CLAUDE CHABAUTY

Sur les équations diophantiennes liées aux unités d'un corps de nombres algébriques fini

Thèses de l'entre-deux-guerres, 1938

<http://www.numdam.org/item?id=THESE_1938__208__123_0>

SÉRIE A, N.° 1815
N.° D'ORDRE 2681

THÈSES

PRÉSENTÉES

A LA FACULTÉ DES SCIENCES DE L'UNIVERSITÉ DE PARIS

POUR OBTENIR

LE GRADE DE DOCTEUR ÈS SCIENCES MATHÉMATIQUES

PAR

CLAUDE CHABAUTY

ANCIEN ÉLÈVE DE L'ÉCOLE NORMALE SUPÉRIEURE

AGRÉGÉ DE L'UNIVERSITÉ

1re THÈSE. - SUR LES ÉQUATIONS DIOPHANTIENNES LIÉES AUX UNITÉS D'UN CORPS DE NOMBRES ALGÉBRIQUES FINI

2e THÈSE. - PROPOSITIONS DONNÉES PAR LA FACULTÉ.

SOUTENUES LE 25 juin 1938 DEVANT LA COMMISSION D'EXAMEN

MM. E. CARTAN, Président

P. MONTEL, R. GARNIER } Examinateurs

FACULTÉ DES SCIENCE DE L'UNIVERSITÉ DE PARIS

MM.

Doyen honoraire . . . M. MOLLIARD.

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

Professeurs honoraires

H. LEBESGUE.	BLAISE.	G. BERTRAND.
A. FERNBACH.	DANGEARD.	ABRAHAM.
Émile PICARD.	LESPIEAU.	Ch. FABRY.
Léon BRILLOUIN.	MARCHIS.	Léon BERTRAND.
GUILLET.	VESSIOT.	WINTREBERT.
PECHARD.	PORTIER.	DUBOSCQ.
FREUNDLER.	MOLLIARD.	BOHN.
AUGER.	LAPICQUE.	

PROFESSEURS

M. CAULLERY . . .	T	Zoologie (Évolution des êtres organisés).
G. URBAIN	T	Chimie générale.
Émile BOREL . . .	T	Calcul des probabilités et Physique mathématique.
Jean PERRIN . . .	T	Chimie physique.
E. CARTAN	T	Géométrie supérieure.
A. COTTON	T	Recherches physiques.
J. DRACH	T	Analyse supérieure et Algèbre supérieure.
Charles PÉREZ . .	T	Zoologie.
E. RABAUD	T	Biologie expérimentale.
M. GUICHARD . . .		Chimie minérale.
Paul MONTEL . . .	T	Théorie des fonctions et Théorie des transformations.
L. BLARINGHEM .	T	Botanique.
G. JULIA	T	Mécanique analytique et Mécanique céleste.
C. MAUGUIN	T	Minéralogie.
A. MICHEL-LÉVY .	T	Pétrographie.
H. BÉNARD	T	Mécanique expérimentale des fluides.
A. DENJOY	T	Application de l'analyse à la Géométrie.
L. LUTAUD	T	Géographie physique et géologie dynamique.
Eugène BLOCH . .	T	Physique.
G. BRUHAT	T	Physique.
E. DARMOIS	T	Enseignement de Physique.
A. DEBIERNE . . .	T	Physique Générale et Radioactivité.
A. DUFOUR	T	Physique (P. C. B.).
L. DUNOYER		Optique appliquée.
A. GUILLIERMOND	T	Botanique.
M. JAVILLIER . . .	T	Chimie biologique.
L. JOLEAUD		Paléontologie.
ROBERT-LÉVY . . .	T	Physiologie comparée.
F. PICARD		Zoologie (Évolution des êtres organisés).
Henri VILLAT . .	T	Mécanique des fluides et applications.
Ch. JACOB	T	Géologie.
P. PASCAL	T	Chimie minérale.
M. FRÉCHET . . .	T	Calcul différentiel et Calcul intégral.
F. ESCLANGON . .	T	Astronomie.
M. RAMART-LUCAS	T	Chimie organique.
H. BÉGHIN	T	Mécanique physique et expérimentale.
FOCH		Mécanique expérimentale des fluides.
PAUTHENIER		Physique (P. C. B.)
De BROGLIE . . .	T	Théories physiques.
CHRÉTIEN		Optique appliquée.
P. JOB		Chimie générale.
LABROUSTE		Physique du Globe.
PRENANT	T	Anatomie et Histologie comparées.
VILLEY		Mécanique physique et expérimentale
COMBES	T	Physiologie végétale.
GARNIER	T	Mathématiques générales.
PERES		Mécanique théor. des fluides.
HACKSPILL		Chimie (P. C. B.).
LAUGIER	T	Physiologie générale.
TOUSSAINT		Technique Aéronautique.
M. CURIE		Physique (P. C. B.).
G. RIBAUD	T	Hautes températures.
CHAZY	T	Mécanique rationelle.
GAULT		Chimie (P. C. B.).
CROZE		Recherches physiques.
DUPONT	T	Théories chimiques.
LANQUINE	T	Géologie structurale et Géologie appliquée.
VALIRON		Mathématiques générales.
BARRABÉ		Géologie structurale et géologie appliquée.
MILLOT		Biologie animale (P. C. B).
F. PERRIN		Théories physiques.
VAVON		Chimie organique.
G. DARMOIS		Calcul des probabilités et Physique-Mathématique.
CHATTON	T	Biologie maritime.
AUBEL		Chimie biologique.
Jacques BOURCART .		Géographie physique et Géologie dynamique.
M.me JOLIOT-CURIE		Physique générale et Radioactivité.
PLANTEFOL		Biologie végétale (P. C. B.).
CABANNES		Enseignement de Physique.
GRASSE		Biologie animale (P. C. B.).
PREVOST		Chimie (P. C. B.).

Secrétaire . . . . . A. PACAUD.

Secrétaire honoraire . . . . . D. TOMBECK.

Hommage amical

E Labauty

Sur les équations diophantiennes liées aux unités d'un corps de nombres algébriques fini.

Par CLAUDE CHABAUTY (à Paris).

Introduction.

Soit à résoudre en entiers rationnels X_i l'équation

$$\text{Norme}\,(X_1\omega_1 + \ldots + X_n\omega_n) = \pm 1 \tag{1}$$

où les ω_i forment une base des entiers d'un corps de nombres algébriques K de degré n (1). A une telle solution correspond une unité $\varepsilon = X_1\omega_1 + \ldots + X_n\omega_n$ de K, et réciproquement les composantes d'une unité de K, par rapport à la base considérée, fournissent une solution de (1) en entiers rationnels. L'existence et la structure des solutions nous sont donc données par le théorème de DIRICHLET: Les unités de K forment, par rapport à la multiplication, un groupe abélien Γ admettant une base minima formée de r éléments d'ordre infini et d'un élément d'ordre fini, et l'on a $r = r_1 + r_2 - 1$, r_1 désignant le nombre de corps réels, $2r_2$ le nombre de corps complexes, parmi les n corps conjugués de K. Nous appellerons r le nombre de DIRICHLET de K.

Le résultat classique de THUE (2) sur les solutions en entiers rationnels d'une équation $F(X, Y) = 1$ où F est une forme homogène à coefficients rationnels, peut s'interpréter comme suit: S'il y a une infinité d'unités dans un module de dimension 2 de nombres de K, les unités contenues dans ce module sont toutes les unités d'un sous-corps quadratique réel de K, multipliées par une unité fixe de K.

Plus généralement, on peut se proposer d'étudier des conditions de possibilité à l'existence d'une infinité de solutions en entiers rationnels à l'équation (1) à laquelle on adjoint un certain nombre d'équations algébriques

$$F_j(X_1, \ldots, X_n) = 0 \qquad j = 1, 2, \ldots, h \tag{2}$$

(1) Après les expressions: « degré, ou corps conjugués d'un corps de nombres algébriques », « module », nous supposons toujours qu'il est sous-entendu « par rapport au corps R des nombres rationnels ».

(2) A. THUE, « Journ. für Math. », Bd. 135 (1909).

dont nous pouvons, sans restreindre la généralité du problème, supposer les coefficients rationnels. (Le cas envisagé par THUE correspond à un système (2) formé de $n-2$ équations linéaires, homogènes, indépendantes, sur les X_i).

On obtient facilement des conditions suffisantes assez larges, que doit remplir le système d'équations (1), (2), pour qu'il ait une infinité de solutions en entiers rationnels X_i. Alors l'ensemble des unités de K qui correspondent à ces solution, a une structure assez simple: A condition de négliger peut-être un nombre fini d'entre elles, il est constitué par la réunion des éléments d'un nombre fini de sous-groupes de Γ ou de classes de Γ par rapport à des sous-groupes. On peut conjecturer que ces conditions suffisantes sont aussi nécessaires, et que les solutions du système ont toujours cette structure. C'est ce que confirme le résultat de THUE qui donne une condition nécessaire et suffisante à l'existence d'une infinité d'unités dans un module de dimension 2, et le résultat analogue que nous établirons dans ce travail pour certains modules de dimension 3. Mais rien de pareil n'est démontré dans des cas plus généraux, et l'on obtient des conditions nécessaires qui ne sont pas suffisantes.

Les résultats antérieurs à ce travail, autres que ceux de THUE, concernent encore le cas où (2) est un système d'équations linéaires et homogènes. En approfondissant les méthodes d'approximation diophantiennes de THUE, C. SIEGEL a montré ([3]) que dans un module de base 1, ω, ω', ..., ω^{s-1} du corps $K=R[\omega]$ de degré n, il n'y a qu'un nombre fini d'unités quand s ést suffisamment petit par rapport à n ($n>4s^4-2s^2+1$). En se servant d'une métrique p-adique convenable, T. SKOLEM ([4]) a montré que pour un corps de degré 5 ayant 4 corps conjugués imaginaires, il n'y a qu'un nombre fini d'unités dans un module de dimension 3.

Les résultats de ce travail concernent le cas suivant: les équations du système (2) sont en général de degré quelconque, mais la variété algébrique W définie dans l'espace de $X_1, \ldots, X_n$ par les équations (1) et (2) est supposée formée de composantes irréductibles de dimension $s \leq n-r-1$, r étant toujours le nombre de DIRICHLET de K. Le résultat central est le suivant:

A tout ensemble & d'une infinité d'unités de K *appartenant à une variété algébrique* W *de dimension* s *correspond au moins un sous-groupe* γ *de* Γ *ayant les propriétés suivantes:*

([3]) C. SIEGEL, « Math. Zeit. », Bd. 10 (1921).
([4]) T. SKOLEM, « Math. Annal », Bd. 111 (1936).

1°) *Il y a au moins une classe de* Γ/γ *qui contient un sous-ensemble infini de* $\mathfrak{E}$.

2°) *Entre* $\sigma = r + s - 1$ *quelconques des conjugués d'une unité* ε *appartenant à* γ, *soient* $\varepsilon^{(q_1)}, \ldots, \varepsilon^{(q_\sigma)}$, *il y a une relation*

$$\varepsilon^{(q_1)m_{q_1}} \ldots \varepsilon^{(q_\sigma)m_{q_\sigma}} = 1 \tag{3}$$

les exposants $m_{q_1}, \ldots, m_{q_\sigma}$ *étant des entiers rationnels non tous nuls, ne dépendant que du choix des conjugués, mais non du choix de* ε *dans* γ.

Nous donnons deux types d'applications de ce théorème, en examinant la compatibilité des équations (3) avec la nature du groupe de GALOIS G de K, ou avec la nature de la variété W. Nous obtenons ainsi les résultats suivants:

1.° *Pour toute une catégorie de corps de nombres algébriques finis, qui contient en particulier tous les corps de degré premier, et tous les corps dont le groupe de Galois est le groupe symétrique, il ne peut y avoir une infinité d'unités appartenant à une variété algébrique de dimension* $\leq n - r - 1$.

2.° *L'existence d'une infinité d'unités dans un module de nombres algébriques de base* $(1, \alpha, \beta)$, *où le corps* $K = R[\alpha, \beta]$ *a au moins* 4 *corps conjugués complexes, admet une condition nécessaire et suffisante analogue à celle trouvée par* THUE *pour les modules de dimension* 2, *à savoir que le module considéré contienne le module des nombres d'un certain sous-corps de* K.

Nous en déduisons que *l'inégalité*

$$|X + Y\alpha + Z\beta| \leq \frac{c}{(|X| + |Y| + |Z|)^{n-1}}$$

où n *est le degré de* $K = R[\alpha, \beta]$, *toujours assujetti à avoir au moins* 4 *conjugués imaginaires, n'a qu'un nombre fini de solutions en entiers rationnels* X, Y, Z, *quelle que soit la constante réelle positive* c.

Le chapitre I est consacré à l'étude des variétés algébroïdes dans un espace où les points sont des systèmes de n nombres pris dans un corps p-adique algébriquement fermé. Nous démontrons principalement que ces variétés sont localement décomposables en variétés irréductibles, et que chaque élément irréductible est susceptible d'une représentation paramétrique locale de « WEIERSTRASS », le nombre de paramètres indépendants définissant la dimension de l'élément.

Dans le chapitre II, nous considérons un « groupe abélien multiplicatif de points » de X^n, Γ, de « rang » r, $r \leq n - 1$, dont les points de base ont pour coordonnées des nombres algébriques. Nous supposons qu'une variété algébrique W de X^n de dimension $s \leq n - r$ contienne un ensemble

infini $\mathfrak{S}$ d'éléments de Γ. Nous étudions les relations entre W et Γ par l'intermédiaire de sous-variétés algébriques de W et de sous-groupes de Γ « minimaux » par rapport à l'ensemble $\mathfrak{S}$. Nous utilisons des transformations de l'espace X^n (congruences) et des procédés de composition de variété (produits de variétés). Ils nous permettent de construire dans X^n une variété algébrique $\widehat{W}$ de dimension $\leq s+r-1$ contenant tous les éléments d'un sous-groupe convenablement choisi de Γ. Il en résulte un théorème analogue au théorème (3.1).

Dans le chapitre III, nous supposons que le groupe Γ est le groupe des points ayant pour coordonnées une unité de K et ses conjuguées, le théorème précédent donne alors le théorème (3.1). Nous en faisons ensuite les applications mentionnées plus haut à des équations diophantiennes particulières.

Une partie de ces résultats a été résumée dans trois notes aux « Comptes Rendus de l'Académie des Sciences de Paris » (5).

Monsieur GARNIER m'a donné de précieux conseils durant la rédaction de ce travail. Je suis heurex de l'en remercier.

CHAPITRE I. - Séries entières à coefficients p-adiques.

Corps p-adiques. — Rappelons quelques définitions et propriétés des corps p-adiques qui nous seront utiles par la suite (6).

Soit R le corps des nombres rationnels, p un nombre naturel premier. Tout nombre q de R peut se mettre sous la forme $q=p^\lambda q'$, où λ est un entier rationnel, q' un nombre de R égal au quotient de deux entiers de R premiers entre eux, dont aucun n'est multiple de p; p^λ s'appelle la participation de p à q, λ l'ordre de q (pour p). On appelle *valeur absolue* p-*adique de* q, que l'on notera $|q|_p$, le nombre réel $\left(\frac{1}{p}\right)^\lambda$ quand $q\neq 0$. On pose $|0|_p=0$. On a:

$$(1)\quad \begin{cases} |q_1\cdot q_2|_p=|q_1|_p\cdot|q_2|_p \\ |q_1+q_2|_p=\operatorname{Max}(|q_1|_p,\ |q_2|_p) \end{cases} \qquad (2)\quad \begin{cases} \lambda(q_1\cdot q_2)=\lambda(q_1)+\lambda(q_2) \\ \lambda(q_1+q_2)=\operatorname{Min}(\lambda(q_1),\ \lambda(q_2)). \end{cases}$$

Si l'on prend comme distance de deux éléments q_1, q_2 de R, $|q_2-q_1|_p$, R devient un espace métrique. Sa fermeture topologique R_p s'appelle *le corps*

(5) « C. R. », t. 202, p. 2117, Juin 1936; t. 204, p. 942, Mars 1937; t. 205, p. 943, Novembre 1937.

(6) Pour leur démonstration, Cf. CHEVALLEY, « Thèse «, Paris, 1933, *Sur la théorie du corps de classe*, chap. V, p. 407-423, et « Journ. of the faculty of sciences », Tokyo, 1933.

des nombres rationnels p-*adiques*. La valeur absolue p-adique définie dans R induit une valeur absolue p-adique dans R_p.

On sait (7) que pour tout corps on peut former *des extensions algébriquement fermées* (c. à. d. dans laquelle tout polynôme d'une variable à coefficients dans le premier corps se décompose en un produit de facteurs linéaires) qui soient algébriques sur ce corps, et de telles extensions sont équivalentes. Soit H_p l'une d'elle. Soit q un élément de H_p, $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ l'équation irréductible à coefficients dans R_p à laquelle satisfait q, μ l'ordre de la norme a_n de q, on démontre que la valeur absolue $|q|_p = \left(\frac{1}{p}\right)^{\frac{\mu}{n}}$ est un prolongement de la valeur absolue définie dans R_p et elle satisfait encore aux relations (1). Nous appellerons $\lambda = \frac{\mu}{n}$ l'ordre de q, il satisfait aux relations (2).

Les nombres de H_p d'ordre ≥ 0 sont dits *entiers* p-*adiques*. Ils forment un anneau E_p dans H_p. Ceux d'ordre nul ont aussi leurs inverses dans E_p; ils sont dits *unités* p-*adiques*. Ils forment un groupe abélien multiplicatif. Les entiers et les unités algébriques sont des entiers et unités p-adiques.

La valeur absolue p-adique fait du corps H_p un espace métrique, mais il n'est plus complet, comme l'était R_p (une suite de nombres de H_p, convergente au sens de CAUCHY, n'a pas nécessairement une limite dans H_p). Les relations (1) entraînent:

THÉORÈME 1.1. — *La condition nécessaire et suffisante pour qu'une suite* a_n *d'éléments de* H_p *soit convergente au sens de Cauchy, est que* $\lim_{n=\infty} (a_{n+1} - a_n) = 0$.

Soit K_p un sous-corps de H_p qui soit une extension algébrique finie de R_p. Il y a (6) dans K_p un nombre π, entier p-adique, qui n'est pas une unité p-adique et dont l'ordre est minimal. L'ordre de tout nombre de K_p est un multiple de celui de π, de sorte que tout nombre de K_p peut se mettre sous la forme $\pi^\mu u$, μ entier rationnel, u une unité p-adique de K_p. Les seuls idéaux de l'anneau des entiers de K_p sont les idéaux $(\pi)^m$, le seul idéal premier est (π). En particulier (p) est un idéal de la forme $(\pi)^e$. Le nombre de classes de restes de l'anneau des entiers de K_p par rapport à l'idéal (π), est un nombre fini p^f. Cela permet de démontrer que K_p est localement compact (de toute suite infinie d'éléments bornés de K_p on peut extraire une suite convergente au sens de CAUCHY).

(7) Cf. Van der WAERDEN, *Moderne Algebra*, Bd. 1, § 60.

On démontre aussi ([6]) que K_p peut être obtenu en adjoignant à R_p un nombre θ, algébrique sur R, et que K_p est la fermeture topologique de $K = R[\theta]$ pour la valeur absolue p-adique. Donc K_p est complet et les suites convergentes qu'on peut extraire d'une suite infinie d'éléments bornés de K_p convergent vers un élément de K_p. C'est la propriété de compacité en soi. *Tout sous-corps de* $\mathrm{H_p}$ *qui est une extension algébrique finie de* $\mathrm{R_p}$ *est localement compact en soi.*

Séries à coefficients p-adiques. — Dans la suite, nous considérerons des systèmes de n valeurs $x_1, \ldots, x_n$, prises dans H_p comme un point d'un espace X^n, produit direct de n espaces H_p. La métrique p-adique definie dans H_p, induit dans X^n une topologie qu'on peut engendrer par la métrique $Dist\,(A_1A_2) = \sum_{i=1}^{n} |a_{2i} - a_{1i}|_p$, par exemple. Nous appellerons *voisinage d'un* point Q de X^n un domaine de X^n contenant pour certaines valeurs des nombres réels positifs m_2 tous les points tels que

$$|x_i - x_{iQ}|_p \leq m_i \qquad (i = 1, 2, \ldots, n).$$

Nous considérerons des séries de puissances entières rationnelles positives de n variables $x_1, \ldots, x_n$

$$A = \sum_{h_1, \ldots, h_n} a_{h_1 \ldots h_n} x_1^{h_1} \ldots x_n^{h_n}$$

où nous supposerons que les coefficients appartiennent à une même extension algébrique finie $\mathrm{K_p}$ *de* $\mathrm{R_p}$, de sorte que si la série converge quand on substitue aux x_i des valeurs x_i^0 de H_p, elle converge vers un nombre du corps topologiquement complet $K_p[x_1^0, \ldots, x_n^0]$. Par définition, une *fonction analytique* de n variables $x_1, \ldots, x_n$ est la somme d'une telle série dans son domaine de convergence.

Appelons *hauteur* d'un terme de la série le nombre naturel $h = h_1 + \ldots + h_n$. D'après le théorème (1.1), on a:

THÉORÈME 1.2. — *La condition nécessaire et suffisante pour qu'une série multiple* $\sum_{h_1, \ldots, h_n} b_{h_1, \ldots, h_n}$ $(h_1, \ldots, h_n = 0, 1, 2, \ldots, +\infty)$ *converge, est que la valeur absolue du terme général tende vers zéro quand* h *croit indéfiniment.*

Ce théorème donne pour la convergence des séries une condition beaucoup plus large qu'en analyse ordinaire. Aussi dès qu'une série à coefficients p-adiques est convergente, elle aura des propriétés qui en analyse ordinaire, caractérisent les séries absolument convergentes. En effet, du théorème (1.2)

résulte que: toute série extraite d'une série p-adique convergente A, est elle-même convergente. Soit une suite de telles séries partielles A_n. Soit h_n la plus petite hauteur des termes de A figurant dans A_n, si h_n croit indéfiniment avec n alors $|A_n|_p$ tend vers zéro. Donc:

THÉORÈME 1.3. — *Si on somme les termes d'une série convergente par un procédé quelconque qui épuise tous les termes de la série, on obtient la même limite qu'avec le procédé qui définit la série* (8).

Du théorème (1.2) résulte aussi que *si une série entière à* n *variables est convergente pour* $x_i = b_i$ *elle converge uniformément pour tout le domaine* $|x_i|_p \leq |b_i|_p$. Si tous les b_i sont $\neq 0$, nous appellerons un tel domaine un *cube de convergence.*

Si une suite de points Q de X^n tend vers le point Q_0 de coordonnées x_{i0}, on finit par avoir $|x_i|_p = |x_{i0}|_p$ pour les valeurs de l'indice i telles que $x_{i0} \neq 0$; il en résulte que si une série entière converge pour une suite de points de l'espace des variables, elle converge pour tous les points limites de la suite,

On démontre aisément que *si la somme d'une série entière est nulle dans tout un voisinage de l'origine, la série est identiquement nulle, c. a. d. tous ses coefficients sont nuls.*

THÉORÈME 1.4. — *Si une série entière* $f(x_1, \ldots, x_n)$ *converge au voisinage de l'origine, si l'on fait le changement de coordonnées* $(x_i \to a_i + y_i)$, a_i *étant un point où* f *converge, et si l'on ordonne la série obtenue par rapport aux puissances des* y_i, *on obtient une série entière* $\varphi_a(y_1, \ldots, y_n)$ *qui a même domaine de convergence que* f, *et même somme que* f *aux mêmes points.* (Il n'y a donc pas de prolongement analytique).

En effet, considérons la série entière à $2n$ variables $F(x_1, \ldots, x_n, y_1, \ldots, y_n)$, obtenue en substituant dans f, $x_i + y_i$ à x_i. Si f admet le cube de convergence $|x_i|_p = |p^{m_i}|_p$, faisons le changement de variables $x_i' = x_i/p^{m_i}$, $y_i' = y_i/p^{m_i}$. Appelons f', φ', F', les fonctions correspondantes. Comme f' converge pour $|x_i'|_p = 1$, le valeur absolue p-adique de ses coefficients tend vers 0 quand la hauteur de leur indice croit indéfiniment. Comme chacun des coefficients de F' est égal à un coefficient de f' multiplié par un entier rationnel, ils ont aussi cette propriété, et F' admet le cube $|x_i|_p \leq 1$,

(8) Le théorème (1.3) est valable plus généralement pour toute série d'éléments d'un espace vectoriel normé quelconque lorsque la série est *commutativement convergente* c. a. d. qu'elle reste convergente après un changement quelconque de l'ordre de ses termes (cf. BANACH, *Opérations linéaires*, p. 240). Les séries p-adiques sont un exemple de séries qui peuvent être commutativement convergentes sans être absolument convergentes.

$|y_i|_p \leq 1$ comme cube de convergence. Puisque pour un système de valeurs a_i', b_i', des x_i', y_i' en valeur absolue ≤ 1 la valeur de f s'obtient en sommant les termes de la série convergente $F'(a_i'; b_i')$ suivant une loi qui les épuise tous, il résulte du théorème (1.3) que $f'(a_i' + b_i') = F'(a_i'; b_i')$. Mais le même théorème montre que $\varphi_a'(b_i')$ converge alors vers la même valeur. Donc, dans tout domaine où f converge, φ converge vers la même valeur, et réciproquement puisque f et φ jouent un rôle symétrique.

On déduit facilement du théorème (1.4):

THÉORÈME 1.5. — *Si une série entière est identiquement nulle, dans tout un voisinage d'un point du domaine de convergence, elle est identiquement nulle.*

REMARQUE. — Ayant défini comme en analyse ordinaire, les dérivées partielles d'un polynôme en $x_1, \ldots, x_n$ par rapport aux différentes variables, et celles d'une série entière $f(x_1, \ldots, x_n)$ comme obtenues par la dérivation terme à terme, on voit facilement que si f converge dans le cube $|x_i|_p = |a_i|_p$ ses dérivées convergent aussi dans le même cube. On a donc l'interprétation des coefficients du développement de f, et du développement de $\varphi_a(y_1, \ldots, y_n) \equiv \equiv f(a_1 + y_1, \ldots, a_n + y_n)$ par les formules de MAC-LAURIN et TAYLOR

$$\varphi_a = \sum_{h_1, \ldots, h_n} b_{h_1, \ldots, h_n} y_1^{h_1} \ldots y_n^{h_n} = \sum_n \frac{1}{n!} \left\| y_1 \frac{\partial f}{\partial x_1} + \ldots + y_n \frac{\partial f}{\partial x_n} \right\|^n.$$

On démontre de même à l'aide du théorème (1.2) l'analyticité d'une fonction analytique de fonctions analytiques:

THÉORÈME 1.6. — *Soient* A *une série entière de* n *variables* $x_1, \ldots, x_n$, *convergente dans un voisinage* D *de* $x_1 = \ldots = x_n = 0$; $B_1, \ldots, B_n$ *des séries entières de* m *variables,* $y_1, \ldots, y_m$ *convergentes dans un voisinage* D' *de* $y_1 = \ldots = y_m = 0$, *nulles pour* $y_1 = \ldots = y_m = 0$; *si nous effectuons dans* A *la substitution* $x_i = B_i$, $i = 1, 2, \ldots, n$, *on obtient une série entière* A' *en* y_i *qui converge pour tous les systèmes de valeurs des* y_i *de* D' *qui donnent des systèmes de valeurs des* x *appartenant à* D.

Et le théorème:

THÉORÈME 1.7. — *Soient* $A_1, \ldots, A_r$ *des séries entières de* n *variables* $x_1, \ldots, x_n$, *convergentes dans un voisinage de* $x_1 = \ldots = x_n = 0$, *telles que la matrice à* r *lignes et* n *colonnes* $\left\| \frac{\partial A_i}{\partial x_j} \right\|$ *soit de rang* r *pour* $x_1 = \ldots = x_n = 0$. *Soient* $B_1, \ldots, B_n$, n *séries entières de* n *variables* $y_1, \ldots, y_n$, *convergentes au voisinage de* $y_1 = \ldots = y_n = 0$, *telles que la matrice à* n *lignes et* n *colonnes* $\left\| \frac{\partial B_i}{\partial x_j} \right\|$ *soit de rang* n *pour* $y_1 = \ldots = y_n = 0$. *Effectuons dans les* A *la*

substitution $x_i = B_i$, $i = 1, 2, \ldots, n$, *les* A *deviennent des fonctions des* y *telles que la matrice à* r *lignes et* n *colonnes* $\left\| \frac{\partial A_i}{\partial y_j} \right\|$ *soit de rang* r *pour* $y_1 = \ldots = y_n = 0$.

Idéaux de séries entières convergentes. — Considérons toutes les séries entières de n variables $x_1, \ldots, x_n$ à coefficients dans H_p

$$A = \sum_{h_1,\ldots,h_n} a_{h_1,\ldots,h_n} x_1^{h_1} \ldots x_n^{h_n} \qquad (h_1,\ldots,h_n = 0, 1, 2, \ldots, +\infty($$

satisfaisant aux conditions suivantes: chacune d'elles est convergente dans un voisinage de l'origine et ses coefficients sont dans une même extension algébrique finie de R_p. Elles forment un anneau d'intégrité U_n.

Pour l'anneau analogue dans les séries dont les coefficients sont des nombres complexes ordinaires, il y a des théorèmes classiques renseignant sur la structure des idéaux et des variétés des zéros de ces idéaux. Les mêmes problèmes se posent pour U_n. Nous y trouverons des réponses analogues, principalement: le résultat que pour la variété des zéros d'un idéal premier, il y a une représentation paramétrique de « WEIERSTRASS ». Pour les obtenir, nous démontrerons entre éléments de U_n une identité connue dans le cas classique sous le nom de formule de WEIERSTRASS. Nous référerons pour le détail des démonstrations de ses conséquences à un mémoire de W. RUCKERT (9), (mémoire désigné dans la suite par W. R.), car elles en sont déduites par des procédés purement algébriques, valables encore dans le cas que nous considérons.

Donnons quelques définitions préalables. Un élément de U_n sera dit *unité* quand il existe un élément B de U_n tel que $AB = 1$. Alors, on a nécessairement $A(0, \ldots, 0) \neq 0$. L'identité $(1-a)^{-1} = \sum_{n=0}^{\infty} a^n$ et une majoration facile permettent de démontrer que cette condition est suffisante pour que A soit une unité. Deux éléments A, B de U_n seront dits *équivalents* s'il existe une unité C de U_n telle que $A = BC$.

Si $A(0, \ldots, 0, x_n) \neq 0$, A sera dit *régulier en* x_n de degré s, s étant la plus petite puissance de x_n à coefficient non nul dans $A(0, \ldots, 0, x_n)$. Par un changement de coordonnées, portant seulement sur $x_1, \ldots, x_{n-1}$, on peut toujours amener un élément A à être régulier en x_n

Si A est un polynôme en x_n, à coefficients non unités de U_{n-1} (anneau analogue à U_n pour les séries entières en $x_1, \ldots, x_{n-1}$), à l'exception du terme

(9) W. RUCKERT, « Math. Annal. », Bd. 107 (1932), p. 259-281.

de plus haut degré x_n^s dont le coefficient est 1, A est dit un *polynôme distingué* en x_n de degré s.

Démontrons alors la

FORMULE DE WEIERSTRASS. — *Soit* F *un élément de* U_n, *régulier en* x_n *de degré* s, *à tout élément* A *de* U_n *correspondent les éléments* B *et* C *de* U_n. C *étant en* x_n *un polynome de degré* $\leq s-1$, *tels que l'on ait identiquement* $A = FB + C$.

Prenons un voisinage de zéro $|x_i|_p \leq |\lambda|_p$ suffisamment petit pour que A et F y convergent tous deux. Par un changement de variables $x_i' = \frac{x_i}{\lambda}$ $i = 1, \ldots, n$, A et F donnent deux séries que nous continuons à appeler A et F, convergentes pour $|x_i'|_p = 1$, dont les coefficients ont une valeur absolue p-adique qui tend vers zéro avec l'inverse de la hauteur de leur indice. Par une changement de variables $x_n'' = \frac{x_n'}{\lambda'}$ avec $|\lambda'|_p$ suffisamment petit, nous obtenons que le coefficient de $x_n'^s$ dans F soit le plus grand de ces coefficients des pures puissances de x_n, et en faisant ensuite $x_i'' = \frac{x_i'}{\lambda''}$ $(i = 1, \ldots, n-1)$, avec $|\lambda''|_p$ assez petit, nous obtenons que ce coefficient soit le plus grand de tous les coefficients dans F.

Dans le corps K_p algébrique fini sur R_p, qui contient les coefficients de F et A on peut trouver un nombre π tel que tout nombre a du corps, se mette sous la forme $a = \pi^h \varepsilon$, ε étant une unité p-adique du corps, c'est-à-dire un nombre d'ordre zéro. Comme les coefficients de F et G tendent vers zéro quand la hauteur de leur indice croit indéfiniment, il n'y en a qu'un nombre fini de même ordre, on peut donc écrire:

$$A = \pi^h(g_0 + \pi g_1 + \ldots + \pi^q g_q + \ldots)$$

les g_i étant des polynômes en $x_1, \ldots, x_n$ à coefficients unités de K_p, de même pour F, avec cette remarque que f_0 se réduit à $\varepsilon_0 x_n^s$

$$F = \pi^{h'}(\varepsilon_0 x_n^s + \pi f_1 + \ldots + \pi^q f_q + \ldots).$$

Nous pouvons supposer $h = h' = 0$, $\varepsilon_0 = 1$, car nous ne considérons pas comme différents deux éléments de U_n dont le quotient est une constante.

Considérons des éléments de U_n, B, C:

$$B = \sum_{q=0}^{+\infty} \pi^q b_q \qquad C = \sum_{q=0}^{+\infty} \pi^q c_q$$

b_q et c_q étant des éléments de U_n à déterminer. L'identité $A = FB + C$ est

équivalente au système de l'infinité de congruences $A \equiv FB + C \pmod{\pi^q}$ ($q = 1, 2, \ldots$ à l'infini). Ce système est satisfait s'il en est de même pour le système d'une infinité d'égalités:

$$(q) \qquad a_q = x_n^s b_q + f_1 b_{q-1} + \ldots + f_q b_0 + c_q$$

obtenu en égalant les coefficients des différentes puissances de π.

Supposons qu'on ait pu, pour $q = 0, 1, \ldots, h-1$, déterminer des éléments de U_n, b_q, c_q, qui satisfassent aux égalités d'indices (0), (1), ..., $(h-1)$, et qui soient des polynômes en $x_1, \ldots, x_n$, à coefficients d'ordre ≥ 0, les c_q de degré $\leq s-1$ en x_n. Alors, posant $d_h = a_q - x_n^s b_q - \ldots - f_q b_0$, d_h est encore un polynome en $x_1, \ldots, x_n$ à coefficients d'ordre ≥ 0. La relation (q) s'écrit, pour $q = h$:

$$(h) \qquad d_h = x_n^s b_h + c_h$$

d_h est connu. Si on prend pour b_h, c_h, respectivement le quotient et le reste de la division de d_h suivant les puissances décroissantes de x_n par x_n^s, l'égalité (h) est satisfaite et b_h et c_h sont des polynomes en $x_1, \ldots, x_n$ à coefficients d'ordre ≥ 0, c_h étant de degré $\leq s-1$ en x_n. Nous formons donc ainsi par récurrence tous les polynômes b_q, c_q.

Dans $\sum_{q=0}^{+\infty} \pi^q b_q$ développé suivant les monômes en $x_1, \ldots, x_n$, le coefficient du monôme $x_1^{r_1} \ldots x_n^{r_n}$ est égal à $\sum_{q=0}^{+\infty} \varepsilon_{r_1, \ldots, r_n, q}\, \pi^q$, $\varepsilon_{r_1, \ldots, r_n, q}$ étant le coefficient de $x_1^{r_1} \ldots x_n^{r_n}$ dans b_q, coefficient qui est d'ordre ≥ 0, le terme général de cette série tend vers 0 et c'est toujours un nombre de K_p, cette série converge vers une limite $b_{r_1, \ldots, r_n}$ de K_p d'ordre ≥ 0, donc $B = \sum_{r_1, \ldots, r_n} b_{r_1, \ldots, r_n} x_1^{r_1} \ldots x_n^{r_n}$ converge pour $|x_i|_p = 1$ et tous ses coefficients appartiennent à K_p. B est donc un élément de U_n. De même C, qui en outre, est un polynome en x_n de degré $\leq s-1$. Et ils satisfont bien à l'identité $A = FB + C$. On a donc trouvé les éléments cherchés.

APPLICATIONS. — Prenons $A = x_n^s$. A F correspond un élément B tel que $FB = A - C$ soit un polynome en x_n à coefficient dans U_{n-1}, dont le terme de degré la plus élevé est x_n^s. On montre facilement que B est une unité de U_n, que $A - C$ est un polynome distingué en x_n et qu'il est uniquement déterminé (Cf. W. R., p. 262). On a donc le

LEMME DE WEIERSTRASS [10]. — *Tout élément de* U_n, *régulier en* x_n, *de*

[10] Voir pour une démonstration directe Th. SKOLEM, « Math. Ann. », 111, 1936, p. 399. Mais le lemme de WEIERSTRASS ne nous suffirait pas pour obtenir la représentation paramétrique dont nous avons besoin pour des variétés algébroïdes.

degré s, *est équivalent à un polynôme distingué de degré* s *en* x_n, *uniquement déterminé.*

Comme cas particulier pour les éléments de degré 1 en x_n, on a le:

THÉORÈME DE L'INVERSION. — *A étant un élément de* U_n *tel que* $A = 0$ *et* $\frac{\partial A}{\partial x_n} \neq 0$, *à l'origine, l'équation* $A = 0$ *définit* x_n *comme fonction analytique de* $x_1, \ldots, x_{n-1}$ *au voisinage de* $x_1 = \ldots = x_{n-1} = 0$.

Par récurrence, on obtient le théorème analogue pour les fonctions implicites de plusieurs variables.

THÉORÈME GÉNÉRAL DE L'INVERSION. — *Soient* $F_1, \ldots, F_h$, h *fonctions analytiques des* $h + m$ *variables* $u_1, \ldots, u_h$, $x_1, \ldots, x_m$, *nulles quand les* u *et les* x *sont nuls, convergentes au voisinage de ce système de valeurs, et telles que le déterminant fonctionnel* $\frac{D(F_1, \ldots, F_h)}{D(u_1, \ldots, u_h)}$ *soit différent de zéro quand les* x *et les* u *sont nuls. Alors les équations* $F_1 = 0, \ldots, F_h = 0$ *définissent les* u *comme fonctions analytiques des* x, *nulles pour les* x *nuls, et convergentes dans un voisinage de ce système de valeurs des* x.

Variétés algébroïdes. — Appelons *variété algébroïde* en 0 ($x_1 = \ldots = x_n = 0$) l'ensemble des points de l'espace X^n qui sont des zéros communs à un système d'éléments de U_n.

La formule de WEIERSTRASS permet, par récurrence, sur le nombre des variables, de démontrer la propriété triviale dans $U_0 = H_p$ qui est un corps, que dans U_n tout idéal a une base finie (Cf. W. R., p. 264) et par conséquent pent se représenter comme intersection d'un nombre fini d'idéaux primaires. A chaque idéal primaire est attaché un idéal premier (qui possède la même variété de zéros). La condition nécessaire et suffisante pour qu'une variété algébroïde soit *irréductible* (c'est-à-dire qu'elle ne puisse être représentée comme la somme de deux variétés algébroïdes en 0 dont aucune ne contient l'autre) est que son idéal propre (c'est-à-dire l'idéal de tous les éléments de A s'annulant sur tout un voisinage de 0 de la variété) soit premier. Il en résulte:

THÉORÈME 1.8. — *Une variété algébroïde en* 0 *est décomposable dans un voisinage de* 0, *en un nombre fini de variétés algébroïdes en* 0, *irréductibles.*

Soit alors $\mathfrak{S}$ un idéal premier de U_n, Π_n le corps quotient de l'anneau de classes de restes $U_n/\mathfrak{S}$. On trouve (Cf. W. R., p. 266–269), qu'après, au besoin, une substitution linéaire et homogène non singulière sur les variables, il y a k des variables, soient $x_1, \ldots, x_k$, telles qu'on ait l'isomorphie $\Pi_n \backsim \Lambda_k$, Λ_k étant le corps quotient de U_k, ω un élément algébrique sur U_k satisfaisant

à une équation irréductible dans U_k, $g(\omega) = \omega^s + g_1\omega^{s-1} + \ldots + g_s = 0$, où les g_i sont des éléments non unités de U_k. On en déduit (Cf. W. R., p. 275-280):

THÉORÈME 1.9. — *Une variété de* X^n, *algébroïde en* 0, *irréductible, admet au voisinage de* 0 *une représentation paramétrique « de* WEIERSTRASS »

$$x_{k+h} = \frac{P_h(x_1, \ldots, x_k, \omega)}{D(x_1, \ldots, x_k)} \qquad (h = 1, 2, \ldots, n-k) \tag{3}$$

les P_h *étant des polynômes de degré* $s-1$ *en* ω, *à coefficients éléments de* U_k, ω *satisfaisant à une équation irréductible* $g(\omega) \equiv \omega^s + g_1\omega^{s-1} + \ldots + g_s = 0$ *où les* g_i *sont des éléments de* U_k *nuls à l'origine,* D *étant le discriminant de l'équation* $g(\omega) = 0$.

Tout système de valeurs $x_1, \ldots, x_k$ *de* H_p *suffisamment petites, telles que* $D(x_1, \ldots, x_k) \neq 0$, *donne par ces formules* s *points de la variété voisin de l'origine, et tout point de la variété suffisamment voisin de l'origine, tel que* $D(x_1, \ldots, x_k) \neq 0$, *est ainsi obtenu.*

Les points de la variété tels que $D(x_1, \ldots, x_k) \neq 0$ seront appelés *points réguliers* de la variété. Sil n'y a que des points réguliers ($s = 1$) la variété algébroïde sera dite réguliere.

L'ensemble des points qui fournit une représentation paramétrique, telle que (3), sera appelé un *élément de* WEIERSTRASS. Le théorème (1.9) peut s'énoncer ainsi: *les points d'une variété* V, *algébroïde en* 0, *irréductible forment, au voisinage de* 0, *un élément de* WEIERSTRASS, *à condition de négliger au besoin les points d'une vraie sous-variété algébroïde de* V. Le nombre k est dit la dimension de l'élément. C'est aussi par définition la dimension de la variété algébroïde irréductible V car on démontre (Cf. W. R., p. 274) qu'il ne dépend pas de la façon dont on a choisi les variables $x_1, \ldots, x_k$. On montre aussi que les composants irréductibles d'une vraie sous-variété algébroïde de V ont des dimensions $< k$.

Démontrons maintenant quelques conséquences du théorème (1.9) qui nous seront utiles pour la suite. Les points de la variété V, tels que $D(x_1, \ldots, x_n) = 0$ sont les zéros de l'idéal $(\mathfrak{F}, D)$. En leur appliquant le théorème (1.9), on obtient finalement:

THÉORÈME 1.10. — *On obtient tous les points appartenant à un voisinage de l'origine suffisamment petit d'une variété algébroïde, en* 0, *irréductible, en réunissant un nombre fini d'éléments de* WEIERSTRASS.

Parmi ceux-ci l'élément de WEIERSTRASS qui donne les points réguliers de V sera appelé l'élément de WEIERSTRASS principal.

Les éléments de WEIERSTRASS de dimension zéro fournissent un nombre fini de points. Il en résulte:

THÉORÈME 1.11. — *Si deux variétés algébroïdes en* 0, *ont en commun une infinité de points convergents en* 0, *elles ont en commun au moins un élément de* WEIERSTRASS *de dimension au moins* 1, *qui contient une infinité de ces points.*

Nous appellerons *élément paramétrique* de centre 0 l'ensemble des points

$$x_i = f_i(t_1, \ldots, t_s) \qquad (i = 1, 2, \ldots, n)$$

où les f_i étant des fonctions analytiques définies au voisinage de $t_1 = \ldots = t_s = 0$ et nulles pour ce système de valeurs.

Soit F l'idéal des éléments de U_n qui s'annulent sur tous ces points. On démontre facilement que cet idéal est premier. La variété algébroïde des zéros de l'idéal F sera dite la *variété algébroïde de l'élément.* Elle contient tous les points de l'élément paramétrique, mais par contre, celui-ci n'en représente pas nécessairement tous les points voisins de 0 quand on donne aux t_j des valeurs voisines de 0.

Si la matrice fonctionnelle $\left\| \frac{\partial f_i}{\partial t_j} \right\|$ est de rang s en 0, donc au voisinage de 0, nous dirons que l'élément paramétrique est *régulier* de dimension s; en effet le théorème de l'inversion permet facilement de montrer que la variété algébroïde de l'élément est régulière en 0 et de dimension s et que dans ce cas, l'élément paramétrique donne toute sa variété algébroïde au voisinage de 0.

Si la matrice fonctionnelle $\left\| \frac{\partial f_i}{\partial t_j} \right\|$ est « en général » de rang s au voisinage de 0, mais non au point 0 même, la variété algébroïde de l'élément n'est plus nécessairement régulière en 0. On voit immédiatement qu'elle est de dimension $\geq s$. On peut montrer, qu'en fait, elle est exactement s.

En faisant un changement de coordonnées convenable et en utilisant encore le théorème de l'inversion, on voit aussi que si J est un élément de WEIERSTRASS de dimension k, A un point de J, le voisinage de A sur J est un élément régulier de dimension k.

Nous démontrerons d'autre part:

THÉORÈME 1.12. — *Soit* V *une variété irréductible algébroïde en* 0; *soit* A *un point régulier de l'élément de* WEIERSTRASS *principal de* V. *Si tout un voisinage de* A *est contenu dans une variété algébrique* W, *alors* W *contient toute la variété* V *au voisinage de* 0.

Soit $x_{k+h} = \dfrac{P(x_1, \ldots, x_k;\ \omega)}{D(x_1, \ldots, x_k)}$ $(h = 1, 2, \ldots, n-k)$ la représentation de WEIERSTRASS de V, valable dans le domaine $|x_1|_p, \ldots, |x_k|_p \leq m$ pour les

points réguliers $D(x_1, \ldots, x_k) \neq 0$. Soit $Q(x_1, \ldots, x_n) = 0$ l'une des équations algébriques qui définissent W; $Q_1(x_1, \ldots, x_k; \omega)$ le résultat de la substitution aux x_{k+h} de leurs valeurs en fonction de $x_1, \ldots, x_k, \omega$; $Q_2(x_1, \ldots, x_k) =$ $=$ Norme $(Q, (x_1, \ldots, x_k; \omega))$. le produit des expressions obtenues en remplaçant ω par ses conjugués dans Q_1; Q_2 est un élément de U_n qui converge dans tout le domaine $|x_1|_p, \ldots, |x_k|_p \leq m$. Si $a_1, \ldots, a_n$ sont les coordonnées du point régulier A de l'énoncé ($|a_1|_p, \ldots, |a_k|_p < m$), Q_2 est nul pour tout le voisinage du système de valeurs $a_1, \ldots, a_k$, donc (théorème 1.5) Q_2 est identiquement nul. Pour tout système de valeurs $x_1, \ldots, x_k$ en valeur absolue p-adique $\leq m$, il y a donc un des s points correspondants sur V (s degré de l'équation de ω) qui est sur la variété algébroïde (Q) d'équation $Q = 0$, (Q) contient donc l'origine. Si (Q) ne contient pas V, comme V est irréductible, son intersection avec V se compose d'un nombre fini d'éléments de dimensions $\leq k-1$ dont la projection sur l'espace des $x_1, \ldots, x_k$ ne peut recouvrir tout un voisinage de l'origine de cet espace à k dimensions. (Q) contient donc V tout entier. En appliquant ce résultat aux éléments d'une base de V, on obtient donc le résultat à démontrer.

REMARQUE. — Si on remplace le polynome en $x_1, \ldots, x_n$ par un élément quelconque s de U_n, la démonstration demeure encore valide. Donc on pourrait remplacer dans l'énoncé (1.12) les mots variété algébrique par variété algébroïde en 0. D'autre part, il en résulte que si un élément de U_n n'est pas identiquement nul sur V, tout point de V pour lequel il est nul est limite des points pour lesquels il n'est pas nul. Si on applique ce résultat au discriminant de l'équation de ω on voit que *tout point de* V *qui n'est pas régulier pour une représentation de Weierstrass donnée, est limite de points réguliers.* Nous mentionnons seulement ces propriétés que nous n'aurons pas à utiliser.

Fonctions exponentielles et logarithmes p-adiques. — Il est bien connu qu'on peut définir dans H_p des fonctions analogues aux fonctions exponentielles et logarithmiques de l'analyse classique. Considérons la série:

$$1 + x + \frac{x^2}{2} + \ldots + \frac{x^n}{n!} + \ldots$$

p^ν désignant la plus haute puissance de p ne dépassant pas n, on a

$$\text{ordre } (n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^\nu}\right] \leq \frac{n}{p^\nu}\frac{p^\nu - 1}{p-1}$$

$$\text{ordre } \left(\frac{x^n}{n!}\right) \geq n\left(\text{ordre } (x) - \frac{1}{p-1} + \frac{1}{p^\nu(p-1)}\right).$$

La série est donc convergente si ordre $(x) > \frac{1}{p-1}$ et elle représente alors une fonction analytique de x que nous désignerons par *Exp* (x).

On vérifie par un calcul formel, valable quand les $\operatorname{Exp} x_1$, $\operatorname{Exp} x_2$ convergent, que

$$\operatorname{Exp}(x_1 + x_2) = \operatorname{Exp}(x_1) \cdot \operatorname{Exp}(x_2).$$

Considérons la série

$$\xi - \frac{\xi^2}{2} + \ldots + (-1)^n \frac{\xi^n}{n} + \ldots;$$

On a:

$$\text{Ordre}\left(\frac{\xi^n}{n}\right) = n \cdot \text{ordre}(\xi) - \text{ordre}(n).$$

La série converge donc si ordre $(\xi) > 0$, c'est-à-dire si ξ est un entier p-adique qui n'est pas une unité p-adique. Elle représente alors une fonction analytique de x que nous désignerons par *Log* $(1 + \xi)$.

Pour y_1 et y_2 suffisamment voisins de 1, $\operatorname{Log} y_1$, $\operatorname{Log} y_2$ et $\operatorname{Log} y_1 y_2$ sont définis et on vérifie par un calcul formel $\operatorname{Log}(y_1 \cdot y_2) = \operatorname{Log} y_1 + \operatorname{Log} y_2$.

Pour x suffisamment petit $\operatorname{Log}(\operatorname{Exp} x)$ est défini et on vérifie formellement que sa valeur est x. De même pour y suffisamment voisin de 1, $\operatorname{Exp}(\operatorname{Log} y)$ est définie et sa valeur est y. Les fonctions $\operatorname{Exp} x$ et $\operatorname{Log} y$ sont des fonctions inverses.

Soit a un nombre tel que $\operatorname{Log} a$ existe. La fonction $\operatorname{Exp}(x \operatorname{Log} a)$ est une fonction analytique convergente pour x suffisamment voisin de zéro, et

$$\operatorname{Exp}(x_1 + x_2) \operatorname{Log} a = \operatorname{Exp}(x_1 \operatorname{Log} a) \cdot \operatorname{Exp}(x_2 \operatorname{Log} a).$$

Si ordre $(\operatorname{Log} a) > \frac{1}{p-1}$ alors $\operatorname{Exp}(x \operatorname{Log} a)$ converge pour tout x entier p-adique, en particulier pour tout x entier rationnel. On voit que cette fonction coïncide, pour $x = q$ entier rationnel, avec a « à la puissance q », les puissances entières rationnelles étant définies à partir de la multiplication et de l'inversion comme d'habitude. Pour abréger, nous la désignerons par a^x.

Les nombres pour lesquels a^y existe et converge pour tout y entier p-adique, sont des unités p-adiques suffisamment voisines de 1. Nous les appellerons *unités* p-*adiques distinguées.*

THÉORÈME 1.13. — *Si* K_p *est une extension algébrique finie de* R_p, *il y a un nombre naturel* m *tel que pour toute unité* p-*adique* ε *de* K_p, ε^m *soit une unité* p-*adique distinguée.*

Soit n le degré de K_p sur R_p, alors on peut trouver n entiers p-adiques de K_p tels que tout entier p-adique de K_p soit de la forme

$$x_1\omega_1 + \ldots + x_n\omega_n$$

les x_i étant des entiers de R_p. Chacun des x_i peut être mis sous la forme $\sum_{i=0}^{+\infty} a_i p^i$, les a_i étant pris parmi p entiers rationnels incongrus (mod p). Donc, E_{K_p} désignant l'anneau des entiers p-adiques de K_p, h étant un nombre naturel quelconque, le nombre $C(h)$ de classes de restes de E_{K_p} modulo l'idéal principal (p^h), est fini.

Pour tout élément ε de E_{K_p}. premier à p, donc unité p-adique, on a

$$\varepsilon^{C(h)-1} \equiv 1(p^h)$$
$$\varepsilon^{C(h)-1} = 1 + \eta \qquad \text{avec ordre } (\eta) \geq h$$

il nous suffira donc de prendre $h > \dfrac{1}{p-1}$ pour que la valeur correspondante de $C(h) - 1$ donne le nombre m cherché.

Chapitre II. - **Groupes abéliens de points.**

Opérations sur les points et variétés de X^n.

Congruences. — Soit, comme dans le chapitre précédent, X^n le produit topologique de n espaces H_p; un point de X^n est un système de n nombres $x_1, \ldots, x_n$, de H_p, que nous appellerons les coordonnées du point. Nous définirons le *produit* $A_3 = A_1 \cdot A_2$ de deux points A_1, A_2 de X^n, comme étant le point ayant pour coordonnées les produits des coordonnées de même indice de A_1 et de A_2. Désignons par $\{X^n\}$ l'ensemble des points de X^n qui n'ont aucune coordonnée nulle. Ils forment un groupe abélien par rapport à la multiplication que nous venons de définir. Si nous multiplions tous les points de X^n par un même point A de $\{X^n\}$, nous obtenons une transformation de X^n en lui-même que nous appellerons une *congruence*. L'ensemble de toutes les congruences forme un groupe abélien isomorphe à $\{X^n\}$. Deux figures formées de points de X^n qui se correspondent dans une même congruence seront dites *congrues*. C'est évidemment une relation transitive. Une congruence étant une transformation affine non singulière de X^n, deux figures congrues ont en même temps le caractère d'être une variété algébrique irréductible, de dimension s, ou d'être une variété algébroïde irréductible de dimension s,

μ-Variétés. — Soient $A_1, \ldots, A_r$, r points de X^n de coordonnées $a_{11}, \ldots, a_{1n}; \ldots; a_{r1}, \ldots, a_{rn}$ Nous supposons que l'on a $r < n$, que les $\mathrm{Log}\,(a_{ij})$ existent, et que les r vecteurs

$$(\mathrm{Log}\,(a_{j1}), \ldots, \mathrm{Log}\,(a_{jn})) \qquad (j = 1, 2, \ldots, r) \tag{1}$$

sont linéairement indépendants par rapport à H_n. Alors pour des valeurs des paramètres y suffisamment voisines de zéro $|y_i|_p \leq c$, les exponentielles $a_{ij}^{y_i}$ sont définies et sont des fonctions analytiques des y. Le point

$$\begin{aligned} x_i &= \mathrm{Exp}\,(y_1 \mathrm{Log}\, a_{1i} + \ldots + y_r \mathrm{Log}\, a_{ri}) \\ &= a_{1i}^{y_1} \ldots a_{ri}^{y_r} \end{aligned} \qquad (i = 1, 2, \ldots, n) \tag{2}$$

pour $|y_i|_p \leq c$, engendre un élément régulier, ayant pour centre le point $(1, \ldots, 1)$, et de dimension r. Une telle variété ou ses variétés congrues

$$x_i = q_i a_{1i}^{y_1} \ldots a_{ri}^{y_r} \qquad (i = 1, 2, \ldots, n) \tag{3}$$

(où $q_1, \ldots, q_n \neq 0$) seront dites des *μ-variétés* de dimension r.

On voit facilement que si

$$(b_{m1}, \ldots, b_{mn}) \qquad (m = 1, 2, \ldots, n - r)$$

sont $n - r$ vecteurs linéairement indépendants, dont chacun est orthogonal à tous les vecteurs (1), les équations implicites

$$b_{m1} \mathrm{Log} \frac{x_1}{q_1} + \ldots + b_{mn} \mathrm{Log} \frac{x_n}{q_n} = 0 \qquad (m = 1, 2, \ldots, n - r) \tag{4}$$

définissent la même variété que les équations paramétriques (3).

Les μ-variétés jouent exactement par rapport au groupe des congruences, le rôle des variétés linéaires par rapport au groupe des translations. En effet, soient $y_1^0, \ldots, y_r^0$ un système de valeurs des exposants telles que $|y_i|_p \leq c$, posons

$$q_i' = q_i a_{1i}^{y_1^0} \ldots a_{ri}^{y_r^0} \qquad (i = 1, 2, \ldots, n)$$

les formules

$$x_i = q_i' a_{1i}^{y_1'} \ldots a_{ri}^{y_r'} \qquad (i = 1, 2, \ldots, n \tag{3'}$$

pour $|y_i'|_p \leq c$ fournissent les mêmes points que les formules (3). On voit qu'une *μ-variété est invariante globalement par la congruence qui fait passer de l'un à l'autre de deux quelconques de ses points.* Il en résulte qu'une μ-variété est bien définie quand on sait qu'elle est congrue à une μ-variété donnée, et qu'elle passe par un point donné (qu'il faut supposer appartenir à $\{X^n\}$).

Soit Q, $(q_1, \ldots, q_n)$ un point de $\{X^n\}$. Considérons la transformation

$$\bar{x}_i = \mathrm{Log}\left(\frac{x_i}{q_i}\right). \qquad (i = 1, 2, \ldots, n) \tag{5}$$

Soit v un voisinage de Q, $\bar{v}$ le voisinage correspondant de l'origine. Supposons v suffisamment petit pour que la transformation soit biunivoque et bianalytique. Nous appellerons v un *voisinage propre de* Q. *Dans la suite de ce chapitre nous supposerons toujours pour toutes les études locales que nous ferons, que tous les points, les éléments de variétés, les voisinages considérés, sont intérieurs au voisinage propre d'un même point fixe de* $\{X^n\}$.

Par la transformation (5), aux μ-variétés passant par des points voisins correspondent des variétés linéaires de mêmes dimensions, voisines de l'origine et réciproquement. Aux congruences voisines de la transformation identique correspondent des translations d'amplitudes voisines de zéro. Moyennant la restriction indiquée, et grâce à la transformation (5) et au théorème (1.12) on voit facilement que:

H_A *étant un élément algébroïde irréductible au voisinage d'un point* A, *et* I_B *le voisinage sur* H_A *d'un point* B *régulier de* H_A, *si* I_B *est contenu dans une* μ*-variété* M, H_A *tout entier est contenu dans* M. *En particulier, si on montre que* I_B *est une* μ*-variété, il en résulte que* H_A *est une* μ*-variété.* On obtient aisément aussi grâce à la transformation (5), la démonstration de la réciproque d'une proposition énoncée plus haut:

Si I_A *est un élément régulier de centre* A, *et si pour tout point* B *de* I_A *il y a un voisinage de ce point sur* I_A *congru à un voisinage de* A *sur* I_A, I_A *est une* μ*-variété.*

Produit de deux variétés. — Nous appellerons *produit de deux figures* $F_1 \cdot F_2$, formées de points de X^n, la figure $F_3 = F_1 \cdot F_2$ formée par l'ensemble des points produits d'un point quelconque de la première par un point quelconque de la seconde. Nous appellerons *inverse d'une figure* F, la figure F^{-1} formée par l'ensemble des points inverses des points de F qui n'ont aucune coordonnée nulle. Nous nous occuperons de figures qui ne sont tout entières dans aucun des hyperplans de coordonnées $x_i = 0$. Dans ces conditions, $F_3 = F_1 \cdot F_2$ contient au moins une figure congrue à F_1 et une figure congrue à F_2, et F^{-1} existe.

Le produit de deux variétés algébriques irréductibles (11), W_1 *de dimen-*

(11) Une variété algébrique W est dite irréductible quand son idéal propre (W) dans l'anneau des polynômes en $x_1, \ldots, x_n$, est premier. C'est une irréductibilité globale, dif-

sion s_1, W_2 *de dimension* s_2, *est une variété algébrique irréductible* W_3 *de dimension* $s_3 \leq s_1 + s_2$.

En effet, le point général de W_1 admet une représentation paramétrique, les coordonnées étant des fonctions algébriques de s_1 paramètres; de même W_2 avec s_2 autres paramètres. Donc les coordonnées du point général de W_3 sont des fonctions algébriques de $s_1 + s_2$ paramètres. Il en résulte que W_3 est une variété algébrique irréductible de dimension $\leq s_1 + s_2$.

On verrait de façon analogue que *si* W *est une variété algébrique irréductible de dimension* s, *non tout entière située dans un hyperplan de coordonnée,* W^{-1} *est une variété algébrique irréductible, de dimension* s.

Intersections de μ-variétés et de variétés algébriques.

LEMME 2.1. — *Soit* W *une variété algébrique irréductible de* X^n, *de dimension* s. *Soit* A *un point de* W, *non singulier et non situé dans un des hyperplans de coordonnées. Soit* M_A *une* μ*-variété de dimension* r, *passant par* A. *Supposons que* $M_A \cap W$ *soit, au voisinage de* A, *un élément régulier* I_A *de dimension* $k \geq 1$ *et qu'il n'y ait pas de variété algébrique de dimension inférieure à* s *qui contienne* I_A. *Alors en tout point* Q *de* W *étranger à une vraie sous-variété algébrique* w *de* W, *l'intersection* $M_Q \cap W$ (M_Q *étant la* μ*-variété congrue à* M_A *passant par* Q) *est un élément régulier* I_Q *de dimension* k, *qui dépend analytiquement des coordonnées locales de* Q, *quand on fait varier* Q *sur* W *au voisinage d'un point* Q_0 *étranger à* w.

Soient

$$F_h(x_1, \ldots, x_n) = 0 \qquad (h = 1, 2, \ldots, f)$$

les équations qui définissent W

$$b_{m1} \operatorname{Log} \frac{x_1}{a_n} + \ldots + b_{mr} \operatorname{Log} \frac{x_n}{a_n} = 0 \qquad (m = 1, 2, \ldots, n - r)$$

celles de M_A, les $n - r$ vecteurs $(b_{m1}, \ldots, b_{mn})$ étant par hypothèse linéairement indépendants. Celles de M_Q, Q étant un point quelconque de $\{X^n\}$,

---

férente de l'irréductibilité locale définie au chapitre I pour toute variété algébroïde. La dimension s de W, définie algébriquement à partir de cet idéal de polynômes, coïncide en tout point avec la dimension définie localement comme au chap. I. On démontre qu'il existe une représentation, comme fonctions algébriques de s paramètres, des coordonnées de tous les points de W étrangers à une vraie sous-variété de W ou comme on dit du point général de W

(Cf. Van der WAERDEN, *Moderne Algebra*. tome II, chap. 13).

de coordonnées $q_1, \ldots, q_n$, sont

$$b_{m1} \operatorname{Log} \frac{x_1}{q_1} + \ldots + b_{mr} \operatorname{Log} \frac{x_n}{q_n} = 0. \qquad (m = 1, 2, \ldots, n-r)$$

Considérons les système d'équations aux différentielles totales

$$(D) \quad \begin{cases} dx_1 \dfrac{\partial F_j}{\partial x_1} + \ldots + dx_n \dfrac{\partial F_j}{\partial x_n} = 0 & (j = 1, 2, \ldots, f) \\ dx_1 \dfrac{b_{m1}}{x_1} + \ldots + dx_n \dfrac{b_{mn}}{x_n} = 0. & (m = 1, 2, \ldots, n-r) \end{cases}$$

Il est satisfait quand le point $(x_1, \ldots, x_n)$ parcourt l'élément I_A qui est une variété intégrale à k dimensions de (D). D'autre part, (D) est un système d'équations linéaires et homogènes par rapport aux dx, dont les coefficients sont des fonctions rationnelles des x. Son rang a donc la même valeur ρ en tous les points de W, sauf peut-être sur une vraie sous-variété algébrique de la variété algébrique irréductible W. Nous désignerons par w la réunion de cette sous-variété avec celles qui portent les points singuliers de W et les intersections de W avec les hyperplans coordonnées, s'ils n'étaient déjà contenus dans la première. w est une vraie sous-variété algébrique de W. Il est impossible que I_A soit contenu tout entier dans w donc ρ est égal à $n - k$. En un point quelconque Q_0 de W étranger à w le système (D) peut donc être résolu par rapport à k variables auxiliaires $d\xi_1, \ldots, d\xi_k$ sous la forme

$$(D') \qquad dx_i = g_{i1} d\xi_1 + \ldots + g_{ik} d\xi_k. \qquad (i = 1, 2, \ldots, n)$$

Les g_{ij} sont des fonctions rationnelles des x, et les k vecteurs $(g_{j1}, \ldots, g_{jn})$ sont linéairement indépendants. Les conditions d'intégrabilité de (D') sont des équations algébriques en x. Comme elles sont vérifiées sur I_A, elles sont nécessairement identiquement vérifiées sur tout W.

Soit maintenant

$$(1) \qquad x_i = f_i(t_1, \ldots, t_s) \qquad (i = 1, 2, \ldots, n)$$

l'élément régulier, de dimension s, qui représente W au voisinage de Q_0 (Q_0 correspond à $t_1 = \ldots = t_s = 0$). Substituons les f aux x dans (D). Les premières équations de (D) sont identiquement vérifiées, les $n - r$ restantes forment un système (D'') complètement intégrable. On peut l'écrire à l'aide de k éléments auxiliaires $d\theta_1, \ldots, d\theta_k$, sous la forme

$$(D'') \qquad dt_j = h_{1j} d\theta_1 + \ldots + h_{kj} d\theta_k \qquad (j = 1, 2, \ldots, s)$$

les h_{ij} étant des fonctions analytiques des t, au voisinage de $t_1 = \ldots = t_s = 0$, et les k vecteurs à s dimensions $(h_{i1}, \ldots, h_{is})$ étant linéairement indépendants.

On peut calculer le développement en série des t suivant les puissances entières positives de k variables auxiliaires $\theta_1, \ldots, \theta_k$. En effet les conditions d'intégrabilité étant identiquement vérifiées, on obtient les dérivées partielles des t par rapport aux θ pour les valeurs initiales t_i^0 comme fonctions analytiques des t_i^0 grâce aux formules

$$\frac{\partial}{\partial\theta_g} = \frac{\partial}{\partial t_1} h_{g1} + \ldots + \frac{\partial}{\partial t_s} h_{gs} \qquad (g = 1, 2, \ldots . k)$$

d'où

$$\frac{\partial^\nu t_j}{\partial\theta_1^{\nu_1} \ldots \partial\theta_k^{\nu_k}} = \Theta_{j,\nu_1,\ldots,\nu_k}(t_1^0, \ldots, t_s^0) \qquad (j = 1, \ldots, s)$$

$$t_j = t_j + h_{1j}(t_1^0, \ldots, t_s^0)\theta_1 + \ldots + h_{kj}(t_1^0, \ldots, t_s^0)\theta_k + \ldots$$

$$\ldots + \Theta_{j,\nu_1,\ldots,\nu_k}(t_1^0, \ldots, t_s^0) \frac{\theta_1^{\nu_1} \ldots \theta_k^{\nu_k}}{(\nu_1 + \ldots + \nu_k)!} + \ldots .$$

On vérifie aisément que cette série, considérée comme série en $\theta_1, \ldots, \theta_k, \ldots, t_1^0, \ldots, t_s^0$, converge pour les t^0 et θ assez petits (en supposant qu'on ait fait au besoin un changement de variables $\theta_g = p^N\theta_g'$, N étant un nombre naturel assez grand). Substituons aux t les expressions qu'on vient de calculer, dans les équations (1), on obtient

$$x_i = \Phi_i(t_1^0, \ldots, t_s^0, \theta_1, \ldots, \theta_k) \qquad (i = 1, 2, \ldots, n) \tag{2}$$

les fonctions Φ_i étant des fonctions analytiques des t' et des θ. Pour $\theta_1 = \ldots = \theta_k = 0$, elles se réduisent à

$$x_i = \Phi_i(t_1^0, \ldots, t_s^0, 0, \ldots, 0) \equiv f_i(t_1, \ldots, t_s) \qquad (i = 1, 2, \ldots, n)$$

et représentent tout le voisinage de Q_0 sur W.

Si on y laisse $t_1^0, \ldots, t_s^0$ fixes et si l'on fait varier les θ alors (2) représente un élément I_Q de dimension k, régulier autour du point $Q\ (q_1, \ldots, q_n)$ de W, correspondant à $\theta_1 = \ldots = \theta_k = 0$. Il est évidemment sur W. D'autre part, il satisfait à

$$dx_1 \frac{b_{m1}}{x_1} + \ldots + dx_n \frac{b_{mn}}{x_n} = 0 \qquad (m = 1, 2, \ldots, n - r)$$

donc, en tenant compte des conditions initiales, on voit qu'il est sur la μ-variété M_Q

$$b_{m1} \operatorname{Log} \frac{x_1}{q_1} + \ldots + b_{mr} \operatorname{Log} \frac{x_n}{q_n} = 0 \qquad (m = 1, 2, \ldots, n - r)$$

qui est la μ-variété congrue à M passant par Q. I_Q appartient donc à $W \cap M_A$, comme il est de dimension k, il constitue tout le voisinage de Q sur $W \cap M_Q$, le lemme est démontré.

LEMME 2.2. — *Conservons les notations et les hypothèses du lemme* 2.1. *Supposons en outre qu'il n'existe pas de* μ*-variété de dimension inférieure à* r *qui contienne* I_A. *Alors il existe une variété algébrique* $\widehat{W}$ *de dimension* $\widehat{s} \leq s + r - k$ *contenant* M_A.

Prenons un point Q_0 de W, étranger à w et situé sur I_A. C'est toujours possible, puisque w ne peut contenir I_A. Alors Q_0 étant un point de M_A, M_{Q_0} est identique à M_A. Soit I_{Q_0} le voisinage de Q_0 sur I_A, c'est un élément régulier de dimension k qui représente $W \cap M_{Q_0}$ au voisinage de Q_0; W et M_{Q_0} sont la variété algébrique et la μ-variété de dimension minima contenant I_{Q_0}. Utilisons la représentation paramétrique (2) du lemme précédent pour le voisinage de Q_0 sur W. Soit C une courbe algébrique irréductible, située sur W, passant par Q_0 et régulière en Q_0. On peut la définir au voisinage de Q_0 par l'intermédiaire de (2), en se donnant les t comme fonctions analytiques convenablement choisies d'un paramètre ζ

$$t_j = u_j(\zeta) \qquad (j = 1, 2, \ldots, s)$$

et en laissant les θ nuls. Nous supposons que grâce à une congruence convenable sur la figure initiale les coordonnées de Q_0 sont $1, \ldots, 1$. Formons la variété algébrique $W_1 = W \cdot C^{-1}$. Elle est irréductible et contient W comme sous-variété. Elle est donc de dimension $s + 1$ ou s. Dans ce dernier cas, elle coincide avec W. Elle contient les points de l'élément paramétrique

$$x_i = \Phi_i(t_1, \ldots, t_s, \theta_1, \ldots, \theta_k)\Phi_i^{-1}(u_1(\zeta), \ldots, u_s(\zeta), 0, \ldots, 0) \qquad (i = 1, 2, \ldots, n).$$

C'est même la variété algébroïde de cet élément.

Donnons à ζ une valeur fixe ζ^0 et faisons $t_1 = u_1(\zeta^0), \ldots, t_s = u_s(\zeta^0)$ et faisons varier les θ. On obtient ainsi un élément I_Q' congru à $I_Q = M_Q \cap W$ d'après le lemme précédent, (Q étant le point de coordonnées $x_i = \Phi_i(u_1(\zeta^0), \ldots, u_s(\zeta^0), 0, \ldots, 0)$). Faisons $\theta_1 = \ldots = \theta_k = 0$ dans la représentation paramétrique de I_Q'. On obtient le point $Q_0(1, \ldots, 1)$. Donc I_Q' appartient à M_{Q_0}. Il en résulte que l'élément paramétrique

$$(J_1) \qquad x_i = \Phi_i(u_1(\zeta), \ldots, u_s(\zeta), \theta_1, \ldots, \theta_k)\Phi_i^{-1}(u_1(\zeta), \ldots, u_s(\zeta), 0, \ldots, 0) \qquad (i = 1, 2, \ldots, n)$$

appartient à $W \cap M_{Q_0}$ et qu'il contient des éléments congrus à chacun des éléments réguliers de dimension k, $I_Q = W \cap M_Q$, pour chaque point Q de la courbe C voisin de Q_0.

Si tous ces éléments I_Q sont congrus à I_{Q_0}, quel que soit le choix de la courbe algébrique C passant par Q_0, ils sont congrus à I_{Q_0} quel que soit Q

sur W dans tout un voisinage de Q_0; en particulier quel que soit Q sur I_{Q_0}. Tous les voisinages sur I_{Q_0} sont congrus, I_{Q_0} est donc une μ-variété. Mais alors comme M_{Q_0} est la μ-variété de la plus petite dimension contenant I_{Q_0}, I_{Q_0} coincide avec M_{Q_0}, c'est-à-dire avec M_A, et k est égal à r. W est elle-même la variété algébrique $\widehat{W}$ cherchée.

S'il n'en est pas ainsi, on pourra choisir la courbe algébrique C de façon qu'un des I_Q, Q étant sur C, ne soit pas congru à I_{Q_0}. J_1 sera nécessairement de dimension plus grande que k. L'intersection de W_1 et M_{Q_0} est au voisinage de Q_0 une variété algébroïde. Il y a au moins une de ses composantes irréductibles, soit H_1, qui contient J_1; soit k_1 la dimension de H_1; on a $k_1 \geq k+1$. Soit A_1 un point de H_1 régulier et étranger aux autres composantes de $W_1 \cap M_{Q_0}$. Le voisinage de A_1 sur H_1 est un élément régulier I_{A_1} de dimension k_1, qui représente toute l'intersection $W_1 \cap M_{A_1}$ au voisinage de A_1 (M_{A_1} est identique à M_A). On voit facilement que W_1 est la variété algébrique de dimension minima contenant I_{A_1} et que $M_A \equiv M_{A_1}$ est la μ-variété de dimension minima contenant I_{A_1}.

On peut donc opérer à partir de W_1, de dimension $s_1 = s+1$, I_{A_1} de dimension $k_1 \geq k+1$ et M_{A_1} ($\equiv M_A$) comme on vient de faire à partir de W, I_A, M_A. Ou bien, $k_1 = r$, I_{A_1} est identique à M_{A_1} donc à M_A, ou bien on peut construire W_2 de dimension $s_2 = s_1 + 1$, telle que $W_2 \cap M_{A_2}$ ait au voisinage de A_2 une composante irréductible contenant I_{A_1} et de dimension $k_2 \geq k_1 + 1$, etc... Au bout de $r - k - 1$ opérations au plus, on arrive donc à une variété W_m telle que $W_m \cap M_{A_m}$ ait une composante de dimension r, c'est-à-dire que W_m contienne M_{A_m} c'est-à-dire M_A. W_m est de dimension $\leq r+s-k$. C'est la variété $\widehat{W}$ cherchée.

Remarquons que le résultat peut être trivial si l'on n'a pas $r+s-k<n$ car alors W peut être l'espace X^n tout entier.

LEMME 2.3. — *Si une variété algébrique de dimension* s *contient une* μ*-variété, entre* s + 1 *quelconques des coordonnées d'un point de la* μ*-variété, soient* $x_{q_1}, \ldots, x_{q_{s+1}}$, *il y a une relation*

$$x_{q_1}^{Nq_1}, \ldots, x_{q_{s+1}}^{Nq_{s+1}} = C_{q_1, \ldots, q_{s+1}}$$

où les exposants $N_{q_1}, \ldots, N_{q_{s+1}}$ *sont des entiers rationnels, non tous nuls et* $C_{q_1, \ldots, q_{s+1}}$ *un nombre différent de zéro indépendant du choix du point sur la* μ*-variété.*

Nous pouvons, par une congruence, amener le centre de la μ-variété, au point de coordonnées 1, ..., 1. Soient M la μ-variété, W la variété algébrique (toujours de dimension s), déduites des premières par la congruence.

$s+1$ coordonnées d'un point de W, soient $x_1, \ldots, x_{s+1}$ sont liées par une équation algébrique

$$f(x_1, \ldots, x_{s+1}) = 0.$$

Soient $b_1, \ldots, b_n$ les coordonnées d'un point de M autre que le point de coordonnées $1, \ldots, 1$, alors M contient aussi le point de coordonnées $b_1^h, \ldots, b^h$ quelque soit le nombre naturel h. Donc W le contient aussi, et l'on a

$$f(b_1^h, \ldots, b_{s+1}^h) = 0.$$

Soit ν le nombre de termes dans f. Ecrivons les équations précédentes pour $h = 1, 2, \ldots, \nu$. On a ainsi, entre les coefficients de f, ν équations linéaires et homogènes dont les coefficients sont des monômes en $b_1, \ldots, b_s$, et dont le déterminant est un déterminant de VAN DER MONDE. Pour que ces équations aient une solution non triviale, il faut que ce déterminant soit nul, donc qu'il ait deux colonnes égales, ce qui entraîne l'égalité de deux monômes en $b_1, \ldots, b_{s+1}$. On obtient un nombre fini de variétés algébriques, chacune définie par une équation du type

$$x_1^{N_1}, \ldots, x_{s+1}^{N_{s+1}} = 1$$

(les N étant des entiers rationnels non tous nuls), dont la réunion doit contenir tous les points de M. Comme M considéré comme variété algébroïde est irréductible, l'une des variétés précédentes doit contenir M tout entier. En revenant à la μ-variété initiale par la congruence inverse de la première, on trouve la propriété annoncée.

Groupes abéliens de points à bases finies. — Considérons des points à n coordonnées, qui soient des nombres algébriques, formant un groupe abélien Γ par rapport à la multiplication définie au début de ce chapitre et possédant une base minima finie à r générateurs d'ordre infini et r' générateurs d'ordre fini. Nous appellerons r le *rang* du groupe et nous supposerons $r > n$. Soient $(a_{11}, \ldots, a_{1m}), \ldots, (a_{r1}, \ldots, a_{rm})$, les coordonnées des points de base d'ordre fini, $(a'_{11}, \ldots, a'_{1n}), \ldots, (a'_{r'1}, \ldots, a'_{r'n})$ celles des points de base d'ordre infini. Alors un élément quelconque du groupe Γ a pour coordonnées

$$\begin{cases} a_1 = a_{11}^{m_1} \ldots a_{1r}^{m_r} a'^{m'_1}_{11} \ldots a'^{m'_{r'}}_{nr'} \\ a_n = a_{n1}^{m_1} \ldots a_{nr}^{m_r} a'^{m'_1}_{n1} \ldots a'^{m'_{r'}}_{nr'} \end{cases}$$

les exposants m étant des entiers rationnels.

Choisissons comme il est toujours possible, le nombre naturel premier p, de façon que les coordonnées des éléments de base, et par suite celle d'un

élément quelconque du groupe, soient des unités p-adiques. Formons le corps H_p et l'espace X^n définis précédemment. Nous considérerons les éléments de Γ comme des points de l'espace X^n.

Nous dirons qu'un sous-groupe γ de Γ est *distingué* s'il admet une base minima formée de points dont les coordonnées sont des unités distinguées de H_p. Ces points de base sont tous des éléments d'ordre infini de γ car la seule unité p-adique distinguée qui soit racine de l'unité est 1. Leur nombre est donc égal au rang du sous-groupe.

Soit K_p l'extension finie de R_p, qu'on obtient en adjoignant à R_p les coordonnées des points de base. D'après le théorème (1.14) il existe un nombre naturel h_0 tel que, pour toute unité p-adique u de K_p, u^{h_0} soit une unité p-adique distinguée.

Posons

$$a_{ij}^{h_0} = b_{ij}. \qquad (i = 1, 2, \ldots, r;\ j = 1, 2, \ldots, n)$$

Le groupe

$$\Gamma_d, \quad a_i = b_{1i}^{m_1} \ldots b_{ri}^{m_r} \qquad (i = 1, 2, \ldots, n)$$

où les m_i sont des entiers rationnels, est un *sous-groupe d'indice fini de* Γ, *qui est distingué.*

Pour un sous-groupe quelconque γ, l'intersection de γ et de Γ_d nous fournira donc un sous-groupe γ^* de γ d'indice fini par rapport à γ (donc de même rang que γ) qui est distingué.

Nous appellerons *dimension* d'un sous-groupe distingué γ^*

$$\gamma^*, \quad a_i = c_{1i}^{m_1} \ldots c_{pi}^{m_p} \qquad (i = 1, 2, \ldots, n)$$

le nombre d (au plus égal au rang de γ^*) de vecteurs linéairement indépendants par rapport à H, parmi les vecteurs formant « la base logarithmique » de γ^*. Nous entendons par là les vecteurs ayant chacun pour coordonnées les logarithmes p-adiques des coordonnées d'un même point de la base distinguée de γ^*. Soient $(c_{11}, \ldots, c_{1n}), \ldots, (c_{d1}, \ldots, c_{dn})$, les points de base correspondant à d de ces vecteurs linéairement indépendants. La μ-variété de dimension d

$$\{\gamma^*\}, \quad x_i = c_{1i}^{y_1} \ldots c_{di}^{y_d} \qquad (i = 1, 2, \ldots, n)$$

contient tous les points de γ^* pour lesquels les m sont en valeur absolue p-adique, suffisamment voisins de zéro. Nous appellerons $\{\gamma\}$ *la* μ-*variété de* γ^*. On voit facilement qu'un ensemble infini $\mathcal{E}$ d'éléments de γ^*, a au moins un point d'accumulation, soit C, et que la μ-variété $C \cdot \{\gamma^*\}$ congrue à $\{\gamma^*\}$ et passant par C, contient un sous-ensemble infini d'éléments de $\mathcal{E}$,

s'accumulant autour de C. On a le même résultat pour l'ensemble d'une infinité d'éléments appartenant à une même classe de Γ/γ.

Soit $\mathfrak{E}$ l'ensemble d'une infinité d'éléments de Γ, nous dirons qu'un sous-groupe γ de rang ρ est *minimal* par rapport à $\mathfrak{E}$ pour la classe $c\gamma$ de Γ/γ si les deux conditions snivantes sont remplies:

1°) la classe $c\gamma$ de Γ/γ contient un sous-ensemble infini $\mathfrak{E}_1$ de $\mathfrak{E}$;

2°) il n'y a pas de sous-groupe γ' de Γ, de rang moindre que celui de γ, tel qu'il y ait une classe de Γ/γ contenant un sous-ensemble infini de $\mathfrak{E}_1$.

Si γ est minimal par rapport à $\mathfrak{E}$ pour la classe $c\gamma$ le sous-groupe distingué $\gamma^* = \gamma \cap \Gamma_d$ est minimal par rapport à $\mathfrak{E}$, pour l'une au moins des classes de Γ/γ^* dont la réunion forme la classe $c\gamma$, car celles-ci sont en nombre fini.

Si $\mathfrak{E}$ est un ensemble infini d'éléments de Γ il y a toujours au moins un sous-groupe minimal, donc au moins un sous-groupe distingué minimal par rapport à $\mathfrak{E}_1$.

$\mathfrak{E}$ étant encore l'ensemble d'une infinité d'éléments de Γ, nous dirons qu'une variété algébrique W irréductible est *minimale* par rapport à $\mathfrak{E}$ si:

1°) elle contient les éléments d'un sous-ensemble infini $\mathfrak{E}_1$ de $\mathfrak{E}$, et si

2°) il n'y a aucune de ses variété algébriques de dimension inférieurs à celle de W qui contienne les éléments d'un sous-ensemble infini de $\mathfrak{E}_1$.

Si les éléments de $\mathfrak{E}$ sont contenus dans une variété algébrique de dimension s il y au moins une variété algébrique minimale par rapport à $\mathfrak{E}$ de dimension $\leq s$.

THÉORÈME 2.4. — *Soit* Γ *un groupe abélien multiplicatif de points à coordonnées algébriques, de rang* r *inférieur au nombre* n *de coordonnées des points. Soit*

$$F_h(x_1, \ldots, x_n) = 0 \qquad (h = 1, 2, \ldots, s') \tag{1}$$

un système d'équations algébriques à coefficients algébriques dont les premiers membres forment la base d'un idéal de polynômes premier de dimension s. *Supposons que les éléments de* Γ *satisfaisant à* (1) *forment un ensemble infini* $\mathfrak{E}$.

A tout sous-ensemble infini $\mathfrak{E}'$ *de* $\mathfrak{E}$ *correspond au moins un sous-groupe* γ *de* Γ *ayant les propriétés suivantes*:

1°) *il y a au moins une classe de* Γ/γ *qui contient un sous-ensemble infini d'élément de* $\mathfrak{E}'$.

2°) *Posons* $\sigma = s + r$; *entre* σ *quelconques des coordonnées d'un élément de* γ, *soient* $x_{q_1}, \ldots, x_{q_\sigma}$ *il y a une relation*

$$x_{q_1}^{N_1} \ldots x_{q_\sigma}^{N_{q_\sigma}} = 1$$

où les exposants N *sont des entiers rationnels non tous nuls indépendants du choix de l'élément dans* γ.

(*Ces résultats deviennent triviaux si l'on n'a pas* $s \leq n - r - 1$).

Choisissons p de façon que les coordonnées des points d'une base de Γ soient des unités p-adiques. Supposons les points de Γ représentés dans l'espace X^n construit à l'aide du corps p-adique H_p. Désignons par W la variété algébrique de X^n, de dimension s, définie par les équations (1). Soit γ^* un sous-groupe de Γ distingué, minimal par rapport à l'ensemble $\mathcal{E}'$ pour une classe de Γ/γ^*. Soit $\mathcal{E}''$ le sous-ensemble infini de $\mathcal{E}'$ dont cette classe contient les éléments. Les éléments de $\mathcal{E}''$ sont dans W de dimension s, donc il y a une variété algébrique W_0 (sous-variété de W) minimale par rapport à $\mathcal{E}''$ et de dimension $s_0 \leq s$. Soit $\mathcal{E}_0$ le sous-ensemble infini de $\mathcal{E}''$ dont elle contient les éléments. γ^* est encore évidemment minimal par rapport à $\mathcal{E}_0$ pour la classe de Γ/γ^* considérée plus haut. Il y a au moins un point d'accumulation C des éléments de $\mathcal{E}_0$. Soit M_C la μ-variété congrue à la μ-variété $\{\gamma^*\}$ de γ^* et passant par C. Elle a une dimension $d \leq r$, Elle contient un sous-ensemble infini $\mathcal{E}_C$ d'éléments de $\mathcal{E}_0$ convergents vers le point C, et aucune μ-variété de dimension plus petite ne peut contenir un sous-ensemble infini de $\mathcal{E}_C$. W_0 et M_C ont une infinité de points communs convergents en C. Leur intersection est au voisinage de C une variété algébroïde qui a au moins une composante irréductible H de dimension $k \geq 1$ contenant un sous-ensemble infini $\mathcal{E}_C'$ de $\mathcal{E}_C$. H ne peut être contenu dans une variété algébrique de dimension moindre que celle de W_0, une telle sous-variété contiendrait les éléments du sous-ensemble infini $\mathcal{E}_C'$ de $\mathcal{E}_0$ ce qui est contradictoire avec le choix de W_0. Soit A un point régulier de H et non situé sur une autre des composantes de $W_0 \cap M_C$. $W_0 \cap M_A$ est au voisinage de A un élément analytique régulier I_A de dimension $k \geq 1$. Et I_A ne peut être contenu dans aucune variété algébrique de dimension inférieure à s_0 car une telle sous-variété contiendrait H ce qui est impossible. I_A ne peut être contenu dans aucune μ-variété de dimension inférieure à celle de M_A, car une telle μ-variété contenant I_A contiendrait H, donc l'ensemble infini $\mathcal{E}_C'$, ce qui est impossible. On peut donc appliquer à W_0 le lemme 2.2. Il en résulte que M_A est contenu dans une variété algébrique irréductible W de dimension $s \leq s_0 + d - 1$, $\leq s + r - 1 = \sigma - 1$. Il en résulte d'après le lemme 2.3 que σ coordonnées d'un point de M_A sont liées par une relation

$$x_{q_1}^{N_{q_1}} \ldots x_{q_\sigma}^{N_{q_\sigma}} = \text{constante}.$$

Donc pour les coordonnées des points de la μ-variété de γ^* et finalement pour celles des éléments de tout γ^* on obtient les relations annoncées.

Nous pouvons ajouter ce complément à l'énoncé:

p *étant un nombre naturel premier tel que les coordonnées des éléments de base de* Γ *soient des entiers* p*-adiques; tout sous-groupe de* Γ *distingué pour ce choix de* p, *et minimal par rapport à* $\mathfrak{E}'$ *pour au moins une claese de* Γ/γ *fournit un sous-groupe ayant les proprietés indiquées dans le théorème* 2.4.

Chapitre III. - **Equations diophantiennes.**

Considérons le système d'équations diophantiennes à résoudre en entiers rationnels X_i

$$(I)\qquad \begin{cases} (1) & \text{Norme } (X_1\omega_1 + \ldots + X_n\omega_n) = \pm 1 \\ (2) & F_j(X_1, \ldots, X_n) = 0 \qquad (j = 1, 2, \ldots, m) \end{cases}$$

où $(\omega_1, \ldots, \omega_n)$ représentent une base d'un corps de nombres algébriques fini K de degré n, et où les équations (2) sont des équations algébriques en $X_1, \ldots, X_n$ (que nous pouvons sans restreindre la généralité du problème supposer à coefficients rationnels).

A toute solution $(A_1, \ldots, A_n)$ en entiers rationnels de l'équation (1) correspond un entier de K, $\alpha = A_1\omega_1 + \ldots + A_n\omega_n$ dont la norme est ± 1, c'est-à-dire une unité de K. Réciproquement les composantes d'une unité de K par rapport à la base $(\omega_1, \ldots, \omega_n)$ fournissent une solution en entiers rationnels de (1).

Nous représenterons dans la suite tout nombre α de K par le point ayant pour coordonnées les n conjugués de α par rapport au corps des nombres rationnels

$$x_1 = \alpha^{(1)} = \alpha\,;\ x_2 = \alpha^{(2)}, \ldots,\ x_n = \alpha^{(n)}$$

dans l'espace X^n (X^n est toujours le produit topologique de n corps p-adiques identiques au corps p-adique algébriquement fermé H_p, qu'on a considéré dans les chapitres précédents, le choix du nombre naturel premier p étant indifférent).

La transformation linéaire non singulière

$$x_i = X_1\omega_1^{(i)} + \ldots + X_n\omega_n^{(i)} \qquad (i = 1, 2, \ldots, n)$$

où $\omega_j^{(1)}, \ldots, \omega_j^{(n)}$ sont les conjugués de $\omega_j = \omega_j^{(1)}$ peut être interprétée comme un changement des coordonnées dans X^n, Le système I définit une variété algébrique W de X^n qui a pour équations en x

$$(I')\qquad \begin{cases} (1') & x_1, \ldots, x_n = \pm 1 \\ (2') & f_j(x_1, \ldots, x_n) = 0. \qquad (j = 1, 2, \ldots, m) \end{cases}$$

Nous appellerons du même nom le nombre de K et le point qui le représente.

De la sorte *l'étude du système* I *est l'étude des unités de* K *appartenant à la variété algébrique* W. Nous énoncerons en général les résultats que nous obtiendrons sur le système I dans ce langage géométrique.

Le théorème de DIRICHLET sur les unités d'un corps algébrique fini nous apprend que ces unités forment un groupe abélien par rapport à la multiplication, admettant une base minima à r générateurs d'ordre infini, et un générateur d'ordre fini. r, que nous appellerons le *nombre de Dirichlet* de K, est défini de la façon suivante: soient r_1 le nombre de corps réels, $2r_2$ le nombre de corps complexes, parmi les n corps conjugués de K, $K^{(1)} = K, K^{(2)}, \ldots, K^{(n)}$, on a $r = r_1 + r_2 - 1$.

Les corps $K^{(1)}, \ldots, K^{(n)}$ étant isomorphes, les éléments conjugués à ceux d'une base minima des unités de K forment des bases minima des unités des corps conjugués correspondants. On voit que les unités de K sont représentées dans X^n par un groupe abélien multiplicatif de points dont les coordonnées sont des unités p-adiques, et ce groupe est de rang $r < n$. Nous pouvons donc lui appliquer le théorème (2.4). Nous obtenons ainsi:

THÉORÈME 3.1. — *Soit* $\mathfrak{E}$ *l'ensemble, supposé infini, des unités d'un corps de nombres algébriques* K *de degré* n, *de nombre de* DIRICHLET r, *qui appartiennent à une variété algébrique* W *de dimension* s. *A tout sous-ensemble infini* $\mathfrak{E}'$ *de* $\mathfrak{E}$ *il correspond au moins un sous-groupe* γ *du groupe* Γ *des unités de* K, *ayant les propriétés suivantes:*

1°) *il y a au moins une classe de* Γ/γ *qui contient un sous-ensemble infini d'élément de* $\mathfrak{E}'$;

2°) σ *quelconques des conjugués d'un élément de* γ, *soient* $\varepsilon^{(q_1)}, \ldots, \varepsilon^{(q_\sigma)}$, *satisfont à une relation indépendante du choix de l'élément dans* γ

$$\varepsilon^{(q_1)N_{q_1}} \ldots \varepsilon^{(q_\sigma)N_{q_\sigma}} = 1 \tag{3}$$

les N *étant des entiers rationnels non tous nuls, et* σ *étant égal à* $r + s$.

(*Le résultat devient trivial si l'on n'a pas* $s \leq n - r - 1$).

Nous avons donc obtenu une condition nécessaire pour l'existence d'une infinité de solutions en entiers rationnels au système I. Nous donnerons deux types d'applications de ce résultat à des systèmes I spécialisés, soit quant à la nature du corps K, soit quant à la nature de la variété W.

1° – Nous avons obtenu pour les unités de K appartenant au sous-groupe γ et leurs conjugués des relations (3) rationnelles entières à coefficients rationnels. En effectuant sur les conjugués des permutations du groupe de GALOIS G de K (nous entendons par là le groupe de GALOIS de l'équation rationnellement irréductible d'un élément primitif de K), nous

obtenons de nouvelles relations dont nous examinerons la compatibilité pour certains types de groupe de GALOIS.

2° - Comme il y a une classe de Γ/γ contenant une infinité des unités situées snr W, les unités correspondantes de γ sont sur une variété W' congrue à W. Nous examinerons la compatibilité des relations (3) avec les équations de W' quand les équations (2) du système I sont linéaires et homogènes (problème des unités dans un module).

Première application. — Soit G le groupe de GALOIS de K. Une opération de g est une permutation entre les nombres conjugués de K

$$\alpha^{(1)}, \ldots, \alpha^{(n)}$$
$$\alpha^{(h_1)}, \ldots, \alpha^{(h_n)}.$$

Dans l'espace des n variables $x_1, \ldots, x_n$, les transformations $(x_i \to x_{h_i})$ correspondantes, nous donnent une représentation du groupe de GALOIS dans X^n. Etant donné un vecteur issu de l'origine dans X^n, il lui correspond par ces transformations, des vecteurs que nous appelons les transformés du vecteur donné, par les permutations de G.

Considérons le corps K du théorème (3.1) et supposons qu'uue infinité d'unités de K appartiennent à une variété algébrique W de dimension $s \leq n - r - 1$. Le sous-groupe γ mis en évidence dans le théorème (3.1) est d'ordre infini. Il contient donc au moins une unité ε qui n'est pas une racine de l'unité. $n-1$ de ses conjugués, soient $\varepsilon^{(1)}, \ldots, \varepsilon^{(n-1)}$, satisfont à une relation $\varepsilon^{(1)N_1}, \ldots, \varepsilon^{(n-1)N_{n-1}} = 1$, les N_i étant des entiers rationnels non tous nuls. On en déduit en multipliant au besoin membre à membre cette égalité et l'égalité $(\varepsilon^{(1)} \ldots \varepsilon^{(n)})^h = 1$ une relation

$$\varepsilon^{(1)m_1} \ldots \varepsilon^{(n)m_n} = 1$$

où les m sont des entiers rationnels non tous égaux et tels que $m_1 + \ldots + m_n \neq 0$.

Considérons le vecteur $\vec{M}$ à coordonnées entières rationnelles $x_1 = m_1, \ldots, x_n = m_n$, et les vecteurs transformés de $\vec{M}$ par les permutations du groupe de GALOIS de K. Supposons qu'aucune sous-variété linéaire de l'espace de représentation ne contienne $\vec{M}$ et ses transformés. On peut choisir n de ces vecteurs linéairement indépendants, soient

$$\vec{M}_1(m_{11}, \ldots, m_{1n})$$
$$\vec{M}_n(m_{n1}, \ldots, m_{nn}).$$

L'unité ε considérée satisfait aux n relations :

$$\varepsilon^{(1)m_{11}} \dots \varepsilon^{(n)m_{1n}} = 1,$$
$$\varepsilon^{(1)m_{n1}} \dots \varepsilon^{(n)m_{nn}} = 1.$$

Le déterminant des m_{ij} est $\neq 0$. Soit d sa valeur. C'est un nombre entier rationnel. Donc les équations

$$\begin{aligned} y_1 m_{11} + \dots + y_n m_{n1} &= d \\ y_1 m_{12} + \dots + y_n m_{n2} &= 0 \\ \dots\dots\dots\dots\dots & \\ y_1 m_{1n} + \dots + y_n m_{nn} &= 0 \end{aligned}$$

ont une solution en entiers rationnels $q_1, \dots, q_n$ non tous nuls. De

$$(\varepsilon^{(1)m_{11}} \dots \varepsilon^{(n)m_{1n}})^{q_1} \dots (\varepsilon^{(1)m_{n1}} \dots \varepsilon^{(n)m_{nn}})^{q_n} = 1$$

on tire ainsi

$$(\varepsilon^{(1)})^d = 1$$

et ε serait une racine de l'unité, ce qui est contraire à l'hypothèse.

Si, au contraire, le vecteur $\vec{M}$ et ses conjugués sont dans un même sous-espace linéaire L, celui-ci est un sous-espace invariant dans la représentation considérée de G, et il est défini par des équations à coefficients rationnels. Il y a toujours dans cette représentation, quelle que soit la nature de G, deux sous-espaces invariants rationnels triviaux : le sous-espace $x_1 + \dots + x_n = 0$ et le sous-espace $x_1 = \dots = x_n$. L contenant le vecteur $\vec{M}$ étranger à ces deux sous-espaces, ne peut être confondu avec l'un d'eux. On a donc le théorème suivant :

THÉORÈME 3.2. — *Soient* K *un corps de nombres algébriques de degré* n, G *son groupe de* GALOIS. *Supposons que la représentation de* G *dans un espace de dimension* n *par des permutations des* n *coordonnées soit rationnellement complètement réduite quand on a mis en évidence les sous-espaces invariants triviaux* $x_1 = \dots = x_n$ *et* $x_1 + \dots + x_n = 0$. *Alors il est impossible qu'il y ait une infinité d'unités de* K *appartenant à une variété algébrique de dimension* $s \leq n - r - 1$, r *désignant le nombre de* DIRICHLET *de* K. *En particulier, il n'y a qu'un nombre fini d'unités dans un module de dimension* $h \leq n - r$ *de nombres de* K.

La valeur de la limite imposée à h est $n - r$ et non $n - r - 1$, car quand on assujettit des unités de K à être sur un module de dimension h, c'est-à-dire sur une variété linéaire de dimension h, on les assujettit par là même à être sur l'une des deux variétés algébriques de dimension $h - 1$,

intersections avec la variété linéaire précédente des variétés $x_1 \dots x_n = \pm 1$ (Cf. démonstration du théorème (3.4)).

Comme exemple de tels corps, il y a d'abord évidemment les corps ayant pour groupe de Galois, le *groupe symétrique*. En effet, s'il y avait un sous-espace invariant autre que les sous-espaces invariants totalement orthogonaux E_1 $x_1 = \dots = x_n$ et E_2 $x_1 + \dots + x_n = 0$, il y aurait un sous-espace invariant E_3 intérieur et non identique à E_2, donc de dimension $\leq n - 2$. Il y aurait donc un point à coordonnées $a_1, \dots, a_n$ non toutes nulles et non toutes égales, satisfaisant à une relation

$$a_1 m_1 + \dots + a_{n-1} m_{n-1} = 0$$

à coefficients non tous nuls, ainsi qu'à toute relation déduite de celle-ci en y remplaçant $a_1, \dots, a_n$ par une permutation quelconque de ceux-ci.

Supposons que m_1, par exemple, soit $\neq 0$. Effectuons la permutation qui échange m_1 en m_n en laissant les autres inchangés, on voit que $a_1 = a_n$ et parconséquent, grâce à une permutation convenable de G, $a_i = a_j$ quels que soient i et j, ce qui est contraire à l'hypothèse.

Un autre exemple de tels corps est donné par les corps *de degré* n *premier*. En effet, l'ordre du groupe de GALOIS G est un multiple de n, en vertu d'un théorème de CAUCHY ([12]), G contient un élément d'ordre n. Une permutation d'ordre n sur n éléments, n étant premier, est nécessairement formée d'un seul cycle, puisque l'ordre d'une permutation est égal au p. p. c. m. du nombre de termes de chaque cycle. S'il y avait un sous-espace invariant rationnel autre que E_1 et E_2 dans la représentation considérée de G, il y aurait un vecteur à composantes rationnelles $a_1, \dots, a_n$, non toutes égales, et de somme non nulle, tel que ses n transformés par la permutation cyclique, mise tout à l'heure en évidence, et ses puissances, ne soient pas indépendantes. Le déterminant

$$\Delta = \begin{vmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ a_2 & a_3 & \dots & a_n & a_1 \\ \dots & \dots & \dots & \dots & \dots \\ a_n & a_1 & \dots & a_{n-2} & a_{n-1} \end{vmatrix}$$

serait donc nul. Or, il est bien connu que

$$\Delta = (a_1 + a_2 + \dots + a_n)(a_1 + a_2\xi_1 + \dots + a_n\xi_1^{n-1})$$
$$(a_1 + a_2\xi_{n-1} + \dots + \xi a_n{}^{n-1}_{n-1})$$

([12]) SPEISER, *Theorie der Gruppen von endlicher Ordnung*, p. 64

$\xi_1, \ldots, \xi_{n-1}$ étant les racines de l'équation

$$\frac{x^n - 1}{x - 1} \equiv x^{n-1} + \ldots + x + 1 = 0$$

qui est rationnellement irréductible puisque n est premier.

Le facteur $a_1 + \ldots + a_n$ est $\neq 0$ par hypothèse, supposons que le facteur $a_1 + a_2\xi_1 + \ldots + a_n\xi_1^{n-1}$ par exemple soit nul. On a aussi $1 + \xi_1 + \ldots + \xi_1^{n-1} = 0$, et comme les a_i sont des nombres rationnels non tous nuls, et non tous égaux, on tirerait de ces deux relations une équation à coefficients rationnels de degré $n - 1$ pour ξ_1, ce qui est impossible. Δ est donc $\neq 0$, on arrive à une contradiction.

On a donc le résultat suivant:

THÉORÈME 3.3. — *Les résultats du théorème* 3.2 *s'appliquent en particulier à tous les corps pour lesquels le groupe* G *est le groupe symétrique, et à tous les corps de degré* n *premier.*

Par exemple, posons $\theta = 2^{1/29}$, alors pour $K = R(\theta)$, $n = 29$, $r_1 = 1$, $2r_2 = 28$, $r = 14$, $n - r = 15$. Il n'y a donc qu'un nombre fini de solutions en entiers rationnels X_i à l'équation

$$\text{Norme } (X_0 + X_1\theta + \ldots + X_{14}\theta^{14}) = \pm 1.$$

Deuxième application. — Sans faire d'hypothèse sur le groupe de Galois de K, nous étudions maintenant une infinité d'unités de K appartenant à un sous-module du module de dimension n par rapport au corps des rationnels, que forment les nombres du corps K.

Pour étudier les unités appartenant à un module de nombres algébriques, on peut évidemment supposer que la base du module a été amenée à la forme $1, \alpha_1, \ldots, \alpha_{h-1}$ par division par une des unités contenues dans le module initial.

Soit $K = R[\alpha_1, \ldots, \alpha_{h-1}]$ le corps obtenu en adjoignant $\alpha_1, \ldots, \alpha_{h-1}$ au corps R des rationnels. Soit n son degré. Représentons tout nombre de K comme d'habitude par le point ayant pour coordonnées ce nombre et ses conjugués. Les points du module sont sur la variété linéaire L de dimension h

$$(L) \qquad x_i = X_0 + X_1\alpha_1^{(i)} + \ldots + X_{h-1}\alpha_h^{(i)} \qquad (i = 1, 2, \ldots, n)$$

dans laquelle les $X_1, \ldots, X_{h-1}$ forment un système de coordonnées cartésiennes. Les unités sont sur l'une des variétés

$$(N) \qquad x_1 \ldots x_n = +1 \qquad\qquad (N') \qquad x_1, \ldots, x_n = -1.$$

L'intersection d'au moins l'une d'elles, soit N, avec L contient une infinité

d'unités de K. Cette intersection W a pour équation en X_i

$$\text{(W)} \qquad \prod_{i=1}^{n} (X_0 + X_1\alpha_1^{(i)} + \ldots + X_{h-1}\alpha_{h-1}^{(i)}) = 1.$$

Cette équation ne peut être une identité en X_i, car une telle identité entrainerait la proportionnalité d'au moins deux facteurs du produit. Soit

$$X_0 + X_1\alpha_1^{(i)} + \ldots + X_{h-1}\alpha_{h-1}^{(i)} \equiv \lambda(X_0 + X_1\alpha_1^{(j)} + \ldots + X_{h-1}\alpha_{h-1}^{(j)})$$

il en résulterait

$$\alpha_1^{(i)} = \alpha_1^{(j)}, \ldots, \quad \alpha_{h-1}^{(i)} = \alpha_{h-1}^{(j)}$$

ce qui est en contradiction avec le fait que K a été défini comme égal à $R[\alpha_1, \ldots, \alpha_{h-1}]$. W est donc une sous-variété algébrique de L dont les composantes irréductibles sont de dimension $h-1$. (On pourrait démontrer facilement qu'elle est en fait irréductible).

Supposons que, r étant toujours le nombre de DIRICHLET de K, on ait $h - 1 \leq n - r$, alors il résulte du théorème (3.1) qu'il y a un sous-groupe γ du groupe des unités de K, dont les coordonnées satisfont à une relation

$$x_1^{N_1} \ldots x_{n-1}^{N_{n-1}} = 1$$

les N étant des entiers rationnels non tous nuls. En la combinant à la relation à laquelle satisfont les coordonnées de toutes les unités considérées:

$$x_1 \ldots x_n = 1$$

on peut toujours obtenir une relation homogène

$$x_1^{q_1} \ldots x_n^{q_n} = 1 \qquad (q_1 + \ldots + q_n = 0)$$

où les q_i sont des entiers rationnels non tous nuls, à laquelle satisfont les coordonnées de tous les éléments de γ. D'autre part, nous savons aussi qu'il y a au moins une classe de Γ/γ qui contient une infinité des unités situées sur W. Soit ε_0 un représentant de cette classe. Posons

$$c = \varepsilon_0^{(1)q_1} \ldots \varepsilon_0^{(n)q_n}$$

il y a donc une infinité des unités situées sur W qui sont aussi sur la sous-variété C de L d'équation

$$\text{(C)} \qquad \prod_{i=1}^{n} (X_0 + X_1\alpha_1^{(i)} + \ldots + X_{h-1}\alpha_{h-1}^{(i)})^{q_i} = c.$$

Comme pour l'équation de W, on démontre que celle-ci ne peut être une

identité en X_i. Comme $q_1 + \ldots + q_n = 0$ elle représente un cône dans L. W n'étant pas un cône ne peut avoir en commun avec C que des variétés de dimension $h-2$ en nombre fini. On a donc le théorème:

THÉORÈME 3.4. — *Soit* M *un module d'entiers algébriques de dimension* h, *de base* $(1, \alpha_1, \ldots, \alpha_{h-1})$. *Soient* n *le degré*, r *le nombre de* DIRICHLET *du corps* $K = R[\alpha_1, \ldots, \alpha_{h-1}]$. *A tout ensemble infini* $\mathcal{E}$ *d'unités de* K *situées sur* M *correspond un sous-ensemble infini* $\mathcal{E}'$ *de* $\mathcal{E}$ *dont les éléments sont sur une variété de dimension* $h-2$.

Appliquons ce résultat à un module de dimension 2: comme une variété algébrique de dimension zéro se reduit à un nombre fini de points, il ne peut exister d'ensemble infini $\mathcal{E}'$. D'autre part, la condition $r \leq n-2$ peut se mettre sous la forme: le corps K n'a pas tous ses conjugués réels. On a donc:

THÉORÈME 3.5. — $K = R[\alpha]$ *étant un corps de nombres algébriques de degré* n, *dont les corps conjugués ne sont pas tous réels, il ne peut y avoir qu'un nombre fini d'unités du corps dans le module de base* $(1, \alpha)$.

On en deduit facilement: f(t) *étant une équation algébrique de degré* n *à coefficients rationnels, qui est rationnellement irréductible et dont les racines ne sont pas toutes réelles, l'équation*

$$F(X, Y) = 1 \quad \text{où} \quad F(X, Y) \equiv Y^n f\left(\frac{X}{Y}\right)$$

n'a qu'un nombre fini de solutions en entiers rationnels X, Y.

C'est le résultat de THUE, restreint au cas où l'équation $f(t)$ n'a as toutes ses racines réelles; il est obtenu indépendamment de l'étude de l'approximation des nombres algébriques par les nombres rationnels. Le travail de M. SKOLEM cité dans l'introduction donnait déjà ce résultat.

Le théorème (3.4) appliqué au cas d'un module de dimension 3, nous montre que si $r \leq n-3$, et si $\mathcal{E}$ désigne l'ensemble d'une infinité d'unités contenues dans le module, $\mathcal{E}$ admet un sous-ensemble infini $\mathcal{E}'$ dont les éléments appartiennent à une courbe algébrique. En utilisant alors un résultat de M. SIEGEL sur les courbes algébriques contenant une infinité de points dont les coordonnées sont des entiers rationnels ou des entiers d'un même corps algébrique fini, nous pouvons démontrer un résultat plus précis. Ce résultat, à l'encontre des précédents, n'est plus indépendant des travaux sur l'approximation des nombres algébriques, puisque le théorème de M. SIEGEL qu'on utilise, tire de là son origine.

LEMME 3.6. — *Soient* K *un corps algébrique de degré* n *et* $(\omega_1, \ldots, \omega_n)$ *une base des entiers de ce corps. Soit* (N) *la variété Norme* $(X_1\omega_1 + \ldots + X_n\omega_n) = 1$.

Supposons qu'une courbe algébrique irréductible C *contienne une infinité de points à coordonnées* $X_1, \ldots, X_n$ *entières rationnelles, de* (N), *alors* K *doit contenir un sous-corps quadratique réel* k *et les points entiers de* C *correspondent à des unités de* K *qui forment une classe de restes du groupe des unités de* K *par rapport au sous-groupe des unités à norme positive de* k.

Le même résultat subsiste si on substitue à N *la variété* (N')

$$\text{Norme } (X_1\omega_1 + \ldots + X_n\omega_n) = -1.$$

La courbe C contenant une infinité de points entiers, admet ([13]) une représentation paramétrique des X_i par des polynômes en t et t^{-1}, donc

$$x_i = X_1\omega_1^{(i)} + \ldots + X_n\omega_n^{(i)} = \frac{P_i(t)}{t^{h_i}}. \qquad (i = 1, 2, \ldots, n)$$

On a $x_1 \ldots x_n = 1$, donc $x_i = \lambda_i t^{m_i}$, les λ_i désignant des constantes et les m_i des entiers rationnels avec $\sum_{i=1}^{n} m_i = 0$. Soient $x_i = \varepsilon_0^{(i)}$ les coordonnées d'un point entier fixe de C. $x_i = \varepsilon^{(i)}$ celles d'un point entier quelconque de C, les $\varepsilon_0^{(i)}$. $\varepsilon^{(i)}$, sont des unités de K et leurs conjugués. Posons $u_i = \frac{\varepsilon^{(i)}}{\varepsilon_0^{(i)}}$; $u_1, \ldots, u_n$, sont les conjugués d'une même unité de K; on a pour $f = 1, \ldots, n$; $g = 1, \ldots, n$

$$u_f^{m_f} = u_g^{m_g}.$$

Soit T_{fg} la transformation du groupe de GALOIS de K qui transforme u_f en u_g; cette transformation est permutable avec l'élévation à une puissance entière rationnelle. On a donc

$$u_f^{m_g} = T_{fg}\, u_f^{m_f}$$
$$u_f^{(m_g^2)} = T_{fg} u_f^{m_f m_g} = T_{fg}^2 u_f^{(m_f^2)}$$

et plus généralement

$$u_f^{(m_g^q)} = T_{fg}^q u_f^{(m_f^q)}.$$

Soit Q l'ordre de T_{fg}; donnons à q la valeur Q. Il vient

$$u_f^{(m_g^Q)} = u_f^{(m_f^Q)}.$$

Comme il y a une infinité d'unités ε donc d'unités u différentes, elles ne

([13]) C.-L. SIEGEL, « Abh. Preuss. Akad. Wiss. », n. 1, 1929, p. 45

peuvent toutes être des racines de l'unité, donc $m_g^Q = m_f^Q$, et comme m_f, m_g sont des entiers rationnels, Q un nombre naturel, on a $m_g = \pm m_f$. Les exposants m_i ne sont donc susceptibles que de deux valeurs au plus $\pm m$, donc $u_{(i)} = t_i^{\pm m}$. Les unités u ont donc au plus deux conjugués distincts; donc elles sont rationnelles ou quadratiques. Comme il y a une infinité de ces unités distinctes, ce sont des unités de corps quadratiques réel.

Il y a un nombre fini de sous-corps quadratiques réels de K, il y en a donc un, soit k qui contient une infinité des unités u. La courbe C' d'équation $x_i = \pm t_i^m$ a donc une infinité de points communs avec l'hyperbole H qui porte les unités à norme positive de k, ou avec l'hyperbole H' qui porte les unités à norme négative de k. Elle est donc confondue avec H ou H'. Dans les deux cas, on voit que C correspond à H dans l'une des transformations $X_i' = {}^{(i)}x_i$ $(i = 1, 2, \ldots, n)$. Le résultat subsisterait si on était parti d'une courbe C située sur N'. La propriété énoncée dans le lemme en résulte immédiatement.

THÉORÈME 3.7. — *Soit un module* M_3 *de nombres algébriques de base* $(1, \alpha, \beta)$. *Supposons que le corps* $K = R[\alpha, \beta]$ *ait au moins deux paires de corps conjugués imaginaires. La condition nécessaire et suffisante pour qu'il y ait une infinité d'unités de* K *appartenant à* M_3, *est que* M_3 *contienne deux nombres* φ, ψ, *dont le quotient soit un nombre quadratique réel* $\theta = \frac{\psi}{\varphi}$, φ *étant une unité de* K. *Soit* ε *l'unité fondamentale du sous-corps* $k = R[\theta]$ *de* K, *toutes les unités* $\varphi\varepsilon^n$ (n, *entier rationnel*) *appartiennent à* M_3 *et toutes les unités contenues dans* M_3 *à un nombre fini d'exceptions près, sont données par cette formule.*

K ayant au moins deux paires de conjugués imaginaires, son nombre de DIRICHLET satisfait à l'inégalité $r < n - 3$. On peut donc appliquer le théorème 3.4.

De tout ensemble infini des unités de K appartenant au module, on peut extraire un sous-ensemble infini dont les éléments sont situés sur une courbe algébrique. Cette courbe doit être, en vertu du lemme précédent, la transformée d'une hyperbole portant les unités à norme positive d'un sous-corps quadratique réel $k = R[\theta]$ de K, par une transformation $(x_i \to \varphi^{(i)}x_i)$ φ étant une unité fixe de K. Le module M_3 contient donc le module de base $(\varphi, \varphi\theta)$ transformé du module des nombres de k. Il contient donc toutes les unités données par la formule $\varphi\varepsilon^n$, ε étant l'unité fondamentale de k, et n un entier rationnel quelconque. Si les unités de M_3 ne sont pas, à un nombre fini d'exceptions près, données par cette formule, le raisonnement précédent montre que M_3 contient encore un autre module de base $(\varphi', \varphi'\theta')$, θ' étant aussi

un nombre quadratique réel, appartenant à K. Mais ceci est impossible. En effet, φ. $\varphi\theta$, φ', $\varphi'\theta'$, formeraient une base (surabondante) de M_3. Ils ne seraient pas rationnellement indépendants; $\frac{\varphi'}{\varphi}$ serait le quotient de deux nombres quadratiques réels, donc un nombre totalement réel. Le module M_3' de base $1, \frac{\varphi}{\theta}, \frac{\varphi'}{\varphi}, \frac{\varphi'}{\varphi}\theta'$ ne contiendrait que des nombres totalement réels. Comme M_3 contient le nombre 1, M_3' contiendrait le nombre $\frac{1}{\varphi}$, qui serait donc totalement réel; φ, et par conséquent φ', auraient aussi cette propriété, et M_3 serait composé de nombres totalement réels, ce qui est contraire aux hypothèses. Le théorème est donc démontré.

Remarquons que si le degré de K est impair, K ne peut avoir de sous-corps quadratique. Il ne peut y avoir qu'un nombre fini d'unités dans M_3. Si en particulier K est de degré 5, nous obtenons le résultat de M. SKOLEM, cité dans l'introduction. C'est aussi d'ailleurs un cas particulier du théorème (3.3) puisque 5 est un nombre premier.

Nous allons maintenant déduire du résultat précédent un théorème sur l'approximation de 0 par des formes linéaires et homogènes à trois variables à coefficients algébriques, pour des valeurs entières rationnelles des variables. Considérons une telle forme, nous pouvons sans restreindre la généralité, l'écrire $X + Y\alpha + Z\beta$, α et β étant des entiers algébriques. Soit n le degré de $K = R[\alpha, \beta]$. Posons $H = |X| + |Y| + |Z|$ (la valeur absolue étant la valeur absolue ordinaire). Comme Norme $(X + Y\alpha + Z\beta)$, pour X, Y, Z entiers rationnels quelconques, est nécessairement un entier rationnel, il est trivial qu'il y a une constante positive c_0 telle que $|X + Y\alpha + Z\beta| > \frac{c_0}{H^{n-1}}$ quels que soient X, Y, Z entiers rationnels. Nous allons démontrer le résultat plus précis suivant:

THÉORÈME 3.8. — *Si le corps* $K = R[\alpha, \beta]$ *de degré* n *a au moins deux paires de corps conjugués imaginaires, l'inégalité*

$$|X + Y\alpha + Z\beta| < \frac{c}{H^{n-1}} \quad \text{où} \quad (H = |X| + |Y| + |Z|)$$

n'a qu'un nombre fini de solutions en entiers rationnels X, Y, Z, *quelle que soit la constante positive* c.

Posons

$$A = \max(1, |\alpha^{(1)}|, |\beta^{(1)}|, \ldots, |\alpha^{(n)}|, |\beta^{(n)}|).$$

Supposons que l'inégalité ait une infinité de solutions en entiers rationnels X, Y, Z. Soient $\varphi = X + Y\alpha + Z\beta$ les entiers de K correspondant à ces solutions. On a

$$\text{Norme } \varphi = (X + Y\alpha + Z\beta) \prod_{i=2}^{n} (X + Y\alpha^{(i)} + Z\beta^{(i)})$$

donc

$$|\text{Norme } \varphi| \leq \frac{c}{H^{n-1}} A^{n-1} H^{n-1} = c'.$$

Ainsi les nombres $|\text{Norme } \varphi|$ étant des entiers rationnels bornés, ne peuvent prendre qu'un nombre fini de valeurs. Les idéaux principaux (φ) ne représentent qu'un nombre fini d'idéaux distincts. Il y a au moins un de ces idéaux qui est identique à l'idéal principal d'une infinité de nombres φ, soient $\varphi_0, \varphi_1, \ldots, \varphi_m, \ldots$.

On a $(\varphi_0) = (\varphi_m)$, donc $\frac{\varphi_m}{\varphi_0} = \varepsilon$, ε étant une unité de K. Il y a donc une infinité d'unités dans le module de base $\left(\frac{1}{\varphi_0}, \frac{\alpha}{\varphi_0}, \frac{\beta}{\varphi_0}\right)$. Alors on peut facilement montrer grâce au théorème 3.8 que K contient un sous-corps quadratique réel $k = R[\theta]$, que le module initial contient un sous-module $(\lambda, \lambda\theta)$, et que les nombres φ correspondant aux solutions en entiers rationnels de l'inégalité étudiée, sont à un nombre fini d'exceptions près, des nombres de ce sous-module $\varphi = \lambda(X' + X'\theta)$, X', Y' étant des entiers rationnels. Posons $H' = |X'| + |Y'|$, θ étant quadratique $|X' + Y'\theta| < \frac{c''}{H'^{1+q}}$ n'a qu'un nombre fini de solutions, quelles que soient les constantes réelles positives c'' et q. Mais on voit facilement qu'il y a une constante positive c''' telle que $H' < c'''H$. Une infinité de ces nombres ne peut donc satisfaire à $|\varphi| < \frac{c}{H^{n-1}}$ puisque n est supérieur à 4. On arrive donc à une contradiction et le théorème est démontré.

Notons que: le résultat du théorème (3.8) n'est plus précis que celui qu'on peut tirer des résultats de SIEGEL (« Math. Zeit. », Bd. 10, 1921) que quand n est < 57.

REMARQUE. — L'exemple simple auquel nous faisions allusion dans l'introduction, de variétés algébriques contenant une infinité d'unités de K est le suivant: Supposons que K contienne des unités ε satisfaisant avec leurs conjugués à un système de relations

$$\varepsilon^{(1)^{N_{1j}}} \ldots \varepsilon^{(n)^{N_{nj}}} = +1 \qquad (j = 1, 2, \ldots, h)$$

les N étant des entiers rationnels non tous nuls; toutes les unités du sous-

groupe γ engendré par ces unités, satisfont à ces relations. Si au moins l'une d'elles n'est pas une racine de l'unité, ce sous-groupe est d'ordre infini, et la variété algébrique

$$(W^*) \qquad x_1^{N_{1j}} \dots x_n^{N_{nj}} = 1 \qquad (j = 1, 2, \dots, h)$$

« contient une infinité d'unités » dans notre représentation habituelle des nombres de K.

De même η étant une unité quelconque de K

$$(W^{*\prime}) \qquad x_1^{N_{1j}} \dots x_n^{N_{nj}} = \eta^{(1)N_{1j}} \dots \eta^{(n)N_{nj}} \qquad (j = 1, 2, \dots, h)$$

contient une infinité d'unités: toutes les unités de la classe de Γ/γ de représentant η.

Soient W_1^*, W_2^*, ... les variétés algébriques irréductibles de dimension minima du type W^*, contenant au moins une unité de K non racine de l'unité, donc un sous-groupe d'ordre infini de Γ. La conjecture dont nous parlions dans l'introduction est la suivante: si une variété algébrique V contient une infinité d'unités, c'est qu'elle contient comme sous-variétés, des variétés W_i^*, ou des variétés congrues à des variétés W_i^* en nombre fini, et que les sous-groupes γ_i de Γ ou les classes de Γ/γ_i correspondant à ces sous-variétés ont tous leurs éléments contenus dans V, et donnent toutes les unités contenues dans V, à un nombre fini d'unités près. Alors si V est un hyperplan passant par l'origine (unités dans un module) les sous groupes γ_i mis en évidence seraient nécessairement les groupes des unités de sous-corps de K.

Remarquons que pour une variété algébrique V quelconque cette dernière proprieté des γ_i n'est sûrement pas nécessaire, comme on peut le voir par des exemples simples. Par exemple, considérons le corps k formé par l'adjonction à un corps k_1 de degré p_1 premier, d'un corps de degré p_2, premier. Soit N_1 la variété algébrique portant les unités à norme positive de k_1, N_2 la variété portant sur les unités à norme positive de k_2, la variété $N_1 \cdot N_2$ dans la représentation habituelle de k, contient toutes les unités d'un sous-groupe du groupe Γ des unités de K, qui n'est sûrement pas le groupe des unités d'un sous-corps de K, ni la réunion d'un nombre fini de classes de Γ par rapport à de tels sous-groupes.

Les résultats obtenus dans ce travail sont bien en accord avec la conjecture énoncée. Dans le cas étudié par le théorème (3.2), il ne peut exister de variété W^* (autre que les variétés triviales, d'équations $x_1 \dots x_n = \pm 1$), et nous trouvons que sur aucune des variétés que nous considérons il ne peut y

avoir une infinité d'unités. Dans le théorème (3.7) la condition nécessaire et suffisante obtenue, pour l'existence d'une infinite d'unités dans les modules de dimension 3 considerés, est que la variété linéaire que définit le module, contienne une variété congrue à la variété formée par les 2 hyperboles portant les unités d'un sous-corps quadratique réel de K, hyperboles qui sont bien des variétés W^*. Et l'on a bien ainsi toutes les unités contenues dans le module, à un nombre fini d'exceptions près peut-être.