Cette quantité est nulle car $X^p - \xi^{p^{r-i+1}}$ est le polynome minimal de $\xi^{p^{r-i}}$ sur $\Omega\left(\frac{n_r}{p^{r-i+1}}\right)$.

Remarque III.3.B

$$Tr_{K_{l-1}/Q}(\theta_{l-1}) = (-1)^{m_r+1}$$

Il suffit d'appliquer le lemme III.1 à $\Omega\left(\frac{n_r}{p^{r-l+1}}\right)$ ou $\Omega\left(\frac{n_r}{2^{r-l+2}}\right)$, suivant les cas.

Remarque III.3.C

Dans le cas où $p = 2$ et $u_r \geqq 3$, on a:

$$\sum_{s \in S_r} \xi^{s2^{r-l+1}} = 0$$

En effet:

$$\sum_{s \in S_r} \xi^{s2^{r-l+1}} = Tr_{\Omega\left(\frac{n_r}{2^{r-l+1}}\right)/K_{l-1}}\left(\xi^{2^{r-l+1}}\right)$$

et d'autre part

$$K_{l-1} \subseteq \Omega\left(\frac{n_r}{2^{r-l+3}}\right)$$

et

$$Tr_{\Omega\left(\frac{n_r}{2^{r-l+1}}\right)/\Omega\left(\frac{n_r}{2^{r-l+3}}\right)}\left(\xi^{2^{r-l+1}}\right) = 0$$

car $X^2 - \xi^{2^{r-l+2}}$ est le polynome minimal de $\xi^{2^{r-l+1}}$ sur $\Omega\left(\frac{n_r}{2^{r-l+3}}\right)$.

III.5. Exemple

Soit B la base introduite à la proposition III.3. On se propose de chercher les polynomes caractéristiques des θ_i. Pour cela, il faut pouvoir calculer les coordonnées, par rapport à B, des produits mutuels d'éléments de B.

Les θ_i sont des périodes de Gauss ([7] chapitre 7). On pose pour tout entier a: $\eta(a) = \sum_{s \in S_r} \xi^{as}$.

On a en particulier:

$$\theta_i = \eta(p^{r-i}) \quad \text{pour} \quad l \leqq i \leqq r$$

et suivant les cas:

$$\theta_{l-1} = \eta(p^{r-l+1}) \quad \text{ou} \quad \tfrac{1}{2}\eta(2^{r-l+2}).$$

Pour tout b appartenant à $G(n_r)$, le transformé de $\eta(a)$ par b est $\eta(ab)$. En particulier les conjugués de θ_i, pour $l \leqq i \leqq r$, seront:

$$\sigma^k(\theta_i) = \eta(g^k p^{r-i}).$$

Le produit de deux périodes $\eta(a)$ et $\eta(a')$ est donné par: $\eta(a)\eta(a') = \sum_{s \in S_r} \eta(a+a's)$. Appliquant cette formule à deux éléments de B, on est alors ramené au problème suivant: donner les coordonnées de $\eta(a)$, a entier quelconque, dans la base B.

c et c' désignent dans ce qui suit, des nombres premiers avec p.

1. Dans le cas p impair ou $p = 2$ et $u_r = 2$, $\eta(p^u c)$, avec $u \geqq r - l + 2$, peut s'exprimer comme somme de périodes de la forme $\eta(p^{r-l+1}c')$. Il suffit d'écrire l'égalité:

$$\sum_{0<k<p} \xi^{\frac{n_r}{p}k} = -1;$$

multipliant alors cette égalité par $\xi^{p^u c}$ on obtient:

$$\sum_{0<k<p} \eta\left(\frac{n_r}{p}k + p^u c\right) = -\eta(p^u c).$$

Les quantités $\frac{n_r}{p}k + p^u c$ sont de la forme $p^{r-l+1}c'$.

Dans le cas où $p = 2$ et $u_r \geqq 3$, $\eta(2^u c)$, avec $u \geqq r - l + 3$, est l'opposé d'une période $\eta(2^{r-l+2}c')$.

2. $\eta(p^u c)$, avec $u \leqq r - l + 1$ (ou $u \leqq r - l + 2$, suivant les cas) peut s'exprimer comme somme de périodes de la forme $\eta(p^u c')$, c' appartenant à $G(n_r)$, en procédant de la même façon qu'au lemme III.2. C'est-à-dire: si v désigne le $PGCD$ de c et de n_r, et m_v le nombre de diviseurs premiers de v, on a:

$$\sum_{\substack{0<k<v \\ PGCD(k,v)=1}} \xi^{\frac{n_r}{v}k} = (-1)^{m_v}$$

d'où:

$$(-1)^{mv}\,\eta\,(p^u c) \;=\; \sum_{\substack{0<k<v\\ PGCD(k,v)=1}} \eta\left(\frac{n_r}{v}k + p^u c\right)$$

Les quantités $\frac{n_r}{v}k + p^u c$ sont de la forme $p^u c'$, avec c' premier avec n_r.

Cas particulier :

Si $K_r \cap \Omega\left(\frac{n_r}{v}\right) \subset K_r \cap \Omega\left(\frac{n_r}{p^u}\right)$ et $u \leqq r - l$, alors $\eta\,(p^u c) = 0$.

En effet on a: $$PGCD\left(\frac{n_r}{p^u}, \frac{n_r}{v}\right) = \frac{n_r}{p^u v}.$$

D'où $K_r \cap \Omega\left(\frac{n_r}{v}\right) \subset \Omega\left(\frac{n_r}{p^u v}\right)$. En employant la même méthode que dans la démonstration de la proposition III.3, $\eta\,(p^u c)$ est égal, à un coefficient près, à:

$$Tr_{\Omega\left(\frac{n_r}{p^u v}\right)/K_r \cap \Omega\left(\frac{n_r}{v}\right)}\left(\xi^{p^u c}\right)$$

Comme $K_r \cap \Omega\left(\frac{n_r}{p^u}\right) \supset K_r \cap \Omega\left(\frac{n_r}{v}\right)$ et comme $u \leqq r - l$, on aura donc:

$$K_r \cap \Omega\left(\frac{n_r}{p^{u+1}}\right) \supseteq K_r \cap \Omega\left(\frac{n_r}{v}\right).$$

$\Omega\left(\frac{n_r}{p^{u+1} v}\right)$ sera donc compris entre $K_r \cap \Omega\left(\frac{n_r}{v}\right)$ et $\Omega\left(\frac{n_r}{p^u v}\right)$ et l'on a

$$Tr_{\Omega\left(\frac{n_r}{p^u v}\right)/\Omega\left(\frac{n_r}{p^{u+1} v}\right)}\left(\xi^{p^u c}\right) = 0$$

3. $\eta\,(p^u c)$, avec $u \leqq r - l + 1$ (ou $u \leqq r - l + 2$ suivant le cas) et c premier avec n_r, est un conjugué de $\eta\,(p^u) = \theta_{r-u}$ (à moins qu'il ne soit nul; remarque III.3.C).
S'il n'est pas dans B, alors ses conjugués sur K_{r-u-1}, seront dans B et il suffit alors d'utiliser la remarque III.3.A.

Considérons par exemple, la suite de corps cyclotomiques vérifiant les conditions I.2.A *bis* et I.2.B *bis*: $\Omega(17)$, $\Omega(8.17)$, $\Omega(16.17)$.
On a donc $r = 3$; $l = 2$; $m_1 = m_2 = m_3 = 1$; $p_1 = 17$.
Il y a quatre extensions K_3, cycliques de degré 8 sur Q associées à cette suite (proposition I.5 *bis*).
Elles ont pour discriminant sur Q: $2^{22}\,17^7$ (proposition II.3).
$T(16.17, 17)$ a pour éléments 1, 35, 69, 103, 137, 171, 205, 239.
$a_0 = 239$ et l'on peut choisir comme générateur de $T(16.17, 4.17)$:

$a_0' = 69$.

On cherche de même les éléments de $T(16.17, 16)$ et un générateur c_1 de ce sous-groupe. On peut prendre par exemple $c_1 = 65$. Les puissances successives de c_1 sont données par le tableau suivant:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
65	145	177	81	97	49	193	33	241	161	129	225	209	257	113

S_3 est engendré par $\{ c_1^8, c_1^{\alpha_0} a_0, c_1^{\alpha_0'} a_0' \}$, α_0 et α_0' vérifiant les conditions $\alpha_0 \equiv 0\ (4)$; $\alpha_0' \equiv 0\ (2)$ et $\alpha_0' \not\equiv 0\ (4)$ (proposition I.4 *bis*). Les éléments de S_3 sont de la forme:

$$s = c_1^{8\beta_1 + \alpha_0\beta_0 + \alpha_0'\beta_0'}\, a_0^{\beta_0}\, a_0'^{\beta_0'}$$

avec $\beta_0 = 0$ ou 1; $\beta_0' = 0, 1, 2$ ou 3; $\beta_1 = 0$ ou 1.

Prenons par exemple: $\alpha_0 = 4$ et $\alpha_0' = 2$.

Le tableau suivant donne les valeurs de s, en fonction de β_0, β_0', β_1. On trouve donc à la dernière ligne les éléments de S_3:

β_0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
β_0'	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
β_1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
s	1	213	217	253	33	229	89	189	47	219	135	195	191	155	103	179

On remarque que $3^4 = 81$ n'appartient pas à S_3, c'est-à-dire que la classe de 3 modulo S_3 est un générateur de $\dfrac{G(16.17)}{S_3}$.

On prendra donc $g = 3$. Les classes de $G\,(16.17)$ mod. S_3 sont données dans le tableau suivant:

S_3	1	213	217	253	33	229	89	189	47	219	135	195	191	155	103	179
$3S_3$	3	95	107	215	99	143	267	23	141	113	133	41	29	193	37	265
3^2S_3	9	13	49	101	25	157	257	69	151	67	127	123	87	35	111	251
3^3S_3	27	39	147	31	75	199	227	207	181	201	109	97	261	105	61	209
3^4S_5	81	117	169	93	225	53	137	77	271	59	55	19	239	43	183	83
3^5S_3	243	79	235	7	131	159	139	231	269	177	165	57	173	129	5	249
3^6S_3	185	237	161	21	121	205	145	149	263	259	223	171	247	115	15	203
3^7S_3	11	167	211	63	91	71	163	175	245	233	125	241	197	73	45	65

$B = \{\,\eta\,(1), \eta\,(3), \eta\,(3^2), \eta\,(3^3), \eta\,(2), \eta\,(2.3), \tfrac{1}{2}\,\eta\,(8), \tfrac{1}{2}\,\eta\,(8.3)\,\}$ est une base de l'anneau des entiers de K_3. On cherche le polynome minimal de $\eta\,(1)$ sur K_2. Le conjugué de $\eta\,(1)$ sur K_2 est $\eta\,(3^4)$ et d'après la remarque III.3.A, $\eta\,(1) + \eta\,(3^4) = 0$.

D'autre part: $\eta\,(1)^2 = \sum_{s \in S_3} \eta\,(1+s)$.

Il reste à exprimer chacun des $\eta\,(1+s)$ en fonction de: $\eta\,(2)$, $\eta\,(2.3)$, $\eta\,(8)$, et $\eta\,(8.3)$.

Par exemple: pour $s = 213$: $\eta\,(1+213) = \eta\,(2.107) = \eta\,(2.3)$ car $107 \in 3\,S_3$.

Pour $s = 33$: $\eta\,(1+33) = \eta\,(2.17) = 0$ car $\Omega\,(16) \cap K_3 = Q \subset K_2 = \Omega\,(8.17) \cap K_3$.

Pour $s = 47$, on écrit $\xi^{8.17} = -1$ d'où $\xi^{8.17+48} = -\xi^{48}$ c'est-à-dire: $\eta\,(1+47) = -\eta\,(8.23) = -\eta\,(8.3)$.

Pour $s = 195$: $\eta\,(1+195) = \eta\,(4.49) = 0$ compte tenu de la remarque III.3.C.

Finalement on obtient: $\eta\,(1)^2 = -16 - \eta\,(2) - 2\eta\,(8.3) + \eta\,(8)$. Le polynome minimal de $\eta\,(1)$ sur K_2 est donc:

$$X^2 + 16 + \eta\,(2) + 2\eta\,(3.8) - \eta\,(8)$$

On calcule de la même façon le polynome minimal de η (2) sur K_1: $X^2 - \eta(8) - 16$ et celui de η (8) sur Q: $X^2 - 2X - 16$.

Les 8 nombres:

$$\frac{1+\sqrt{17}}{2}, \frac{1-\sqrt{17}}{2}, \sqrt{17+\sqrt{17}}, \sqrt{17-\sqrt{17}},$$

$$\sqrt{-17+3\sqrt{17}-\sqrt{17+\sqrt{17}}}, \sqrt{-17-3\sqrt{17}-\sqrt{17-\sqrt{17}}}$$

$$\sqrt{-17+3\sqrt{17}+\sqrt{17+\sqrt{17}}} \text{ et } \sqrt{-17-3\sqrt{17}+\sqrt{17-\sqrt{17}}}$$

forment une base de l'anneau des entiers de K_3.

Pour les autres valeurs de α_0 et α_0' le résultat est le suivant: les polynomes minimaux de η (8) et η (2) restent les mêmes que précédemment. Pour obtenir une base des entiers des autres extensions K_3 admettant la même suite de corps cyclotomiques associée: Ω (17), Ω (8.17), Ω (16.17), il suffit d'ajouter aux quatre nombres:

$$\frac{1+\sqrt{17}}{2}, \frac{1-\sqrt{17}}{2}, \sqrt{17+\sqrt{17}}, \sqrt{17-\sqrt{17}},$$

les quatre autres quantités:

Pour le corps K_3 correspondant à $\alpha_0 = 4$ et $\alpha_0' = 6$:

$$\sqrt{-17+3\sqrt{17}+3\sqrt{17+\sqrt{17}}-4\sqrt{17-\sqrt{17}}},$$

$$\sqrt{-17-3\sqrt{17}+3\sqrt{17-\sqrt{17}}+4\sqrt{17+\sqrt{17}}},$$

$$\sqrt{-17+3\sqrt{17}-3\sqrt{17+\sqrt{17}}+4\sqrt{17-\sqrt{17}}},$$

$$\sqrt{-17-3\sqrt{17}-3\sqrt{17-\sqrt{17}}-4\sqrt{17+\sqrt{17}}},$$

Pour le corps K_3 correspondant à $\alpha_0 = 8$ et $\alpha_0' = 2$:

$$\sqrt{17+3\sqrt{17}+\sqrt{17-\sqrt{17}}}, \sqrt{17-3\sqrt{17}-\sqrt{17+\sqrt{17}}}$$

$$\sqrt{17+3\sqrt{17}-\sqrt{17-\sqrt{17}}}, \sqrt{17-3\sqrt{17}+\sqrt{17+\sqrt{17}}}$$

Pour le corps K_3 correspondant à $\alpha_0 = 8$ et $\alpha_0' = 6$:

$$\sqrt{17 - 3\sqrt{17} + 3\sqrt{17 + \sqrt{17}} - 4\sqrt{17 - \sqrt{17}}},$$

$$\sqrt{17 + 3\sqrt{17} + 3\sqrt{17 - \sqrt{17}} + 4\sqrt{17 + \sqrt{17}}},$$

$$\sqrt{17 - 3\sqrt{17} - 3\sqrt{17 + \sqrt{17}} + 4\sqrt{17 - \sqrt{17}}},$$

$$\sqrt{17 + 3\sqrt{17} - 3\sqrt{17 - \sqrt{17}} - 4\sqrt{17 + \sqrt{17}}}.$$

BIBLIOGRAPHIE

[1] Samuel, P. Théorie algébrique des nombres (Hermann).
[2] Mac Carthy, P. J. Algebraic extensions of fields (Blaisdell Publishing Company).
[3] Herbrand, J. Développement moderne de la théorie des corps algébriques. *Mémorial des Sciences Mathématiques* (fasc. LXXV, 1936).
[4] Chevalley, C. Théorie du corps de classes dans les corps finis et les corps locaux. *Journ. of the Faculty of Sciences*, Tokyo 1933, 365.
[5] Lang, S. Algebraic Numbers (Addison-Wesley Publishing Company).
[6] —— Algebra (Addison-Wesley Publishing Company).
[7] Van der Waerden, B. L. Modern Algebra, vol. I (F. Ungar Publishing Company).

(Reçu le 26 octobre 1971)

Bernard Oriat
Faculté des sciences
Route de Gray
F-25 — Besançon