ANDRÉ WEIL

L'arithmétique sur les courbes algébriques

Thèses de l'entre-deux-guerres, 1928

<http://www.numdam.org/item?id=THESE_1928__95__1_0>

N° D'ORDRE 2025
SÉRIE A
N° DE SÉRIE 1165

THÈSES

PRESENTÉES

A LA FACULTÉ DES SCIENCES DE PARIS

POUR OBTENIR

LE GRADE DE DOCTEUR ES SCIENCES MATHÉMATIQUES

Par M. André WEIL

1re THÈSE

L'ARITHMÉTIQUE SUR LES COURBES ALGÉBRIQUES

2e THÈSE

PROPOSITIONS DONNÉES PAR LA FACULTÉ

SOUTENUES LE NOVEMBRE 1928 DEVANT LA COMMISSION D'EXAMEN

MM. ÉMILE PICARD — Président
MONTEL, GARNIER — Examinateurs

UPPSALA 1928
ALMQVIST & WIKSELLS BOKTRYCKERI-A.-B.

FACULTÉ DES SCIENCES DE L'UNIVERSITÉ DE PARIS

MM.

Doyen . . . . . C. MAURAIN, *Professeur*, Physique du globe.

Doyens honoraires . . . . . P. APPELL, M MOLLIARD.

Professeurs honoraires . . . . . P. PUISEUX.
V. BOUSSINESQ.
A JOANNIS.
H. LE CHATELIER.
H. LEBESGUE.
A. FERNBACH.
A. LEDUC.

Professeurs . . . . . ÉMILE PICARD . . . . . Analyse supérieure et algèbre supérieure.
G. KŒNIGS . . . . . Mécanique physique et expérimentale.
E. GOURSAT . . . . . Calcul différentiel et calcul intégral.
P. JANET . . . . . Électrotechnique générale.
F. WALLERANT . . . . . Minéralogie.
H. ANDOYER . . . . . Astronomie.
P. PAINLEVÉ . . . . . Mécanique analytique et mécanique céleste.
Gabriel BERTRAND . . . . Chimie biologique.
Mme P. CURIE . . . . . Physique générale et radioactivité.
M. CAULLERY . . . . . Zoologie (Évolution des êtres organisés).
G. URBAIN . . . . . Chimie minerale.
Émile BOREL . . . . . Calcul des probabilités et Physique mathém.
L. MARCHIS . . . . . Aviation.
Jean PERRIN . . . . . Chimie physique.
Rémy PERRIER . . . . . Zoologie (Enseignement P. C. N.).
H ABRAHAM . . . . . Physique.
M. MOLLIARD . . . . . Physiologie végétale.
E. CARTAN . . . . . Géométrie supérieure.
L. LAPICQUE . . . . . Physiologie générale.
E VESSIOT . . . . . Théorie des fonctions et théorie des transformations.
A. COTTON . . . . . Physique générale.
J. DRACH . . . . . Application de l'analyse à la géométrie.
Charles FABRY . . . . . Physique
Charles PÉREZ . . . . . Zoologie.
Léon BERTRAND . . . . . Géologie structurale et géologie appliquée.
R. LESPIEAU . . . . . Théories chimiques.
E. RABAUD . . . . . Biologie expérimentale.
P. PORTIER . . . . . Physiologie comparée.
É. BLAISE . . . . . Chimie organique.
P.-A. DANGEARD . . . . . Botanique
Paul MONTEL . . . . . Mécanique rationnelle.
P. WINTREBERT . . . . . Anatomie et histologie comparées.
O. DUBOSCQ . . . . . Biologie maritime.
G. JULIA . . . . . Mathématiques générales.
A. JOB . . . . . Chimie generale.
A. MAILHE . . . . . Étude des combustibles.
L. LUTAUD . . . . . Géographie physique et géologie dynamique.
Eugène BLOCH . . . . . Physique theorique et physique céleste.
Henri VILLAT . . . . . Mécanique des fluides et applications.
Ch. JACOB . . . . . Géologie
P. PASCAL . . . . . Chimie appliquée.

E. HÉROUARD . . . . . Zoologie.
E. PÉCHARD . . . . . Chimie (Enseig' P. C. N.).
V. AUGER . . . . . Chimie analytique.
M. GUICHARD . . . . . Chimie minérale.
A. GUILLET . . . . . Physique.
G. MAUGUIN . . . . . Minéralogie.
L. BLARINGHEM . . . . Botanique.
A. MICHEL-LÉVY . . . . Pétrographie.
A. DEREIMS . . . . . Géologie.
R. DONGIER . . . . . Physique du globe
A. DENJOY . . . . . Calcul différentiel et intégral.
H. BÉNARD . . . . . Physique (P. C. N.).

E. DARMOIS . . . . . Physique.
G. BRUHAT . . . . . Physique.
H. MOUTON . . . . . Chimie physique.
L. JOLEAUD . . . . . Paléontologie.
M JAVILLIER . . . . . Chimie biologique.
A. DUFOUR . . . . . Physique (P. C. N.).
F. PICARD . . . . . Zoologie (Évolution des êtres organisés).
ROBERT-LÉVY . . . . . Zoologie.
L. DUNOYER . . . . . Optique appliquée.
A. GUILLIERMOND . . . Botanique (P. C. N.).
A. DEBIERNE . . . . . Radioactivité.

Secrétaire . . . . Daniel TOMBECK.

L'ARITHMÉTIQUE SUR LES COURBES ALGÉBRIQUES.

Par

ANDRÉ WEIL

à PARIS.

Introduction.

La géométrie sur une courbe algébrique **a pour objet l'étude des propriétés** des points et systèmes de points[1] sur la courbe qui sont invariantes par **rapport aux** transformations birationnelles. Mais soit C une courbe algébrique **donnée** par une équation $f(x, y) = 0$ *à coefficients rationnels* (dans un certain domaine **de** rationalité k): appelons *points rationnels* les points qui sont à coordonnées **rationnelles** (dans k), et points algébriques ceux qui sont à coordonnées algébriques; appelons *système rationnel* de n points tout système de n points tel **que** les fonctions symétriques des coordonnées de ces points soient rationnelles, **et** système algébrique tout système de points algébriques; l'on peut se **proposer** d'étudier les propriétés des points et systèmes de points rationnels ou **algébriques** sur la courbe C, et particulièrement celles de ces propriétés qui sont **invariantes** par rapport aux transformations birationnelles à coefficients rationnels: **c'est** cette étude qui constitue l'objet de ce que je nomme *l'arithmétique sur* ***la*** *courbe* C. En particulier, la recherche des points rationnels sur une **courbe donnée** C est évidemment un problème invariant par rapport aux transformations **birationnelles** à coefficients rationnels, et rentre, à ce titre, dans l'**arithmétique** sur les courbes algébriques: lorsque le domaine de rationalité se **réduit à** l'ensemble des nombres rationnels, ce problème n'est autre que celui de **la résolution** en nombres rationnels des équations diophantiennes à deux variables, **ou**

[1] Afin de reserver le mot de groupe au sens qu il a pris depuis Galois, je parlerai **toujours de** systemes de points, bien qu on ait l habitude en geometrie algebrique de parler de groupes **de points sur une courbe.**

36 – 2822. *Acta mathematica.* 52. Imprimé le 4 novembre 1928.

encore (ce qui revient au même) de la résolution en nombres entiers des équations diophantiennes *homogènes* à trois variables.

Depuis Diophante, qui leur a laissé son nom, l'on a étudié une foule d'équations particulières de cette sorte, et certaines d'entre elles ont provoqué des efforts considérables: il suffira de citer l'équation $x^n + y^n = 1$, dont l'impossibilité en nombres rationnels pour $n > 2$, affirmée par Fermat dans ses Observations sur Diophante, est restée indémontrée jusqu'à ce jour. Mais ce n'est qu'à une époque toute récente que les progrès de la géométrie sur les courbes algébriques suggérèrent d'aborder par des méthodes analogues l'étude générale des équations diophantiennes à deux variables. Hilbert et Hurwitz[2] remarquèrent les premiers que la recherche des points rationnels sur une courbe algébrique est un problème invariant par les transformations birationnelles à coefficients rationnels: il en résultait que l'élément fondamental de classification des équations diophantiennes à deux variables est le genre de l'équation et non son degré; en utilisant des travaux de Noether, ils montrèrent comment les transformations birationnelles fournissent un procédé simple pour résoudre complètement toutes les équations diophantiennes de genre 0. Poincaré[3], sans connaître, à ce qu'il semble, le travail de Hilbert et Hurwitz, en retrouva les résultats, parmi beaucoup d'autres, dans un mémoire étendu, qui constitue au reste, comme il le dit lui-même, »plutôt un programme d'étude qu'une véritable théorie»; la plus grande partie de ce mémoire est consacrée à l'étude des points rationnels sur les courbes de genre 1, et particulièrement sur les cubiques. Ce qui s'y trouve de plus important, c'est la définition du *rang* d'une courbe de genre 1 à coefficients rationnels: admettons que la courbe contienne un point rationnel au moins, on pourra la ramener, par une transformation birationnelle à coefficients rationnels, à la forme canonique $y^2 = 4x^3 - g_2 x - g_3$; soit alors u l'argument elliptique sur la courbe, de sorte que $x = \wp u$ et $y = \wp' u$: si u et v sont les arguments de deux points rationnels, les formules d'addition des fonctions elliptiques montrent que les points d'arguments $u + v$, $u - v$ sont aussi rationnels (ce qu'on peut voir géométriquement, car les droites qui joignent le point $-u$ aux points $-v$, $+v$, coupent respectivement la courbe aux points $u + v$, $u - v$). En d'autres termes, les arguments des points rationnels forment un module; soit q le plus petit entier (fini ou infini) tel qu'il y ait dans ce module q nombres $u_1, u_2, \ldots, u_q$

[2] *Ueber die diophantischen Gleichungen vom Geschlecht Null*, Acta math. t. 14 1890, p. 217.

[3] *Sur les propriétés arithmétiques des courbes algébriques*, J. de Liouville V), t. 7 1901, p. 161.

formant une base (ce qui veut dire que tout nombre du module sera de la forme $m_1u_1 + m_2u_2 + \cdots + m_qu_q$, les m_i étant entiers): $q + 1$ est appelé par Poincaré le *rang* de la cubique et de la courbe initiale; c'est un invariant par les transformations birationnelles à coefficients rationnels; on peut dire, brièvement, que c'est le nombre minimum de points rationnels sur la courbe à partir desquels tous les autres puissent se déduire par des opérations rationnelles.

Dans le dernier paragraphe de son mémoire, où il aborde les courbes de genre p quelconque, Poincaré montre que, pour généraliser les résultats trouvés pour le genre 1, il faut considérer, non plus les points rationnels sur la courbe, mais les systèmes rationnels de p points: là encore, il définit un invariant de la courbe par les transformations birationnelles à coefficients rationnels, le *rang*, qui est le nombre minimum des systèmes rationnels de p points à partir desquels tous les autres se déduisent par des opérations rationnelles.

Depuis Poincaré, le progrès le plus important a été fait par Mordell[4], qui démontra que le rang des courbes de genre 1 est nécessairement fini lorsque le domaine de rationalité se réduit à l'ensemble des nombres rationnels; son analyse, très ingénieuse, est une application, aux équations de la forme $ay^2 = x^4 - px^3 - qx^2 - rx - s$, de la méthode de descente infinie: cette méthode, appliquée systématiquement pour la première fois par Fermat qui lui donna ce nom, consiste, comme on sait, à donner un procédé par lequel, de toute solution d'une équation à étudier, on peut en déduire une autre, et à montrer que l'itération de ce procédé ne peut être poursuivie indéfiniment; c'est ainsi, par exemple, que Fermat démontra l'impossibilité de $y^2 = x^4 - z^4$ en nombres entiers, en faisant voir que de toute solution l'on peut en déduire une autre en nombres entiers plus petits.

Dans le présent travail, je démontre que le rang d'une courbe C est fini quel que soit son genre p et quel que soit le corps de nombres (algébrique et fini) que l'on choisit comme domaine de rationalité. Cette démonstration est exposée au chapitre II: comme celle de Mordell, elle consiste en une application de la méthode de descente infinie, et se divise par suite en deux parties: dans la première (§§ 11—14), l'étude arithmétique de la courbe C fournit un procédé par lequel, de tout système rationnel de p points sur C, l'on en déduit un autre;

[4] *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. of the Cambridge Philos. Soc., t. 21 (1922), p. 179. — Sur l'ensemble de la question, on consultera T. Nagell, *L'Analyse Indéterminée de degré supérieur* Paris, Gauthiers-Villars, Collection »Mémorial des Sciences Mathématiques», ou se trouve aussi une bibliographie étendue.

de même que le procédé de Mordell reposait sur la bissection des fonctions elliptiques, le mien est tiré de la bissection des fonctions abéliennes; du reste on pourrait utiliser la division par n quelconque avec la même facilité. Dans les §§ 15—19, je montre que l'itération du procédé ainsi trouvé ne peut être poursuivie indéfiniment, ou plutôt qu'elle conduit, à partir d'un certain moment, à des systèmes de p points faisant partie d'un ensemble fini assignable a priori: c'est ce qui résulte de l'étude arithmétique de la variété algébrique à p dimensions dont les éléments sont les systèmes de p points sur C, et qu'on appelle ordinairement la variété jacobienne de C; et l'on verra que la descente infinie fournit, dans ces conditions, le résultat désiré. Dans ce chapitre II se trouvent du reste quelques points qui ne sont peut-être pas sans intérêt pour la théorie des fonctions abéliennes, même indépendamment des conséquences arithmétiques qui en découlent.

Pour pouvoir effectuer la descente infinie dans un cas aussi général, où l'on ne dispose plus de l'appareil si commode des fonctions elliptiques, j'emploie des théorèmes généraux d'arithmétique sur les variétés algébriques, que je nomme théorèmes de décomposition: le chapitre I leur est consacré. Une propriété essentielle des courbes de genre 0 est que toute fonction rationnelle d'un point de la courbe peut être décomposée en facteurs dont chacun est relatif, soit à un seul pôle, soit à un seul zéro de la fonction. Si t est le paramètre sur la courbe, on a en effet:

$$f(M) = k \cdot \frac{(t-\xi)(t-\xi')\cdots(t-\xi^{(l)})}{(t-\eta)(t-\eta')\cdots(t-\eta^{(m)})}$$

ou d'une manière plus symétrique, en posant $t = \frac{x}{y}$ et en rendant homogène:

$$f(M) = \frac{\lambda \prod_{i=1}^{n} (\alpha_i x - \beta_i y)}{\mu \prod_{i=1}^{n} (\gamma_i x - \delta_i y)}.$$

Si de plus les coefficients de f et les coordonnées de M sont des nombres algébriques, on pourra supposer que $\lambda, \mu, \alpha_i, \beta_i, \gamma_i, \delta_i, x, y$ sont des entiers algébriques.

Pour une courbe quelconque, une telle décomposition en facteurs n'est évidemment plus possible. Il est vrai que la considération des idéaux dans le

corps des fonctions rationnelles sur la courbe fournit des décompositions qui, d'un point de vue purement algébrique, sont susceptibles de rendre des services analogues: mais elles ne sont pas arithmétiquement utilisables. Or, si l'on se borne aux courbes et fonctions à coefficients algébriques et aux points à coordonnées algébriques, il existe, sur une courbe de genre quelconque, une décomposition effective des fonctions rationnelles en facteurs dont chacun est relatif à un seul pôle de la fonction s'il se trouve au dénominateur ou à un seul zéro s'il se trouve au numérateur: cette décomposition est donc l'analogue exact de la formule rappelée plus haut; il est vrai que l'on ne peut plus supposer que les facteurs accessoires, qui remplacent les facteurs λ et μ de cette formule, soient constants: mais en tout cas ils sont bornés, c'est-à-dire qu'ils divisent des entiers constants. Ce résultat constitue le théorème de décomposition», et se trouve démontré dans les §§ 1—3. Le reste du chapitre I (§§ 4—10) est consacré à la généralisation de ce théorème aux variétés à plusieurs dimensions sans point singulier: la démonstration donnée pour les courbes s'étend à ce cas avec des modifications convenables. Je ne sais pas si le même théorème reste vrai pour les variétés les plus générales.

Les résultats exposés au chapitre I ont naturellement des rapports étroits avec la théorie des idéaux dans les corps de fonctions algébriques, qui pourrait du reste servir à en démontrer au moins une partie. Mais l'on peut lire le présent travail sans rien connaître de cette théorie, qui d'ailleurs, malgré l'importance des résultats déjà acquis, a sans doute encore bien des progrès à faire: je me suis contenté de renvoyer en note aux principaux mémoires où elle se trouve traitée.[5]

Dans la conclusion (§ 20) je donne au résultat du chapitre II sa forme définitive: on trouve que *tous les systèmes rationnels* de points sur une courbe dérivent d'un nombre fini d'entre eux par addition et soustraction. On constate en même temps qu'à toute courbe est attaché un groupe abélien de base finie, qui ne dépend que du domaine de rationalité, mais qui reste invariant par toutes les transformations birationnelles à coefficients dans ce domaine de rationalité; de là on déduit facilement la définition d'une infinité d'invariants numériques des courbes à coefficients algébriques.

[5] Je dois encore signaler tout particulièrement de remarquables résultats de B. L. van der Waerden, qui paraîtront dans les Math. Ann. sous le titre *Zur Produktzerlegung der Ideale in ganz-abgeschlossenen Ringen*, et qui, entre autres applications importantes, semblent susceptibles d'être employés avec fruit à l'étude des questions abordées dans notre chapitre I.

Enfin, au § 21, je signale quelques-unes des questions les plus difficiles qui se posent à propos des résultats trouvés. Il y en a encore bien d'autres, car l'arithmétique sur les courbes algébriques est un domaine presque inexploré.

J'ai reçu de MM. Garnier. Siegel, van der Waerden, des avis précieux au cours de la rédaction de ce travail: qu'il me soit permis de les remercier ici.

CHAPITRE I.

Le théorème de décomposition.

Par *corps* nous entendrons toujours un corps de nombres algébrique et fini. Si k est un corps, un surcorps de k est un corps contenant k.

Dans ce travail, nous prendrons pour domaine de rationalité un corps k, et le mot »rationnel» devra s'entendre, sauf indication contraire, au sens de *rationnel relativement à* k. K désignera toujours un surcorps arbitraire de k.

1. Un nombre sera dit rationnel relativement à K s'il appartient à K. Un être géométrique est dit *rationnel relativement à* K s'il peut être défini par des équations rationnelles à coefficients rationnels relativement à K, et il est dit simplement *rationnel* s'il est rationnel relativement au domaine de rationalité k. En particulier: une courbe algébrique plane sera rationnelle relativement à K si les coefficients de son équation sont dans K; une fonction des points de la courbe sera rationnelle relativement à K si c'est une fonction rationnelle, à coefficients dans K, des coordonnées d'un point de la courbe. Un point sera rationnel relativement à K si ses coordonnées sont dans K; un système de points le sera si les fonctions symétriques rationnelles, à coefficients dans K, des coordonnées de ses points ont des valeurs rationnelles relativement à K. Un point sera dit algébrique si ses coordonnées sont des nombres algébriques.

Soit S un système de points algébriques; nous appellerons $K(S)$ le plus petit surcorps de K relativement auquel S est rationnel, c'est à-dire le corps obtenu en adjoignant à K les fonctions symétriques rationnelles des coordonnées des points de S. Si S se compose d un seul point M, $K(M)$ sera le corps obtenu en adjoignant à K les coordonnées de M. $K(M_1, M_2, \ldots, M_l)$ désignera le corps obtenu en adjoignant à K les coordonnées des points $M_1, M_2, \ldots, M_k$.

Soit alors C une courbe algébrique rationnelle Considérons une fonction des points algébriques de C, qui à chaque point algébrique M sur C fasse

correspondre un idéal entier du corps $K(M)$, de telle sorte qu'à des points conjugués relativement à K correspondent des idéaux conjugués relativement à K: une telle fonction sera appelée une *distribution sur* C, rationnelle relativement à K. On peut former le produit et le pgcd (plus grand commun diviseur) de deux ou plusieurs distributions.

Deux distributions $\mathfrak{d}, \mathfrak{d}'$ sont dites *équivalentes*, et l'on écrit $\mathfrak{d} \sim \mathfrak{d}'$, s'il y a deux entiers fixes a, a', tels que les idéaux δ, δ' que $\mathfrak{d}, \mathfrak{d}'$ font correspondre à M satisfassent, quel que soit le point algébrique M, aux relations[6]:

$$\delta / a\delta', \quad \delta' / a'\delta .$$

La relation d'équivalence est symétrique et transitive. Si $\mathfrak{d} \sim \mathfrak{d}'$, $\mathfrak{e} \sim \mathfrak{e}'$, les produits $\mathfrak{d} . \mathfrak{e}$ et $\mathfrak{d}' . \mathfrak{e}'$ sont équivalents, les pgcd $(\mathfrak{d}, \mathfrak{e})$ et $(\mathfrak{d}', \mathfrak{e}')$ le sont aussi. Deux distributions $\mathfrak{d}, \mathfrak{d}'$ sont dites premières entre elles si $(\mathfrak{d}, \mathfrak{d}') \sim 1$. Convenons d'appeler *idéal borné* un idéal qui divise un entier fixe: alors deux distributions sont premières entre elles si leur pgcd est un idéal borné.

Une distribution $\mathfrak{d}$ est dite divisible par une autre $\mathfrak{a}$, et l'on écrit $\mathfrak{a} / \mathfrak{d}$, s'il y en a une troisième $\mathfrak{b}$ telle que $\mathfrak{d} \sim \mathfrak{a} . \mathfrak{b}$. Si $\mathfrak{d}$ et $\mathfrak{a}$ font correspondre à un point M les idéaux δ, α, il y aura alors un entier fixe a tel que $\alpha \mid a\delta$; réciproquement, s'il en est ainsi, on aura $\mathfrak{a} \mid \mathfrak{d}$. Si même l'on a trouvé un entier fixe a tel que l'on ait $\alpha \mid a\delta$ partout sauf en un nombre fini de points dont aucun n'est un zéro de $\mathfrak{a}$, l'on aura encore $\mathfrak{a} \mid \mathfrak{d}$, car il suffira de prendre pour a_1 un multiple commun de a et des valeurs de $\mathfrak{a}$ aux points exceptionnels pour que la relation $\alpha' \mid a_1 \delta$ soit vérifiée partout.

Soit $f(M)$ une fonction des points de C, rationnelle relativement à K. Si M est un point algébrique sur C, $f(M)$ sera un nombre du corps $K(M)$, qui pourra être considéré, dans ce corps, comme le quotient de deux idéaux premiers entre eux: $f(M) = \frac{\lambda}{\sigma}$; en un pôle de f, nous prendrons $\lambda = 1$, $\sigma = 0$, et en un zéro de f, $\lambda = 0$ et $\sigma = 1$. A tout point algébrique M correspond ainsi un idéal σ; la distribution qui prend la valeur σ en tout point M sera appelée la *distribution engendrée par* f, et sera notée $[f]$; elle est rationnelle relativement à K.

2. Nous nous bornerons dorénavant à considérer les distributions engendrées par des fonctions sur C, et les distributions déduites de celles-là par les opérations du produit et du pgcd; appelons distributions naturelles celles qu'on

[6] $\lambda \mid \mu$ signifie que l'idéal μ est divisible par λ.

peut obtenir ainsi. Nous allons montrer qu'à tout point algébrique sur C correspond une distribution naturelle indécomposable, c'est-à-dire qui n'est divisible par aucune distribution naturelle non équivalente à elle ou à 1; et toute distribution naturelle est équivalente à un produit bien déterminé de ces distributions indécomposables.

Jusqu'au § 4, nous désignerons par des minuscules latines les fonctions des points de C, rationnelles relativement à un corps K, ou bien la valeur en un point algébrique M d'une de ces fonctions; nous emploierons des minuscules grecques exclusivement pour désigner des idéaux entiers, valeurs en M de distributions sur C, ou bien ces distributions elles-mêmes. Nous écrirons des équations contenant des idéaux, où figurera le signe +: ces équations auront un sens purement symbolique, et signifieront que chaque terme est divisible par le pgcd de tous les autres; de telles équations peuvent être divisées par tout idéal entier qui divise tous les termes. Dans ces équations, un astérisque désignera un facteur idéal indéterminé.

Soient x, y deux fonctions des points de C, rationnelles relativement à K. *Si y n'a d'autres pôles que ceux de x*, avec des multiplicités au plus égales, $[x]$ *est divisible par* $[y]$. On a en effet: $ay^k + xP(x,y) + Q(y) = 0$, $a \neq 0$, P, Q étant de degré $\leq k-1$. Si donc $x = \frac{\lambda}{\sigma}$, $y = \frac{\mu}{\sigma}$, λ, μ, σ étant des idéaux premiers entre eux de $K(M)$, on aura: $a\mu^k + *\lambda + *\sigma = 0$, donc $(\lambda, \sigma)/a$. La distribution σ, qui est multiple de $[y]$, est donc équivalente à $[x] = \frac{\sigma}{(\lambda, \sigma)}$.

Il s'ensuit que *deux fonctions ayant mêmes pôles* (avec les mêmes multiplicités) *engendrent des distributions équivalentes*: car chacune de ces distributions est divisible par l'autre.

Deux fonctions x, y sans pôle commun engendrent des distributions premières entre elles. On a en effet: $ax^k y^l + P(x,y) = 0$, $a \neq 0$, P étant de degré $\leq k+l-1$ en x et y, de degré $\leq k$ en x et $\leq l$ en y. Si $x = \frac{\lambda}{\sigma}$, $y = \frac{\mu}{\tau}$, et $(\lambda, \sigma) = (\mu, \tau) = 1$ on a: $a\lambda^k \mu^l + *(\sigma, \tau) = 0$, d'où $(\sigma, \tau)/a$, sauf en un pôle de x ou de y: mais ces pôles sont en nombre fini, et en un tel pôle, par hypothèse, $(\sigma, \tau) \neq 0$, donc la remarque du § 1 s'applique.

Si f a parmi ses pôles tous les pôles communs de x et de y, $[f]$ est divisible par le pgcd de $[x]$, $[y]$. En effet, ajoutons préalablement à f une constante, de façon que f n'ait pour zéro aucun des pôles de y: cela remplace $[f]$ par une

distribution équivalente. Cela fait, $\frac{x}{f}$ et y sont sans pôle commun. Soient $x=\frac{\lambda}{\sigma}$, $y=\frac{\mu}{\tau}$, $f=\frac{\alpha}{\delta}$, avec $(\lambda,\sigma)=(\mu,\tau)=(\alpha,\delta)=1$. $\left[\frac{x}{f}\right]$ et $[y]$ sont premières entre elles:

$$\left(\frac{\alpha\sigma}{(\alpha\sigma,\lambda\delta)},\tau\right)/a$$

d'où $(\sigma,\tau)/a\,(\alpha\sigma,\lambda\delta)$, et $(\sigma,\tau)/a\delta$.

Si f a pour pôles tous les pôles communs à x et y et ceux-là seulement, $[f]$ divisera $[x]$ et $[y]$ et sera divisible par le pgcd de $[x]$ et $[y]$, on aura donc:

$$[f]\sim([x],[y]).$$

Si les pôles communs à f et g sont les mêmes que les pôles communs à x et y, $[f]$ et $[g]$ seront divisibles par le pgcd de $[x]$ et $[y]$, et de même $[x]$ et $[y]$ seront divisibles par le pgcd de $[f]$ et $[g]$, donc:

$$([f],[g])\sim([x],[y]).$$

3. Par suite, si A est un point algébrique, le pgcd des distributions engendrées par deux fonctions dont A est le seul pôle commun est une distribution parfaitement définie, à une équivalence près, par la donnée de A; nous la noterons $\boldsymbol{d}_A$; si A et B sont distincts, $\boldsymbol{d}_A$ et $\boldsymbol{d}_B$ sont premières entre elles, car si x et y sont deux fonctions sans pôle commun, dont la première admet le pôle A et la seconde le pôle B, $[x]$ et $[y]$ seront premières entre elles, $\boldsymbol{d}_A$ divisera $[x]$, et $\boldsymbol{d}_B$ divisera $[y]$.

Soit alors f une fonction, rationnelle relativement à K, ayant pour pôles distincts les points $A_1, A_2, \ldots, A_m$ avec des multiplicités respectives $r_1, r_2, \ldots, r_m$. Choisissons $2m$ fonctions x_i, y_i de telle sorte que x_i, y_i soient rationnelles relativement à $K(A_i)$, aient A_i pour seul pôle commun, et que deux fonctions d'indices différents soient sans pôle commun. On aura: $\boldsymbol{d}_{A_i}\sim([x_i],[y_i])$. Or f a pour pôles les pôles communs à $\prod_1^m x_i^{r_i}$ et à $\prod_{i=1}^m y_i^{r_i}$; $[f]$ est donc équivalente au pgcd de $\left[\prod_i x_i^{r_i}\right]$ et $\left[\prod_i y_i^{r_i}\right]$, et divise par suite le pgcd de $\prod_i [x_i]^{r_i}$ et $\prod_i [y_i]^{r_i}$; mais pour $i\neq j$ $[x_i]$ et $[y_j]$ sont premières entre elles, on a donc:

$$\left(\prod_i [x_i]^{r_i},\ \prod_i [y_i]^{r_i}\right) \sim \prod_i \boldsymbol{d}_{A_i}^{r_i}.$$

D'autre part f a parmi ses pôles tous les pôles communs à $x_i^{r_i}$ et $y_i^{r_i}$, $[f]$ est donc divisible par $\boldsymbol{d}_{A_i}^{r_i}$ quel que soit i, et par conséquent aussi par $\prod_i \boldsymbol{d}_{A_i}^{r_i}$ puisque $\boldsymbol{d}_{A_i}$ et $\boldsymbol{d}_{A_j}$ sont premières entre elles pour $i \neq j$. Donc enfin:

$$[f] \sim \prod_{i=1}^{m} \boldsymbol{d}_{A_i}^{r_i}.$$

Faisons alors correspondre à tout point algébrique A de C, par une règle univoque mais arbitraire, deux fonctions x_A, y_A rationnelles relativement à $k(A)$ et ayant A pour seul pôle commun; supposons seulement que la règle choisie soit telle qu'à des points A conjugués relativement à k correspondent des fonctions x_A, y_A relativement conjuguées. Prenons pour $\boldsymbol{d}_A$ le pgcd des distributions $[x_A]$ et $[y_A]$; et soit $\omega(A, M)$ l'idéal que $\boldsymbol{d}_A$ fait correspondre au point M.

Soit f une fonction rationnelle relativement à K, de pôles (distincts ou non) $A_1, A_2, \ldots, A_n$, et de zéros $B_1, B_2, \ldots, B_n$. On aura:

$$[f] \sim \boldsymbol{d}_{A_1} . \boldsymbol{d}_{A_2} . \ldots \boldsymbol{d}_{A_n},\quad \left[\begin{matrix} 1 \\ f \end{matrix}\right] \sim \boldsymbol{d}_{B_1} . \boldsymbol{d}_{B_2} . \ldots \boldsymbol{d}_{B_n}.$$

En d'autres termes, nous avons démontré le théorème suivant:

Théorème de décomposition. — C étant une courbe algébrique rationnelle relativement à k, l'on peut faire correspondre à tout couple de points algébriques A, M sur C un idéal $\omega(A, M)$ du corps $k(A, M)$ de telle sorte que l'on ait, si f est une fonction rationnelle, arbitrairement choisie, d'un point de C, si $A_1, A_2, \ldots, A_n$ sont les pôles de f, $B_1, B_2, \ldots, B_n$ ses zéros et M un point algébrique quelconque:

$$f(M) = \frac{\lambda\, \omega(B_1, M) . \omega(B_2, M) . \ldots \omega(B_n, M)}{\mu\, \omega(A_1, M) . \omega(A_2, M) . \ldots \omega(A_n, M)}$$

λ, μ et le pgcd du numérateur et du dénominateur étant des idéaux bornés, c'est-à-dire divisant des entiers indépendants de M.

Il importe de remarquer que si un système de points $A_1, A_2, \ldots, A_n$ est rationnel, la distribution $\boldsymbol{d}_{A_1} . \boldsymbol{d}_{A_2} . \ldots \boldsymbol{d}_{A_n}$ est rationnelle, c'est-à-dire que l'idéal $\omega(A_1, M) . \omega(A_2, M) . \ldots \omega(A_n, M)$ est un idéal du corps $k(M)$: ce produit est en

effet une norme ou un produit de normes relativement à $k(M)$. Pour une raison analogue, si $\mathfrak{d}$ est une distribution rationnelle, faisant correspondre à tout point algébrique M un idéal $\delta(M)$, et si $M_1, M_2, \ldots, M_n$ forment un système rationnel, l'idéal $\delta(M_1).\delta(M_2).\ldots\delta(M_n)$ est un idéal du corps k.[7]

Observons encore, sans démonstration, que l'on peut (après avoir au besoin étendu le domaine de rationalité) admettre que $\omega(A, M)$ dépend symétriquement de A et de M, c'est-à-dire que $\omega(A, M) = \omega(M, A)$.

4. *Multiplicités à plusieurs dimensions.* — Les résultats précédents peuvent être étendus aux fonctions algébriques de plusieurs variables; une étude complète de ce cas serait cependant difficile, et exigerait sans doute une théorie préalable des idéaux dans les corps de fonctions que l'on aurait à considérer.[8] Nous nous occuperons seulement des variétés sans point singulier, en nous attachant aux résultats les plus simples et à ceux dont nous aurons besoin dans le chapitre suivant.

Soit donc V une variété algébrique à n dimensions, plongée dans un espace projectif à l dimensions, dépourvue de point singulier, et rationnelle, c'est-à-dire définie par des équations à coefficients rationnels relativement à k. Pour abréger, nous appellerons *surfaces* les variétés algébriques irréductibles à $n-1$ dimensions, situées sur V, et rationnelles relativement à un surcorps K de k (c'est-à-dire définies par des équations à coefficients dans K). U étant une surface, $k(U)$ désignera le plus petit surcorps de k relativement auquel U est rationnelle.

Nous aurons à considérer des fonctions sur V, rationnelles relativement à un surcorps K de k; une telle fonction est le quotient de deux formes de même degré par rapport aux coordonnées homogènes d'un point de V, les coefficients de ces formes étant dans K. Les infinis d'une fonction rationnelle relativement à K forment un système de surfaces (où chaque surface possède une multiplicité

[7] La définition des distributions rationnelles et la règle faisant correspondre à tout A des fonctions x_A, y_A ont été formulées justement de telle sorte qu'il en soit bien ainsi.

[8] Une telle théorie serait également indispensable pour asseoir sur des bases solides la théorie des fonctions algébriques de plusieurs variables et la géométrie algébrique (cf. pour les courbes algébriques le mémoire bien connu de Dedekind et Weber, *Theorie der algebraischen Funktionen einer Veranderlichen*, J. de Crelle, t. 92 (1882), p. 181). Elle rentre naturellement dans le cadre des travaux généraux de E. Noether (v. p. ex. *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörper*, Math. Ann. t. 96 (1926), p. 26) et de W. Krull (*Theorie der allgemeinen Zahlringe*, Math. Ann. t. 99 (1928), p. 51); elle présente cependant encore des difficultés considérables. Dans cet ordre d'idées, on consultera avec grand profit les travaux de B. L. van der Waerden, particulièrement *Zur Nullstellentheorie der Polynomideale*, Math. Ann. t. 96 (1926), p. 183, ainsi que le mémoire cité note [5].

déterminée), qui sera appelé le système d'infinis de la fonction et sera dit rationnel relativement à K. Soient deux ou plusieurs systèmes de surfaces, rationnels relativement à K: s'il n'y a aucune surface qui figure à la fois dans tous ces systèmes, ils seront dits premiers entre eux; dans le cas contraire, attribuons à chaque surface figurant à la fois dans tous ces systèmes la plus petite des multiplicités qu'elle y possède: on a ainsi un nouveau système, qui sera dit, lui aussi, rationnel relativement à K, et que nous nommerons le pgcd des systèmes initiaux. Soient de même deux ou plusieurs systèmes; et à chaque surface figurant au moins dans l'un d'entre eux attribuons une multiplicité égale à la somme des multiplicités qu'elle possède dans tous ces systèmes: le nouveau système ainsi formé sera appelé le produit des systèmes initiaux. Si un système S est le produit d'un autre T par un troisième, ce dernier est appelé le quotient de S par T et se notera $S:T$; on dira dans ce cas que S est multiple de T et T diviseur de S. Le ppcm (plus petit commun multiple) de plusieurs systèmes est le pgcd de tous les multiples communs de ces systèmes.[9] Soient $x_1, x_2, \ldots, x_m$ des fonctions rationnelles relativement à K, et soit S le ppcm des systèmes d'infinis de ces fonctions: S est multiple du système d'infinis de $\sum_1^m a_i x_i$, quelles que soient les constantes a_i, et est identique à ce système si les a_i sont pris au hasard; on nommera S le système d'infinis de la famille $x_1, x_2, \ldots, x_m$.

5. Comme pour les courbes, une distribution $\mathfrak{d}$ sur V sera une fonction qui, à tout point algébrique M de V, fera correspondre un idéal δ du corps $K(M)$, de sorte qu'à des points conjugués relativement à K correspondent des idéaux conjugués relativement à K. Soit $f(M)$ une fonction rationnelle relativement à K; soit, en tout point algébrique M où f n'est pas indéterminée, $f=\frac{\lambda}{\sigma}$, λ et σ étant des idéaux premiers entre eux de $K(M)$, de sorte que $\lambda=0$, $\sigma=1$ en un zéro de f, et $\lambda=1$, $\sigma=0$ en un infini de f; soit $\lambda=\sigma=0$ aux points d'indétermination de f, qui sont les points communs aux systèmes d'infinis de f et de $\frac{1}{f}$; on dira que σ et λ sont les valeurs respectives, en M, des distributions

[9] Ces dénominations de pgcd, de produit, etc., reçoivent leur sens plein par la considération des idéaux dans le corps des fonctions rationnelles sur V. Nos »surfaces» et nos »systèmes de surfaces» ne sont autres, en effet, que les *Primdivisoren*» et les »*Divisoren*» de B. L. van der Waerden (loc. cit. note [5], § 8, au travail duquel on pourra donc se reporter pour des démonstrations purement algébriques de nos affirmations.

$[f]$ et $\left[\frac{1}{f}\right]$ engendrées par f et $\frac{1}{f}$. Si $x_1, x_2, \ldots, x_m$ sont des fonctions rationnelles relativement à K, le ppcm des distributions qu'elles engendrent est une distribution qui est multiple de $\left[\sum_1^m a_i x_i\right]$ quelles que soient les constantes a_i, et qui sera dite *engendrée par la famille* $x_1, x_2, \ldots, x_m$: on la notera $[x_1, x_2, \ldots, x_m]$. Nous nous bornerons à considérer les distributions «naturelles», c'est-à-dire les distributions engendrées par des fonctions ou des familles de fonctions et les distributions qui se déduisent de celles là par les opérations du produit et du pgcd.

Soient $\mathfrak{d}, \mathfrak{d}'$ deux distributions, faisant correspondre à un point M les idéaux δ, δ'; $\mathfrak{d}$ sera dite divisible par $\mathfrak{d}'$ si l on a $\delta' \alpha \delta$, α étant un entier indépendant de M; si $\delta' \alpha \delta$ en tout M sauf en certains points M exceptionnels, $\mathfrak{d}$ sera dite divisible par $\mathfrak{d}'$ sauf en ces points; si ces points exceptionnels appartiennent tous à un système de surfaces déterminé, $\mathfrak{d}$ sera dite divisible par $\mathfrak{d}'$ presque partout. Deux distributions $\mathfrak{d}, \mathfrak{d}'$ seront dites équivalentes, équivalentes sauf en certains points, équivalentes presque partout, suivant que chacune est divisible par l'autre, divisible par l'autre sauf en certains points, divisible par l'autre presque partout. Deux ou plusieurs distributions seront dites premières entre elles, premières entre elles sauf en certains points, premières entre elles presque partout, suivant que leur pgcd est équivalent à 1, équivalent à 1 sauf en certains points, équivalent à 1 presque partout. Par exemple, si la fonction f est rationnelle relativement à K, $[f]$ et $\left[\frac{1}{f}\right]$ sont premières entre elles presque partout (partout sauf aux points d'indétermination de f).

6. Soient $x_1, x_2, \ldots, x_m$ des fonctions rationnelles relativement à K; soient S_ν et T_ν les systèmes d'infinis respectifs de x_ν et de $\frac{1}{x_\nu}$, et soit S le système d'infinis de la famille $x_1, x_2, \ldots, x_m$. On dira que $x_1, x_2, \ldots, x_m$ forment une *famille régulière* si, à tout point A de V, l'on peut faire correspondre un indice ν tel que A ne soit ni sur $S : S_\nu$ ni sur T_ν. S'il en est ainsi, m combinaisons linéaires indépendantes des x_i, à coefficients constants, forment également une famille régulière.

Soit $x_1, x_2, \ldots, x_m$ une famille régulière. soit S son système d'infinis, et soit y une fonction dont le système d'infinis soit diviseur de S: *dans ces conditions,* $[y]$ *divise* $[x_1, x_2, \ldots, x_m]$. Considérons en effet, dans un espace projectif à $m+1$ dimensions, la variété algébrique irréductible décrite par le point de

coordonnées homogènes $x_1, x_2, \ldots, x_m, y, 1$ quand le point argument décrit V: cette variété ne passe pas par le point $(0, 0, \ldots, 0, 1, 0)$, car en tout point de V on peut déterminer ν de façon que $\frac{y}{x_\nu}$ y reste fini; elle est donc contenue dans une variété à m dimensions qui ne passe pas non plus par le point $(0, 0, \ldots, 0, 1, 0)$; autrement dit, l'on a: $ay^k + \sum_i x_i P_i(x_1, x_2, \ldots, x_m, y) + Q(y) = 0$, $a \neq 0$, les P_i et Q étant de degré $\leq k-1$. Soient, en un point non situé sur S, $x_i = \frac{\lambda_i}{\sigma}$, $y = \frac{\mu}{\sigma}$, et $(\lambda_1, \lambda_2, \ldots, \lambda_m, \mu, \sigma) = 1$; on aura $a\mu^k + \Sigma * \lambda_i + * \sigma = 0$, d'où $(\lambda_1, \lambda_2, \ldots, \lambda_m, \sigma)/a$: σ, multiple de $[y]$, est donc équivalente à $[x_1, x_2, \ldots, x_m]$.

Il s'ensuit que *deux familles régulières, ayant même système d'infinis, engendrent des distributions équivalentes.*

Soient $x_1, x_2, \ldots, x_m$ des fonctions dont les systèmes d'infinis sont sans point commun: *elles engendrent des distributions premières entre elles presque partout,* ou, plus précisément, partout sauf aux points d'indétermination de l'une de ces fonctions. Considérons en effet, dans un espace à m dimensions, la variété algébrique irréductible décrite par le point $\frac{1}{x_1}, \frac{1}{x_2}, \ldots, \frac{1}{x_m}$ quand le point argument décrit V: cette variété ne passe pas par l'origine, elle est donc contenue dans une variété à $m-1$ dimensions qui n'y passe pas non plus; autrement dit, l'on a: $F\left(\frac{1}{x_1}, \frac{1}{x_2}, \ldots, \frac{1}{x_m}\right) = 0$, F ayant un terme constant $a \neq 0$. Si l'on pose, en un point où tous les x_ν ont des valeurs déterminées (finies ou infinies), $x_\nu = \frac{\lambda_\nu}{\sigma_\nu}$, avec $(\lambda_\nu, \sigma_\nu) = 1$, on aura: $a\lambda_1^{k_1}\lambda_2^{k_2} \ldots \lambda_m^{k_m} + \sum_1^m * \sigma_\nu = 0$, d'où $(\sigma_1, \sigma_2, \ldots, \sigma_m)/a$.

7. Considérons maintenant des fonctions $x_1, x_2, \ldots, x_m$ ayant respectivement $S_1, S_2, \ldots, S_m$ pour systèmes d'infinis, et telles que, si S est le pgcd des S_ν, les m quotients $S_\nu : S$ soient sans point commun. Soit d'autre part $f_1, f_2, \ldots, f_p$ une famille régulière dont le système d'infinis Σ soit multiple de S: *la distribution* $[f_1, f_2, \ldots, f_p]$ *sera divisible par* $([x_1], [x_2], \ldots [x_m])$ *presque partout,* ou, plus précisément, partout sauf en un point d'indétermination de l'un des x_i. En effet, d'après la définition des familles régulières, les systèmes d'infinis des mp fonctions $\frac{x_i}{f_i}$ sont sans point commun. Posons donc, en un point où les $\frac{x_\nu}{f_i}$ sont

déterminées, $x_\nu = \frac{\lambda_\nu}{\sigma_\nu}$, avec $(\lambda_\nu, \sigma_\nu) = 1$, et $[f_1, f_2, \ldots, f_p] = \delta, f_i = \frac{\alpha_i}{\delta}$. On aura: $\left(\begin{matrix}\alpha_i\sigma_\nu \\ (\alpha_i\sigma_\nu, \lambda, \delta)\end{matrix}\right)/a$, le premier membre désignant le pgcd des distributions engendrées par les mp fonctions $\frac{x_\nu}{f_i}$, d'où $(\sigma_1, \sigma_2, \ldots, \sigma_m)/a\delta$: cette relation est du reste vérifiée d'elle-même en un zéro de x_ν, car alors $\sigma_\nu = 1$, et en un point de Σ, car alors $\delta = 0$: elle est donc bien vérifiée partout sauf aux points d'indétermination des x_ν.

Soient alors m familles régulières $x_1^{(\nu)}, x_2^{(\nu)}, \ldots, x_{h_\nu}^{(\nu)}$ $(\nu = 1, 2, \ldots, m)$ ayant les systèmes S_ν pour systèmes d'infinis respectifs, et telles que, si S est le pgcd des S_ν, les $S_\nu : S$ soient sans point commun; et soit de nouveau $f_1, f_2, \ldots, f_p$ une famille régulière dont le système d'infinis soit multiple de S: $[f_1, f_2, \ldots, f_p]$ *sera divisible par le pgcd des m distributions* $[x_1^{(\nu)}, x_2^{(\nu)}, \ldots, x_{h_\nu}^{(\nu)}]$. Posons en effet, en un point M, $[f_1, f_2, \ldots, f_p] = \delta$ et $[x_i^{(\nu)}] = \sigma_i^{(\nu)}$; d'après ce qui précède, on pourra choisir l'entier a de manière à avoir $(\sigma_{i_1}^{(1)}, \sigma_{i_2}^{(2)}, \ldots, \sigma_{i_m}^{(m)})/a\delta$ quels que soient les indices i_ν et le point M, sauf peut-être si M est un point d'indétermination de l'un des $x_{i_\nu}^{(\nu)}$; mais si $x_{i_1}^{(1)}$, par exemple, est indéterminé en M, M sera sur S_1, et il y aura j_1 tel que $x_{j_1}^{(1)}$ soit déterminé et infini en M, remplaçons de même chacun des $x_{i_\nu}^{(\nu)}$ qui sont indéterminés en M par un $x_{j_\nu}^{(\nu)}$ déterminé et infini en M, et soit $j_\nu = i_\nu$ quand $x_{i_\nu}^{(\nu)}$ est déterminé en M: on aura, en M, $(\sigma_{j_1}^{(1)}, \sigma_{j_2}^{(2)}, \ldots, \sigma_{j_m}^{(m)})/a\delta$ et $\sigma_{j_\nu}^{(\nu)} = \sigma_{i_\nu}^{(\nu)}$ quel que soit ν. La relation $(\sigma_{i_1}^{(1)}, \sigma_{i_2}^{(2)}, \ldots, \sigma_{i_m}^{(m)})/a\delta$ est donc vérifiée en tout point quels que soient les i_ν; si donc, en M, $[x_1^{(\nu)}, x_2^{(\nu)}, \ldots, x_{h_\nu}^{(\nu)}] = \tau_\nu$, on a bien $(\tau_1, \tau_2, \ldots, \tau_m)/a\delta$ quel que soit M. Si l'on considère alors p familles régulières telles que leurs systèmes d'infinis respectifs aient S pour pgcd et que les quotients de ces systèmes par S soient sans point commun, elles engendrent des distributions dont le pgcd est équivalent au pgcd des $[x_1^{(\nu)}, x_2^{(\nu)}, \ldots, x_{h_\nu}^{(\nu)}]$, car chacun de ces pgcd, d'après ce qui précède, est divisible par l'autre; *si donc, S étant donné, on peut choisir de telles familles* d'une manière au moins, *le pgcd des distributions qu'elles engendrent est parfaitement déterminé* (à une équivalence près) *par la donnée de S*; on le nommera *la distribution appartenant à S*, et on le notera $\boldsymbol{d}_S$.

Soient $x_1, x_2, \ldots, x_m$ et $y_1, y_2, \ldots, y_p$ deux familles régulières, ayant pour systèmes d'infinis S et T, et considérons la famille constituée par les mp fonctions $x_i y_j$: *c'est une famille régulière ayant S . T pour système d'infinis*, que nous

nommerons *le produit des familles x_i et y_j*; et *la distribution qu'elle engendre est équivalente au produit des distributions engendrées par les familles x_i et y_j*: car elle est équivalente à la distribution engendrée par la famille régulière, de système d'infinis ST, qui est constituée par les $3mp$ fonctions $x_i y_j$, $(x_i+1)y_j$ et $x_i(y_j+1)$; mais cette dernière famille engendre la distribution $[x_1, x_2, \ldots, x_m].[y_1, y_2, \ldots, y_p]$, car cela résulte du fait qu'en général le ppcm de $[xy]$, $[(x+1)y]$ et $[x(y+1)]$ est $[x].[y]$. Considérons alors m familles régulières, ayant respectivement pour systèmes d'infinis $S_1, S_2, \ldots, S_m$ et engendrant des distributions $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m$, et p autres familles régulières, ayant pour systèmes d'infinis $T_1, T_2, \ldots, T_p$ et engendrant des distributions $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_p$; formons le produit de chacune des familles du premier groupe par chacune des familles du second: nous obtenons mp familles régulières, ayant pour systèmes d'infinis respectifs les systèmes $S_\mu T_\nu$, et engendrant respectivement les distributions $\boldsymbol{a}_\mu \boldsymbol{b}_\nu$. Soient S le pgcd des S_μ, T celui des T_ν, et supposons qu'il n'y ait aucun point commun aux systèmes $S_\mu : S$, ni aux systèmes $T_\nu : T$: alors le pgcd des $\boldsymbol{a}_\mu$ est la distribution $\boldsymbol{d}_S$ appartenant à S, et de même le pgcd des $\boldsymbol{b}_\nu$ est $\boldsymbol{d}_T$. Dans ce cas *il n'y a non plus aucun point commun aux mp systèmes $(S_\mu T_\nu) : (ST)$, de sorte que le pgcd $\boldsymbol{d}_S . \boldsymbol{d}_T$ des mp distributions $\boldsymbol{a}_\mu \boldsymbol{b}_\nu$ est équivalent à la distribution $\boldsymbol{d}_{S.T}$ appartenant à $S.T$*: $\boldsymbol{d}_{S.T} \sim \boldsymbol{d}_S . \boldsymbol{d}_T$.

8. Or, la variété V étant sans point singulier, l'on peut faire correspondre, à tout système S, des familles régulières telles que leurs systèmes d'infinis aient S pour pgcd et que les quotients de ces systèmes par S soient sans point commun[10]: tout système étant un produit de »surfaces», il suffit de montrer qu'il en est ainsi pour toute surface V. Soient en effet $X_0, X_1, \ldots, X_l$ les coordonnées homogènes d'un point de V, soit U une surface rationnelle relativement à K, et considérons l'ensemble des polynômes en $X_0, X_1, \ldots, X_l$, à coefficients rationnels relativement à K, qui s'annulent chaque fois que le point $(X_0, X_1, \ldots, X_l)$ se trouve sur U. D'après un théorème célèbre de Hilbert[11], on peut choisir dans cet ensemble des polynômes $P_1, P_2, \ldots, P_N$ en nombre fini, tels que tout

[10] Il est essentiel, pour qu'il en soit ainsi, que V soit sans singularité ou du moins transformable en une variété sans singularité par une transformation birationnelle et biunivoque sans exception; et il n'en serait pas ainsi, par exemple, sur un cône du second degré. Je dois cette remarque et cet exemple à B. L. van der Waerden.

[11] Hilbert, *Ueber die Theorie der algebraischen Formen*, Math. Ann. t. 36 (1890), p. 473 (v. § 1, Th. I). Cf. sur ce théorème les mémoires de E. Noether et B. L. van der Waerden déjà cités.

autre polynôme de l'ensemble soit de la forme $\sum_1^N P_i Q_i$, les Q_i étant des polynômes quelconques; dans le cas présent, on peut même supposer que les P_i sont homogènes, de degrés respectifs d_i. Soient $P_1, P_2, \ldots, P_\varrho$ ceux des P_i qui ne s'annulent pas en tout point de V: ils ne s'annulent simultanément en aucun point de V non situé sur U; si P_λ est l'un d'eux, les fonctions $\frac{X_0^{\alpha_0} X_1^{\alpha_1} \ldots X_l^{\alpha_l}}{P_\lambda}$, où l'on donne aux α tous les systèmes de valeurs entières ≥ 0 de somme d_λ, forment une famille régulière dont le système d'infinis est l'intersection Σ_λ de V avec la variété à $l-1$ dimensions $P_\lambda(X_0, X_1, \ldots, X_l) = 0$. Et les systèmes $\Sigma_\lambda : U$ sont sans point commun. Car supposons un instant qu'ils passent tous par A: alors, en désignant par P un quelconque des polynômes qui s'annulent sur U et par Σ l'intersection de V avec $P=0$, on aurait $P = \Sigma P_i Q_i$, et $\Sigma : U$ passerait par A. Mais, A étant un point simple de V, V a en A une variété linéaire tangente à n dimensions: soient $Y_0 = Y_1 = \cdots = Y_n = 0$ les équations d'une variété linéaire L à $l-n-1$ dimensions qui ne coupe pas cette variété tangente, les Y étant des combinaisons linéaires des X à coefficients dans K; et soit $F(Y_0, Y_1, \ldots, Y_n)$ le polynôme irréductible en $Y_0, Y_1, \ldots, Y_n$ qui s'annule sur U, de sorte que $F=0$ sera l'équation de la variété projetant V à partir de L. Si nous prenons $P = F(Y_0, Y_1, \ldots, Y_n)$, le point A, étant simple sur V, aura sur U et sur Σ le même ordre de multiplicité, et par suite $\Sigma : U$ ne passera pas par A.

Faisons alors correspondre à toute surface U, par une règle univoque mais arbitraire, des familles régulières telles que leurs systèmes d'infinis respectifs aient U pour pgcd et que les quotients de ces systèmes par U soient sans point commun: supposons seulement que ces familles soient formées de fonctions rationnelles relativement à $k(V)$, et que les fonctions des familles correspondant à des surfaces conjuguées relativement à k soient respectivement conjuguées relativement à k. La règle adoptée permet de calculer en tout point algébrique la distribution $\boldsymbol{d}_V$ appartenant à une surface V, distribution qui n'était définie jusqu'à présent (en supposant qu'elle existât) qu'à une équivalence près; soit $\omega(U, M)$ la valeur de $\boldsymbol{d}_V$ en M, fournie par cette règle: c'est un idéal du corps $k(U, M)$ (c'est-à-dire du plus petit surcorps de k relativement auquel V et M sont rationnels).

9. Convenons de dire qu'un système de surfaces est constitué par les sur-

faces $U_1, U_2, \ldots, U_m$ s'il se compose de celles des U_i qui sont distinctes, chacune étant prise autant de fois qu'elle figure dans la suite $U_1, U_2, \ldots, U_m$. Nous avons démontré le théorème suivant:

Théorème. — Soit S un système de surfaces rationnel relativement à K, constitué par les surfaces $U_1, U_2, \ldots, U_m$: à S appartient une distribution $\boldsymbol{d}_S$ rationnelle relativement à K, et l'on a:

$$\boldsymbol{d}_S \sim \boldsymbol{d}_{U_1} . \boldsymbol{d}_{U_2} . \ \ldots \ \boldsymbol{d}_{U_n} .$$

Soit x une fonction rationnelle relativement à K; soient S et T les systèmes d'infinis respectifs de x et de $\frac{1}{x}$. Considérons m familles régulières $f_1^{(\nu)}, f_2^{(\nu)}, \ldots, f_{h_\nu}^{(\nu)}$ $(\nu = 1, 2, \ldots, m)$ telles que leurs systèmes d'infinis respectifs soient des multiples $R_\nu T$ de T, et que les quotients R_ν soient sans point commun: alors le pgcd des m distributions $[f_1^{(\nu)}, f_2^{(\nu)}, \ldots, f_{h_\nu}^{(\nu)}]$, qui est multiple de $\left[\frac{1}{x}\right]$, est équivalent à $\boldsymbol{d}_T$; soit donc $\boldsymbol{a}$ une distribution telle que $\boldsymbol{d}_T \sim \boldsymbol{a}\left[\frac{1}{x}\right]$. Les fonctions $xf_1^{(\nu)}, xf_2^{(\nu)}, \ldots, xf_{h_\nu}^{(\nu)}$ forment une famille régulière de système d'infinis $R_\nu S$; donc le pgcd des m distributions $[xf_1^{(\nu)}, xf_2^{(\nu)}, \ldots, xf_{h_\nu}^{(\nu)}]$ est équivalent à $\boldsymbol{d}_S$: mais il est équivalent à $\boldsymbol{a}[x]$, puisque x est égal en tout point au quotient des valeurs de $\left[\frac{1}{x}\right]$ et de $[x]$. Nous avons ainsi le théorème suivant:

Théorème de décomposition. — V étant une variété algébrique sans singularité, et rationnelle relativement à k, l'on peut faire correspondre à toute »surface» algébrique U et à tout point algébrique M sur V un idéal $\omega(U, M)$ du corps $k(U, M)$, ayant la propriété suivante: soit f une fonction arbitraire d'un point de V, rationnelle relativement à K, et soient respectivement $U_1, U_2, \ldots, U_p$ et $U'_1, U'_2, \ldots, U'_q$ les surfaces constituant les systèmes d'infinis de f et de $\frac{1}{f}$; on aura, en tout point algébrique M sur V:

$$f(M) = \frac{\lambda \omega(U'_1, M) . \omega(U'_2, M) . \ \ldots \ \omega(U'_q, M)}{\mu \omega(U_1, M) . \omega(U_2, M) . \ \ldots \ \omega(U_p, M)}$$

λ et μ étant des idéaux bornés, c'est-à-dire divisant des entiers indépendants de M.[12]

[12] Ici, contrairement au cas ou V était à une dimension, le pgcd du numérateur et du dénominateur n'est plus nécessairement un idéal borné.

Observons que toutes les notions que nous avons définies jouissent, comme on dit, de l'*invariance relative*, c'est-à-dire qu'elles sont invariantes par toute transformation birationnelle et biunivoque sans exception. En particulier, nos résultats sont valables, non seulement pour les variétés sans singularités, mais encore pour celles qui sont en correspondance birationnelle et biunivoque sans exception avec une variété sans singularités.

10. Démontrons encore un résultat dont nous aurons besoin au chapitre II. Soit de nouveau V sans singularités, et soit t une transformation de V en elle-même qui, à tout point M de V, fasse correspondre sans exception un point bien déterminé tM de V dépendant rationnellement de M, de telle sorte que tout point P de V, sans exception, corresponde à r points bien déterminés, distincts ou confondus, qui seront appelés $t^{-1}P$: une telle transformation sera appelée une transformation $(1, r)$ sans exception de V en elle-même. U étant une surface sur V, et P un point qui décrit U, nous appellerons $t^{-1}U$ le système de surfaces composé des surfaces décrites par les points $t^{-1}P$, chacune de ces surfaces étant affectée d'une multiplicité égale au nombre de points $t^{-1}P$ qui coïncident avec un point pris génériquement sur elle; et, si S est un système de surfaces constitué par les surfaces $U_1, U_2, \ldots, U_m$, nous appellerons $t^{-1}S$ le produit des m systèmes $t^{-1}U_i$. De toute fonction $f(M)$, ayant S pour système d'infinis, l'on déduit au moyen de t une fonction $f(tM)$ ayant $t^{-1}S$ pour système d'infinis; et si les fonctions $f_1, f_2, \ldots, f_h$ forment une famille régulière de système d'infinis S, les fonctions $f_1(tM), f_2(tM), \ldots, f_h(tM)$ formeront une famille régulière de système d'infinis $t^{-1}S$.

Soit alors S un système quelconque, et considérons m familles régulières $f_1^{(\nu)}, f_2^{(\nu)}, \ldots, f_{h_\nu}^{(\nu)}$ $(\nu = 1, 2, \ldots, m)$ telles que leurs systèmes d'infinis aient S pour pgcd et que les m quotients soient sans point commun. Le pgcd des m distributions $[f_1^{(\nu)}, f_2^{(\nu)}, \ldots, f_{h_\nu}^{(\nu)}]$ est équivalent à $\mathfrak{d}_S$: soit $\omega(S, M)$ sa valeur en un point M. Alors les m familles $f_1^{(\nu)}(tM), f_2^{(\nu)}(tM), \ldots, f_{h_\nu}^{(\nu)}(tM)$ seront régulières, et telles que leurs systèmes d'infinis aient $t^{-1}S$ pour pgcd et que les quotients soient sans point commun. Par conséquent le pgcd des distributions qu'elles engendrent est équivalent à $\mathfrak{d}_{t^{-1}S}$: mais ce pgcd a pour valeur en M l'idéal $\omega(S, tM)$. Donc *la distribution qui a pour valeur $\omega(S, tM)$ en tout point algébrique M est équivalente à la distribution appartenant à $t^{-1}S$.* Si l'on connait la distribution appartenant à S, on en déduit ainsi celle qui appartient à $t^{-1}S$. Ce résultat peut aussi s'écrire, en désignant par $\omega(t^{-1}S, M)$ la valeur en M d'une distribution appartenant à $t^{-1}S$: $\omega(S, tM) = \omega(t^{-1}S, M)$.

CHAPITRE II.

Les systèmes rationnels de p points sur les courbes de genre p.

11. Soit C une courbe algébrique de genre p, rationnelle relativement à k. Soient w_ν $(\nu = 1, 2, \ldots, p)$ les p intégrales normées de première espèce sur C. Prenons un système fixe Γ de p points $A_1, A_2, \ldots, A_p$ sur C: à tout système de p points $M_1, M_2, \ldots, M_p$ nous ferons correspondre le point de l'espace $(u_1, u_2, \ldots, u_p)$ qui a pour coordonnées:

$$u_\nu = \sum_{i=1}^{p} \int_{A_i}^{M_i} dw_\nu .$$

Convenons de considérer des points de l'espace (u) comme identiques si les différences de leurs coordonnées forment un système de périodes des intégrales w_ν. A tout système S de p points correspond alors un point u et un seul; et un point u correspond en général à un système S bien déterminé (ou en tout cas à une série linéaire complète de systèmes équivalents). En raison de cette correspondance, nous parlerons indifféremment du système S ou du point u qui lui correspond; cela conduit à *ne pas distinguer entre des systèmes équivalents*, et aussi, par exemple, à dire qu'un point u est rationnel relativement à K s'il correspond à un système rationnel relativement à K. Si les systèmes S, S', T correspondent aux points u, u', v, nous noterons $S + S' - T$ le système correspondant à $u + u' - v$, c'est à-dire au point dont les coordonnées sont les combinaisons $u_\nu + u'_\nu - v_\nu$ des coordonnées de u, u', v: ce n'est là, du reste, que la notation courante en géométrie algébrique.

Dans ce qui suit, et jusqu'à la fin de ce chapitre, le mot de système désignera, sauf indication contraire, un système de p points sur C.

12. Γ étant le système fixe choisi plus haut, soit $f_\gamma(M)$ une fonction de degré $2p$ ayant chacun des points de Γ pour pôle double, et ayant des zéros doubles en p points formant un système γ. Si s est un système quelconque formé des points $M_1, M_2, \ldots, M_p$, nous posons:

$$F_\gamma(s) = h \, . f_\gamma(M_1) f_\gamma(M_2) \cdots f_\gamma(M_p),$$

h étant une constante que nous fixerons plus loin.

Considérons deux systèmes variables g, g' et deux systèmes fixes g_0, g'_0, ainsi que les systèmes $G = g + g' - \Gamma$ et $G_0 = g_0 + g'_0 - \Gamma$; soit φ la fonction de degré $2p$ qui a pour pôles les points de G et Γ et pour zéros ceux de g et g'; soit de même φ_0 la fonction ayant pour pôles G_0 et Γ et pour zéros g_0 et g'_0. Supposons que Γ et γ n'aient aucun point commun avec g, g', G, g_0, g'_0, G_0, et traçons sur la surface de Riemann de C un contour fermé Σ divisant cette surface en deux morceaux, dont l'un $\mathfrak{I}$ contienne Γ et γ et l'autre $\mathfrak{S}$ contienne g, g', G, g_0, g'_0, G_0. La fonction $\psi = \frac{\varphi}{\varphi_0}$ aura pour pôles G, g_0, g'_0 et pour zéros G_0, g, g'.

Considérons l'intégrale:

$$\frac{1}{2\pi i}\int_{\Sigma} \log f_\gamma \, . \, d(\log \psi).$$

Dans $\mathfrak{S}$, $\log f_\gamma$ est régulier, cette intégrale aura donc pour valeur:

$$\log \left[\frac{F_\gamma(G)\, F_\gamma(g_0)\, F_\gamma(g'_0)}{F_\gamma(G_0)\, F_\gamma(g)\, F_\gamma(g')}\right].$$

D'autre part, quand on décrit Σ, $\log f_\gamma$ et $\log \psi$ reviennent à leurs valeurs initiales, on peut donc intégrer par parties et écrire notre intégrale:

$$-\frac{1}{2\pi i}\int_{\Sigma} \log \psi \, . \, d(\log f_\gamma).$$

Posons, s étant un système de points $M_1, M_2, \ldots, M_p$:

$$\Phi(s) = \psi(M_1) \, . \, \psi(M_2) \, . \, \ldots \, \psi(M_p)$$

on trouve, pour valeur de l'intégrale, $\log \psi$ étant régulier dans $\mathfrak{I}$: $2 \log \frac{\Phi(\Gamma)}{\Phi(\gamma)}$.

Choisissons alors h de façon que $F_\gamma(g_0)\, F_\gamma(g'_0) = F_\gamma(G_0)$; nous aurons:

$$\frac{F_\gamma(G)}{F_\gamma(g)\, F_\gamma(g')} = \left[\frac{\Phi(\Gamma)}{\Phi(\gamma)}\right]^2, \quad G = g + g' - \Gamma \tag{A}$$

et en particulier, pour $g = g'$:

$$F_\gamma(G) = \left[F_\gamma(g)\frac{\Phi(\Gamma)}{\Phi(\gamma)}\right]^2, \quad G = 2g - \Gamma. \tag{B}$$

13. Supposons maintenant qu'il existe sur C des systèmes rationnels de p points, et que Γ, g_0, g'_0 soient de tels systèmes. Si les points u, v de l'espace (u) sont rationnels, les points $u \pm v$ le seront aussi: les points rationnels forment un *module* (ou. en d'autres termes, un groupe abélien par rapport à l'addition).

Nous nous proposons, au cours de ce chapitre, de démontrer le théorème suivant:

Théorème de la base finie. — Le module des points rationnels de l'espace (u) *possède une base formée d'un nombre fini de points.*

En d'autres termes, il suffit de connaître sur C un nombre fini de systèmes rationnels pour trouver rationnellement tous les autres.

Si ce théorème est vrai pour un surcorps K de k, il sera aussi vrai pour k. Car le module des points u rationnels relativement à k est contenu dans le module des points rationnels relativement à K et est de base finie si c'est le cas pour ce dernier. Cette remarque nous autorise à remplacer, au cours de la démonstration, k par tel surcorps que nous voudrons, sans que cela diminue en rien la généralité du résultat. Nous supposerons en particulier que *les* $2^{2p}-1$ *systèmes* γ (qui se déduisent de Γ par l'addition, au point correspondant à Γ dans l'espace (u), des $2^{2p}-1$ demi-périodes non nulles) *sont tous rationnels*: car il en est ainsi si l'on a remplacé k par un surcorps convenable.

Appliquons le théorème de décomposition à la fonction $f_\gamma(M)$; nous obtenons:

$$f_\gamma(M) = \frac{\lambda \eta^2(M)}{\mu H^2(M)}.$$

$\eta(M)$ et $H(M)$ étant les valeurs en M de distributions rationnelles et λ et μ divisant des entiers fixes. On a donc, si S est un système rationnel formé des points $M_1, M_2, \ldots, M_p$:

$$F_\gamma(S) = h \cdot \frac{\lambda_1 \lambda_2 \ldots \lambda_p}{\mu_1 \mu_2 \ldots \mu_p} \left[\begin{matrix} \eta(M_1) \ldots \eta(M_p) \\ H(M_1) \ldots H(M_p) \end{matrix} \right]^2.$$

Soit $h = \frac{\varrho}{\sigma}$, ϱ et σ étant des idéaux entiers, et posons

$$\Omega = \frac{1}{\sigma . \mu_1 \ldots \mu_p} \cdot \frac{\eta(M_1) \ldots \eta(M_p)}{H(M_1) \ldots H(M_p)}:$$

Ω est un idéal de k. Prenons, dans chaque classe d'idéaux de k, un idéal fixe; si α est celui qui est de la classe de Ω, l'on aura:

$$F_\gamma(S) = (\varrho\sigma \,.\, \lambda_1 \ldots \lambda_p \,.\, \mu_1 \ldots \mu_p \,.\, \alpha^2) \times \left(\frac{\Omega}{\alpha}\right)^2$$

où le premier facteur est un idéal principal entier qui n'est susceptible que d'un nombre fini de valeurs: désignons celles-ci par $(m'_1), (m'_2), \ldots, (m'_M)$, les m'_i étant des entiers de k. Soit donc (m'_i) ce premier facteur et soit $\frac{\Omega}{\alpha} = (a')$, a' étant un nombre de k; $\frac{F_\gamma(S)}{m'_i a'^2}$ sera une unité, qu'on pourra écrire $\varepsilon_0^{k_0} \,.\, \varepsilon_1^{k_1} \ldots \varepsilon_r^{k_r}$ si $\varepsilon_0, \varepsilon_1 \ldots \varepsilon_r$ est une base pour le groupe des unités de k. Prenons l_i égal à 0 ou 1 suivant que k_i est pair ou impair; on aura:

$$F_\gamma(S) = m'_i \varepsilon_0^{l_0} \varepsilon_1^{l_1} \ldots \varepsilon_r^{l_r} \times \left(\varepsilon_0^{\frac{k_0-l_0}{2}} \,.\, \varepsilon_1^{\frac{k_1-l_1}{2}} \ldots \varepsilon_r^{\frac{k_r-l_r}{2}} \,.\, a'\right)^2;$$

$m'_i \varepsilon_0^{l_0} \ldots \varepsilon_r^{l_r}$ n'est susceptible que d'un nombre fini de valeurs distinctes, donc:

$$F_\gamma(S) = m \,.\, a^2 \qquad \text{(C)}$$

a étant un nombre de k, et m étant un entier qui ne prend qu'un nombre fini de valeurs distinctes quand on prend pour S tous les systèmes rationnels.

Si le système S correspond au point u, nous poserons $F_\gamma(u) = F_\gamma(S)$; $F_\gamma(u)$ est une fonction abélienne de u.

14. Disons que deux points rationnels u, v appartiennent à la même *classe*, et écrivons $u \infty v$, si chacun des $2^{2p}-1$ nombres $\frac{F_\gamma(u)}{F_\gamma(v)}$, obtenus en choisissant γ de toutes les manières possibles, est le carré d'un nombre de k. (C) montre que le nombre h des classes est fini. (A) montre que si $u \infty v$, $u' \infty v'$, on a aussi $u+u' \infty v+v'$; il en résulte que par rapport à l'addition des systèmes, les classes forment un groupe abélien fini. La classe unité est la classe des points u tels que chacun des nombres $F_\gamma(u)$ soit le carré d'un nombre de k; dans ce cas nous écrivons $u \infty 0$. (B) montre que si u est un point rationnel, $2u \infty 0$: le groupe des classes n'a donc que des éléments d'ordre 2.

Inversement, *si* $u \infty 0$, *les* 2^{2p} *points* $\frac{u}{2}$ (qui se déduisent de l'un d'entre eux par l'addition de toutes les demi-périodes) *sont rationnels*. L'on a dans ce cas, par hypothèse:

$$\sqrt{F_\gamma(u)} = F_\gamma\left(\frac{u}{2}\right) \frac{\Phi(\Gamma)}{\Phi(\gamma)} = a_\gamma$$

a_γ étant un nombre de k qui dépend de γ. Dans cette équation, $\Phi(\Gamma)$ et $\Phi(\gamma)$ représentent les produits, étendus à tous les points de Γ et de γ respectivement, des valeurs de la fonction ψ qui a pour pôles les points du système u, de g_0 et de g'_0, pour zéros doubles les points du système $\frac{u}{2}$ et pour zéros simples ceux de G_0. Or si A et B sont deux points fixes, $\frac{\psi(A)}{\psi(B)}$ est une fonction abélienne de $\frac{u}{2}$; par suite $\frac{\Phi(\Gamma)}{\Phi(\gamma)}$ est une fonction abélienne de $\frac{u}{2}$, et il en est de même de la fonction $F_\gamma\left(\frac{u}{2}\right)\frac{\Phi(\Gamma)}{\Phi(\gamma)}$. Quand les coordonnées de u augmentent d'un système de périodes, cette dernière fonction, étant égale à $\sqrt{F_\gamma(u)}$, se trouve multipliée par un facteur ± 1: mais ce facteur ne peut être $+1$ quelle que soit la période, sans quoi la fonction serait une fonction abélienne de u; et en laissant fixes $p-1$ points du système u, la fonction, considérée comme fonction du $p^{\text{ième}}$, serait rationnelle sur C et aurait pour pôles simples les points de Γ et pour zéros simples ceux de γ, ce qui est impossible.

Il y a donc des périodes pour lesquelles la fonction se multiplie par -1; donc, parmi les 2^{2p} points $\frac{u}{2}$, il y en a 2^{2p-1} pour lesquels elle prend la valeur a_γ et 2^{2p-1} pour lesquels elle prend la valeur $-a_\gamma$. Soient g, g' des systèmes correspondant à des points pour lesquels elle prend *la même valeur*, on a:

$$\frac{F_\gamma(g)}{F_\gamma(g')}\cdot\begin{matrix}\Phi_g(\Gamma) & \Phi_{g'}(\gamma)\\ \Phi_g(\gamma) & \Phi_{g'}(\Gamma)\end{matrix} = +1.$$

Posons $\theta = \frac{\psi_{g'}}{\psi_g}$, c'est la fonction qui a pour pôles doubles les points de g et pour zéros doubles ceux de g'; et, si s est un système formé des points $M_1, M_2, \ldots, M_p$, soit $\Theta(s) = \theta(M_1)\theta(M_2)\ldots\theta(M_p) = \frac{\Phi_{g'}(s)}{\Phi_g(s)}$; l'égalité précédente devient:

$$\frac{F_\gamma(g)}{F_\gamma(g')} = \frac{\Theta(\Gamma)}{\Theta(\gamma)}.$$

En se reportant aux définitions de F_γ et Θ, on voit que cette égalité est parfaitement symétrique en Γ et γ d'une part et g et g' de l'autre. Nous venons de démontrer que si Γ, γ, g sont donnés, il y a 2^{2p-1} choix de g' pour lesquels

elle n'est pas satisfaite: donc, si g, g', Γ sont donnés, il y a 2^{2p-1} choix de γ pour lesquels elle n'est pas satisfaite. Autrement dit, de quelque manière que l'on choisisse g et g', il y a 2^{2p-1} choix de γ pour lesquels $F_\gamma(g)\frac{\Phi_g(\Gamma)}{\Phi_g(\gamma)}$ et $F_\gamma(g')\frac{\Phi_{g'}(\Gamma)}{\Phi_{g'}(\gamma)}$ ont des valeurs *rationnelles* opposées. Par suite, dans l'équation de degré 2^{2p} dont dépend la recherche des systèmes correspondant aux points $\frac{u}{2}$, les racines correspondant aux systèmes g, g' ne peuvent appartenir à un même facteur irréductible, et cela quels que soient g, g'; ces racines sont donc bien toutes rationnelles.

14 bis. (Observons, pour ceux qui connaissent la théorie des fonctions abéliennes, que les considérations précédentes ont des rapports étroits avec la théorie des demi-périodes syzygétiques et azygétiques, et peuvent servir à la reconstruire par une voie purement algébrique.

Remarquons aussi que, dans les §§ 11—14, nous aurions pu sans difficulté supplémentaire nous servir, non pas de la bissection des fonctions abéliennes, mais de la division par n, n étant un entier quelconque; au § 11, il aurait alors fallu appeler $f_\gamma(M)$ une fonction de degré np, ayant chacun des points de Γ pour pôle d'ordre n, et ayant des zéros d'ordre n en p points formant un système γ. Dans la formule (A), il n'y aurait qu'à remplacer, au second membre, l'exposant 2 par l'exposant n; la formule (B) serait remplacée par une autre, obtenue en itérant n fois la précédente, et qui donnerait $F_\gamma(ng-(n-1)\Gamma)$ comme puissance n-ième exacte. La suite subsiste presque sans modification, à condition de supposer qu'on a, au besoin, adjoint préalablement au corps k les racines n-ièmes de l'unité.

Cette remarque est importante, car il arrive, dans certaines questions, qu'il faille utiliser la division par n avec des valeurs élevées de n).

15. Supposons dorénavant qu'il y ait dans l'espace (u) une infinité de points rationnels (sans quoi le théorème de la base finie n'aurait pas besoin d'être démontré). Dans chaque classe, choisissons un tel point, et soient $a_1, a_2, \ldots, a_h$ les points ainsi choisis. Soit u un point rationnel quelconque, soit a celui des a_i qui est de la classe de u, on a $u+a\propto 0$, donc (§ 14) les points $\frac{u+a}{2}$ sont rationnels; soit u' l'un d'eux, soit de nouveau a' celui des a_i qui est de la classe de u': on obtient ainsi un point rationnel $u''=\frac{u'+a'}{2}$, sur lequel on opérera de

même, et ainsi de suite indéfiniment. Le théorème de la base finie sera démontré si nous faisons voir que la suite de ces opérations conduit nécessairement à un point $u^{(\nu)}$ faisant partie d'un nombre fini de points $b_1, b_2, \ldots, b_m$ déterminés a priori: car alors les a et les b forment ensemble une base pour le module des points rationnels de l'espace (u).

Pour achever la démonstration, nous étudierons, par les méthodes du chapitre précédent, la »variété jacobienne» de la courbe C: on appelle ainsi toute variété algébrique dont les points sont en correspondance birationnelle et biunivoque avec les séries linéaires complètes de systèmes de p points sur la courbe C; elle est aussi en correspondance biunivoque avec les points de l'espace (u), si l'on considère comme identiques des points de cet espace qui ne diffèrent que par un système de périodes; et elle est en correspondance birationnelle avec les systèmes de p points sur C.

v étant le vecteur de composantes $v_1, v_2, \ldots, v_p$, nous désignerons par $\vartheta(v)$ la fonction thêta des p variables v_i qui est formée avec les périodes des intégrales normées $w_1, w_2, \ldots, w_p$.[13] Si P est un point (que nous prendrons algébrique) sur C, et si $\mathfrak{G}^{2p-2}$ désigne le système des $2p-2$ zéros d'une différentielle de première espèce, on sait qu'il y a 2^{2p} systèmes R_i de p points tels que $2R_i$ soit équivalent à $2P+\mathfrak{G}^{2p-2}$, chacun de ces systèmes correspondant à une des 2^{2p} demi-périodes; et si R est celui qui correspond à la demi-période o, l'équation $\vartheta(u)=0$, où u désigne le point qui correspond à un système S, signifie que le point P fait partie d'un système équivalent à $R+S-\Gamma$. Nous supposerons que R, et par suite le point P, sont rationnels, ce qu'on obtient au besoin en remplaçant k par un surcorps.

Pour fixer les idées, nous nous servirons des fonctions thêta du 3e ordre de caractéristique o: on sait qu'on appelle ainsi toute fonction entière $\Theta(v)$ des p variables $v_1, v_2, \ldots, v_p$ telle que $\dfrac{\Theta(v)}{\vartheta^3(v)}$ se reproduise lorsqu'on ajoute à v un système quelconque de périodes; il y a $P=3^p$ de ces fonctions qui sont linéairement indépendantes, toutes les autres s'exprimant linéairement en fonction de celles-là. Soit $\Theta(v)$ l'une d'entre elles, et soit u le point correspondant à un système $(M_1, M_2, \ldots, M_p)$: alors $\dfrac{\Theta(u)}{\vartheta^3(u)}$ est une fonction symétrique des coordonnées de $M_1, M_2, \ldots, M_p$, qui s'exprime rationnellement (avec des coefficients peut-

[13] Sur les propriétés, utilisées ici, des fonctions thêta, v. p. ex. Krazer-Wirtinger, *Enzykl. d. math. Wiss.* II, B. 7.

être irrationnels) en fonction de ces coordonnées. Réciproquement, soit f une fonction symétrique rationnelle de ces coordonnées, à coefficients rationnels ou non, telle que $f.\vartheta^3(u)$ soit fini pour tout u: $f.\vartheta^3(u)$ sera alors une fonction thêta du troisième ordre de caractéristique o. Or, R et P étant rationnels relativement à k, la condition, pour une fonction symétrique f des coordonnées des M_i, d'être telle que $f.\vartheta^3(u)$ soit toujours fini, est une condition rationnelle relativement à k: puisqu'elle est satisfaite par $P=3^p$ fonctions linéairement indépendantes, on peut choisir ces P fonctions de manière qu'elles soient rationnelles relativement à k: soient $f_1, f_2, \ldots, f_P$ les fonctions ainsi choisies, et soient $\Theta_i(u) = f_i.\vartheta^3(u)$ les fonctions thêta correspondantes.

16. Considérons, dans un espace projectif à $P-1$ dimensions, la variété V à p-dimensions décrite par le point de coordonnées homogènes $X_i = \Theta_i(u)$ $(i = 1, 2, \ldots, P)$ quand u décrit l'espace (u); V est aussi la variété décrite par le point de coordonnées $f_1, f_2, \ldots, f_P$ quand $M_1, M_2, \ldots, M_p$ décrivent indépendamment la courbe C: c'est donc une variété algébrique rationnelle relativement à k. V n'est autre que la variété jacobienne de C, car: 1° à tout point u correspond un point et un seul de V; en effet, si toutes les fonctions Θ_i s'annulaient en un point u_0, la fonction $\vartheta(u-a)\vartheta(u-b)\vartheta(u+a+b)$, qui est une fonction thêta du troisième ordre et par conséquent de la forme $\sum_1^P c_i \Theta_i(u)$, s'annulerait en u_0 quels que soient a, b, ce qui n'est pas; 2° à tout point de V ne correspond qu'un point u, à un système de périodes près; sinon, en effet, il y aurait deux points u_0, v_0 et un nombre ϱ tels que l'on ait, quels que soient a, b:

$$\vartheta(u_0-a)\vartheta(u_0-b)\vartheta(u_0+a+b) = \varrho\,\vartheta(v_0-a)\vartheta(v_0-b)\vartheta(v_0+a+b)$$

ce qui est également impossible.

De plus, la variété jacobienne V est sans singularités. Car si un point u_0 correspondait à un point singulier de V, la matrice à P lignes et $p+1$ colonnes:

$$\left\| \Theta_i(u) \quad \frac{\partial \Theta_i(u)}{\partial u_1} \quad \frac{\partial \Theta_i(u)}{\partial u_p} \right\| \qquad (i = 1, 2, \ldots, P)$$

serait de rang $< p+1$ en u_0, et il y aurait $c_0, c_1, \ldots, c_p$ tels que l'on ait en u_0, quelle que soit la fonction Θ du 3^e ordre: $c_0\Theta + \sum_1^p c_i \frac{\partial \Theta}{\partial u_i} = 0$. Soit en particulier $\Theta(u) = \vartheta(u-u_0+a)\vartheta(u-b)\vartheta(u+u_0-a+b)$, a et b étant tels que $\vartheta(a)=0$,

$\vartheta(u_0-b)\vartheta(2u_0-a+b)\neq 0$. On devra avoir $\sum_1^p c_\nu \frac{\partial\vartheta(a)}{\partial a_\nu}=0$, et cela en tout point a où $\vartheta(a)=0$: mais on sait qu'à un tel point l'on peut faire correspondre un système de $p-1$ points $P_1, P_2, \ldots, P_{p-1}$ sur C, et réciproquement, de telle sorte que $a_\nu = a_\nu^{(0)} + \sum_1^{p-1} \int_{.1}^{P_i} dw_\nu$, donc $\sum_{,-1}^{p} \frac{\partial\vartheta(a)}{\partial a_\nu} dw_\nu(P_i)=0$ $(i=1,2,\ldots,p-1)$. Le déterminant $|c_\nu dw_\nu(P_i)|$ s'annulerait alors quels que soient les P_i: mais c'est impossible, puisque les différentielles dw_ν sont linéairement indépendantes.

Alors, les résultats du chapitre I s'appliquent à V. Soit $\Theta(u)=\sum_1^P e_i\Theta_i(u)$ une fonction du 3e ordre, s'exprimant en fonction des Θ_i avec des coefficients e_i rationnels relativement à k: l'équation $\Theta(u)=0$ définit sur V un système de surfaces rationnel relativement à k, qui est l'intersection de V par le plan $\sum_1^P e_i X_i=0$; soit $\omega(u)$ la valeur, en un point rationnel u, de la distribution qui appartient à ce système de surfaces: c'est un idéal du corps k. Soit, de plus, a un point rationnel fixe, et considérons la transformation qui, à tout point u, fait correspondre le point $U=2u-a$; U correspondra ainsi à 2^{2p} points u distincts. C'est une transformation $(1, 2^{2p})$ sans exception de V en elle-même. Si donc nous considérons le système de surfaces, défini par $\Theta(2u-a)=0$, qui est le transformé du système $\Theta(u)=0$ par cette transformation, la distribution appartenant à ce nouveau système aura pour valeur en u, en vertu du § 10, l'idéal $\omega(2u-a)$.

Soit maintenant ε une demi-période quelconque; elle correspond à un système γ que nous avons supposé rationnel (§ 13). Considérons la fonction:

$$F(u)=C\frac{\Theta^2(u)\vartheta^3(u-a-\varepsilon)\vartheta^3(u-a+\varepsilon)}{\Theta(2u-a)}.$$

a, ε et les coefficients e_i de $\Theta=\Sigma e_i\Theta_i$ étant rationnels, les systèmes d'infinis de F et de $\frac{1}{F}$ sur V sont des systèmes rationnels; si donc on a choisi convenablement le coefficient C, la fonction F est, sur V, une fonction rationnelle relativement à k. Soit $\eta(u)$ la distribution correspondant au système de surfaces défini par $\vartheta(u-a\pm\varepsilon)=0$; on aura:

$$F(u) = \frac{\lambda\,\omega^2(u)\,\eta^6(u)}{\mu\,\omega(2u-a)}$$

λ et μ divisant des entiers indépendants de u.

Supposons que $\vartheta(u-a\pm\varepsilon)\neq 0$, et par suite $\eta(u)\neq 0$, donc $N\eta(u)\geq 1$. En prenant les normes des deux membres, on obtient l'inégalité:

$$[N\omega(u)]^2 \leq m(a,\varepsilon)\,.\,|NF(u)|\,.\,N\omega(2u-a).$$

17. Admettons, pour simplifier le langage, que k soit normal, c'est-à-dire identique à ses conjugués (sinon on remplacerait k par un surcorps normal). Considérons les automorphismes de k, c'est-à-dire les transformations de k en lui-même qui conservent les relations rationnelles: ce sont les opérations qui constituent le groupe de Galois de k. Si k est imaginaire, ces automorphismes se répartissent en paires d'automorphismes imaginaires conjugués, et nous ne garderons qu'un automorphisme de chaque paire; si k est réel, nous garderons tous les automorphismes; soit σ égal à 2 dans le premier cas, à 1 dans le second; et soient en tout cas $A, A, A, \ldots$ les automorphismes conservés, A étant l'automorphisme identique.

$\bar{A}$ transforme C en une courbe C', également rationnelle relativement à k. Tout système de points (ou toute fonction) rationnel sur C' est transformé en un système (ou en une fonction) rationnel sur C'. Choisissons sur C' les p intégrales normées de première espèce, et formons avec leurs périodes la fonction thêta, $\bar{\vartheta}(r)$. A tout point rationnel u de l'espace (u) correspond un système rationnel S sur C', et par suite (au moyen de l'automorphisme A) un système rationnel S sur C, donc aussi un point rationnel $\bar{u}$ de l'espace $(\bar{u})$; et réciproquement; et si $\vartheta(u)=0$, le point P fait partie d'un système équivalent à $R+S-I$, donc le point transformé P' fait partie d'un système équivalent à $\bar{R}+\bar{S}-I'$, et $\vartheta(\bar{u})=0$. Les fonctions symétriques rationnelles f_i des coordonnées de $M_1, M_2, \ldots, M_p$ sur C, telles que $f_i\vartheta^3(u)$ soit toujours fini, sont transformées en des fonctions symétriques rationnelles $\bar{f}_i$ des coordonnées de $M_1, M_2, \ldots, M_p$ sur C, telles que $\bar{f}_i\,.\,\vartheta^3(\bar{u})$ soit toujours fini; et par suite V, variété jacobienne de C, qui est engendrée par le point $(f_1, f_2, \ldots f_p)$, est transformée en V', variété jacobienne de C', engendrée par le point $(\bar{f}_1, \bar{f}_2, \ldots, \bar{f}_p)$. Nous poserons $\bar{\Theta}_i = \bar{f}_i\bar{\vartheta}^3$, et $\Theta = \sum_1^p \bar{e}_i\Theta_i$, si $\bar{A}$ transforme e_i en $\bar{e}_i$.

A $F(u)$ correspond, dans l'automorphisme $\bar{A}$, une fonction $\bar{F}$ rationnelle sur $\bar{V}$; les systèmes d'infinis de $\bar{F}$ et $\frac{\mathrm{I}}{\bar{F}}$ étant les transformés de ceux de F et $\frac{\mathrm{I}}{F}$ par l'automorphisme $\bar{A}$, $\bar{F}$ est de la forme:

$$F(\bar{u}) = \bar{C}\,\frac{\bar{\Theta}^2(\bar{u})\,\bar{\vartheta}^3(\bar{u}-\bar{a}-\bar{\varepsilon})\,\bar{\vartheta}^3(\bar{u}-\bar{a}+\varepsilon)}{\bar{\Theta}(2\,\bar{u}-\bar{a})}.$$

$\bar{C}$ étant une certaine constante. Mais on a, pour u rationnel:

$$|\,N\,F(u)\,| = |\,F(u)\,.\,\bar{F}(\bar{u})\,.\,\bar{F}(\bar{\bar{u}})\,.\,\ldots\,|^{\sigma}.$$

Posons alors, pour simplifier:

$$\Omega(u) = \frac{N\,\omega(u)}{|\,\Theta(u)\,.\,\bar{\Theta}(\bar{u})\,.\,\bar{\bar{\Theta}}(\bar{\bar{u}})\,.\,\ldots\,|^{\sigma}}, \qquad \mathcal{A}(u,\bar{u},\ldots) = |\,\vartheta^3(u-a-\varepsilon)\,\bar{\vartheta}^3(\bar{u}-\bar{a}-\bar{\varepsilon})\ldots \,.\,\vartheta^3(u-a+\varepsilon)\,\bar{\vartheta}^3(\bar{u}-\bar{a}+\bar{\varepsilon})\ldots\,|^{\sigma}.$$

L'inégalité de la fin du § 16 devient alors:

$$[\Omega(u)]^2 \leq m_1\,.\,\mathcal{A}(u,\bar{u},\ldots)\,.\,\Omega(2u-a)$$

où le facteur m_1 ne dépend que de $a, \bar{a}, \ldots, \varepsilon, \bar{\varepsilon}, \ldots$.

18. Jusqu'à présent, nous étions convenus de ne pas distinguer, dans l'espace (u), entre des points ne différant que par un système de périodes. Abandonnant maintenant cette convention, choisissons dans chacun des espaces (u), $(\bar{u}), \ldots$ un parallélotope de périodes $\Pi, \bar{\Pi}, \ldots$. Revenons alors aux notations du début du § 15, que nous préciserons comme il suit: soit u un point rationnel quelconque dans Π, nous définirons les points rationnels $u', u'', \ldots$ par récurrence; soit a_{i_1} celui des points $a_1, a_2, \ldots, a_h$ du § 15 qui est de la classe de $u^{(1)}$, nous appellerons $u^{(2)}$ un point de Π tel que les coordonnées de $a^{(1)} = 2\,u^{(2)} - u^{(1)}$ ne diffèrent de celles de a_{i_1} que par un système de périodes; nous appellerons $\bar{u}^{(1)}, \bar{u}^{(2)}, \ldots$ les points rationnels de $\bar{\Pi}, \Pi, \ldots$ qui correspondent à $u^{(1)}$; et nous poserons $\bar{a}^{(1)} = 2\,\bar{u}^{(2)} - \bar{u}^{(1)}, \ldots$; dans ces conditions, si $a^{(\nu)}$ n'est pas nécessairement dans Π, il n'est pourtant susceptible que d'un nombre fini de positions, et il en est de même pour $\bar{a}^{(\nu)}, \bar{\bar{a}}^{(\nu)}, \ldots$. Dans la dernière inégalité trouvée, remplaçons alors $u, \bar{u}, \ldots, a, \bar{a}, \ldots$ par $u^{(2)}, \bar{u}^{(2)}, \ldots, a^{(1)}, \bar{a}^{(1)}, \ldots$; prenons pour ε une demi-période telle que $\vartheta(u^{(2)} - a^{(1)} \pm \varepsilon) \neq 0$, et prenons $\varepsilon, \bar{\varepsilon}, \ldots$ dans $\Pi, \bar{\Pi}, \ldots$. Il n'y a qu'un nombre fini de possibilités pour

$a^{(\nu)}, \bar{a}^{(\nu)}, \ldots, \varepsilon, \bar{\varepsilon}, \ldots$: à chacune correspond une valeur du facteur m_1, soit M_1 la plus grande de ces valeurs. De plus, $u^{(\nu+1)} - a^{(\nu)} \pm \varepsilon$, $\bar{u}^{(\nu+1)} - \bar{a}^{(\nu)} \pm \varepsilon, \ldots$ ne peuvent se trouver que dans des portions finies des espaces (u), $(\bar{u}), \ldots$: dans ces conditions, $A(u, \bar{u}, \ldots)$ admet une borne supérieure M_2. On a donc enfin:

$$[\Omega(u^{(\nu+1)})]^2 \leq M_1 M_2 \Omega(u^{(\nu)}).$$

Il en résulte que pour ν suffisamment grand, $\Omega(u^{(\nu)})$ sera inférieur à une constante, qui pourra être prise égale à $M_1 M_2 + 1$. Mais, $u, \bar{u}, \ldots$ étant dans $\Pi, \bar{\Pi}, \ldots$, $|\Theta(u)\bar{\Theta}(\bar{u})\ldots|^{\sigma}$ admet une borne supérieure M_3. Posons $L = M_3(M_1 M_2 + 1)$; on aura, pour ν suffisamment grand:

$$N\omega(u^{(\nu)}) \leq L$$

le nombre L ne dépendant que de la fonction Θ considérée.

Le raisonnement précédent est en défaut si l'un des nombres $\Theta(u^{(\nu)})$ s'annule, car alors $\omega(u^{(\nu)}) = 0$ et $\Omega(u^{(\nu)})$ est indéterminé. Mais il est aisé de combler cette lacune en sautant, pour ainsi dire, des échelons dans la descente de u à u', de u' à u'', ... Appelons $F_\nu(u)$ la fonction qui se déduit de $F(u)$ en y remplaçant a par $a^{(\nu)}$ et ε par une demi-période, située dans Π, telle que $\vartheta(u^{(\nu+1)} - a^{(\nu)} \pm \varepsilon) \neq 0$. Supposons alors, pour fixer les idées, que l'on ait $\Theta(u^{(\nu)}) \neq 0$, $\Theta(u^{(\nu+1)}) = 0$, $\Theta(u^{(\nu+2)}) \neq 0$: dans ce cas, au lieu de passer de $u^{(\nu)}$ à $u^{(\nu+1)}$ au moyen de $F_\nu(u)$, puis de $u^{(\nu+1)}$ à $u^{(\nu+2)}$ au moyen de $F_{\nu+1}(u)$, nous passerons directement de $u^{(\nu)}$ à $u^{(\nu+2)}$ au moyen de la fonction $F_{\nu+1}(u) \cdot F_\nu(2u - a^{(\nu+1)})$; en raisonnant sur elle comme nous avons fait plus haut sur $F(u)$, on arrive à l'inégalité $[\Omega(u^{(\nu+2)})]^4 \leq M_1^3 M_2^3 \Omega(u^{(\nu)})$, avec les mêmes quantités M_1 et M_2 que précédemment, ce qui conduit au même résultat.

19. Prenons pour $e_1, e_2, \ldots, e_P$ des entiers ordinaires (rationnels au sens absolu): nous avons démontré que si l'on pose $\Theta = \sum_{i=1}^{P} e_i \Theta_i$ et si $\omega(u)$ est la distribution correspondante, $N\omega(u^{(\nu)})$ est inférieur, pour ν assez grand, à une quantité déterminée qui ne dépend que des e_i. Soit en particulier $\omega_i(u)$ la distribution correspondant à Θ_i.

Soient $X_1^{(\nu)}, X_2^{(\nu)}, \ldots, X_P^{(\nu)}$ les coordonnées homogènes du point de V qui correspond à $u^{(\nu)}$; l'on a d'après le théorème de décomposition:

$$\frac{\sum_{i=1}^{P} e_i X_i^{(\nu)}}{X_i^{(\nu)}} = \frac{\Theta(u^{(\nu)})}{\Theta_i(u^{(\nu)})} = \frac{\lambda_i \omega(u^{(\nu)})}{\mu_i \omega_i(u^{(\nu)})}$$

λ_i et μ_i étant des idéaux bornés. Dans chaque classe d'idéaux de k choisissons un idéal a_k: $u^{(\nu)}$ étant rationnel, nous pouvons supposer que $X_1^{(\nu)}, X_2^{(\nu)}, \ldots, X_P^{(\nu)}$ sont des entiers de k et que leur pgcd est l'un des idéaux a_k, donc un idéal borné. Dans ces conditions, pour ν assez grand, $N\left(\sum_{i=1}^{P} e_i X_i^{(\nu)}\right)$ sera bornée, et cela quels que soient les e_i: mais, les e_i étant des entiers rationnels au sens ordinaire, cette norme est un polynôme homogène en $e_1, e_2, \ldots, e_P$, dont les coefficients sont des entiers ordinaires, pour ν assez grand, ce polynôme étant borné quelles que soient les valeurs attribuées aux variables e_i, ses coefficients seront eux-mêmes bornés et ne seront donc susceptibles que d un nombre fini de valeurs, de sorte que le polynôme $N\left(\sum_{i=1}^{P} e_i X_i^{(\nu)}\right)$ ne sera plus susceptible que d'un nombre fini de déterminations. Alors $\sum_{i=1}^{P} e_i X_i^{(\nu)}$, qui, en tant que forme linéaire en $e_1, e_2, \ldots, e_P$, est un diviseur de ce polynôme, n'est plus susceptible elle-même, à un facteur constant près, que d'un nombre fini de déterminations, ou, en d'autres termes, le point de coordonnées homogènes $X_1^{(\nu)}, X_2^{(\nu)}, \ldots, X_P^{(\nu)}$ n'est plus susceptible, pour ν assez grand, que d'un nombre fini de positions $b_1, b_2, \ldots, b_m$. Dans ces conditions, d'après le § 15, le théorème de la base finie est complètement démontré.

Conclusion.

20. Reprenons l'étude de la courbe C relativement au domaine de rationalité primitif k; et rappelons d'abord la notion, due à Severi, de systèmes virtuels (gruppi virtuali). g et g' étant deux systèmes, composés respectivement de m et de n points, sur C, le symbole $g-g'$ est appelé un *système virtuel* de degré $m-n$; deux systèmes virtuels $g-g'$ et $h-h'$ de même degré sont dits *équivalents*, et sont considérés comme identiques, si $g+h'$ est équivalent à $g'+h$; un système virtuel est dit *effectif* s'il est équivalent à un système de points au sens ordinaire

du mot; il résulte du théorème de Riemann-Roch que, sur la courbe C de genre p, tout système virtuel de degré $\geqslant p$ est effectif. $g-g'$ et $h-h'$ étant deux systèmes virtuels, de degrés respectifs μ et ν, ils ont pour somme le système virtuel $(g+h)-(g'+h')$, de degré $\mu+\nu$, et pour différence le système virtuel $(g+h')-(g'+h)$ de degré $\mu-\nu$.

Un système virtuel sera dit *rationnel* s'il est équivalent à un système virtuel $g-g'$ tel que g et g' soient deux systèmes rationnels. La somme et la différence de deux systèmes virtuels rationnels étant encore de tels systèmes, ces systèmes forment un groupe abélien $\mathfrak{G}$. Leurs degrés forment donc un module d'entiers rationnels, et sont tous multiples du degré ϱ d'un certain système virtuel rationnel A_0. ϱ est un invariant de C par les transformations birationnelles à coefficients rationnels relativement à k; c'est du reste un diviseur de $2p-2$, car le système des $2p-2$ zéros d'une différentielle de première espèce est toujours équivalent à un système rationnel. Si A est un système virtuel rationnel quelconque, son degré sera $k\varrho$, et $A-kA_0$ sera de degré 0.

Il reste à étudier les systèmes virtuels rationnels de degré 0, qui forment un sous-groupe $\mathfrak{g}$ de $\mathfrak{G}$. Soit K un surcorps de k relativement auquel il existe un système rationnel Γ de p points: d'après le chapitre II, il y a des systèmes de p points en nombre fini, $g_1, g_2, \ldots, g_n$, qui forment une base de l'ensemble des systèmes de p points rationnels relativement à K. Alors, si B est un système virtuel de degré 0, rationnel relativement à k, $\Gamma+B$ est un système de degré p, donc *effectif*, et rationnel relativement à K: il sera donc de la forme $\Gamma+\sum_1^n m_i(g_i-\Gamma)$, et par suite B est équivalent à $\sum_1^n m_i(g_i-\Gamma)$. $\mathfrak{g}$, faisant partie du groupe de base finie composé de tous les systèmes virtuels de la forme $\Sigma m_i(g_i-\Gamma)$, est lui-même de base finie. On sait alors, d'après la théorie des groupes abéliens, que l'on peut trouver des éléments $B_1, B_2, \ldots, B_r, C_1, C_2, \ldots, C_s$, tels que l'on obtienne tous les éléments du groupe une fois et une seule au moyen de l'expression $\sum_1^r m_i B_i + \sum_1^s n_j C_j$ en donnant aux m_i toutes les valeurs entières, et à n_j (pour $1 \leq j \leq s$) les valeurs $0, 1, 2, \ldots, \tau_j - 1$, les τ_j étant des entiers dont chacun divise le suivant; $r, \tau_1, \tau_2, \ldots, \tau_s$ sont les invariants du groupe: r est sa dimension, $\tau_1, \tau_2, \ldots, \tau_s$ sont ses nombres de Poincaré. Nous avons donc le résultat final que voici:

40—2822. *Acta mathematica.* 52. Imprimé le 5 novembre 1928.

Les systèmes virtuels de degré 0, *rationnels relativement à* k, *forment un groupe abélien* $\mathfrak{g}$ *de base finie: en adjoignant à une base de* $\mathfrak{g}$ *un certain système virtuel rationnel* A_0, *on obtient une base du groupe abélien* $\mathfrak{G}$ *formé par tous les systèmes virtuels rationnels relativement à* k. *Les invariants* $r, \tau_1, \tau_2, \ldots, \tau_s$ *du groupe* $\mathfrak{g}$, *ainsi que le degré* ϱ *du système* A_0, *sont des invariants de la courbe* C *par les transformations birationnelles à coefficients dans* k.

21. Nous avons ainsi démontré l'existence des invariants pour chaque domaine de rationalité k contenant les coefficients de C, donc d'une infinité d'invariants arithmétiques de C, puisque k peut être choisi d'une infinité de manières; il serait aisé, du reste, de définir d'autres invariants encore: si par exemple $\mathfrak{g}_k$ et $\mathfrak{g}_K$ désignent les groupes formés respectivement par les systèmes virtuels de degré 0 rationnels relativement à k et à un surcorps K de k, les invariants du groupe quotient $\mathfrak{g}_K \mathfrak{g}_k$ sont des invariants de C. Mais il serait sans doute difficile de déterminer les relations mutuelles de ces invariants, qui ne sont peut-être pas tous indépendants et de trouver quelles sont les valeurs qu'ils sont susceptibles de prendre. Il serait particulièrement intéressant de savoir si, lorsque le genre p et le domaine de rationalité k sont donnés, l'invariant r peut prendre des valeurs aussi grandes qu'on veut: ce problème n'a même pas été abordé jusqu'ici dans le cas le plus simple, celui où $p = 1$ et où k se compose des nombres rationnels au sens ordinaire.

Avant tout, il importerait de donner une méthode qui permît de déterminer dans chaque cas la valeur exacte des invariants et de trouver effectivement une base du groupe des systèmes virtuels rationnels: la démonstration du théorème de la base finie n'est en effet qu'une démonstration d'existence; elle permet bien, au moins théoriquement, de trouver dans chaque cas une limite supérieure de r, mais elle ne semble pas susceptible de rien fournir de plus.

Mais admettons même qu'on connaisse une base du groupe $\mathfrak{G}$: on peut alors considérer comme connu l'ensemble des systèmes virtuels rationnels, et par suite tous les systèmes rationnels de m points pour $m \geq p$, puisque tout système virtuel de degré $\geq p$ est nécessairement effectif. En revanche, un système virtuel de degré $\leq p-1$ n'est pas effectif en général, et, lorsqu'on connaît la base de $\mathfrak{G}$, c'est un problème très difficile que d'en déduire les systèmes rationnels de moins de p points, et en particulier les *points rationnels*, qui sont précisément ce que l'on recherche dans la résolution des équations diophantiennes. Le problème le plus important de la théorie est sans doute précisément de savoir si, parmi tous les systèmes virtuels de degré $\leq p-1$ qui se déduisent d'une base finie, il peut

s'en trouver une infinité d'effectifs: si la question devait être résolue par la négative, il s'ensuivrait en particulier que sur une courbe de genre $p > 1$ il n'y a qu'un nombre fini de points rationnels quel que soit le domaine de rationalité (par exemple l'équation de Fermat, $x^n + y^n = z^n$, n'aurait qu'un nombre fini de solutions pour chaque valeur de $n > 2$). Cette conjecture, déjà énoncée par Mordell (loc. cit. note [4]) semble confirmée en quelque mesure par un important résultat démontré récemment, et que je suis heureux de pouvoir citer ici grâce à l'obligeante permission de son auteur: «Sur toute courbe de genre $p > 0$, et quel que soit le corps k pris pour domaine de rationalité, il ne peut y avoir qu'un nombre fini de points dont les coordonnées soient des entiers de k».[14] Il est vrai que les points à coordonnées entières ne sont pas invariants par les transformations birationnelles, de sorte que ce résultat ne ressort pas de ce que nous avons appelé l'arithmétique sur les courbes algébriques et se distingue essentiellement des questions que nous avons essayé d'aborder ici.

[14] La démonstration repose d'une part sur l'application, convenablement effectuée, du théorème de la base finie démontré dans le présent travail, et d'autre part sur une extension nouvelle des méthodes d'approximation des nombres algébriques qui tirent leur origine des travaux de Axel Thue. Les théorèmes antérieurs de Thue et de Siegel sur les équations indéterminées ne sont que des cas particuliers du résultat général cité ici.