CREATIVE MATH. & INF.
16 (2007), 63 - 69

Dedicated to Professor Ioan A. RUS on the occasion of his 70^{th} anniversary

Artin symbol of the Kummer fields

DIANA SAVIN

ABSTRACT. Let l and p be odd prime distinct natural numbers, ξ be a primitive root of order l of unity. It is known that the field extension $\mathbf{Q}(\xi) \subset \mathbf{Q}(\xi, \sqrt[l]{p})$ is a Galois extension.
In this article we study the Artin symbol in the Galois group $G\left(\mathbf{Q}(\xi, \sqrt[l]{p})/\mathbf{Q}(\xi)\right)$.

1. INTRODUCTION

First, we recall some results we are using here:

Theorem 1.1. ([3]). *Let $n \in \boldsymbol{N}$, $n \geq 2$ and $\boldsymbol{Q} \subset \boldsymbol{K}$ be an extension of fields of degree $[\boldsymbol{K} : \boldsymbol{Q}] = n$, p be a prime natural number. There exist positive integers e_i, $i = \overline{1, g}$ such that*

$$p\mathbf{Z}_K = \prod_{i=1}^{g} P_i^{e_i},$$

where all P_i, $i = \overline{1, g}$, are prime ideals above p and $\mathbf{Z}_K$ is the ring of integers of $\boldsymbol{K}$ over $\boldsymbol{Q}$.

Definition 1.1. ([3]). The integer e_i is called the ramification index of p at P_i. The degree f_i of the field extension defined by

$$f_i = [\mathbf{Z}_K/P_i : \mathbf{Z}/p\mathbf{Z}]$$

is called the **residual degree of** p.

Theorem 1.2. ([3]). *We have the following formulas:*

$$N(P_i) = p^{f_i},$$

and

$$\sum_{i=1}^{g} e_i f_i = n = [\boldsymbol{K} : \boldsymbol{Q}].$$

In the case when $\mathbf{K}/\mathbf{Q}$ is a Galois extension, the result is more specific:

Theorem 1.3. ([3]). *Assume that $\boldsymbol{K}/\boldsymbol{Q}$ is a Galois extension. Then, for all P_i, the ramification indices e_i are equal (say to e), the residual degrees f_i are equal as well (say to f) and $efg = n$.*

Received: 20.09.2006. In revised form: 19.02.2007.
2000 *Mathematics Subject Classification.* 11R18.
Key words and phrases. *Kummer fields, cyclotomic fields.*

Proposition 1.1. ([5]). *Let L/K be a Galois extension and $\mathbf{Z}_K$, $\mathbf{Z}_l$ be the rings of algebraic integers of the fields K and L.Let $P \in Spec(\mathbf{Z}_K)$ such that the extension K⊂L is unramified in P. Let $P^{'}$ be a prime ideal in the ring $\mathbf{Z}_L$ such that $P^{'}/P\mathbf{Z}_L$. Then there exists a unique automorphism $\sigma \in G(L/K)$ such that:*

$$\sigma(x) \equiv x^{N(P)}(modP^{'}).$$

Definition 1.2. ([1]). The element σ of the Proposition 1.1. is denoted $\left(\frac{L/K}{P'}\right)$.
If the extension K⊂L is Abelian, then $\left(\frac{L/K}{P'}\right)$ does not depend on $P^{'} \in Spec(\mathbf{Z}_L)$, but only on $P = P^{'} \cap \mathbf{Z}_K$ and it is denoted $\left(\frac{L/K}{P}\right)$

Definition 1.3. ([1]). Let K⊂L be a Galois extension of fields, and let $P^{'}$ be a maximal ideal in the ring $\mathbf{Z}_L$. The set

$$Z_{P'} = \left\{\tau \in G(L/K)/\tau(P^{'}) = P^{'}\right\}$$

is a subgroup in $G(L/K)$ and it is called **the group of decomposition of** $P^{'}$ in the extension $K \subset L$.

Theorem 1.4. ([1]). *Let K⊂L be a Galois extension of fields, and let P be a maximal ideal in the ring $\mathbf{Z}_K$.*
i) For any $P^{'} \in Max_P(\mathbf{Z}_L)$ we have $[G(L/K) : Z_{P'}] = g_P$, where g_P is the number of prime ideals from$\mathbf{Z}_L$ which divide P.

ii) If K⊂L is a unramified in P and Abelian extension of fields and $\mathbf{Z}_K/P$ is a finite field, then $\left(\frac{L/K}{P'}\right)$ generate the group $Z_{P'}$ and $|Z_{P'}| = f_{P'}$

Proposition 1.2. ([6]). *Let l be a prime natural number $l \geq 3$ and ξ be a primitive root of unity of l- th order. A prime natural number $p \geq 3$ is a prime in the ring $Z[\xi]$ if and only if $\overline{p}$ is generating the group $(\mathbf{Z}_l^*, \cdot)$*

Let l be a odd prime natural number and ξ be a primitive root of unity of order l. $Z[\xi]$ is the ring of integers of the cyclotomic field $\mathbf{Q}(\xi)$.
Let p be a prime natural number, $p \neq l$, and P be a prime ideal in the ring $Z[\xi]$, P dividing the ideal generated by p, (p), in the ring $Z[\xi]$.

Proposition 1.3. ([3]). *Let $\alpha \in Z[\xi]$, $\alpha \notin P$. There is an integer c, unique modulo l, such that $\alpha^{\frac{N(P)-1}{l}} \equiv \xi^c$ (modP).*

Definition 1.4. ([3]). The root of unity ξ^c is called the **power-character of the number** α with respect to the prime ideal P in the ring $Z[\xi]$. Following Hilbert([3]), we denote ξ^c by $\left\{\frac{\alpha}{P}\right\}$.

Proposition 1.4. ([3]). *If $\alpha, \beta \in Z[\xi]$, (α), (β) are not divisible with P, then:*

$$\left\{\frac{\alpha\beta}{P}\right\} = \left\{\frac{\alpha}{P}\right\} \cdot \left\{\frac{\beta}{P}\right\}.$$

Definition 1.5. ([3]). Let $\alpha \in Z[\xi]$. If the congruence $x^l \equiv \alpha \pmod{P}$ has solutions in the ring $Z[\xi]$, we say that α **is a power-residue of order** l with respect to the prime ideal P.

Proposition 1.5. ([5]). *Let P be a prime ideal in the ring $Z[\xi]$, $P \neq (1-\xi)$, $\alpha \in Z[\xi]$, α being relatively prime with P. Then α is a power-residue of order l with respect to the ideal P, if and only if* $\left\{\frac{\alpha}{P}\right\} = 1$

Theorem 1.5. ([3]). *Let ξ be a primitive root of l-order, of unity, where l is a prime natural number. A prime ideal P in the ring $Z[\xi]$, is in the ring of integers in the Kummer field $Q(M;\xi)$ (where $M = \sqrt[l]{\mu}$, $\mu \in \mathbf{Z}$) in one of the situations:*
i) is equal with the l-power of a prime ideal, if $\left\{\frac{\mu}{P}\right\} = 0$,

ii) it decomposes in l different prime ideals, if $\left\{\frac{\mu}{P}\right\} = 1$,

iii) is a prime ideal, if $\left\{\frac{\mu}{P}\right\} =$ *a root of order l of unity, different from* 1.

Proposition 1.6. ([8]). *Let A be the ring of integers of the Kummer field $\mathbf{Q}\left(\sqrt[l]{p};\xi\right)$ where p is a prime natural number, $p \neq l$ and ξ is a primitive root of order l of unity. Let G be the Galois group of the Kummer field $\mathbf{Q}\left(\sqrt[l]{p};\xi\right)$ over $\mathbf{Q}(\xi)$. Then G is an Abelian group and for any $\sigma \in G$ and for any $P \in Spec(A)$, we have $\sigma(P) \in Spec(A)$.*

Proposition 1.7. ([7]). *Let p and r be prime integers, $p \equiv 1 \pmod{r}$ and take ξ a primitive root of order r of the unity. If $\mathbf{Q}\left(\xi;\sqrt[r]{p}\right)$ is the Kummer field with the ring of integers A, y_1 and y_2 are integer numbers such that $gcd(y_1, y_2) = 1$, p does not divide y_2, $m, n \in \{0, 1, ..., r-1\}$, $y_2 - y_1$ is not divisible with r, then,*

$$\left(y_2 - \xi^m \sqrt[r]{p} y_1\right) A \text{ and } \left(y_2 - \xi^n \sqrt[r]{p} y_1\right) A$$

are comaximal ideals of A.

2. Main results

Proposition 2.8. *Let p, q and l be prime distinct integers, $\overline{q}$ is generating the group $(\mathbf{Z}_l^*, \cdot)$ and take ξ a primitive root of order l of the unity. If $L = \mathbf{Q}\left(\xi;\sqrt[l]{p}\right)$ is the Kummer field with the ring of integers A and $K = \mathbf{Q}(\xi)$, then*:

$$\left(\frac{L/K}{q\mathbf{Z}[\xi]}\right)\left(\sqrt[l]{p}\right) = \left\{\frac{p}{q\mathbf{Z}[\xi]}\right\}\sqrt[l]{p}.$$

Proof. Since p and q are prime distinct natural numbers, this implies

$$\left\{\frac{p}{q\mathbf{Z}[\xi]}\right\} \neq 0.$$

The case I: If $\left\{\frac{p}{q\mathbf{Z}[\xi]}\right\} = 1$

We know that $\dfrac{L/K}{q\mathbf{Z}[\xi]}$ is the trivial automorphism, therefore

$$\left(\frac{L/K}{q\mathbf{Z}[\xi]}\right)(\sqrt[l]{p}) = \sqrt[l]{p} = \left\{\frac{p}{q\mathbf{Z}[\xi]}\right\}\sqrt[l]{p}.$$

The case II: If $\left\{\dfrac{p}{q\mathbf{Z}[\xi]}\right\} \neq 1$, we obtain that $f_{q\mathbf{Z}_L} = l$.
We denote

$$\left(\frac{L/K}{q\mathbf{Z}[\xi]}\right)(\sqrt[l]{p}) = \xi^c\sqrt[l]{p}.$$

Uging Proposition 1.1. we have:

$$\left(\frac{L/K}{q\mathbf{Z}_L}\right)(\sqrt[l]{p}) \equiv \sqrt[l]{p}^{N(q\mathbf{Z}_L)}(mod q\mathbf{Z}_L).$$

But $N(q\mathbf{Z}[\xi]) = N(q\mathbf{Z}_L)$,therefore

$$\xi^c\sqrt[l]{p} \equiv \sqrt[l]{p}^{N(q\mathbf{Z}[\xi])}(mod q\mathbf{Z}_L).$$

The last congruence implies that:

$$\sqrt[l]{p}\left((\sqrt[l]{p})^{N(q\mathbf{Z}[\xi])-1} - \xi^c\right) \equiv (mod q\mathbf{Z}_L).$$

Since $\sqrt[l]{p} \in U(\mathbf{Z}_L)$ and $P \in Spec(\mathbf{Z}_L)$, it results that:

$$\sqrt[l]{p}^{N(q\mathbf{Z}[\xi])-1} \equiv \xi^c(mod q\mathbf{Z}_L).$$

This equality is equivalent with:

$$\sqrt[l]{p}^{\frac{q^{l-1}-1}{l}} \equiv \xi^c(mod q\mathbf{Z}_L).$$

But $\sqrt[l]{p}^{\frac{q^{l-1}-1}{l}} - \xi^c \in \mathbf{Z}[\xi]$ and $q\mathbf{Z}_L \cap \mathbf{Z}[\xi] = q\mathbf{Z}[\xi]$, therefore we obtain:

$$\sqrt[l]{p}^{\frac{q^{l-1}-1}{l}} \equiv \xi^c(mod q\mathbf{Z}[\xi]).$$

According to the Proposition 1.3. and Definion 1.4., we get that

$$\xi^c = \left\{\frac{p}{q\mathbf{Z}[\xi]}\right\}.$$

From the previously proved, we obtain:

$$\left(\frac{L/K}{q\mathbf{Z}[\xi]}\right)(\sqrt[l]{p}) = \left\{\frac{p}{q\mathbf{Z}[\xi]}\right\}\sqrt[l]{p}.$$

□

We give now an application of the above result:

Proposition 2.9. *Let p and l be odd prime distinct natural numbers, $l \equiv 1(mod3)$,ϵ be a primitive root of order 3 of unity, $K = \mathbf{Q}(\epsilon)$ be the cyclotomic field. Let $L = \mathbf{Q}\left(\epsilon; \sqrt[3]{l}\right)$ be the Kummer field with the ring of integers A. If there exist $x, y \in \mathbf{N}$, p does not divide x such that $p = x^3 + ly^3$, then the Artin symbol*:

$$\left(\frac{L/K}{P}\right) = \mathbf{1}_L,$$

$(\forall)$ $P \in Spec(\mathbf{Z}[\epsilon])$, $P/p\mathbf{Z}[\epsilon]$.

Proof. We know that: $pZ[\epsilon] = P_1...P_r$, where $P_i \in Spec(Z[\epsilon])$, $i = \overline{1, r}$, $r = \dfrac{\varphi(3)}{ord_{(\mathbf{Z}_3^*, \cdot)}\overline{p}}$.
We obtain that: if $p \equiv 1(mod3)$ then $r = 2$;
if $p \equiv 2(mod3)$ then $r = 1$.
The case I: $p \equiv 1(mod3)$. We obtain that: $pZ[\epsilon] = P_1P_2$, where P_1, $P_2 \in Spec(Z[\epsilon])$.

The equality $p = x^3 + ly^3$ is equivalent with:

$$p = (x + \sqrt{3}ly)(x + \epsilon\sqrt[3]{l}y)(x + \epsilon^2\sqrt[3]{l}y). \tag{2.1}$$

Passing to the ideals in the ring A, in the equality (1), we have:

$$P_1A \cdot P_2A = (x + \sqrt[3]{l}y)A(x + \epsilon\sqrt[3]{l}y)A(x + \epsilon^2\sqrt[3]{l}y)A. \tag{2.2}$$

$N(P_1) = N(P_2) = p^f$, where f is the inertial degree of P_1, in the extension of fields $\mathbf{Q} \subset \mathbf{Q}(\epsilon)$.
From the Theorem 1.3., we have that $efg = [\mathbf{Q}(\epsilon) : \mathbf{Q}] = 2$. But $g = 2$,$e = 1$, therefore $f = 1$ and $N(P_1) = N(P_2) = p$.
Using the Proposition 1.3. and the Definition 1.4., we have:

$$\left\{\frac{l}{P_i}\right\} \equiv l^{\frac{p-1}{3}}(modP_i), i = \overline{1, 2}. \tag{2.3}$$

But $\left\{\frac{l}{P_i}\right\} \in \{1, \epsilon, \epsilon^2\}$, $i = \overline{1, 2}$. We can have:

$$\left\{\frac{l}{P_1}\right\} = \epsilon^{c_1} \neq 1,$$

$$\left\{\frac{l}{P_2}\right\} = \epsilon^{c_2} \neq 1$$

or

$$\left\{\frac{l}{P_1}\right\} = 1,$$

$$\left\{\frac{l}{P_2}\right\} = \epsilon^{c} \neq 1$$

or

$$\left\{\frac{l}{P_1}\right\} = \left\{\frac{l}{P_2}\right\} = 1.$$

If $\left\{\dfrac{l}{P_1}\right\} = \epsilon^{c_1} \neq 1$, $\left\{\dfrac{l}{P_2}\right\} = \epsilon^{c_2} \neq 1$, using the Theorem 1.5., it results P_1A,$P_2A \in Spec(A)$. This implies that the equality (2.2) is impossible. Therefore, cannot have $\left\{\dfrac{l}{P_1}\right\} = \epsilon^{c_1} \neq 1$, $\left\{\dfrac{l}{P_2}\right\} = \epsilon^{c_2} \neq 1$.
If $\left\{\dfrac{l}{P_1}\right\} = 1$, $\left\{\dfrac{l}{P_2}\right\} = \epsilon^{c} \neq 1$, usind the Theorem 1.5. we obtain that $P_1A = P_1^{'}P_2^{'}P_3^{'}$, where $P_i^{'} \in Spec(A)$ and $P_2A \in Spec(A)$.

Passing to the ideals in the ring A, in the equality (2.1), we have:

$$P_1^{'}P_2^{'}P_3^{'}(P_2A) = (x + \sqrt[3]{l}y)A(x + \epsilon\sqrt[3]{l}y)A(x + \epsilon^2\sqrt[3]{l}y)A. \tag{2.4}$$

We know that p does not divide x, $l \equiv 1(mod3)$ and we can prove easily that 3 does not divide $x + y$, $g.c.d.(x, y) = 1$. According to the Proposition 1.7., the ideals

$$(x + \sqrt[3]{l}y)A,\ (x + \epsilon\sqrt[3]{l}y)A,\ (x + \epsilon^2\sqrt[3]{l}y)A$$

are comaximal ideals in pairs.

It is known that the Galois group $G(L/K)$ is a cyclic group and let $\sigma \in G(L/K)$, $\sigma{:}L \mapsto L$, $\sigma(\epsilon) = \epsilon$, $\sigma(\sqrt[3]{l}) = \epsilon\sqrt[3]{l}$. We consider three cases.
(i) If $\left(x + y\sqrt[3]{l}\right) A \in$Spec(A), using the Proposition 1.6., we obtain that

$$\sigma\left(\left(x + y\sqrt[3]{l}\right) A\right) = \left(x + y\epsilon\sqrt[3]{l}\right) A \in Spec(A)$$

and

$$\sigma^2\left(\left(x + y\sqrt[3]{l}\right) A\right) = \left(x + y\epsilon^2\sqrt[3]{l}\right) A \in Spec(A).$$

This implies that the equality (2.4) is impossible. Similarly we obtain that the equality (2.4) is impossible, in the case (ii) (when the ideal $\sigma\left(\left(x + y\sqrt[3]{l}\right) A\right)$ is a product of two distinct prime ideals in the ring A) and in the case (iii) (when the ideal $\sigma\left(\left(x + y\sqrt[3]{l}\right) A\right)$ is the 2-power of a prime ideal in the ring A).
If $\left\{\frac{l}{P_1}\right\} = \left\{\frac{l}{P_2}\right\} = 1$, using the congruences (2.3) and the fact that P_1,$P_2 \in Spec(\mathbf{Z}[\epsilon])$, we obtain that:

$$1 \equiv l^{\frac{p-1}{3}} (modp\mathbf{Z}[\epsilon]).$$

But $p, l \in \mathbf{N}^*$, therefore $1 \equiv l^{\frac{p-1}{3}} (modp)$.
The last congruence is possible because $p \equiv 1(mod3)$.
Since $\left\{\dfrac{l}{P_1}\right\} = \left\{\dfrac{l}{P_2}\right\} = 1$, using the Proposition 2.8., we obtain that:

$$\left(\frac{L/K}{P_i}\right) = \mathbf{1}_L,\ (\forall)\, i = \overline{1,2}$$

The case II: $p \equiv 2(mod3)$. This implies that the ideal $pZ[\epsilon] \in Spec(Z[\epsilon])$.
Similarly with the case I we obtain that $N(pZ[\epsilon]) = p^2$.

Using the Proposition 1.3. and the Definition 1.4., we have:

$$\left\{\frac{l}{pZ[\epsilon]}\right\} \equiv l^{\frac{p^2-1}{3}}(modpZ[\epsilon]).$$

Since p and l are prime distinct natural numbers, it results that $\left\{\frac{l}{pZ[\epsilon]}\right\} \neq 0.$

If $\left\{\frac{l}{pZ[\epsilon]}\right\} = \epsilon^c \neq 1$, hence $pA \in Spec(A)$.

Passing to the ideals in the ring A, in the equality (1), we have:

$$pA = (x + \sqrt[3]{l}y)A(x + \epsilon\sqrt[3]{l}y)A(x + \epsilon^2\sqrt[3]{l}y)A.$$

The last equality is impossible. Therefore, we cannot have

$$\left\{\frac{l}{pZ[\epsilon]}\right\} = \epsilon^c \neq 1.$$

If $\left\{\frac{l}{pZ[\epsilon]}\right\} = 1$ similar with the case I we obtain:

$$1 \equiv l^{\frac{p^2-1}{3}}(modp\mathbf{Z}[\epsilon]).$$

But $p,\ l^{\frac{p^2-1}{3}} \in \mathbf{N}^*$, therefore $1 \equiv l^{\frac{p^2-1}{3}}(modp)$.

From $p \equiv 2(mod3)$ results $(p-1)/\frac{p^2-1}{3}$. This implies that the last congruence is true.

$\left\{\frac{l}{pZ[\epsilon]}\right\} = 1$ implies that $\left(\frac{L/K}{pZ[\epsilon]}\right) = \mathbf{1}_L$. □

References

[1] Albu T. and Ion D.I, *Chapters of the algebraic theory of numbers* (in Romanian), Ed. Academiei, Bucureşti, 1984

[2] Cohen H., *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993

[3] Hilbert D., *The theory of algebraic number fields* (translated into Romanian), Ed. Corint, Bucureşti, 1998

[4] Ireland K. and Rosen M., *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1992

[5] Magioladitis M., *Primes of the form* $x^2 + ny^2$, University of Duisburg-Essen, June 2004

[6] Savin D., *About systems of Diophantine equations*, Automation, Computers, Applied Mathematics, 13 (2004), 191-196.

[7] Savin D., *Using the properties of Kummer fields in the proof on the diophantine equation* $x^4 - q^4 = py^r$, Conference on Combinatorics, Automata and Number Theory, University of Liege, Belgium, May 2006 (paper submitted)

[8] Ştefănescu M., *Galois Theory* (in Romanian), Ed. Ex Ponto, Constanta, 2002

[9] Stevenhagen P., *Kummer Theory and Reciprocity Laws*, Universiteit Leiden, 2005

"Ovidius" University of Constanţa
Faculty of Mathematics and Informatics
Department of Mathematics
Bd. Mamaia 124
900527 Constanta, Romania
E-mail address: savin.diana@univ-ovidius.ro
E-mail address: dianet72@yahoo.com