Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 8 (1962)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: INTRODUCTION A LA THÉORIE DES NOMBRES ALGÉBRIQUES
Autor: Pisot, Charles
DOI: https://doi.org/10.5169/seals-37964

INTRODUCTION A LA THÉORIE DES NOMBRES ALGÉBRIQUES [1])

par Charles PISOT.

ORIGINE DE LA THÉORIE DES NOMBRES ALGÉBRIQUES. — L'un des principaux problèmes dont s'occupe la théorie des nombres est celui de la résolution des équations, en ajoutant la condition que les solutions doivent être des nombres entiers. Pour attaquer cette question, on a été amené à étendre la notion de nombre entier et plus généralement celle de nombre rationnel, non seulement à celle de nombre réel ou complexe, mais à des ensembles moins généraux. Nous allons essayer d'expliquer ce problème sur une équation particulière, à savoir

$$x^2 - dy^2 = 1$$

appelée ÉQUATION DE PELL-FERMAT; d est un entier ne contenant aucun facteur carré parfait, donc aussi $d \neq 0$. On peut écrire cette équation sous la forme

$$(x - y\sqrt{d})\ (x + y\sqrt{d}) = 1\ . \qquad (1)$$

Cette écriture suppose bien entendu que nous connaissions déjà l'ensemble $\mathfrak{R}$ des nombres réels et même (si $d < 0$) l'ensemble $\mathfrak{C}$ des nombres complexes.

ANNEAU. — La forme (1) de l'équation de *Pell-Fermat* suggère d'étudier les quantités de la forme $\alpha = a + a'\sqrt{d}$ où a et a' sont des entiers. Nous appellerons $\mathscr{A}$ l'ensemble de ces quantités α.

Il est clair que *si* $\alpha \in \mathscr{A}$, $\beta \in \mathscr{A}$, *on a aussi* $\alpha + \beta \in \mathscr{A}$ *et* $\alpha\beta \in \mathscr{A}$. *On dit que* $\mathscr{A}$ *est un* ANNEAU. Ainsi l'ensemble $\mathscr{Z}$ des entiers est un anneau.

---

[1]) Conférence prononcée à Grenoble, dans le cadre des « Journées mathématiques de Grenoble », 21-22 mai 1960.

CORPS. — Plus généralement considérons des nombres de la forme $\sigma = s+s'\sqrt{d}$, $\tau = t+t'\sqrt{d}$, où s, s', t, t' sont des nombres rationnels. Nous appellerons leur ensemble $\mathscr{C}$. Il est encore clair que $\mathscr{C}$ est un anneau et que $\mathscr{C} \in \mathscr{A}$; mais ici il y a plus. Définissons en effet pour tout nombre $\sigma = s+s'\sqrt{d} \in \mathscr{C}$ son CONJUGUÉ $\bar{\sigma}$ par $\bar{\sigma} = s-s'\sqrt{d}$, alors aussi $\bar{\sigma} \in \mathscr{C}$, et appelons NORME de σ le nombre $N(\sigma) = \sigma\bar{\sigma} = s^2-ds'^2$ alors $N(\sigma)$ est rationnel et $N(\sigma) = 0$ entraîne $\sigma = 0$, car d n'est pas le carré d'un nombre rationnel.

Par suite si $\tau \in \mathscr{C}$, $\sigma \in \mathscr{C}$ avec $\sigma \neq 0$, on a

$$\frac{\tau}{\sigma} = \frac{\tau\bar{\sigma}}{\sigma\bar{\sigma}} = \frac{\tau\bar{\sigma}}{N(\sigma)},$$

donc $\dfrac{\tau}{\sigma} \in \mathscr{C}$. On dit que l'ensemble $\mathscr{C}$ est un CORPS. Ainsi l'ensemble des nombres rationnels $\mathfrak{Q}$, celui des nombres réels $\mathfrak{R}$, celui des nombres complexes $\mathfrak{C}$, sont des corps.

Remarquons encore tout élément $\sigma = s+s'\sqrt{d} \in \mathscr{C}$ est racine d'une équation du second degré $(x-s)^2 - ds'^2 = 0$ à coefficients rationnels.

De tels nombres sont appelés NOMBRES ALGÉBRIQUES. Plus généralement, *on appellera* NOMBRE ALGÉBRIQUE *tout zéro réel ou complexe d'un polynôme à coefficients rationnels.*

ANNEAU EUCLIDIEN. — Un anneau a des propriétés semblables à celles de l'ensemble des entiers. Cherchons à pousser cette analogie plus loin en essayant de *définir une division avec reste dans l'anneau* $\mathscr{A}$ précédent. Nous dirons que $\mathscr{A}$ est un ANNEAU EUCLIDIEN, si $\mathscr{A}$ possède la propriété suivante:

Quels que soient $\alpha \in \mathscr{A}$ *et* $\beta \in \mathscr{A}$ *avec* $\beta \neq 0$, *on peut toujours trouver dans* $\mathscr{A}$ *deux éléments* γ *et* ρ *tels que l'ont ait:*

$$\alpha = \beta\gamma + \rho \quad et \quad |N(\rho)| < |N(\beta)|.$$

On n'exige pas l'unicité pour ces nombres γ et ρ. Si $\mathscr{A}$ est euclidien, on peut définir l'algorithme d'*Euclide* pour deux éléments $\alpha \neq 0$, $\beta \neq 0$ de $\mathscr{A}$, donc leur p.g.c.d. et de là, comme pour les entiers, obtenir la décomposition d'un élément $\alpha \in \mathscr{A}$,

$\alpha \neq 0$ en « *nombres premiers* » de $\mathscr{A}$, c'est-à-dire en nombres de $\mathscr{A}$ n'ayant pas d'autres diviseurs dans $\mathscr{A}$ qu'eux-mêmes ou des « *unités* » de $\mathscr{A}$; on dira que $\eta \in \mathscr{A}$ est une *unité* de $\mathscr{A}$ si $\eta \neq 0$ et si $\frac{1}{\eta} \in \mathscr{A}$. La décomposition de α en nombres premiers est alors unique à des unités près.

EXEMPLE : $d = -1$, alors $\alpha = a+a'\sqrt{-1} = a+ia'$ et $\bar{\alpha} = a-ia'$, donc $N(\alpha) = a^2+a'^2 = |\alpha|^2$. L'égalité $\alpha = \beta\gamma+\rho$ s'écrit aussi $\frac{\alpha}{\beta}-\gamma = \frac{\rho}{\beta}$ et $|N(\rho)| < |N(\beta)|$ s'écrit $|\rho|^2 < |\beta|^2$ ou encore $\left|\frac{\rho}{\beta}\right| < 1$.

Il est clair que quels que soient α, $\beta \neq 0$, on peut trouver $\gamma = c+ic'$, c, c' entiers tels que $\left|\frac{\alpha}{\beta}-\gamma\right| < 1$. Donc l'anneau $\mathscr{A}$, appelé dans ce cas ANNEAU DE GAUSS, est un anneau euclidien.

Etudions les « *nombres premiers* » de cet anneau. Soit π un tel nombre premier, alors $\bar{\pi}$ est manifestement aussi premier. Le nombre $N(\pi) = \pi\bar{\pi}$ est entier et cet entier n'a, dans l'anneau de *Gauss*, que la décomposition unique $N(\pi) = \pi\bar{\pi}$. Donc, ou bien $\pi = p$ est un nombre premier ordinaire, alors $\bar{\pi} = p$ et $N(\pi) = p^2$, ou alors $N(\pi) = p$ nombre premier ordinaire, qui par suite est décomposable en $p = \pi\bar{\pi}$ dans $\mathscr{A}$. Dans ce dernier cas, soit $\pi = u+iu'$, alors $p = \pi\bar{\pi} = u^2+u'^2$, donc $p \equiv 1 \pmod 4$. Réciproquement, si $p = 4n+1$ avec $n > 1$, le théorème de *Wilson* montre que $(4n)!+1 \equiv 0 \pmod p$; or $2n+k \equiv k+1-2n \pmod p$, en remplaçant pour $k = 1, \ldots, 2n$ on voit aussi que $(-1)^{2n}(2n!)^2+1 \equiv 0 \pmod p$. Si p était premier dans $\mathscr{A}$, il diviserait l'un des facteurs $(2n)!+i$, $(2n)!-i$, donc aussi l'autre, par suite aussi leur somme $2(2n)!$, ce qui est impossible car $p = 4n+1 > 2n$.

Ainsi *un nombre premier ordinaire p impair n'est pas premier dans* $\mathscr{A}$ *et se décompose dans* $\mathscr{A}$ *en* $p = \pi\bar{\pi}$, *où* π *est premier dans* $\mathscr{A}$, *si et seulement si* $p \equiv 1 \pmod 4$.

On peut déduire de cela que tout diviseur d'une somme de deux carrés $a^2+a'^2$, où a et a' sont des entiers premiers entre eux est lui-même une somme de carrés.

IDÉAUX. — Malheureusement tous les anneaux $\mathscr{A}$ ne sont pas euclidiens et il existe des anneaux $\mathscr{A}$ où la décomposition en nombres premiers de l'anneau n'est pas unique à des unités près. Exemple: $d = -5$. On a $(2+i\sqrt{5})(2-i\sqrt{5}) = 3.3$; 3 et $2+i\sqrt{5}$ sont premiers dans $\mathscr{A}$ et $\frac{2 \pm i\sqrt{5}}{3}$ n'est pas une unité de $\mathscr{A}$.

La propriété caractéristique des multiples d'un élément de $\mathscr{A}$ est la suivante: les multiples forment *un ensemble* $\mathscr{I}$ *tel que si* $\alpha \in \mathscr{I}$ *et* $\beta \in \mathscr{I}$, *on a* $\alpha \pm \beta \in \mathscr{I}$ *et* $\alpha\gamma \in \mathscr{I}$ *quel que soit* $\gamma \in \mathscr{A}$. Tout ensemble $\mathscr{I}$ ayant ces deux propriétés *est appelé un* IDÉAL *de* $\mathscr{A}$. Les multiples d'un élément $\alpha \in \mathscr{A}$ forment donc un idéal noté (α) et appelé IDÉAL PRINCIPAL. Dans tout anneau euclidien, tous les idéaux sont principaux. Dans l'anneau $\mathscr{A}$ avec $d = -5$, il existe des idéaux non principaux, par exemple l'ensemble des éléments de la forme $3u+(2+i\sqrt{5})v$, où u et v sont des entiers ordinaires arbitraires est un idéal non principal. On s'assure en effet sans peine que cet ensemble est un idéal et cet idéal ne peut être principal, car pour $v = 0$, $u = 1$ et pour $u = 0$, $v = 1$ on obtient deux nombres premiers dans $\mathscr{A}$, dont le rapport n'est pas une unité de $\mathscr{A}$.

La notion d'idéal est due à *Kummer* qui en 1840 s'en est servi pour étudier l'équation de *Fermat* $x^n+y^n = z^n$. La définition donnée ici est due à *Dedekind.*

NOMBRES ALGÉBRIQUES. — Nous allons maintenant indiquer comment on peut généraliser les idées précédentes.

Soit $P(x)$ un polynôme de degré $n \geqq 2$, à coefficients rationnels. Nous supposons $P(x)$ IRRÉDUCTIBLE sur le corps $\mathfrak{Q}$ des nombres rationnels, c'est-à-dire *nous supposons que* $P(x)$ *ne puisse pas être décomposé en un produit de deux polynômes non constants à coefficients rationnels.* Alors tout polynôme $A(x)$ à coefficients rationnels est ou bien divisible par $P(x)$ ou premier à $P(x)$, car le p.g.c.d. de $A(x)$ et de $P(x)$ divise $P(x)$ et est à coefficients rationnels (car il est obtenu par l'algorithme d'*Euclide*); il est donc, ou constant, ou égal à $P(x)$.

Dans l'anneau, noté $\mathfrak{Q}[x]$, des polynômes à une variable x, à coefficients dans le corps des nombres rationnels $\mathfrak{Q}$ *nous*

définissons une relation d'équivalence par $A_1(x) \sim A_2(x)$ *si* $A_1(x) - A_2(x)$ *est divisible par* $P(x)$ (en convenant que le polynôme identiquement nul est divisible par tout polynôme). Il est immédiat de voir que nous avons bien défini une relation d'équivalence.

Désignons par α la classe du polynôme $A(x)$, par β la classe du polynôme $B(x)$, alors tout polynôme de α est de la forme $A(x) + U(x)\,P(x)$ et tout polynôme de β est de la forme $B(x)+V(x)\,P(x)$, où $U(x)$ et $V(x)$ sont des polynômes arbitraires de $\mathfrak{Q}[x]$. On voit ainsi que la classe de $A(x)+B(x)$ est indépendante des polynômes choisis dans α et β; nous noterons cette classe $\alpha+\beta$. De même la classe de $A(x)\,B(x)$ est indépendante des polynômes choisis dans α et β; nous la noterons $\alpha\beta$. L'ensemble de ces classes est donc un anneau. La classe 0 est la classe des polynômes divisibles par $P(x)$. Soit alors $\beta \neq 0$; si $B(x)$ est un polynôme de β, les polynômes $B(x)$ et $P(x)$ sont donc premiers entre eux. Si $A(x)$ est un polynôme arbitraire, l'identité de *Bezout* montre qu'il existe deux polynômes $U(x)$ et $V(x)$ dans $\mathfrak{Q}[x]$ tels que $U(x)\,B(x)+V(x)\,P(x) = A(x)$. En passant aux classes et en appelant η la classe de $U(x)$, on a $\eta\beta+0 = \alpha$ donc $\dfrac{\alpha}{\beta} = \eta$ existe pour tout $\beta \neq 0$. *L'ensemble de ces classes forme donc un corps* $\mathscr{C}$.

Dans chaque classe α de $\mathscr{C}$ il y a un polynôme et un seul soit $a_1+a_2x+\ldots+a_nx^{n-1}$ de degré $n-1$ au plus; en effet, si $A(x)$ est un polynôme de la classe α, le reste de la division de $A(x)$ par $P(x)$ est aussi dans la classe α. Deux polynômes de degré $n-1$ au plus ne peuvent être dans la même classe sans être identiques, car leur différence doit être divisible par $P(x)$; comme le degré de cette différence est au plus $n-1$, cette différence est le polynôme identiquement nul.

Les classes contenant un polynôme constant forment un sous-corps de $\mathscr{C}$ isomorphe à $\mathfrak{Q}$; *nous identifions ce sous-corps avec* $\mathfrak{Q}$ *et écrivons* $a =$ classe du polynôme constant a.

Soit ξ la classe contenant le polynôme x, alors la classe $P(\xi)$ contient le polynôme $P(x)$, donc est la classe 0; on peut donc écrire $P(\xi) = 0$. Le polynôme $P(x)$ n'est donc plus inéductible

dans l'anneau des polynômes $\mathscr{C}[x]$ à coefficients dans $\mathscr{C}$, car il possède le facteur $x-\xi$. Au lieu de $\mathscr{C}$ on emploie alors la notation $\mathfrak{Q}[\xi]$ et *on appelle ce corps l'*EXTENSION ALGÉBRIQUE *de* $\mathfrak{Q}$ *par le polynôme* $P(x)$, *ou aussi l'*ADJONCTION *à* $\mathfrak{Q}$ *d'un zéro* ξ *de* $P(x)$.

Si la classe α contient le polynôme $a_1+a_2x+\ldots+a_nx^{n-1}$ de degré $n-1$ au plus, on a $a_1+a_2\xi+\ldots+a_n\xi^{n-1}$ = classe du polynôme $a_1+a_2x+\ldots.+a_nx^{n-1}=\alpha$, Tout $\alpha\in\mathscr{C}$ se représente donc d'une manière et d'une seule sour la forme

$$\alpha = a_1+a_2\xi+\ldots+a_n\xi^{n-1}\,.$$

BASE: Soit $\vec{a}$ le vecteur de l'espace vectoriel $\mathfrak{Q}^n$, ayant pour composantes $(a_1, a_2, \ldots, a_n)$. La correspondance $\alpha\to\vec{a}$ est alors un isomorphisme entre $\mathscr{C}$ et $\mathfrak{Q}^n$ pour l'addition des classes et la multiplication par un nombre de $\mathfrak{Q}$.

A toute base $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n$ de $\mathfrak{Q}^n$ correspond par cet isomorphisme un système $(\omega_1, \omega_2, \ldots, \omega_n)$ d'éléments de $\mathscr{C}$ tels que, quel que soit $\alpha\in\mathscr{C}$, on ait

$$\alpha = u_1\omega_1+u_2\omega_2+\ldots+u_n\omega_n$$

avec $u_j\in\mathfrak{Q}$ pour $j=1, 2, \ldots, n$, et cette représentation est unique. Elle correspond en effet par l'isomorphisme à la représentation $\vec{a}=u_1\vec{b}_1+u_2\vec{b}_2+\ldots+u_n\vec{b}_n$. *Le système* $(\omega_1, \ldots, \omega_n)$ *est appelé une* BASE *de* $\mathscr{C}$.

Considérons alors une base $(\omega_1, \ldots, \omega_n)$ fixe de $\mathscr{C}$. Pour tout $\alpha\in\mathscr{C}$, on a

$$\begin{aligned}
\alpha\omega_1 &= a_{11}\omega_1+\ldots+a_{1n}\omega_n\\
&\cdots\cdots\cdots\cdots\\
\alpha\omega_n &= a_{n1}\omega_1+\ldots+a_{nn}\omega_n
\end{aligned}\qquad (2)$$

où $a_{ij}\in\mathfrak{Q}$ pour $i=1, \ldots, n$; $j=1, \ldots, n$. On associe ainsi à tout $\alpha\in\mathscr{C}$ une matrice

$$A=\begin{pmatrix} a_{11} & \ldots & a_{1n}\\ \cdots & \cdots & \cdots\\ a_{n1} & \ldots & a_{nn}\end{pmatrix}$$

à éléments a_{ij} de $\mathfrak{Q}$. *Cette correspondance est un isomorphisme entre* $\mathscr{C}$ *et un sous-ensemble des matrices carrés à n lignes et n colonnes à éléments dans* $\mathfrak{Q}$.

En effet plaçons-nous dans l'espace vectoriel $\mathscr{C}^n$ sur le corps $\mathscr{C}$ et soit $\vec{\omega} = (\omega_1, \ldots, \omega_n) \in \mathscr{C}^n$. Le système (2) s'écrit alors $\alpha\vec{\omega} = A(\vec{\omega})$.

Soit I la matrice unité à n lignes et n colonnes; on a donc $(\alpha I - A)(\vec{\omega}) = 0$; α est donc zéro du polynôme $D(xI - A)$ où $D(A)$ représente le déterminant de la matrice A.

Comme $D(xI - A) \in \mathfrak{Q}[x]$, on voit ainsi que *tout nombre* $\alpha \in \mathscr{C}$ *est un nombre algébrique, zéro d'un polynôme inéductible de degré n au plus* (car il divise nécessairement $D(xI - A)$). $D(xI - A)$ est appelé POLYNÔME NORMAL de α.

Soit B la matrice associée à un nombre $\beta \in \mathscr{C}$, on a donc $\beta\vec{\omega} = B(\vec{\omega})$ dans $\mathscr{C}^n$ et

$$(\alpha+\beta)\vec{\omega} = A(\vec{\omega})+B(\vec{\omega}) = (A+B)(\vec{\omega})$$

$$\alpha\beta\vec{\omega} = \alpha B(\vec{\omega}) = B(\alpha\vec{\omega}) = BA(\vec{\omega}) .$$

Par suite $A+B$ correspond à $\alpha+\beta$ et BA correspond à $\alpha\beta$ nous avons bien un isomorphisme. Comme $\alpha\beta = \beta\alpha$, on a $BA = AB$, les matrices sont permutables.

Si $a \in \mathfrak{Q}$, on a $a\omega_i = a\omega_i$ donc la matrice correspondante à a est aI; en particulier à $a = 0$ correspond la matrice 0 et à $a = 1$ la matrice I.

Un changement de base se traduit par $\vec{\omega}' = U(\vec{\omega})$, où U est une matrice carrée à n lignes et n colonnes inversible, donc avec $D(U) \neq 0$, à éléments dans $\mathfrak{Q}$. Si $\alpha\vec{\omega} = A(\vec{\omega})$, on a

$$\alpha\omega' = \alpha U(\vec{\omega}) = U(\alpha\vec{\omega}) = UA(\vec{\omega}) = UAU^{-1}(\vec{\omega}')$$

donc la matrice associée à α dans la base ω' est $A' = UAU^{-1}$. *Le polynôme normal* est le déterminant de $xI - A'$; mais

$$xI - A' = U(xI - A)U^{-1}$$

et

$$D(xI - A') = D(U)D(xI - A)D(U^{-1}) = D(xI - A) ;$$

$D(xI - A)$ est indépendant de la base particulière choisie pour $\mathscr{C}$.

Les coefficients du polynôme normal de α ne dépendent donc que de $\mathscr{C}$ et non de la base. En particulier le terme constant multiplié par $(-1)^n$, c'est-à-dire $D(A)$ est indépendant de la base et est appelé NORME de α et noté $N(\alpha)$. Comme $D(AB)=D(A)D(B)$ on a $N(\alpha\beta) = N(\alpha)N(\beta)$ et $N(\alpha) = 0$ si et seulement si $\alpha \doteq 0$.

Le coefficient de $-x^{n-1}$ dans $D(xI-A)$ est $a_{11}+\ldots+a_{nn}$, il est appelé TRACE de α et noté $Tr(\alpha)$. On a $Tr(\alpha+\beta)=Tr(\alpha)+Tr(\beta)$. Les nombres $N(\alpha)$ et $Tr(\alpha)$ sont tous les deux rationnels.

CONJUGUÉS. — Le polynôme dérivé $P'(x)$ est de degré $n-1$ et appartient à $\mathfrak{Q}[x]$, donc il est premier à $P(x)$; les racines $\xi_1, \ldots, \xi_n$ de $P(x) = 0$ sont donc toutes distinctes. Nous posons $\alpha_j = a_1+a_2\xi_j+\ldots+a_n\xi_j^{n-1}$ et nous dirons que $\alpha_1, \ldots, \alpha_n$ sont CONJUGUÉS.

Soit $W(x)$ un polynôme de $\mathfrak{Q}[x]$; si pour un indice k on a $W(\alpha_k) = 0$, on a aussi $W(\alpha_j) = 0$ pour tout $j = 1, \ldots, n$. En effet le polynôme $W^*(x) = W(a_1+a_2x+\ldots+a_nx^{n-1}) \in \mathfrak{Q}[x]$. On a $W^*(\xi_k) = 0$; par suite $W^*(x)$ et $P(x)$ ne sont pas premiers entre eux, donc $W^*(x)$ est divisible par $P(x)$ et $W^*(\xi_j)=W(\alpha_j)=0$ pour tout $j = 1, \ldots, n$.

Désignons par $a(x)$ le POLYNÔME MINIMAL ayant pour zéro α_k, c'est-à-dire $a(x)$ est le polynôme de plus petit degré de $\mathfrak{Q}[x]$ ayant α_k pour zéro; $a(x)$ *est alors irréductible* De plus $a(x)$ est polynôme minimal pour tous les conjugués.

Le polynôme normal $D(xI-A)$ a aussi pour zéros tous les α_j; si donc $a(x)$ est de degré n, on aura $D(xI-A)=a(x) = \prod_{j=1}^{n}(x-\alpha_j)$. Si les α_j ne sont pas tous distincts, il y a une infinité de nombres rationnels r tels que les nombres $\alpha_j+r\xi_j$ soient tous distincts, car l'égalité de deux tels nombres n'est possible que pour une seule valeur de r. Soit A la matrice correspondant aux α_j et X celle correspondant aux ξ_j, alors on aura $D(xI-A-rX) = \prod_{j=1}^{n}(x-\alpha_j-r\xi_j)$ pour une infinité de r. Mais les coefficients de ces deux polynômes en x sont des polynômes en r de degré n au plus; ils sont égaux pour une infinité de valeurs de r, donc ils sont identiques et par suite, *que les conjugués soient distincts ou*

non, on a $D(xI-A)=\prod_{j=1}^{n}(x-\alpha_j)=(a(x))^s$. Le degré de $a(x)$ est donc un diviseur de n. On voit aussi que $N(\alpha_k)=\prod_{j=1}^{n}\alpha_j$ et que $Tr(\alpha_k)=\sum_{j=1}^{n}\alpha_j$.

DISCRIMINANT D'UNE BASE. — Soit $\omega_1=(\omega_{11},\ \ldots,\ \omega_{1n})$ une base du corps $\mathfrak{Q}[\xi_1]$; soient ω_{jk} les conjugués de ω_{1k} alors $\vec{\omega}_j=(\omega_{j1},\ \ldots,\ \omega_{jn})$ est une base de $\mathfrak{Q}[\xi_j]$. On pose

$$\Delta(\omega)=D^2(\omega_1,\ \ldots,\ \omega_n)=\begin{vmatrix}\omega_{11} & \ldots & \omega_{1n}\\ & & \\ \omega_{n1} & \ldots & \omega_{nn}\end{vmatrix}^2=\begin{vmatrix}Tr(\omega_{11}\omega_{11}) & \ldots & Tr(\omega_{11}\omega_{1n})\\ \ldots & \ldots & \ldots\\ Tr(\omega_{1n}\omega_{11}) & \ldots & Tr(\omega_{1n}\omega_{1n})\end{vmatrix}$$

donc $\Delta(\omega)$ *est un nombre rationnel, appelé* DISCRIMINANT DE LA BASE $\omega=(\omega_1,\ \ldots,\ \omega_n)$.

En changeant la base, soit $\omega_j'=U(\omega_j)$, on aura

$$D(\omega_1',\ \ldots,\ \omega_n')=D(U)D(\omega_1,\ \ldots,\ \omega_n),$$

donc $\Delta(\omega')=D^2(U)\Delta(\vec{\omega})$, Le signe de $\Delta(\vec{\omega})$ ne change donc pas. Si $\vec{\omega}_1$ est la base particulière $1,\ \xi_1,\ \ldots,\ \xi_1^{n-1}$, son discriminant est $\prod_{j>i}(\xi_j-\xi_j)^2\neq 0$, donc *pour chaque base* $\Delta(\vec{\omega})\neq 0$.

ENTIERS ALGÉBRIQUES. — Nous considérons maintenant des polynômes à coefficients *entiers*; nous désignons leur ensemble par $\mathfrak{Z}[x]$. Un polynôme de $\mathfrak{Z}[x]$ est appelé PRIMITIF, si ses coefficients sont des entiers premiers dans leur ensemble. Pour des polynômes primitifs, on a le lemme suivant:

LEMME DE GAUSS: *Le produit de deux polynômes primitifs est primitif.* Soit en effet $A(x)=a_0+a_1x+\ldots+a_nx^n$,

$$B(x)=b_0+b_1x+\ldots+b_mx^m$$

et

$$A(x)\,B(x)=C(x)=c_0+c_1x+\ldots+c_{n+m}x^{n+m}.$$

Supposons $A(x)$ et $B(x)$ primitifs et $C(x)$ non primitif. Alors il existe un nombre premier p divisant tous les c_j, mais il ne peut

diviser tous les a_j, ni tous les b_j. Soit h le plus petit indice tel que p ne divise pas a_h et k le plus petit indice tel que p ne divise pas b_k. On a alors

$$c_{h+k} = (a_0 b_{k+h} + \ldots + a_{h-1} b_{k+1}) + a_h b_k + (a_{k+1} b_{k-1} + \ldots + a_{h+k} b_0)$$

alors p divise toutes ces quantités sauf $a_h b_k$ ce qui est une contradiction.

COROLLAIRE: *Si* $C(x) = \sum_{j=0}^{n+m} c_j x^j \in \mathfrak{Z}[x]$ *avec* $c_{n+m} = 1$ *et si dans* $\mathfrak{Z}[x]$, $C(x) = A'(x) B'(x)$ *avec*

$$A'(x) = \sum_{j=0}^{n} a'_j x^j \quad B'(x) = \sum_{j=0}^{m} b'_j x^j, \quad a'_j \in \mathfrak{Q}, \; b'_j \in \mathfrak{Q},$$

alors il existe aussi deux polynômes

$$A(x) = \sum_{j=0}^{n} a_j x^j \in \mathfrak{Z}[x], \quad B(x) = \sum_{j=0}^{m} b_j x^j \in \mathfrak{Z}[x]$$

avec $a_n = 1$, $b_m = 1$ *tels que* $C(x) = A(x)B(x)$.

En effet, il existe deux nombres rationnels r_a et r_b tels que $r_a A'(x) = A(x) \in \mathfrak{Z}[x]$ et $r_b B'(x) = B(x) \in \mathfrak{Z}[x]$ et que $A(x)$ et $B(x)$ soient primitifs. Alors $A(x)B(x)$ est primitif, donc

$$A(x)B(x) = C(x) \text{ et } a_n b_m = 1, \text{ d'où } a_n = 1, \; b_m = 1.$$

DÉFINITION: *Un nombre algébrique* α *est appelé* ENTIER ALGÉBRIQUE *s'il existe un polynôme dans* $\mathfrak{Z}[x]$, *ayant* α *pour zéro et ayant* 1 *pour coefficient du terme de plus haut degré.*

Le polynôme minimal de α a alors aussi cette propriété; par suite aussi le polynôme normal et $Tr(\alpha)$ et $N(\alpha)$ sont des entiers ordinaires, qui sont *les entiers du corps* $\mathfrak{Q}$ et que *nous appellerons maintenant* ENTIERS RATIONNELS.

Les entiers algébriques forment un anneau. En effet, soit α zéro du polynôme $A(x) = x^n + \sum_{j=0}^{n-1} a_j x^j \in \mathfrak{Z}[x]$ et β zéro de $B(x) = x^m + \sum_{j=0}^{m-1} b_j x^j \in \mathfrak{Z}[x]$. Posons $\omega_j = \alpha^{h-1} \beta^{k-1}$ pour $h = 1, \ldots, n$; $k = 1, \ldots, m$, alors $j = 1, \ldots, N = nm$. En

tenant compte de ce que $\alpha^n = -\sum_{j=0}^{n-1} a_j \alpha^j$, $\beta^m = -\sum_{j=0}^{m-1} b_j \beta^j$ et en désignant pour γ soit le nombre $\alpha+\beta$, soit le nombre $\alpha\beta$, on a

$$\gamma\omega_j = u_{j1}\omega_1 + \ldots + u_{jN}\omega_N \text{ pour } j = 1, \ldots, N$$

et les u_{ji} sont des entiers rationnels. Si U désigne la matrice (u_{ji}), on a $D(\gamma I - U) = 0$; le polynôme $D(xI - U) \in \mathscr{Z}[x]$ et son terme de plus haut degré a pour coefficient 1. Par suite γ est un entier algébrique.

Pour tout nombre algébrique α on peut trouver un entier rationnel q tel que $\gamma = q\alpha$ soit entier algébrique. En effet si α est racine de $A(x) = \sum_{j=0}^{n} a_j x^j \in \mathscr{Z}[x]$ alors $q = a_n$ est une valeur possible; en effet γ est alors zéro du polynôme $q^{n-1} A\left(\frac{x}{q}\right) \in \mathscr{Z}[x]$, dont le coefficient du terme de plus haut degré est 1.

Base des entiers. — Si $\omega_1', \ldots, \omega_n'$ est une base de l'extension algébrique $\mathfrak{Q}[\xi]$, on peut multiplier ω_j' par un entier q_j tel que $\omega_j' q_j = \omega_j$ soit un entier algébrique; $\omega_1, \ldots, \omega_n$ est encore une base de $\mathfrak{Q}[\xi]$ et ses éléments sont des entiers algébriques. Soit γ un entier algébrique arbitraire de $\mathfrak{Q}[\xi]$, alors $\gamma = c_1\omega_1 + \ldots + c_n\omega_n$ avec $c_j \in \mathfrak{Q}$. Si $c_1 \neq 0$, alors $\gamma, \omega_2, \ldots, \omega_n$ est aussi une base de $\mathfrak{Q}[\xi]$. En effet, la matrice de passage d'une base à l'autre est

$$U = \begin{pmatrix} c_1 & c_2 & \ldots & c_n \\ 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 \end{pmatrix}$$

et $D(U) = c_1 \neq 0$, donc U est inversible.

Si $\vec{\omega} = (\omega_1, \ldots, \omega_n)$ est une base formée d'entiers algébriques de $\mathfrak{Q}[\xi]$, le discriminant $\Delta(\vec{\omega})$ est un entier rationnel, car c'est le déterminant des traces des $\omega_i\omega_j$ qui sont des entiers algébriques. D'autre part $\Delta(\vec{\omega}) \neq 0$; il existe donc au moins une base, supposons que ce soit la base $\omega_1, \ldots, \omega_n$, telle que $|\Delta(\vec{\omega})|$ prenne sa plus petite valeur. Alors si on écrit un entier algébrique arbitraire γ de $\mathfrak{Q}[\xi]$ sous la forme $\gamma = u_1\omega_1 + \ldots + u_n\omega_n$ avec $u_j \in \mathfrak{Q}$, les u_j sont des entiers rationnels. En effet, supposons le

contraire et que par exemple u_1 ne soit pas un entier. Alors $u_1 = u+r$, où $u = [u_1]$ est la partie entière de u_1 et r un nombre rationnel avec $0 < r < 1$. Le nombre $\gamma' = \gamma - u\omega_1$ est encore un entier algébrique et on a $\gamma' = r\omega_1 + u_2\omega_2 + \ldots + u_n\omega_n$. Soit $\vec{\omega}' = (\gamma', \omega_2, \ldots, \omega_n)$, comme $r \neq 0$, $\vec{\omega}'$ est une base et son discriminant est $\Delta(\vec{\omega}') = r^2\Delta(\vec{\omega})$ donc $|\Delta(\vec{\omega}')| < |\Delta(\vec{\omega})|$ ce qui contredit notre hypothèse de minimum. Ainsi:

Il existe dans le corps $\mathfrak{Q}[\xi]$ *des bases* $\omega_1, \ldots, \omega_n$ *formées d'entiers algébriques telles que tout entier algébrique* γ *de* $\mathfrak{Q}[\xi]$ *est de la forme* $\gamma = u_1\omega_1 + \ldots + u_n\omega_n$, *où* $u_1, \ldots, u_n$ *sont des entiers rationnels. La base* $\omega_1, \ldots, \omega_n$ *est appelée une* BASE DES ENTIERS *de* $\mathfrak{Q}[\xi]$. On passe d'une base d'entiers à une autre par une matrice à coefficients entiers rationnels de déterminant $\neq 1$. Le discriminant d'une base des entiers du corps $\mathfrak{Q}[\xi]$ est donc un entier rationnel non nul indépendant de la base. Cet entier rationnel s'appelle le DISCRIMINANT DU CORPS.

UNITÉS ALGÉBRIQUES. — *Le nombre algébrique* α *est appelé* UNITÉ ALGÉBRIQUE *si* α et $\dfrac{1}{\alpha}$ *sont à la fois des entiers algébriques;* alors $N(\alpha)$ et $N\left(\dfrac{1}{\alpha}\right) = \dfrac{1}{N(\alpha)}$ sont des entiers rationnels, donc $N(\alpha) = \pm 1$. Réciproquement, si α est un entier algébrique avec $N(\alpha) = \pm 1$, alors l'équation normale de α est de la forme $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x \pm 1 = 0$ où $a_1, \ldots, a_{n-1}$ sont entiers rationnels. Donc $\dfrac{1}{\alpha} = \mp(a_1 + \ldots + a_{n-1}\alpha^{n-2} + \alpha^{n-1})$ et $\dfrac{1}{\alpha}$ est un entier algébrique, donc α est une unité algébrique.

L'ensemble des unités algébriques d'une extension $\mathfrak{Q}[\xi]$ *forme un* GROUPE *relativement à la multiplication.* En effet, si α et β sont des unités algébriques, $\alpha\beta$ l'est aussi, car

$$N(\alpha\beta) = N(\alpha)N(\beta) = \pm 1, \text{ ainsi que } \frac{1}{\alpha}, \text{ car } N\left(\frac{1}{\alpha}\right) = \frac{1}{N(\alpha)} = \pm 1;$$

enfin $N(1) = 1$, donc 1 est une unité algébrique.

Si α_j est un conjugué d'une unité algébrique, α_j est aussi une unité. Posons $\eta_j = \log |\alpha_j|$ et considérons le vecteur $\vec{\eta}$ de com-

posantes $\eta_1, \ldots, \eta_n$ dans $\mathfrak{R}^n$. Les vecteurs $\vec{\eta}$ correspondant aux unités algébriques des corps $\mathfrak{Q}[\xi_j]$ forment donc un groupe additif $\mathscr{M}$, ce que l'on appelle aussi un MODULE. Si les η_j sont bornés, les nombres $|\alpha_j| = e^{\eta_j}$ le sont aussi, donc les coefficients du polynôme normal $\prod_{j=1}^{n}(x-\alpha_j)$ sont bornés en valeur absolue; ce sont des entiers rationnels et leur nombre est n, donc il y en a au plus un nombre fini. Soient $\vec{\xi}_1, \ldots, \vec{\xi}_r$ un nombre maximum de vecteurs linéairement indépendants de $\mathscr{M}$, il y a par conséquent un nombre fini de vecteurs $\vec{\eta} \in \mathscr{M}$ de la forme $\vec{\eta} = \lambda_1 \vec{\xi}_1 + \ldots + \lambda_r \vec{\xi}_r$ avec $0 \leqq \lambda_1 \leqq 1, \ldots, 0 \leqq \lambda_r \leqq 1$. Pour l'ensemble des $\vec{\eta} \in \mathscr{M}$, les λ_j forment eux-mêmes des modules, or $\lambda_j = 1$ est une valeur qui convient, donc $\lambda_j = \frac{m_j}{q_j}$ où q_j, m_j sont des entiers rationnels. En posant $\vec{\xi}'_j = \frac{1}{q_j}\vec{\xi}_j$, on a donc $\eta = m_1 \vec{\xi}'_1 + \ldots + m_r \vec{\xi}'_r$, où $m_1, \ldots, m_r$ sont des entiers rationnels. Le déterminant des entiers m_j correspondant à r vecteurs linéairement indépendants de $\mathscr{M}$ est donc un entier non nul. En considérant alors un système $\vec{\theta}_1, \ldots, \vec{\theta}_r$ de tels vecteurs $\vec{\eta}$ de $\mathscr{M}$ pour lequel la valeur absolue du déterminant précédent est la plus petite possible, on voit (de manière analogue à ce qui a été fait pour les bases des entiers) que tout $\vec{\eta} \in \mathscr{M}$ est de la forme $\vec{\eta} = n_1 \vec{\theta}_1 + \ldots + n_r \vec{\theta}_r$, où $n_1, \ldots, n_r$ sont des entiers rationnels arbitraires.

Soient $\varepsilon_1, \ldots, \varepsilon_r$ des unités algébriques correspondant aux vecteurs $\vec{\theta}_1, \ldots, \vec{\theta}_r$, et α une unité algébrique arbitraire correspondant à $\vec{\eta}$, alors $\log|\alpha| = n_1 \log|\varepsilon_1| + \ldots + n_r \log|\varepsilon_r|$ donc $\alpha = \varepsilon_0 \varepsilon_1^{n_1} \ldots \varepsilon_r^{n_r}$, où ε_0 est une unité telle que toutes ses conjuguées vérifient $|\varepsilon_{0_j}| = 1$. Il en est alors ainsi pour toutes ses puissances entières ε_0^m; les équations $\prod_{j=1}^{n}(x-\varepsilon_{0_j}^m)$ correspondantes sont à coefficients entiers bornés, donc n'ont qu'un nombre fini de possibilités. Il existe donc m et $m+k$ telles que les équations soient égales donc $\varepsilon_0^m = \varepsilon_0^{m+k}$, c'est-à-dire $\varepsilon_0^k = 1$; ε_0 est une racine de l'unité.

Supposons que parmi les nombres ξ_j on ait r_1 racines réelles et $2r_2$ racines complexes, donc $r_1+2r_2 = n$. Si $\overline{\xi_i} = \xi_j$, on a $\eta_i = \log |\alpha_i| = \log |\alpha_j| = \eta_j$.

Les composantes de $\vec{\eta} \in \mathcal{M}$ vérifient donc r_2 relations linéaires. D'autre part $N(\alpha) = \pm 1$, donc $\sum_{j=1}^{n} \eta_j = 0$; le nombre r de vecteurs $\vec{\eta} \in \mathcal{M}$ linéairement indépendants est donc au plus $n - (r_2+1) = r_1+r_2 - 1$.

On montre alors que l'on a effectivement $r = r_1+r_2 - 1$, *ce nombre r s'appelle le* NOMBRE DE DIRICHLET *du corps* $\mathfrak{Q}[\xi]$. *Toute unité algébrique de* $\mathfrak{Q}[\xi]$ *s'exprime d'une manière et d'une seule sous la forme* $\alpha = \varepsilon_0 \varepsilon_1^{n_1} \ldots \varepsilon_r^{n_r}$, *où* ε_0 *est une racine de l'unité du corps et* $\varepsilon_1, \ldots, \varepsilon_r$ *des unités algébriques non racines de l'unité,* $r_1, \ldots, n_r \in \mathcal{Z}$; $r = r_1+r_2 - 1$ *où* r_1 *est le nombre de racines néelles de* $P(x) = 0$ *et* $2r_2$ *le nombre de racines non réelles.*

EXEMPLE: Revenons à l'équation de *Pell-Fermat* (1). En posant $\alpha = x+y\sqrt{d}$, on voit que α est racine de l'équation en t suivante $(t-x)^2 - dy^2 = 0$, α est donc un entier algébrique. L'équation (1) s'écrit $\alpha\bar{\alpha} = N(\alpha) = 1$. La résolution de (1) revient ainsi à la recherche des unités α du corps $\mathfrak{Q}[\sqrt{d}]$ telles que $N(\alpha) = +1$. Ces unités forment manifestement un sous-groupe du groupe de toutes les unités du corps. Le nombre de Dirichlet $r = r_1+r_2 = 1$ de ce corps est 0 si $d < 0$ et 1 si $d > 0$. Pour $d < 0$, il n'y a donc qu'un nombre fini de solutions qui sont toutes racines de l'unité. Pour $d > 0$ il existe une unité particulière $\varepsilon_1 = x_1+y_1\sqrt{d}$ telle que $\alpha = \pm (x_1 + y_1\sqrt{d})^n$, en effet ici $\mathfrak{Q}[\sqrt{d}]$ est réel, donc $\varepsilon_0 = \pm 1$, n est un entier rationnel arbitraire. On en déduit toutes les solutions de (1) par les formules

$$x = \pm \frac{1}{2}(\varepsilon_1^n + \bar{\varepsilon}_1^n), \quad y = \pm \frac{1}{2\sqrt{d}}(\varepsilon_1^n - \bar{\varepsilon}_1^n).$$

Par exemple pour $d = 2$, on a $\varepsilon_1 = 3+2\sqrt{2}$; il existe des tables numériques donnant ε_1 pour tout entier $d < 10^4$.

Institut Henri Poincaré
11, rue Pierre Curie
Paris V^e.