transforme (F') en un ensemble fini de *points multiples* sur (F). Dans cette formule, $(\mathcal{Q})$ est une correspondance simplement rationnelle sur Oy, à coefficients dans K, vérifiant le système d'équations en $(\mathcal{Q})$:

$$(\mathrm{E}', 2) \qquad (\mathcal{Q})^{(i)} \times (\mathcal{A}_i) = (\mathcal{A}'_i) \times (\mathcal{Q}) \qquad (i = 1, 2, \ldots, \mathrm{N}),$$

où les $(\mathcal{A}_i)$ et les $(\mathcal{A}'_i)$ sont les mêmes homographies non dégénérées sur Oy que dans le système (E, 2).

Je ne détaille pas la démonstration de cette propriété que j'ai développée sous une forme plus générale dans la *Géométrie galoisienne*. J'indique seulement que les cas d'exceptions proviennent du fait suivant : il peut exister des correspondances $(\mathfrak{C})$, transformant (F') en un nombre fini de points multiples sur (F), telles que le produit $(\mathfrak{C}) \times (\mathcal{F})^{-1}$ transforme (F') en un *ensemble vide*.

J'appelle ce nouveau système (E′, 2) (concernant les solutions dégénérées) **système étendu d'équivalence entre** (F′) **et** (F).

D'un cas particulier de la propriété précédente, je déduis le résultat suivant :

Les points rationnels simples [8] *sur* (F) *peuvent être déterminés par les solutions homographiques dégénérées du système d'équations* (E′, 2) (c'est-à-dire par les homographies dégénérées sur Oy, à coefficients dans K, qui vérifient ce système).

En effet, un point rationnel *simple* M sur (F) détermine une correspondance simplement rationnelle dégénérée entre (F′) et (F), à coefficients rationnels

$(\mathcal{C})$: tout point (x', y', z') sur (F') $\rightarrow$ le point M ;

réciproquement, si une correspondance simplement rationnelle, à coefficients rationnels, transforme la courbe (F′) en un seul point, ce dernier est rationnel. De plus, une telle correspondance se déduit, au moyen de la formule (E′, 1), d'une solution $(\mathfrak{T})$ du système (E′, 2) qui transforme l'axe Oy en un seul point de cet axe, donc est une homographie dégénérée sur Oy.

Ce théorème montre que l'existence d'une solution homographique dégénérée pour le système (E′, 2) est indépendante du choix de (F′). On constate d'ailleurs directement qu'un changement du coefficient $(\mathfrak{A}'_i)$ ne modifie pas les solutions homographiques dégénérées de ce système, car en multipliant à gauche une homographie dégénérée sur Oy par une homographie non dégénérée sur cet axe on ne modifie pas la première.

III. — Le premier théorème.

Je démontre maintenant le théorème suivant qu'il suffit de comparer à celui du paragraphe précédent pour en déduire le premier théorème de Nœther-Poincaré.

Si un système étendu d'équivalence entre (F′) *et* (F) *admet une solution homographique dégénérée,* (F) *est équivalente à* Oy.

La remarque de la fin du paragraphe précédent montre qu'il suffit de prouver ce théorème pour un choix arbitraire de (F′); il est donc équivalent à : *si un système étendu d'équivalence entre* Oy *et* (F) *admet des solutions homographiques dégénérées, il admet aussi des solutions homographiques non dégénérées.* C'est sous cette forme que je vais le démontrer; de plus je puis faire un choix particulier des correspondances $(\mathcal{F}')$ et $(\mathcal{F})$, car un changement de ces correspon-

(8) Je ne fais pas de distinction ici entre les points à distance finie ou infinie du plan (projectif) et j'appelle *point rationnel*, ou point dans K, sur (F) un point de cette courbe dont les coordonnées homogènes ont des rapports deux à deux rationnels, ou dans K.

dances ne modifie ni l'existence d'une solution homographique dégénérée, ni celle d'une solution homographique non dégénérée.

Je choisis pour représentation $(\mathcal{F}')$ de Oy la correspondance identique sur cet axe; les homographies $(\mathfrak{A}'_i)$ sont donc toutes identiques à l'unité. Je considère d'autre part, une représentation propre $(\mathcal{F}_1)$ de (F) et un corps algébrique normal K contenant les coefficients de $(\mathcal{F}_1)$. Je suppose que le système étendu d'équivalence, déduit des représentations $(\mathcal{F}_1)$ et $(\mathcal{F}')$, ait une solution homographique dégénérée $(\mathcal{T}_1)$. L'homographie $(\mathcal{T}_1)$ transforme l'axe Oy en un seul point N_1 dans K; je sais construire une homographie $(\mathcal{L}_1)$ non dégénérée sur Oy, à coefficients dans K, qui transforme le point à l'infini de Oy en N_1. Je choisis pour correspondance $(\mathcal{F})$ le produit $(\mathcal{L}_1)\times(\mathcal{F}_1)$ et je forme le système étendu d'équivalence :

$$(\mathrm{E}', 2) \qquad (\mathcal{T})^{(i)}\times(\mathfrak{A}_i)=(\mathcal{T}) \qquad (i=1, 2, \ldots, \mathrm{N}),$$

déduit des correspondances $(\mathcal{F})$ et $(\mathcal{F}')$ dans le corps K. Ce système en $(\mathcal{T})$ admet pour solution l'homographie dégénérée

$$(\mathcal{T}_1)\times(\mathcal{L}_1)^{-1}: \quad \text{tout point } (0, u, v) \text{ sur } Oy \quad \to \quad \text{le point à l'}\infty \text{ sur } Oy.$$

Ceci n'est possible que si chacune des correspondances $(\mathfrak{A}_i)$ conserve le point à l'∞ sur Oy, donc si ces homographies sont des transformations *linéaires* sur Oy.

Pour simplifier légèrement les notations, je définis les transformations linéaires sur Oy en coordonnées *non homogènes* $t=u:v$,

$$(\mathfrak{A}): \qquad \{t'=at+b\}.$$

Je définis, suivant l'habitude, la somme de telles transformations par l'addition de leurs coefficients :

$$\sum_s\{t'=a_st+b_s\} = \left\{t'=\left(\sum_s a_s\right)t+\sum_s b_s\right\}.$$

Le produit des transformations linéaires est une opération distributive par rapport à leur somme ainsi définie.

A partir des produits $(\mathfrak{A}_i)$, qui sont des transformations linéaires,

$$(\mathfrak{A}_i): \qquad \{t'=a_it+b_i\},$$

et d'une transformation linéaire $(\mathcal{L})$ sur Oy quelconque, à coefficients dans K

$$(\mathcal{L}): \qquad \{t'=lt+m\},$$

je forme la somme

$$(\mathcal{T})=\sum_i(\mathcal{L})^{(i)}\times(\mathfrak{A}_i) \qquad (i \text{ de } 1 \text{ à } \mathrm{N}).$$

C'est une solution du système (E′, 2); en effet, des relations de compatibilité (E, 3) et de la distributivité des produits de transformations linéaires par rapport à leur somme, il résulte que :

$$(\mathfrak{T})^{(j)} = \sum_i (\mathcal{L})^{(k)} \times (\mathfrak{A}_i)^{(j)} = \sum_k (\mathcal{L})^{(k)} \times (\mathfrak{A}_k) \times (\mathfrak{A}_j)^{-1} = (\mathfrak{T}) \times (\mathfrak{A}_j)^{-1}$$

$$(\text{pour tout } j \text{ de } 1 \text{ à } N).$$

Je vais montrer que pour un choix convenable de $(\mathcal{L})$, $(\mathfrak{T})$ n'est pas dégénérée, c'est-à-dire que le coefficient de t dans cette transformation n'est pas nul. Ce coefficient est

$$p = \sum_i l^{(i)} a_i;$$

en prenant successivement pour l les N premières puissances de Θ, j'obtiens N valeurs de p qui ne peuvent être toutes nulles : ces N valeurs se présentent comme N formes linéaires des N nombres $a_1, a_2, \ldots, a_N$; d'une part, le déterminant de ces formes $|\Theta_i^s|$ n'est pas nul, puisqu'il est égal au discriminant dans K d'un élément primitif Θ de ce corps; d'autre part, aucun des nombres $a_1, a_2, \ldots, a_N$ n'est nul, puisque aucune des transformations $(\mathfrak{A}_i)$ n'est dégénérée. Donc il existe une puissance Θ^r de Θ pour laquelle la somme

$$(\mathfrak{T}) = \sum_i (\mathcal{L})^{(i)} \times (\mathfrak{A}_i) \qquad \text{avec} \quad (\mathcal{L}) = \{ t' = \Theta^r t \},$$

est une solution homographique non dégénérée de (E′, 2) et le théorème est démontré.

IV. — Introduction de relations matricielles.

J'ai obtenu, au paragraphe précédent, une solution du système d'équivalence en *additionnant* des transformations linéaires. Cette notion d'addition ne s'étend pas aux homographies sur Oy, mais seulement aux matrices, ou tableaux de coefficients, qui les représentent. Aussi vais-je utiliser ces matrices; je rappelle d'abord les relations qui existent entre elles et les homographies sur Oy.

Une matrice carrée L régulière (à déterminant non nul), du deuxième ordre, à termes dans K, définit une homographie $(\mathcal{L})$ sur Oy, à coefficients dans K et non dégénérée; réciproquement, une telle homographie $(\mathcal{L})$ peut être représentée par une matrice L ayant les propriétés précédentes, *définie au produit près par un scalaire λ de* K. J'utilise de nouveau les coordonnées *homogènes*; l'homographie

$$(\mathcal{L}) \qquad \left\{ \frac{u'}{au + bv} = \frac{v'}{cu + dv} \right\},$$

est représentée par la matrice

$$L = \lambda \times \begin{Vmatrix} a & c \\ b & d \end{Vmatrix}.$$

Une matrice carrée irrégulière du deuxième ordre définit une homographie dégénérée sur Oy et réciproquement une homographie dégénérée sur Oy, à coefficients dans K, peut être représentée par une matrice irrégulière, à termes dans K, définie au produit près, à gauche, par une matrice régulière arbitraire à termes dans K.

A la multiplication des matrices correspond la multiplication des homographies; je puis donc exprimer toute relation entre homographies sur Oy par une relation entre les matrices qui les représentent, compte tenu de l'indétermination relative de ces matrices. Notamment, le système d'équivalence :

(E, 2) $$(\mathcal{L})^{(i)} \times (\mathfrak{A}_i) = (\mathfrak{A}'_i) \times (\mathcal{L}) \qquad (i = 1, \ldots N),$$

est équivalent au système d'équations en L et λ_i :

(E.M, 2) $$L^{(i)} \times A_i = \lambda_i \times A'_i \times L \qquad (i = 1, 2, \ldots, N);$$

A_i est une matrice à termes dans K représentant $(\mathfrak{A}_i)$, A'_i une matrice à termes dans K représentant $(\mathfrak{A}'_i)$; L est une matrice représentant $(\mathcal{L})$, donc une matrice régulière à termes dans K arbitraire; λ_i est un scalaire arbitraire de K.

J'appelle, par la suite, **ensemble de matrices associé à la courbe** (F), l'ensemble des N matrices A_i représentant les homographies

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

Cet ensemble vérifie les **relations de compatibilité matricielles** :

(C.M.) $$A_i^{(j)} = A_k \times A_j^{-1} \times a_{i,j} \qquad \text{si} \quad \Theta_i^{(j)} = \Theta_k,$$

où $a_{i,j}$ est un scalaire de K, ces relations sont équivalentes aux relations de compatibilité (E, 3) vérifiées par les homographies $(\mathfrak{A}_i)$. J'appelle les N^2 nombres $a_{i,j}$ **ensemble de scalaires associé à la courbe** (F).

Si deux courbes (F) et (F′) (unicursales et rationnelles) sont associées au même ensemble de matrices A_i, elles sont équivalentes; les coefficients $(\mathfrak{A}_i)$ et $(\mathfrak{A}'_i)$ du système d'équivalence entre (F′) et (F) correspondant

$$(\mathcal{L})^{(i)} \times (\mathfrak{A}_i) = (\mathfrak{A}'_i) \times (\mathcal{L}) \qquad (i = 1, 2, \ldots, N),$$

sont respectivement identiques et ce système admet au moins une solution non dégénérée, la correspondance identique sur Oy.

Je vais établir le théorème plus général :

Si deux courbes unicursales et rationnelles sont associées au même ensemble de scalaires, elles sont équivalentes.

Je considère deux telles courbes (F) et (F′) associées respectivement aux ensembles de matrices A_i et A'_i tels que

$$A_i^{(j)} = A_k \times A_j^{-1} \times a_{i,j}, \qquad A_i'^{(j)} = A'_k \times A_j'^{-1} \times a_{i,j}.$$

A partir d'une matrice carrée V, d'ordre 2, à termes dans K, arbitraire, je forme la somme

$$P = \sum_i A_i'^{-1} \times V^{(i)} \times A_i \qquad (i \text{ de } 1 \text{ à } N).$$

Cette matrice P représente une homographie ($\mathfrak{T}$) qui vérifie le système étendu d'équivalence

$$(E', 2) \qquad (\mathfrak{T})^{(i)} \times (\mathcal{A}_i) = (\mathcal{A}'_i) \times (\mathfrak{T}) \qquad (i = 1, 2, \ldots, N).$$

Car les relations (C.M.) montrent que

$$P^{(j)} = \sum_i [(A_i'^{(j)})^{-1} \times V^{(k)} \times A_i^{(j)}] = \sum_k [a_{i,j}^{-1} \times A'_j \times A_k'^{-1} \times V^{(k)} \times A_k \times A_j^{-1} \times a_{i,j}];$$

j'en déduis, en utilisant les faits qu'un scalaire est permutable avec toute matrice et que le produit des matrices est distributif par rapport à leur somme :

$$P^{(j)} = A'_j \times \left[\sum_k (A_k'^{-1} \times V^{(k)} \times A_k) \right] \times A_j^{-1} = A'_j \times P \times A_j^{-1};$$

d'où résulte à fortiori la $j^{\text{ième}}$ relation du système (E′, 2).

Si P est régulière, l'homographie ($\mathfrak{T}$) n'est pas dégénérée et les courbes (F) et (F′) sont équivalentes entre elles. Si P est irrégulière, (F) est équivalente à Oy, d'après le théorème du paragraphe III. Mais je puis aussi former de la même façon une matrice P′ après avoir interverti le rôle de (F) et de (F′); j'en déduis que : ou bien (F) et (F′) sont équivalentes entre elles, ou bien (F′) est équivalente à Oy. Comme l'équivalence de (F) et de (F′) à Oy entraîne leur équivalence entre elles, la proposition est démontrée.

Je fais remarquer que toute homographie ($\mathfrak{T}$) (dégénérée ou non) qui vérifie le système (E′, 2) (s'il en existe) peut être représentée par une somme de la forme

$$P = \sum_i A_i'^{-1} \times V^{(i)} \times A_i.$$

En effet, si V_1 est une matrice, à termes dans K, arbitraire, représentant cette homographie, chacun des produits $A_i'^{-1} \times V_1^{(i)} \times A_i$ représente aussi cette homographie, en vertu des relations (E′, 2). Donc la somme P_1 de ces produits représente encore ($\mathfrak{T}$).

En particulier toute correspondance birationnelle entre la courbe (F) et elle-même peut être représentée par une somme de la forme

$$P = \sum_i A_i^{-1} \times V^{(i)} \times A_i.$$

V. — **Corps quadratiques de représentation.**

J'appelle **corps de représentation d'une courbe** (F) (unicursale et rationnelle) un corps de nombres algébriques fini K_1 tel que (F) admette une représentation unicursale propre à coefficients dans K_1.

Pour toute courbe unicursale et rationnelle, il existe au moins un corps quadratique de représentation.

Pour reconnaître si un corps K_1 est corps de représentation de (F), je puis choisir pour corps K une extension de K_1, former un système d'équivalence entre Oy et (F), à coefficients dans K,

$$(\mathcal{L})^{(i)} \times (\mathcal{C}_i) = (\mathcal{L}) \qquad (i = 1, 2, \ldots, N), \tag{E, 2}$$

et ne conserver de ce système que les équations qui correspondent aux conjugués relatifs Θ_i, de Θ *par rapport à* K_1 et non à tous les conjugués *absolus* de Θ.

J'obtiens ainsi un système d'équivalence *relative dans* K_1 entre Oy et (F) et je puis prouver que :

Pour que K_1 *soit corps de représentation de* (F), *il faut et il suffit que le système* (E, 2) *d'équivalence relative dans* K_1 *ait au moins une solution.*

En effet, les correspondances birationnelles entre Oy et (F), à coefficients dans K_1, se déduisent des solutions du système d'équivalence relative dans K_1 (E, 2) au moyen de la formule :

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

Je n'insiste pas sur la démonstration complète de ce fait, elle est analogue à celle du paragraphe I; j'en ai donné un exposé détaillé dans la *Géométrie galoisienne*.

Enfin la propriété du paragraphe III s'étend aux systèmes d'équivalence relative dans K_1; cette extension qui est assez évidente est aussi démontrée dans la *Géométrie galoisienne*.

Si un système d'équivalence relative dans K_1 *entre deux courbes* (unicursales et rationnelles) (F′) *et* (F) *admet des solutions homographiques dégénérées, le corps* K_1 *est corps de représentation de* (F).

Je vais maintenant construire un corps quadratique K_1 vérifiant cette dernière propriété pour deux courbes identiques entre elles [ce qui est utile pour obtenir toutes les correspondances birationnelles à coefficients rationnels sur (F)].

J'ai dit que toute correspondance birationnelle à coefficients rationnels entre la courbe (F) et elle-même peut être représentée par une somme de la forme

$$P = \sum_i A_i^{-1} \times V^{(i)} \times A_i,$$

qui vérifie le système particulier d'équations matricielles en P

$$\text{(M)} \qquad P^{(i)} \times A_i = A_i \times P \qquad (i = 1, \ldots, N).$$

Parmi ces correspondances se trouve la correspondance identique sur Oy, représentée par une matrice scalaire obtenue notamment en prenant pour V une matrice scalaire.

Mais il existe aussi d'autres correspondances représentées par des matrices P non scalaires. Je remplace V successivement par les produits d'une matrice arbitraire V_1 et des N premières puissances de Θ; j'obtiens ainsi N matrices :

$$P_1 = \sum_i [A_i^{-1} \times (\Theta \times V_1)^{(i)} \times A_i] = \sum_i [\Theta_i \times A_i^{-1} \times V_1^{(i)} \times A_i],$$

$$P_2 = \sum_i [A_i^{-1} \times (\Theta^2 \times V_1)^{(i)} \times A_i] = \sum_i [\Theta_i^2 \times A_i^{-1} \times V_1^{(i)} \times A_i],$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$P_N = \sum_i [A_i^{-1} \times (\Theta^N \times V_1)^{(i)} \times A_i] = \sum_i [\Theta_i^N \times A_i^{-1} \times V_1^{(i)} \times A_i],$$

qui toutes vérifient le système de relations (M). Ces N matrices sont des formes linéaires à coefficients scalaires (dans K) des N produits $A_i^{-1} \times V_1^{(i)} \times A_i$; le déterminant de ces N formes $|\Theta_i^s|$ est le discriminant de Θ dans K, donc il n'est pas nul. Par suite, je puis exprimer inversement chacun des N produits $A_i^{-1} \times V_1^{(i)} \times A_i$ en fonction linéaire à coefficients scalaires (dans K) de $P_1, P_2, \ldots, P_N$.

Si $P_1, P_2, \ldots, P_N$ sont tous scalaires, il résulte des faits précédents que chaque produit $A_i^{-1} \times V_1^{(i)} \times A_i$, et notamment $V_1 = A_N^{-1} \times V_1^{(N)} \times A_N$, est aussi un scalaire. Il suffit donc de choisir pour V_1 une matrice non scalaire pour obtenir parmi les N matrices $P_1, P_2, \ldots, P_N$ au moins une solution non scalaire du système (M).

Je considère une telle matrice P non scalaire; si P est irrégulière, (F) est équivalente à Oy et tous les corps de nombres algébriques sont corps de représentation de (F). Si P est régulière, elle vérifie une équation déterminée du deuxième degré à coefficients scalaires de K (équation en λ ou équation caractéristique de cette matrice) :

$$f(P) = P^2 - (a + d) P + ad - bc = 0,$$

pour la matrice

$$P = \left\| \begin{matrix} a & c \\ b & d \end{matrix} \right\| \qquad (bc \neq 0 \text{ ou } a \neq d, \quad \text{matrice non scalaire}).$$

Mais les relations (M) montrent que les conjugués de P vérifient aussi cette équation, car

$$f(P^{(i)}) = f(A_i^{-1} \times P \times A_i) = A_i^{-1} \times f(P) \times A_i = 0.$$

Donc les polynomes caractéristiques des matrices $P^{(i)}$, polynomes qui ne sont autres que les conjugués de $f(x)$, sont tous identiques à $f(x)$; il en résulte que les coefficients de $f(x)$ sont nécessairement rationnels.

Les zéros ω et ω' du polynome $f(x)$ à coefficients rationnels définissent un corps algébrique K_1 qui est soit l'ensemble de tous les nombres rationnels, soit un corps quadratique. Je change au besoin le choix du corps K de façon qu'il contienne le corps K_1 et je montre que K_1 *est corps de représentation de* (F). En effet, la matrice

$$P_0 = \| P - \omega \| = \left\| \begin{matrix} a - \omega & c \\ b & d - \omega \end{matrix} \right\|,$$

est une matrice irrégulière solution du système relatif (M) dans K_1. D'une part, le déterminant de cette matrice est $f(\omega)$, donc est nul. D'autre part, P vérifie le système absolu (M), donc à fortiori le système relatif; en désignant par $\Theta_{i'}$ les conjugués *relatifs* de Θ par rapport à K_1, j'obtiens

$$P_0^{(i')} \times A_{i'} = \| P^{(i')} \times A_{i'} - \omega \times A_{i'} \| = \| A_{i'} \times P - A_{i'} \times \omega \| = A_{i'} \times P_0,$$

puisque les conjugués relatifs $\omega_{i'}$ sont égaux à ω et que ω est permutable avec toute matrice.

Le théorème est ainsi démontré.

VI. — Le second théorème.

Puisque j'ai obtenu un corps quadratique de représentation de (F), je puis former dans un tel corps un système d'équivalence absolue entre Oy et (F). De ce système, je vais déduire une conique rationnelle (C) et établir qu'elle est équivalente à (F). Ce qui démontrera le second théorème de Nœther-Poincaré.

Je suppose donc que le corps K est un corps quadratique et je choisis dans ce corps un nombre primitif Θ dont le carré soit un nombre rationnel b. Le nombre Θ a seulement deux conjugués absolus $\Theta_1 = -\Theta$ et $\Theta_2 = \Theta$. Le système de matrices associé à (F) comprend deux matrices dont la seconde A_2 peut être choisie identique à l'unité. Les relations de compatibilité matricielles sont

$$A_1^{(1)} = A_2 \times A_1^{-1} \times a_{1,1}, \qquad A_2^{(1)} = A_1 \times A_1^{-1} \times a_{2,1},$$
$$A_1^{(2)} = A_1 \times A_2^{-1} \times a_{1,2}, \qquad A_2^{(2)} = A_2 \times A_2^{-1} \times a_{2,2};$$

elles se réduisent à

$$a_{1,2}=a_{2,1}=a_{2,2}=1, \qquad a_{1,1}=A_1^{(1)}\times A_1=A_1\times A_1^{(1)}.$$

Le nombre $a_{1,1}$ est égal à son conjugué, c'est un nombre rationnel que je désigne encore par a.

Le système d'équivalence entre Oy et (F) comprend deux relations dont la seconde est identiquement vérifiée; la première est

$$(\mathcal{L})^{(1)}\times(\mathcal{A}_1)=(\mathcal{L});$$

qui est équivalente à l'équation matricielle en L et λ

$$L^{(1)}\times A_1=\lambda\times L,$$

où λ est un scalaire de K.

Je décompose L, A_1 et λ en fonctions linéaires à coefficients rationnels de Θ

$$L=\overline{L}+\Theta\overline{L'}, \qquad A_1=\overline{A}_1+\Theta\overline{A'_1}, \qquad \lambda=\overline{\lambda}+\Theta\overline{\lambda'};$$

la relation précédente est équivalente à l'équation en $\overline{L}$, $\overline{L'}$, $\overline{\lambda}$, $\overline{\lambda'}$:

$$\left(\overline{L}-\Theta\overline{L'}\right)\times\left(\overline{A}_1+\Theta\overline{A'_1}\right)=\left(\overline{\lambda}+\Theta\overline{\lambda'}\right)\times\left(\overline{L}+\Theta\overline{L'}\right),$$

ou encore au système à coefficients rationnels

$$\begin{gathered}\overline{L}\times\left(\overline{A}_1-\overline{\lambda}\right)-b\times\overline{L'}\times\left(\overline{A'_1}+\overline{\lambda'}\right)=0,\\ \overline{L}\times\left(\overline{A'_1}-\overline{\lambda'}\right)-\overline{L'}\times\left(\overline{A}_1+\overline{\lambda}\right)=0.\end{gathered}$$

Pour que ce système ait une solution en matrices régulières $\overline{L}$, $\overline{L'}$, il est nécessaire que

$$\overline{A}_1^2-\overline{\lambda}^2-b\times\overline{A'_1}^2+b\times\overline{\lambda'}^2=0.$$

Dans cette égalité,

$$\overline{A}_1^2-b\times\overline{A'_1}^2=\left(\overline{A}_1+\Theta\overline{A'_1}\right)\times\left(\overline{A}_1-\Theta\overline{A'_1}\right)$$

n'est autre que le produit $A_1\times A_1^{(1)}=a$. La recherche des nombres rationnels $\overline{\lambda}$, $\overline{\lambda'}$ vérifiant la relation

$$a-\overline{\lambda}^2+b\overline{\lambda'}^2=0$$

est équivalente à la recherche des points rationnels sur la conique (C)

$$x^2-by^2-az^2=0.$$

Cette conique (C) admet une représentation unicursale propre $(\mathcal{C})$ à coefficients dans K,

$$\frac{x}{au^2+v^2}=\frac{\Theta y}{au^2-v^2}=\frac{z}{2uv}; \qquad \frac{u}{z}=\frac{v}{x-\Theta z}.$$

Le système de matrices *associé à la conique* (C) est donc

$$\begin{Vmatrix} 0 & a \\ 1 & 0 \end{Vmatrix}, \quad \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix} = 1;$$

et le système de scalaires *associé à la même conique est* a, 1, 1, 1. D'après les résultats du paragraphe III, la conique (C) est équivalente à (F). Le second théorème de Noether-Poincaré est démontré.

Enfin je rappelle le critère de Lagrange :

Pour qu'il existe des points rationnels sur la conique (C)

$$x^2 - by^2 - az^2 = 0,$$

il faut et il suffit que l'entier b soit resté quadratique (*mod. a*).

M. Hasse [9] a montré qu'il était intéressant d'énoncer ce théorème sous la forme suivante :

Pour qu'il existe des points rationnels sur la conique (C), *il faut et il suffit que* (C) *soit équivalente à* Oy *dans tout corps p-adique*, *p nombre premier arbitraire*.

CHAPITRE II.

ÉTUDE GALOISIENNE DES VARIÉTÉS DE BRAUER.

Je vais généraliser les méthodes du premier Chapitre en vue de problèmes plus complexes. D'une part, au lieu d'étudier des courbes, j'étudie des variétés d'un hyper-espace de dimension arbitraire; d'autre part, au lieu de ne considérer que des courbes et des correspondances à coefficients rationnels, j'envisage des variétés et des correspondances à coefficients dans un corps Ρ [9bis] quelconque, mais fixé à priori. Je définis ainsi l'équivalence, au sens de Poincaré, des variétés dans le corps Ρ; l'équivalence absolue, étudiée au premier Chapitre, n'est autre que l'équivalence dans le corps $Ρ_0$ des nombres rationnels. Comme je n'ai étudié dans le premier Chapitre que l'équivalence des courbes unicursales, j'étudie seulement dans ce mémoire l'équivalence des *variétés de Brauer* du corps Ρ.

Ce Chapitre est consacré aux premiers résultats de cette étude : définition des problèmes d'équivalence entre variétés de Brauer de Ρ et mise en équation de ces problèmes suivant la méthode galoisienne; ce qui généralise les paragraphes I, II et IV du Chapitre I.

---

(9) *Voir* le Mémoire cité dans la note (6) et les Mémoires du *Journal de Crelle*, Bd. 152, 1923, S. 129-148, *et* 205-224; Bd. 153, 1923, S. 113-130 et 158-162.

(9bis) La lettre Ρ est la majuscule de la lettre grecque ρ, il ne faut pas la confondre avec P (p français majuscule).

I. — Système d'équivalence entre deux variétés de Brauer.

Dans le premier Chapitre, j'ai introduit, incidemment, un système d'équivalence *relative dans un corps* K_1 entre deux courbes unicursales et rationnelles. Il est utile de généraliser ce procédé : je vais étudier non seulement les correspondances birationnelles à coefficients rationnels entre deux courbes, qui définissent l'équivalence absolue, mais aussi les correspondances birationnelles à coefficients dans un corps P quelconque qui définissent l'équivalence (relative) dans ce corps P. Parallèlement, j'étudie, en généralisation des problèmes diophantiens sur les courbes rationnelles, la recherche des points à coordonnées dans P sur les courbes à coefficients dans P, recherche que j'appelle problème diophantien (relatif) dans P.

Le corps K_1 utilisé au premier Chapitre est un corps de nombres algébriques; j'élargis également cette hypothèse. L'énoncé du critère de Lagrange donné par H. Hasse montre en effet l'intérêt de la notion d'équivalence par rapport à un corps local de Hensel; et c'est sous cette forme que j'ai pu généraliser ce critère. J'envisage donc le cas d'un *corps de base* P quelconque; ce qui soulève plusieurs difficultés : qu'appelle-t-on courbe, point, correspondance dans un tel corps ? Dans la *Géométrie galoisienne*, j'ai réuni les définitions précises des êtres géométriques dans le corps P et j'ai étudié les relations les plus simples existant entre eux, formant ainsi les éléments d'une géométrie dans ce corps.

D'autre part, je désire étudier non plus les courbes, mais les variétés. Alors que la définition de l'équivalence, telle qu'elle a été donnée par Poincaré, s'impose pour les courbes planes, on peut envisager plusieurs notions d'équivalence pour les variétés d'un hyper-espace, suivant la nature des correspondances recherchées entre ces variétés. Dans la *Géométrie galoisienne*, j'ai défini les correspondances homographiques (elles admettent des formules du premier degré); les correspondances birationnelles (elles admettent des correspondances inverses et ne sont pas dégénérées entre les variétés sur lesquelles elles opèrent); les correspondances de Poincaré (elles sont birationnelles et tous leurs points critiques sont isolés). Ce sont ces dernières qui définissent *l'équivalence au sens de Poincaré* que j'envisage ici (je dirai par la suite *équivalence* au lieu de *équivalence au sens de Poincaré* lorsqu'il n'y aura pas de confusion à craindre).

J'étudie donc l'équivalence dans un corps de base P des variétés de ce corps; je me limite aux *variétés de Brauer* de P, ou variétés de P équivalentes à un espace de référence, dans l'extension algébriquement fermée Ω de P. J'ai donné dans la *Géométrie galoisienne* un procédé pour reconnaître si une variété donnée (F) de P est une variété de Brauer; ce procédé permet, le cas échéant, de construire dans Ω une représentation de Poincaré de (F), c'est-à-dire une correspondance de Poincaré entre un espace de référence et (F), ce qui est nécessaire pour pouvoir appliquer à (F) les méthodes de ce mémoire. J'ai aussi défini pour les êtres géométriques d'une extension k de P, la notion de conjugué introduite au Chapitre I pour les correspondances à coefficients algébriques. Ce qui m'a permis de démontrer les *critères de Galois* qui généralisent une propriété utilisée au Chapitre I, paragraphe I. Je puis alors aborder la recherche des correspondances de Poincaré dans le corps de base P entre deux variétés données de P, généralisation de l'étude du paragraphe I du Chapitre précédent.

Je rappelle les propriétés ainsi obtenues en indiquant les particularités qui se présentent ici dans le cas de deux variétés de Brauer. J'ai considéré deux variétés de P équivalentes entre elles dans l'extension algébriquement fermée Ω de P; ce sont ici deux variétés de Brauer de P de même dimension r. J'ai considéré une variété de comparaison (A) équivalente à (F) et à (F′) dans P : c'est ici l'espace de référence (E_r) de dimension r. J'ai construit deux correspondances de Poincaré à coefficients algébriques et séparables par rapport à P

$$(\mathcal{F}) : \quad \text{espace } (E_r) \to \text{variété } (F),$$
$$(\mathcal{F}') : \quad \text{espace } (E_r) \to \text{variété } (F');$$

ce sont ici des représentations de Poincaré de (F) et de (F′). Je choisis une extension finie et séparable k de P contenant $(\mathcal{F})$ et $(\mathcal{F}')$, (cette extension n'est pas nécessairement normale comme au Chapitre I); je désigne par K l'extension normale de P engendrée par k. Enfin, le groupe des correspondances de Poincaré (G. P. $_{\mathrm{P}}E_r$) de P sur (E_r), ou plus généralement (G. P. $_{k}E_r$) de k sur (E_r), est formé par toutes les homographies non dégénérées sur (E_r) à coefficients dans P, ou dans k.

Si je considérais l'équivalence birationnelle et les variétés unicursales de P (ou variétés birationnellement équivalentes dans Ω à un espace de référence), ce n'est pas ce groupe (G. P. $_{\mathrm{P}}E_r$) qu'il me faudrait considérer, mais le groupe (G. R. $_{\mathrm{P}}E_r$) des correspondances birationnelles de P sur (E_r); ce dernier groupe est formé par les correspondances de Cremona sur (E_r), correspondances plus complexes que les correspondances homographiques et dont la connaissance actuelle semble insuffisante pour résoudre les problèmes de ce Mémoire.

Le résultat fondamental est le suivant :

(E) — *Les correspondances de Poincaré de* P *entre* (F′) *et* (F)

$$(\mathcal{R}) : \quad \text{variété } (F') \to \text{variété } (F)$$

peuvent être déterminées par la formule

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

dans cette formule, la correspondance $(\mathcal{L})$ *est une homographie non dégénérée sur* (E_r), *arbitraire, à coefficients dans* k, *qui vérifie les équations en* $(\mathcal{L})$

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

où les $(\mathfrak{A}_i)$ *et les* $(\mathfrak{A}'_i)$ *sont les homographies non dégénérées sur* (E_r) *définies par*

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

La formule (E, 1) *établit une correspondance biunivoque entre les correspondances* $(\mathcal{R})$ *et les solutions* $(\mathcal{L})$ *du système* (E, 2).

En particulier, **pour que** (F) **et** (F′) **soient équivalentes dans** P, **il faut et il suffit que le système d'équations** (E, 2) **soit vérifié par au moins une homographie** $(\mathcal{L})$ **de k, non dégénérée sur** (E_r).

Le système (E, 2) est le **système d'équivalence dans** P **entre** (F′) **et** (F), par abréviation de « système des équations d'équivalence dans P entre (F′) et (F), déduit des éléments de comparaison : espace (E_r), représentations $(\mathcal{F})$ et $(\mathcal{F}')$, corps K ».

Les homographies $(\mathfrak{A}_i)$ [et les homographies $(\mathfrak{A}'_i)$] vérifient les relations

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

ces relations sont appelées **relations de compatibilité du système d'équivalence** (E, 2).

Je puis notamment former un système d'équivalence entre la variété (F) et elle-même; il est indiqué de choisir dans ce cas les représentations de comparaison $(\mathcal{F})$ et $(\mathcal{F}')$ identiques entre elles. Les homographies $(\mathfrak{A}_i)$ et $(\mathfrak{A}'_i)$ sont respectivement identiques deux à deux; le système d'équivalence ainsi formé a au moins une solution, l'homographie identique sur (E_r). De façon plus précise, *les solutions de ce système forment un groupe multiplicatif*, que je désigne par (G. E. $_{\rm P}$F) et qui est isomorphe au groupe (G. P. $_{\rm P}$F) [groupe des correspondances de Poincaré sur (F) dans P].

Si un système d'équivalence entre (F′) et (F) a au moins une solution $(\mathcal{L}_1)$, toutes ses solutions s'obtiennent soit en multipliant $(\mathcal{L}_1)$ à droite par un élément quelconque de (G. E. $_{\rm P}$F), soit en multipliant $(\mathcal{L}_1)$ à gauche par un élément quelconque de (G. E. F′). Dans ce cas, les groupes (G. E. $_{\rm P}$F) et (G. E. $_{\rm P}$F′) sont isomorphes entre eux.

II. — Problèmes diophantiens et notion de similitude.

Comme au Chapitre I, le système d'équivalence permet, outre la recherche des correspondances de Poincaré de P entre (F′) et (F), la recherche des points de (F) qui sont dans P. Il permet même une généralisation de ce dernier problème : la recherche de certaines sous-variétés de (F) que je nomme sous-variétés normales de (F) dans P.

J'appelle encore **système étendu d'équivalence entre** (F′) **et** (F), le système d'équations en ($\mathfrak{T}$)

$$(E', 2) \qquad (\mathfrak{T})^{(i)} \times (\mathfrak{A}_i) = (\mathfrak{A}'_i) \times (\mathfrak{T}) \qquad (i = 1, 2, \ldots, n),$$

où ($\mathfrak{T}$) est une correspondance simplement rationnelle sur (E_r) à coefficients dans k. Je rappelle la propriété démontrée dans la *Géométrie galoisienne* :

(E′) — Si une correspondance (simplement rationnelle) de p

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

transforme (F′) en une sous-variété *simple* de (F), elle peut-être déterminée par la formule

$$(E', 1) \qquad (\mathfrak{C}) = (\mathcal{F}')^{-1} \times (\mathfrak{T}) \times (\mathcal{F});$$

dans cette formule, ($\mathfrak{T}$) est un élément quelconque de (E. C. ${}_kE_r$), [ensemble des correspondances sur (E_r) dans k], vérifiant le système étendu d'équivalence

$$(E', 2) \qquad (\mathfrak{T})^{(i)} \times (\mathfrak{A}_i) = (\mathfrak{A}'_i) \times (\mathfrak{T}) \qquad (i = 1, 2, \ldots, n).$$

La relation entre ($\mathfrak{T}$) et ($\mathfrak{C}$) est encore biunivoque.

J'en déduis la propriété suivante :

Les points simples de (F) *qui sont dans* p *peuvent être déterminés biunivoquement par les solutions* (homographiques et dégénérées) *de* (E′, 2) *qui transforment* (E_r) *en un point.*

En effet, un point *simple* M de p sur (F) définit une correspondance dégénérée entre (F′) et (F)

$$(\mathfrak{C}) : \qquad \text{variété}(F) \rightarrow \text{le point } M,$$

à laquelle s'applique la propriété (E′); l'élément de (E. C. ${}_kE_r$) ainsi obtenu transforme (E_r) en un point, c'est une homographie dégénérée de cet espace (de nature particulière d'ailleurs). Réciproquement, si une solution (nécessairement homographique et dégénérée) de (E′, 2) transforme (E_r) en un point, elle détermine une correspondance qui transforme (F′) en un point de (F) qui est dans p.

Plus généralement, toute solution ($\mathfrak{T}$) dégénérée du système (E′, 2) définit une sous-variété (G) de (F) dans p, à savoir la sous-variété transformée de (F′) par la correspondance $(\mathfrak{C}) = (\mathcal{F}')^{-1} \times (\mathfrak{T}) \times (\mathcal{F})$, ou, ce qui revient au même, la transformée de (E_r) par la correspondance $(\mathfrak{T}) \times (\mathcal{F})$. On peut encore représenter cette sous-variété (G) par une *variété-image* dans (E_r) : la transformée de (E_r) par ($\mathfrak{T}$); la sous-variété (G) est la transformée par ($\mathcal{F}$) de sa variété-image.

Parmi ces sous-variétés (G), les plus importantes sont celles qui sont définies par des solutions $(\mathcal{T})$ *homographiques* (dégénérées) de $(E', 2)$, c'est-à-dire celles dont les variétés-images sont des *sous-espaces* de (E_r). Je les appelle **sous-variétés normales de** (F) **dans** P.

La notion de sous-variété normale est indépendante du choix du système d'équivalence étendu $(E', 2)$. Changer ce système revient à multiplier $(\mathcal{F})$ et $(\mathcal{F}')$ par des correspondances homographiques $(\mathcal{L})$ et $(\mathcal{L}')$ non dégénérées sur (E_r); une sous-variété (G) de (F), normale dans le premier système, admet, dans ce système, une variété-image qui est un sous-espace (E) de (E_r); (G) admet, dans le second système, pour variété-image la transformée (E') de (E) par $(\mathcal{L})^{-1}$, puisque $(\mathcal{L})\times(\mathcal{F})$ transforme cette variété (E') en (G); (E') est aussi un sous-espace de (E_r), donc (G) est aussi une variété normale de F dans le second système.

Je vais établir quelques propriétés importantes de ces sous-variétés normales.

Toute sous-variété normale (G) *de* (F) *dans* P *est une variété de Brauer de* P; *le groupe* (G. E. $_P$G) *est homomorphe à un sous-groupe de* (G. E. $_P$F).

Par définition une sous-variété normale (G) de (F) dans P est équivalente dans Ω (extension algébriquement fermée de P) à sa variété-image (E), car la correspondance $(\mathcal{F})$ définit une correspondance de Poincaré entre (E) et (G). Le sous-espace (E) de (E_r) est lui-même équivalent à un espace de référence; donc (G) est équivalente dans Ω à un espace de référence, c'est une variété de Brauer. C'est d'ailleurs une variété de P, comme toute variété définie par une solution dégénérée de $(E', 2)$.

Pour étudier plus facilement le groupe (G. E. $_P$G), je forme le système d'équivalence étendu $(E', 2)$ de façon que la variété-image de (G) soit un espace de référence. Ce que je puis faire de la façon suivante : je suppose que j'ai choisi, sans précaution, le système $(E', 2)$, que (G) est définie dans ce système par l'homographie dégénérée $(\mathcal{T}_1)$ sur (E_r) et que $(\mathcal{T}_1)$ transforme (E_r) en le sous-espace (E) [qui est la variété-image de (G) dans le système $(E', 2)$ d'équivalence]. L'espace (E) est dans k et je sais former dans k une homographie non dégénérée $(\mathcal{L}_1)$ qui transforme (E) en un espace de référence (E_q) (tel que $q<r$, bien entendu). Je remplace le système $(E', 2)$ par le système déduit des éléments de comparaison suivants : l'espace (E_r), la correspondance $(\mathcal{F}_1)=(\mathcal{L}_1)^{-1}\times(\mathcal{F})$ entre (E_r) et (F), le corps k. Pour ce nouveau système, la variété (G) est définie par l'homographie dégénérée $(\mathcal{T}_1)\times(\mathcal{L}_1)$, car le produit

$$(\mathcal{T}_1)\times(\mathcal{L}_1)\times(\mathcal{F}_1)=(\mathcal{T}_1)\times(\mathcal{L}_1)\times(\mathcal{L}_1)^{-1}\times(\mathcal{F})=(\mathcal{T}_1)\times(\mathcal{F})$$

transforme, par hypothèse (E_r) en (G). Comme $(\mathcal{T}_1)\times(\mathcal{L}_1)$ transforme (E_r) en (E_q), la variété-image de (G) dans ce nouveau système est (E_q).

La trace sur (E_q) de la correspondance $(\mathcal{F}_1)$ est alors une représentation de Poincaré de (G) dans k. Je puis donc former un système d'équivalence entre (G) et elle-même en choisissant comme éléments de comparaison : l'espace (E_q), la correspondance trace de $(\mathcal{F}_1)$ sur (E_q), le corps k. Les homographies $(\mathcal{B}_i)$, coefficients du système d'équivalence ainsi formé, entre (G) et elle-même, sont les traces sur (E_q) des homographies $(\mathcal{A}_i)$, coefficients du système d'équivalence (E, 2) entre (F) et elle-même et le groupe (G. E, $_{\mathrm{P}}$G) contient les traces sur (E_q) des éléments de (G. E. $_{\mathrm{P}}$G) qui conservent cet espace. Inversement tout élément $(\mathcal{T})$ de (G. E. $_{\mathrm{P}}$G) est la trace d'au moins un élément de (G. E. $_{\mathrm{P}}$F) : la correspondance obtenue en effectuant sur les coordonnées relatives à (E_q) la transformation $(\mathcal{T})$ et en laissant invariantes les autres coordonnées. Donc le groupe (G. E. $_{\mathrm{P}}$G) est homomorphe à un sous-groupe de (G. E. $_{\mathrm{P}}$F), à savoir le sous-groupe formé par les éléments de ce dernier groupe qui laisse invariant l'espace de référence (E_q). Ces faits seront d'ailleurs encore précisés par la suite (Ch. IV, § II).

Je dis que *deux variétés de* P sont *semblables entre elles dans* P, *s'il existe une sous-variété normale de l'une équivalente à une sous-variété normale de l'autre.* Cette condition de similitude n'exige pas, comme la condition d'équivalence, que les variétés aient même dimension.

La condition nécessaire et suffisante pour qu'une variété de Brauer (F) de P contienne des points de P est qu'elle soit semblable dans P à un point. Les problèmes diophantiens sur deux variétés de Brauer semblables ne sont pas essentiellement distincts : si l'un est résoluble, l'autre l'est aussi. L'étude de la similitude ne me paraît cependant pas suffisante; car je désire non seulement étudier l'existence des points de P sur une variété de Brauer (F) donnée, mais aussi obtenir *tous* ces points par un procédé rationnel. C'est en vue de ce problème que j'établis ci-dessous la généralisation suivante du premier théorème de Nœther-Poincaré :

Une variété de Brauer semblable dans P *à un point est équivalente dans* P *à un espace de référence.*

Les relations qui existent entre la notion de similitude et celle d'équivalence sont encore précisées par le théorème suivant que j'établis aussi ci-dessous :

Si deux variétés de Brauer de P *semblables entre elles ont même dimension, elles sont équivalentes entre elles, dans* P.

III. — Introduction de relations matricielles.

Comme au paragraphe IV du Chapitre I, j'utilise la représentation matricielle des homographies par des matrices. J'indique les rapports qui existent entre ces homographies et ces matrices; je forme les relations entre matrices qui peuvent remplacer les relations entre homographies envisagées aux paragraphes précédents. Enfin, j'établis une propriété importante généralisant celle de l'association d'une courbe à un ensemble de scalaires (Chap. I, § IV).

Je puis définir une homographie $(\mathcal{L})$ de P sur (E_r) par des relations linéaires en $x_0, x_1, \ldots, x_r$ dans P

$$\frac{y_0}{a_0 x_0 + \ldots + a_r x_r} = \frac{y_1}{b_0 x_0 + \ldots + b_r x_r} = \ldots = \frac{y_r}{l_0 x_0 + \ldots + l_r x_r},$$

et représenter cette homographie par la matrice

$$L = \begin{Vmatrix} a_0 & b_0 & . & . & . & l_0 \\ a_1 & b_1 & . & . & . & l_1 \\ . & . & . & . & . & . \\ a_r & b_r & . & . & . & l_r \end{Vmatrix}.$$

Si L est *régulière*, l'homographie $(\mathcal{L})$ n'est pas dégénérée et réciproquement. L'homographie $(\mathcal{L})$ transforme alors l'espace (E_r) en lui-même et chaque point de (E_r) est le transformé d'un seul point de (E_r) dans $(\mathcal{L})$. Les polynomes qui déterminent $(\mathcal{L})$ sont définis au produit près par une même fraction rationnelle. Pour que ces polynomes restent linéaires, il faut que ce facteur multiplicatif soit un élément de P, car ces polynomes sont premiers entre eux. La matrice L est définie au produit près par un scalaire arbitraire λ de P.

Si L est *irrégulière*, l'homographie $(\mathcal{L})$ est dégénérée et réciproquement. L'homographie $(\mathcal{L})$ transforme alors l'espace (E_r) en un sous-espace (E') dont la dimension est égale au rang de L diminué d'une unité; chaque point de (E_r) est le transformé dans $(\mathcal{L})$ d'un sous-espace de (E_r). La matrice L est définie au produit près à gauche par certaines matrices dont il n'est pas utile de préciser davantage la nature.

Le *produit de deux matrices*, régulières ou non, représente le produit des homographies représentées par chacun des facteurs. Si deux matrices, régulières ou non, représentent la même homographie, leur somme représente aussi cette homographie.

Le système d'équivalence (E. 2) entre (F') et (F) est équivalent au système matriciel d'équations en L et λ_i

$$\text{(E. M. 2)} \qquad L^{(i)} \times A'_i = A_i \times L \times \lambda_i \qquad (i = 1, 2, \ldots, n);$$

A_i est une matrice à termes dans K qui représente l'homographie $(\mathcal{A}_i)$, A'_i une matrice à termes dans K qui représente $(\mathcal{A}'_i)$; L est une matrice *régulière* arbitraire à termes dans k, les λ_i des scalaires arbitraires de K. La condition nécessaire et suffisante pour que (F) et (F') soient équivalentes dans P est encore que *le système d'équations* (E. M. 2) *ait au moins une solution en* L, $\lambda_1, \lambda_2, \ldots, \lambda_n$.

Je ne cherche pas à quoi est équivalent le système étendu d'équivalence, puisque les solutions de ce système ne sont pas nécessairement des homographies. Je constate seulement que si P est une matrice, régulière ou non, à termes dans k qui vérifie les relations

$$P^{(i)} \times A_i = A'_i \times P \qquad (i = 1, 2, \ldots, n);$$

elle représente une solution homographique du système étendu (E', 2).

Les relations de compatibilité (E, 3) sont équivalentes aux relations de compatibilité matricielles

$$\text{(C. M.)} \qquad \sigma(A_i) = A_k \times A_j^{-1} \times a_{\sigma,i}, \qquad \text{si} \quad \begin{cases} \sigma(0) = 0_j, \\ \sigma(0_i) = 0_k, \end{cases}$$

où les $a_{\sigma,i}$ sont des scalaires de K, qui sont d'ailleurs déterminés par les matrices A_i.

Une représentation de Poincaré ($\mathcal{F}$) d'une variété de Brauer (F) de P donnée étant choisie, je puis former l'ensemble des n matrices A_i, puis calculer les $n.N$ scalaires $a_{\sigma,i}$; j'appelle **système de matrices associé dans P à** (F) l'ensemble des matrices A_i et **système de scalaires associé dans P à** (F) l'ensemble des scalaires $a_{\sigma,i}$.

Si deux variétés (F) et (F') sont associées au même système de matrices A_i, elles sont équivalentes; car le système matriciel (E. M. 2) a alors au moins une solution : L matrice unité, $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 1$. Je vais démontrer que :

Si deux variétés de Brauer (F) *et* (F') *de* P *sont associées au même système de scalaires* $a_{\sigma,i}$, *elles sont semblables entre elles dans* P.

[C'est la généralisation de la propriété du paragraphe IV, Chapitre I].

Je considère deux variétés de Brauer (F) et (F') de P associées au même système de scalaires $a_{\sigma,i}$, dont les dimensions r et r' peuvent être différentes.

Il est aisé de former une variété, semblable à une variété donnée (F) de dimension donnée $r_1 \geqq r$ et associée au même système de scalaires $a_{\sigma,i}$. Si (F) est une variété d'un espace (E_s) je choisis un système d'équation définissant (F) sur cet espace (E_s) et je considère la variété (F_1) définie sur l'espace (E_{s_1}), [où $s_1 - s = r_1 - r$], par ce système d'équations; (F_1) peut encore être définie par la représentation ($\mathcal{F}_1$) obtenue en ajoutant à un système de formules d'une représentation ($\mathcal{F}$) de (F) les relations

$$\frac{y_{s+1}}{x_{r+1}} = \frac{y_{s+2}}{x_{r+2}} = \ldots = \frac{y_{s_1}}{x_{r_1}}.$$

Le système de matrices associé à (F_1) s'obtient de la façon suivante : je borde chaque matrice A_i par $r_1 - r$ lignes et $r_1 - r$ colonnes identiques aux dernières lignes et colonnes d'une matrice unité (formées d'unités dans la diagonale principale et de zéros partout ailleurs). Les variétés (F) et (F_1) sont toutes deux associées au système de scalaires $a_{\sigma,i}$; la variété (F) est une sous-variété normale de (F_1) qui peut être définie, dans un système d'équivalence entre (E_{r_1}) et (F_1) par une homographie dégénérée qui transforme (E_{r_1}) en (E_r).

Je puis ainsi former deux variétés de Brauer respectivement semblables à (F) et à (F′) et de même dimension. De façon plus précise, je suppose avoir rangé (F) et (F′) dans un ordre tel que $r \geqq r'$; je garde la variété $(F_1)=(F)$ et je remplace la variété (F′) par une variété semblable (F'_1), associée au même système de scalaires et de dimension r. Je désigne par A_i et A'_i les systèmes de matrices respectivement associées à (F_1) et à (F'_1), intervenant dans le système matriciel correspondant; elles vérifient les relations de compatibilité matricielles

$$\sigma(A_i) = A_k \times A_j^{-1} \times a_{\sigma,i},$$
$$\sigma(A'_i) = A'_k \times A'^{-1}_j \times a_{\sigma,i}.$$

A partir d'une matrice carrée V d'ordre r, arbitraire, à termes dans k, je forme la somme

$$P = \sum A'^{-1}_i \times V^{(i)} \times A_i \qquad (i \text{ de } 1 \text{ à } n).$$

Cette somme est *a priori* une matrice à termes dans K; les relations de compatibilité matricielles précédentes permettent d'obtenir les conjugués par rapport à P de cette matrice

$$\sigma(P) = \sum_i [\sigma(A'_i)^{-1} \times V^{(k)} \times \sigma(A_i)] = \sum_i [a_{\sigma,i}^{-1} \times A'_j \times A'^{-1}_k \times V^{(k)} \times A_k \times A_j^{-1} \times a_{\sigma,i}]$$
$$= A' \times \left[\sum_k (A'^{-1}_k \times V^{(k)} \times A_k)\right] \times A_j^{-1} = A'_j \times P \times A_j^{-1}.$$

On voit que $\sigma(P)$ ne dépend que du conjugué $\theta_j = \sigma(\theta)$ de θ; d'après les critères de Galois, P est donc une matrice à termes dans k et $\sigma(P)$ est la $j^{\text{ème}}$ conjuguée $P^{(j)}$. Enfin P représente une homographie ($\mathfrak{T}$) de k, dégénérée ou non, qui vérifie les relations

$$(\mathfrak{T})^{(j)} \times (\mathfrak{A}_j) = (\mathfrak{A}'_j) \times (\mathfrak{T}) \qquad (j = 1, 2, \ldots, n);$$

($\mathfrak{T}$) est une solution homographique du système étendu d'équivalence (E′, 2).

Si P *est régulière*, ($\mathfrak{T}$) est une solution du système d'équivalence proprement dit (E, 2); (F_1) et (F'_1) sont équivalentes, donc (F) et (F′) sont semblables entre elles dans P.

Si P *est irrégulière*, elle définit une sous-variété canonique (F_2) de (F_1) dans P. Je remplace alors le couple (F_1), (F'_1) par le couple (F_2), $(F'_2)=(F'_1)$; ce dernier est formé de variétés respectivement semblables à celles du couple précédent; la plus grande des dimensions de (F_2) et (F'_2) est inférieure (et non égale) à la plus grande des dimensions de (F_1) et (F'_1). Je range (F_2) et (F'_2) par ordre décroissant des dimensions et je recommence sur ce nouveau couple les opérations déjà effectuées sur le couple (F_1), (F'_1). Comme précédemment, ou bien je constate la similitude de (F_2) et (F'_2), ou bien je construis un troisième couple (F_3), (F'_3) de variétés respectivement semblables à (F_2) et (F'_2) tel que la plus grande des dimensions de (F_3) et (F'_3) soit inférieure (et non égale) à la plus grande des dimensions de (F_2) et (F'_2). Et ainsi de suite. Je remplace ainsi le couple (F), (F') successivement par des couples (F_u), (F'_u) (u entier), de variétés respectivement semblables à (F) et (F'); à chaque opération le maximum des deux dimensions de (F_u) et (F'_u) diminue. Ou bien ces opérations s'arrêtent lorsque je constate la similitude des variétés (F_u), (F'_u) d'un couple ainsi formé; ou bien j'obtiens finalement un couple (F_u), (F'_u) de variétés réduites chacune à un point de P. Comme deux points de P sont des variétés équivalentes entre elles dans P, les variétés (F) et (F') sont, dans tous les cas, semblables entre elles dans P.

CHAPITRE III.

RECOURS A LA THÉORIE DES ALGÈBRES.

Je pourrais continuer simplement à généraliser les méthodes du Chapitre I, comme je l'ai fait au Chapitre précédent. Mais il se trouve qu'une partie des résultats peut se déduire de la Théorie des Algèbres, constituée et étudiée pour un but tout à fait différent par Wedderburn, Dickson, R. Brauer, E. Nœther, Hasse, etc. L'étude actuelle devient par suite une application inédite de cette théorie.

Je montre pour cela, dans ce chapitre, que les solutions homographiques d'un système étendu d'équivalence entre une variété de Brauer (F) et elle-même peuvent être représentées par un ensemble de matrices qui constituent une *Algèbre de Brauer* [10] sur le corps de base P, que j'appelle *associée à la variété* (F) *dans* P. Je montre que les critères d'équivalence et de similitude entre variétés de Brauer peuvent être exprimés simplement par des conditions connues concernant les algèbres associées, ce qui permet d'établir un ensemble de propriétés constituant l'extension des deux théorèmes de Nœther-Poincaré.

I. — Les Algèbres de Brauer.

Je rappelle, dans ce paragraphe, les définitions et résultats de la Théorie des Algèbres qui me serviront par la suite [11].

---

[10] *Voir* au sujet de cette expression la note [4] de l'Introduction.

[11] Pour la Théorie des Algèbres, j'ai surtout utilisé l'exposé d'ensemble de Deuring : *Algebren*, paru dans la Collection des *Ergebnisse der Mathematik*, tome IV, fascicule 1. C'est à cet Ouvrage

Une *algèbre sur un corps* P est un anneau ([12]), non nécessairement commutatif, (O) contenant P et admettant par rapport à P une base finie $A_1, A_2, \ldots, A_l$; c'est-à-dire que tout élément A de (O) peut être mis sous la forme

$$A = \sum x_i A_i \quad (i \text{ de } 1 \text{ à } l), \tag{1}$$

où les x_i sont des éléments, ou scalaires, arbitraires du corps de base P. Une algèbre (O) est déterminée par une de ses bases, à condition de connaître, d'une part toutes les relations linéaires

$$\sum_i a_i A_i = 0 \quad (i \text{ de } 1 \text{ à } l;\quad \text{les } a_i \text{ scalaires de P}),$$

qui sont vérifiées par les éléments A_i de cette base; d'autre part une table de multiplication de ces éléments entre eux. Dans toute algèbre, il existe au moins une base *minima*, ou *réduite*, dont tous les termes sont *linéairement indépendants*, c'est-à-dire ne vérifient aucune relation linéaire. Par rapport à une telle base tout élément de (O) n'admet qu'une représentation de la forme (1); à l'élément nul correspondent notamment des a_i tous nuls. Toutes les bases réduites d'une même algèbre ont un même nombre d'éléments *qui est le rang de l'algèbre sur le corps de base* P.

Une *extension finie et séparable* k de degré n sur P est une algèbre commutative sur P de rang n; elle peut être définie par la base minima formée par les puissances $\theta, \theta^2, \ldots, \theta^n$ d'un élément primitif θ. L'ensemble des matrices carrées d'ordre r à termes dans P est une algèbre de rang r^2 sur P, appelée *anneau complet des matrices d'ordre r sur* P; elle peut être engendrée par la base minima formée par les r^2 matrices différentes dont un terme est égal à l'unité et dont tous les autres sont nuls.

Le *produit direct* de deux algèbres (O) et (O') sur P, définies respectivement par les bases minima $A_1, A_2, \ldots, A_l$ et $B_1, B_2, \ldots, B_{l'}$ est l'algèbre sur P définie par la base minima que forment les produits symboliques

$$A_i B_j \quad (i = 1, 2, \ldots, l;\ j = 1, 2, \ldots, l').$$

Le produit direct d'une algèbre (O) sur P et d'une extension finie k de P est

---

que je renvoie le lecteur pour les démonstrations non développées dans ce Mémoire et pour toute autre précision sur ce sujet. Il existe aussi des exposés français (plus anciens et moins complets) de la Théorie des Algèbres dans la Collection des Conférences au *Séminaire de mathématiques* dirigé par M. G. Julia, année 1932-1933, Conférences de Dubreil, Chevalley, Dieudonné, etc. et un exposé anglais de A. Adrian Albert dans le volume XXIV des *Colloques de l'American Math. Soc.* (1939). Enfin on trouvera quelques aperçus sur ces questions dans le tome II de la *Moderne Algebra* de Van der Waerden, Chapitres XV, XVI et XVII (2e édition).

([12]) Les notions d'*anneau*, de *corps*, d'*extension finie*, ..., sont définies dans la *Géométrie galoisienne*. On peut également en trouver un exposé dans plusieurs Traités classiques (*Moderne Algebra* de Van der Waerden; *Éléments de Mathématiques* de Bourbaki, Chapitre I du Livre II sur les structures algébriques).

donc identique, en tant qu'anneau, à l'algèbre sur k engendrée par une base minima formée d'éléments de (O) linéairement indépendants sur P. En particulier, l'anneau complet des matrices d'ordre r sur k est identique, en tant qu'anneau, au produit direct du corps k et de l'anneau complet des matrices d'ordre r sur P, considérés comme algèbres sur P.

On définit généralement les *algèbres normales et simples sur* P, ou **algèbres de Brauer sur** P, par des conditions concernant les éléments et les idéaux de ces anneaux [13]. J'utilise seulement la propriété caractéristique suivante :

Pour une algèbre de Brauer (O) sur P, il existe au moins une extension finie et séparable k de P qui soit *corps de décomposition* de (O)[14]; c'est-à-dire une extension finie et séparable k telle que le produit direct de (O) et de k, considéré comme algèbre sur P, soit isomorphe, en tant qu'anneau, à un anneau complet de matrices sur k.

Ceci est encore équivalent au fait que :

(O) *est isomorphe à un ensemble* (Ens. P) *de matrices carrées* P, *de même ordre* r, *à termes dans* k, *et telles que* :

1° *toute matrice carrée* V *d'ordre* r *à termes dans* k *est identique à une combinaison linéaire, à coefficients scalaires, d'éléments de* (Ens. P).

2° *Les seuls scalaires contenus dans* (Ens. P) *sont tous les scalaires de* P.

Il en résulte, en particulier, que le rang d'une Algèbre de Brauer (O) par rapport à P est égale à un carré r^2.

II. — Algèbre définie par un système de matrices.

Je vais maintenant établir la propriété des algèbres de Brauer qui permet d'associer une telle algèbre à chaque variété de Brauer. Cette propriété n'a pas encore été mentionnée, à ma connaissance, par les auteurs qui se sont occupés de ces questions.

Je considère une extension finie et séparable k de degré n du corps de base P et j'en choisis un élément primitif θ. J'utilise, comme au chapitre précédent,

---

(13) Une algèbre est normale (*normale Algebra*) quand les éléments du corps de base sont les seuls êtres permutables avec tous ses éléments (p. 9 des *Algebren*); elle est simple (*einfache Algebra*) si ses idéaux bilatères (invariants pour tout produit à droite et à gauche) sont les seuls idéaux triviaux : zéro et l'algèbre (O) elle-même (p. 17 des *Algebren*).

(14) La définition ci-dessus d'un corps de décomposition (*Zerfallungskörper*) est celle de la page 46 des *Algebren*; le théorème 18 de la page 47 de cet ouvrage montre l'existence d'un tel corps qui soit une extension finie et séparable du corps de base P, pour toute Algèbre de Brauer sur P. Quant au fait que l'existence d'un corps de décomposition soit une propriété caractéristique d'une telle algèbre, il résulte simplement des théorèmes 5 de la page 37 et 1 de la page 15 des *Algebren*.

les notations de la *Géométrie galoisienne* pour les conjugués des êtres numériques, algébriques et géométriques de k par rapport à p et pour les éléments du groupe de Galois G de k par rapport à p. En particulier K désigne le corps normal, extension de k.

J'appelle *système compatible de matrices* un ensemble de n matrices carrées A_i d'ordre r, régulières, à termes dans K et vérifiant les relations de compatibilité matricielles

$$(\text{C. M.}) \qquad \sigma(A_i) = A_k \times A_j^{-1} \times a_{\sigma,i}, \qquad \text{si} \begin{cases} \sigma(\theta) = \theta_j, \\ \sigma(\theta_i) = \theta_k, \end{cases}$$

où $a_{\sigma,i}$ est un scalaire quelconque de K.

Je considère l'anneau complet (Ens. V) des matrices carrées d'ordre r à termes dans k et je vais montrer que :

L'ensemble (Ens. P) *des éléments de* (Ens. V) *qui vérifient le système d'équations en* P

$$(\text{M}, 1) \qquad P^{(i)} \times A_i = A_i \times P, \qquad (i = 1, 2, \ldots, n),$$

est une algèbre de Brauer sur p, *dont* k *est un corps de décomposition.*

L'algèbre (Ens. P) est **l'algèbre définie par le système de matrices** A_i.

Comme au paragraphe III du Chapitre II, je forme, à partir d'un élément arbitraire V de (Ens. V), la somme

$$P = \sum_i A_i^{-1} \times V^{(i)} \times A_i \qquad (i \text{ de } 1 \text{ à } n).$$

C'est, *a priori*, une matrice d'ordre r à termes dans K. Je cherche l'effet produit sur cette matrice par une substitution σ du groupe de Galois G de K par rapport à p; j'obtiens

$$\sigma(P) = \sum_i [\sigma(A_i)^{-1} \times V^{(k)} \times \sigma(A_i)],$$

ou, en tenant compte des relations de compatibilité (C. M.),

$$\sigma(P) = \sum_k [a_{\sigma,i}^{-1} \times A_j \times A_k^{-1} \times V^{(k)} \times A_k \times A_j^{-1} \times a_{\sigma,i}] = A_j \times P \times A_j^{-1}.$$

Le conjugué $\sigma(P)$ ne dépend que de l'effet $\theta_j = \sigma(\theta)$ de σ sur θ; d'après les critères de Galois, P est une matrice à termes dans k. De plus, elle vérifie les relations

$$P^{(j)} = A_j \times P \times A_j^{-1} \qquad (j = 1, 2, \ldots, n);$$

c'est donc une solution du système (M, 1). Réciproquement, toute solution P du système (M, 1) peut être mise sous la forme d'une telle somme (de plusieurs façons possibles), par exemple

$$P = \sum_i \left[A_i^{-1} \times \left(\frac{P}{n}\right)^{(i)} \times A_i \right].$$

Par ailleurs, les solutions dans k du système (M, 1) forment un anneau [la somme, la différence et le produit de 2 d'entre elles vérifient aussi ce système et ont tous leurs termes dans k]. Cet anneau contient le corps P et il admet une base par rapport à P, puisqu'on peut obtenir ses éléments sous la forme de sommes

$$P = \sum_i [A_i^{-1} \times V^{(i)} \times A_i],$$

où les matrices V appartiennent à un anneau de base finie par rapport à P : *l'anneau* (Ens. P) *est donc une algèbre sur* P.

Je considère alors les n éléments de (Ens. P) suivants :

$$P_1 = \sum_i [A_i^{-1} \times (\theta\ .V)^{(i)} \times A_i] = \sum_i [\theta_i \times A_i^{-1} \times V^{(i)} \times A_i],$$

$$P_2 = \sum_i [A_i^{-1} \times (\theta^2.V)^{(i)} \times A_i] = \sum_i [\theta_i^2 \times A_i^{-1} \times V^{(i)} \times A_i],$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots,$$

$$P_n = \sum_i [A_i^{-1} \times (\theta^n.V)^{(i)} \times A_i] = \sum_i [\theta_i^n \times A_i^{-1} \times V^{(i)} \times A_i],$$

où V est un élément arbitraire de (Ens. V). Puisque θ est un élément primitif de k, le déterminant

$$\Delta = |\theta_i^j| = |(\theta^j)^{(i)}|$$

est différent de o; et les produits $A_i^{-1} \times V^{(i)} \times A_i$ peuvent être tous exprimés en fonctions linéaires à coefficients scalaires (dans K) de $P_1, P_2, \dots, P_n$. Or la relation de compatibilité (C. M.) qui correspond au choix de $i = 1$ et de σ identique à l'opération unité du groupe G montre que A_1 est un scalaire; donc :

$$V = A_1^{-1} \times V^{(1)} \times A_1.$$

Ainsi V s'exprime en fonction linéaire des éléments $P_1, P_2, \dots, P_n$ de (Ens. P). Les coefficients de cette fonction linéaire qui, *a priori*, sont dans K, sont les mineurs de Δ relatifs à la première colonne, et sont des scalaires de k. Le corps k vérifie donc la propriété 1° des corps de décomposition de l'algèbre (Ens. P) (paragraphe I de ce Chapitre).

En outre, les relations (M, 1) prouvent que les seuls scalaires contenus dans (Ens. P) sont ceux de P : le corps k vérifie aussi la propriété 2° des corps de décomposition de l'algèbre (Ens. P), c'est donc un corps de décomposition de cette algèbre. Par suite, *l'algèbre* (Ens. P) *est une algèbre de Brauer* (d'après leur propriété caractéristique).

Inversement :

Une algèbre de Brauer (O) *sur* P *est isomorphe à* (au moins) *une algèbre définie par un système compatible de matrices.*

Je choisis un corps de décomposition k de cette algèbre (O), corps qui soit une extension finie et séparable de P. Je forme l'anneau de matrices (Ens. P) correspondant à ce corps de décomposition; les éléments de (Ens. P) sont d'ordre r (r^2 étant le rang de (O) sur P). Je construis la $i^{\text{ème}}$ conjuguée $\mathrm{P}^{(i)}$ de chaque élément P de (Ens. P); l'ensemble (Ens. $\mathrm{P}^{(i)}$) de ces matrices est un anneau isomorphe à (Ens. P), donc aussi à l'algèbre de Brauer (O). En vertu d'un théorème d'E. Nœther [15], l'existence de deux anneaux de matrices (Ens. P) et (Ens. $\mathrm{P}^{(i)}$), isomorphes tous deux à (O), entraîne l'existence d'une matrice régulière A_i, d'ordre r, à termes dans K, réalisant cette isomorphie par la transmutation

$$\mathrm{P}^{(i)} = \mathrm{A}_i \times \mathrm{P} \times \mathrm{A}_i^{-1}.$$

J'ai ainsi formé n matrices régulières $\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n$: elles constituent un système compatible. En effet, je puis calculer $\sigma(\mathrm{A}_i)$ en effectuant l'opération σ sur la relation

$$\mathrm{P}^{(i)} = \mathrm{A}_i \times \mathrm{P} \times \mathrm{A}_i^{-1};$$

j'obtiens

$$\sigma(\mathrm{P}^{(i)}) = \mathrm{P}^{(k)} = \sigma(\mathrm{A}_i) \times \mathrm{P}^{(j)} \times \sigma(\mathrm{A}_i)^{-1},$$

ou encore, en tenant compte des relations vérifiées par $\mathrm{P}^{(k)}$ et $\mathrm{P}^{(j)}$

$$\mathrm{A}_k \times \mathrm{P} \times \mathrm{A}_k^{-1} = \sigma(\mathrm{A}_i) \times \mathrm{A}_j \times \mathrm{P} \times \mathrm{A}_j^{-1} \times [\sigma(\mathrm{A}_i)]^{-1},$$
$$\mathrm{P} \times \mathrm{A}_k^{-1} \times \sigma(\mathrm{A}_i) \times \mathrm{A}_j = \mathrm{A}_k^{-1} \times \sigma(\mathrm{A}_i) \times \mathrm{A}_j \times \mathrm{P}.$$

La dernière relation montre que la matrice $[\mathrm{A}_k^{-1} \times \sigma(\mathrm{A}_i) \times \mathrm{A}_j]$ est permutable avec chaque élément de (Ens. P); comme elle est permutable avec tout scalaire, elle est aussi permutable avec tous les éléments du produit direct de k et de (Ens. P), considérés comme algèbres sur P. Ce produit direct est, par hypothèse, l'anneau complet des matrices d'ordre r sur k; cela exige que cette matrice soit un scalaire $a_{\sigma,i}$ (de K), de sorte que

$$\sigma(\mathrm{A}_i) = \mathrm{A}_k \times \mathrm{A}_j^{-1} \times a_{\sigma,i}.$$

L'ensemble des matrices A_i est bien un système compatible. Il détermine sur P une algèbre (O') qui admet k comme corps de décomposition; je vais montrer que cette algèbre est identique à (Ens. P).

Il est d'abord clair que (O') contient tous les éléments de (Ens. P), puisqu'un tel élément vérifie, par construction des A_i, les relations

$$\mathrm{P}^{(i)} \times \mathrm{A}_i = \mathrm{A}_i \times \mathrm{P} \qquad (i = 1, 2, \ldots, n),$$

qui définissent (O'). D'autre part, k est, par hypothèse, corps de décomposition de (O), donc aussi de (Ens. P); k est également corps de décomposition de (O'), d'après les propriétés de cette algèbre. Les produits directs de k, soit

[15] C'est le théorème 3 de la page 42 des *Algebren*.

avec (O'), soit avec (Ens. P), sont donc tous deux identiques à l'anneau complet des matrices d'ordre r sur k et par suite confondus. L'algèbre ne peut, par suite, contenir d'éléments extérieurs à (Ens. P), car dans le cas contraire le produit direct de k et de (O') contiendrait des éléments extérieurs au produit direct de k et de (Ens. P). Ce qui montre bien que (O') contient tous les éléments de (Ens. P) et ceux-là seuls.

Ainsi l'algèbre (O) est isomorphe à l'algèbre (Ens. P) définie par le système compatible de matrices A_i.

III. — Algèbre associée à une variété de Brauer.

Au paragraphe III du Chapitre II, j'ai associé, à chaque variété de Brauer (F) sur P, un système de matrices dont j'ai montré qu'il est compatible. D'après les résultats du précédent paragraphe, ce système définit une algèbre de Brauer sur P, que j'appelle **algèbre de Brauer associée dans P à la variété** (F). J'établis quelques propriétés essentielles de cette algèbre qui montrent l'utilité de cette notion pour les problèmes d'équivalence.

Les solutions homographiques d'un système étendu d'équivalence entre (F) *et elle-même peuvent être représentées par tous les éléments de l'algèbre* (Ens. P.) *associée dans* P *à* (F).

Je considère une telle solution $(\mathfrak{T})$ et je choisis une des matrices V, à termes dans k, qui représentent cette homographie. Les relations du système étendu d'équivalence montrent que $(\mathfrak{T})$ est ausssi représentée par chacune des matrices $A_i \times V^{(i)} \times A_i^{-1}$ et par leur somme

$$P = \sum_i [A_i \times V^{(i)} \times A_i^{-1}] \qquad (i \text{ de } 1 \text{ à } n).$$

Mais d'après les raisonnements du paragraphe précédent, cette somme est un élément de (Ens. P).

Ce résultat contient notamment le suivant :

Le groupe (G. P. $_{\mathrm{P}}$F) *des correspondances de Poincaré sur* (F) *dans* P *est isomorphe au groupe-quotient du groupe formé par les éléments réguliers de* (Ens. P) *par le groupe de scalaires de* P.

Je précise encore une propriété utile pour la suite :

Quand on remplace le corps de base P *par une de ses extensions finies et séparables* P′, *l'algèbre* (Ens. P) *associée à* (F) *dans* P *est remplacée par le produit direct de* (Ens. P) *et de* P′, *considérés comme algèbres sur* P.

Je choisis un système compatible de matrices, associé dans P à (F). Pour obtenir un système de matrices, associé dans P′ à (F), je puis parmi elles prendre celles qui correspondent aux conjugués relatifs θ_i de θ par rapport à P′; ce fait est démontré dans la *Géométrie galoisienne*. Ces matrices définissent donc une algèbre (O') formée par les solutions d'un système dont toutes les relations sont vérifiées par les éléments de (Ens. P) : de sorte que (O') contient les éléments de (Ens. P). Comme (O') est une algèbre sur P′, elle contient aussi tous les scalaires du corps de base P′, et le produit direct de (Ens. P) et de P′, considérés comme algèbres sur P. Ce produit direct est une algèbre de rang $[(r+1)^2.\ n']$ sur P (r désignant toujours la dimension de (F) et n' le degré de P′ par rapport à P) c'est donc une algèbre de rang $(r+1)^2$ sur P′. Comme (O') est aussi une algèbre de rang $(r+1)^2$ sur P′, elle ne peut contenir d'autres éléments que ceux de ce produit direct avec lequel elle est confondue.

Enfin, je démontre la propriété fondamentale :

Pour que deux variétés de Brauer sur P *soient équivalentes, au sens de Poincaré, dans* P, *il faut et il suffit que les algèbres associées à ces variétés dans* P *soient isomorphes entre elles.*

Je considère deux variétés de Brauer (F) et (F′) sur P et deux systèmes compatibles de matrices A_i et A'_i respectivement associées dans P à ces variétés. Si (F) et (F′) sont équivalentes dans P, elles ont même dimension r et les systèmes A_i et A'_i sont formés par des matrices de même ordre $r+1$. De plus, d'après les résultats du Chapitre II, paragraphe III, il existe une matrice régulière L_0, d'ordre $r+1$, à termes dans K, qui vérifie les relations

$$L_0^{(i)} \times A_i = A'_i \times L_0 \times \lambda_i \qquad (i = 1, 2, \ldots, n),$$

où $\lambda_1, \lambda_2, \ldots, \lambda_n$ sont des scalaires de K.

La transmutation définie par les formules

$$P' = L_0 \times P \times L_0^{-1} \qquad \text{ou} \qquad P = L_0^{-1} \times P' \times L_0,$$

transforme alors l'algèbre associée à (F) en l'algèbre associée à (F′) dans P. En effet, l'algèbre associée à (F) est l'ensemble des solutions du système

$$P^{(i)} \times A_i = A_i \times P \qquad (i = 1, 2, \ldots, n);$$

la transmutation précédente transforme cet ensemble en l'ensemble des solutions du système

$$(L_0^{(i)})^{-1} \times P'^{(i)} \times L_0^{(i)} \times A_i = A_i \times L_0^{-1} \times P' \times L_0,$$

qui est équivalent à

$$P'^{(i)} \times L_0^{(i)} \times A_i \times L_0^{-1} = L_0^{(i)} \times A_i \times L_0^{-1} \times P',$$

ou, en tenant compte des relations vérifiées par L_0, à

$$P'^{(i)} \times A'_i \times \lambda_i = \lambda_i \times A'_i \times P',$$

ou, puisqu'un scalaire est permutable avec toute matrice, au système

$$P'^{(i)} \times A'_i = A'_i \times P \qquad (i = 1, 2, \ldots, n),$$

dont les solutions forment bien l'algèbre associée à (F′) dans P.

Réciproquement, si les algèbres associées à (F) et à (F′) dans P sont isomorphes, les systèmes A_i et A'_i sont formés par des matrices de même ordre, soit $r+1$; de plus, d'après le théorème rappelé d'E. Nœther [16], il existe une matrice L qui réalise cette isomorphie par la transmutation

$$P = L_0^{-1} \times P' \times L_0.$$

Ce qui veut dire que les deux systèmes

$$P'^{(i)} \times A'_i = A'_i \times P,$$

$$(L_0^{(i)})^{-1} \times P'^{(i)} \times L_0^{(i)} \times A_i = A_i \times L_0^{-1} \times P' \times L_0$$

ont mêmes solutions, celles-ci formant l'algèbre de Brauer (Ens. P′), associée dans P à (F′). J'en déduis que tout élément de (Ens. P′) vérifie encore les relations

$$A'_i \times P' \times A'^{-1}_i \times L_0^{(i)} \times A_i \times L_0^{-1} = L_0^{(i)} \times A_i \times L_0^{-1} \times P'$$

ou

$$P' \times A'^{-1}_i \times L_0^{(i)} \times A_i \times L_0^{-1} = A'^{-1}_i \times L_0^{(i)} \times A_i \times L_0^{-1} \times P'.$$

Donc la matrice $A'^{-1}_i \times L_0^{(i)} \times A_i \times L_0^{-1}$ est permutable avec chaque élément de (Ens. P′); comme elle est permutable avec tout scalaire, elle est aussi permutable avec tout élément du produit direct de (Ens. P′) et de k, considérés comme algèbres sur P. Puisque (Ens. P′) est une algèbre de Brauer et admet k comme corps de décomposition, ce produit direct est un anneau complet de matrices sur k; ce qui exige que la matrice précédente soit un scalaire λ_i (de K) :

$$A'^{-1}_i \times L_0^{(i)} \times A_i \times L_0^{-1} = \lambda_i \qquad \text{ou} \qquad L_0^{(i)} \times A_i = A'_i \times L_0 \times \lambda_i.$$

D'après les résultats du Chapitre II, paragraphe III, l'existence d'une matrice L_0 régulière vérifiant ces relations entraîne l'équivalence de (F) et (F′) dans P.

CHAPITRE IV.

THÉORIE GÉNÉRALE DES VARIÉTÉS DE BRAUER.

Je traduis maintenant des résultats connus de la théorie des algèbres en langage de la théorie des variétés de Brauer. Je commence par des propriétés générales valables, quel que soit le corps de base P. Ces propriétés comprennent notamment des généralisations des deux théorèmes de Nœther-Poincaré.

---

(16) *Voir* la Note (15) du Chapitre III, paragraphe II.

I. — Premier théorème et corps de représentation.

Je vais établir une généralisation du premier théorème de Nœther-Poincaré, ainsi que des généralisations des propriétés des corps de représentation (exposées au paragraphe V du Chapitre I).

Si une variété de Brauer (F) *admet une représentation de Poincaré dans le corps de base* P, *les points simples sur* (F) *qui sont dans* P *sont ceux dont le paramètre* (dans cette représentation) *est dans* P; *réciproquement s'il existe au moins un point simple sur* (F) *dans* P, *cette variété admet* (au moins) *une représentation de Poincaré dans* P.

La propriété directe est immédiate, puisqu'une représentation de Poincaré de (F) dans P définit une correspondance du même nom entre l'espace des paramètres et la variété (F). Pour démontrer la réciproque, j'utilise un théorème fondamental de Wedderburn ([17]).

Toute algèbre de Brauer (O) *sur* P *est isomorphe à un anneau complet de matrices sur un corps gauche.*

Ce corps gauche est lui-même une algèbre de Brauer sur P qui admet les mêmes corps de décomposition que (O); il est isomorphe à un ensemble de matrices (à coefficients dans un de ces corps de décomposition k) dont l'ordre est appelé l'index de l'algèbre (O).

Je considère une variété de Brauer (F) de dimension r, un système étendu d'équivalence $(E', 2)$ entre (F) et elle-même dans P et l'algèbre (O) définie par ce système. D'après les résultats du Chapitre II, paragraphe II, les points simples sur (F) dans P peuvent être déterminés par les solutions homographiques et dégénérées (si elles existent) du système $(E', 2)$ qui transforment l'espace (E_r) en un point. Comme je l'ai établi au paragraphe III du Chapitre II, ces solutions sont représentées par les éléments de rang 1 de (O). Pour chercher s'il existe des points simples sur (F) qui sont dans P, je puis donc chercher s'il existe des éléments de rang 1 dans (O).

J'applique le théorème de Wedderburn à l'algèbre (O); je désigne par (O_0) le corps gauche ainsi obtenu et je représente ses éléments par des matrices à coefficients dans un corps de décomposition k de (O). Puisque (O_0) ne contient pas de diviseurs de zéro, chacune de ces matrices est régulière; son rang est égal à son ordre qui n'est autre que l'index t de (O). L'algèbre (O) est ainsi isomorphe à un anneau (Ens. P) de matrices composées : matrices d'ordre u à termes matriciels d'ordre t, donc encore matrices d'ordre $u.t$, à termes scalaires

---

([17]) Ce théorème est énoncé et démontré à la page 18 (théorème 3) des *Algebren*.

de k. Comme les éléments de (O) sont des matrices d'ordre $r+1$ sur k, il en résulte que

$$r+1=u.t;$$

l'index t est un diviseur de $r+1$. De plus le rang de tout élément de (Ens. P), considéré comme matrice sur k, est au moins égal à t, puisque cet élément contient des mineurs (les éléments du corps gauche) réguliers et d'ordre t. En particulier (O) ne peut contenir d'éléments de rang 1 que si $t=1$, donc si (O) est isomorphe à l'anneau complet des matrices d'ordre $r+1$ sur P.

Enfin l'algèbre associée dans P à l'espace de référence de dimension r est isomorphe à l'anneau complet des matrices d'ordre $r+1$ sur P. Pour le constater, il suffit de former le système étendu d'équivalence dans P entre l'espace (E_r) et lui-même déduit des éléments de comparaison : espace (E_r), correspondance identique sur (E_r), corps P. Le système de matrices correspondant contient une seule matrice identique à la matrice unité; l'algèbre associée est l'ensemble des solutions de la seule relation identiquement vérifiée $P^{(1)}=P$. Cette algèbre est bien l'anneau complet des matrices d'ordre $r+1$ sur P. D'après les résultats du paragraphe précédent, il est nécessaire, pour qu'il existe des points simples de P sur (F), que (F) soit équivalente à l'espace (E_r). Cette condition entraîne immédiatement celle de l'énoncé, puisqu'une représentation de Poincaré de (F) définit une correspondance du même nom entre (E_r) et (F) et inversement.

J'applique ce résultat à la recherche des **corps de représentation de** (F); comme au paragraphe V du Chapitre I, j'appelle ainsi toute extension (finie et séparable) P′ de P dans laquelle existent des points simples sur (F), ou, d'après le résultat précédent, une représentation de Poincaré de (F).

Pour qu'une extension (finie et séparable) P′ *de* P *soit corps de représentation de* (F), *il faut et il suffit que* P′ *soit corps de décomposition de l'algèbre* (O) *associée à* (F) *dans* P.

Je viens de montrer que, pour que P′ soit corps de représentation de (F), il faut et il suffit que l'algèbre associée à (F) dans P′ soit isomorphe à un anneau complet de matrices sur P′. Mais j'ai aussi montré, au paragraphe III du Chapitre III, que l'algèbre associée à (F) dans P′ est isomorphe au produit direct de l'algèbre associée à (F) dans P et du corps P′, considérés comme algèbres sur P. Le théorème résulte immédiatement de ces deux propriétés et de la définition des corps de décomposition.

L'index t de l'algèbre de Brauer associée dans P *à* (F) *divise le degré par rapport à* P, *de tout corps de représentation de* (F). *Il existe des corps de représentation de* (F) *dont le degré relatif par rapport à* P *est égal à t*. Pour exprimer ces propriétés, j'appelle encore t **l'index de la variété de Brauer** (F) **dans** P.

Ceci résulte de ce qui précède et des propriétés suivantes des corps de décomposition : l'index t d'une algèbre de Brauer (O) sur P divise le degré relatif par rapport à P de tout corps de décomposition de (O) ; il existe effectivement du corps de décomposition de (O) de degré t par rapport à P [18].

J'ai montré, au cours d'une démonstration précédente de ce paragraphe, que l'index t d'une algèbre de Brauer divise aussi l'ordre des matrices qui forment cette algèbre. Donc le dernier théorème a pour conséquence :

Si une variété de Brauer (F) *sur* P *est de dimension* r, *il existe des corps de représentation de* (F) *dont le degré, par rapport à* P, *divise* $r+1$. Ceci généralise le résultat du paragraphe V du Chapitre I montrant l'existence d'un corps quadratique de représentation pour toute courbe unicursale et rationnelle (dont la dimension est 1).

S'il existe des corps de représentation de (F) *dont le degré relatif par rapport à* P, *est premier avec* $r+1$ [où r est la dimension de (F)], P *est lui-même corps de représentation de* (F).

En effet, l'index t de (F) divise $r+1$; ainsi que le degré de tout corps de représentation de (F). Si ces deux nombres sont premiers entre eux, t est nécessairement égal à 1, c'est-à-dire que P est corps de représentation (F).

Ce théorème comporte comme cas particulier une propriété bien connue :

Il existe des points rationnels simples sur toute courbe unicursale et rationnelle de degré impair.

En effet, pour une courbe, $r+1$ est égal à 2. D'autre part, en coupant une courbe de degré impair par une droite rationnelle, j'obtiens plusieurs points à coordonnées algébriques, dont l'un au moins engendre un corps de degré impair.

II. — Sous-variétés normales et condition de similitude.

Dans ce paragraphe, j'établis quelques propriétés des sous-variétés normales d'une variété de Brauer et j'indique une condition générale de similitude de ces variétés.

Un raisonnement analogue à celui de l'extension du premier théorème de Nœther-Poincaré montre que :

S'il existe une sous-variété normale de (F) *dans* P *de dimension* r', *l'index* t *de* (F) *dans* P *divise* $r'+1$.

---

(18) La première partie de cette propriété n'est autre que le théorème 17 de la page 47 des *Algebren*; la seconde résulte immédiatement des théorèmes 16 et 18 de la même page.

D'une part, les sous-variétés normales de (F) dans P de dimension r' sont déterminées par les éléments irréguliers de rang $r'+1$ de l'algèbre associée à (F) dans P. J'ai montré, au paragraphe II du Chapitre II, que les sous-variétés normales de (F) dans P peuvent être déterminées par les solutions homographiques et dégénérées d'un système étendu d'équivalence entre (F) et elle-même dans P. Ces éléments sont représentés par les éléments irréguliers de l'algèbre (O). En outre une sous-variété normale de dimension r' est représentée par un élément de rang $r'+1$, puisque l'homographie correspondante transforme (E_r) en un espace de dimension r'.

D'autre part, j'ai montré, au paragraphe précédent, que le rang d'un élément irrégulier de (O) est au moins égal à l'index t de (O); de façon plus précise, ce rang est un multiple de t. En effet, chaque élément de (O) est identique à une matrice composée : matrice d'ordre u à termes dans le corps gauche (O_0), c'est-à-dire termes matriciels d'ordre t. Le rang de cette matrice composée est égal au produit de t et du rang de la matrice à termes dans (O_0). Le théorème énoncé résulte immédiatement de la comparaison de ces deux faits.

Il existe des sous-variétés normales de (F) *dans* P *de dimension* $t-1$, *nombre qui est donc le minimum de la dimension des sous-variétés canoniques de* (F).

Car il existe des éléments de rang t dans (O), par exemple la matrice composée dont un terme est identique à l'unité de (O_0) et dont tous les autres termes sont identiques à l'élément nul de (O_0).

Une sous-variété normale de (F) *dans* P *est associée à une algèbre semblable dans* P *à l'algèbre* (O) *associée dans* P *à* (F).

Deux algèbres sur P sont *semblables*, si elles sont isomorphes à des anneaux complets de matrices sur le même corps gauche (O_0)[19].

Je reprends la construction faite au paragraphe II du Chapitre II d'un système étendu d'équivalence entre une sous-variété canonique (G) de (F) et elle-même : je puis choisir la correspondance de comparaison pour la variété (F) en sorte que la sous-variété (G) soit déterminée par une homographie qui transforme (E_r) en un espace de référence (E_q); les solutions d'un système étendu d'équivalence entre (G) et elle-même peuvent être obtenues en prenant la trace sur (E_q) des solutions du système étendu d'équivalence entre (F) et elle-même. Donc les éléments de l'algèbre $(\mathfrak{J})$ associée dans P à (F′) sont les mineurs, formés par les $q+1$ premières lignes et colonnes, des éléments de l'algèbre (O) associée dans P à (F). Ces mineurs forment un anneau complet de matrices

(19) C'est la définition de la page 45 des *Algebren*.

sur (O_0), de même que ces matrices elles-mêmes. En particulier, les sous-variétés normales de (F) de dimension minima $t-1$ sont associées dans P au corps gauche (O_0).

Je suis maintenant en mesure d'établir un critère de similitude entre variétés de Brauer :

Pour que deux variétés de Brauer soient semblables entre elles dans P, *il faut et il suffit que les algèbres qui leur sont respectivement associées dans* P *soient semblables entre elles.*

En effet, si deux variétés (F) et (F′) de P sont semblables entre elles, il existe une sous-variété normale de (F) équivalente dans P à une sous-variété normale de (F′). Les algèbres respectivement associées à ces sous-variétés sont isomorphes entre elles; comme elles sont semblables respectivement aux algèbres associées à (F) et à (F′) dans P, ces dernières sont semblables entre elles.

Inversement, je considère deux variétés de Brauer (F) et (F′) associées dans P à des algèbres (O) et (O') semblables entre elles. Ces algèbres sont donc isomorphes à des anneaux complets de matrices sur un même corps gauche (O_0) et, par suite, ont même index t. Il existe des sous-variétés normales de (F) et de (F′), toutes deux de dimension $t-1$; elles sont toutes deux associées dans P au corps gauche (O_0) et par suite équivalentes entre elles, ce qui démontre la similitude de (F) et (F′).

Il en résulte les propriétés suivantes :

Pour que deux variétés de Brauer de P *soient semblables entre elles dans* P, *il faut et il suffit que tout corps de représentation de l'une soit aussi corps de représentation de l'autre.*

En effet, pour que deux algèbres de Brauer sur P soient semblables entre elles dans P, il faut et il suffit que tout corps de décomposition de l'une soit corps de décomposition de l'autre.

Si deux variétés de Brauer de P *de même dimension r sont semblables entre elles, elles sont équivalentes.*

En effet, les algèbres associées sont isomorphes à des anneaux complets de matrices sur un même corps gauche (O_0); de plus ces anneaux sont formés par des matrices de même ordre, à savoir $\frac{r+1}{t}$, (t désignant l'index commun à ces deux algèbres). Ces anneaux, et, par suite, les algèbres associées elles-mêmes sont donc isomorphes entre eux.

III. — Second théorème.

Pour obtenir une généralisation du second théorème de Nœther-Poincaré, il reste à trouver une variété (C), aussi simple que possible, semblable à une variété de Brauer donnée.

Je montre d'abord que :

Pour qu'une variété de Brauer (F), *associée dans* P *au système de scalaire* $a_{\sigma,i}$ *de* K, *soit semblable dans* P *à un point, il faut et il suffit qu'il existe n scalaires* $\lambda_1, \lambda_2, \ldots, \lambda_n$ *du corps k tels que*

$$\sigma(\lambda_i) = \lambda_k \times \lambda_j^{-1} \times a_{\sigma,i} \qquad (i = 1, 2, \ldots, n; \qquad \sigma \text{ opération de G}).$$

Je suppose (F) semblable à un point et je forme un système de matrices A_i de K, associé dans P à (F). D'après les résultats du paragraphe III, Chapitre II, il existe une matrice régulière P à termes dans k vérifiant le système matriciel d'équivalence

$$\text{(E. M. 2)} \qquad P^{(i)} \times A_i = \lambda_i \times P \qquad (i = 1, 2, \ldots, n),$$

où les λ_i sont des scalaires de K. Je déduis de la relation de rang i de ce système, par application de l'élément σ du groupe de Galois G de k par rapport à P, que

$$P^{(k)} \times \sigma(A_i) = \sigma(\lambda_i) \times P^{(j)},$$

ou, en tenant compte des relations de compatibilité matricielles vérifiées par les A_i,

$$P^{(k)} \times A_k \times A_j^{-1} \times a_{\sigma,i} = \sigma(\lambda_i) \times P^{(j)}.$$

J'applique les relations de rang k et j du système (E. M. 2)

$$\lambda_k \times P \times a_{\sigma,i} = \sigma(\lambda_i) \times \lambda_j \times P,$$

j'obtiens finalement

$$\sigma(\lambda_i) \times \lambda_j = \lambda_k \times a_{\sigma,i}.$$

Réciproquement, je suppose qu'il existe n scalaires $\lambda_1, \lambda_2, \ldots, \lambda_n$ de K vérifiant cette relation. Puisque la matrice A_i n'est définie qu'au produit près par un scalaire de K, je puis la remplacer par $B_i = \lambda_i^{-1} \times A_i$. Or je constate que

$$\sigma(B_i) = \sigma(\lambda_i)^{-1} \times \sigma(A_i) = \lambda_j \times a_{\sigma,i}^{-1} \times \lambda_k^{-1} \times A_k \times A_j^{-1} \times a_{\sigma,i} = B_k \times B_j^{-1}.$$

Ceci montre que (F) peut être aussi associée au système de scalaires tous identiques à l'unité; en vertu du résultat final du paragraphe III, Chapitre III, (F) est semblable à un point dans P.

Je vais construire une variété (C) répondant à la question posée. La condition précédente exprime l'existence, dans k, de solutions $\lambda_1, \ldots, \lambda_n$ pour un système de relations à coefficients dans K, mais non rationnelles (à cause de l'intervention des éléments σ du groupe G). Mais je puis exprimer $\lambda_1, \ldots, \lambda_n$ en fonction d'éléments de P à l'aide d'une base de k par rapport à P et remplacer ainsi le système de relations en $\lambda_1, \ldots, \lambda_n$ par un système de relations rationnelles à coefficients dans P. La condition précédente est donc équivalente à l'existence dans P de solutions pour ce nouveau système, ou encore d'un point de P sur la variété qu'il définit.

De façon précise, dans les relations

$$\sigma(\lambda_i) = \lambda_k \times \lambda_j^{-1} \times a_{\sigma,i},$$

je remplace les λ_i par

$$\begin{aligned}
\lambda_1 &= \Theta \frac{x_1}{x_0} + \Theta^2 \frac{x_2}{x_0} + \ldots + \Theta^{\mathrm{N}} \frac{x_{\mathrm{N}}}{x_0}, \\
\lambda_2 &= \Theta \frac{x_{\mathrm{N}+1}}{x_0} + \Theta^2 \frac{x_{\mathrm{N}+2}}{x_0} + \ldots + \Theta^{\mathrm{N}} \frac{x_{2\mathrm{N}}}{x_0}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\
\lambda_n &= \Theta \frac{x_{(n-1)\mathrm{N}+1}}{x_0} + \Theta^2 \frac{x_{(n-1)\mathrm{N}+2}}{x_0} + \ldots + \Theta^{\mathrm{N}} \frac{x_{n\mathrm{N}}}{x_0},
\end{aligned}$$

et $\sigma(\lambda_1), \sigma(\lambda_2), \ldots, \sigma(\lambda_n)$ par les expressions analogues obtenues en remplaçant Θ par $\sigma(\Theta)$ (Θ désigne comme précédemment un élément primitif du corps K). Je substitue à $\sigma(\Theta)$ son expression en fonction linéaire, à coefficients dans P, de $\Theta, \Theta^2, \ldots, \Theta^{\mathrm{N}}$, puis j'identifie à o les coefficients de $\Theta, \Theta^2, \ldots, \Theta^{\mathrm{N}}$ dans chacune des relations obtenues. Je forme ainsi un système ($\mathfrak{T}$) de relations algébriques homogènes à coefficients dans P entre $x_0, x_1, \ldots, x_{n\mathrm{N}}$ qui définit une variété (C) de P sur l'espace ($\mathrm{E}_{n\mathrm{N}}$). La condition nécessaire et suffisante précédente est équivalente à l'existence dans P d'une solution en $x_0, x_1, \ldots, x_{n\mathrm{N}}$ du système ($\mathfrak{T}$), ou encore à l'existence d'un point de P sur (C).

Cette variété (C) est une variété de Brauer. En effet, je considère le système linéaire en $\frac{x_1}{x_0}, \frac{x_2}{x_0}, \ldots, \frac{x_{n\mathrm{N}}}{x_0}$,

$$\begin{gathered}
\Theta \frac{x_{(i-1)\mathrm{N}+1}}{x_0} + \Theta^2 \frac{x_{(i-1)\mathrm{N}+2}}{x_0} + \ldots + \Theta^{\mathrm{N}} \frac{x_{i\mathrm{N}}}{x_0} = \frac{u_i}{u_0}, \\
\sigma(\Theta) \frac{x_{(i-1)\mathrm{N}+1}}{x_0} + \sigma(\Theta^2) \frac{x_{(i-1)\mathrm{N}+2}}{x_0} + \ldots + \sigma(\Theta^{\mathrm{N}}) \frac{x_{i\mathrm{N}}}{x_0} = \frac{u_k}{u_j} a_{\sigma,i} \\
(i = 1, 2, \ldots, n; \qquad \sigma \text{ élément de G}).
\end{gathered}$$

Ce système peut être décomposé en un ensemble de n systèmes à N inconnues dont chacun a pour déterminant le discriminant de Θ, donc est résoluble. J'exprime ainsi $\frac{x_1}{x_0}, \frac{x_2}{x_0}, \ldots, \frac{x_{n\mathrm{N}}}{x_0}$, en fonctions rationnelles à coefficients dans K de $u_1, u_2, \ldots, u_n$; ces expressions constituent une représentation unicursale propre $(\mathcal{C})$ de (C), puisque $\frac{u_1}{u_0}, \frac{u_2}{u_0}, \ldots, \frac{u_n}{u_0}$ peuvent s'exprimer en fonctions rationnelles à coefficients dans K de $x_0, x_1, \ldots, x_{nN}$. De plus cette représentation est une représentation de Poincaré, car il est facile de constater que ni $(\mathcal{C})$ ni son inverse $(\mathcal{C})^{-1}$ n'ont de points critiques.

Si je remplace le corps de base P par une extension finie et séparable P′, je puis choisir pour corps de comparaison k un corps contenant P′ et la condition

$$\sigma(\lambda_i) \times \lambda_j = \lambda_k \times a_{\sigma,i}$$

reste valable à condition de considérer seulement les éléments σ du groupe de Galois G′ de k par rapport à P′ (et non plus par rapport à P). La condition ainsi obtenue est équivalente à l'existence d'un point de P′ sur (C).

J'en déduis que :

La variété (C) *est semblable dans* P *à* (F).

En effet, la condition nécessaire et suffisante pour qu'une extension P′ de P soit corps de représentation de (F) est qu'il existe des points de P′ sur (C), donc encore que P′ soit corps de représentation de (C). Le dernier résultat du paragraphe précédent montre que cette condition entraîne la similitude de (F) et de (C).

Le second théorème de Nœther-Poincaré peut maintenant être généralisé de la façon suivante :

Une variété de Brauer (F) *de* P *de dimension* r *est semblable dans* P *à une variété* (C) *définie par un système de la forme*

$$\sigma(\lambda_i) \times \lambda_j = \lambda_k \times a_{\sigma,i},$$

dans un corps k *dont le degré divise* $r + 1$.

C'est une conséquence directe d'une propriété des corps de représentation établie au paragraphe I de ce chapitre et des résultats qui viennent d'être établis.

IV. — Cas cyclique.

Je donne quelques précisions sur les variétés de Brauer qui admettent un *corps de représentation relativement cyclique par rapport au corps de base* P. La variété semblable (C), construite au paragraphe précédent, se simplifie dans ce cas, et je l'utiliserai dans les applications du Chapitre V.

Je suppose que le corps k soit une extension normale et cyclique de P; j'en choisis un élément primitif θ; et je désigne par $\theta_1, \theta_2, \ldots, \theta_n$ ses conjugués que je classe dans un ordre tel que l'élément σ_1 du groupe de Galois G qui transforme θ en θ_1 soit un élément primitif de G et que l'élément σ_i de G qui transforme θ en θ_i soit la $i^{\text{ième}}$ puissance de σ_1. En particulier, $\sigma_n = \sigma_1^n$ est l'élément unité de G.

Les relations de compatibilité exigent que

$$\sigma_1(A_1) = A_2 \times A_1^{-1} \times a_{1,\sigma_1},$$

où a_{1,σ_1} est un scalaire de k. Les matrices A_i ne sont définies qu'à la multiplication près par un scalaire de k; je puis donc choisir pour matrice A_2 la matrice $A_2 = \sigma_1(A_1) \times A_1$. De même A_3 doit vérifier la relation

$$\sigma_1(A_2) = A_3 \times A_1^{-1} \times a_{2,\sigma_1},$$

et je puis choisir pour A_3 la matrice

$$A_3 = \sigma_1^2(A_1) \times \sigma_1(A_1) \times A_1 = \sigma_2(A_1) \times \sigma_1(A_1) \times A_1.$$

De façon générale, je puis choisir

$$A_i = \sigma_{i-1}(A_1) \times \sigma_{i-2}(A_1) \times \ldots \times \sigma_1(A_1) \times A_1 \qquad (i = 1, \ldots, n).$$

Mais la matrice A_n, qui représente l'homographie identique, est un scalaire

$$\sigma_{n-1}(A_1) \times \sigma_{n-2}(A_1) \times \ldots \times \sigma_1(A_1) \times A_1 = a.$$

C'est, *a priori*, un élément de k. Mais une permutation circulaire des facteurs ne change pas la valeur de ce produit de sorte que, pour tout i,

$$\begin{aligned}\sigma_i(a) &= \sigma_1^{n+i-1}(A_1) \times \sigma_1^{n+i-2}(A_2) \times \ldots \times \sigma_1^{i+1}(A_1) \times \sigma_1^i(A_1)\\ &= \sigma_{i-1}(A_1) \times \sigma_{i-2}(A_1) \times \ldots \times A_1 \times \sigma_{n-1}(A_1) \times \ldots \times \sigma_i(A_1) = a;\end{aligned}$$

donc d'après le critère de Galois, a est scalaire de P.

D'autre part, si $i + j \leqq n$,

$$\sigma_j(A_i) = \sigma_1^{i+j-1}(A_1) \times \sigma_1^{i+j-2}(A_1) \times \ldots \times \sigma_1^j(A_1) = A_k \times A_j^{-1};$$

le scalaire a_{i,σ_j} est égal à 1. Si $n < i + j \leqq 2n$,

$$\begin{aligned}\sigma_j(A_i) &= \sigma_1^{i+j-1}(A_1) \times \sigma_1^{i+j-2}(A_1) \times \ldots \times \sigma_1^j(A_1)\\ &= \sigma_{i+j-n-1}(A_1) \times \sigma_{i+j-n-2}(A_1) \times \ldots \times A_1 \times \sigma_{n-1}(A_1) \times \ldots \times \sigma_j(A_1) = A_k \times a \times A_j^{-1};\end{aligned}$$

le scalaire a_{i,σ_j} est égal à a. Le système de scalaires associé dans P à (F) est, en tout cas, déterminé par le seul scalaire a de P.

J'en déduis que :

Pour que (F) *soit semblable dans* P *à un point, il faut et il suffit qu'il existe un élément* λ *de* k *dont la norme relative par rapport à* P *soit égale à* a.

La variété (F) *est semblable dans* P *à la variété définie par la relation*

$$N(\lambda) = a,$$

où $N(\lambda)$ *désigne la norme de* λ *par rapport à* P.

En reprenant le même calcul que pour les matrices A_i, je vois que les relations définissant la variété se réduisent à

$$\lambda_i = \sigma_{i-1}(\lambda_1)\sigma_{i-2}(\lambda_1)\ldots\sigma_1(\lambda_1)\lambda_1 \qquad (i = 1, 2, \ldots, n);$$
$$a = \sigma_n(\lambda_1)\sigma_{n-1}(\lambda_1)\ldots\sigma_1(\lambda_1).$$

Les n premières déterminent $\lambda_1, \lambda_2, \ldots, \lambda_n$ en fonction de λ_1; la dernière est équivalente à $N(\lambda) = a$.

Comme au paragraphe précédent, je puis remplacer cette relation non rationnelle en λ, par un système de relations rationnelles à coefficients dans P. J'obtiens une seule relation de degré n, elle définit *une hypersurface de degré n dans l'espace* (E_n), semblable à (F) dans P.

En particulier, si la variété (F) est une courbe, elle admet, comme je l'ai déjà rappelé, un corps de représentation quadratique par rapport à P, donc cyclique par rapport à ce corps. Ce corps peut être engendré par adjonction à P d'un élément θ dont le carré est un nombre b de P.

Dans la relation $N(\lambda) = a$, je remplace λ par l'expression

$$\lambda = \frac{x}{y} + \theta\frac{y}{z};$$

j'obtiens

$$\left(\frac{x}{z} + \theta\frac{y}{z}\right)\left(\frac{x}{z} - \theta\frac{y}{z}\right) = \frac{x^2 - by^2}{z^2} = a,$$

qui définit une conique de Lagrange. Je retrouve ainsi les résultats de la fin du Chapitre I; d'ailleurs les démonstrations du paragraphe actuel sont des généralisations directes de celles du paragraphe VI du Chapitre I.

CHAPITRE V.

CORPS DE BASE PARTICULIERS.

Je vais indiquer comment ces résultats et ces méthodes peuvent être précisés et complétés pour certains corps de base. La théorie des algèbres de Brauer est particulièrement féconde pour les corps de base suivants : *champs de Galois; corps de nombres réels; corps locaux de Hensel; corps de nombres algébriques.*

J'examine chacun de ces cas, je rappelle les propriétés spéciales des algèbres de Brauer dans chacun d'eux et j'indique les conséquences qui en résultent pour les variétés du même nom. Le cas d'un corps de nombres algébriques est particulièrement important : il comporte la solution des problèmes diophantiens sur les variétés de Brauer dans ces corps et généralisent immédiatement les recherches de Lagrange, Gauss, Hilbert et Poincaré concernant les courbes unicursales et rationnelles.

I. — Champ de Galois.

Le cas le plus simple est celui d'un champ de Galois qui donne lieu au théorème suivant :

Toute variété de Brauer sur un champ de Galois est semblable, dans ce champ, à un point.

C'est une conséquence du théorème de Wedderburn [20] : *Tout corps gauche* (O_0) *formé d'un nombre fini d'éléments est un champ de Galois* (commutatif).

Toute algèbre de Brauer (O) sur un champ de Galois P est semblable à son corps de base P. En effet, d'après le théorème général de Wedderburn [21] utilisé au Chapitre IV, paragraphe I, (O) est semblable à un corps gauche (O_0); mais il n'y a qu'un nombre fini d'éléments dans (O), et dans le corps gauche (O_0); ce dernier est donc un champ de Galois (commutatif). Le corps (O_0), qui est à la fois algèbre de Brauer sur P et corps commutatif ne peut être que P lui-même : le produit direct de (O_0) et d'un de ces corps de décomposition doit être isomorphe à un anneau complet de matrices sur ce corps; comme ce produit direct est aussi un corps commutatif, c'est l'anneau des matrices d'ordre 1 et (O_0) est confondu avec P. Ainsi toute algèbre de Brauer sur un champ de Galois est isomorphe à un anneau complet de matrices sur ce corps. Les résultats du Chapitre IV, paragraphe II, démontrent alors le théorème énoncé.

Les problèmes d'équivalence des variétés de Brauer dans un champ de Galois se résolvent très facilement : *il n'y a qu'une classe de similitude sur* P; *toutes les variétés de Brauer de même dimension sont équivalentes entre elles dans* P; *il existe des points sur toute variété de Brauer sur* P.

Le problème diophantien dans P *sur chaque variété de Brauer* (F) *de* P *est résoluble*. Pour obtenir effectivement les points sur (F) qui sont dans P, il suffit de faire un nombre fini d'essais, puisqu'il n'y a qu'un nombre fini de points sur chaque espace de P.

Je note encore un cas particulier des résultats précédents :

Si $f(x, y)$ est un polynome à coefficients rationnels entiers, indécomposable suivant un module premier p, et si $f(x, y) = 0$ représente une courbe unicursale,

---

(20) C'est le théorème 1 de la page 49 des *Algebren*.

(21) *Voir* la note (17) (Chap. IV, § I).

la congruence $f(x, y) \equiv 0$, (mod. p), a des solutions (dans l'ensemble des entiers rationnels, mod. p) [22].

En effet, la congruence

$$f(x, y) \equiv 0 \qquad (\text{mod. } p),$$

définit, dans le corps des restes (mod. p), des entiers rationnels, une courbe unicursale, donc une variété de Brauer sur ce corps.

II. — Corps des nombres réels.

Je fais remarquer que les problèmes diophantiens et d'équivalence ne se posent pas dans un corps algébriquement fermé. Dans un tel corps, il existe des points simples sur toute variété et toute variété de Brauer admet une représentation de Poincaré. Il n'y a donc pas lieu d'étudier le cas du corps formé par tous les nombres complexes : il n'existe, dans ce corps, qu'une seule classe de similitude de variétés de Brauer.

Le corps des nombres réels donne lieu au théorème suivant :

Une variété de Brauer sur le corps des nombres réels est semblable, dans ce corps, soit à un point, soit à la conique définie par l'équation

$$x_0^2 + x_1^2 + x_2^2 = 0.$$

Ceci résulte du théorème : *Un corps gauche, qui est algèbre de Brauer sur le corps des nombres réels, est isomorphe soit à* P *soit à l'algèbre des quaternions sur* P [23].

Il en résulte que toute algèbre de Brauer sur P est semblable soit à P, soit à l'algèbre des quaternions sur P. Il n'y a donc que deux classes de similitude d'algèbres de Brauer sur P, donc aussi de variétés de Brauer. Enfin, comme la conique d'équation

$$x_0^2 + x_1^2 + x_2^2 = 0$$

ne contient aucun point simple réel, elle est nécessairement associée dans P à l'algèbre des quaternions sur P.

Pour reconnaître pratiquement dans quelle classe de similitude se trouve une variété de Brauer donnée (F) de P, on procède de la façon suivante : On choisit pour corps de représentation de (F) le corps Ω des nombres complexes; c'est une extension quadratique, en particulier, normale et cyclique, du corps de

---

(22) Ce théorème particulier a été démontré, par une autre voie, par Siegel et Hasse.

(23) C'est le théorème 2 de la page 50 des *Algebren*.

base P. On peut donc former une variété de Brauer, définie par une relation de la forme

$$N(\lambda) = a,$$

semblable à (F) dans P, suivant la méthode du paragraphe IV du Chapitre IV.

La condition nécessaire et suffisante pour que (F) *soit semblable à un point dans* P *est que le nombre réel a soit positif.*

En effet, la norme d'un nombre de Ω par rapport à P n'est autre que le module de ce nombre complexe et la condition nécessaire et suffisante pour qu'un nombre réel soit le module d'un nombre complexe est qu'il soit positif.

Si a est négatif, (F) est semblable à la conique d'équation

$$x_0^2 + x_1^2 + x_2^2 = 0.$$

III. — Corps local de Hensel.

Pour les variétés de Brauer sur un corps local de Hensel, j'établis d'abord le théorème :

Une variété de Brauer de dimension r sur un corps local de Hensel P *admet, comme corps de représentation, toute extension de degré $r+1$ du corps* P.

C'est une conséquence immédiate du théorème :

Une algèbre de Brauer de rang m^2 sur un corps local P, *admet, comme corps de décomposition, toute extension de degré m du corps* P (²⁴).

Pour reconnaître si une variété de Brauer (F) de P donnée est semblable à un point, je procède de la façon suivante : D'après le théorème précédent, je puis choisir, comme corps de comparaison k d'un système d'équivalence entre (F) et elle-même, toute extension de degré $r+1$ de P [r étant la dimension de (F)]; je choisis une telle extension normale et cyclique particulière. Je désigne par $\mathfrak{p}$ l'idéal premier (unique) de P et par g le nombre d'éléments du corps P/$\mathfrak{p}$ des restes de P (mod. $\mathfrak{p}$). Une racine primitive d'ordre $(g^{r+1}-1)$ de l'unité engendre une extension normale et cyclique de P, que je choisis pour corps k. Je construis une variété de la forme

$$N(\lambda) = a,$$

semblable dans P à (F), suivant la méthode du paragraphe IV du chapitre IV; [$N(\lambda)$ étant la norme, par rapport à P, d'un nombre λ de k].

---

[24] C'est le théorème 4 *bis* de la page 113 des *Algebren.*

La condition nécessaire et suffisante pour que (F) *soit semblable dans* P *à un point est que l'idéal* (a) *engendré dans* P *par l'élément a de* P *soit divisible par* $\mathfrak{p}^{r+1}$.

En effet, la condition de l'énoncé n'est autre que la condition nécessaire et suffisante pour qu'il existe un nombre de k dont la norme, par rapport à P, soit égale à a ([25]).

Cela résout les problèmes diophantiens dans P sur les variétés de Brauer; car on peut ainsi reconnaître si un tel problème, sur une variété donnée (F), est possible et, le cas échéant, former une représentation de Poincaré de (F) dans P. On pourrait encore préciser la répartition des classes de similitude des variétés de Brauer en utilisant les théorèmes qui précisent la répartition des classes de similitude d'algèbres du même nom ([26]). Je me contente de montrer que :

Si une variété de Brauer (F) *sur* P *est indécomposable, dans le corps des restes* P/$\mathfrak{p}$, *elle est semblable, dans* P, *à un point.*

En effet, si a n'est pas divisible par $\mathfrak{p}$, la variété (F) est semblable, dans P, à un point, puisque la condition du théorème précédent est vérifiée dans ce cas. Le corps k, extension finie de P, est aussi un corps local, dont l'idéal premier $\mathfrak{P}$ divise $\mathfrak{p}$. Si a est divisible par $\mathfrak{p}$, donc *a fortiori* par $\mathfrak{P}$, plusieurs des matrices A_i sont diviseurs de zéro dans le corps des restes $k/\mathfrak{P}$ de k, (mod. $\mathfrak{P}$); ces matrices A_i sont irrégulières dans ce corps et définissent des homographies ($\mathcal{A}_i$) dégénérées sur (E_r). D'autre part, je puis choisir un système de formules de transformation de ($\mathcal{F}$) dont un coefficient au moins n'est pas divisible par $\mathfrak{P}$; ce système définit, dans le corps $k/\mathfrak{P}$ une transformation $(\mathcal{F})_{\mathfrak{p}}$ l'espace (E_r) en une variété $(G)_{\mathfrak{p}}$. De même, je puis choisir un système d'équations de (F) dans P dont un coefficient au moins soit entier $\mathfrak{p}$-adique; ce système définit, dans le corps des restes P/$\mathfrak{P}$, une variété $(F)_{\mathfrak{p}}$. Si la variété $(F)_{\mathfrak{p}}$ est indécomposable, elle est confondue avec $(G)_{\mathfrak{p}}$ et admet donc $(\mathcal{F})_{\mathfrak{p}}$ comme représentation de Poincaré; ce qui est incompatible avec le fait qu'une homographie ($\mathcal{A}_i$) est dégénérée.

IV. — Corps de nombres algébriques.

Enfin, j'envisage le cas où le corps de base est un corps de nombres algébriques. J'obtiens le théorème :

Pour qu'une variété de Brauer (F) *sur un corps* P *de nombres algébriques soit semblable dans* P *à un point, il faut et il suffit qu'il en soit ainsi pour toute variété déduite de* (F) *par extension* $\mathfrak{p}$*-adique du corps de base* P.

([25]) C'est le théorème 6 de la page 110 des *Algebren.*

([26]) *Voir* le théorème 3 de la page 112 des *Algebren.*

C'est une conséquence immédiate du théorème fondamental sur les algèbres de Brauer sur un corps P de nombres algébriques ([27]) :

Pour qu'une algèbre de Brauer (O) sur un tel corps P *soit isomorphe à un anneau complet de matrices sur* P, *il faut et il suffit qu'il en soit ainsi pour toute algèbre déduite de* (O) *par extension* $\mathfrak{p}$*-adique de son corps de base* P.

Ce théorème permet de reconnaître si (F) est équivalente à un espace de référence, donc de résoudre le problème diophantien sur (F) dans P, en appliquant *un nombre fini de fois* la méthode du paragraphe précédent. En effet, le dernier résultat du même paragraphe montre que la variété (F) est semblable à un point dans l'extension $\mathfrak{p}$-adique $P_{\mathfrak{p}}$ de P pour tous les idéaux premiers $\mathfrak{p}$ de P qui vérifient la condition : (F) définit une variété de Brauer (donc indécomposable) dans le corps des restes de $P_{\mathfrak{p}}$, mod. $\mathfrak{p}$, corps qui n'est autre d'ailleurs que le corps des restes de P, mod. $\mathfrak{p}$. Il suffit donc d'appliquer la méthode du paragraphe précédent aux seuls idéaux premiers de P qui ne vérifient pas cette condition. Pour chercher ces derniers idéaux, je commence par remplacer (F) par une variété (C) semblable dans P à (F) et définie par des relations de la forme

$$\sigma(\lambda_i)\times\lambda_j=\lambda_k\times a_{\sigma,i},$$

variété que je forme suivant le procédé du paragraphe III, Chapitre IV. Dans ce même paragraphe, j'ai montré que cette variété (C) est une variété de Brauer, donc indécomposable, en construisant une de ses représentations de Poincaré; mais cette construction n'est possible que grâce aux deux propriétés suivantes, vérifiées par le corps K et le système de scalaires $a_{\sigma,i}$:

1° *le discriminant, par rapport à* P, *d'un élément primitif* (Θ) *du corps* K *est différent de zéro;*

2° *aucune des inconnues* λ_i *n'est identiquement nulle*, c'est-à-dire *qu'aucun des scalaires* $a_{\sigma,i}$ *n'est égal à zéro.*

La variété (C) définit donc une variété de Brauer (indécomposable) dans le corps des restes de P, mod. $\mathfrak{p}$, si ces deux propriétés sont encore vérifiées lorsqu'on remplace P par son corps des restes, mod. $\mathfrak{p}$, et K par l'extension de ce corps des restes engendrée par Θ. La seconde condition est équivalente à $N(a_{\sigma,i})\neq 0$ [où $N(a_{\sigma,i})$ désigne la norme par rapport à P de $a_{\sigma,i}$]; ce qui remplace une condition sur des nombres de K par une condition sur des nombres de P. La variété (C) définit donc certainement une variété de Brauer (indécomposable) dans le corps des restes de P, mod. $\mathfrak{p}$, pour tous les idéaux premiers $\mathfrak{p}$ de P qui ne divisent ni le discriminant de Θ par rapport à P, ni aucun des nombres $N(a_{\sigma,i})$; pour ces idéaux, (C) définit une variété semblable à un point dans l'extension $\mathfrak{p}$-adique de P. Il n'y a qu'un nombre fini d'idéaux

([27]) C'est le théorème 1 de la page 117 des *Algebren*.

premiers de P qui divisent un des nombres précédents; c'est à ces seuls idéaux qu'il suffit d'appliquer la méthode du paragraphe précédent pour reconnaître si (C), donc aussi (F), est semblable dans P à un point.

Le théorème précédent a pour conséquence :

Pour qu'une extension (finie et séparable) P′ *de* P *soit corps de représentation de* (F), *il faut et il suffit que toute extension locale de* P′ *soit corps de représentation de* (F).

Les remarques faites montrent d'ailleurs qu'il ne peut y avoir qu'un nombre fini d'extensions locales de P qui ne soient pas corps de représentation de (F).

Enfin le théorème fondamental est généralisé par la propriété :

Pour que deux variétés de Brauer (F) *et* (F′) de P *soient semblables entre elles dans* P, *il faut et il suffit que* (F) et (F′) *soient semblables dans toute extension locale de* P.

Ce qui résulte immédiatement du théorème précédent et de la condition de similitude indiquée au paragraphe II du Chapitre IV : pour que (F) et (F′) soient semblables entre elles dans P, il faut et il suffit qu'elles aient les mêmes corps de représentation.

Je signale que, pour reconnaître si (F) et (F′) sont semblables entre elles dans P, il suffit de reconnaître si elles le sont dans *un nombre fini d'extensions* locales de P : les extensions qui ne sont pas corps de représentation, soit pour (F), soit pour (F′).

Exemples.

La variété (F), définie dans l'espace (E_3) par l'équation

$$x_1^3+x_2^3+x_3^3+2x_1^2x_3-x_1x_2^2+x_1x_3^2-x_2x_3^2-3x_1x_2x_3=bx_0^3$$

est une variété de Brauer, si b est un nombre non nul.

Si Θ, Θ' et Θ'' sont les racines de l'équation (absolument irréductible)

$$\Theta^3-\Theta-1=0$$

et, si Δ est le discriminant (absolu) de Θ, la variété (F) admet la représentation de Poincaré

$$\begin{aligned}&\frac{y_1^2y_2(\Theta'\Theta''^2-\Theta''\Theta'^2)+y_1y_2^2(\Theta''\Theta^2-\Theta\Theta''^2)+by_0^3(\Theta\Theta'^2-\Theta'\Theta^2)}{x_1}\\ &=\frac{y_1^2y_2(\Theta'^2-\Theta''^2)+y_1y_2^2(\Theta''^2-\Theta^2)+by_0^3(\Theta^2-\Theta'^2)}{x_2}\\ &=\frac{y_1^2y_2(\Theta''-\Theta')+y_1y_2^2(\Theta-\Theta'')+by_0^3(\Theta'-\Theta)}{x_3}=\frac{\Delta y_1y_2y_3}{x_0};\end{aligned}$$

$$\frac{x_1+\Theta x_2+\Theta^2x_3}{y_1}=\frac{x_1+\Theta'x_2+\Theta'^2x_3}{y_2}=\frac{x_0}{y_0}.$$

Si b est un nombre rationnel quelconque, on peut, par un changement de variable simple, se ramener au cas où b est un entier rationnel sans diviseurs cubiques. Dans ce cas, la variété (F) contient des points rationnels si et seulement si la congruence

$$\Theta^3 - \Theta - 1 = 0 \qquad (\text{mod. } b)$$

a des solutions rationnelles.

Par exemple

pour $b = 1$, la variété (F) admet le point rationnel 1, 0, 0;

pour $b = 5$, la congruence

$$\Theta^3 - \Theta - 1 = 0 \qquad (\text{mod. } 5)$$

admet 2 pour solution, la variété (F) admet le point rationnel 1, 2, 0;

pour $b = 7$, la congruence

$$\Theta^3 - \Theta - 1 = 0 \qquad (\text{mod. } 7),$$

admet 5 pour solution, la variété (F) admet le point rationnel 2, 1, 0;

pour $b = 2$, ou 3, ou 13, la congruence

$$\Theta^3 - \Theta - 1 = 0 \qquad (\text{mod. } b)$$

n'a pas de solutions rationnelles et la variété (F) n'admet pas de points rationnels.

D'autre part, la variété (F) est semblable à un point dans tout corps de congruences, mod. p, pour lequel p ne divise pas b. La variété (F) est semblable à un point dans le corps p-adique, si p ne divise pas b ou si la congruence

$$\Theta^3 - \Theta - 1 = 0 \qquad (\text{mod. } p^e)$$

a des solutions rationnelles, p^e étant la plus grande puissance de p contenue dans b.

Les calculs concernant ces exemples et d'autres encore seront développés dans un Mémoire ultérieur.

CONCLUSION.

Ainsi que je l'avais annoncé, j'ai résolu les problèmes diophantiens sur les variétés de Brauer, généralisant les résultats de Lagrange, Gauss, Hilbert, Poincaré concernant les courbes unicursales. J'ai résolu accessoirement les problèmes d'équivalence et de similitude entre ces variétés. Ceci appelle d'autres études analogues, dont la plus simple semble être celle des variétés unicursales générales. Je n'ai pu encore aborder cette étude; je ne connais à ce sujet que l'étude d'un cas très particulier : celui des hypersurfaces du second degré par Hasse ([28]). Il peut sembler étonnant que cette étude soit plus complexe que celle des variétés de Brauer. Pourtant la difficulté est réelle et même d'ordre algébrique autant qu'arithmétique : alors qu'on sait reconnaître (*Géométrie galoisienne*) si une variété définie par un système d'équations à coefficients dans un corps P est une variété de Brauer de ce corps, on ne sait pas reconnaître si une variété donnée de P est unicursale dans P.

En terminant ce Mémoire, je désire remercier tous ceux dont l'intérêt ou l'amitié a soutenu mes efforts durant son élaboration; ils sont responsables pour beaucoup de son achèvement.

([28]) *Journal de Crelle,* t. 152, 1923, p. 129-148 et 205-224; t. 153, 1923, p. 113-130 et 158-162