Séminaire Delange-Pisot-Poitou. Théorie des nombres

Gabriel Archinard

Théorie de Chabauty sur les équations diophantiennes, I

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 7, n° 2 (1965-1966), exp. n° 16, p. 1-23

<http://www.numdam.org/item?id=SDPP_1965-1966__7_2_A5_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
7e année, 1965/66, n° 16

18 avril 1966
(Rédaction corrigée en mars 1967)

THÉORIE DE CHABAUTY SUR LES ÉQUATIONS DIOPHANTIENNES, I.

par Gabriel ARCHINARD

Introduction. - La thèse de Claude CHABAUTY [2] se divise en trois chapitres de la manière suivante :

Chapitre I : Séries entières à coefficients p-adiques.

Chapitre II : Groupe abélien de points.

Chapitre III : Equations diophantiennes.

Dans les deux premiers chapitres, C. CHABAUTY étudie certaines séries entières à coefficients p-adiques à n variables, prises dans le corps des coefficients, et, par des procédés de géométrie algébrique, démontre un théorème qui peut être considéré comme le théorème central de sa thèse. Le troisième chapitre est une suite d'applications de ce théorème à la théorie des nombres algébriques et à celle des équations diophantiennes.

Les deux premiers chapitres ont déjà fait l'objet d'une conférence à ce Séminaire et l'on se bornera, ici, à exposer le troisième chapitre, après un rappel, sans démonstration, du théorème central.

1. Rappel concernant les variétés algébriques [5], [6]

Soient k un corps commutatif et K un corps algébriquement clos, contenant k, et soit

$$f_i(X_1 , \dots , X_n) = f_i(X) , \quad i = 1 , 2 , \dots , m ,$$

une famille finie de polynômes de l'anneau $k[X_1 , \dots , X_n] = k[X]$.

On peut alors considérer l'ensemble E des éléments $(x_1 , \dots , x_n) = x \in K^n$ tel que $f_i(x) = 0 , \quad i = 1 , 2 , \dots , m$.

DÉFINITION 1.1. - Un tel ensemble E est une k-variété algébrique affine dans K^n .

Remarque. - E est aussi l'ensemble des zéros dans K^n de l'idéal

$$\alpha = (f_i(X))_{i=1,2,\dots,m}$$

engendré dans $k[X]$ par la famille $f_i(X)$, $i = 1 , 2 , \ldots , m$.

Comme l'anneau $k[X]$ est noethérien (Basissatz de Hilbert), l'ensemble $V(\alpha)$ des zéros communs des polynômes d'un idéal α de $k[X]$ est une k-variété algébrique affine de K^n (c'est l'ensemble des zéros d'une famille finie de générateurs de α dans $k[X]$).

On dira que $V(\alpha)$ est la variété algébrique affine associée à l'idéal α .

Inversement, on voit que l'ensemble $i(E)$ des polynômes de $k[X]$, qui s'annulent sur un sous-ensemble quelconque E de K^n , est un idéal de $k[X]$; on l'appelle idéal associé de E .

PROPRIÉTÉ 1.1. - D'après le théorème des zéros de Hilbert (Nullstellensatz), on a

$$V(\alpha) \neq \emptyset \iff \alpha \neq k[X] \quad .$$

On en tire l'existence de variétés non vides.

PROPRIÉTÉ 1.2. - On a

$$i(V(\alpha)) \supset \alpha \quad , \qquad i(V(i(E))) = i(E) \quad ,$$

$$V(i(E)) \supset E \quad , \qquad V(i(V(\alpha))) = V(\alpha) \quad .$$

DÉFINITION 1.2. - Une k-variété algébrique affine de K^n est dite réductible si elle peut être exprimée comme réunion finie non triviale d'autres k-variétés algébriques affines, c'est-à-dire : V est réductible si

$$V = V_1 \cup V_2 \quad \text{avec} \quad V_i \neq V \quad .$$

Dans le cas contraire, la variété est irréductible (cette notion dépend de k).

THÉORÈME 1.1. - Une k-variété algébrique affine V est irréductible si, et seulement si, son idéal associé $i(V)$ dans $k[X]$ est premier.

THÉORÈME 1.2. - Toute k-variété algébrique affine s'exprime de manière unique comme réunion finie de k-variétés algébriques irréductibles qui sont ses composantes irréductibles, i. e.

$$V = \cup V_i \quad , \qquad V_i \text{ irréductibles.}$$

DÉFINITION 1.3. - Soit V une k-variété algébrique affine irréductible. La dimension de V est alors celle de $i(V)$ dans $k[X]$, i. e.

$$\dim V = \dim i(V)$$

= degré de transcendance sur k du corps des fractions de $k[X]/i(V)$.

C'est aussi le nombre s d'idéaux premiers différents de $i(V)$ et de $k[X]$ dans une chaîne maximale

$$i(V) < p_1 < \ldots < p_s < k[X] \ .$$

C'est donc le nombre maximum d'indéterminées, soient X_{i_1} , ... , X_{i_s} , telles qu'aucun polynôme de $i(V)$ ne contienne que X_{i_1} , ... , X_{i_s} . On voit par cette définition qu'une variété de dimension 0 ne contient qu'un nombre fini de points et, d'autre part, que l'on a $0 \leqslant \dim V \leqslant n$. On dira d'une variété quelconque qu'elle est de dimension s , si s est le maximum des dimensions de ses composantes irréductibles. Si toutes les composantes irréductibles d'une variété ont même dimension, on dit que cette variété est équidimensionnelle.

THÉORÈME 1.3. - Soit α un idéal de $k[X]$, engendré par la famille $f_i(X)$, $i = 1 , 2 , \ldots , s$, et supposons les $f_i(X)$ algébriquement indépendants sur k . Alors, $\dim V(\alpha) = n - s$, et $V(\alpha)$ est équidimensionnelle.

Soit k' un corps tel que $k \subset k' \subset K$, et soit α un idéal de $k[X]$ engendré par $f_i(X)$, $i = 1 , 2 , \ldots , m$. On peut être amené à considérer l'idéal $\mathfrak{A}$, engendré dans $k'[X]$ par les $f_i(X)$.

THÉORÈME 1.4. - On a alors $V(\alpha) = V(\mathfrak{A})$ dans K^n , et si $V(\alpha)$ est une k-variété équidimensionnelle, $V(\mathfrak{A})$ est une k'-variété équidimensionnelle, et l'on a

$$\dim V(\alpha) = \dim V(\mathfrak{A}) \ .$$

Si p est un idéal premier de $k[X]$, l'idéal p^e , qui lui correspond dans $k'[X]$, n'est pas forcément premier, ce qui montre que la notion d'irréductibilité d'une k-variété algébrique affine dépend de k .

Considérons un exemple qui sera utile dans la suite de l'exposé.

Soit K un corps algébrique sur Q , et soit L un sous-espace vectoriel de K^n considéré comme un espace vectoriel sur K , de base $(\omega_{i1} , \omega_{i2} , \ldots , \omega_{in})$, $i = 1 , 2 , \ldots , h$; supposons $h < n$, et posons $k = Q[(\omega_{ij})]$. On peut prendre l'ordre des indices de telle sorte que

$$\Delta = \begin{vmatrix} \omega_{11} & \omega_{21} & \cdots & \omega_{h1} \\ \omega_{12} & \omega_{22} & \cdots & \omega_{h2} \\ \cdots & \cdots & \cdots & \cdots \\ \omega_{1h} & \omega_{2h} & \cdots & \omega_{hh} \end{vmatrix} \neq 0 \ .$$

Soit $x = (x_1 , x_2 , \dots , x_n)$ un point quelconque de L , on a alors

$$x_i = \lambda_1 \omega_{1i} + \lambda_2 \omega_{2i} + \dots + \lambda_h \omega_{hi} , \quad i = 1 , 2 , \dots , n \text{ avec } \lambda_i \in K .$$

D'après les formules de Cramer, on a

$$\lambda_j = \frac{1}{\Delta} \begin{vmatrix} \omega_{1,1} & \cdots & \omega_{j-1,1} & x_1 & \omega_{j+1,1} & \cdots & \omega_{h,1} \\ \omega_{1,2} & \cdots & \omega_{j-1,2} & x_2 & \omega_{j+1,2} & \cdots & \omega_{h,2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \omega_{1,h} & \cdots & \omega_{j-1,h} & x_h & \omega_{j+1,h} & \cdots & \omega_{h,h} \end{vmatrix} = \Delta_j(x_1 , \dots , x_h) ,$$

$$j = 1 , 2 , \dots , h$$

$\Delta_j(X_1 , \dots , X_h)$ étant une forme linéaire homogène de $k[X_1 , \dots , X_h]$. On a donc

$$x_{h+k} = \Delta_1(x_1 , \dots , x_h)\omega_{1,h+k} + \dots + \Delta_h(x_1 , \dots , x_h)\omega_{h,h+k}$$

$$= f_{h+k}(x_1 , \dots , x_h) , \text{ avec } k = 1 , 2 , \dots , n - h ,$$

pour tous les points de L ; soit

$$F_k(x_1 , \dots , x_n) = x_{h+k} - f_{h+k}(x_1 , \dots , x_h) = 0 , \quad k = 1 , \dots , n - h .$$

Donc $L \subset V(\alpha)$, α étant l'idéal de $k'[X_1 , \dots , X_n]$ engendré par la famille $F_k(X)$.

Inversement, soit $x = (x_1 , \dots , x_n) \in V(\alpha)$, alors

$$x_{h+k} = \Delta_1(x_1 , \dots , x_h)\omega_{1,h+k} + \dots + \Delta_h(x_1 , \dots , x_h)\omega_{h,h+k} ,$$

$$k = 1 , 2 , \dots , n - h$$

et on a les identités

$$x_i = \Delta_1(x_1 , \dots , x_h)\omega_{1i} + \dots + \Delta_h(x_1 , \dots , x_h)\omega_{hi} , \quad i = 1 , 2 , \dots , h .$$

Donc $V(\alpha) \subset L$, et finalement on a

$$L = V(\alpha) .$$

Les polynômes $F_k(X_1 , \dots , X_n) = X_{h+k} - f_{h+k}(X_1 , \dots , X_n)$ étant algébriquement indépendants sur k et sur toute extension algébrique de k , $V(\alpha)$ est une k'-variété algébrique affine de dimension $n - (n - h) = h$, équidimensionnelle.

De plus, l'idéal $(iV(\alpha))$, considéré dans $K[X]$, est premier.

Soit en effet

$$\mathbf{F(X)}\ G(X) \in \mathfrak{i}(V(\alpha)) \ .$$

Considérons $F^*(\lambda_1 , \ldots , \lambda_h)$, obtenu en remplaçant, dans $F(X_1 , \ldots , X_h)$, X_i par $\lambda_1 \omega_{1i} + \ldots + \lambda_h \omega_{hi}$ pour $i = 1 , 2 , \ldots , n$. On a alors

$$F^*(\lambda_1 , \ldots , \lambda_h).G^*(\lambda_1 , \ldots , \lambda_h) = 0$$

pour toutes les valeurs (en nombre infini) de $\lambda_i \in K$. Donc, on a l'identité

$$F^*(\lambda_1 , \ldots , \lambda_h).G^*(\lambda_1 , \ldots , \lambda_h) \equiv 0$$

et (par exemple) $F^*(\lambda_1 , \ldots , \lambda_h) \equiv 0$, ceci montre que

$$F(X) \in \mathfrak{i}(V(\alpha)) \ .$$

On a ainsi montré que tout sous-espace vectoriel de K^n est une k-variété algébrique affine irréductible de dimension égale à celle de sous-espace vectoriel.

2. Théorème central (CHABAUTY [2], chapitre II, théorème 2.4)

On considère un groupe multiplicatif Γ de points $(a_1 , a_2 , \ldots , a_n)$ à n coordonnées a_i algébriques sur Q (corps des rationnels), la multiplication étant définie par

$$(a_1 , a_2 , \ldots , a_n)(b_1 , b_2 , \ldots , b_n) = (a_1.b_1 , a_2.b_2 , \ldots , a_n.b_n) \ .$$

On suppose que Γ est de type fini et possède une base minimale comprenant r éléments d'ordre infini.

Soit p un idéal premier dans $k[X_1 , \ldots , X_n]$, de dimension s (k étant une extension algébrique quelconque de Q) telle que $\sigma = s + r \leqslant n$.

Alors, s'il existe un sous-ensemble infini E de Γ , dont les points sont des zéros de p , il existe aussi un sous-groupe γ de Γ ayant les propriétés suivantes :

1° Une classe au moins $\overline{a} \in \Gamma/\gamma$ contient une infinité de points de E ,

2° A tout système d'entiers rationnels q_i , $i = 1 , \ldots , \sigma$, tels que

$$1 \leqslant q_1 < q_2 \leqslant \ldots \leqslant q_\sigma \leqslant n \ ,$$

correspond une suite d'entiers rationnels non tous nuls $N_{q_1} , \ldots , N_{q_\sigma}$ tels que

$$e_{q_1}^{N_{q_1}} \times e_{q_2}^{N_{q_2}} \times \ldots \times e_{q_\sigma}^{N_{q_\sigma}} = 1 \ , \quad \forall\ e = (e_1 \ , \ \ldots \ , \ e_n) \in \gamma \ .$$

Remarque. - Pour la démonstration, on choisit un nombre premier p tel que les coordonnées des points de Γ soient des unités p-adiques (i. e. valeur absolue p-adique, $|a_i|_p \leqslant 1$, $i = 1 \ , \ 2 \ , \ \ldots \ , \ n$, $\forall\ a \in \Gamma$), et l'on plonge le sous-ensemble E dans la k-variété algébrique affine $V(p)$ de Ω_p^n (Ω_p étant la clôture algébrique du corps p-adique Q_p). On peut alors appliquer les théorèmes établis précédemment.

3. Le chapitre III de CHABAUTY [2]

(A) Généralités.

Soit K un corps de nombres algébriques de degré n (extension algébrique de Q , de degré n) ; soient $(\omega_1 \ , \ \omega_2 \ , \ \ldots \ , \ \omega_n)$ une base d'entiers de K et $(\omega_1^{(i)} \ , \ \omega_2^{(i)} \ , \ \ldots \ , \ \omega_n^{(i)})$, $i = 1 \ , \ 2 \ , \ \ldots \ , \ n$, les bases conjuguées.

On se propose d'étudier la possibilité d'existence d'une infinité de solutions en entiers rationnels au système d'équations :

$$(I) \quad \begin{cases} (1) \quad \text{Norme}(X_1\ \omega_1 + \ldots + X_n\ \omega_n) = \prod_{i=1}^{n} (X_1\ \omega_1^{(i)} + \ldots + X_n\ \omega_n^{(i)}) = \pm\ 1 \\ \\ (2) \quad F_j(X_1 \ , \ \ldots \ , \ X_n) = 0 \ , \quad j = 1 \ , \ 2 \ , \ \ldots \ , \ m \ , \end{cases}$$

où $F_j(X_1 \ , \ \ldots \ , \ X_n) \in k[X_1 \ , \ \ldots \ , \ X_n]$, k étant un corps de nombres algébriques.

Il est évident qu'à toute solution en entiers rationnels $A_1 \ , \ A_2 \ , \ \ldots \ , \ A_n$ correspond une unité de K : $a = A_1\ \omega_1 + \ldots + A_n\ \omega_n$.

On cherche donc les points à coordonnées entières rationnelles d'une K^*-variété dans Ω^n , où K^* est une extension algébrique de Q contenant k et K , et où Ω est un corps algébriquement clôs contenant Q (donc aussi K^*).

La transformation affine

$$x_i = X_1\ \omega_1^{(i)} + X_2\ \omega_2^{(i)} + \ldots + X_n\ \omega_n^{(i)} \ , \quad i = 1 \ , \ 2 \ , \ \ldots \ , \ n$$

transforme les équations (I) en

$$(I') \quad \begin{cases} (1') \quad x_1 x_2 \dots x_n = \pm 1 \\ (2') \quad f_j(x_1 , x_2 , \dots , x_n) = 0 , \quad j = 1 , 2 , \dots , m , \end{cases}$$

où $F_j(X_1 , \dots , X_n) = f_j(X_1 \omega_1^{(1)} + \dots + X_n \omega_n^{(1)} , \dots , X_1 \omega_1^{(n)} + \dots + X_n \omega_n^{(n)})$ et $f_j(x_1 ; \dots , x_n) \in K^*[x_1 , \dots , x_n]$.

Comme $[\text{dét}(\omega_j^{(i)})]^2 =$ discriminant de $K \neq 0$, la transformation est régulière et les solutions de (I) et de (I') se correspondent bijectivement, en particulier les solutions en entiers rationnels correspondent bijectivement aux solutions de (I') dont les coordonnées sont des unités algébriques de K conjuguées. Les K^*-variétés correspondant aux équations (I) et (I') sont de même dimension, et ont simultanément la propriété d'être réductible ou irréductible.

Par la suite, on dira d'un nombre $x \in K$ qu'il est situé sur une variété $V \subset \Omega^n$ si $(x^{(1)} , x^{(2)} , \dots , x^{(n)}) \in V$.

L'existence de solutions en entiers rationnels des équations (I) est donc ramenée à l'existence d'unités $e = e^{(1)} \in K$ situées sur la K^*-variété associée à l'idéal engendré dans $K^*[x]$ par les polynômes $f_j(x_1 , \dots , x_n)$, $j = 1 , 2 , \dots , m$.

Or, d'après un théorème de Dirichlet, le groupe des unités de K est de type fini, et a une base formée d'un élément d'ordre fini et de r éléments d'ordres infinis, avec $r = r_1 + r_2 - 1$, où r_1 est le nombre de corps conjugués réels de $K = K^{(1)}$ et $2r_2$ le nombre de ses corps conjugués complexes.

On appelle r , nombre de Dirichlet de K , et si n est le degré de K , on a $r < n$.

Comme les corps conjugués $K^{(1)} , K^{(2)} , \dots , K^{(n)}$, sont isomorphes, le groupe multiplicatif Γ des éléments $(e^{(1)} , e^{(2)} , \dots , e^{(n)})$, où $e^{(i)}$ sont les conjugués d'une unité $e = e^{(1)}$ de K , est aussi engendré par un élément d'ordre fini et r éléments d'ordres infinis.

Pour appliquer le théorème central, on remarquera que, si une infinité de points de Γ sont sur une k-variété de dimension s , on a une infinité de ces points sur une composante irréductible de cette variété, dont la dimension est $\leqslant s$.

On obtient le théorème suivant par application du théorème central :

THÉORÈME 3.1. - Soient K un corps de nombres algébriques de degré n , r le nombre de Dirichlet de K , Γ le groupe des unités de K (considéré dans $K^{(1)} \times K^{(2)} \times \dots \times K^{(n)}$) et V une k-variété de dimension s où k est une extension algébrique de $\mathbb{Q}$.

Supposons que $\sigma = r + s \leqslant n$ et que $E = \Gamma \cap V$ soit infini.

Alors il existe un sous-groupe γ de Γ, tel que :

1° $\exists\, \overline{a} \in \Gamma/\gamma$ tel que $\overline{a} \cap E$ soit infini.

2° A tout système d'entiers rationnels q_i, $i = 1, 2, \ldots, \sigma$, tels que $1 \leqslant q_1 < q_2 < \ldots < q_\sigma \leqslant n$, correspond un système d'entiers rationnels non tous nuls $N_{q_1}, N_{q_2}, \ldots, N_{q_\sigma}$, tels que, pour tout $e \in \gamma$, on a

$$(3) \qquad e^{(q_1)^{N_{q_1}}} \; e^{(q_2)^{N_{q_2}}} \; \ldots \; e^{(q_\sigma)^{N_{q_\sigma}}} = 1 \; .$$

On a ainsi une condition nécessaire pour l'existence d'une infinité de solutions en entiers rationnels, au système d'équations (I), lorsque $\dim(F_j(X)) = s$ et nombre de Dirichlet de $K = r$, avec $r + s < n$, degré de K.

Si $r + s \geqslant n$, ce théorème est trivial, le sous-groupe Γ satisfaisant les conditions 1° et 2°.

(B) Applications.

On va maintenant appliquer ce théorème, et ceci de la manière suivante : on considère le cas où $r + s < n$, et on cherche dans quelles conditions il est impossible que (3) soit satisfaite ; il sera, alors, impossible également qu'il y ait une infinité d'unités de K dans V.

On distinguera deux cas généraux : celui où l'impossibilité de (3) vient d'une propriété de K, et celui où elle vient d'une propriété de V.

Première application.

Rappel [3]. - Soit K une extension algébrique de degré n de Q. On peut trouver $\theta \in K$, zéro d'un polynôme irréductible de degré n, $F(X) \in Q[X]$ tel que $K = Q[\theta]$ (théorème de l'élément primitif). Soit L le corps de décomposition de $F(X)$, L ne dépend pas de $F(X)$, mais seulement de K.

Le groupe de Galois de K, que nous noterons $G(K)$, est le groupe de Galois $G_{L:Q}$ des automorphismes de L qui laissent Q invariant. Le nombre des éléments de $G(K)$ est fini, et divise $n!$, et les opérations $g \in G(K)$ correspondent à des permutations des nombres conjugués $\theta^{(i)}$, $i = 1, 2, \ldots, n$, l'image de $G(K)$ dans le groupe des permutations de n éléments étant un groupe transitif.

Nous représenterons par la suite le groupe $G(K)$ par les permutations correspon-

dantes des coordonnées d'un point dans un espace à n dimensions (en général, ce sera Q^n).

On a alors le théorème suivant :

THÉORÈME 3.2. - Soient K un corps de nombres algébriques de dimension n, dont le nombre de Dirichlet est r, V une k-variété algébrique affine, de dimension $s \leqslant n - r - 1$, et k extension algébrique de Q.

Alors, si dans Q^n, considéré comme espace vectoriel sur Q, $G(K)$ ne laisse inchangé aucuns sous-espaces vectoriels propres autres que

$$E_1 \quad (x_1 = x_2 = \ldots = x_n) \quad \text{et} \quad E_2 \quad (x_1 + x_2 + \ldots + x_n = 0) \quad ,$$

il est impossible que V contienne une infinité d'unités de K.

Remarque. - E_1 et E_2 sont des sous-espaces vectoriels propres de Q^n, laissés inchangés par toutes les permutations des coordonnées. On a

$$\dim E_1 = 1 \ , \quad \dim E_2 = n - 1 \ , \quad E_1 + E_2 = Q^n \ ,$$

et E_1 et E_2 sont orthogonaux.

Démonstration. - Supposons, par l'absurde, que V contienne une infinité d'unités de K ; alors, d'après le théorème 3.1, on a

$$e^{(1)N_1} \, e^{(2)N_2} \ldots e^{(n-1)N_{n-1}} = 1 \tag{3'}$$

pour une infinité d'unités de K, les N_i étant des entiers rationnels non tous nuls. Mais on a toujours :

$$(e^{(1)} \, e^{(2)} \ldots e^{(n)})^h = 1 \ ,$$

en prenant éventuellement h pair ; donc :

$$e^{(1)N_1+h} \, e^{(2)N_2+h} \ldots e^{(n-1)N_{n-1}+h} \, e^{(n)h} = 1 \ .$$

Prenons h entier rationnel pair $\geqslant -\frac{1}{n}(N_1 + \ldots + N_{n-1})$, et posons

$$m_1 = N_1 + h \ , \quad m_2 = N_2 + h \ , \ \ldots \ , \quad m_{n-1} = N_{n-1} + h \ , \quad m_n = h \ .$$

Alors, $m_1 + m_2 + \ldots + m_n > 0$, et, puisque les N_i ne sont pas tous nuls, les m_i ne sont pas égaux.

Ainsi, on a $(m_1 \ , m_2 \ , \ldots \ , m_n) \notin E_1 \cup E_2$, et

$$e(1)^{m_1}\ e(2)^{m_2}\ \dots\ e(n)^{m_n} = 1 \quad .$$

Soient $g \in G(K)$, et $\begin{pmatrix} 1 & 2 & \dots & n \\ h_1 & h_2 & \dots & h_n \end{pmatrix}$ sa permutation associée, on a alors

$$e(1)^{m_1}\ e(2)^{m_2}\ \dots\ e(n)^{m_n} = e^{(h_1)^{m_1}\ (h_2)^{m_2}\ \dots\ (h_n)^{m_n}} = 1 \quad ,$$

donc la permutation inverse $\begin{pmatrix} h_1 & h_2 & \dots & h_n \\ 1 & 2 & \dots & n \end{pmatrix}$ effectuée sur $(m_1 , m_2 , \dots , m_n)$ ne change pas la valeur de

$$e(1)^{m_1}\ e(2)^{m_2}\ \dots\ e(n)^{m_n} \text{ , i. e. } e(1)^{m_{h_1}}\ \dots\ e(n)^{m_{h_n}} = 1 \quad .$$

Ainsi, pour toute permutation $\begin{pmatrix} 1 & 2 & \dots & n \\ h_1 & h_2 & \dots & h_n \end{pmatrix}$ associée à une opération de $G(K)$, on a

$$e(1)^{m_{h_1}}\ e(2)^{m_{h_2}}\ \dots\ e(n)^{m_{h_n}} = 1 \quad .$$

Or $(m_1 , \dots , m_n) \notin E_1 \cup E_2$, donc, d'après l'hypothèse faite sur $G(K)$, $(m_1 , \dots , m_n)$ et ses permutés par les opérations de $G(K)$ engendrent Q^n tout entier, et il existe n permutés de $(m_1 , \dots , m_n)$, soient $(m_{j1} , m_{j2} , m_{jn})$, $j = 1 , 2 , \dots , n$, tels que

$$\det(m_{ji}) = d \neq 0 \qquad (\ d \text{ entier rationnel}).$$

Le système d'équations

$$\begin{aligned} y_1 m_{11} + y_2 m_{21} + \dots + y_n m_{n1} &= d \\ y_1 m_{12} + y_2 m_{22} + \dots + y_n m_{n2} &= 0 \\ \dots \quad \dots \quad \dots \quad \dots \quad \dots & \\ y_1 m_{1n} + y_2 m_{2n} + \dots + y_n m_{nn} &= 0 \end{aligned}$$

a alors une solution $(q_1 , q_2 , \dots , q_n)$ en entiers rationnels, de sorte que

$$(e(1)^{m_{11}} \dots e(n)^{m_{1n}})^{q_1} \dots (e(1)^{m_{n1}} \dots e(n)^{m_{nn}})^{q_n} = e(1)^d = 1 \quad ,$$

donc $e = e^{(1)}$ est racine de l'unité.

Comme K ne contient qu'un nombre fini de racines de l'unité, on a contradiction.

C. Q. F. D.

Nous allons expliciter deux cas où ce théorème s'applique.

(a) $G(K)$ <u>est le groupe symétrique</u> S_n . - Donc $G(K)$ est représenté dans Q^n par l'ensemble des permutations des n coordonnées.

Supposons qu'il existe un sous-espace vectoriel propre E de Q^n , différent de E_1 et de E_2 , inchangé par les opérations de $G(K)$.

On voit qu'on a alors $E_3 = E \cap E_2 \neq E_2$, donc $\dim E_3 \leqslant n - 2$. On aurait alors, pour tout vecteur $(a_1 , a_2 , \ldots , a_n) \in E_3$, une relation

$$a_1 m_1 + a_2 m_2 + \ldots + a_{n-1} m_{n-1} = 0 \quad ,$$

avec m_i , $i = 1 , 2 , \ldots , n - 1$, entiers rationnels non tous nuls. Supposons $m_1 \neq 0$, alors on a aussi

$$a_n m_1 + a_2 m_2 + \ldots + a_{n-1} m_{n-1} = 0 \quad ,$$

d'où $a_1 = a_n$, puis en permutant a_1 et a_i , on voit que $a_i = a_n$, $i = 1,2,\ldots,n$ donc $(a_1 , \ldots , a_n) \in E_1$, ce qui est contradictoire avec l'hypothèse

$$(a_1 , \ldots , a_n) \in E \cap E_2 \quad .$$

(b) <u>Le degré de</u> K <u>sur</u> Q <u>est un nombre premier</u> p . - D'après la théorie des extensions algébriques finies de Q , le nombre $O(G(K))$ des éléments de $G(K)$ est divisible par p , donc $O(G(K)) = m.p$, m étant un entier rationnel positif.

D'après un théorème de Cauchy-Sylow, [3], il existe un élément d'ordre p , soit $g_1 \in G(K)$, auquel correspond une permutation d'ordre p dans S_p . Mais on sait qu'une permutation est décomposable en cycles et que l'ordre de la permutation est le p. p. c. m. des ordres de ces cycles. Comme p est premier, la décomposition est réduite à un seul cycle d'ordre p . Soit

$$\begin{pmatrix} 1 & 2 & \ldots & p-1 & p \\ 2 & 3 & \ldots & p & 1 \end{pmatrix}$$

cette permutation (on fait éventuellement une permutation préalable des coordonnées dans Q^n pour obtenir cette forme). S'il existe un sous-espace vectoriel propre E de Q^n , différent de E_1 et de E_2 et invariant pour les opérations de $G(K)$, on a un vecteur $(a_1 , a_2 , \ldots , a_n)$, avec a_i non tous nuls ni tous égaux, tel que

$$\Delta = \begin{vmatrix} a_1 & a_2 & \ldots & a_p \\ a_2 & a_3 & \ldots & a_1 \\ \ldots & \ldots & \ldots & \ldots \\ a_p & a_1 & \ldots & a_{p-1} \end{vmatrix} = 0 \quad .$$

Or, on sait que ([1], chap. VI) :

$$\Delta = (a_1 + a_2 + \ldots + a_p)(a_1 + a_2\,\xi_1 + \ldots + a_p\,\xi_1^{p-1}) \ldots (a_1 + a_2\,\xi_{p-1} + \ldots + a_p\,\xi_{p-1}^{p-1}) \ ,$$

les ξ_i étant les racines de l'équation

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1 = 0 \ ,$$

i. e. les racines de l'unité d'ordre p non triviales.

Alors $\Delta = 0 \implies a_1 + a_2\,\xi_k + \ldots + a_p\,\xi_k^{p-1} = 0$ pour un certain k, mais on a aussi $1 + \xi_k + \ldots + \xi_k^{p-1} = 0$.

Comme les a_i ne sont pas tous nuls, ni tous égaux, on a pour ξ_k une équation à coefficients rationnels de degré $< p - 1$. Ceci est contradictoire, car le polynôme $x^{p-1} + x^p + \ldots + x + 1$, avec p premier, est irréductible sur Q.

Donc $\Delta \neq 0$, et Q^n ne contient pas de sous-espaces vectoriels propres invariants pour $G(K)$ autres que E_1 et E_2.

Deuxième application.

PROBLÈME. - Etant donné un nombre fini h de nombres algébriques sur Q, $\alpha_1 , \alpha_2 , \ldots , \alpha_h$, linéairement indépendants sur Q, on cherche à savoir s'il peut y avoir une infinité d'unités de $K = Q[\alpha_1 , \alpha_2 , \ldots , \alpha_h]$ dans

$$U = Q.\alpha_1 + Q.\alpha_2 + \ldots + Q.\alpha_h \ .$$

Les théorèmes suivants donneront certaines réponses à ce problème.

LEMME 3.1. - Si des unités de même norme (positive par exemple) d'une extension K de Q, de degré n, se trouvent sur un sous-espace vectoriel L de Ω^n (Ω étant une clôture algébrique de Q), de dimension h, alors elles sont situées sur une k-variété algébrique affine équidimensionnelle de Ω^n de dimension $h - 1$, k étant une extension algébrique finie de Q.

Démonstration. - Soit $(\omega_{i1} , \omega_{i2} , \ldots , \omega_{in})$, $i = 1 , 2 , \ldots , h$, une base de L sur Ω, et soit $k = Q[\omega_{ij}]$.

On sait, d'après l'exemple donné à la fin du § 1, que $L = V(\alpha)$, où α est l'idéal engendré dans $k[X_1 , X_2 , \ldots , X_n]$ par les polynômes $F_k(X_1 , X_2 , \ldots , X_n)$, $k = 1 , 2 , \ldots , n - h$.

Les unités de K qui nous intéressent sont situées sur la variété $V(\alpha_1)$, où α_1 est l'idéal engendré dans $k[X_1 , X_2 , \dots , X_n]$ par les polynômes $F_k[X_1 , X_2 , \dots , X_n]$, $k = 1 , 2 , \dots , n - h$ et $X_1 X_2 \dots X_n - 1$. On peut voir que ces $n - h + 1$ polynômes sont algébriquement indépendants sur K , donc $V(\alpha_1)$ est équidimensionnelle de dimension $n - (n - h + 1) = h - 1$.

C. Q. F. D.

LEMME 3.2. - Si une infinité d'unités d'une extension K de Q , de degré n , se trouvent sur un sous-espace vectoriel L de Ω^n , de dimension h , et si $h + r \leqslant n$, r étant le nombre de Dirichlet de K , alors une infinité de ces unités sont situées sur une k-variété équidimensionnelle de Ω^n , de dimension $h - 2$, k étant une extension algébrique finie de Q .

Démonstration. - On peut supposer que ces unités de K , situées sur L , sont de norme $+ 1$, alors elles sont aussi sur une k-variété $V_1 = V(\alpha_1)$ de dimension $h - 1$ (voir lemme 3.1).

D'après les hypothèses, on a $r + \dim V_1 < n$, et on peut appliquer le théorème 3.1 :

Il existe un sous-groupe γ du groupe Γ des unités de K tel que :

1° une classe au moins de Γ/γ contient une infinité d'unités de K situées sur V_1 ,

2° il existe des entiers rationnels non tous nuls, $N_1 , \dots , N_{n-1}$, tels que

$$x_1^{N_1} x_2^{N_2} \dots x_{n-1}^{N_{n-1}} = 1 , \quad \forall\, x \in \gamma .$$

Posons :

$$q_i = nN_i - (N_1 + N_2 + \dots + N_{n-1}) , \quad i = 1 , 2 , \dots , n - 1$$

$$q_n = - (N_1 + N_2 + \dots + N_{n-1}) .$$

Les q_i sont des entiers rationnels non tous nuls, ni tous égaux, tels que $q_1 + q_2 + \dots + q_n = 0$, et on a

$$x_1^{q_1} x_2^{q_2} \dots x_n^{q_n} = 1 , \quad \forall\, x \in \gamma$$

(si la norme des unités de K considérées est $- 1$, on remplacera q_i par $2q_i$).

Soit e un élément de la classe de Γ/γ qui contient une infinité d'unités de K situées sur V_1 , et soit

$$c = e^{(1)q_1}\, e^{(2)q_2} \ldots e^{(n)q_n} \quad .$$

Les unités de K situées sur V_1 satisfont donc l'équation

$$x_1^{q_1}\, x_2^{q_2} \ldots x_n^{q_n} - c = 0 \quad .$$

On a ainsi une infinité d'unités de K situées sur $V_2 = V(\alpha_2)$, où α_2 est l'idéal engendré dans $k(c)[X_1 , X_2 , \ldots , X_n]$ par les $n - h + 2$ polynômes $F_k(X_1 , X_2 , \ldots , X_n)$, $k = 1 , 2 , \ldots , n - h$,

$$X_1 X_2 \ldots X_n - 1 \quad \text{et} \quad X_1^{q_1} X_2^{q_2} \ldots X_n^{q_n} - c \quad .$$

Or ces polynômes sont algébriquement indépendants sur $k' = k(c)$, donc V_2 est une k'-variété équidimensionnelle de dimension $n - (n - h + 2) = h - 2$.

C. Q. F. D.

LEMME 3.3. - *Soient* $\alpha_1 , \alpha_2 , \ldots , \alpha_h$, h *nombres algébriques d'une extension finie de* K *de* Q , *de dimension* n , *soient* $\alpha_j^{(i)}$, $i = 1 , 2 , \ldots , n$, *les* n *conjugués algébriques par rapport à* K *de* $\alpha_j = \alpha_j^{(i)}$, *pour* $j = 1 , 2 , \ldots , h$, *et soit* Ω *un corps algébrique sur* Q , *contenant tous les* $\alpha_j^{(i)}$. *Alors, les* h *vecteurs* $(\alpha_1^{(1)} , \alpha_2^{(2)} , \ldots , \alpha_n^{(n)}) , \ldots , (\alpha_h^{(1)} , \alpha_h^{(2)} , \ldots , \alpha_h^{(n)})$ *sont linéairement indépendants sur* Ω , *et engendrent un sous-espace vectoriel de* Ω^n *de dimension* h .

Démonstration. - On peut trouver $\beta_{h+1} , \ldots , \beta_n$, tels que

$$\alpha_1 , \ldots , \alpha_h \, \beta_{h+1} , \ldots , \beta_n$$

forment une base de K sur Q . Alors

$$\begin{vmatrix} \alpha_1^{(1)} & \ldots & \alpha_h^{(1)} & \beta_{h+1}^{(1)} & \ldots & \beta_n^{(1)} \\ \alpha_1^{(2)} & \ldots & \alpha_h^{(2)} & \beta_{h+1}^{(2)} & \ldots & \beta_n^{(2)} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{(n)} & \ldots & \alpha_h^{(n)} & \beta_{h+1}^{(n)} & \ldots & \beta_n^{(n)} \end{vmatrix} = \text{Cte} \times \text{discriminant } (K) \neq 0 \quad .$$

Par un raisonnement de récurrence, on voit qu'il existe $1 \leqslant i_1 < i_2 < \ldots < i_h \leqslant n$ tel que

$$\begin{vmatrix} \alpha_1^{(i_1)} & \alpha_2^{(i_1)} & \ldots & \alpha_h^{(i_1)} \\ \ldots & & & \\ \alpha_1^{(i_h)} & \alpha_2^{(i_h)} & \ldots & \alpha_h^{(i_h)} \end{vmatrix} \neq 0 \quad .$$

C. Q. F. D.

Exemple. - Soit $K = Q[\theta]$, où $\theta = 2^{1/29}$. Alors il ne peut y avoir qu'un nombre fini d'unités de K dans

$$U = Q + Q.\theta + \ldots + Q.\theta^{14} \quad .$$

En effet, $\deg K = 29$, $r_1 = 1$, $2r_2 = 28$, $r = 14$, $h = 15$. D'après les lemmes 3.3 et 3.1, les unités de $K \cap U$ sont situées sur une variété V_1 de dimension $s = h - 1 = 14$. Comme 29 est premier, on peut appliquer le théorème 3.2 (en tenant compte de (b) suivant la démonstration de ce théorème), et il ne peut y avoir une infinité d'unités de K sur V_1 , car

$$\dim V_1 + r = 14 + 14 = 28 < 29 = \deg K \quad .$$

D'après le § 3(A), on voit que l'équation :

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

ne peut avoir qu'un nombre fini de solutions en entiers rationnels.

THÉORÈME 3.3. - Soient α_1 , α_2 , ... , α_h , h nombres algébriques sur Q , linéairement indépendants ; soient $K = Q[\alpha_1$, ... , $\alpha_h]$, n son degré et r son nombre de Dirichlet.

Supposons $h + r \leqslant n$.

Alors, si une infinité d'unités de K sont dans $U = Q.\alpha_1 + \ldots + Q.\alpha_h$, une infinité de ces unités sont aussi situées sur une k-variété équidimensionnelle de dimension $h - 2$ $(k = Q[\alpha_j^{(i)}])$.

Démonstration. - D'après le lemme 3.3, les unités de K , appartenant à U , sont situées dans l'espace vectoriel de base $(\alpha_j^{(1)}$, $\alpha_j^{(2)}$, ... , $\alpha_j^{(n)})$, $j = 1,2,\ldots,h$, et l'on peut appliquer le lemme 3.2.

COROLLAIRE 3.1. - Soit $K = Q[\alpha]$, une extension algébrique de Q dont les corps conjugués ne sont pas tous réels (i. e. tels que $r \leqslant n - 2$).

Alors, il ne peut y avoir une infinité d'unités de K dans $U = Q + Q.\alpha$.

En effet, dans le cas contraire, on pourrait appliquer le théorème 3.3, et on devrait avoir une infinité d'unités de K sur une variété de dimension 0 , ce qui est contradictoire, car une variété de dimension 0 n'a qu'un nombre fini de points.

Exemple. - Soit $f(x) \in Z[x]$ un polynôme irréductible de degré n , et dont les racines ne sont pas toutes réelles. (Z étant l'ensemble des entiers rationnels.)

Alors l'équation

(4) $$Y^n f(\frac{X}{Y}) = b ,$$

où b est un entier rationnel, ne peut avoir qu'un nombre fini de solutions entières rationnelles X , Y .

En effet, soient a_n le coefficient du terme de degré n dans $f(x)$, et $\alpha = \alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(n)}$ les zéros des $f(x)$. Alors $a_n \alpha$ est un entier algébrique et $f(x) = a_n \prod_{i=1}^{n} (x - \alpha^{(i)})$, d'où

$$Y^n f(\frac{X}{Y}) = a_n \prod_{i=1}^{n} (X - Y\alpha^{(i)}) \quad \text{et} \quad Y^n f(\frac{X}{Y}) = b \iff \prod_{i=1}^{n} (Xa_n - Ya_n \alpha^{(i)}) = (a_n)^{n-1} b .$$

Si l'équation (4) a une infinité de solutions entières rationnelles X , Y , il y a une infinité d'entiers algébriques $\varphi = Xa_n - Ya_n \alpha$, de norme $(a_n)^{n-1} b$, dans $Q[\alpha]$.

Considérons les idéaux principaux (φ) engendrés dans l'anneau A des entiers algébriques de $Q[\alpha]$ par ces nombres φ . On a norme $(\varphi) = \text{card } A/(\varphi) = |(a_n)^{n-1} b|$, et on sait ([4], vol. II, chap. 2, § 7) qu'il existe seulement un nombre fini d'idéaux de A ayant même norme. Donc une infinité de ces nombres φ engendre le même idéal, soit φ_0 l'un de ces nombres. Il y a alors une infinité d'unités dans $Q[\alpha]$ de type $\frac{\varphi}{\varphi_0} = Xa_n \frac{1}{\varphi_0} - Ya_n \frac{\alpha}{\varphi_0}$.

Mais $Q[\frac{1}{\varphi_0}, \frac{\alpha}{\varphi_0}] = Q(\frac{1}{\varphi_0}, \frac{\alpha}{\varphi_0}) = Q[\alpha]$ et $Q[\alpha]$ a un nombre de Dirichlet $r \leq n - 2$. On applique le corollaire 3.1, et on aboutit à une contradiction.

COROLLAIRE 3.2. - Soient α , β , γ trois nombres algébriques sur Q , linéairement indépendants sur Q . Considérons $K = Q[\alpha,\beta,\gamma]$, et supposons que $r \leqslant n - 3$, où n est le degré de K et r son nombre de Dirichlet.

Alors, s'il existe une infinité d'unités de K dans $Q.\alpha + Q.\beta + Q.\gamma$, une infinité d'entre elles sont situées sur une k-variété irréductible de dimension 1 dans Ω^n (k extension algébrique finie de Q , Ω clôture algébrique de Q), c'est-à-dire sur une courbe algébrique irréductible.

Un théorème de Siegel [7]. - Si une courbe algébrique irréductible de Ω^n a une infinité de points dont toutes les coordonnées sont des entiers algébriques, alors elle a une représentation paramétrique $x_i = \frac{P_i(t)}{t^{m_i}}$, où m_i est un entier rationnel et $P_i(t)$ un polynôme en t , à coefficients algébriques, et inversement.

On ne démontrera pas ce théorème ici, mais on remarquera que cette démonstration est basée sur une méthode d'approximation, alors que tous les résultats précédents sont obtenus indépendamment de telles méthodes.

LEMME 3.4. - Soient K un corps algébrique de degré n, C une courbe algébrique irréductible de Ω^n.

Alors, si C contient un ensemble infini E de points entiers algébriques de K de norme c, K contient un sous-corps quadratique réel k, et l'on a pour C la représentation

$$x_i = a^{(i)} y_i ,$$

où $a^{(1)} = a \in E$ et où y_i, $i = 1, 2, \ldots, n$, sont les coordonnées de l'hyperbole H de Ω^n portant les unités à norme positive de k.

Démonstration. - D'après le théorème de Siegel, C a la représentation paramétrique $x_i = \dfrac{P_i(t)}{t^{m_i}}$, $i = 1, 2, \ldots, n$, et on a

$$\prod_{i=1}^{n} \frac{P_i(t)}{t^{m_i}} = c$$

pour une infinité de valeurs (algébriques) du paramètre t, c'est-à-dire

$$\prod_{i=1}^{n} P_i(t) - c\, t^m = 0 , \quad m = m_1 + m_2 + \ldots + m_n .$$

Ce polynôme est donc identiquement nul, donc

$$\prod_{i=1}^{n} P_i(t) \equiv c\, t^m ,$$

d'où $P_i(t) = \lambda_i t^{h_i}$, où λ_i sont des nombres algébriques avec $\lambda_1 \lambda_2 \ldots \lambda_n = c$ et h_i des entiers rationnels avec $h_1 + h_2 + \ldots + h_n = m$.

D'autre part, comme on a une infinité d'entiers algébriques $x \in E$ ayant même norme c, on peut trouver un de ces nombres, soit a, tel que $e = x/a$ soit une unité de norme positive pour une infinité de tels nombres x (voir l'exemple suivant le corollaire 3.1).

Soit $a^{(i)} = \lambda_i t_a^{h_i}$, $i = 1, 2, \ldots, n$, la représentation paramétrique de $a^{(1)} = a$ et de ses conjugués ; la représentation des unités $e = e^{(1)}$ est alors

$$e^{(i)} = \left(\frac{t}{t_a}\right)^{h_i} , \quad i = 1, 2, \ldots, n$$

et on a, pour $f = 1, 2, \ldots, n$ et $g = 1, 2, \ldots, n$,

$$e^{(f)^{h_g}} = e^{(g)^{h_f}} .$$

L'image du groupe de Galois $G(K)$ dans le groupe des permutations des conjugués étant transitive, il existe $T_{fg} \in G(K)$ tel que $T_{fg}\, e^{(g)} = e^{(f)}$, et on a

$$e^{(f)^{h_f}} = T_{fg}\, e^{(g)^{h_f}} = T_{fg}\, e^{(f)^{h_g}} ,$$

de même

$$e^{(f)^{h_f^\nu}} = T_{fg}^\nu\, e^{(f)^{h_g^\nu}} .$$

Soit alors q l'ordre (fini) de T_{fg}, on a :

$$e^{(f)^{h_f^q}} = T_{fg}^q\, e^{(f)^{h_g^q}} = e^{(f)^{h_g^q}} ,$$

d'où

$$e^{(f)^{(h_f^q - h_g^q)}} = 1 \quad \text{et} \quad e^{h_f^q - h_g^q} = 1 .$$

Or K contient un infinité d'unités de ce type. Ces unités ne sont donc pas toutes des racines de l'unité, et on doit avoir $h_f^q = h_g^q$ pour tous $f = 1, 2, \ldots, n$, $g = 1, 2, \ldots, n$, donc $h_f = \pm h$, h étant fixé. Alors

$$e^{(i)} = \left(\frac{t}{t_a}\right)^{\pm h} ;$$

ces unités ont donc, au plus, deux conjugués distincts ; comme il y a une infinité de telles unités, ce sont des unités quadratiques réelles. Or, il ne peut y avoir qu'un nombre fini de sous-corps quadratiques (réels) de K, donc il y a une infinité de ces unités dans un certain sous-corps quadratique réel k de K.

Soit H l'hyperbole de Ω^n portant les unités de k. H correspond à l'idéal α engendré dans $Q[x_1, x_2, \ldots, x_n]$ par les $n - 1$ polynômes :

$$x_{i_k} - x_1 , \quad k = 2, \ldots, \frac{n}{2} \quad \text{et} \quad x_{i_{k+\ell}} . x_1 - 1 , \quad \ell = \frac{n}{2} + 1, \ldots, n .$$

Ces polynômes sont algébriquement indépendants et l'idéal $i(H)$ est premier, donc H est une variété irréductible de dimension 1 ainsi que la variété aH dont les points ont les coordonnées $x_i = a^{(i)} y_i$, $y = (y_1, y_2, \ldots, y_n) \in H$.

Comme C et aH sont deux courbes algébriques irréductibles, ayant une infinité de points entiers algébriques communs, elles sont confondues, ce qui donne la représentation annoncée pour C.

C. Q. F. D.

THÉORÈME 3.4. - Soient α et β deux nombres algébriques sur Q, tels que 1, α, β soient linéairement indépendants sur Q, et tels que $K = Q[\alpha, \beta]$ ait au moins deux paires de corps complexes conjugués, et soit U l'espace vectoriel sur Q engendré par ces trois nombres $(U = Q + Q\alpha + Q\beta)$. Alors :

(i) Si U contient une infinité d'entiers algébriques de norme c, U contient au moins deux entiers algébriques φ et ψ, de norme c, et dont le quotient $\theta = \psi/\varphi$ soit un nombre quadratique réel. De plus, ε étant une unité fondamentale de $Q[\theta]$, U contient tous les nombres $\varphi\varepsilon^n$, $n \in Z$.

(ii) $Q[\theta]$ est défini de manière unique, et tous les entiers algébriques de norme c, situés dans U, sont, à un nombre fini d'exceptions possibles près, de la forme $\varphi\varepsilon^n$ pour un entier algébrique φ de norme c, situé dans U. Si deux entiers de norme c, φ et φ', tels que $\varphi\varepsilon^n \in U$ et $\varphi'\varepsilon^n \in U$, pour tout $n \in Z$, sont associés dans K, ils le sont aussi dans $Q[\theta]$, et les ensembles $\{\varphi\varepsilon^n\}$ et $\{\varphi'\varepsilon^n\}$ sont égaux.

Démonstration.

(i) U contenant une infinité d'entiers algébriques de K de norme c, il existe un de ces entiers, soit φ_0, tel que $\frac{1}{\varphi_0} U$ contient une infinité d'unités de K. Comme le nombre de paires de corps complexes conjugués de K est au moins égal à 2, le nombre de Dirichlet de K est $\leqslant n - 3$, et on peut appliquer le corollaire 3.2 du théorème 3.3 : une infinité de ces unités sont situées sur une courbe algébrique irréductible C. D'après le lemme 3.4, C a la représentation $x_i = a^{(i)} y_i$, $i = 1, 2, \ldots, n$, $a^{(1)}$ étant une unité de K, située dans $\frac{1}{\varphi_0} U$ et $(y_1, y_2, \ldots, y_n)$ les points de l'hyperbole portant les unités à norme positive d'un sous-corps quadratique de K.

Soit u une unité de $\frac{1}{\varphi_0} U$, différente de $a^{(1)}$, et située sur C, donc de la forme $u = a^{(1)} y_1$. Alors, $y_1 = \frac{u}{a^{(1)}}$ est une unité de K, mais c'est aussi une unité quadratique, puisqu'elle est située sur une hyperbole. Donc $Q[y_1]$ est un sous-corps quadratique de K, et, comme K ne peut contenir qu'un nombre fini de sous-corps, on peut trouver une de ces unités, soit θ, telle que $Q[y_1] = Q[\theta]$ pour une infinité de ces unités y, et θ est réel, puisque $Q[\theta]$ contient une infinité d'unités distinctes. On a finalement

$$\psi = a^{(1)} \theta\varphi_0 \in U, \text{ car } a^{(1)} \theta = u \in \frac{1}{\varphi_0} U,$$

$$\varphi = a^{(1)} \varphi_0 \in U, \text{ car } a^{(1)} \in \frac{1}{\varphi_0} U,$$

ψ et φ entiers algébriques dont le quotient est θ.

De plus, comme $\theta \in \frac{1}{\varphi} U$, on a $\frac{1}{\varphi} U \supset Q[\theta]$, d'où $U \supset \varphi Q[\theta]$ et $\varphi\varepsilon^n \in U$, pour tout $n \in Z$, où ε est une unité fondamentale de $Q[\theta]$.

(ii) En itérant le raisonnement fait en (i) , on voit que tous les entiers algébriques de norme c , situés dans U , sont, à un nombre fini d'exceptions possibles près, de la forme $\varphi\varepsilon^n$, où $n \in Z$, où φ est un entier algébrique de norme c , situé dans U , et où ε est une unité fondamentale d'un sous-corps quadratique réel de K .

Soient φ et φ' deux entiers algébriques de norme c , situés dans U , et k et k' deux sous-corps quadratiques réels de K , dont les unités fondamentales sont respectivement ε et ε' , tels que $\varphi\varepsilon^n \in U$ et $\varphi'\varepsilon'^n \in U$, pour tout $n \in Z$. Alors $\varphi \in U$ et $\varphi\varepsilon \in U \Rightarrow \varphi.Q[\varepsilon] = \varphi.k \subset U$, de même, $\varphi'.k' \subset U$.

On va montrer que $\varphi.k = \varphi'.k'$; pour ceci, on suppose $\varphi.k \neq \varphi'.k'$.

$$\varphi.\varphi\varepsilon \ , \ \varphi'.\varphi'\varepsilon' \in U \ ,$$

donc

$$U \supset U^* = Q\varphi + Q\varphi\varepsilon + Q\varphi' + Q\varphi'\varepsilon'$$

et

$$\dim U^* \leqslant \dim U = 3 \ .$$

D'autre part, comme $Q\varphi + Q\varphi\varepsilon \neq Q\varphi' + Q\varphi'\varepsilon'$, on a $\dim U^* \geqslant 3$. Donc $\dim U^* = 3$ et $U^* = U$. Alors,

$$\varphi' \in Q\varphi + Q\varphi\varepsilon + Q\varphi'\varepsilon' \ ,$$

d'où

$$\frac{\varphi'}{\varphi} \in Q + Q\varepsilon + Q\frac{\varphi'}{\varphi}\varepsilon' \quad \text{et} \quad \frac{\varphi'}{\varphi} \in Q[\varepsilon \ , \ \varepsilon'] \ ,$$

$\frac{\varphi'}{\varphi}$ est donc un nombre totalement réel, et $\frac{1}{\varphi} U = \frac{1}{\varphi} U^* = Q + Q\varepsilon + Q\frac{\varphi'}{\varphi} + Q\frac{\varphi'}{\varphi}\varepsilon'$ est totalement réel, et comme $1 \in U$, $\frac{1}{\varphi}$ est aussi totalement réel, ainsi que φ . Finalement $U = U^*$ est totalement réel, ce qui est contraire à l'hypothèse faite sur K .

Donc $\varphi k = \varphi' k'$, d'où $\frac{\varphi'}{\varphi} \in k$ et $\frac{\varphi}{\varphi'} \in k'$. Si $\varphi = \varphi'$, on a évidemment $k = k'$, sinon on a $Q[\frac{\varphi'}{\varphi}] = k = k'$. φ'/φ étant un nombre de k , on voit que si φ et φ' sont associés dans K , ils le sont aussi dans k , et alors les ensembles $\{\varphi\varepsilon^n\}$ et $\{\varphi'\varepsilon\}$ sont égaux.

C. Q. F. D.

Remarque. - Si le degré de K est impair, K ne peut pas avoir de sous-corps quadratique, et U ne peut pas contenir une infinité d'unités.

On déduit de ce théorème, un résultat sur l'approximation de 0 par une forme linéaire homogène à trois variables et à coefficients algébriques, pour des valeurs entières rationnelles des variables. On peut, sans restreindre la généralité, considérer seulement les formes du type $X + Y\alpha + Z\beta$, où α et β sont des entiers algébriques.

Rappelons un résultat connu : Considérons deux entiers algébriques α et β d'un corps K de degré n sur Q , et soient $\alpha^{(i)}$ et $\beta^{(i)}$, $i = 1, 2, \ldots, n$, les conjugués de α et β . Posons

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

$$H = |X| + |Y| + |Z| \qquad \text{(valeur absolue ordinaire).}$$

Comme $\text{Norme}(X + Y\alpha + Z\beta)$ est un entier rationnel, pour tous X , Y , Z entiers rationnels, on a

$$\prod_{i=1}^{n} |X + Y\alpha^{(i)} + Z\beta^{(i)}| \geqslant c$$

entier rationnel positif, d'où

$$|X + Y\alpha + Z\beta| \geqslant \frac{c}{\prod_{i=2}^{n} |X + Y\alpha^{(i)} + Z\beta^{(i)}|}$$

$$\geqslant \frac{c}{(|X| + |Y| + |Z|)^{n-1} A^{n-1}} = \frac{c_0}{H^{n-1}} \quad .$$

Le théorème 3.4 permet de montrer un résultat plus précis :

THÉORÈME 3.5. - <u>Si le corps</u> $K = Q[\alpha , \beta]$, α <u>et</u> β <u>étant des entiers algébriques, est de degré</u> n , <u>et a au moins deux paires de corps conjugués imaginaires, alors l'inégalité</u>

$$|X + Y\alpha + Z\beta| \leqslant \frac{M}{H^{n-1}}$$

<u>n'a qu'un nombre fini de solutions en entiers rationnels</u> X , Y , Z , <u>quelle que soit la constante réelle positive</u> M .

<u>Démonstration</u>. - Fixons M , et supposons que l'inégalité ait une infinité de solutions en entiers rationnels ; et soient $\gamma = X + Y\alpha + Z\beta$ les entiers de K correspondants. On a alors :

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

d'où

$$|\text{Norme}(\gamma)| \leqslant \frac{M}{H^{n-1}} A^{n-1} H^{n-1} = M' \quad .$$

Mais les divers $\text{Norme}(\gamma)$ sont des entiers rationnels, donc étant bornés, ils ne peuvent prendre qu'un nombre fini de valeurs : il existe donc un entier rationnel c tel que $\text{Norme}(\gamma) = c$ pour une infinité de nombres

$$\gamma = X + Y\alpha + Z\beta \in U = Q + Q.\alpha + Q.\beta \quad .$$

Comme d'après les hypothèses, le nombre de Dirichlet de K, r, satisfait l'inégalité $r \leqslant n - 3$, on peut appliquer le théorème 3.4 : il existe φ et ψ dans U, où φ est entier algébrique de norme c, et où $\theta = \psi/\varphi$ est quadratique réel, tels que

$$U \supset Q.\varphi + Q.\psi = \varphi.Q[\theta]$$

et tous les nombres $\varphi\varepsilon^n$, où $n \in \mathbb{Z}$ et où ε est une unité fondamentale de $Q[\theta]$, sont des entiers algébriques de norme c, situés dans U. Or on peut trouver un nombre quadratique réel θ' tel que $Q[\theta'] = Q[\theta]$ et tel que 1 et θ' forment une base d'entiers de $Q[\theta]$. Dans ces conditions, $\varepsilon \in Z + Z\theta'$, pour tout entier rationnel n, et on a une infinité d'entiers algébriques

$$\gamma = X + Y\alpha + Z\beta = \varphi(X' + Y'\theta')$$

tels que

$$|\gamma| \leqslant \frac{M}{H^{n-1}} \qquad (\text{et } \text{Norme}(\gamma) = c \ ).$$

Mais

$$H' = |X'| + |Y'| \leqslant M''H \ , \qquad \text{i. e. } \frac{M''}{H'} \geqslant \frac{1}{H} \quad .$$

Donc on a aussi une infinité de solutions en entiers rationnels à l'inégalité :

$$|X + Y\alpha + Z\beta| = |X' + Y'\theta'||\varphi| \leqslant \frac{M(M'')^{n-1}}{(H')^{n-1}} \quad ,$$

donc aussi à l'inégalité :

$$|X' + Y'\theta'| \leqslant \frac{M'''}{(H')^{n-1}} \quad . \tag{5}$$

On sait d'autre part ([4], Vol. II, chap. IV) que, si ω est un nombre algébrique de degré $n \geqslant 2$, il existe une constante positive N telle que

$$|X + Y\omega| \geqslant \frac{N}{|Y|^{n-1}} \quad \text{pour tous } X \text{ et } Y \text{ entiers rationnels.}$$

Pour θ', on a ainsi

$$|X' + Y'\theta'| \geqslant \frac{N}{|Y'|} \geqslant \frac{N}{H'} \quad .$$

Or, pour H' assez grand, on a

$$\frac{M''}{(H')^{n-1}} < \frac{N}{H'}$$

car d'après les hypothèses, $n - 1 \geqslant 2$.

Donc, il ne peut y avoir qu'un nombre fini de couples d'entiers rationnels X' et Y' tels que

$$|X' + Y'\theta'| \leqslant \frac{M''}{(H')^{n-1}} ,$$

et ceci est en contradiction avec (5), ce qui achève la démonstration.

C. Q. F. D.

BIBLIOGRAPHIE

[1] AITKEN (A. C.). - Determinants and matrices, 9th edition. - Edingurgh, Oliver and Boyd, 1956 (University mathematical Texts).

[2] CHABAUTY (Claude). - Sur les équations diophantiennes liées aux unités d'un corps de nombres algébriques fini, Annali di Mat. pura e appl., Serie 4, t. 17, 1938, p. 127-168 (Thèse Sc. math. Paris, 1938).

[3] DUBREIL (P.) et DUBREIL-JACOTIN (M.-L.). - Leçons d'algèbre moderne, 2e édition. - Paris, Dunod, 1964 (Collection universitaire de Mathématiques, 6).

[4] LeVÊQUE (W. J.). - Topics in number theory. - Reading (Mass.), Addison-Wesley publishing Company, 1956 (Addison-Wesley Mathematics Series).

[5] NÉRON (André). - Cours de mathématiques approfondies, professé à la Faculté des Sciences d'Orsay, 1964/65.

[6] SAMUEL (P.) and ZARISKI (O.). - Commutative algebra, Vol. 1 and 2. - Princeton, D. Van Nostrand, 1958-1960 (The University Series in higher Mathematics).

[7] SIEGEL (Carl Ludwig). - Über einige Anwendungen Diophantischer Approximationen, Abh. Preuss. Akad. Wiss., 1929, n° 1, 70 p.