Mohamed Zitouni

Quelques propriétés des corps cycliques de degré 4

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 14, nº 1 (1972-1973), exp. nº 4, p. 1-8

<http://www.numdam.org/item?id=SDPP_1972-1973__14_1_A3_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
14e année, 1972/73, n° 4, 8 p.

30 octobre 1972

QUELQUES PROPRIÉTÉS DES CORPS CYCLIQUES DE DEGRÉ 4

par Mohamed ZITOUNI

0. Introduction.

Cette étude s'inspire largement de "l'Arithmétique des corps abéliens de degré 3" de A. CHÂTELET [1]. En particulier, nous avons suivi le même plan, employé de façon systématique les résolvantes de Lagrange, et adopté certaines définitions.

1. Groupe de Galois et résolvantes de Lagrange.

(a) Nous dirons corps cyclique de degré 4 pour désigner une extension cyclique de $\mathbb{Q}$ de degré 4 .

Soient K un corps cyclique de degré 4 , G son groupe de Galois, et θ_1 un générateur de K . Ce nombre θ_1 admet 4 conjugués θ_u par un $\mathbb{Q}$-automorphisme σ , générateur de G :

$$\sigma^h(\theta_u) = \theta_{u+h} \ , \quad h \ , \ u \ \text{ et } \ u + h \ \text{ entiers rationnels } \ \text{mod } 4 \ .$$

(b) Les résolvantes de θ_1 , définies par les formules :

$$\langle \theta_1 \ , \ z \rangle = \sum_{x=0}^{3} z^x . \sigma^x(\theta_1) \ , \quad z \ \text{ racine 4-ième de } \ 1 \ ,$$

sont :

$$\langle \theta_1 \ , \ 1 \rangle = \theta_1 + \theta_2 + \theta_3 + \theta_4 \ ;$$

$$\langle \theta_1 \ , \ - 1 \rangle = \theta_1 - \theta_2 + \theta_3 - \theta_4 \ ;$$

$$\langle \theta_1 \ , \ i \rangle = \theta_1 + i\theta_2 - \theta_3 - i\theta_4$$

et

$$\langle \theta_1 \ , \ - i \rangle = \theta_1 - i\theta_2 - \theta_3 + i\theta_4 \ .$$

Posons $\langle \theta_1 , 1 \rangle = m$, $\langle \theta_1 , - 1 \rangle = \alpha$, $\langle \theta_1 , i \rangle = \beta$ et $\langle \theta_1 , - i \rangle = \beta'$.

(c) Les résolvantes β et β' sont dans le corps $K(i)$ qui est une extension de $\mathbb{Q}$ de degré 4 ou 8 selon que i est dans K , ou non. Mais on démontre que i n'est pas dans K . Alors $K(i)$ est un corps abélien de degré 8 . On prolonge σ à $K(i)$, et on introduit le K-automorphisme τ de $K(i)$ qui change i en $- i$.

2. Propriétés des résolvantes.

(a) Caractérisons les corps $\mathbb{Q}$, $\mathbb{Q}(i)$ et K au moyen de σ et τ .

---

[1] CHÂTELET (Albert). - Arithmétique des corps abéliens du 3e degré, Annales scient. Ec. Norm. Sup., t. 63, 1946, p. 109-160.

$$x \in \mathbb{Q} \leftrightarrow \sigma(x) = \tau(x) = x \,.$$
$$x \in \mathbb{Q}(i) \leftrightarrow \sigma(x) = x \quad \text{et} \quad \tau(x) \neq x \,.$$
$$x \in K \leftrightarrow \sigma(x) \neq x \quad \text{et} \quad \tau(x) = x \,.$$

(b) Ces équivalences permettent de trouver les nombres de $\mathbb{Q}$ et ceux de $\mathbb{Q}(i)$ parmi les résolvantes et leurs combinaisons.

$\sigma(m) = \tau(m) = m$; donc m est rationnel ; c'est la trace de θ_1 .
$\sigma(\alpha) = -\alpha$ et $\tau(\alpha) = \alpha$; donc $\alpha \notin \mathbb{Q}(i)$.
$\sigma(\beta) = -i\beta$ et $\tau(\beta) = \beta'$; donc $\beta \notin \mathbb{Q}(i)$.
$\sigma(\beta') = +i\beta'$ et $\tau(\beta') = \beta$; donc $\beta' \notin \mathbb{Q}(i)$.

(c) Nous cherchons les combinaisons donnant des nombres rationnels.

$$\sigma(\alpha^2) = \tau(\alpha^2) = \alpha^2 \;;$$
$$\sigma(\beta\beta') = \tau(\beta\beta') = \beta\beta' \;;$$
$$\sigma(\beta^4 + \beta'^4) = \tau(\beta^4 + \beta'^4) = \beta^4 + \beta'^4 \;;$$
$$\sigma(\alpha/(\beta^2 + \beta'^2)) = \tau(\alpha/(\beta^2 + \beta'^2)) = \alpha/(\beta^2 + \beta'^2) \,.$$

Donc les nombres α^2 , $\beta\beta'$, $\beta^4 + \beta'^4$ et $\alpha/(\beta^2 + \beta'^2)$ sont rationnels.

(d) Nous cherchons les combinaisons donnant des nombres de $\mathbb{Q}(i) - \mathbb{Q}$.

$$\sigma(\beta^4) = \beta^4 \quad \text{et} \quad \tau(\beta^4) = \beta'^4 \;;$$
$$\sigma(\beta^3/\beta') = \beta^3/\beta' \quad \text{et} \quad \tau(\beta^3/\beta') = \beta'^3/\beta \,.$$

Donc β^4 et β'^4 sont conjugués dans $\mathbb{Q}(i)$, ainsi que β^3/β' et β'^3/β .

(e) Les nombres β , β^2 , β^3 , β' , β'^2 , β'^3 , $\beta^2 \pm \beta'^2$, β/β' , β'/β ne sont pas dans $\mathbb{Q}(i)$.

3. Puissance 4-ième $\langle\theta_1 , i\rangle^4$ de la résolvante β .

(a) Le nombre β^3/β' est dans $\mathbb{Q}(i)$; (§2 (d)). Posons $\beta^3 = \lambda\beta'$, et appliquons le K-automorphisme τ . On obtient :

$$\beta^8 = \lambda^3.\tau(\lambda) \,.$$

Mais $\beta^8 = (\beta^4)^2$ est le carré d'un nombre de $\mathbb{Q}(i)$, et $\mathbb{Q}(i)$ est principal. Tout facteur premier de λ , rationnel, ou dans $\mathbb{Q}(i)$, figure à une puissance paire dans $\lambda^3.\tau(\lambda)$. On trouve $\lambda^3.\tau(\lambda) = \varepsilon^2\, r'^4(s' + it')^6\,(s' - it')^2$ et

$$\beta^4 = \pm\, \varepsilon\, r'^2(s' + it')^3\,(s' - it') \,, \quad r' , s' \text{ et } t' \text{ rationnels} .$$

En remarquant que ε est une unité de $\mathbb{Q}(i)$ et que i se met sous la forme $i = (\frac{1}{2})^2\,(1 + i)^3\,(1 - i)$, nous prenons β^4 sous la forme

$$\beta^4 = r^2(s + it)^3\,(s - it) \,, \quad r , s , t \text{ rationnels.}$$

Alors $\beta'^4 = r^2(s - it)^3\,(s + it)$, et

$$\lambda = r(s + it)^2 \,.$$

Or $\beta^2 = \pm\, r(s+it)\sqrt{s^2+t^2}$ n'est pas dans $\underset{\sim}{Q}(i)$; ce qui entraîne la propriété " s^2+t^2 non carré dans $\underset{\sim}{Q}$ ".

(b) Valeurs de $\beta\beta'$, $\beta^2 \pm \beta'^2$ et $\beta \pm \beta'$.

De l'identité $(\beta\beta')^4 = \beta^4\,\beta'^4$, on déduit :

$$\beta\beta' = \pm\, r(s^2+t^2) .$$

Des identités $(\beta^2 \pm \beta'^2)^2 = \beta^4 + \beta'^4 \pm 2\,\beta^2\beta'^2$, on déduit :

$$\beta^2 + \beta'^2 = \pm\, 2rs\sqrt{s^2+t^2} \quad \text{et} \quad \beta^2 - \beta'^2 = \pm\, 2irt\sqrt{s^2+t^2} .$$

Des identités $(\beta \pm \beta')^2 = \beta^2 + \beta'^2 \pm 2\beta\beta'$, on déduit :

$$\beta + \beta' = \pm\sqrt{2r(s^2+t^2 \pm s\sqrt{s^2+t^2}\,)}$$

et

$$\beta - \beta' = \pm\, i\sqrt{2r(s^2+t^2 \pm s\sqrt{s^2+t^2})} .$$

4. Les 2 formes de l'élément primitif θ_1 .

(a) θ_1 et ses conjugués permettent de calculer les résultantes de θ_1 .

Réciproquement les résolvantes de θ_1 permettent de calculer les θ_u ; on a :

$$4\theta_1 = m + \alpha + \beta + \beta' \; ; \quad 4\theta_2 = m - \alpha - i\beta + i\beta' \; ;$$

$$4\theta_3 = m + \alpha - \beta - \beta' \quad \text{et} \quad 4\theta_4 = m - \alpha + i\beta - i\beta' .$$

(b) Grâce au §2 (c), nous calculons la résolvante α :

$$\alpha = \pm\, 2a'rs\sqrt{s^2+t^2} , \quad a' \text{ rationnel} .$$

(c) La somme $\beta + \beta'$, dans $4\theta_1$, se calcule soit avec §3(a) ou §3(b).

Avec $\beta = \sqrt[4]{\beta^4}$, nous obtenons la première forme de θ_1 et de ses conjugués :

$$4\theta_1 = m \pm 2a'rs\sqrt{s^2+t^2} + \varepsilon\,\sqrt[4]{r^2(s+it)^3(s-it)} + \tau(\varepsilon)\,\sqrt[4]{r^2(s-it)^3(s+it)} .$$

Les 4 conjugués de θ_1 s'obtiennent en prenant le signe de α et la valeur de l'unité ε conformes aux formules (§4(a)) ; soit $\varepsilon = \pm 1$ pour $+\alpha$ et $\varepsilon = \pm i$ pour $-\alpha$.

Avec $\beta + \beta' = \pm\sqrt{2r(s^2+t^2 \pm s\sqrt{s^2+t^2})}$, nous obtenons la deuxième forme de θ_1 et de ses conjugués :

$$4\theta_1 = m \pm 2a'rs\sqrt{s^2+t^2} \pm \sqrt{2r(s^2+t^2 \pm s\sqrt{s^2+t^2})} .$$

Les quatre conjugués de θ_1 s'obtiennent en prenant les signes de $s\sqrt{s^2+t^2}$ et du grand radical. L'équivalence des 2 formes de θ_1 se vérifie par le calcul.

(d) Il faut s'assurer que K est effectivement un corps cyclique de degré 4 . La propriété " s^2+t^2 non carré dans $\underset{\sim}{Q}$ " entraîne que $\underset{\sim}{Q}(\sqrt{s^2+t^2})$ est un sous-corps quadratique de K .

Or les nombres $\beta + \beta'$ ne sont pas dans le sous-corps à la seule condition " s^2+t^2 non carré dans $\underset{\sim}{Q}$ ". Donc K est un corps cyclique de degré 4 .

(e) Soient a et b deux entiers rationnels premiers entre eux, c un entier sans facteur carré, et a'' et r' deux rationnels tels que :

$$s = a''a \ , \quad t = a''b \ , \quad a^2 + b^2 = p \quad \text{et} \quad 2r = r'^2 c \ .$$

Alors $\beta + \beta' = \pm\, r'a'' \sqrt{c(p \pm a\sqrt{p})}$.

Posons $\varphi_1 = \sqrt{c(p + a\sqrt{p})}$ et $\varphi_2 = \sqrt{c(p - a\sqrt{p})}$.

Nous obtenons la forme $\theta_1 = m_1 + m_2\sqrt{p} + m_3\,\varphi_1$, m_u rationnels, $\beta = 2m_3(\varphi_1 + i\varphi_2)$ et $\beta' = 2m_3(\varphi_1 - i\varphi_2)$.

5. Propriétés de φ_1 et φ_2 .

(a) Les relations $b\varphi_2 = \varphi_1(\sqrt{p} - a)$, $\varphi_1^2 = c(p + a\sqrt{p})$ et $\varphi_2^2 = c(p - a\sqrt{p})$ montrent l'égalité $\mathbb{Q}(\varphi_1) = \mathbb{Q}(\varphi_2)$.

Avec $\theta_1 = m_1 + m_2\sqrt{p} + m_3\,\varphi_1$ et $\varphi_1 = \frac{1}{m_3}(\theta_1 - m_1 - m_2\sqrt{p})$, $m_3 \neq 0$, nous obtenons l'égalité $\mathbb{Q}(\varphi_1) = K$.

Donc φ_1 et φ_2 sont éléments primitifs de K .

(b) Les transformés de $\sqrt{p}$, φ_1 et φ_2 par σ proviennent des transformés des résolvantes de θ_1 et des relations liant $\sqrt{p}$, φ_1 et φ_2 à ces résolvantes.
Ainsi " $\alpha = m_2\sqrt{p}$ et $\sigma(\alpha) = -\alpha$ " donne " $\sigma(\sqrt{p}) = -\sqrt{p}$ ".
" $m_3 \neq 0$, $\varphi_1 = \frac{1}{m_3}(\beta + \beta')$, $\varphi_2 = \frac{i}{m_3}(\beta - \beta')$, $\sigma(\beta) = -i\beta$ et $\sigma(\beta') = i\beta'$ " donne " $\sigma(\varphi_1) = \varphi_2$ et $\sigma(\varphi_2) = -\varphi_1$ ".

D'où les résolvantes de φ_1 :

$$\langle\varphi_1 \ , \ 1\rangle = \langle\varphi_1 \ , \ -1\rangle = 0 \ ;$$

$$\langle\varphi_1 \ , \ i\rangle = 2(\varphi_1 + i\varphi_2) \ ;$$

$$\langle\varphi_1 \ , \ -i\rangle = 2(\varphi_1 \ , \ -i\varphi_2) \ .$$

Réciproquement, ces résolvantes déterminent de façon unique φ_1 et φ_2 . De plus, nous avons :

$$\langle\varphi_1 \ , \ i\rangle^2 = 8c(a + ib)\sqrt{p} \ , \ \text{et} \ \ \langle\varphi_1 \ , \ i\rangle^4 = 64c^2(a + ib)^3(a - ib) \ .$$

(c) Ainsi, tout nombre x de K peut se mettre sous forme de polynôme en φ_1 , à coefficients rationnels, de façon unique :

$$x \in K : \ x = d_0 + d_1\,\varphi_1 + d_2\,\varphi_1^2 + \ldots + d_n\,\varphi_1^n \ , \quad d_u \in \mathbb{Q} \ .$$

En remplaçant les puissances de φ_1 par leurs valeurs, nous obtenons la forme équivalente :

$$x = m_1 + m_2\sqrt{p} + m_3\,\varphi_1 + m_4\,\varphi_2 \ , \quad m_u \in \mathbb{Q} \ .$$

(d) Réciproquement, soient trois entiers rationnels a , b et c , et trois rationnels m_1 , m_2 et $m_3 \neq 0$, c sans facteur carré, a et b premiers entre eux; $p = a^2 + b^2$ non carré. Les nombres $\sqrt{p}$, φ_1 , φ_2 et $\theta_1 = m_1 + m_2\sqrt{p} + m_3\,\varphi_1$ ne sont pas rationnels. θ_1 vérifie une équation à une inconnue du 4e degré, à coefficients rationnels :

$$X^4 - 4m_1X^3 + 2(3m_1^2 - pm_2^2 - cpm_3^2)X^2 - 4X(m_1^3 - pm_1\, m_2^2 - cpm_1\, m_3^2 + acpm_2\, m_3^2) + (m_1^2 + pm_2^2 - cpm_3^2)^2 - p(2m_1\, m_2 - acm_3^2)^2 = 0 .$$

Les autres racines sont $\theta_2 = m_1 - m_2\sqrt{p} + m_3\,\varphi_2$, $\theta_3 = m_1 + m_2\sqrt{p} - m_3\,\varphi_1$ et $\theta_4 = m_1 - m_2\sqrt{p} - m_3\,\varphi_2$. Il existe un automorphisme de $\mathbb{Q}(\theta_1)$ qui permute ces quatre racines, et par suite, engendre un groupe cyclique d'ordre 4 . Il en résulte l'égalité des corps conjugués $\mathbb{Q}(\theta_u)$.

Les nombres $\sqrt{p}$, φ_1 et φ_2 sont des combinaisons linéaires des θ_u ; d'où l'égalité :

$$\mathbb{Q}(\varphi_1) = \mathbb{Q}(\theta_1) .$$

Nous avons obtenu un premier résultat :

PROPOSITION 1. - Toute extension cyclique K de $\mathbb{Q}$ de degré 4 est caractérisée par les propriétés suivantes :

(a) K ne contient pas i ;

(b) K possède un élément primitif $\varphi_1 = \sqrt{c(p + a\sqrt{p})}$, c entier sans facteur carré, $p = a^2 + b^2$ non carré, a et b entiers premiers entre eux ;

(c) un générateur du groupe de Galois de K transforme $\sqrt{p}$ en $-\sqrt{p}$, φ_1 en φ_2 et φ_2 en $-\varphi_1$;

(d) la résolvante $\langle\varphi_1 , i\rangle$, son carré et son cube ne sont pas dans $\mathbb{Q}(i)$; $\langle\varphi_1 , i\rangle^4 = 64c^2(a + ib)^3(a - ib)$ est un nombre de $\mathbb{Q}(i)$, non puissance 4-ième exacte.

6. Corps cycliques égaux.

Pour reconnaître deux corps cycliques K et K' égaux, nous comparons un élément primitif , θ_1 , de K à un autre, θ'_1 , de K' ; si θ'_1 est fonction rationnelle de θ_1 et de ses conjugués, alors $K = K'$. Sinon nous disposons de la proposition suivante :

PROPOSITION 2. - Soient K et K' deux corps cycliques de degré 4 , d'éléments primitifs respectifs $\varphi_1 = \sqrt{c(p + a\sqrt{p})}$ et $\varphi'_1 = \sqrt{c'(p' + a'\sqrt{p'})}$. Les propriétés suivantes sont équivalentes :

(i) les corps K et K' sont égaux ;

(ii) l'un des nombres $\langle\varphi'_1 , i\rangle/\langle\varphi_1 , \pm i\rangle$, rapports des résolvantes de φ'_1 et de φ_1 , est dans $\mathbb{Q}(i)$.

La preuve de (i) entraîne (ii). - Soit $K = K'$; alors K et K' ont même sous-corps quadratique $\mathbb{Q}(\sqrt{p'}) = \mathbb{Q}(\sqrt{p})$, soit $p' = pm^2$, m rationnel. Notons σ le générateur du groupe de Galois de K tel que $\sigma(\varphi_1) = \varphi_2$ et $\sigma(\varphi_2) = -\varphi_1$; alors

$$\sigma(\langle\varphi_1 , i\rangle) = - i\langle\varphi_1 , i\rangle \quad \text{et} \quad \sigma(\langle\varphi_1 , - i\rangle) = i\langle\varphi_1 , - i\rangle .$$

Or φ'_1 , générateur de K' , est un nombre de K ; donc σ agit sur φ'_1 ; $\sigma(\varphi'_1) = \pm \varphi'_2$, ce qui entraîne :

$$\sigma(\langle\varphi'_1 , i\rangle) = \begin{cases} - i\langle\varphi'_1 , i\rangle & \text{si } \sigma(\varphi'_1) = \varphi'_2 , \\ + i\langle\varphi'_1 , i\rangle & \text{si } \sigma(\varphi'_1) = - \varphi'_2 . \end{cases}$$

L'un des rapports $\langle\varphi'_1 , i\rangle/\langle\varphi_1 , \pm i\rangle$ est invariant par σ , tandis que l'autre est transformé en son opposé. Mais, d'après §2(a), le nombre invariant par σ est dans $\underset{\sim}{Q}(i)$.

<u>La preuve de</u> (ii) <u>entraîne</u> (i). - Soient K et K' tels que

$$\langle\varphi'_1 , i\rangle = (x + iy)\langle\varphi_1 , i\rangle , \quad x + iy \in \underset{\sim}{Q}(i) .$$

Cette relation s'écrit :

$$\varphi'_1 + i\varphi'_2 = (x\varphi_1 - y\varphi_2) + i(x\varphi_2 + y\varphi_1) .$$

Sa conjuguée par τ est :

$$\varphi'_1 - i\varphi'_2 = (x\varphi_1 - y\varphi_2) - i(x\varphi_2 + y\varphi_1) .$$

D'où $\varphi'_1 = x\varphi_1 - y\varphi_2$ et $\varphi'_2 = x\varphi_2 + y\varphi_1$, soit l'inclusion $K' \subset K$.

Avec $x + iy \neq 0$, nous calculons φ_1 et φ_2 :

$$\varphi_1 = \frac{1}{x^2 + y^2}(x\varphi'_1 + y\varphi'_2) \quad \text{et} \quad \varphi_2 = \frac{1}{x^2 + y^2}(x\varphi'_2 - y\varphi'_1) ,$$

soit l'inclusion $K \subset K'$. Par suite, nous obtenons l'égalité $K = K'$.

Remarquons que les nombres $\varphi_1 = \sqrt{c(p + a\sqrt{p})}$ et $\varphi'_1 = \sqrt{c(p + b\sqrt{p})}$, dont les rapports $\langle\varphi'_1 , i\rangle/\langle\varphi_1 , \pm i\rangle$ ne sont pas dans $\underset{\sim}{Q}(i)$, engendrent deux corps cycliques de degré 4 différents.

<u>Exemple</u> : $\varphi_1 = \sqrt{3(61 + 5\sqrt{61})}$, $\varphi'_1 = \sqrt{6(61 + 6\sqrt{61})}$ et $\varphi''_1 = \sqrt{15(1525 + 9\sqrt{1525})}$ engendrent le même corps cyclique de degré 4 .

7. Forme réduite de φ_1 .

Le critère d'égalité de deux corps cycliques de degré 4 montre qu'il existe des éléments primitifs de formes distinctes ; on définit parmi elles une privilégiée, dite de forme réduite, dont les éléments a , b , c et p vérifient la proposition suivante :

PROPOSITION 3. - <u>Dans tout corps cyclique de degré</u> 4 , <u>il existe un couple unique d'éléments primitifs</u> $\varphi_1 = \sqrt{c(p + a\sqrt{p})}$ <u>et</u> $\varphi_2 = \sqrt{c(p - a\sqrt{p})}$, <u>où</u> a , b <u>et</u> c <u>sont des entiers rationnels</u>, a <u>et</u> b <u>premiers entre eux</u>, $a^2 + b^2 = p$ <u>sans facteur carré</u>, c <u>impair sans facteur carré et premier à</u> p .

<u>Les résolvantes</u> $\langle\varphi_1 , \pm 1\rangle$ <u>sont nulles</u>.

<u>Les résolvantes</u> $\langle\varphi_1 , \pm i\rangle$, <u>leurs carrés et leurs cubes ne sont pas dans</u> $\underset{\sim}{Q}(i)$.

Leurs puissances 4-ièmes sont des nombres de $\underset{\sim}{Q}(i)$, non puissances 4-ièmes exactes.

Preuve de a , b et c entiers rationnels. - Soit $\varphi_1' = \sqrt{c'(p' + a'\sqrt{p'})}$ un générateur de K .

Soit d le plus petit dénominateur commun à c' , b' et a' ; alors $a' = a/d$, $b' = b/d$ et $c' = c''/d$, avec a , b , c'' et d entiers rationnels.

On a $\varphi_1' = \frac{1}{d^2}\sqrt{c''d(p + a\sqrt{p})}$. Les nombres φ_1' et $\varphi_1 = \sqrt{c(p + a\sqrt{p})}$, $c = c''d$, ayant un quotient rationnel, engendrent le même corps K .

Preuve de $p = a^2 + b^2$ sans facteur carré. - Soit $\varphi_1' = \sqrt{c'(p' + a'\sqrt{p'})}$ avec $p' = (a^2 + b^2)(m^2 + n^2)^2 = (a' + ib')(a' - ib')$ (Le cas $p' = m^2(a^2 + b^2)$ entraîne $\varphi_1' = m\sqrt{c'(p + a\sqrt{p})}$, $p = a^2 + b^2$).

La puissance 4-ième de la résolvante $\langle\varphi_1' , i\rangle$ est :

$\langle\varphi_1' , i\rangle^4 = 64c'^2(a' + ib')^3(a' - ib') = 64c'^2(m^2 + n^2)^2(a + ib)^3(a - ib)(m + in)^4.$

D'après la proposition 2, nous pouvons remplacer φ_1' par φ_1 tel que

$$\langle\varphi_1' , i\rangle/\langle\varphi_1 , i\rangle \in \underset{\sim}{Q}(i) ,$$

ce qui permet d'éliminer les facteurs à la puissance 4 dans $\langle\varphi_1' , i\rangle^4$. On en déduit $\langle\varphi_1 , i\rangle^4 = 64c^2(a + ib)^3 (a - ib)$, en posant $c'(m^2 + n^2) = c$ et $\varphi_1 = \sqrt{c(p + a\sqrt{p})}$.

Preuve de c entier impair et sans facteur carré. - Soit φ_1' avec a' , b' , c' entiers et p' sans facteur carré.

(a) Quand c' a un facteur carré, $c' = cd^2$, alors

$$\varphi_1' = d\sqrt{c(p' + a'\sqrt{p'})} = d\varphi_1 ;$$

nous pouvons remplacer φ_1' par φ_1 , puisque leur quotient est rationnel.

(b) Quand c' est pair, $c' = 2c$, la puissance 4-ième de la résolvante $\langle\varphi_1' , i\rangle$ est :

$$\langle\varphi_1' , i\rangle^4 = 64(4c^2)(a' + ib')^3 (a' - ib') .$$

Mais $-4 = (1 \pm i)^4$ est puissance 4-ième dans $\underset{\sim}{Q}(i)$. Par suite :

$$\langle\varphi_1' , i\rangle^4 = 64c^2 i^2(a' + ib')^3 (a' - ib')(1 \pm i)^4 .$$

Pour faire apparaître la forme convenable de la puissance 4-ième de $\langle\varphi_1 , i\rangle$, nous écrivons $i^2(a' + ib')^3 (a' - ib')$ sous la forme équivalente.

$$(b' - ia')^3 (b' + ia') ,$$

et nous obtenons $\varphi_1 = \sqrt{c(p' + b'\sqrt{p'})}$, où c est impair et sans facteur carré.

Preuve de c et p premiers entre eux. - Soit $\varphi_1' = \sqrt{c'(p' + a'\sqrt{p'})}$, avec c' impair et sans facteur carré, p' sans facteur carré mais ayant un facteur commun avec c' . Alors

$$p' = a'^2 + b'^2 = (a''^2 + b''^2)(m^2 + n^2) \quad \text{et} \quad c' = c(m^2 + n^2) \ .$$

Exprimons la puissance 4-ième de la résolvante $\langle \varphi'_1 , i \rangle$:

$$\langle \varphi'_1 , i \rangle^4 = 64c^2(a'' + ib'')^3 (a'' - ib'')(m + in)^5 (m - in)^3 \ .$$

Éliminons le facteur $(m + in)^4$ qui est à la puissance 4 :

$$\langle \varphi_1 , i \rangle^4 = 64c^2[(a'' + ib'')(m - in)]^3 [(a'' - ib'')(m + in)] \ .$$

Posons $a''m + b''n = a$, $b''m - a''n = b$ et $a^2 + b^2 = p$; nous obtenons :

$$\varphi_1 = \sqrt{c(p + a\sqrt{p})} \ , \quad p = p' \ ,$$

qui est sous forme réduite.

<u>Preuve de l'unicité du couple</u> φ_1 , φ_2 . - Nous l'obtenons à l'aide de la proposition 2 .

<u>Valeur des résolvantes</u> $\langle \varphi_1 , \pm 1 \rangle$ <u>et</u> $\langle \varphi_1 , \pm i \rangle$. - Le calcul donne :

$$\langle \varphi_1 , \pm 1 \rangle = 0 \ .$$

Avec l'automorphisme σ de $K(i)$, nous obtenons : $\sigma(\langle \varphi_1 , i \rangle) = - i \langle \varphi_1 , i \rangle$, ce qui indique que les résolvantes $\langle \varphi_1 , \pm i \rangle$, leurs carrés et leurs cubes ne sont pas dans $\underset{\sim}{Q}(i)$ et que $\langle \varphi_1 , \pm i \rangle^4$ sont dans $\underset{\sim}{Q}(i)$.

Nous avons, plus précisément :

$$\langle \varphi_1 , i \rangle^4 = 64c^2(a + ib)^3 (a - ib) \ .$$

(Texte reçu le 30 octobre 1972)

Mohamed ZITOUNI
Université de Besançon
Mathématiques
La Bouloie. Route de Gray
25030 BESANCON CEDEX