ARKIV FÖR MATEMATIK Band 5 nr 4

Communiqué le 24 octobre 1962

Sur les sous-corps des corps métacycliques du sixième degré

PAR TRYGVE NAGELL

1. Introduction

Nous prenons pour domaine de rationalité fondamental un *corps quelconque* donné Ω, et nous entendons, sauf avis contraire, par nombre rationnel un nombre appartenant à Ω. Le corps des *nombres rationnels ordinaires* sera désigné par $\mathbf{R}$. Les notions suivantes sont toujours supposées d'être *relatives par rapport à* Ω : Équation algébrique irréductible. Nombre algébrique de degré n. Corps algébrique de degré n. Nombres conjugués. Corps conjugués. Équation génératrice d'un corps algébrique. Corps métacyclique. Corps de Galois. Corps abélien. Corps cyclique. Par $\mathbf{K}(\Omega; \xi)$ ou plus court $\mathbf{K}(\xi)$ nous désignons le corps algébrique obtenu en adjoignant le nombre algébrique ξ à Ω. D'une manière analogue $\mathbf{K}(\xi, \eta)$ désigne le corps engendré par les deux nombres ξ et η.

Il résulte d'un théorème bien connu d'Abel (voir [1], tome II, p. 217, ou H. Weber [2], Bd. 2, p. 358) (1) :

Théorème 1. *Tout corps métacyclique dont le degré N n'est pas une puissance d'un nombre premier, contient au moins un sous-corps d'un degré $\geqslant 2$.*

2. Lemmes sur les corps composés

Soient α un nombre algébrique de degré m, et β un nombre algébrique de degré n. Désignons par $\alpha^{(1)} = \alpha, \alpha^{(2)}, \ldots, \alpha^{(m)}$ les nombres conjugués de α et par $\beta^{(1)} = \beta$, $\beta^{(2)}, \ldots, \beta^{(n)}$ les nombres conjugués de β. Cela posé, on a le théorème suivant :

Lemme 1. *Si u et v sont des nombres rationnels tels que le nombre $\omega = u\alpha + v\beta$ soit différent de tous les autres nombres $u\alpha^{(i)} + v\beta^{(j)}$, $i = 1, 2, \ldots, m$; $j = 1, 2, \ldots n$; $i \neq j$, le nombre ω engendre le corps composé $\mathbf{K}(\alpha, \beta)$.*

Voir p. ex. E. Hecke [3], p. 67–68. Il n'est pas nécessaire d'exiger que tous les nombres $u\alpha^{(i)} + v\beta^{(j)}$ soient différents entre eux.

Dans les lemmes suivants nous désignons pas ξ un nombre algébrique de degré n, par α et α' (ou bien α_1 et α'_1) deux nombres algébriques conjugués du deuxième degré et par β, β' et β'' trois nombres algébriques conjugués du troisième degré.

La proposition suivante est évidente :

(1) Les numéros figurant entre crochets renvoient à la bibliographie placée à la fin de ce mémoire.

Lemme 2. *Le corps composé* $\mathbf{K}(\alpha, \xi)$ *est de degré n ou 2n selon que* α *appartient à* $\mathbf{K}(\xi)$ *ou non.*

On a encore :

Lemme 3. *Le corps composé* $\mathbf{K}(\beta, \xi)$ *est de degré n quand* β *appartient à* $\mathbf{K}(\beta)$, *et de degré 2n quand* $\mathbf{K}(\xi)$ *contient* β' *tandis que* β *et* β'' *n'appartiennent pas à ce corps. Dans les autres cas son degré est égal à 3n.*

Démonstration. Si le nombre β est du second degré par rapport à $\mathbf{K}(\xi)$, celui-ci est racine d'une équation du second degré dont les coefficients appartiennent à $\mathbf{K}(\xi)$; l'autre racine de cette équation soit β'. Alors $\beta+\beta'$ est un nombre dans $\mathbf{K}(\xi)$. Vu que la somme $\beta+\beta'+\beta''$ est rationnel on en conclut que β'' appartient à $\mathbf{K}(\xi)$. D'autre part, si β'' appartient à $\mathbf{K}(\xi)$ le nombre β est au plus du second degré par rapport à ce corps.

Nous allons y ajouter le

Lemme 4. *On a* $\mathbf{K}(\beta, \sqrt{D(\beta)}) = \mathbf{K}(\beta, \beta')$, *quand* $D(\beta)$ *signifie le discriminant de* β.

Démonstration. Soit β racine de l'équation $x^3 = px^2 - qx + r$ aux cofficients rationnels p, q et r. De l'identité

$$(\beta-\beta')(\beta-\beta'')(\beta'-\beta'') = \pm\sqrt{D(\beta)}$$

on tire

$$2\beta'+\beta-p = \frac{\pm\sqrt{D(\beta)}}{3\beta^2-2p\beta+q}. \tag{1}$$

Donc β' appartient à $\mathbf{K}(\beta, \sqrt{D(\beta)})$ et $\sqrt{D(\beta)}$ appartient à $\mathbf{K}(\beta, \beta')$. Cela démontre le lemme 4.

Un supplément à ce résultat est le

Lemme 5. *Le nombre* $\beta-\beta'$ *engendre le corps* $\mathbf{K}(\beta, \beta')$.

Démonstration. Supposons comme tout à l'heure que $\beta+\beta'+\beta''=p$ et posons $\gamma=\beta-\beta'$, $\gamma_1=\beta-\beta''$ et $\gamma_2=\beta'-\beta''$. Alors, d'après le lemme 1 il suffit de montrer que γ est différent de chacun des nombres $-\gamma$, $\pm\gamma_1$ et $\pm\gamma_2$. On ne peut pas avoir $\gamma=-\gamma$ vu que $\beta\neq\beta'$. $\gamma=\gamma_1$ entraînerait $\beta'=\beta''$. De $\gamma=-\gamma_1$ on aurait $3\beta=p$. De $\gamma=\gamma_2$ on aurait $3\beta'=p$. Enfin l'égalité $\gamma=-\gamma_2$ entraînerait $3\beta''=p$. Tout cela étant impossible il est évident que le corps $\mathbf{K}(\beta, \beta')$ sera engendré par $\beta-\beta'$.

Nous avons encore besoin des lemmes suivants :

Lemme 6. *Si* α *et* α_1 *engendrent des corps quadratiques différents, le nombre* $\alpha+\alpha_1$ *engendre les corps composé* $\mathbf{K}(\alpha, \alpha_1)$ *du quatrième degré.*

Lemme 7. *Le nombre* $\alpha+\beta$ *engendre les corps composé* $\mathbf{K}(\alpha, \beta)$ *du sixième degré.*

Démonstration du lemme 6. Il est évident que les nombres $\alpha+\alpha_1$, $\alpha'+\alpha_1'$, $\alpha'+\alpha_1$, $\alpha+\alpha'_1$, sont différents entre eux. Alors on peut appliquer les lemmes 1 et 2.

Démonstration du lemme 7. D'une relation de la forme $\alpha+\beta=\alpha'+\beta'$ on aurait $\beta-\beta'=\alpha'-\alpha$. Ici le nombre $\alpha'-\alpha$ est du second degré. Or, d'après le lemme 5 le nombre $\beta-\beta'$ est ou du troisième ou du sixième degré. Donc on aura seulement à appliquer le lemme 1 pour achever la démonstration du lemme 7. On trouvera les lemmes 1–7 dans un travail antérieur, voir Nagell [4], p. 3–6.

Lemme 8. *Le nombre $\alpha\beta$ engendre le corps composé $\mathbf{K}(\alpha, \beta)$ du sixième degré, sauf dans le cas suivant : $\alpha = a\varrho$, $\beta^3 = c$, où a et c sont rationnels et $\varrho^2 + \varrho + 1 = 0$.*

Démonstration. Les nombres conjugués de $\omega = \alpha\beta$ dans $\mathbf{K}(\alpha, \beta)$ sont évidemment

$$\alpha\beta,\ \alpha\beta',\ \alpha\beta'',\ \alpha'\beta,\ \alpha'\beta',\ \alpha'\beta''.$$

Supposons que le degré m de ω soit < 6. Il est évident que, parmi les six nombres conjugués, on ne peut trouver aucun triplet de nombres coincidants. Ainsi $m \neq 2$, et il reste seulement à examiner le cas de $m = 3$. Dans ce cas il faut qu'on ait

$$\alpha\beta = \alpha'\beta',\quad \alpha\beta' = \alpha'\beta'',\quad \alpha'\beta = \alpha\beta''.$$

Donc

$$\frac{\alpha}{\alpha'} = \frac{\beta'}{\beta} = \frac{\beta''}{\beta'} = \frac{\beta'}{\beta''}$$

et par suite

$$\beta^3 = \beta\beta'\beta'' = c = \text{nombre rationnel.}$$

Il en resulté que $\alpha' = \varrho\alpha$ avec $\varrho^2 + \varrho + 1 = 0$. Cela entraîne $\alpha = a\varrho$, où a est un nombre rationnel.

3. Les sous-corps d'un corps du sixième degré

Dans la suite $\mathbf{K}_N$ désignera un corps de degré N. Désignons par m le nombre des sous-corps quadratiques et par n le nombre des sous-corps cubiques d'un $\mathbf{K}_6$. Alors, en prenant $N = 6$ dans le théorème 1, on aura :

Théorème 2. *La condition nécessaire et suffisante pour qu'un corps du sixième degré soit métacyclique est qu'on ait $m + n > 0$.*

Ce resultat peut être précisé comme il suit.

Théorème 3. *Pour un $\mathbf{K}_6$ métacyclique il y a les quatre possibilités suivantes : 1) $m = 1$ et $n = 0$; 2) $m = 0$ et $n = 1$; 3) $m = n = 1$; 4) $m = 1$ et $n = 3$. Dans le dernier cas les trois sous-corps cubiques sont conjugués et différents. Le sous-corps quadratique est engendré par la racine carrée du discriminant d'une équation génératrice des sous-corps cubiques.*

Démonstration. $\mathbf{K}_6$ ne peut pas contenir deux sous-corps quadratiques vu que son degré n'est pas divisible par 4 (Lemme 2). L'existence de deux sous-corps cubiques non-conjugués est exclue puisque son degré n'est pas divisible par 9 (Lemme 3). Si $\mathbf{K}_6$ contient deux corps cubiques conjugués il contient aussi le troisième corps conjugué; et dans ce cas il contient la racine carrée du discriminant d'une équation génératrice des corps cubiques (Lemme 4). Le théorème 3 se trouve ainsi démontré.

Si $\mathbf{K}_6$ contient et un sous-corps quadratique engendré par α et un sous-corps cubique engendré par β, il est évident que $\mathbf{K}_6$ sera engendré par $\alpha + \beta$ (Lemme 7). Si $\alpha = \sqrt{\Delta}$, Δ rationnel, $\mathbf{K}_6$ sera engendré par $\beta\sqrt{\Delta}$ (Lemme 8).

Si $\mathbf{K}_6$ admet le sous-corps quadratique $\mathbf{K}_2$ tout nombre ξ de $\mathbf{K}_6$ est racine d'une équation cubique

$$x^3 + \gamma x^2 + \gamma_1 x + \gamma_2 = 0,$$

où γ, γ_1 et γ_2 appartiennent à $\mathbf{K}_2$. Nous allons montrer qu'on peut choisir un nombre

générateur ξ de $\mathbf{K}_6$ tel que $\gamma = 0$. Cela est évident quand le nombre $\theta = \xi + \frac{1}{3}\gamma$ est du sixième degré. Si $\mathbf{K}_6$ admet un sous-corps cubique $\mathbf{K}_3$ engendré par β, on peut supposer que $\beta + \beta' + \beta'' = 0$; alors, si $\mathbf{K}_2$ est engendré par $\alpha = \sqrt{\Delta}$, le nombre $\xi = \beta\sqrt{\Delta}$ est du sixième degré (Lemme 8) et racine d'une équation de la forme

$$x^3 + ax + b\sqrt{\Delta} = 0,$$

où a et b sont rationnels.

Supposons ensuite que $\mathbf{K}_6$ n'admet aucun sous-corps cubique. Alors, si θ n'est pas du sixième degré, ce nombre est du second degré. Donc $\theta - \frac{1}{3}\gamma = \xi$ serait du second degré, ce qui est contre l'hypothèse.

Si $\mathbf{K}_6$ admet le sous-corps cubique $\mathbf{K}_3$, tout nombre ξ de $\mathbf{K}_6$ est racine d'une équation quadratique

$$x^2 + \gamma x + \delta = 0,$$

où γ et δ appartiennent à $\mathbf{K}_3$. Nous allons montrer qu'il existe un nombre ω de $\mathbf{K}_3$ tel que $\sqrt{\omega}$ soit un nombre générateur de $\mathbf{K}_6$. Cela est évident quand le nombre $\theta = \xi + \frac{1}{2}\gamma$ est du sixième degré. Supposons que $\mathbf{K}_6$ admet un sous-corps quadratique $\mathbf{K}_2$ engendré par $\alpha = \sqrt{\Delta}$, et que $\mathbf{K}_3$ est engendré par β. Cela étant, le nombre $\xi = \beta\sqrt{\Delta}$ est du sixième degré (Lemme 8) et racine de l'équation

$$x^2 - \Delta\beta^2 = 0.$$

Supposons ensuite que $\mathbf{K}_6$ n'admet aucun sous- corps quadratique. Alors, si θ n'est pas du sixième degré, ce nombre est du troisième degré. θ ne peut pas appartenir au corps cubique $\mathbf{K}_3$ vu que $\xi = \theta - \frac{1}{2}\gamma$. Donc, θ doit appartenir á un corps cubique conjugué de $\mathbf{K}_3$ (Théorème 3). On en conclut que $\mathbf{K}_6$ contient la racine carrée $\sqrt{D(\theta)}$, nombre du second degré, ce qui est contre l'hypothèse.

Nous avons ainsi établi le

Lemme 9. *Si $\mathbf{K}_6$ admet le sous-corps quadratique $\mathbf{K}_2$ il existe un nombre générateur de $\mathbf{K}_6$ qui est racine d'une équation cubique de la forme*

$$x^3 + \gamma_1 x + \gamma_2 = 0,$$

où γ_1 et γ_2 appartiennent à $\mathbf{K}_2$. Si $\mathbf{K}_6$ admet le sous-corps cubique $\mathbf{K}_3$ il existe un nombre ω de $\mathbf{K}_3$ tel que $\sqrt{\omega}$ soit un nombre générateur de $\mathbf{K}_6$.

Si le même corps $\mathbf{K}_6$ est engendré par les deux nombres $\xi = \sqrt{\omega}$ et $\xi_1 = \sqrt{\omega_1}$, où ω et ω_1 sont des nombres du troisième degré, il faut évidemment qu'on ait $\mathbf{K}(\omega) = \mathbf{K}(\omega_1)$ et $\omega_1 = \omega\eta^2$, η étant un nombre dans $\mathbf{K}(\omega)$.

4. Corps de Galois

Si $\mathbf{K}$ est un corps de Galois il est évident que la racine carrée du discriminant d'une équation génératrice du corps appartient au corps. Il en résulte

Théorème 4. *Dans un corps de Galois de degré impair le discriminant d'une équation génératrice est le carré d'un nombre rationnel (= nombre dans Ω).*

Si le corps est cubique ce résultat peut être précisé de la manière suivante :

Théorème 5. *La condition nécessaire et suffisante pour qu'un corps cubique soit un corps de Galois est que le discriminant d'une équation génératrice soit le carré d'un nombre rationnel (= nombre dans* Ω*). Un corps cubique de Galois est cyclique.*

Théorème 5bis. *Pour que l'équation cubique, à coefficients rationnels a et b,*

$$x^3 - ax + b = 0 \tag{2}$$

définisse un corps cubique de Galois, il faut et il suffit, à condition que $a \neq 0$*, qu'on ait*

$$a = 3(U^2 - UV + V^2) \tag{3}$$

et

$$b = U^3 + V^3, \tag{4}$$

où U et V sont des nombres rationnels tels que l'équation (2) *soit irréductible. Si* $a = 0$ *il faut et il suffit que le nombre* $\sqrt{-3}$ *soit rationnel (= nombre dans* Ω*) et que le nombre b ne soit pas le cube d'un nombre rationnel.*

Démonstration. La première partie de ce théorème est une conséquence du théorème 4 et de la relation (1) dans le n° 2. Donc, pour que l'équation (2) définisse un corps de Galois il faut et il suffit qu'on ait

$$4a^3 - 27b^2 = c^2, \tag{5}$$

c étant un nombre rationnel. Si $a \neq 0$ nous posons

$$U = \frac{9b + c}{6a}, \quad V = \frac{9b - c}{6a}. \tag{6}$$

On vérifie aisément que ces valeurs de U et V satisfont aux relations (3) et (4). Pour cela il faut, bien entendu, avoir égard à la relation (5). Inversement, si a et b sont donnés par les expressions (3) et (4), on aura pour c l'expression

$$c = 9(U^2 - UV + V^2)(U - V), \tag{7}$$

et alors on voit que les nombres a, b et c satisfont aux relations (6).

Si $a = 0$ les conditions du théorème 5bis sont évidentes.

Remarque I. Le théorème 5bis peut évidemment être énoncé comme il suit :

Théorème 6. *Si* Ω *est un domaine de rationalité quelconque, la solution complète de l'équation diophantienne*

$$X^3 = 3Y^2 + Z^2 \tag{8}$$

en nombres X, Y et Z appartenant à Ω*,* $X \neq 0$*, est donnée par les formules*

$$X = 3(U^2 - UV + V^2), \tag{9}$$

$$\pm 2Y = 3(U^3 + V^3), \tag{10}$$

$$\pm 2Z = 9(U^2 - UV + V^2)(U - V), \tag{11}$$

où U et V sont des nombres quelconques de Ω*.*

En effet, on aura seulement à remplacer a par X, b par $\frac{2}{3}y$ et c par $2Z$.

Si on remplace ensuite X par $3X$, Y par $3Y$ et Z par $9Z$, les équation (8)–(11) se transforment en

$$X^3 = Y^2 + 3Z^2, \tag{8'}$$

$$X = U^2 - UV + V^2, \tag{9'}$$

$$\pm 2Y = U^3 + V^3, \tag{10'}$$

$$\pm 2Z = (U^2 - VV + V^2)(U - V). \tag{11'}$$

C'est un fait remarquable que la solution complète de l'équation (8) dans un *corps quelconque* est donnée par une *identité*.

Nous allons retourner sur les applications du théorème 6 dans un travail ultérieur.

Remarque II. Pour compléter le théorème 5bis il fallait une méthode pour reconnaître si l'équation (2) est irréductible quand les coefficients a et b sont donnés par les formules (3) et (4). Si nous désignons par X, Y et Z les racines de l'équation (2), nous aurons pour a et b les expressions

$$a = X^2 + XY + Y^2, \tag{12}$$

$$b = XY(X + Y). \tag{13}$$

Inversement, si les coefficients a et b ont ces valeurs-ci, les racines de (2) sont X, Y et $Z = -X - Y$. Si l'équation (2) est réductible, une au moins des racines est rationnelle. Soit la racine Z rationnelle. Alors, vu que le discriminant de (2) a la valeur

$$[9(U^2 - UV + V^2)(U - V)]^2,$$

il résulte de la relation (1) du n° 2 que les racines X et Y sont aussi rationnelles. Ainsi, pour trouver les coefficients a et b pour lesquels l'équation (2) soit réductible, il faut résoudre le système

$$a = 3(U^2 - UV + V^2) = X^2 + XY + Y^2, \tag{14}$$

$$b = U^3 + V^3 = XY(X + Y), \tag{15}$$

en nombres rationnels U, V, X et Y. En posant dans (14) $U = V + u$, $X = V + v$, $Y = V + w$, on aura la représentation paramétrique

$$V = \frac{-3u^2 + v^2 + w^2 + vw}{3u - 3v - 3w}, \tag{16}$$

$$U = \frac{v^2 + w^2 - 3uv - 3uw + vw}{3u - 3v - 3w}, \tag{17}$$

$$X = \frac{-3u^2 - 2v^2 + w^2 + 3uv - 2vw}{3u - 3v - 3w}, \tag{18}$$

$$Y = \frac{-3u^2 + v^2 - 2w^2 + 3uw - 2vw}{3u - 3v - 3w}, \tag{19}$$

En introduisant ces valeurs de U, V, X et Y dans l'équation (15) nous aurons une courbe algébrique du sixième degré à coefficients rationnels appartenant à $\mathbf{R}$, homogène dans les coordonnées u, v et w. Ainsi, pour trouver les nombres a et b pour lesquels l'équation (2) est réductible on aura à déterminer tous les points rationnels (dans $\mathbf{\Omega}$) sur la sextique. Nous allons retourner sur cette question bientôt.

5. Classification des corps du sixième degré

Soit $\mathbf{K}_N$ un corps de Galois de degré N, et désignons par $\mathbf{G}$ le groupe de Galois appartenant à ce corps. L'ordre de $\mathbf{G}$ est égal à N. Soit p un nombre premier divisant N. Alors, $\mathbf{G}$ admet un sous-groupe cyclique d'ordre p, et à ce sous-groupe correspond un sous-corps de $\mathbf{K}_N$ d'ordre p. (Voir p. ex. D. Hilbert [5], p. 250.) Il en résulte qu'un corps de Galois du sixième degré contient et un sous-corps quadratique et un sous-corps cubique. Ainsi, seulement dans les deux derniers cas du théorème 3 le corps $\mathbf{K}_6$ peut être un corps de Galois. Dans ces cas le corps est engendré par un nombre de la forme $\alpha+\beta$, où α est du second degré et β du troisième degré. Si $\mathbf{K}(\beta)$ est un corps de Galois, il est évident que $\mathbf{K}(\alpha,\beta)$ est un corps de Galois et même un corps abélien et cyclique. Si $\mathbf{K}(\beta)$ n'est pas un corps de Galois, $\mathbf{K}(\alpha,\beta)$ est un corps de Galois seulement quand $\mathbf{K}(\alpha)$ est engendré par la racine carrée du discriminant d'une équation génératrice de $\mathbf{K}(\beta)$. Cependant, dans ce cas $\mathbf{K}(\alpha,\beta)$ n'est pas abélien vu que $\mathbf{K}(\beta)$ n'est pas abélien.

Pour les $\mathbf{K}_6$ métacycliques nous aurons ainsi la classification donnée dans le tableau ci-dessous. Comme plus haut m désigne le nombre des sous-corps quadratiques et n le nombre des sous-corps cubiques. Pour les types des corps nous employons les raccourcissements suivants : N signifie que le corps n'est pas un corps de Galois. G signifie que le corps est un corps de Galois non abélien. C signifie que le corps est abélien et cyclique. N^* signifie que le sous-corps cubique n'est pas un corps de Galois, le cas échéant aucun des trois sous-corps cubiques n'est un corps de Galois. C^* signifie que le sous-corps cubique est cyclique.

Classe	1	2	3	4	5	6
m	1	0	0	1	1	1
n	0	1	1	1	1	3
$\mathbf{K}_6$	N	N	N	N	C	G
$\mathbf{K}_3$		N*	C*	N*	C*	N*

Remarque III. Un corps de Galois du sixième degré est toujours métacyclique, mais il n'est pas toujours abélien; s'il est abélien il est cyclique. Comparez les classifications des corps biquadratiques que nous avons données dans un travail antérieur, voir Nagell [6], p. 351–352. Un corps de Galois du quatrième degré est, bien entendu, toujours abélien.

Considérons ensuite le cas d'un $\mathbf{\Omega}$ réel, et désignons par ϱ le nombre des corps conjugués réels. Prenons d'abord la classe 1 dans le tableau ci-dessus. Si le sous-corps quadratique est réel on voit aisément que tous les trois cas $\varrho=2$, 4 et 6 peuvent se présenter. Si le sous-corps quadratique est imaginaire on a toujours $\varrho=0$. Examinons ensuite les classes 2 et 3, dans lesquelles il y a un sous-corps cubique. Si le discriminant d'une équation génératrice de ce corps cubique est positif, on peut

avoir chacun des cas $\varrho = 0$, 2, 4 et 6. Si le discriminant est négatif on a ou $\varrho = 0$ ou $\varrho = 2$.

Considérons enfin les classes 4, 5 et 6. Dans ces cas le corps $\mathbf{K}_6$ est engendré par un nombre $\theta = \alpha + \beta$, où α est du second degré et β du troisième degré. Si α est réel et $D(\beta) > 0$ on a $\varrho = 6$. Si α est réel et $D(\beta) < 0$ on a $\varrho = 2$. Si α est imaginaire on a $\varrho = 0$.

Remarque IV. Quand le domaine fondamental $\mathbf{\Omega}$ est quelconque il n'y a aucune méthode générale pour déterminer les sous-corps d'un $\mathbf{K}_6$ arbitrairement donné. Cependant, dans des cas spéciaux on peut y arriver. Prenons par exemple le cas suivant : Soit θ une racine de l'équation $x^6 - a = 0$, où a est un nombre dans $\mathbf{\Omega}$ qui n'est ni un cube ni un carré dans $\mathbf{\Omega}$. Alors le corps $\mathbf{K}(\theta)$ du sixième degré contient les sous-corps $\mathbf{K}(\theta^2)$ et $\mathbf{K}(\theta^3)$ du troisième et du second degré respectivement. Si $\mathbf{\Omega}$ ne contient pas le nombre $\sqrt{-3}$ et si a n'est pas de la forme $-3b^6$, b nombre dans $\mathbf{\Omega}$, il est évident que $\mathbf{K}(\theta)$ appartient à la classe 4. Dans tous les autres cas le corps appartient à la classe 5.

Quand $\mathbf{\Omega}$ est un corps algébrique on peut toujours déterminer les sous-corps de $\mathbf{K}_6$; voir Nagell [4], p. 11–13.

Si $\mathbf{K}_6$ est un corps du sixième degré qui admet un sous-corps cubique, nous avons montré (Lemme 9) que $\mathbf{K}_6$ peut être engendré par un nombre de la forme $\theta = \sqrt{\beta}$, où β est un nombre du troisième degré, racine de l'équation

$$x^3 - px^2 + qx - r = 0, \tag{20}$$

p, q et r appartenant à $\mathbf{\Omega}$. Le nombre β engendre le sous-corps cubique. Nous allons établir le résultat suivant :

Théorème 7. *Pour que le corps $\mathbf{K}_6$ du sixième degré engendré par le nombre $\theta = \sqrt{\beta}$, où β est une racine de l'équation* (20), *admette un sous-corps quadratique, il faut et il suffit que r ne soit pas un carré dans $\mathbf{\Omega}$ et que*

$$\beta = r\gamma^2, \tag{21}$$

où γ est un nombre dans $\mathbf{K}(\beta)$. Par conséquent, le sous-corps quadratique, s'il existe, est engendré par le nombre $\sqrt{r}$.

Démonstration. Supposons qu'il existe un sous-corps quadratique engendré par le nombre $\sqrt{\Delta}$, Δ nombre dans $\mathbf{\Omega}$. Alors le nombre $\theta = \sqrt{\beta}$ est racine d'une équation, irréductible dans $\mathbf{K}(\sqrt{\Delta})$, de la forme

$$x^3 + (a + b\sqrt{\Delta})x^2 + (c + d\sqrt{\Delta})x + f + g\sqrt{\Delta} = 0, \tag{22}$$

où a, b, c, d, f et g sont rationnels (= nombres dans $\mathbf{\Omega}$). Désignons par θ, θ_1 et θ_2 les racines de cette équation. Les trois conjugués restants de θ sont les racines de l'équation

$$x^3 + (a - b\sqrt{\Delta})x^2 + (c - d\sqrt{\Delta})x + f - g\sqrt{\Delta} = 0.$$

Il est évident que ces racines sont $-\theta$, $-\theta_1$ et $-\theta_2$. On en conclut que $a = d = f = 0$. Donc l'équation (22) aura la forme

$$x^3 + b\sqrt{\Delta}x^2 + cx + g\sqrt{\Delta} = 0. \tag{23}$$

En y introduisant $x = \theta = \sqrt{\beta}$ nous aurons

$$\sqrt{\frac{\beta}{\Delta}} = \frac{-g - b\beta}{c + \beta}, \tag{24}$$

ou bien $$\beta(c^2 + 2c\beta + \beta^2) = \Delta(g^2 + 2bg\beta + b^2\beta^2).$$

Vu que $\beta^3 = p\beta^2 - q\beta + r$, cette équation entraîne

$$2c + p = \Delta b^2, \quad c^2 - q = 2\Delta bg, \quad r = \Delta g^2.$$

En introduisant la valeur $\Delta = rg^{-2}$ dans (24) on aura

$$\beta = r\left[\frac{g + b\beta}{g(c + \beta)}\right]^2 = r\gamma^2,$$

où γ appartient au sous-corps cubique $\mathbf{K}(\beta)$. Donc la condition (21) est nécessaire.

Inversement, si la relation (21) subsiste le nombre $\sqrt{r}$ appartient à $\mathbf{K}_6$. Vu que le nombre $\sqrt{\beta} = \gamma\sqrt{r}$ est du sixième degré, le nombre $\sqrt{r}$ est du second degré. Si r est un carré dans $\mathbf{\Omega}$ il n'y a aucun sous-corps quadratique. Le théorème 7 se trouve ainsi établi.

6. Exemples numériques

Considérons l'équation réciproque

$$x^6 + ax^4 + bx^3 + ax^2 + 1 = 0, \tag{25}$$

à coefficients a et b appartenant à $\mathbf{\Omega}$. En posant $y = x + x^{-1}$ on aura

$$y^3 + (a - 3)y + b = 0 \tag{26}$$

et $$x = \tfrac{1}{2}y \pm \tfrac{1}{2}\sqrt{y^2 - 4}.$$

Soient ξ une racine de (25) et η la racine corréspondante de (26). Si nous supposons que (25) est irréductible dans $\mathbf{\Omega}$, il est évident que (26) est aussi irréductible dans $\mathbf{\Omega}$. Donc $b \neq 0$. Le nombre ξ est du sixième degré et le nombre η du troisième degré. Le corps $\mathbf{K}(\xi)$ admet le sous-corps cubique $\mathbf{K}(\eta)$ et peut être engendré par le nombre $\sqrt{\eta^2 - 4}$. Ainsi les corps définis par (25) sont toujours métacycliques. On peut se demander sous quelles conditions il y a un sous-corps quadratique. Pour cela posons $\beta = \eta^2 - 4$ et déterminons les coefficients p, q et r de l'équation irréductible

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

dont β est une racine. Alors on aura

$$\left.\begin{aligned} p &= -2a - 6, \\ q &= a^2 + 10a + 9, \\ r &= b^2 - 4(a + 1)^2. \end{aligned}\right\} \tag{27}$$

Donc, d'après le théorème 7, pour l'existence d'un sous-corps quadratique il faut et il suffit qu'on ait $r+s^2$ et

$$\beta=[b^2-4(a+1)^2]\gamma^2, \tag{28}$$

où γ est un nombre dans $\mathbf{K}(\beta)$ et s un nombre dans $\mathbf{\Omega}$.

Prenons p. ex. $a=3$, $b=16$, c'est-à-dire une équation génératrice (dans $\mathbf{R}$)

$$x^6+3x^4+16x^3+3x^2+1=0.$$

En posant $\omega=2^{1/3}$ on aura

$$\eta=-2\omega, \quad \xi=-\omega\pm\sqrt{\omega^2-1}, \quad \beta=4(\omega^2-1), \quad r=3\cdot 8^2.$$

Donc, s'il y a un sous-corps quadratique celui-ci est généré par le nombre $\sqrt{3}$. En réalité, on vérifie aisément qu'on ait

$$\tfrac{3}{4}\beta=3(\omega^2-1)=(1-\omega+\omega^2)^2.$$

On aura un autre exemple en posant $a=3$, $b=2$. Dans ce cas il vient, ω ayant la même signification que tout à l'heure,

$$\eta=-\omega, \quad \xi=-\tfrac{1}{2}\omega\pm\tfrac{1}{2}\sqrt{\omega^2-4}, \quad \beta=\omega^2-4, \quad r=-60.$$

Donc, un sous-corps quadratique eventuel serait généré par le nombre $\sqrt{-15}$. Or, on montre aisément que l'équation

$$-15\beta=15(4-\omega^2)=(a+b\omega+c\omega^2)^2$$

n'admet aucune solution en nombres entiers rationnels (dans $\mathbf{R}$). Par conséquent il n'existe aucun sous-corps quadratique dans ce cas.

Si, dans (27), le nombre r est un carré dans $\mathbf{\Omega}$, il est évident que la relation (28) ne peut pas subsister. En effet, l'équation (25) étant irréductible dans $\mathbf{\Omega}$, le nombre β ne peut pas être un carré dans $\mathbf{K}(\beta)$. Ainsi il n'y a aucun sous-corps quadratique dans ce cas.

Pour une étude approfondie des corps engendrés par les équations du type (25) dans un domaine réel $\mathbf{\Omega}$ on a besoin du résultat suivant :

Désignons par M le nombre des racines réelles de l'equation (25), *où les coefficients a et b sont réels. Pour qu'on ait $M=0$ il faut et il suffit que $|b|<2a+2$. Pour que $M=4$ il faut et il suffit qu'on ait ou $|b|<-2a-2$ ou $|b|=-2a-2<16$. Pour que $M=6$ il faut et il suffit qu'on ait*

$$16\leqslant -2a-2\leqslant|b|\leqslant\tfrac{2}{3}(3-a)\sqrt{\tfrac{1}{3}(3-a)}.$$

Dans tous les autres cas on a $M=2$.

Nous finissons avec quelques exemples numériques dans le domaine fondamental $\mathbf{R}$ des nombres rationnels ordinaires.

Exemple 1. Le corps du sixième degré $\mathbf{R}(\xi)$ engendré par le nombre réel

$$\xi=\sqrt[3]{2+\sqrt{2}}$$

réalise la classe 1 du numéro 5. En effet, le nombre réel

$$\xi_1 = \sqrt[3]{2-\sqrt{2}}$$

est un conjugué de ξ. Les quatre autres conjugués sont $\xi\varrho$, $\xi\varrho^2$, $\xi_1\varrho$, $\xi_1\varrho^2$, où $\varrho^2+\varrho+1=0$. $\mathbf{R}(\xi)$ admet le sous-corps quadratique engendré par $\sqrt{2}$. Nous allons montrer qu'il n'y a aucun sous-corps cubique. S'il existait un tel sous-corps $\mathbf{K}_3$ celui-ci serait égal à $\mathbf{R}(\beta_1, \beta_2)$ où

$$\beta_1 = \xi + \xi^{(i)}, \beta_2 = \xi\xi^{(i)},$$

$\xi^{(i)}$ étant un nombre conjugué de ξ; voir Nagell [4], p. 17–19. Vu que $\mathbf{R}(\xi)$ est réel, le nombre $\xi^{(i)}$ est aussi réel. Donc $\xi^{(i)} = \xi_1$. Il en résulterait

$$\beta_1 = \sqrt[3]{2+\sqrt{2}} + \sqrt[3]{2-\sqrt{2}} \text{ et } \beta_2 = \sqrt[3]{2}.$$

On aurait donc $\mathbf{K}_3 = \mathbf{R}(\beta_1, \beta_2) = \mathbf{R}(\beta_2) = \mathbf{R}(\beta_1\beta_2)$.

Ici le nombre $\beta_1\beta_2$ est racine de léquation

$$x^3 - 6x - 8 = 0,$$

dont le discriminant a la valeur $-2^5 \cdot 3^3$. D'autre part le discriminant de β_2 est égal á $-2^2 \cdot 3^3$. Vu que le quotient des discriminants n'est pas un carré, les corps $\mathbf{R}(\beta_2)$ et $\mathbf{R}(\beta_1\beta_2)$ sont différents. Ainsi il n'existe aucun sous-corps cubique.

Exemple 2. Désignons par β une racine de l'équation $x^3 - x^2 - 1 = 0$, et considérons le corps du sixième degré $\mathbf{R}(\xi)$ engendré par le nombre $\xi = \sqrt{\beta}$. Le sous-corps cubique $\mathbf{R}(\beta)$ n'est pas un corps de Galois. Vu que $r = 1$, il n'existe aucun sous-corps quadratique de $\mathbf{R}(\xi)$. Celui-ci n'est pas un corps de Galois. Ainsi nous avons un représentant de la classe 2.

Exemple 3. Considérons le corps du sixième degré $\mathbf{R}(\xi)$ engendré par le nombre $\xi = \sqrt{\beta}$, où β est une racine de l'équation cyclique du troisième degré $x^3 - 3x - 1 = 0$. Vu que $r = 1$, il n'y a aucun sous-corps quadratique de $\mathbf{R}(\xi)$. Celui-ci n'est pas un corps de Galois. Donc il appartient à la classe 3.

Exemple 4. Le corps du sixième degré engendré par le nombre $\xi = \sqrt{2} + \sqrt[3]{2}$ admet et un sous-corps quadratique et un (seul) sous-corps cubique. Comme $\mathbf{R}(\xi)$ n'est pas un corps de Galois, il appartient à la classe 4.

Exemple 5. Soit $\mathbf{R}(\xi)$ le corps cyclotome engendré par une septième racine primitive de l'unité. Ce corps est abélien et cyclique. Il est bien connu qu'il contient le sous-corps quadratique engendré par $\sqrt{-7}$ ainsi que le sous-corps cubique engendré par le nombre $2\cos\frac{2}{7}\pi$. Le corps $\mathbf{R}(\xi)$ appartient donc à la classe 5.

Un autre représentant de la même classe est donné par le corps cyclotome engendré par le nombre $\xi = 2\cos\frac{2}{13}\pi$. En effet, le corps $\mathbf{R}(\xi)$ contient les deux nombres $\sqrt{13}$ et $\cos\frac{2}{13}\pi + \cos\frac{10}{13}\pi$. On vérifie aisément que le dernier nombre est du troisième degré.

Exemple 6. Désignons par β une racine de l'équation $x^3+x^2-1=0$, dont le discriminant à la valeur -23. Alors le corps composé $\mathbf{R}(\beta, \sqrt{-23})$ est un corps de Galois qui n'est pas abélien. Il est évident qu'il appartient à la classe 6.

INDEX BIBLIOGRAPHIQUE

1. ABEL, N. H., Œuvres complètes, Oslo, 1881.
2. WEBER, H., Lehrbuch der Algebra, Berlin, 1896.
3. HECKE, E., Theorie der algebraischen Zahlen, Leipzig 1923.
4. NAGELL, T., Bemerkungen über zusammengesetzte Zahlkörper. Avhandl. Det Norske Videnskaps-Akademi, Oslo, Matem.-Naturv. Klasse. 1937, No. 4.
5. HILBERT, D., Die Theorie der algebraischen Zahlkörper. Jahresber. d. Deutschen Mathem.-Vereinigung, Bd. 4, 1898.
6. NAGELL, T., Sur quelques questions dans la théorie des corps biquadratiques. Arkiv för Matematik, Bd. 4, nr. 26, Stockholm, 1961.

Tryckt den 1 mars 1963

Uppsala 1963. Almqvist & Wiksells Boktryckeri AB