Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Odile Zink

Extensions cycliques de degré 2^n sur Q

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 8, n° 2 (1966-1967), exp. n° 16, p. 1-12

<http://www.numdam.org/item?id=SDPP_1966-1967__8_2_A7_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
8e année, 1966/67, n° 16

20 mars 1967

EXTENSIONS CYCLIQUES DE DEGRÉ 2^n SUR Q

par Odile ZINK

I. Etude des extensions quadratiques d'une extension cyclique de degré 2^n

1. Notations.

Soit k_n une extension cyclique de degré 2^n sur Q. Son groupe de Galois (σ) admet un sous-groupe unique d'ordre 2^p $(p = 0, 1, \dots, 2^n)$, et k_n admet une sous-extension unique k_p de degré 2^p.

L'extension k_n, supposée abélienne, est cyclique, si, et seulement si, elle contient un sous-corps quadratique unique.

L'extension k_n étant supposée cyclique, on cherche à quelle condition on peut en construire une extension quadratique $k_{n+1} = k_n(\sqrt{\alpha})$, avec α élément non carré de k_n, qui soit encore cyclique sur Q.

2. Condition pour que $k_{n+1} = k_n(\sqrt{\alpha})$ soit galoisienne sur Q.

Pour que k_{n+1} soit galoisienne, il faut et il suffit que les 2^n conjugués de α engendrent le même corps sur k_n, c'est-à-dire que $\sigma^i(\alpha).\sigma^j(\alpha)$ soit un carré dans k_n, $\forall\, i, j = 1, 2, \dots, 2^n$, ou encore que $\alpha.\sigma^k(\alpha)$ soit carré dans k_n, $\forall\, k = 1, 2, \dots, 2^n$, condition qui se réduit à

$$\alpha.\sigma(\alpha) = \beta^2, \qquad \text{avec } \beta \in k_n .$$

3. Condition pour que l'extension $k_{n+1} = k_n(\sqrt{\alpha})$ soit abélienne sur Q.

Supposons k_{n+1} galoisienne, et soient G et H les groupes de Galois, d'ordre 2^{n+1} et 2, de k_{n+1} par rapport à Q et k_n.

k_n étant une extension cyclique de a, H est un sous-groupe invariant de G, et G/H est cyclique.

Si $H = \{e, a\}$,

$$ab = ba, \qquad \forall\, b \in G .$$

$$G/H = \{B_1 , B_2 , \dots , B_{2^n} = \varepsilon\} ,$$

où B_i est de la forme $\{b_i , ab_i\}$.

Si B_1 est un générateur de G/H , $(B_1)^i = B_i$ ou $\{(b_1)^i , a(b_1)^i\} = \{b_i , ab_i\}$.

$\forall\, i$, b_i est égal à $(b_1)^i$ ou à $a(b_1)^i$, et dans les deux cas G est abélien.

Donc, pour que l'extension k_{n+1} soit abélienne, il faut et il suffit qu'elle soit galoisienne.

4. Condition pour que l'extension $k_{n+1} = k_n(\sqrt{\alpha})$, supposée galoisienne, soit cyclique sur Q .

Supposons que α soit de la forme $b\lambda^2$, avec $\lambda \in k_n$ et $b \in k_p$ $(0 \leqslant p < n)$, mais $\sqrt{b} \notin k_n$. Les deux sous-corps, de degré 2^{p+1} de k_{n+1} , k_{p+1} et $k_p(\sqrt{\alpha})$, sont distincts, et k_{n+1} n'est pas cyclique.

Supposons k_{n+1} non cyclique. Il admet deux sous-corps quadratiques distincts, k_1 et $Q(\sqrt{b})$, avec $b \in Q$ et $\sqrt{b} \notin k_n$. Les deux extensions k_{n+1} et $k_n(\sqrt{b})$ de même degré, dont l'une contient l'autre, sont égales, et $\sqrt{\alpha} = a_1 + a_2\sqrt{b}$, avec $a_1 , a_2 \in k_n$ et $a_2 \neq 0$. Alors $2a_1 a_2\sqrt{b} = \alpha - (a_1)^2 - (a_2)^2$, $b \in k_n$; et comme $\sqrt{b} \notin k_n$, $a_1 = 0$, d'où

$$\alpha = b\lambda^2 , \qquad \text{avec} \quad b \in Q \quad \text{et} \quad \lambda \in k_n .$$

Donc, pour que l'extension galoisienne $k_n(\sqrt{\alpha})$ soit cyclique, il faut et il suffit que α ne soit pas de la forme $b\lambda^2$.

Dans ce cas, $Q(\sqrt{\alpha})$, extension de Q contenue dans $k_n(\sqrt{\alpha})$, de même degré 2^{n+1} , lui est égale :

$$k_{n+1} = Q(\sqrt{\alpha}) .$$

5. Condition pour qu'il existe une extension $k_{n+1} = k_n(\sqrt{\alpha})$ cyclique sur Q .

D'après ce qui précède, il faut et il suffit qu'il existe un élément α de k_n , non carré dans k_n et non rationnel, tel que $\alpha.\sigma(\alpha)$ soit un carré β^2 dans k_n.

1° Supposons ces conditions vérifiées. $k_{n+1} = k_n(\sqrt{\alpha})$ est cyclique.

$$\alpha.\sigma(\alpha) = \beta^2 \qquad \text{entraîne} \qquad [N_{k_n/Q}(\alpha)]^2 = [N(\beta)]^2 \quad \text{où} \quad N(\tfrac{\alpha}{\beta}) = \pm 1 .$$

Si $N(\frac{\alpha}{\beta}) = +1$, d'après le théorème 90 de Hilbert, il existe un élément λ de

k_n , tel que $\frac{\alpha}{\beta} = \frac{\lambda}{\sigma(\lambda)}$.

$$\sigma\left(\frac{\alpha}{\lambda^2}\right) = \sigma(\alpha) \times \frac{\alpha^2}{\beta^2\,\lambda^2} = \frac{\alpha}{\lambda^2} , \qquad \text{donc} \quad \alpha = a\lambda^2 \quad \text{avec} \quad a \in Q , \ \sqrt{a} \notin k_n .$$

Alors $Q(\sqrt{a})$ et k_1 sont deux sous-corps quadratiques distincts de k_{n+1} , ce qui n'est pas possible.

Nécessairement $N(\frac{\alpha}{\beta}) = -1$, c'est-à-dire qu'il existe un nombre de k_n , de norme -1 , et le générateur α est solution de $\frac{\alpha}{\sigma(\alpha)} = \rho^2$, avec $N(\rho) = -1$.

2° Inversement, supposons qu'il existe un élément ρ de k_n , de norme -1 . $N(\rho^2) = +1$, et il existe un élément α de k_n , vérifiant $\frac{\alpha}{\sigma(\alpha)} = \rho^2$.

$\alpha.\sigma(\alpha) = \rho^2$. $\sigma(\alpha^2)$ est un carré dans k_n .

$\alpha \neq \sigma(\alpha)$, sinon ρ , égal à ± 1 , aurait pour norme $+1$, donc $\alpha \notin Q$.

α n'est pas un carré dans k_n , car si $\alpha = \alpha'^2$, $\rho = \pm \frac{\alpha'}{\sigma(\alpha')}$ aurait pour norme $+1$. Par conséquent, l'extension $k_{n+1} = k_n(\sqrt{\alpha})$ est cyclique sur Q . D'où le résultat :

THÉORÈME. - k_n étant une extension cyclique de degré 2^n sur Q , la condition nécessaire et suffisante pour qu'il existe une extension $k_n(\sqrt{\alpha}) = k_{n+1}$, qui soit encore cyclique sur Q , est que -1 soit norme d'un nombre dans k_n .

α est alors solution de $\frac{\alpha}{\sigma(\alpha)} = \rho^2$, avec $\rho \in k_n$ et $N(\rho) = -1$.

Remarques.

(a) Les résultats restent vrais en prenant pour corps de base un sur-corps de Q , et en particulier une des extensions intermédiaires k_p .

(b) Si $k_1 = Q(\sqrt{a})$ peut être prolongé par k_2 cyclique,

$$-1 = m^2 - an^2 , \qquad m , n \in a ,$$

donc a est positif, et k_1 réel.

On vérifie de la même façon, par récurrence, que pour pouvoir prolonger l'extension cyclique k_n par une extension $k_n(\sqrt{\alpha})$ cyclique, il est nécessaire que k_n soit réelle.

(c) La solution générale de $N(\rho) = -1$ est

$$\rho = \rho_0 \times \frac{\lambda}{\sigma(\lambda)} ,$$

où $\lambda \in k_n$, et où ρ_0 est une solution particulière.

La solution générale de $\frac{\alpha}{\sigma(\alpha)} = \rho_0^2 \times \frac{\lambda^2}{\sigma(\lambda^2)}$ est

$$\alpha = b\alpha_1 \ ,$$

où $b \in Q$, et où α_1 en est solution particulière. On peut prendre

$$\alpha_1 = \alpha_0 \lambda^2 \ , \qquad \text{avec } \frac{\alpha_0}{\sigma(\alpha_0)} = \rho_0^2 \ ,$$

par exemple

$$\alpha_0 = 1 + \rho_0^2 + \ldots + \rho_0^2 \sigma(\rho_0^2) \ldots \sigma^{2^n-1}(\rho_0^2) \ ,$$

d'où, en supprimant les facteurs carrés dans α , on obtient des générateurs de toutes les extensions k_{n+1} cycliques, de la forme $\alpha = b\alpha_0$, $b \in Z$, à partir d'un nombre particulier de norme -1 , sans avoir à les utiliser tous.

6. Exemple : Extensions biquadratiques cycliques.

$$Q \rightarrow k_1 = Q(\sqrt{a}) \rightarrow k_2 = k_1(\sqrt{\alpha}) \ ,$$

$a \in Z$, $\sqrt{a} \notin Z$, a sans facteur carré.

On peut construire une extension k_2 de k_1 cyclique sur a , si, et seulement si, -1 est norme dans k_2 . Alors, a peut être mis sous la forme $a = c^2 + d^2$, $c , d \in Z$, $(c , d) = 1$, et les facteurs premiers de a sont, soit 2 , soit de la forme $4k + 1$.

$$N\left(\frac{d + \sqrt{a}}{c}\right) = -1 \ , \qquad \rho_0 = \frac{d + \sqrt{a}}{c} \ , \qquad 1 + \rho_0^2 = \frac{2\sqrt{a}(d + \sqrt{a})}{c^2} \ .$$

On obtient donc toutes les extensions k_2 cycliques, avec $\alpha = \frac{2b\sqrt{a}(d + \sqrt{a})}{c^2}$, ou en supprimant les facteurs carrés,

$$\alpha = b(a + d\sqrt{a}) \ , \qquad b \in Z \ .$$

Remarques.

(a) Si on choisit $\rho_0' = \frac{c + \sqrt{a}}{d}$, on obtient

$$\alpha' = b'(a + c\sqrt{a}) \ ,$$

on vérifie que

$$Q(\sqrt{b(a + d\sqrt{a})}) = Q(\sqrt{2b(a + c\sqrt{a})}) \ ,$$

car $2b(a + c\sqrt{a}) \times b(a + d\sqrt{a}) = b^2[a + (c + d)\sqrt{a}]^2$ est un carré dans k_1 .

(b) La formule donnant α permet de construire toutes les extensions cycliques, mais pour avoir tous les générateurs, il faut prendre $\alpha = b\lambda^2(a + d\sqrt{a})$, $b \in Q$ et $\lambda \in Z[\sqrt{a}]$, qui est encore de la forme $B(A + D\sqrt{A})$ avec B rationnel, A entier rationnel positif non carré, $A - D^2$ carré entier rationnel. $\sqrt{\alpha}$ est alors racine de l'équation bicarrée :

$$\theta^4 - 2AB\theta^2 + AB^2 C^2 = 0 , \qquad A , C \in Z , \quad B \in Q .$$

Par comparaison, on vérifie que, pour que l'équation bicarrée

$$a_4 \theta^4 - a_2 \theta^2 + a_0 = 0 , \qquad a_0 , a_2 , a_4 \in Z , \quad a_4 \neq 0$$

soit abélienne cyclique, il faut et il suffit que $(a_2)^2 a_0 . a_4 . [(a_2)^2 - 4a_0 a_4]$ soit un carré non nul dans Z .

II. Construction d'une extension cyclique de degré 8 sur Q

k_2 étant biquadratique cyclique sur Q , pour construire k_3 cyclique, nous allons introduire le corps $Q(\varepsilon)$ des racines 8e de l'unité. Les conditions nécessaires et suffisantes qui seront obtenues pour la possibilité de la construction fourniront des conditions pour que -1 soit norme dans k_2 .

Nous supposerons $a \neq 2$.

1. Le corps $Q(\varepsilon)$.

$\varepsilon = e^{i\pi/4}$ est racine primitive 8e de 1 . Le corps $Q(\varepsilon)$ principal contient trois sous-corps quadratiques, $Q(i)$, $Q(\sqrt{2})$, $Q(i\sqrt{2})$. Son groupe de Galois est produit direct de deux groupes d'ordre 2 , (s) et (s') .

	s	s'	s ∘ s'
1	1	1	1
ε	ε^3	$-\varepsilon$	$-\varepsilon^3$
i	$-i$	i	$-i$
ε^3	ε	$-\varepsilon^3$	$-\varepsilon$

s conserve $Q(i\sqrt{2})$,
s' conserve $Q(i)$,
s ∘ s' conserve $Q(\sqrt{2})$.

Nous utiliserons les propriétés suivantes :

(a) Tout nombre rationnel a , norme à la fois dans deux des sous-corps quadratiques de $Q(\varepsilon)$, est le produit d'un carré rationnel par une norme de $Q(\varepsilon)$.

Supposons a norme dans $Q(i)$ et $Q(i\sqrt{2})$:

$$a = b\, s(b) , \qquad b \in Q(i) \qquad b = s'(b) ,$$

$$a = c\, s'(c) , \qquad c \in Q(i\sqrt{2}) , \qquad c = s(c) .$$

Le système

$$\begin{cases} b = r\xi\, s'(\xi) , & r \in Q , \\ c = r\xi\, s(\xi) , & \xi \in Q(\varepsilon) , \end{cases}$$

équivalent à

$$\begin{cases} \dfrac{b}{c} = \dfrac{s'(\xi)}{s(\xi)} , \\ b = r\xi\, s'(\xi) , \end{cases}$$

admet des solutions, par exemple

$$\xi = 1 + \frac{b}{s'(c)} \qquad \text{et} \qquad r = \frac{a}{b + s(b) + c + s'(c)} ;$$

alors,

$$a = r^2\, N(\xi) .$$

Un tel nombre a , entier, est, à un facteur carré près, produit de nombres de la forme $8k + 1$, et de 2 éventuellement.

(b) Un nombre ρ de $Q(\varepsilon)$, tel que $\rho\, s(\rho)$ soit rationnel, est le produit d'un nombre de $Q(i)$ et d'un nombre de $Q(\sqrt{2})$.

Si $b = \rho\, s(\rho)$ est rationnel,

$$s'(\rho).ss'(\rho) = \rho\, s(\rho) ,$$

et $\dfrac{\rho}{s'(\rho)}$, invariant par ss' , appartient à $Q(\sqrt{2})$. Alors, puisque

$$\frac{\rho}{s'(\rho)} . s'\left(\frac{\rho}{s'(\rho)}\right) = 1 ,$$

il existe un élément μ_1 de $Q(\sqrt{2})$ tel que

$$\frac{\rho}{s'(\rho)} = \frac{\mu_1}{s'(\mu_1)} ,$$

et $\dfrac{\rho}{\mu_1}$, invariant par s' , appartient à $Q(i)$.

On a évidemment des résultats analogues avec les deux autres transformations s' et ss' .

2. Conditions de possibilité de construction de k_3 cyclique.

$$Q \xrightarrow[\alpha]{} k_1 = Q(\sqrt{a}) \xrightarrow[\beta]{} k_2 = k_1(\sqrt{\alpha}) \longrightarrow k_3 = k_2(\sqrt{\beta}) \ ;$$

k_2 , cyclique sur Q , est engendré par $\sqrt{\alpha}$ avec

$$\alpha = b(a + d\sqrt{a}) \ ,$$

$b \in Z$ sans facteur carré, et $a \in Z$ $(a = c^2 + d^2)$ sans facteur carré.

Comment faut-il choisir a et b pour qu'il existe une extension $k_3 = k_2(\sqrt{\beta})$ qui soit cyclique sur Q ?

(a) Conditions nécessaires. - Supposons k_3 cyclique, engendré par $\theta = \sqrt{\beta}$, avec $\beta \in k_2$, et soit σ un générateur de son groupe de Galois d'ordre 8 .

$$\sigma(\sqrt{a}) = -\sqrt{a} \ , \qquad \sigma(\sqrt{\alpha}) = \sqrt{b}(a - d\sqrt{a}) \ , \qquad \sigma^4(\beta) = \beta \ ,$$
$$\sigma^2(\sqrt{a}) = \sqrt{a} \ , \qquad \sigma^2(\sqrt{\alpha}) = -\sqrt{\alpha} \ , \qquad \sigma^4(\theta) = -\theta \ .$$

Considérons les résolvantes de Lagrange :

$$m = \theta + \varepsilon\,\sigma(\theta) + i\,\sigma^2(\theta) + \varepsilon^3\,\sigma^3(\theta) \ ,$$
$$s(m) = n = \theta + \varepsilon^3\,\sigma(\theta) - i\,\sigma^2(\theta) + \varepsilon\,\sigma^3(\theta) \ ,$$
$$s'(m) = p = \theta - \varepsilon\,\sigma(\theta) + i\,\sigma^2(\theta) - \varepsilon^3\,\sigma^3(\theta) \ ,$$
$$ss'(m) = q = \theta - \varepsilon^3\,\sigma(\theta) - i\,\sigma^2(\theta) - \varepsilon\,\sigma^3(\theta) \ ,$$

$m \neq \pm p$, dont le comportement par les différents opérateurs est résumé dans le tableau suivant :

	σ	σ^2	σ^3	σ^4	σ^5	σ^6	σ^7	s	s'	ss'
m	$-\varepsilon^3 m$	$-im$	$-\varepsilon m$	$-m$	$\varepsilon^3 m$	im	εm	n	p	q
n	$-\varepsilon n$	in	$-\varepsilon^3 n$	$-n$	εn	$-in$	$\varepsilon^3 n$	m	q	p
p	$\varepsilon^3 p$	$-ip$	εp	$-p$	$-\varepsilon^3 p$	ip	$-\varepsilon p$	q	m	n
q	εq	iq	$\varepsilon^3 q$	$-q$	$-\varepsilon q$	$-iq$	$-\varepsilon^3 q$	p	n	m

.

m^2 , n^2 , p^2 , q^2 , invariants par σ^4 , appartiennent à $k_2(\varepsilon)$; et

$$\rho = \frac{m^2}{\sqrt{\alpha} + i\ \sigma(\sqrt{\alpha})} \ ,$$

invariant par σ , appartient à $Q(\varepsilon)$, mais non à $Q(i)$.

$$m^2 = \rho[\sqrt{\alpha} + i\ \sigma(\sqrt{\alpha})] \ ,$$

$$n^2 = s(\rho)[\sqrt{\alpha} - i\ \sigma(\sqrt{\alpha})] \ ,$$

$$p^2 = s'(\rho)[\sqrt{\alpha} + i\ \sigma(\sqrt{\alpha})] \ ,$$

$$q^2 = ss'(\rho)[\sqrt{\alpha} - i\ \sigma(\sqrt{\alpha})] \ .$$

$\frac{mn}{\sqrt{a}}$, invariant par σ et s , appartient à $Q(i\sqrt{2})$. Or,

$$m^2\, n^2 = \rho\, s(\rho)[\alpha + \sigma(\alpha)] = 2ab\rho\ s(\rho) \ ,$$

et, en comptant le facteur $2 = (1 + i)(1 - i)$ dans $\rho\ s(\rho)$, il reste

$$b = \rho'\ s(\rho') \ , \qquad \text{avec} \quad \rho' = \frac{u' + i\sqrt{2}\ v'}{\rho} \quad \text{et} \quad \rho \in Q(\varepsilon) \ .$$

mq , invariant par σ et ss' , appartient à $Q(\sqrt{2})$. Or $m^2\, q^2 = 2ab\rho\ ss'(\rho)$ et, comme précédemment,

$$ab = \rho''\ ss'(\rho'') \ , \qquad \text{avec} \quad \rho'' = \frac{u'' + \sqrt{2}\ v''}{\rho} \ .$$

Donc, pour qu'il soit possible de construire k_3 cyclique, il est nécessaire que le système :

$$(1) \quad \begin{cases} b = \rho'\ s(\rho') \ , & \rho\rho' = u' + i\sqrt{2}\ v' \ , \\ ab = \rho''\ ss'(\rho'') \ , & \rho\rho'' = u'' + \sqrt{2}\ v'' \ , \end{cases}$$

admette des solutions $\rho \in Q(\varepsilon)$ et $\rho \notin Q(i)$, u' , v' , u'' , $v'' \in Q$, le nombre a étant lui-même norme dans $Q(i)$: $a = \lambda\ s(\lambda)$, $\lambda \in Q(i)$, k_3 est alors engendré par $\theta = \frac{1}{4}(m + n + p + q)$.

Montrons que les conditions (1) sont équivalentes à :

$$(2) \quad \begin{cases} a = N(\xi) \ , & \xi \in Q(\varepsilon) \ , \\ b = \eta\ s(\eta) \ , & \eta \in Q(i) \ . \end{cases}$$

(1) $\Longrightarrow$ (2) . - D'après 1-(b),

$$\rho' = \mu' \cdot \mu_1' \ , \qquad \text{avec} \quad \mu' \in Q(i) \quad \text{et} \quad \mu_1' \in Q(\sqrt{2}) \ ,$$

$$\rho'' = \mu'' \cdot \mu_1'' \ , \qquad \text{avec} \quad \mu'' \in Q(i) \quad \text{et} \quad \mu_1'' \in Q(i\sqrt{2}) \ ,$$

en groupant dans μ' et μ'' les facteurs rationnels de ρ' et ρ'' .

$$b^2 a = \mu' \, s(\mu') \, \mu'' \, ss'(\mu'') \, \mu_1' \, s(\mu_1') \, \mu_1'' \, ss'(\mu_1'')$$

est norme dans $Q(i)$.

Donc $\mu_1' \, s(\mu_1')$ et $\mu_1'' \, ss'(\mu_1'')$, déjà normes respectivement dans $Q(\sqrt{2})$ et $Q(i\sqrt{2})$, sont normes dans $Q(i)$, et par conséquent normes dans $Q(\varepsilon)$ (1 - (a)) :

$$\mu_1' = \nu' \, ss'(\nu') \quad \text{et} \quad \rho' = \mu' \nu' \, ss'(\nu') \ , \qquad \text{avec} \quad \mu' \in Q(i) \quad \text{et} \quad \nu' \in Q(\varepsilon) \ ,$$

$$\mu_1'' = \nu'' \, s(\nu'') \quad \text{et} \quad \rho'' = \mu'' \nu'' \, s(\nu'') \ , \qquad \text{avec} \quad \mu'' \in Q(i) \quad \text{et} \quad \nu'' \in Q(\varepsilon) \ .$$

Enfin,

$$\frac{\rho'}{\rho''} = \frac{u' + i\sqrt{2}\, v'}{u'' + \sqrt{2}\, v''} \ ,$$

c'est-à-dire que l'élément $\mu = \dfrac{\mu'}{\mu''}$ de $Q(i)$ est produit d'un élément de $Q(i\sqrt{2})$ et d'un élément de $Q(\sqrt{2})$. μ est nécessairement de la forme r ou ir , avec $r \in Q$. Dans les deux cas,

$$\mu' \, s(\mu') = r^2 \, \mu'' \, s(\mu'') \ ,$$

$$ab^2 = r^2 \, \mu''^2 \, s(\mu''^2) \, N(\nu'\nu'') \ ,$$

$$b = r^2 \, \mu'' \, s(\mu'') \, N(\nu') \quad \text{norme dans} \quad Q(i) \ ,$$

$a = \dfrac{1}{r^2} \times N\left(\dfrac{\nu''}{\nu'}\right)$ et, puisque a a été choisi sans facteurs carrés, a est norme dans $Q(\varepsilon)$.

(2) $\Longrightarrow$ (1) . - Supposons

$$\begin{cases} a = N(\xi) \ , & \xi \in Q(\varepsilon) \ , \\ b = \eta \, s(\eta) \ , & \eta \in Q(i) \ . \end{cases}$$

Alors,

$$a = \lambda \, s(\lambda) \ , \qquad \text{avec} \quad \lambda = \xi \, s'(\xi) \in Q(i) \ ,$$

$$b = \rho' \, s(\rho') \ , \qquad \text{avec} \quad \rho' = \eta \ ,$$

$$ab = \rho'' \, ss'(\rho'') \ , \qquad \text{avec} \quad \rho'' = \xi \, s(\xi) \, \eta \ ,$$

$$\rho' = \frac{e}{\xi \, s(\xi)} \frac{1}{\rho} \quad \text{et} \quad \rho'' = e \, \frac{1}{\rho} \ , \qquad \text{avec} \quad \rho = \frac{e}{\eta\xi \, s(\xi)} \in Q(\varepsilon) \quad \text{et} \quad e \in Q \ ,$$

$\rho \notin Q(i)$, sinon a serait un carré.

(b) Conditions suffisantes. - Supposons k_2 cyclique, de groupe de Galois (σ) , d'ordre 4 , et les conditions équivalentes (1) et (2) vérifiées.

ρ étant un élément de $Q(\varepsilon)$, mais non de $Q(i)$, défini par (1), les quatre nombres :

$$m^2 = [\sqrt{\alpha} + i\,\sigma(\sqrt{\alpha})]\,\rho \ ,$$
$$n^2 = [\sqrt{\alpha} + i\,\sigma(\sqrt{\alpha})]\,s(\rho) = s(m^2) \ ,$$
$$p^2 = [\sqrt{\alpha} + i\,\sigma(\sqrt{\alpha})]\,s'(\rho) = s'(m^2) \ ,$$
$$q^2 = [\sqrt{\alpha} - i\,\sigma(\sqrt{\alpha})]\,ss'(\rho) = ss'(m^2) \ ,$$

sont quatre éléments, non carrés, deux à deux différents, de $k_2(\varepsilon)$, conjugués par rapport à $Q(\varepsilon)$. Chacun engendre $k_2(\varepsilon)$ sur Q , car ses seize conjugués sont différents $(\pm m^2 , \pm n^2 , \pm p^2 , \pm q^2 , \pm im^2$, etc.) .

D'après (1), $m^2 n^2 = a(u' + i\sqrt{2}\,v')^2$ et $m^2 q^2 = (u'' + \sqrt{2}\,v'')^2$ sont des carrés dans $k_2(\varepsilon)$, donc aussi $n^2 q^2$ et $m^2 p^2 = s(n^2 q^2)$, et les racines de m^2 , n^2 , p^2 , q^2 engendrent une même extension quadratique K de $k_2(\varepsilon)$, de degré 32 sur Q .

Puisque $\sigma(m^2) = - im^2$, $s(m^2) = n^2$, $s'(m^2) = p^2$, et $ss'(m^2) = q^2$, les éléments $\pm \varepsilon^3 m$, $\pm n$, $\pm p$, $\pm q$, de K , sont des conjugués de m par rapport aux sous-corps k_2 , $Q(i\sqrt{2})$, $Q(\sqrt{2})$ et $Q(i)$. Choisissons des racines m , n , p , de m^2 , n^2 , p^2 ; appelons encore σ , s , s' les Q-automorphismes de K tels que $\sigma(m) = - \varepsilon^3 m$, $s(m) = n$, $s'(m) = p$; et choisissons pour q la racine de q^2 telle que $s'(m) = q$. Alors,

$$\sigma^2(m) = - im \ , \quad \sigma^3(m) = - \varepsilon m \ , \quad \ldots \ , \quad \sigma^8(m) = m \ ,$$

$s^2(m) = m$ et $(ss')^2(m) = m$ (car $s(mn) = mn$ et $ss'(mq) = mq$) .

Les transformés de n , p , q par σ , s , s' sont parfaitement déterminés, et on retrouve le tableau du § 1 du II.

On a ainsi obtenu, pour m , trente-deux conjugués tous différents, et K est une extension normale sur Q , admettant m pour élément primitif. Elle est abélienne puisque σ , s et s' commutent, et son groupe de Galois sur Q est $(\sigma)_8 \times (s)_2 \times (s')_2$. Le sous-corps k_3 de K des invariants par les transformations s et s' , est alors abélien cyclique d'ordre 8 sur Q . On peut l'engendrer par les quatre nombres non nuls, tous différents, de k_3 (car invariants par

s et s'), dont les carrés sont des éléments conjugués de k_2 :

$$\begin{cases} 4\theta_1 = m + n + p + q \ , \\ 4\theta_2 = -\varepsilon^3 m - \varepsilon n + \varepsilon^3 p + \varepsilon q \ , \\ 4\theta_3 = -im + in - ip + iq \ , \\ 4\theta_4 = -\varepsilon m - \varepsilon^3 n + \varepsilon p + \varepsilon^3 q \ , \end{cases}$$

$$\sigma(\theta_1) = \theta_2 \ , \quad \sigma(\theta_2) = \theta_3 \ , \quad \sigma(\theta_3) = \theta_4 \ , \quad \sigma(\theta_4) = -\theta_2 \ , \quad \dots \ .$$

En résumé, pour qu'on puisse construire $k_3 = k_2(\sqrt{\beta})$ cyclique sur Q , c'est-à-dire pour que -1 soit norme dans k_2 , il faut et il suffit que a soit norme d'un nombre de $Q(\varepsilon)$, et b norme d'un nombre de $Q(i)$.

3. Détermination d'un générateur de k_3 dans le cas $a = \gamma^4 + \delta^4$.

$$a = N(\gamma + \varepsilon\delta) \ ,$$

$$b = \eta \, s(\eta) \ , \qquad \eta \in Q(i) \ ,$$

$$\rho = \frac{e}{\eta(\gamma^2 - \delta^2 + i\sqrt{2}\,\gamma\delta)} \ , \qquad e \in Q \ .$$

Le calcul de $\theta^2 = (m + n + p + q)^2$ conduit à

$$\theta^2 = \frac{e(\gamma^2 - \delta^2 + \sqrt{a})}{ab} \left[b\sqrt{a} + \sqrt{\alpha}(s(\eta) + \eta) + i\,\sigma(\sqrt{\alpha})(s(\eta) - \eta) \right] ,$$

avec $e \in Q$ sans facteur carré,

$$\alpha = \sqrt{b}(a + \delta^2\sqrt{a}) \ ,$$

ce qui permet de construire toutes les extensions k_3 cycliques en faisant varier e .

Exemple.

$$a = 17 = N(2 + \varepsilon) \ ,$$

$$b = 1 \ , \quad \eta = 1 \ ,$$

$$\theta^2 = e\,\frac{(3 + \sqrt{17})}{17}\left[\sqrt{17} + 2\sqrt{17 + \sqrt{17}}\right] .$$

BIBLIOGRAPHIE

Pour toute la première partie, voir le § 6 du chapitre IX de :

ALBERT (A. Adrian). - Modern higher algebra. - Chicago, University of Chicago Press, 1948 (The University of Chicago Science Series).