ARKIV FÖR MATEMATIK Band 6 nr 9

1.65 01 1 Communiqué le 13 Janvier 1965

Contributions à la théorie des modules et des anneaux algébriques

Par TRYGVE NAGELL

§ 1. Théorème sur un déterminant

1. Soient $a_1, a_2, \ldots, a_n$ des nombres entiers rationnels tels que $(a_1, a_2, \ldots, a_n) = 1$ et tels que $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n \geqslant 0$. Nous dirons que le système $[a_1, a_2, \ldots, a_n]$ a la *hauteur* $S(a_i) = a_1 + a_2 + \ldots + a_n$. La hauteur a sa valeur *minimum* 1 pour le système $[1, 0, 0, \ldots, 0]$ et seulement pour ce système. En remplaçant le nombre a_1 par la différence $a_1 - a_2$ nous aurons un autre système $[b_1, b_2, \ldots, b_n]$, où $b_1 = a_2, b_2, \ldots, b_n$ sont des nombres entiers rationnels tels que $(b_1, b_2, \ldots, b_n) = 1$ et tels que $b_1 \geqslant b_2 \geqslant \ldots \geqslant b_n \geqslant 0$. Si le système $[a_1, a_2, \ldots, a_n]$ est différent de $[1, 0, 0, \ldots, 0]$ il est évident que $S(b_i) < S(a_i)$. En procédant de cette manière on aura des systèmes de hauteurs toujours décroissantes, et après un certain nombre de fois on finira avec le système $[1, 0, 0, \ldots, 0]$.

2. Ce que nous venons de développer nous servira à établir le résultat suivant :

Théorème 1. *Soient donnés les nombres entiers rationnels $a_1, a_2, \ldots, a_n$, premiers entre eux ($n \geqslant 2$). Alors, l'équation*

$$D = \begin{vmatrix} x_{11} & x_{12} & \ldots & x_{1n} \\ x_{21} & x_{22} & \ldots & x_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ x_{n-1,1} & x_{n-1,2} & \ldots & x_{n-1,n} \\ a_1 & a_2 & \ldots & a_n \end{vmatrix} = 1 \tag{1}$$

a des solutions en nombres entiers rationnels x_{ij} pour $i = 1, 2, \ldots, n-1$; $j = 1, 2, \ldots, n$.

Démonstration. Il suffit évidemment de supposer que $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n \geqslant 0$. Nous nous servirons de la méthode d'induction complète. En effet, le théorème est vrai pour tous les n lorsque la hauteur du système $[a_1, a_2, \ldots, a_n]$ est égal à 1, c'est-à-dire lorsque $a_1 = 1$, $a_2 = a_3 = \ldots = a_n = 0$. Car, dans ce cas l'équation (1) aura la forme

$$\pm \begin{vmatrix} x_{12} & \ldots & x_{1n} \\ x_{22} & \ldots & x_{2n} \\ \cdot & \cdot & \cdot \\ x_{n-1,2} & \ldots & x_{n-1,n} \end{vmatrix} = 1,$$

équation qui a toujours des solutions entières.

Nous supposons maintenant que le théorème est vrai pour tous les n lorsque le système $[a_1, a_2, \ldots, a_n]$ est d'une hauteur $\leqslant N-1$, où N est un nombre naturel $\geqslant 2$. Supposons ensuite que la hauteur du système $[a_1, a_2, \ldots, a_n]$ dans (1) est égal à N. L'équation (1) peut s'écrire

$$\begin{vmatrix} x_{11}-x_{12} & x_{12} & \ldots & x_{1n} \\ x_{21}-x_{22} & x_{22} & \ldots & x_{2n} \\ \ldots\ldots\ldots\ldots\ldots & & & \\ x_{n-1,1}-x_{n-1,2} & x_{n-1,2} & \ldots & x_{n-1,n} \\ a_1-a_2 & a_2 & \ldots & a_n \end{vmatrix} = 1. \tag{2}$$

Ici, les quantités $x_{11}-x_{12}=z_1$, $x_{21}-x_{22}=z_2$, ..., $x_{n-1,1}-x_{n-1,2}=z_{n-1}$ sont des variables libres indépendantes entre elles et des variables x_{ij} pour $i=1, 2, \ldots, n-1$ et $j=2, 3, \ldots, n$. Or, dans le déterminant (2) nous avons

$$a_1-a_2+a_2+a_3+\ldots+a_n=N-a_2\leqslant N-1.$$

Donc, d'après la supposition faite tout à l'heure l'équation (2) est résoluble en nombres entiers x_{ij}. Par conséquent, l'équation (1) l'est aussi, et le théorème 1 se trouve démontré.

§ 2. Remarques sur les groupes abéliens infinis admettant une base finie

3. Dans ce paragraphe **G** signifiera un groupe abélien infini admettant une base finie. La composition dans **G** sera désignée par le symbole de multiplication. Nous supposons qu'il y a dans **G** des éléments d'ordre infini. Alors, il existe des éléments $B_1, B_2, \ldots, B_r$ d'ordre infini tels qu'un élément quelconque A de **G** soit représenté *univoquement* par une expression de la forme

$$A=TB_1^{x_1}B_2^{x_2}\cdots B_r^{x_r},$$

où $x_1, x_2, \ldots, x_r$ sont des entiers rationnels, et où T est un élément d'ordre fini. Nous dirons, pour raccourcir, que $B_1, B_2, \ldots, B_r$ est une base « sans torsion ». Le nombre r est un invariant du groupe (« the torsion free rank »); voir Fuchs [1][1], p. 12. Il est évident qu'un élément quelconque ne peut pas faire partie d'une base. En effet, nous allons établir le

Théorème 2. *Soit A un élément de **G** d'ordre infini. La condition nécessaire et suffisante pour que A fasse partie d'une base de **G** est que A ne soit pas de la forme*

$$TC^m, \tag{3}$$

où C est un élément d'ordre infini et T un élément d'ordre fini; m est un nombre entier rationnel tel que $|m|+1$.

Démonstration. Soit $B_1, B_2, \ldots, B_r$ une base « sans torsion », et considérons les éléments

[1] Les numéros figurant entre crochets renvoient à l'Index bibliographique placé à la fin de ce travail.

$$\left.\begin{aligned} A_1 &= T_1 B_1^{x_{11}} B_2^{x_{12}} \cdots B_r^{x_{1r}}, \\ A_2 &= T_2 B_1^{x_{21}} B_2^{x_{22}} \cdots B_r^{x_{2r}}, \\ &\cdots\cdots\cdots\cdots \\ A_r &= T_r B_1^{x_{r1}} B_2^{x_{r2}} \cdots B_r^{x_{rr}}, \end{aligned}\right\} \tag{4}$$

où les T_i sont des éléments d'ordre fini, et où les x_{ij} signifient des nombres entiers rationnels. Pour que les éléments $A_1, A_2, \ldots, A_r$ constituent une base « sans torsion » il faut et il suffit évidemment que le déterminant $\|x_{ij}\|$ soit égal à ± 1. Supposons maintenant que $A_r = A$. Alors, la condition que A ne soit pas de la forme (3) signifie que $(x_{r1}, x_{r2}, \ldots, x_{rr}) = 1$. D'autre part, d'après le théorème 1, l'équation $\|x_{ij}\| = \pm 1$ est toujours résoluble en nombres entiers rationnels x_{ij}, pour $i = 1, 2, \ldots, r-1$; $j = 1, 2, \ldots, r$, lorsque $x_{r1}, x_{r2}, \ldots, x_{rr}$ sont des entiers rationnels donnés, premiers entre eux. Cela démontre le théorème 2.

Nous allons y ajouter la proposition suivante:

Théorème 3. *Soient $B_1, B_2, \ldots, B_{h-1}$ des éléments faisant partie d'une base « sans torsion » de* **G**, $2 \leqslant h \leqslant r$, *et soit donné un élément A d'ordre infini. Alors, la condition nécessaire et suffisante pour que $B_1, B_2, \ldots, B_{h-1}$ et A fassent à la fois partie de la même base « sans torsion » de* **G**, *est que A ne soit pas de la forme*

$$A = T B_1^{y_1} B_2^{y_2} \cdots B_{h-1}^{y_{h-1}} C^m, \tag{5}$$

où C est un élément d'ordre infini et T un élément d'ordre fini; les y_i sont des nombres entiers rationnels arbitraires; m est un nombre entier rationnel tel que $|m| \neq 1$.

Démonstration. Soit, comme plus haut, $B_1, B_2, \ldots, B_r$ une base « sans torsion » de **G** et considérons le système (4) des éléments $A_1, A_2, \ldots, A_r$. Nous y posons $x_{ii} = 1$ pour $i = 1, 2, \ldots, h-1$ et $x_{ij} = 0$ pour $i = 1, 2, \ldots, h-1$; $j = 1, 2, \ldots, r$ avec $i \neq j$. Alors, pour que le système $A_1, A_2, \ldots, A_r$ constituent une base « sans torsion » il faut et il suffit que le déterminant

$$D = \begin{vmatrix} x_{hh} & x_{h,h+1} & \cdots & x_{hr} \\ x_{h+1,h} & x_{h+1,h+1} & \cdots & x_{h+1,r} \\ \cdots & \cdots & \cdots & \cdots \\ x_{rh} & x_{r,h+1} & \cdots & x_{rr} \end{vmatrix}$$

soit égal à ± 1. Supposons maintenant que $A = A_r$; cela signifie que les nombres entiers rationnels x_{rj} sont donnés pour $j = 1, 2, \ldots r$. Alors, la condition que A ne soit pas de la forme (5) signifie qu'on a $(x_{rh}, x_{r,h+1}, \ldots, x_{rr}) = 1$, ou dans le cas de $r = h$ que $x_{rr} = \pm 1$. Or, d'après le théorème 1 l'équation $D = \pm 1$ est toujours résoluble en nombres entiers x_{ij} pour $i = h, h+1, \ldots, r-1$; $j = h, h+1, \ldots, r$, lorsque $x_{rh}, x_{r,h+1}, \ldots, x_{rr}$ sont des entiers rationnels donnés, premiers entre eux. Donc, le théorème 3 se trouve démontré.

4. Soit **G** le groupe abélien du numéro précédent. Nous supposons ici que **G** est pur (sans torsion) et que $A_1, A_2, \ldots, A_r$ constituent une base du groupe. Rappelons le résultat suivant sur les groupes de cette catégorie :

Théorème 4. *Soit* **U** *un sous-groupe de* **G** *ayant tous les deux le rang r. Pour toutes les valeurs de i $(1 \leqslant i \leqslant r)$ il y a des éléments dans* **U** *de la forme*

$$C_i = A_1^{a_1} A_2^{a_2} \cdots A_i^{a_i},$$

où $a_1, a_2, \ldots, a_i$ *sont des entiers rationnels et* $a_i \neq 0$. *Désignons par* b_{ii} *la plus petite valeur positive de* a_i *qui est possible quand les exposants* $a_1, a_2, \ldots, a_i$ *varient librement de façon que l'élément* C_i *appartienne à* **U**. *Soit maintenant, pour* $i = 1, 2, \ldots, r$,

$$B_i = A_1^{b_{i1}} A_2^{b_{i2}} \cdots A_i^{b_{ii}}$$

un élément de **U**, *les exposants* b_{i1}, b_{i2} *etc. étant des entiers rationnels. Alors, les éléments* $B_1, B_2, \ldots, B_r$ *constituent une base de* **U**.

Les exposants b_{ij}, *pour* $1 \leqslant j \leqslant i-1$, *peuvent être choisis de manière qu'on ait*

$$0 \leqslant b_{ij} < b_{jj}. \tag{6}$$

Il n'y a qu'une seule base $B_1, B_2, \ldots, B_r$ *de* **U** *qui satisfait aux conditions* (6).

Pour la démonstration voir Hecke [2], § 11 et Nagell [3].

§ 3. Sur les bases d'un module algébrique

5. Rappelons quelques faits de la théorie des modules algébriques. Le module algébrique **M** sera appelé *module du n-ième degré* lorsqu'il a les propriétés suivantes : Il y a dans **M** au moins un nombre du n-ième degré; **M** ne contient aucun nombre d'un degré $> n$.

On voit aisément qu'un module **M** du n-ième degré est contenu dans un corps algébrique **K** du n-ième degré. En effet, soit α un nombre dans **M** du n-iéme degré, et soit β un nombre de **M** qui n'est pas contenu dans le corps $\mathbf{K}(\alpha)$. Alors, le degré du corps composé $\mathbf{K}(\alpha, \beta)$ serait nécessairement $> n$. Or, il existe deux nombres naturels u et v tels que le nombre $\gamma = u\alpha + v\beta$ engendre le corps $\mathbf{K}(\alpha, \beta)$. Cela est impossible, vu que le nombre γ appartient à **M**.

Il est évident que tous les modules contenus dans un corps du n-ième degré ont un rang $\leqslant n$. Le module **M** est dit *entier* quand il ne contient que des nombres entiers. Dans ce qui suivra nous considérons seulement des modules entiers du rang n contenus dans un corps de degré n; ces modules sont nécessairement du n-ième degré. Soit donné le corps algébrique $\mathbf{K}(\theta)$ engendré par le nombre entier θ du n-ième degré. *Dorénavant* **M** *désignera un module entier du rang n contenu dans ce corps.* Le module de tous les nombres entiers du corps est un anneau qui s'appellera *l'anneau fondamental.*

Soit $\omega_1, \omega_2, \ldots, \omega_n$ une base de l'anneau fondamental. Vu que les nombres du module **M** forment un groupe abélien additif, nous aurons, d'après le théorème 4 le résultat suivant :

Théorème 5. *Il existe une base* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *du module* **M** *qui satisfait aux conditions suivantes : Pour tous les* $i = 1, 2, \ldots, n$ *on a*

$$\alpha_i = a_{i1}\omega_1 + a_{i2}\omega_2 + \ldots + a_{ii}\omega_i, \tag{7}$$

où a_{ii} *désigne le plus petit nombre naturel tel qu'il existe dans* **M** *des nombres de la forme*

$$b_1\omega_1 + b_2\omega_2 + \ldots + b_{i-1}\omega_{i-1} + a_{ii}\omega_i,$$

où $b_1, b_2, \ldots, b_{i-1}$ *sont des nombres entiers rationnels. Les nombres* a_{ij} *dans* (7) *sont des entiers rationnels qui peuvent être choisis de manière qu'on ait, pour* $1 \leqslant j \leqslant i-1$,

$$0 \leqslant a_{ij} < a_{jj}. \tag{8}$$

Il n'y a qu'une seule base $\alpha_1, \alpha_2, \ldots, \alpha_n$ *de* $\mathbf{M}$ *qui satisfait à* (8).

Nous désignérons par $\mathbf{M}(\beta_1, \beta_2, \ldots, \beta_n)$ le module qui possède la base $\beta_1, \beta_2, \ldots, \beta_n$. Le nombre $D(\mathbf{M}) = D(\beta_1, \beta_2, \ldots, \beta_n)$ sera appelé le *discriminant du module* $\mathbf{M}$. Si une base de $\mathbf{M}$ est donnée par les équations (7) on aura évidemment

$$D(\mathbf{M}) = D(\alpha_1, \alpha_2, \ldots, \alpha_n) = (a_{11} a_{22} \cdots a_{nn})^2 D^*, \tag{9}$$

où D^* signifie le discriminant du corps $\mathbf{K}(\theta)$. Des équations (7), (8) et (9) on obtient le

Théorème 6. *Il n'y a qu'un nombre fini de modules du n-ième degré de discriminant donné dans le corps* $\mathbf{K}(\theta)$. *Ces modules peuvent être déterminés par un nombre fini d'opérations à l'aide des équations* (7) *et* (8).
Si γ *est un nombre entier quelconque de* $\mathbf{K}(\theta)$, *le produit* $a_{11} a_{22} \cdots a_{nn} \gamma$ *appartient à* $\mathbf{M}$.

Voir pour ce théorème Nagell [4] et [5]; comparez aussi le théorème 10.
En appliquant le théorème 2 au module $\mathbf{M}$ nous aurons le

Théorème 7. *La condition nécessaire et suffisante pour que le nombre* α *du module* $\mathbf{M}$ *appartienne à une base de* $\mathbf{M}$, *est que* α *ne soit pas de la forme* $m\beta$, *où* β *est un nombre de* $\mathbf{M}$, *et où* m *est un nombre entier rationnel* $\neq \pm 1$.

Dans la suite nous prenons $\omega_1 = 1$. Alors $\alpha_1 = a_{11}$ est le plus petit nombre naturel dans $\mathbf{M}$. Lorsque $a_{11} = 1$ nous dirons que $\mathbf{M}$ est un module *ordinaire*.
En appliquant le théorème 3 pour $h = 2$ au module $\mathbf{M}$ nous aurons le

Théorème 8. *Soit* α *un nombre irrationnel du module* $\mathbf{M}$. *La condition nécessaire et suffisante pour que les nombres* a_{11} *et* α *fassent à la fois partie de la même base de* $\mathbf{M}$, *est que* α *ne soit pas de la forme*

$$m\beta + m_0 a_{11},$$

où β *est un nombre de* $\mathbf{M}$, *et où* m *et* m_0 *sont des nombres entiers rationnels et* $|m| \neq 1$.

Nous pouvons y ajouter le résultat suivant :

Théorème 9. *Soit, comme plus haut,* $\mathbf{M}$ *un module entier du n-ième degré contenu dans le corps* $\mathbf{K}$ *du n-ième degré. Soit* $\mathbf{K}^*$ *un sous-corps irrationnel de* $\mathbf{K}$, *de degré* v. *Soit enfin* $1, \alpha_1, \alpha_2, \ldots, \alpha_{v-1}$ *une base de l'anneau fondamental* $\mathbf{R}^*$ *de* $\mathbf{K}^*$. *Supposons que les nombres* $\alpha_1, \alpha_2, \ldots, \alpha_{h-1}$, *pour* $h \leqslant v$, *appartiennent à* $\mathbf{M}$. *Alors, il existe une base de* $\mathbf{M}$ *qui contient les nombres* $a_{11}, \alpha_1, \alpha_2, \ldots, \alpha_{h-1}$.

Démonstration. D'après le théorème 3 il suffit de montrer qu'on ne peut pas avoir, pour $1 < i \leqslant h-1$, une relation de la forme

$$\alpha_i = m\beta + m_0 a_{11} + m_1 \alpha_1 + m_2 \alpha_2 + \ldots + m_{i-1} \alpha_{i-1},$$

ou, pour $i = 1$, de la forme

$$\alpha_1 = m\beta + m_0 a_{11},$$

où m, m_0, m_1, ..., m_{i-1} sont des nombres entiers rationnels et $|m| \neq 1$, et où β est un nombre de $\mathbf{M}$. En effet, le nombre

$$\frac{1}{p}(\alpha_i - m_{i-1}\alpha_{i-1} - \ldots - m_2\alpha_2 - m_1\alpha_1 - m_0 a_{11}),$$

où p est un nombre premier, ne peut pas être entier, vu que les nombres $1, \alpha_1, \alpha_2, \ldots, \alpha_i$ appartiennent à une base de $\mathbf{R}^*$.

Les résultats de ce numéro sont, bien entendu, aussi valables pour les anneaux du corps $\mathbf{K}$.

La condition nécessaire et suffisante pour que le module $\mathbf{M}(\beta_1, \beta_2, \ldots, \beta_n)$ soit un anneau, est évidemment que tous les produits $\beta_i\beta_j$ appartiennent au module.

D'après un théorème célèbre de Minkowski il n'y a qu'un nombre fini de corps algébriques de discriminant donné. Par conséquent, de la relation (9) on aura le

Théorème 10. *Il n'y a qu'un nombre fini de modules algébriques entiers de discriminant donné.*

Il faut observer que le module algébrique $\mathbf{M}$ possède un discriminant seulement quand le degré de $\mathbf{M}$ est égal à son rang. Le théorème 10 regarde la totalité des modules entiers sans égard au degré.

Nous dirons qu'un module (ou anneau) est donné lorsqu'une base est donnée.

Remarque 1. Si le module $\mathbf{M}$ dans le théorème 6 est un anneau, on peut y ajouter la proposition suivante (voir Nagell [15]):

Théorème 6 bis. *Le nombre entier α du n-ième degré se trouve seulement dans un nombre fini d'anneaux entiers du n-ième degré. Ces anneaux peuvent être déterminés par un nombre fini d'opérations lorsque α est donné.*

En effet, soit α racine de l'équation irréductible

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

à coefficients entiers rationnels. Si α appartient à l'anneau entier du n-ième degré $\mathbf{R} = \mathbf{R}(\omega_1, \omega_2, \ldots, \omega_n)$, toutes les puissances α^m $(m \geqslant 1)$ aussi bien que le nombre $|a_n| = |N(\alpha)|$ appartiennent à $\mathbf{R}$. Le module $\mathbf{M}(a_n, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ est évidemment un anneau $\mathbf{R}_1$ du n-ième degré contenu dans $\mathbf{R}$. Donc $D(\mathbf{R}_1) = c^2 D(\mathbf{R})$, c étant un nombre naturel. Vu que $D(\mathbf{R}_1) = a_n^2 D(\alpha)$ on obtient

$$|D(\mathbf{R})| \leqslant a_n^2 |D(\alpha)|.$$

Ainsi, il n'y aura qu'un nombre limité de possibilités pour l'anneau $\mathbf{R}$ lorsque α est donné.

Il est évident que le théorème 6 bis n'est pas en général vrai pour les modules.

De plus, on voit de l'exemple suivant qu'il n'est pas vrai pour les anneaux lorsque le nombre α est d'un degré $< n$. En effet, le nombre $\sqrt{2}$ est contenu dans chacun des anneaux

$$\mathbf{R}(1, \sqrt{2}, ci, ci\sqrt{2})$$

du quatrième degré, où c est un nombre naturel quelconque.

Remarque 2. Soit **K** un corps algébrique du n-ième degré dont le discriminant est $=D^*$; et soit c un nombre naturel quelconque. Alors, d'après le théorème 5 il existe toujours des modules dans **K** qui possèdent le discriminant c^2D^*. D'après le théorème 6 le nombre de ces modules est fini. Le nombre c sera appelé l'*index* des modules. Lorsque le nombre c est donné on déterminera tous les modules ayant l'index c à l'aide des relations (8) et $c=a_{11}\,a_{22}\cdots a_{nn}$. A chaque choix des coefficients a_{ij} correspondra un certain module d'index c. Il est évident que tous les modules ainsi obtenus sont différents entre eux.

Prenons un exemple dans le corps cubique engendré par une racine ξ de l'équation $\xi^3=1-\xi$. Ce corps a le discriminant -31. Alors on trouvera que les modules ayant le discriminant $-2^2\cdot 31$ sont donnés par le tableau suivant :

$$\mathbf{M}(1,\xi,2\xi^2),\quad \mathbf{M}(1,2\xi,\xi^2),\quad \mathbf{M}(1,2\xi,\xi+\xi^2),\quad \mathbf{M}(2,\xi,\xi^2),$$

$$\mathbf{M}(2,\xi,1+\xi^2),\quad \mathbf{M}(2,1+\xi,\xi^2),\quad \mathbf{M}(2,1+\xi,1+\xi^2).$$

On vérifiera aisément qu'il n'y a aucun anneau parmi ces modules.

Lorsque le corps est engendré par une racine de l'équation $\xi^3=2+\xi$ on aura 7 modules d'index 2, et parmi ces modules il y a 4 anneaux; voir Nagell [4].

Il est facile de voir que, dans un corps quadratique, il y a, parmi les modules d'index c, toujours un anneau, au moins. En effet, tout module du second degré qui contient le nombre 1, est un anneau.

§ 4. Remarques sur les unités dans un anneau algébrique

6. Comme dans le paragraphe précédent nous désignerons par $\mathbf{K}(\theta)$ le corps algébrique engendré par le nombre entier θ du n-ième degré. **R** désignera un anneau entier du n-ième degré contenu dans le corps; l'épithète « du n-ième degré » signifie que **R** est un module du n-ième degré. Pour que **R** contienne des unités il faut et il suffit que le nombre 1 soit contenu dans **R**; alors **R** est dit *ordinaire*, et on a $a_{11}=1$.

Soit r le rang du groupe des unités du corps, abstraction faite des racines de l'unité. Alors, le rang du groupe des unités d'un anneau ordinaire **R** du corps est aussi égal à r. Nous excluons le corps rationnel et les corps quadratiques imaginaires; donc $r\geqslant 1$.

Vu que les unités de l'anneau **R** forment un groupe abélien multiplicatif du rang r, nous obtenons du théorème 2 le

Théorème 11. *La condition nécessaire et suffisante pour que l'unité η dans* **R** *fasse partie d'une base des unités de* **R**, *est que η ne soit pas de la forme*

$$\xi E^m,$$

où ξ est une racine de l'unité appartenant à **R**, *où E est une unité dans* **R**, *et où m est un nombre naturel >1.*

J'ai déjà établi ce résultat dans des cas particuliers; voir Nagell [6], p. 356, p. 362 (lemme 4) et p. 368 (lemme 7).

Il est évident que le théorème 11 peut être utilisé pour construire une base des unités d'un anneau donné. S'il existe un souscorps $\mathbf{K}^*$ (de rang $\geqslant 1$) de $\mathbf{K}(\theta)$, le nombre η peut être choisi parmi les unités d'une base des unités d'un anneau appartenant à $\mathbf{K}^*$ et à **R**, sauf dans des cas exceptionnels.

7. Considérons maintenant les racines de l'unité contenues dans l'anneau **R**. Il est évident que chacun des anneaux conjugués contient les mêmes racines de l'unité. Supposons que **R** contient des racines imaginaires de l'unité, c'est-à-dire $\neq \pm 1$. Alors, il est évident que **R** et tous les anneaux conjugués sont imaginaires. Donc, on a $r \leq \frac{1}{2}n - 1$.

On peut montrer qu'il existe dans tout corps $\mathbf{K}(\theta)$ des anneaux **R** qui ne contiennent aucune racine imaginaire de l'unité. En effet, nous avons le

Théorème 12. *Le nombre θ ayant la même signification que plus haut, l'anneau*

$$\mathbf{R}(1, t\theta, t\theta^2, \ldots, t\theta^{n-1}), \tag{10}$$

où t est un nombre naturel >1, ne contient aucune racine imaginaire de l'unité.

Démonstration. Il faut d'abord vérifier que les nombres $1, r\theta, r\theta^2, \ldots, t\theta^{n-1}$ constituent une base d'un anneau du corps. Pour cela il suffit évidemment de montrer que le module

$$\mathbf{M}(1, t\theta, t\theta^2, \ldots, t\theta^{n-1}) \tag{11}$$

contient tous les produits

$$t\theta^h \cdot t\theta^j = t^2\theta^{h+j}$$

pour $n \leq h + j \leq 2n - 2$. Supposons que θ est une racine de l'équation irréductible

$$x^n - a_1 x^{n-1} - a_2 x^{n-2} - \ldots - a_n = 0 \tag{12}$$

à coefficients entiers rationnels $a_1, a_2, \ldots, a_n$. Alors, il résulte de la relation

$$t\theta^{n+m} = a_1 t\theta^{n+m-1} + \ldots + a_n t\theta^m$$

que les nombres $t\theta^{n+m}$ appartiennent au module pour tous les $m \geq 0$ (induction complète). Donc, le module (11) est un anneau entier du n-ième degré.

Supposons maintenant que ξ est une racine imaginaire de l'unité dans l'anneau (10). Or, la relation

$$\xi = x_0 + t\theta x_1 + t\theta^2 x_2 + \ldots + t\theta^{n-1} x_{n-1},$$

où $x_0, x_1, \ldots, x_{n-1}$ sont des entiers rationnels, est impossible vu que le nombre

$$\frac{1}{t}(\xi - x_0)$$

ne peut pas être entier pour $t \geq 2$ en vertu du théorème sur les bases des entiers des corps cyclotomiques.

Le théorème 12 se trouve ainsi démontré. En variant le paramètre t on obtient une infinité d'anneaux **R** sans aucune racine imaginaire de l'unité, dans le corps donné $\mathbf{K}(\theta)$.

8. De l'autre coté, nous allons montrer l'existence dans le même corps d'une infinité d'anneaux entiers qui contiennent les puissances d'une racine de l'unité donnée d'avance. Désignons par ξ le nombre $e^{2\pi i/m}$, où m est un nombre naturel. Le corps $K(\xi)$ est de degré $\varphi(m) = \varphi$. Soit θ un nombre algébrique entier de degré ν

relativement à $\mathbf{K}(\xi)$, et soit $\nu \geqslant 2$. Le corps composé $\mathbf{K}(\xi, \theta)$ est de degré $\nu\varphi$, et tout nombre de ce corps peut être mis sous la forme

$$\gamma_0+\gamma_1\theta+\gamma_2\theta^2+\ldots+\gamma_{\nu-1}\theta^{\nu-1}$$

les γ_i étant des nombres dans $\mathbf{K}(\xi)$. Il est évident que les nombres

$$1, \xi, \xi^2, \ldots, \xi^{\varphi-1} \quad \text{et} \quad \xi^h t\theta^k, \tag{13}$$

pour $h=0, 1, 2, \ldots, \varphi-1$ et $k=1, 2, \ldots, \nu-1$, où t est un nombre naturel, constituent une base d'un module entier de rang $\nu\varphi$ dans le corps $K(\xi, \theta)$. Ce module est un anneau de degré $\nu\varphi$. En effet, il est facile de voir que tous les produits

$$\xi^h t\theta^k \cdot \xi^j t\theta^l = \xi^{h+j} t^2 \theta^{k+l}$$

appartiennent au module pour $0 \leqslant h \leqslant \varphi-1$, $0 \leqslant j \leqslant \varphi-1$, $0 \leqslant k \leqslant \nu-1$, $0 \leqslant l \leqslant \nu-1$. Supposons que θ est une racine de l'équation

$$\theta^\nu = \alpha_1\theta^{\nu-1} + \alpha_2\theta^{\nu-2} + \ldots + \alpha_\nu,$$

où l'on a $$\alpha_i = a_{i0} + a_{i1}\xi + a_{i2}\xi^2 + \ldots + a_{i,\varphi-1}\xi^{\varphi-1},$$

les nombres a_{ij} étant des nombres entiers rationnels, et considérons les relations

$$\xi^s t\theta^{\nu+\mu} = \alpha_1\xi^s t\theta^{\nu+\mu-1} + \ldots + \alpha_\nu \xi^s t\theta^\mu,$$

où μ est un entier rationnel $\geqslant 0$. Il en résulte que les nombres

$$\xi^s t\theta^{\nu+\mu}$$

appartiennent au module pour tous les s et $\mu \geqslant 0$. Donc, les nombres (13) constituent une base d'un anneau $\mathbf{R}$ entier du degré $\nu\varphi$ dans le corps $\mathbf{K}(\xi, \theta)$. Cet anneau contient tous les nombres $\pm\xi^h$, h nombre entier rationnel. Si $t \geqslant 2$ on voit aisément que $\mathbf{R}$ ne contient aucune autre racine de l'unité. En effet, soit η une racine de l'unité qui n'est pas de la forme $\pm\xi^h$, et supposons qu'on ait

$$\eta = x_0 + x_1\xi + \ldots + x_{\varphi-1}\xi^{\varphi-1} + t\alpha,$$

où $x_0, x_1, \ldots, x_{\varphi-1}$ sont des nombres entiers rationnels, et où α est un nombre entier dans $\mathbf{R}$. Désignons par ε une racine de l'unité qui engendre le corps $\mathbf{K}(\eta, \xi)$. Nous pouvons supposer $\varepsilon = e^{2\pi i/mq}$ et $\eta = \pm\varepsilon^s$, où q et s sont des nombres naturels; si m est impair on a $q \geqslant 3$; si m est pair on a $q \geqslant 2$; s n'est pas divisible par q. Alors, il est évident que le nombre

$$\frac{1}{t}(\eta - x_0 - x_1\xi - \ldots - x_{\varphi-1}\xi^{\varphi-1}) = \frac{1}{t}(\pm\varepsilon^s - x_0 - x_1\varepsilon^q - \ldots - x_{\varphi-1}\varepsilon^{q(\varphi-1)})$$

ne peut pas être entier pour $t \geqslant 2$, vu qu'on a $\varphi(mq) > 1 + \varphi(m)$ et que les nombres $1, \varepsilon, \varepsilon^2$ etc. forment une base des entiers du corps $\mathbf{K}(\varepsilon)$.

Par conséquent, nous avons obtenu le résultat suivant :

Théorème 13. *Soient ξ et θ des nombres algébriques entiers définis comme plus haut, et soit t un nombre naturel $\geqslant 2$. Alors les nombres* (13) *constituent une base d'un anneau* **R** *entier du degré $v\varphi$ dans le corps* $\mathbf{K}(\xi, \theta)$. *Les racines de l'unité dans cet anneau sont les nombres $\pm\xi^h$, h nombre entier rationnel; il n'y a aucune autre racine de l'unité dans* **R**.

En variant le paramètre t on aura une infinité d'anneaux **R** de ce type. Le théorème 13 est aussi valable pour $m=1$ et $m=2$. D'ailleurs, il est évident qu'on peut supprimer les cas dans lesquels $m=2m_1$, où m_1 est impair. En effet, dans ces cas, si on remplace m par m_1 le corps engendré par ξ restera le même.

Nous terminons ce numéro par le résultat particulier que voici :

Théorème 14. *Soit* **K** *le corps cyclotomique engendré par le nombre $\eta=e^{2\pi i/N}$, où N est un nombre naturel $\geqslant 3$; si N est pair nous supposons que N est divisible par 4. Soit de plus $\xi=e^{2\pi i/m}$ où m est un diviseur de N, tel que $1\leqslant m<N$; si m est pair nous supposons que m est divisible par 4.*

Alors, il existe dans **K** *une infinité d'anneaux* **R** *ordinaires du $\varphi(N)$-ième degré jouissant de la propriété suivante : Les racines de l'unité dans* **R** *sont données par les nombres $\pm\xi^h$ pour $h=0, 1, \ldots, \varphi(m)-1$; il n'y a aucune autre racine de l'unité dans* **R**.

Le nombre η n'est contenu que dans l'anneau fondamental de **K**. *Si N est un nombre premier l'anneau fondamental est le seul anneau dans* **K** *qui contient des racines imaginaires de l'unité.*

La première partie de ce théorème s'obtient évidemment du théorème précédent en y prenant $\theta=\eta$. De plus, un anneau **R** contenant le nombre η contient toutes les puissances de η. Donc, **R** contient tous les nombres entiers de **K**.

9. Il arrive dans certains corps $\mathbf{K}(\theta)$ que toutes les unités sont d'un degré inférieur au degré n de θ. Ce cas se présente, par exemple, pour tout corps biquadratique du premier rang appartenant à l'une ou l'autre des deux classes 5 et 7; pour la théorie de ces corps voir Nagell [6], [7], § 3 et [8], § 2. En effet, dans ce cas l'unité fondamentale du corps $\mathbf{K}(\theta)$ est égale à l'unité fondamentale du sous-corps quadratique réel; de plus, il n'y a aucune racine imaginaire de l'unité dans $\mathbf{K}(\theta)$.

Il existe des corps particuliers $\mathbf{K}(\theta)$ du n-ième degré qui ont la propriété suivante: Il y a dans $\mathbf{K}(\theta)$ des unités du n-ième degré; dans certains anneaux du n-ième degré (ordinaires) toutes les unités sont d'un degré inférieur à n. Pour illustrer cela nous prenons de nouveau des exemples de la théorie des corps biquadratiques du premier rang que nous avons dévéloppée dans les travaux précités [6], [7] et [8].

I) Considérons le corps cyclotomique engendré par le nombre $\xi=e^{\pi i/4}$. Les nombres $1, \xi, \xi^2=i, \xi^3=i\xi$ constituent une base de l'anneau fondamental. L'unité fondamentale peut être choisie égale à $\sqrt{2}+1$. Nous savons d'après le théorème 14 que l'anneau fondamental est le seul anneau qui contient le nombre ξ. Cependant, il y a une infinité d'anneaux (ordinaires) qui contiennent le nombre i.

D'après le théorème 12 les anneaux $\mathbf{R}(1, c\xi, ci, c\xi^3)$ ne contiennent aucune racine imaginaire de l'unité si le nombre naturel c est >1. Donc, toute unité de ces anneaux est de la forme $\pm(1+\sqrt{2})^N$, où N est un nombre entier rationnel tel que

$$(1+\sqrt{2})^N-(1-\sqrt{2})^N$$

soit divisible par c.

II) Considérons ensuite le corps cyclotomique engendré par le nombre $\xi = e^{2\pi i/5}$. Les nombres $1, \xi, \xi^2, \xi^3$ constituent une base de l'anneau fondamental. L'unité fondamentale peut être choisie égale à $\frac{1}{2}(\sqrt{5}+1)$. Nous savons d'après le théorème 14 que l'anneau fondamental est le seul anneau qui contient le nombre ξ. Il en résulte que tous les autres anneaux ne contiennent que des unités de la forme

$$\pm[\tfrac{1}{2}(1+\sqrt{5})]^N,$$

où N est un nombre entier rationnel.

III) Considérons aussi le corps cyclotomique engendré par le nombre $\xi = e^{i\pi/6}$. On vérifie aisément que les nombres $1, i, \varrho$ et $i\varrho$ constituent une base de l'anneau fondamental, où $\varrho = \xi^2$. D'après le théorème 14 le nombre ξ n'est contenu dans aucun autre anneau que l'anneau $\mathbf{R}(1, \xi, \xi^2, \xi^3) = \mathbf{R}(1, i, \varrho, i\varrho)$. On montre sans peine que les anneaux $\mathbf{R}(1, i, c\varrho, ci\varrho)$, où c est un nombre naturel >1, ne contiennent pas d'autres racines imaginaires de l'unité que $\pm i$. D'une façon analogue on vérifie que les anneaux $\mathbf{R}(1, ci, \varrho, ci\varrho)$, où c est un nombre naturel >1, ne contiennent pas d'autres racines imaginaires de l'unité que $\pm\varrho$ et $\pm\varrho^2$.

Considérons maintenant l'anneau

$$\mathbf{R} = \mathbf{R}(1, \sqrt{3}, ci, ci\sqrt{3}),$$

où c est un nombre naturel >1. Cet anneau est contenu dans $\mathbf{K}(\xi)$. Il est évident que les unités réelles contenues dans $\mathbf{R}$ sont données par la formule

$$\pm(2+\sqrt{3})^N, \tag{14}$$

N étant un nombre entier rationnel quelconque. Il est clair que $\mathbf{R}$ ne contient aucun des nombres $\pm i$, $\pm\varrho$, $\pm\varrho^2$. L'unité fondamentale de $\mathbf{K}(\xi)$ peut être choisie égale à $\eta = \frac{1}{2}(1+i)(1+\sqrt{3})$. Posons $E = \eta\zeta$, où ζ est une racine quelconque de l'équation $x^{12}-1=0$. Alors, on montre aisément que aucun des nombres E n'appartient à $\mathbf{R}$. En effet, si l'on pose $\beta = \sqrt{3}$ on aura $\xi = \frac{1}{2}(\xi+i)$ et

$$\eta = \tfrac{1}{2}(1+\beta+i+i\beta), \quad \eta i = \tfrac{1}{2}(-1-\beta+i+i\beta),$$
$$\eta\varrho = -1-\tfrac{1}{2}\beta+\tfrac{1}{2}i, \qquad \eta\varrho^2 = \tfrac{1}{2}-i-\tfrac{1}{2}i\beta,$$
$$\eta\xi = \tfrac{1}{2}+i+\tfrac{1}{2}i\beta, \qquad \eta\xi^{-1} = 1+\tfrac{1}{2}\beta+\tfrac{1}{2}i.$$

Supposons que $\mathbf{R}$ contienne le nombre

$$\xi^k E^{2m+1} = (2i+i\sqrt{3})^m \eta\zeta^{2m+1}\xi^k = (2+\sqrt{3})^m \eta\xi^h,$$

où k, m et h sont des nombres entiers rationnels. Toute puissance de $2+\sqrt{3}$ appartient à $\mathbf{R}$. Alors, il en résulterait que le nombre $\eta\xi^h$ appartiendrait à $\mathbf{R}$. Or, nous venons de voir que cela n'est pas possible. Il en résulte que toute unité de $\mathbf{R}$ doit être de la forme

$$\xi^k E^{2m} = (2i+i\sqrt{3})^m \zeta^{2m}\xi^k = (2+\sqrt{3})^m \xi^h,$$

où k, m et h sont des nombres entiers rationnels. Donc ξ^h doit appartenir à $\mathbf{R}$, ce qui entraîne $\xi^h = \pm 1$. Par conséquent : *On obtiendra toutes les unités de* $\mathbf{R}$ *par la formule* (14).

Remarque 3. Dans les exemples du numéro 9 il s'agissait d'un type particulier de corps algébrique : Le corps **K** du rang r admet un sous-corps **U** du même rang r. Nous nous proposons de caractériser les corps de ce type.

Soient n le degré de **K**, r_1 le nombre de ses corps conjugués réels et $2r_2$ le nombre de ses corps conjugués imaginaires. Alors, on a $n=r_1+2r_2$ et $r=r_1+r_2-1$. Désignons par v, ϱ_1, ϱ_2 et ϱ les quantités correspondantes pour le sous-corps U. Alors, $v=\varrho_1+2\varrho_2$ et $\varrho=\varrho_1+\varrho_2-1$. On a évidemment $v\leqslant\frac{1}{2}n=\frac{1}{2}r_1+r_2$, d'où $\varrho_1+2\varrho_2\leqslant\frac{1}{2}r_1+r_2$. Vu que $r_1+r_2-1=\varrho_1+\varrho_2-1$ il en résulte $\varrho_2\leqslant-\frac{1}{2}r_1$, ce qui entraine $\varrho_2=r_1=0$. Il faut donc que $r_2=\varrho_1$ et $n=2r_2=2\varrho_1=2v$. Par conséquent : La condition nécessaire et suffisante pour le cas en question est que tous les corps conjugués de **K** soient imaginaires, que tous les corps conjugués de **U** soient réels et que **K** soit du second degré relativement à **U**.

§ 5. Nombres algébriques de discriminant donné. Anneaux et formes binaires

10. Dans ce paragraphe $D(\alpha)$ signifiera le discriminant du nombre algébrique α dans $\mathbf{K}(\alpha)$. Si $\mathbf{R}=\mathbf{R}(\beta_1, \beta_2, \ldots, \beta_n)$ est un anneau algébrique du n-ième degré avec la base $\beta_1, \beta_2, \ldots, \beta_n$, le nombre $D(\mathbf{R})=D(\beta_1, \beta_2, \ldots, \beta_n)$ sera appelé le discriminant de l'anneau **R**. Si n est le degré du nombre algébrique α, $\mathbf{R}(\alpha)$ signifiera l'anneau $\mathbf{R}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$.

Nous allons établir quelques résultats sur les nombres algebriques entiers de discriminant donné. Il y a évidemment une infinité de nombres algébriques entiers ayant le même discriminant. En effet, si a est un nombre entier rationnel on a $D(\alpha)=D(\alpha+a)$ pour tout nombre algébrique α.

Nous commençons par le

Théorème 15. *Soient α et β des nombres algébriques entiers du n-ième degré, et soit $D(\alpha)=D(\beta)$. Alors, si β appartient à l'anneau $\mathbf{R}(\alpha)$ on a $\mathbf{R}(\beta)=\mathbf{R}(\alpha)$.*

Démonstration. Nous avons pour $m=0, 1, 2, \ldots, n-1$,

$$\beta^m=a_{m0}+a_{m1}\alpha+\ldots+a_{m,\,m-1}\alpha^{n-1},$$

où les a_{mk} sont des nombres entiers rationnels. Donc

$$D(\beta)=\|a_{mk}\|^2\cdot D(\alpha).$$

Il en résulte que le déterminant $\|a_{mk}\|$ est égal à ±1. Par conséquent, le nombre α appartient à $\mathbf{R}(\beta)$, et cela entraîne $\mathbf{R}(\beta)=\mathbf{R}(\alpha)$.

11. Dans ce numéro nous allons considérer les nombres entiers du second degré et les anneaux ordinaires du second degré dont le discriminant a une valeur donnée. Rappelons le fait suivant de la théorie des corps quadratiques. Pour que le nombre entier rationnel D soit le discriminant d'un nombre entier du second degré ou d'un anneau entier du second degré il faut et il suffit que D satisfasse aux conditions suivantes : 1° D est ou $\equiv1$ ou $\equiv0 \pmod 4$; 2° D n'est pas le carré d'un nombre entier rationnel. Dans la suite nous supposons que ces conditions sont remplies pour tout nombre D désigné pour discriminant d'un nombre ou d'un anneau.

Soit $\Delta(\neq1)$ un nombre entier rationnel qui n'est divisible par aucun carré >1, et posons $\omega=\frac{1}{2}(1+\sqrt{\Delta})$ ou $\omega=\sqrt{\Delta}$ suivant que Δ est $\equiv1 \pmod 4$ ou non. Si D^* désigne

le discriminant du corps quadratique engendré par ω on a $D^*=\Delta$ ou $=4\Delta$ suivant que Δ est $\equiv 1 \pmod 4$ ou non.

Il est évident que tous les anneaux entiers ordinaires du second degré sont donnés par l'expression

$$\mathbf{R}(1, c\omega), \tag{15}$$

où ω a la valeur indiquée tout à l'heure, et où c est un nombre entier rationnel. Le discriminant $D(\mathbf{R})$ de l'anneau (15) est c^2D^*. Il est évident qu'on peut énoncer la proposition suivante :

Théorème 16. *Il n'y a qu'un seul anneau ordinaire du second degré ayant le discriminant donné D.*

En effet, si $D=c^2D^*$, les nombres D^* et c^2 sont univoquement déterminés.

Alors, si α et α_1 sont deux nombres entiers du second degré de même discriminant on a $\mathbf{R}(1, \alpha)=\mathbf{R}(1, \alpha_1)$. Donc, la condition nécessaire et suffisante pour qu'on ait $\mathbf{R}(1, \alpha)=\mathbf{R}(1, \alpha_1)$ est que $\alpha_1=\pm\alpha+h$, où h est un nombre entier rationnel.

Soient α et α' les racines de l'équation irréductible $x^2-px+q=0$, où p et q sont des entiers rationnels. Alors, on a $N(\alpha)=q=\frac{1}{4}[p^2-D(\alpha)]$. Supposons maintenant que les deux nombres $D(\alpha)$ et $N(\alpha)$ sont donnés. Si $p\neq 0$ on aura quatre nombres du second degré pour lesquels le discriminant et la norme ont des valeurs données ($\pm\alpha$, et $\pm\alpha'$). Si $p=0$ on aura deux nombres ayant la propriété en question ($\pm\alpha=\mp\alpha'$).

Nous allons ajouter quelques résultats sur les unités réels du second degré. Sans restreindre à la généralité nous considérons seulement les unités >1.

Théorème 17. *L'unité ε est l'unité fondamentale dans l'anneau $\mathbf{R}(1, \varepsilon)$, sauf dans le cas suivant : $\varepsilon=\frac{1}{2}(3+\sqrt{5})=\eta^2$ où $\eta=\frac{1}{2}(1+\sqrt{5})$ est l'unité fondamentale dans $\mathbf{R}(1, \varepsilon)=\mathbf{R}(1, \eta)$.*

Démonstration. Supposons que l'unité ξ soit l'unité fondamentale dans $\mathbf{R}(1, \varepsilon)$ et qu'on ait $\varepsilon=\xi^m$, où $m\geqslant 2$. Alors on a $\xi=x+y\varepsilon$, x et y étant des entiers rationnels. Donc $D(\xi)=y^2D(\varepsilon)$. On a évidemment $D(\varepsilon)=D(\xi^m)\geqslant D(\xi)$. La seule possibilité est donc $y=\pm 1$, c'est-à-dire $\xi=x\pm\varepsilon$.

Supposons d'abord que ξ est racine de l'équation

$$z^2-pz+1=0,$$

où le nombre entier rationnel p est $\geqslant 2$ vu que $\xi>1$. Il en résulte qu'on a

$$(x\pm\varepsilon)^2-p(x\pm\varepsilon)+1=0$$

et

$$\varepsilon^2+\varepsilon(\pm 2x\mp p)+x^2-px+1=0.$$

Vu que $N(\xi)=+1$ on a aussi $N(\varepsilon)=+1$. Donc $x^2-px+1=1$ et par conséquent $x=p$ et $\varepsilon^2\pm p\varepsilon+1=0$, ce qui est évidemment impossible.

Supposons ensuite que ξ est racine de l'équation

$$z^2-pz-1=0,$$

où p est un nombre naturel. On en obtient

$$(x \pm \varepsilon)^2 - p(x \pm \varepsilon) - 1 = 0$$

et

$$\varepsilon^2 + \varepsilon(\pm 2x \mp p) + x^2 - px - 1 = 0.$$

Si $x^2 - px - 1 = -1$ il faut que $x = p$ et $\varepsilon^2 \pm p\varepsilon - 1 = 0$, ce qui est évidemment impossible. Si $x^2 - px - 1 = +1$ on obtient $p = 1$ et $x = -1$ ou $= 2$. Il en résulte que $\xi^2 - \xi - 1 = 0$, $\xi = \frac{1}{2}(1 + \sqrt{5})$, $\varepsilon^2 - 3\varepsilon + 1 = 0$, $\varepsilon = \frac{1}{2}(3 + \sqrt{5})$ et $\xi = -1 + \varepsilon$.

Cela démontre le théorème 17. Nous y ajoutons le

Théorème 18. *Il n'y a qu'une seule unité ε du second degré > 1 de discriminant donné $D > 5$; cette unité est l'unité fondamentale de l'anneau $\mathbf{R}(1, \varepsilon)$. Lorsque $D = 5$ il y a deux unités > 1 de discriminant 5, à savoir $\frac{1}{2}(1 + \sqrt{5})$ et $\frac{1}{2}(3 + \sqrt{5})$.*

En effet, soit ε une racine de l'équation

$$z^2 - pz \pm 1 = 0,$$

où p est un nombre naturel; ε étant > 1 on a $p > 0$. Lorsque $D > 5$ il est évident qu'on a $D = D(\varepsilon) = p^2 \mp 4$ seulement pour une valeur de p. Pour $D = 5$ on a $5 = 1^2 + 4 = 3^2 - 4$.

12. En passant aux nombres algébriques du troisième degré nous allons d'abord établir le

Théorème 19. *Soit α un nombre algébrique entier, racine de l'équation irréductible*

$$x^3 - px^2 + qx - r = 0,$$

à coefficients entiers rationnels p, q, r.

Supposons que le discriminant $D(\alpha)$ est donné. Alors, si l'un des nombres p, q, r est aussi donné, il n'y a qu'un nombre fini de possibilités pour les deux autres. Particulièrement, il n'y a qu'un nombre fini de nombres α de discriminant donné et de norme donnée.

Démonstration. Soit $1, \omega, \omega_1$ une base des entiers du corps $\mathbf{K}(\alpha)$, et soit $\alpha = u + v\omega + w\omega_1$, où u, v et w sont des nombres entiers rationnels. Le discriminant $D(\alpha)$ est évidemment indépendant de u. Alors on a

$$D(\alpha) = D(v\omega + w\omega_1) = [f[v, w)]^2 \cdot D^*,$$

où D^* est le discriminant du corps $\mathbf{K}(\alpha)$, et où $f(v, w)$ est une forme binaire cubique à coefficients entiers et irréductible. Donc, D^* est limité par $D(\alpha)$. D'après un théorème célèbre d'Axel Thue l'équation

$$f(v, w) = \pm \sqrt{\frac{D(\alpha)}{D^*}}$$

n'a qu'un nombre fini de solutions en nombres entiers rationnels v et w. Donc, si $D(\alpha)$ est donné, les coefficients v et w sont déjà limités. Si, de plus, l'un des nombres p, q ou r est donné, il est évident qu'on n'aura qu'un nombre limité de valeurs de α. Comparez Nagell [9], § 4.

Observons surtout le corrollaire suivant :

Théorème 19 bis. *Le nombre d'unités algébriques du troisième degré de discriminant donné est limité.*

Ce résultat, aussi bien que le théorème 19, regarde la totalité des unités du troisième degré indépendamment des corps cubiques. D'une manière analogue, le théorème 16 regarde la totalité des anneaux entiers du second degré, et le théorème 18 la totalité des unités du second degré de discriminant positif.

Lorsque le discriminant est négatif on peut obtenir un résultat beaucoup plus précis que le théorème 19 bis sur les unités. Dans ce cas il suffit évidemment de regarder les unités réelles, positives et <1. Dans cette condition nous avons le

Théorème 20. *Soit donné le nombre entier négatif D. Les unités ε du troisième degré ayant le discriminant D peuvent être caractérisées de la manière suivante.*

Soient $\mathbf{R}_1, \mathbf{R}_2, \ldots, \mathbf{R}_m$ tous les anneaux entiers ordinaires du troisième degré possédant le discriminant D, et désignons par ξ_k l'unité fondamentale de $\mathbf{R}_k$.

1° *Soit d'abord D différent de -23, -31 et -44. Alors, les unités ε sont ceux des nombres ξ_k qui ont le discriminant D. Seulement dans le cas où ξ est racine d'une équation $z^3 = 1 - qz$ (q nombre naturel $\geqslant 2$) il y a une deuxième unité de discriminant D, à savoir ξ_k^2.*

2° *Il y a deux unités de discriminant $D = -44$, à savoir*

$$\xi \text{ et } \xi^3, \text{ où } \xi^3 = -\xi^2 - \xi + 1.$$

3° *Il y a quatre unités de discriminant $D = -31$, à savoir :*

$$\xi, \xi^2, \xi^3 \text{ et } \xi^5, \text{ où } \xi^3 = 1 - \xi.$$

4° *Il y a six unités de discriminant $D = -23$, à savoir :*

$$\xi, \xi^2, \xi^3, \xi^4, \xi^5 \text{ et } \xi^9, \text{ où } \xi^3 = 1 - \xi^2.$$

Pour la démonstration voir [9]. Il faut observer que les unités sont toujours supposées réelles, positives et <1. Si l'unité ε a le discriminant D il en est de même pour les unités $-\varepsilon$ et $\pm\varepsilon^{-1}$.

Il n'y a pas de résultat analogue pour les discriminants positifs.

13. On peut se demander s'il existe des résultats analogues aux théorèmes 18 et 19 pour des nombres algébriques entiers d'un degré supérieur à 3.

Soit θ un nombre algébrique entier, racine de l'équation irréductible

$$x^4 - px^3 + qx^2 - rx + s = 0, \tag{16}$$

où les coefficients p, q, r et s sont des nombres entiers rationnels. Soit $1, \omega, \omega_1, \omega_2$ une base des entiers du corps $\mathbf{K}(\theta)$, et soit

$$\theta = u + v\omega + w\omega_1 + z\omega_2,$$

où u, v, w et z sont des entiers rationnels. Alors, on a

$$D(\theta) = D(v\omega + w\omega_1 + z\omega_2) = [f(v, w, z)]^2 \cdot D^*,$$

où D^* est le discriminant du corps $\mathbf{K}(\theta)$, et où $f(v, w, z)$ est une forme ternaire du sixième degré à coefficients entiers rationnels. Donc, D^* est limité par $D(\theta)$. Pour obtenir un résultat analogue au théorème 19 on aura à résoudre l'équation

$$f(v, w, z) = \pm \sqrt{\frac{D(\theta)}{D^*}}. \tag{17}$$

en nombres entiers rationnels v, w et z. Si le corps $\mathbf{K}(\theta)$ admet un sous-corps quadratique on voit aisément que $f(v, w, z)$ est décomposable en facteurs à coefficients rationnels. Dans ce cas il est possible de montrer que l'équation (17) a un nombre fini de solutions. Nous allons revenir sur cette question prochainement. Pour le moment nous nous contentons d'établir le résultat particulier que voici :

Théorème 21. *Désignons par Φ le domaine des corps biquadratiques admettant un sous-corps quadratique imaginaire. Parmi les unités du quatrième degré appartenant à ce domaine il n'y a qu'un nombre limité de discriminant donné. Ces unités peuvent être déterminées par un nombre fini d'opérations.*

Démonstration. Soit $\mathbf{K}(\theta)$ un corps biquadratique admettant un sous-corps quadratique imaginaire U engendré par $\sqrt{-\Delta}$, où Δ est un nombre naturel qui n'est divisible par aucun carré >1. Supposons que θ est une racine de l'équation (16); ainsi θ est un nombre entier. Donc θ est racine d'une équation quadratique $x^2 - ax + b = 0$ irréductible dans $\mathbf{U}$, où a et b sont des nombres entiers dans $\mathbf{U}$. Soit θ'' l'autre racine de cette équation quadratique.

Supposons d'abord que $-\Delta$ n'est pas $\equiv 1 \pmod 4$. Alors nous avons

$$\theta + \theta'' = u + v\sqrt{-\Delta}, \quad \theta\theta'' = u_1 + v_1\sqrt{-\Delta}, \tag{18}$$

où u, v, u_1 et v_1 sont des entiers rationnels. Pour les coefficients de l'équation (16) on aura les relations

$$\left.\begin{aligned} p &= 2u, \quad q = u^2 + \Delta v^2 + 2u_1, \\ r &= 2uu_1 + 2\Delta vv_1, \quad s = u_1^2 + \Delta v_1^2. \end{aligned}\right\} \tag{19}$$

Pour le discriminant D de θ on obtiendra la formule

$$D = 16\Delta^2 D_1 D_2, \tag{20}$$

où

$$D_1 = (u^2 - \Delta v^2 - 4u_1)^2 + \Delta(2uv - 4v_1)^2 \tag{21}$$

et

$$D_2 = (uvv_1 - v_1^2 - u_1 v^2)^2. \tag{22}$$

Dans le cas où $-\Delta$ est $\equiv 1 \pmod 4$ on aura seulement à remplacer, dans les formules (18)–(22), les nombres u, v, u_1 et v_1 par $\frac{1}{2}u$, $\frac{1}{2}v$, $\frac{1}{2}u_1$ et $\frac{1}{2}v_1$.

Pour la démonstration de toutes ces formules je renvoie à Nagell [8], § 3.

Soit maintenant θ une unité appartenant à Φ, et supposons que le discriminant $D(\theta) = D$ est donné. Considérons d'abord le cas que $-\Delta$ n'est pas $\equiv 1 \pmod 4$. Alors, il résulte de (20) que les nombres Δ, D_1 et D_2 sont limités. L'équation $s = 1 = u_1^2 + \Delta v_1^2$ entraîne $u_1 = \pm 1$ et $v_1 = 0$; si $\Delta = 1$ on aura aussi la possibilité $u_1 = 0$ et $v_1 = \pm 1$. Les nombres u et v seront évidemment limités par les relations (21) et (22) lorsqu'on a

choisi les valeurs de Δ, D_1 et D_2. Le raisonnement sera tout-à-fait analogue dans le cas où $-\Delta$ et $\equiv 1 \pmod 4$.

Le théorème 21 se trouve ainsi démontré. Il est évident comment on peut le généraliser. Nous allons revenir sur cette question dans un prochain travail.

14. Soit donnée la forme binaire de degré n

$$F(x, y) = x^n + a_1 x^{n-1} y + \ldots + a_n y^n, \tag{23}$$

à coefficients entiers rationnels $a_1, a_2, \ldots, a_n$, et irréductible dans le domaine rationnel. Par la transformation linéaire unimodulaire

$$x = eu + fv, \; y = gu + hv,$$

où e, f, g, h sont des nombres entiers rationnels tels que $eh - fg = \pm 1$, la forme (23) sera transformée dans la forme

$$G(u, v) = u^n + b_1 u^{n-1} v + \ldots + b_n v^n. \tag{24}$$

Cela exige qu'on a $F(e, g) = 1$. Les coefficients $b_1, b_2, \ldots, b_n$ sont des entiers rationnels; et la forme $G(u, v)$ est irréductible. Si θ est une racine de l'équation $F(x, -1) = 0$, il existe une racine θ_1 de l'équation $G(u, -1) = 0$ telle qu'on ait

$$\theta_1 = \frac{f + h\theta}{e + g\theta}.$$

Ici, le nombre $e + g\theta$ est une unité. Vu que le nombre $(e + g\theta)^{-1}$ appartient à l'anneau $\mathbf{R}(\theta)$, on en conclut que le nombre θ_1 appartient à $\mathbf{R}(\theta)$. Inversement il est clair que θ appartient à $\mathbf{R}(\theta_1)$. Par conséquent, on a le

Théorème 22. *Si les formes* (23) *et* (24) *sont équivalentes on a* $\mathbf{R}(\theta) = \mathbf{R}(\theta_1)$.

Pour $n = 2$ ce théorème est reversible. En effet, dans ce cas la relation $\mathbf{R}(\theta) = \mathbf{R}(\theta_1)$ entraine $\theta_1 = \pm\theta + c$, où c est un entier rationnel. Cependant, pour $n \geqslant 4$ le théorème n'est pas en général reversible.

On doit à F. Levi un résultat remarquable qui établit une correspondance biunivoque entre les classes des formes cubiques binaires et les anneaux entiers, ordinaires du troisième degré; voir Levi [10], comparez aussi Delaunay [11] et Nagell [9]. Levi montre d'abord que la base de l'anneau entier cubique $\mathbf{R}(1, \alpha, \beta)$ peut être choisie de façon qu'on ait les relations

$$\alpha^3 - b\alpha^2 + ac\alpha - a^2 d = 0,$$

$$\beta^3 - c\beta^2 + bd\beta - ad^2 = 0,$$

$$\alpha\beta = ad,$$

où a, b, c et d sont des nombres entiers rationnels. Le résultat de Levi peut être formulé ainsi qu'il suit :

Théorème 23. *Soient* α, β, α_1 *et* β_1 *des nombres entiers du troisième degré dans le même corps cubique, tels que*

$$\alpha^3 - b\alpha^2 + ac\alpha - a^2 d = 0, \quad \alpha\beta = ad$$

et

$$\alpha_1^3 - b_1\alpha_1^2 + a_1 c_1 \alpha_1 - a_1^2 d_1 = 0, \quad \alpha_1\beta_1 = a_1 d_1.$$

Alors, si les anneaux $\mathbf{R}(1, \alpha, \beta)$ *et* $\mathbf{R}(1, \alpha_1, \beta_1)$ *sont identiques, les formes binaires cubiques*

$$ax^3 + bx^2y + cxy^2 + dy^3 \quad et \quad a_1 x_1^3 + b_1 x_1^2 y_1 + c_1 x_1 y_1^2 + d_1 y_1^3$$

sont équivalentes; et inversement, l'équivalence des formes entraîne l'identité des anneaux. Les formes et les anneaux ont le même discriminant.

Il est vraisemblable qu'il existe des résultats analogues pour les degrés supérieurs à 3. Si le degré est n on aura évidemment à faire avec des formes décomposables du n-ième degré à $n-1$ variables.

INDEX BIBLIOGRAPHIQUE

1. FUCHS, L., Abelian groups, Budapest 1958.
2. HECKE, E., Vorlesungen über die Theorie der algebraischen Zahlen, Leipzig 1923.
3. NAGELL, T., Remarques sur les groups abéliens infinis admettant une base finie, Arkiv f. matematik, Bd. 4, nr. 41, Stockholm 1962.
4. NAGELL, T., Die Bestimmung der Ringe mit gegebener Diskriminante in einem algebraischen Zahlkörper, Norsk Matematisk Forenings Skrifter, Ser. II, Nr. 9, Oslo 1933.
5. NAGELL, T., Sätze über algebraische Ringe, Mathematische Zeitschrift Bd. 34, Berlin 1931.
6. NAGELL, T., Sur quelques questions dans la théorie des corps biquadratiques, Arkiv f. matematik, Bd. 4, nr. 26, Stockholm 1961.
7. NAGELL, T., Sur une propriété des unités d'un corps algébrique, Arkiv f. matematik, Bd. 5, nr. 25, Stockholm 1964.
8. NAGELL, T., Sur les représentations de l'unité par les formes binaires biquadratiques du premier rang, Bd. 5, nr. 33, 1965.
9. NAGELL, T., Zur Theorie der kubischen Irrationalitäten, Acta Mathematica, Bd. 55, Stockholm 1929.
10. LEVI, F., Kubische Zahlkörper und binäre kubische Formenklassen, Berichte der Sächsischen Ges. d. Wiss., Math.-Phys. Klasse, Bd. 66, Leipzig 1914.
11. DELAUNAY, B., Solution du problème d'équivalence et tabularisation des formes binaires cubiques de discriminant négatif (en russe), Journ. Soc. Math. de Leningrad, 1926.
12. HILBERT, D., Die Theorie der algebraischen Zahlkörper, Ch. IX, Bericht d. Deutschen Mathem.-Vereinigung, Bd. IV, Berlin 1898.
13. BERWICK, W. E. H., Integral Bases, Cambridge 1927.
14. BACHMANN, P., Allgemeine Arithmetik der Zahlenkörper, Leipzig 1905.
15. NAGELL, T., Zur Theorie der algebraischen Ringe, Journ. für Math., Bd. 164, Berlin 1931.

Après avoir reçu les épreuves j'ai appris que le théorème 1 se trouve déjà chez Ch. Hermite, Sur un problème relatif à la théorie des nombres, Journ. de mathém., t. 14, 1849.

Tryckt den 27 juli 1965

Uppsala 1965. Almqvist & Wiksells Boktryckeri AB