Séminaire Delange-Pisot-Poitou. Théorie des nombres

Gabriel Archinard

Théorie de Chabauty sur les équations diophantiennes, II

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 8, n° 1 (1966-1967), exp. n° 5, p. 1-13

<http://www.numdam.org/item?id=SDPP_1966-1967__8_1_A5_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
8e année, 1966/67, n° 5

12 décembre 1966

THÉORIE DE CHABAUTY SUR LES ÉQUATIONS DIOPHANTIENNES, II.

par Gabriel ARCHINARD

1. Théorèmes de Chabauty ([2]).

On énonce sans démonstration le théorème central de la thèse de CHABAUTY.

THÉORÈME 1.1 ([2], chapitre II, théorème 2.4). - Soient Q le corps des nombres rationnels, Ω sa clôture algébrique, V un ensemble algébrique dans Ω^n de dimension h, et soit Γ un groupe multiplicatif dans Ω^n dont le nombre de générateurs d'ordre infini est r. (Les points de Γ se multiplient composante par composante.)

On suppose encore $\operatorname{card}(\Gamma \cap V) = \infty$, et $r + h \leqslant n$, et on pose

$$r + h = \sigma \ .$$

Alors, $\forall\, E \subset \Gamma \cap V$ avec $\operatorname{card} E = \infty$, $\exists\, \gamma$ sous-groupe de Γ tel que :

1° $\exists\, \alpha \in \Gamma$ tel que $\operatorname{card}(\alpha\gamma \cap E) = \infty$;

2° $\forall\, q_i \in Z$, $i = 1, 2, \dots, \sigma$, avec $1 \leqslant q_1 < q_2 < \dots < q_\sigma \leqslant n$, $\exists N_i \in Z$, non tous nuls tels que

$$(1) \qquad \varepsilon_{q_1}^{Nq_1} \times \varepsilon_{q_2}^{Nq_2} \times \dots \times \varepsilon_{q_\sigma}^{Nq_\sigma} = 1 \ , \qquad \forall\, (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \in \gamma \ .$$

Dans toutes les applications qui vont suivre, on s'intéressera à des groupes multiplicatifs de nombres pris dans une extension algébrique finie du corps Q.

Soient K une telle extension, de degré n, Γ un sous-groupe du groupe multiplicatif $K^* = K - \{0\}$, et $\alpha \in \Gamma$. Pour appliquer le théorème 1.1, on considèrera des n-uples $(\alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(n)})$ où $\alpha^{(i)}$, $i = 1, 2, \dots, n$, sont les conjugués de $\alpha = \alpha^{(1)}$ dans K. Ce groupe est isomorphe à Γ, et on le notera aussi Γ, chaque fois que le contexte permettra d'éviter les confusions.

Rappel. - Soient $K = Q[\theta]$ une extension finie de Q, de degré n, $f(X) \in Q[X]$ le polynôme irréductible sur Q de θ, et soit L le corps de décomposition de $f(X)$. (L ne dépend que de K .)

Le groupe de Galois de K , qu'on notera $G(K)$, est alors le groupe des Q-automorphismes de L . A tout g de $G(K)$ correspond une et une seule permutation des n conjugués de θ , et on a card $G(K) | n!$. On peut donc représenter $G(K)$ par un sous-groupe du groupe des permutations de n objets.

Soit Q^n considéré comme espace vectoriel sur Q ; à toute opération $g \in G(K)$, on associe l'application de Q^n dans Q^n , qui à tout point de Q^n fait correspondre le point de Q^n dont les coordonnées sont celles de ce point permutées par la permutation associée à g . On voit que les sous-espaces de Q^n ,

$$E_1 = \{(x_1 , x_2 , \dots , x_n) \in Q^n \mid x_1 = x_2 = \dots = x_n\} ,$$

et

$$E_2 = \{(x_1 , x_2 , \dots , x_n) \in Q^n \mid x_1 + x_2 + \dots + x_n = 0\} ,$$

sont invariants pour toute permutation des coordonnées.

THÉORÈME 1.2 ([2], chapitre III, théorème 3.2). - Soient K une extension finie de Q de degré n , Ω la clôture algébrique de Q , Γ un sous-groupe multiplicatif de K^* ayant s générateurs d'ordre infini, et soit V un ensemble algébrique dans Ω^n de dimension h .

On suppose de plus, que $h + s \leqslant n - 1$, et que les applications de Q^n dans Q^n , associées aux éléments de $G(K)$, ne laissent inchangés aucun autre sous-espace de Q^n que E_1 et E_2 .

Alors, il ne peut y avoir sur V une infinité de points de Γ de même norme.

Démonstration. - On suppose qu'il existe sur $V \cap \Gamma$ une infinité de points de norme c (on notera $N(\alpha)$ pour la norme de $\alpha \in K$, norme relative à K).

D'après le théorème 1.1, $\exists\, \alpha \in \Gamma$ et $\exists\, \gamma$, sous-groupe de Γ , tels que

$$N(\alpha\varepsilon) = c$$

pour une infinité de $\varepsilon \in \gamma$, i. e. $N(\varepsilon) = \frac{c}{N(\alpha)} = e$.

En tenant compte de ceci et de la formule (1) du théorème 1.1, on voit que pour une infinité de $\varepsilon \in \gamma$, on a

$$\varepsilon^{(1)} \times \varepsilon^{(2)} \times \dots \times \varepsilon^{(n)} = e ,$$

et

$$\varepsilon^{(1)N_1} \times \varepsilon^{(2)N_2} \times \dots \times \varepsilon^{(n-1)N_{n-1}} = 1 .$$

On prend $m \in Z$, $m \neq -\frac{1}{n}(N_1 + N_2 + \ldots + N_{n-1})$, et on pose $N_n = 0$ et $m_i = N_i + m$, $i = 1 , 2 , \ldots , n$, alors $\sum m_i = nm + \sum N_i \neq 0$, et $\exists\, i$ tel que $m_i \neq m_n = m$; on a ainsi, pour une infinité de $\varepsilon \in \gamma$,

$$\varepsilon^{(1)m_1} \times \varepsilon^{(2)m_2} \times \ldots \times \varepsilon^{(n)m_n} = e^m ,$$

avec $(m_1 , m_2 , \ldots , m_n) \notin E_i$, $i = 1 , 2$.

Le sous-espace de Q^n , engendré par $(m_1 , m_2 , \ldots , m_n)$ et ses images par les applications associées aux éléments de $G(K)$, est l'espace Q^n tout entier ; il existe donc n permutés de $(m_1 , m_2 , \ldots , m_n)$, soient

$$(m_{i1} , m_{i2} , \ldots , m_{in}) \in Z^n , \qquad i = 1 , 2 , \ldots , n ,$$

tels que $\text{dét}(m_{ij}) = d \neq 0$, $d \in Z$. Le système d'équations $\sum y_i m_{i1} = d$, $\sum y_i m_{ij} = 0$, $j = 2 , \ldots , n$, a donc une solution unique $(q_1 , q_2 , \ldots , q_n) \in Z^n$.

Donc, pour une infinité de $\varepsilon \in \gamma$,

$$(\varepsilon^{(1)m_{11}} \times \ldots \times \varepsilon^{(n)m_{1n}})^{q_1} \times \ldots \times (\varepsilon^{(1)m_{n1}} \times \ldots \times \varepsilon^{(n)m_{nn}})^{q_n} = \varepsilon^{(1)d} .$$

D'autre part, toute permutation, correspondant à un élément de $G(K)$ effectuée sur les exposants de l'expression $\varepsilon^{(1)m_1} \times \ldots \times \varepsilon^{(n)m_n}$, correspond à la permutation inverse effectuée sur $(m_1 , \ldots , m_n)$, donc laisse la valeur e^m de cette expression inchangée. Finalement, on a $e^{m(q_1+\ldots+q_n)} = \varepsilon^{(1)d}$ pour une infinité de $\varepsilon \in K$, et ceci est impossible.

Q. E. D.

On a deux cas simples où $G(K)$ a la propriété de l'énoncé du théorème :

(a) $G(K)$ est représenté par le groupe de toutes les permutations de n objets;
(b) Le degré de K sur Q est un nombre premier (cf. [1], page 11).

PROPOSITION 1.1. - *Soient* K *une extension finie de* Q , *de degré* n , Ω *la clôture algébrique de* Q , *et* $\alpha_i \in K$, $i = 1 , 2 , \ldots , h$, *des nombres linéairement indépendants sur* Q . *Alors, les* h *vecteurs* $(\alpha_i^{(1)} , \ldots , \alpha_i^{(n)})$, $i = 1 , 2 , \ldots , h$, *sont linéairement indépendants sur* Ω , *et le sous-espace de* Ω^n *qu'ils engendrent est une variété algébrique* $V = V(\mathfrak{A})$, *de dimension* h , *où* $\mathfrak{A}$ *est l'idéal engendré par les polynômes*

$$(2) \qquad X_{h+j} - f_{h+j}(X_1 , X_2 , \ldots , X_h) , \qquad j = 1 , \ldots , n - h ,$$

$f_{h+j}(X_1 , X_2 , \ldots , X_h)$ *étant des formes homogènes linéaires à coefficients algébriques.*

Ces $n - h$ polynômes sont algébriquement indépendants, et l'idéal $\mathfrak{A}$ est premier, donc V est une variété algébrique de dimension h (cf. [1], exemple p. 04, et lemme 3.3).

LEMME 1.1. - Soient K une extension finie de Q, de degré n, Ω la clôture algébrique de Q, et $\alpha_i \in K$, $i = 1, 2, \ldots, h$, des nombres linéairement indépendants sur Q.

Alors, des nombres de $\sum Q\alpha_i$, et de même norme, sont dans un ensemble algébrique de Ω^n de dimension $h - 1$.

En effet, un nombre de Q, et de norme c, est sur l'ensemble algébrique $V_1 = V(\mathfrak{A}_1)$, où $\mathfrak{A}_1$ est l'idéal engendré par les polynômes

$$X_{h+j} - f_{h+j}(X_1, X_2, \ldots, X_h), \qquad j = 1, 2, \ldots, n - h, \tag{2}$$

et

$$X_1 \times X_2 \times \ldots \times X_n - c. \tag{3}$$

Ces $n - h + 1$ polynômes à coefficients algébriques sont algébriquement indépendants, donc V_1 est un ensemble algébrique de Ω^n, équidimensionnel de dimension $n - (n - h + 1) = h - 1$.

Exemple 1.1. - Soit $K = Q[\theta]$ une extension finie de Q, de degré $n \geqslant 3$. Si $G(K)$ est représenté par le groupe de toutes les permutations de n objets, il est impossible qu'il y ait une infinité de nombres de Salem dans $Q + Q\theta + \ldots + Q\theta^{n-2}$.

Les nombres de Salem et leurs inverses forment, en effet, un sous-groupe du groupe des unités de K à un générateur d'ordre infini ; on applique alors le lemme 1.1, puis le théorème 1.2 (cf. [3]).

Exemple 1.2. - Soit $K = Q[\theta]$, $\theta = 15^{1/29}$ réel. Il est alors impossible qu'une infinité d'unités de K soient dans

$$Q + Q\theta + \ldots + Q\theta^{14}.$$

En effet, K a un corps conjugué réel et 14 corps conjugués complexes, donc le groupe des unités de K a 14 générateurs d'ordre infini, et on applique le lemme 1.1 et le théorème 1.2.

THÉORÈME 1.3 ([2], chapitre III, théorème 3.4). - Soient K une extension finie de Q, de degré n, Ω la clôture algébrique de Q, Γ un sous-groupe de K^*

à s générateurs d'ordre infini, et $\alpha_i \in K$, $i = 1 , 2 , \dots , h - 1$, linéairement indépendants sur Q . On suppose $s + h \leqslant n$, $Q[\alpha_1 , \dots , \alpha_{h-1}] = K$, et on pose $\alpha_0 = 1$.

Alors, si une infinité de nombres de Γ , de même norme sont dans $\sum Q\alpha_i$, une infinité d'entre eux sont sur un ensemble algébrique de Ω^n de dimension $h - 2$.

Démonstration. - D'après le lemme 1.1, tous ces nombres de même norme, soit c cette norme, sont sur un ensemble algébrique $V_1 = V(\mathfrak{A}_1)$ de Ω^n , où l'idéal $\mathfrak{A}_1$ est engendré par les polynômes

$$(2) \qquad X_{h+j} - f_{h+j}(X_1 , X_2 , \dots , X_h) , \qquad j = 1 , 2 , \dots , n - h ,$$

et

$$(3) \qquad X_1 \times X_2 \times \dots \times X_n - c .$$

On a $s + \dim V \leqslant n - 1$, et on peut appliquer le théorème 1.1 : $\exists\, \alpha \in \Gamma$ et $\exists\, \gamma$, sous-groupe de Γ , tels que, pour une infinité de $\varepsilon \in \gamma$, on a

$$N(\alpha\varepsilon) = c , \qquad \text{i. e.} \quad \varepsilon^{(1)} \times \varepsilon^{(2)} \times \dots \times \varepsilon^{(n)} = e , \qquad \text{où} \quad e = \frac{c}{N(\alpha)} .$$

D'autre part, d'après la formule (1) du théorème 1.1, on a $N_i \in Z$, non tous nuls, $i = 1 , 2 , \dots , n - 1$, tels que

$$\varepsilon^{(1)N_1} \times \varepsilon^{(2)N_2} \times \dots \times \varepsilon^{(n-1)N_{n-1}} = 1 , \qquad \forall\, \varepsilon \in \gamma .$$

On pose $N_n = 0$, $-(N_1 + N_2 + \dots + N_n) = m$, et $M_i = nN_i - m$. Ces M_i ne sont pas tous nuls, leur somme est nulle, et on a, pour une infinité de $\varepsilon \in \gamma$,

$$\varepsilon^{(1)M_1} \times \varepsilon^{(2)M_2} \times \dots \times \varepsilon^{(n)M_n} = e^{-m} .$$

Finalement, une infinité de $\varepsilon \in \gamma$ annulent les polynômes (2) et (3), et le polynôme

$$(4) \qquad X_{i_1}^{M_{i_1}} X_{i_2}^{M_{i_2}} \dots X_{i_k}^{M_{i_k}} - e^{-m} X_{i_{k+1}}^{M_{i_{k+1}}} X_{i_{k+2}}^{M_{i_{k+2}}} \dots X_{i_n}^{M_{i_n}} ,$$

où $M_{i_j} > 0$ et $\sum_{j=1}^{k} M_{i_j} = \sum_{j=k+1}^{n} M_{i_j}$. Ces polynômes sont algébriquement indépendants, donc engendrent un idéal $\mathfrak{A}_2$ équidimentionnel, de dimension $h - 2$, et l'ensemble algébrique $V_2 = V(\mathfrak{A}_2)$ de Ω^n est équidimensionnel de dimension $h - 2$.

Q. E. D.

Exemple 1.3. - Soit $K = \mathbb{Q}[\theta]$, où θ est le seul zéro réel du polynôme

$$X^3 - 2X + 2 \ .$$

Le groupe des unités de K a un seul générateur d'ordre infini et, en appliquant le lemme 1.1 et le théorème 1.2, on voit qu'il ne peut y avoir une infinité d'unités de K dans $\mathbb{Q} + \mathbb{Q}\theta$. On obtient le même résultat en appliquant le théorème 1.3, car un ensemble algébrique de dimension 0 ne contient qu'un nombre fini de points.

Remarque 1.1. -- On ne peut pas itérer le raisonnement du théorème 1.3, car le polynôme (4'), qu'on obtient par un tel raisonnement, et le polynôme (4) ne sont pas forcément algébriquement indépendants.

Remarque 1.2. - Lors de l'application du théorème 1.2, étant donnés K et s , on cherche à obtenir pour h la plus grande valeur possible. En tenant compte du lemme 1.1, on a vu que si $\alpha_i \in K$ sont linéairement indépendants sur $\mathbb{Q}$, et que si le degré de K sur $\mathbb{Q}$, n , est premier, ou si $G(K)$ est représenté par le groupe de toutes les permutations de n objets, il ne peut pas y avoir une infinité d'éléments de Γ sur $\sum_{i=1}^{h} \mathbb{Q}\alpha_i$, pour $h \leqslant n - s$.

Cette valeur de h ne peut pas être améliorée par l'utilisation du théorème 1.3, car, pour ce théorème, on doit aussi avoir $h \leqslant n - s$.

2. Le théorème de Dirichlet-Hasse-Chevalley pour un corps de nombres algébriques ([4]).

Soit K un corps quelconque. Une valuation de K est une application

$$\varphi : K \to \mathbb{R}_+ \qquad (\mathbb{R}_+ \text{ nombres réels positifs ou nuls})$$

telle que :

(i) $$\varphi(a) = 0 \iff a = 0 \ ,$$

(ii) $$\varphi(ab) = \varphi(a).\varphi(b) \ , \qquad \forall\ a\ ,\ b \in K \ ,$$

(iii) $\exists\ C \in \mathbb{R}_+$ telle que $\varphi(a + b) \leqslant C \max\{\varphi(a)\ ,\ \varphi(b)\}$, $\qquad \forall\ a\ ,\ b \in K$.

On appelle norme de φ la valeur $\|\varphi\| = \inf C$, où C sont toutes les constantes possibles pour la condition (iii). Cette condition est alors satisfaite avec $\|\varphi\|$.

On dit que φ est la valuation triviale si $\varphi(a) = 1$, $\forall\ a \in K$, $a \neq 0$, que

φ est archimédienne si $\|\varphi\| > 1$, et que φ est non archimédienne si $\|\varphi\| = 1$. La valuation triviale est non archimédienne.

On montre que si φ est une application de K dans R_+ satisfaisant les conditions (i) et (ii), on a

$$\{\text{(iii) avec } \|\varphi\| < 2\} \iff \{\varphi(a + b) \leqslant \varphi(a) + \varphi(b) \ , \ \forall\ a \ , \ b \in K\} \ .$$

Une valuation de K induit une topologie dans K , et on dit que deux valuations φ et φ' sont équivalentes si elles induisent la même topologie ; alors $\exists\ \alpha \in R$, $\alpha > 0$, telle que $\varphi' = \varphi^{\alpha}$. Si φ est une valuation, sa classe d'équivalence est $\{\varphi^{\alpha} \mid \alpha \in R \ , \ \alpha > 0\}$, et les classes sont appelées diviseurs premiers de K . Comme $\|\varphi^{\alpha}\| = \|\varphi\|^{\alpha}$, on voit que dans tout diviseur premier de K on peut trouver une valuation φ avec $\|\varphi\| < 2$, i. e. satisfaisant l'inégalité du triangle.

Si φ est une valuation archimédienne (resp. non archimédienne), toutes les valuations équivalentes à φ sont aussi archimédiennes (resp. non archimédiennes), et on dit que son diviseur premier est archimédien (resp. non archimédien).

On note $\mathfrak{M}(K)$ l'ensemble de tous les diviseurs premiers de K , à l'exclusion du diviseur trivial, $\mathfrak{M}_0(K)$ l'ensemble des diviseurs non archimédiens, à l'exclusion du diviseur trivial, et $\mathfrak{M}_\infty(K)$ l'ensemble des diviseurs archimédiens. On verra plus loin que $\mathfrak{M}_\infty(K)$ est fini, et que $\mathfrak{M}_0(K)$ est infini dénombrable.

Soit $S \subset \mathfrak{M}(K)$, avec $S \supset \mathfrak{M}_\infty(K)$ et card $S < \infty$. On pose

$$K_S = \{a \in K \mid \varphi(a) \leqslant 1 \ , \ \varphi \in P \ , \ \forall\ P \notin S\} \ ,$$
$$K_S^* = \{a \in K \mid \varphi(a) = 1 \ , \ \varphi \in P \ , \ \forall\ P \notin S\} \ .$$

K_S et K_S^* ne dépendent pas du choix des valuations $\varphi \in P$, et sont respectivement l'anneau des S-idèles principaux de K et le groupe des S-adèles principaux de K . K_S est un anneau de Dedekind.

Comme cas particulier du théorème de Dirichlet-Hasse-Chevalley ([4], chapitre 5, théorème 5.3.10), on a, avec les notations précédentes, le théorème suivant :

THÉORÈME 2.1. - Soient K une extension finie de Q , et $s = \text{card } S$, alors

$$K_S^* = U_K \times (\eta_1) \times \ldots \times (\eta_{s-1}) \qquad \text{(produit direct)} \ ,$$

où U_K est le groupe (cyclique et fini) des racines de l'unité de K , et (η_i) , $i = 1 \ , \ 2 \ , \ \ldots \ , \ s - 1$, des groupes cycliques infinis (d'une manière plus générale, ce théorème s'énonce pour des corps globaux).

K étant une extension finie de Q, toute valuation de K induit une valuation de Q, sa restriction à Q ; ainsi, toute valuation de K est l'extension d'une valuation de Q.

Or $\mathfrak{M}(Q) = \{\infty , 2 , 3 , \dots , p , \dots \mid p \text{ premier}\}$, où ∞ est le diviseur premier de la valeur absolue ordinaire de Q, et p le diviseur premier de la valeur absolue p-adique de Q. On sait que, pour tout $p \in \mathfrak{M}(Q)$, toute valuation $\varphi_p \in p$ s'étend de manière unique au corps Q_p (complétion de Q pour φ_p), puis à la clôture algébrique Ω_p de Q_p (avec $Q_\infty = R$ corps des nombres réels, et $\Omega_\infty = C$ corps des complexes), l'extension d'une valuation archimédienne (resp. non archimédienne) étant archimédienne (resp. non archimédienne).

On a alors la proposition suivante ([4], chapitre 2, proposition 2.4.1).

PROPOSITION 2.1. - *Soit μ un Q-monomorphisme : $K \to \Omega_p$, i. e. un homomorphisme de K dans Ω_p injectif et appliquant tout point de Q sur lui-même, et soit φ_p une valuation de Ω_p.*

Alors $\varphi_p \circ \mu$ est une valuation de K, et toute valuation de K est de cette forme.

Si φ_p et φ'_p sont équivalentes, $\varphi_p \circ \mu$ et $\varphi'_p \circ \mu$ le sont aussi, et on peut parler des extensions des diviseurs premiers de Q, tout diviseur premier de K étant extension d'un diviseur premier de Q.

Soit n le degré de K sur Q, on a alors n Q-monomorphismes de K dans Ω_p ; en effet, si θ est un élément primitif de K et $\theta^{(i)}$, $i = 1, 2, \dots, n$, les conjugués de $\theta^{(1)} = \theta$, on a, pour tout Q-monomorphisme $\mu : K \to \Omega_p$, $\mu(\theta) = \theta^{(i)}$, pour un certain i.

φ étant une valuation de Q, on a donc au plus n extensions différentes de φ à K ; la proposition suivante donne leur nombre exact ([4], chapitre 2, propositions 2.4.5 et 2.4.6).

PROPOSITION 2.2. - *Soient $K = Q[\theta]$, θ algébrique sur Q de degré n, $f(X) \in Q[X]$ le polynôme irréductible de θ, $p \in \mathfrak{M}(Q)$, $\varphi_p \in p$, et*

$$f(X) = f_1(X)\, f_2(X) \dots f_r(X)$$

la décomposition de $f(X)$ en facteurs irréductibles dans $Q_p[X]$.

Alors, il y a exactement r extensions non équivalentes deux à deux de φ_p à K, deux extensions $\varphi_p \circ \mu_1$ et $\varphi_p \circ \mu_2$ étant égales, si $\mu_1(\theta)$ et $\mu_2(\theta)$ sont conjugués algébriques sur Q, et non équivalentes dans le cas contraire.

On notera p_i^* , $i = 1 , 2 , \dots , r$, les extensions de p , et S^* l'ensemble de toutes les extensions des diviseurs premiers contenus dans le sous-ensemble S de $\mathfrak{M}(Q)$. On a

$$\mathfrak{M}_\infty^*(Q) = \mathfrak{M}_\infty(K) \qquad \text{et} \qquad \mathfrak{M}_0^*(Q) = \mathfrak{M}_0(K) \ ;$$

$\mathfrak{M}_\infty(Q)$ étant fini et $\mathfrak{M}_0(Q)$ étant infini dénombrable, $\mathfrak{M}_\infty(K)$ et $\mathfrak{M}_0(K)$ sont respectivement fini et infini dénombrable.

Avec ces notations, on a de plus la proposition suivante ([4], chapitre 4, théorème 4.1.7).

PROPOSITION 2.3. - Soit K une extension finie de Q , et soit $S \subset \mathfrak{M}(Q)$ avec $S \supset \mathfrak{M}_\infty(Q)$.

Alors K est le corps des fractions de K_{S^*} , K_{S^*} est intégralement clos, K_{S^*} est la fermeture intégrale de Q_S dans K , et tout nombre $\alpha \in K$ peut s'écrire $\alpha = \frac{\beta}{c}$, où $\beta \in K_{S^*}$ et $c \in Q$.

3. Applications.

D'après le théorème 2.1 et la proposition 2.2, on peut énoncer la proposition suivante :

PROPOSITION 3.1. - Soient $K = Q[\theta]$ une extension finie de Q , de degré n , $f(X)$ le polynôme irréductible de θ sur Q , et soit

$$S = \{\infty , p_1 , p_2 , \dots , p_r\} \subset \mathfrak{M}(Q)$$

avec card $S < \infty$ et $s = s_\infty + s_1 + \dots + s_r - 1$, s_∞ étant le nombre de facteurs irréductibles dans la décomposition de $f(X)$ dans $R[X]$, et s_i celui des facteurs irréductibles dans la décomposition de $f(X)$ dans $Q_{p_i}[X]$.

Alors le groupe $K_{S^*}^*$ a s générateurs d'ordre infini.

Dans le cas où $S = \{\infty\}$, on retrouve le théorème classique de Dirichlet.

Exemple 3.1. - Comme dans l'exemple 1.2, on considère $K = Q[\theta]$ où θ est la racine réelle du polynôme $X^{29} - 15$, et soit $S = \{\infty , 3 , 5\}$. On a déjà vu que $X^{29} - 15$ se décompose en 15 facteurs irréductibles dans $R[X]$; d'autre part, le polygone de Newton de $X^{29} - 15$ montre que ce polynôme est irréductible dans $Q_3[X]$ et dans $Q_5[X]$. Alors $s = 15 + 1 + 1 - 1 = 16$, et en appliquant la propo-

sition 3.1, le lemme 1.1, et le théorème 1.2, on voit qu'il est impossible qu'une infinité de nombres de $K^*_{S^*}$, de même norme, soient situés dans $Q + Q\theta + \ldots + Q\theta^{12}$.

Soit $M = \{p_1^{n_1} \times p_2^{n_2} \times \ldots \times p_r^{n_r} \mid n_i \in Z,\ n_i \geqslant 0,\ p_i \in S,\ p_i \neq \infty\}$, c'est une partie multiplicative de Z, contenant 1, et soit $Q_S = ZM^{-1}$ l'anneau des fractions de Z relatif à M. Donc, d'après la proposition 2.3, K_{S^*} est la fermeture intégrale de ZM^{-1}. M est aussi une partie multiplicative de l'anneau A des entiers algébriques de K, et on a $K_{S^*} = AM^{-1}$; en effet, pour le voir, il suffit de remarquer que si α est zéro du polynôme

$$X^n + \frac{a_0}{p^{m_0}} X^{n-1} + \ldots + \frac{a_n}{p^{m_n}}, \qquad a_i, p \in Z, \quad p \text{ premier} \quad \text{et} \quad (a_i, p) = 1,$$

$p\alpha$ est zéro du polynôme

$$X^n + \frac{a_0}{p^{m_0-1}} X^{n-1} + \ldots + \frac{a_n}{p^{m_n-n}}.$$

On a aussi la proposition suivante :

PROPOSITION 3.2. - <u>Si une infinité de nombres de K_{S^*} ont la même norme, une infinité d'entre eux sont associés deux à deux dans K_{S^*}</u> (i. e. : <u>le quotient de deux quelconques de ces nombres est une unité de K_{S^*}</u>).

<u>Démonstration</u>. - Avec les notations précédentes, soient $K_{S^*} = AM^{-1}$, et cp la norme de ces nombres, $c \in Z$, $p \in M$ M^{-1}, $(c, p_i) = 1$ pour tout $p_i \in M$. Soit ω un de ces nombres, on peut alors trouver $q \in M$, tel que $q\omega \in A$ et tel que

$$N(q\omega) = cp_1^{e_1} \times p_2^{e_2} \times \ldots \times p_r^{e_r}, \qquad \text{avec } e_i \in Z, \quad e_i \geqslant 0$$

(q et e_i dépendent de ω).

A étant l'anneau des entiers algébriques d'une extension de Q de degré n, tout idéal de A est produit fini d'idéaux premiers de A (A est un anneau de Dedekind) et, à tout idéal premier $\mathfrak{P}$ de A, correspond un nombre premier p et un nombre f, avec $1 \leqslant f \leqslant n$, tels que $N(\mathfrak{P}) = p$, $N(\mathfrak{P})$ étant la norme de l'idéal $\mathfrak{P}$. Comme il y a un nombre fini seulement d'idéaux de A de norme donnée, il existe dans A un nombre fini d'idéaux $\mathfrak{C}_i$, de norme c, et un nombre fini d'idéaux premiers $\mathfrak{P}_j$, $j = 1, 2, \ldots, u$, avec $N(\mathfrak{P}_j) \in M$, tels que, pour tout nombre $q\omega$ considéré, l'idéal principal $(q\omega)$ se décompose comme suit :

$$(q\omega) = \mathfrak{C}_i \times \mathfrak{P}_1^{f_1} \times \mathfrak{P}_2^{f_2} \times \ldots \times \mathfrak{P}_u^{f_u} , \qquad \mathfrak{C}_i \text{ et } f_j \text{ dépendants de } q\omega .$$

En particulier, on a une infinité de ces nombres $q\omega$ pour lesquels

$$(q\omega) = \mathfrak{C} \times \mathfrak{P}_1^{f_1} \times \mathfrak{P}_2^{f_2} \times \ldots \times \mathfrak{P}_u^{f_u} , \qquad \mathfrak{C} \text{ étant l'un des } \mathfrak{C}_i .$$

D'autre part, h étant le nombre de classes de l'anneau A, $\mathfrak{A}^h$ est principal pour tout idéal $\mathfrak{A}$ de A ; soit donc $(\pi_j) = \mathfrak{P}_j^h$, $\pi_j \in A$.

Pour ces nombres $q\omega$, on a ainsi

$$(q\omega) = \mathfrak{C} \times (\pi_1)^{g_1} \times (\pi_2)^{g_2} \times \ldots \times (\pi_u)^{g_u} \times \mathfrak{P}_1^{h_1} \times \mathfrak{P}_2^{h_2} \times \ldots \times \mathfrak{P}_u^{h_u} \text{ avec } 1 \leqslant h_j \leqslant h-1$$

h_j et g_j dépendants du nombre $q\omega$. Donc on a une infinité de ces $q\omega$ pour lesquels les h_j sont fixés, c'est-à-dire pour lesquels

$$(q\omega) = \mathfrak{B} \times \mathfrak{C} \times (\pi_1)^{g_1} \times (\pi_2)^{g_2} \times \ldots \times (\pi_u)^{g_u} , \qquad \text{où } \mathfrak{B} = \mathfrak{P}_1^{h_1} \times \mathfrak{P}_2^{h_2} \times \ldots \times \mathfrak{P}_u^{h_u} ,$$

pour ces h_j fixés.

Si l'ensemble des g_1 a un point d'accumulation fini g_1^*, on a pour une infinité de $q\omega$:

$$(q\omega) = \mathfrak{B} \times \mathfrak{C} \times (\pi_1)^{g_1^*} \times (\pi_2)^{g_2} \times \ldots \times (\pi_u)^{g_u} .$$

En itérant ce raisonnement (et en permutant éventuellement les indices), on voit qu'il existe k tel que, pour une infinité de $q\omega$,

$$(q\omega) = \mathfrak{B} \times \mathfrak{C} \times (\pi_1)^{g_1^*} \times \ldots \times (\pi_k)^{g_k^*} \times (\pi_{k+1})^{g_{k+1}} \times \ldots \times (\pi_u)^{g_u} ,$$

où les g_j^* sont fixés, et où les g_j n'ont pas de point d'accumulation fini. Soit $q_0\ \omega_0$ un de ces nombres, et soit

$$(q_0\ \omega_0) = \mathfrak{B} \times \mathfrak{C} \times (\pi_1)^{g_1^*} \times \ldots \times (\pi_k)^{g_k^*} \times (\pi_{k+1})^{g_{k+1}^*} \times \ldots \times (\pi_u)^{g_u^*} .$$

Pour une infinité de $q\omega$, on a alors

$$(q\omega) = \mathfrak{B} \times \mathfrak{C} \times (\pi_1)^{g_1} \times (\pi_2)^{g_2} \times \ldots \times (\pi_u)^{g_u} ,$$

avec $g_j \geqslant g_j^*$, i. e.

$$(q\omega) = (q_0\ \omega_0)\ (\pi_1)^{m_1} \dots (\pi_u)^{m_u}\ , \qquad m_j \in Z\ ,\quad m_j \geqslant 0\ ,$$

d'où

$$q\omega = q_0\ \omega_0\ \pi_1^{m_1} \times \dots \times \pi_u^{m_u} \times \varepsilon\ ,$$

où ε est une unité de A .

Mais $\pi_j \in A$ et $N(\pi_j) \in M$, donc π_j est une unité de K_{S^*} , et $\omega = \omega_0\ \varphi$ où $\varphi = \frac{q_0}{q}\ \pi_1^{m_1} \times \dots \times \pi_u^{m_u} \times \varepsilon$ est aussi une unité de K_{S^*} , car q et q_0 en sont. On a donc une infinité de nombres ω associés dans K_{S^*} , car si $\omega = \omega_0\ \varphi$ et $\omega' = \omega_0\ \varphi'$, $\frac{\omega'}{\omega} = \frac{\varphi'}{\varphi}$ est une unité de K_{S^*} .

Q. E. D.

Exemple 3.2. - Soient $f(X) \in Z[X]$ un polynôme irréductible de degré n , $M = \{p_i^{n_1} \times p_2^{n_2} \times \dots \times p_r^{n_r} \mid n_i \in Z\ ,\ n_i \geqslant 0\ ,\ p_i$ premiers$\}$, soient s_∞ le nombre de facteurs irréductibles dans la décomposition de $f(X)$ dans $R[X]$, et s_i celui des facteurs irréductibles dans la décomposition de $f(X)$ dans $Q_{p_i}[X]$; soit $b \in Q$. Alors, si $s = s_\infty + s_1 + \dots + s_r \leqslant n - 1$, il est impossible qu'il y ait une infinité de solutions $X\ ,\ Y \in ZM^{-1}$ à l'équation

$$Y^n\ f(\frac{X}{Y}) = b\ . \tag{5}$$

Si $b \notin ZM^{-1}$, l'équation n'a aucune solution. On suppose donc que $b \in ZM^{-1}$ et qu'il y a une infinité de solutions.

Soit $\alpha^{(i)}$, $i = 1\ ,\ 2\ ,\ \dots\ ,\ n$, les n racines de $f(X)$; on a donc

$$f(X) = a \prod_{i=1}^{n} (X - \alpha^{(i)}) = \frac{1}{a^{n-1}} \prod_{i=1}^{n} (aX - a\alpha^{(i)})\ ,$$

où $a \in Z$ est le coefficient directeur de $f(X)$, et

$$Y^n\ f(\frac{X}{Y}) = \frac{1}{a^{n-1}} \prod_{i=1}^{n} (aX - a\alpha^{(i)}\ Y)\ .$$

Mais $a\alpha^{(i)} = \beta^{(i)}$ est un entier algébrique, et $aX \in ZM^{-1}$ pour tout $X \in AM^{-1}$, et de même $a^{n-1}\ b = c \in ZM^{-1}$. Donc, si l'équation (5) a une infinité de solutions $X\ ,\ Y \in ZM^{-1}$, l'équation suivante a aussi une infinité de solutions $X\ ,\ Y \in ZM^{-1}$,

(6) $$\prod_{i=1}^{n} (X + Y\beta^{(i)}) = c \quad .$$

On pose $\alpha = \alpha^{(1)}$, et soient $K = Q[\alpha]$, A l'anneau des entiers de K , et $S = \{\infty , p_1 , p_2 , \dots , p_r\}$. Alors on a une infinité de nombres

$$\omega = X + Y\beta \in AM^{-1} = K_{S*}$$

tels que

$$\prod_{i=1}^{n} \omega^{(i)} = N(\omega) = c \quad .$$

D'après la proposition 3.2, il existe $\omega_0 = X_0 + Y_0\ \beta \in K_{S*}$ tel que, pour une infinité de $\omega = X + Y\beta \in K_{S*}$, on a $\frac{\omega}{\omega_0} \in K^*_{S*}$, avec

$$N(\frac{\omega}{\omega_0}) = 1 \qquad \text{et} \qquad \frac{\omega}{\omega_0} \in Q\,\frac{1}{\omega_0} + Q\,\frac{\beta}{\omega_0} \quad .$$

Soit $\omega_1 = X_1 + Y_1\ \beta$ un de ces nombres ; on a alors une infinité de nombres de K^*_{S*} sur $Q.\frac{\omega_1}{\omega_0} + Q.\frac{\beta}{\omega_0}$, donc aussi sur $Q.1 + Q.\frac{\beta}{\omega_1}$. On peut choisir ω_1 tel que $X_1 \neq 0$, et alors 1 et $\frac{\beta}{\omega_1}$ sont linéairement indépendants sur Q et $Q[\frac{\beta}{\omega_1}] = K$. Comme $s + 1 \leqslant n$, on peut appliquer le théorème 1.3 : on doit avoir une infinité de nombres sur un ensemble algébrique de dimension 0 ; ceci est impossible et achève la démonstration.

BIBLIOGRAPHIE

[1] ARCHINARD (Gabriel). - Théorie de Chabauty sur les équations diophantiennes, I., Séminaire Delange-Pisot-Poitou : Théorie des nombres, 7e année, 1965/66, n° 16, 23 p.

[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] SALEM (Raphael). - Power series with integral coefficients, Duke Math. J., t. 12, 1945, p. 153-172.

[4] WEISS (Edwin). - Algebraic number theory. - New York, McGraw-Hill, 1963 (International Series in pure and applied Mathematics).