

ON THE ORE-KRASNER EQUATION

AKRAM LBEKKOURI

Received November 8, 2011; revised December 5, 2011

ABSTRACT. It is well known that a finite totally ramified extension of a local field can be defined by infinitely many Eisenstein polynomials. Let K be a finite extension of \mathbb{Q}_p . First O.Ore in [5] and [6] found some congruencies that must be satisfied by the Eisenstein polynomials of $K[X]$ of degree p defining cyclic extensions. Then M.Krasner in [2], with a different target defined an equivalence relationship between the Eisenstein polynomials defining the same extension of any degree n over K , then proved the existence of a privileged representative of each equivalence class which he called "Reduite". In a previous work in [4, I have considered the normality problem for an Eisenstein polynomials of degree p and of degree p^2 in the case of the base field is $K = \mathbb{Q}_p$, when the residue field is simply F_p , the finite field of p elements. The aim of the present article is the explicit determination of such characteristically polynomials and their Reduites, in the cyclic case of degree p , where the base field is K a finite extension of \mathbb{Q}_p . Also illustrating examples are given.

1. INTRODUCTION

Let p be an odd prime number. Consider K a finite extension of \mathbb{Q}_p , the field of p -adic numbers. Write e for the ramification index of K/\mathbb{Q}_p . Let L/K be a totally ramified extension of degree p and fix π an uniformiser of L , ($L = K(\pi)$) so that it is a root of an Eisenstein polynomial $f(X) = \sum_{i=0}^p a_i X^i$. Denote by $v(\cdot)$ the normalized valuation of L such that $v(\pi) = 1$. We have $v(p) = ep$, indeed $v(p)$ generates $v(\mathbb{Q}_p^*)$, which is a subgroup of index e in $v(K^*)$, which is itself a subgroup of index p in $v(L^*) = \mathbb{Z}$.

1.1. Calculation of the ramification numbers. For σ a K -homomorphism of L in an algebraic closure, the lower ramification number (jump, break) relative to σ is $v_\sigma = v(\frac{\sigma(\pi) - \pi}{\pi})$, in this case of degree p , v_σ is independent of the choice of σ and satisfies $v_\sigma \leq \frac{ep}{p-1}$, (see [2] ch VI. page 138 and [7] ch IV. page 88) . The following method due to Krasner (see [2] ch V. page 136) gives the value of the lower ramification number with respect to the coefficients of the minimal polynomial. Set $g(X) = X^{-1}f(\pi(X+1)) = \sum_{j=0}^{p-1} d_j X^j$ with $d_j = \sum_{t=j+1}^p a_t \binom{t}{j+1} \pi^t$, so that the lower ramification number is given by $v_\sigma = \frac{v(d_0) - v(d_{p-1})}{p-1}$.

1.2. Needed results:

Lemma 1.1. (Krasner) Let K be a local field, K^a be its algebraic closure, G the Galois group of K^a/K and $w : K^a \rightarrow \mathbb{Q} \cup \{\infty\}$, the normalized valuation with $w(K) = \mathbb{Z} \cup \{\infty\}$.

If $\alpha, \beta \in K^a$ and one has $w(\beta - \alpha) > \sup_{\sigma \in G; \sigma(\alpha) \neq \alpha} (w(\sigma(\alpha) - \alpha))$, then $K(\alpha) \subseteq K(\beta)$.

See for example [1] ch:III, §.3 page:69

The Theorems (Th.I Ch.9 and Th.II Ch.9 pages 128-129 in [2] due to M.Krasner) can be summarized in the following theorem:

Theorem 1.2. *Let $f(X) = \sum_{i=0}^n a_i X^i$ be a polynomial of coefficients in k , a p -adic field having t_j roots of the same valuation α_j corresponding to the segment joining the point $[i_j; v(a_{i_j})]$ to the point $[i_j + t_j; v(a_{i_j+t_j})]$ in the Newton polygon of f . Then:*

- 1.) *These roots satisfy an equation of degree t_j the coefficients of which are in k .*
- 2.) *β is one of the said roots and π is a uniformising element of k then the $\pi^{-\alpha_j} \beta$ satisfies an equation of degree t_j congruent modulo π to*

$$\sum_{i=i_j}^{i_j+t_j} \frac{a_i}{\pi^{-(i-i_j)\alpha_j+v(a_{i_j})}} X^{i-i_j} \equiv 0,$$

$$\text{with } \alpha_j = \frac{v(a_{i_j})-v(a_{i_j+t_j})}{t_j}.$$

For details on the Newton-polygon see for example [1].

Lemma 1.3. (Safarevic) *Let K/Q_p be an extension of degree n , K does not contain the p -th roots of unity. Let G be a p -group of order p^m , having d generators. Denote by α the number of automorphisms of G . If $d \leq n+1$ then the number of galois extensions of K having G as galois group is*

$$\alpha^{-1} p^{(n+1)(m-d)} (p^{n+1} - 1) (p^{n+1} - p) \dots (p^{n+1} - p^{d-1}).$$

See [4]

- Note: The number of all cyclic totally ramified extensions of degree p is then $\frac{p^{n+1}-1}{p-1} - 1$, since only one is unramified. And when $K = Q_p$ the number is p .

2. NORMALITY AND EISENSTEIN POLYNOMIALS

2.1. First conditions on the coefficients of f : Let $f(X) = \sum_{i=0}^p a_i X^i$, be an Eisenstein polynomial with coefficients in K a finite extension of Q_p and $f(\pi) = 0$.

From the paragraph above we have $v = \frac{v(d_0)-v(d_{p-1})}{p-1}$, with $d_0 = \sum_{t=1}^p a_t \binom{t}{1} \pi^t$, and $d_{p-1} = \pi^p$, that is $v = \frac{v(d_0)-p}{p-1}$.

Since in the sum d_0 the valuations of the various terms $v(t) + v(a_t) + t$, are different in pairs thus, there exists only one i_0 ; $1 \leq i_0 \leq p$ such that $v(d_0) = v(i_0) + v(a_{i_0}) + i_0$. Here two cases are to be distinguished:

First case $1 \leq i_0 \leq p-1$, and

Second case $i_0 = p$.

First case:

Assume that there exists an index i_0 , $1 \leq i_0 \leq p-1$, such that the coefficient a_{i_0} satisfies:

$v(d_0) = v(i_0) + v(a_{i_0}) + i_0 = (p-1)v + p$, thus neither $v(d_0)$ nor v are divisible by p .

Furthermore since $v(d_0) < v(p\pi^p)$, we get $v < \frac{v(p)}{p-1} = \frac{ep}{p-1}$.

Then we have the following:

- $v(a_{i_0}) + i_0 = (p-1)v + p$.
- $v(a_{i_0}) \leq v(p) = ep$.
- $v(a_j) \geq v(a_{i_0})$ for $1 \leq j \leq p-1$.

- $v(a_j) > v(a_{i_0})$ for $j < i_0$.

The results above can be so recapitulated:

Proposition 2.1. *Let $K(\pi)/K$ be a totally ramified extension of degree p , where K is a finite extension of \mathbb{Q}_p and π a root of an Eisenstein polynomial $f(X) = \sum_{i=0}^p a_i X^i$.*

Assume that v the lower ramification number of $K(\pi)/K$ is a strictly positive integer.

Then we have:

1. $v < \frac{ep}{p-1}$, and

2. p does not divide v .

If and only if there exists one and only one coefficient a_{i_0} of f ; $1 \leq i_0 \leq p-1$; such that:

- $v(a_{i_0}) + i_0 = (p-1)v + p$.
- $v(a_{i_0}) \leq v(p) = ep$.
- $v(a_j) \geq v(a_{i_0})$ for $1 \leq j \leq p-1$.
- $v(a_j) > v(a_{i_0})$ for $j < i_0$.

Second case:

In this case, $i_0 = p$, and $v(d_0) = v(p\pi^p)$, so $v(d_0) = (e+1)p$.

Since $\frac{v(p\pi^p)-p}{p-1} = \frac{ep}{p-1}$, thus $v = \frac{ep}{p-1}$, v being integer also $(p-1)$ divides e and p divides v .

From $v(d_0) = (e+1)p$, we get $v(a_i) \geq (e+1)p$, for $1 \leq i \leq p-1$.

2.2. Normality and coefficients of f : According to Krasner's Lemma, it is clear that an extension $K(\pi)/K$ of degree p defined by an Eisenstein polynomial $f(X) = \sum_{i=0}^p a_i X^i$, $f(\pi) = 0$, is normal, that is cyclic, if and only if:

- 1.) The lower ramification number v is integer.
- 2.) The roots $\sigma(\pi)$ of f have an Hensel expansion till the order $v+1$ in $K(\pi)$ that is $\sigma(\pi) = \pi + \psi\pi^{v+1} + A(\pi)$ with $A(\pi) \in K(\pi)$, $v(A(\pi)) > v+1$, ψ a $(p^{f_0} - 1)$ -th root of unity belonging to K , and f_0 the residual degree of $K(\pi)$ that is of K . For more details see [3].

Consider $K(\pi)/K$ a totally ramified extension of degree p (where K is a finite extension of \mathbb{Q}_p), such that the ramification number v is an integer.

Define $g(X) = f(X + \pi) = \sum_{t=0}^p b_t X^t$. So,

$$g(X) = \sum_{t=0}^p \sum_{i=t}^p a_i \binom{i}{t} \pi^{i-t} X^t, \text{ with } b_t = \sum_{i=t}^p a_i \binom{i}{t} \pi^{i-t}, b_0 = 0 \text{ and } b_p = 1.$$

The roots of g must be 0 and $(p-1)$ roots β of valuation $v+1$.

Hence the Newton-polygon (See for example [1] Chap. III) of g , will have:

- One infinite vertical segment, the semi line $\{(1, y), v(b_1) \leq y \leq \infty\}$, and
- An oblique segment joining the point $[1; v(b_1)]$ to the the point $[p; 0]$.

By application of Theorem (1.2) above, the condition (2.) is satisfied if and only if the $\pi^{-(v+1)}\beta$, are roots of the congruence:

$$\sum_{t=1}^p \frac{b_t X^{t-1}}{\pi^{v(b_1)-(t-1)(v+1)}} \equiv 0 \text{ modulo } \pi. \quad (2.1)$$

Therefore, we have:

$$\sum_{t=1}^p \frac{b_t X^{t-1}}{\pi^{v(b_1)-(t-1)(v+1)}} \equiv \omega (X^{p-1} - \psi^{p-1}) \text{ modulo } \pi, \quad (2.2)$$

ω being an element of F_p^* . Also the residue classes of the $\pi^{-(v+1)}\beta$, that are the $j\psi$ with $1 \leq j \leq p-1$ and ψ is a $(p^{f_0} - 1)$ -th root of unity, form the elements of the set $F_p^*\psi$ exactly. Since $v(b_t) > v(b_1) - (t-1)(v+1)$, for $1 < t \leq p-1$, then 2.2 is reduced to:

$$\frac{b_p X^{p-1}}{\pi^{v(b_1)-(p-1)(v+1)}} + \frac{b_1}{\pi^{v(b_1)}} \equiv \omega(X^{p-1} - \psi^{p-1}) \text{ modulo } \pi. \quad (2.3)$$

By taking into account the inequalities of (Proposition (2.1) First case) we get $v(b_1) = (p-1)(v+1)$. So,

$$X^{p-1} + \frac{b_1}{\pi^{v(b_1)}} \equiv \omega(X^{p-1} - \psi^{p-1}) \text{ modulo } \pi. \quad (2.4)$$

Therefore, $\omega = 1$.

2.2.1. *First case.* In this case we have, $0 < i_0 < p$.

From $v(a_{i_0}) + v(i_0) + i_0 = v(p-1) + p$, v is integer if and only if $(p-1)$ divides $v(a_{i_0}) + i_0 - p$. To sum up the extension is normal if and only if

- 1.) $(p-1)$ divides $v(a_{i_0}) + i_0 - p$
- 2.)

$$\frac{b_1}{\pi^{v(b_1)}} \equiv -\psi^{p-1} \text{ modulo } \pi. \quad (2.5)$$

We have: $b_1 \equiv i_0 a_{i_0} \pi^{i_0-1} \text{ modulo } \pi^{(p-1)(v+1)+1}$. Set $\pi^p = u\tau$, with u a unit, and write $v(a_{i_0}) = n_0 p$ that is $a_0 = \tau \alpha_0$ with α_0 a unit of K .

So, we want

$$\frac{i_0 a_{i_0} \pi^{i_0-1}}{\pi^{(p-1)(v+1)}} \equiv -\psi^{p-1} \text{ modulo } \pi. \quad (2.6)$$

That is, we must have

$$i_0 a_{i_0} \tau^{-n_0} \equiv -\psi^{p-1} u^{n_0} \text{ modulo } \pi. \quad (2.7)$$

First prove that $u \equiv \tau^{-1} N(\pi) \text{ modulo } \pi$, (where $N(\pi) = N_{K(\pi)/K}(\pi)$), which is equivalent to the fact that $v(N(\pi) - \pi^p) > p$.

Indeed the conjugates of π (distinct from π) can be written in the form $\pi + \pi z_i$, where $v(z_i) = v$ (the lower ramification number), $N(\pi) = \pi(\pi + \pi z_1) \dots (\pi + \pi z_{p-1})$, that is

$$N(\pi) = \pi^p + \sum \pi^p z_{i_1} z_{i_2} \dots z_{i_r}, \text{ with } r \geq 1 \text{ that is, } v(N(\pi) - \pi^p) > p.$$

Now, $N(\pi) = (-1)^p a_0 = -a_0$, p is odd, finally we get $u \equiv -\alpha_0 \text{ modulo } \pi$, so that (2.7) becomes $i_0 a_{i_0} \equiv (-1)^{(n_0+1)} \psi^{p-1} \alpha_0^{n_0} \text{ modulo } \tau^{n_0+1}$.

Conversely, it is clear that if there exists a coefficient a_{i_0} satisfying (2.7) with $n_0 = \frac{v(a_{i_0})}{p}$, then by equivalence, every root $\sigma(\pi)$ of $f(x) = 0$, will have an Hensel expansion till the order $v+1$ in the form $\sigma(\pi) = \pi + \lambda \pi^{v+1} + \dots$, where λ is a primitive $(p^{f_0} - 1)$ -th root of unity of K .

Finally, the normality holds according to Krasner's Lemma.

Therefore the result established above can be formulated as

Theorem 2.2. (*Normality theorem First version*) Let $f(X) = \sum_{i=0}^p a_i X^i$, $f(\pi) = 0$, be an Eisenstein polynomial of degree p ; the coefficients of which are integer in K ; K being a finite extension of \mathbb{Q}_p , and f_0 the residue degree of K .

Assume that there exists an index i_0 , $1 \leq i_0 \leq p-1$, such that $v(a_{i_0}) + i_0 = \inf_{1 \leq i \leq p} (v(a_i) + i)$. Then $K(\pi)/K$ is normal if and only if :

- 1.) $(p-1)$ divides $n_0 + i_0 - p$; with $n_0 = \frac{v(a_{i_0})}{p}$.
- 2.) There exists ψ a $(p^{f_0} - 1)$ -th root of unity of K , such that

$$i_0 a_{i_0} \equiv (-1)^{n_0+1} \psi^{p-1} a_0^{n_0} \text{ modulo } \tau^{n_0+1}. \quad (2.8)$$

(Note that in this case $\frac{v(a_{i_0})+i_0-p}{p-1} = \frac{n_0 p+i_0-p}{p-1} = v$, is the lower ramification number of $K(\pi)/K$, and τ is a uniformizer of K .)

Remark:

It is easy to notice that the principal index i_0 can be expressed as $i_0 = p - \bar{v}$; \bar{v} being the integer belonging to $\{1, 2, \dots, p-1\}$ such that $v \equiv \bar{v} \text{ modulo } p$. We can too express the number n_0 as $n_0 = v - \frac{v-\bar{v}}{p}$.

So, a second version of the result above, can be formulated as follows:

Theorem 2.3. (Normality theorem Second version) Let $f(X) = \sum_{i=0}^p a_i X^i$, $f(\pi) = 0$, be an Eisenstein polynomial of degree p ; the coefficients of which are integer in K ; K being a finite extension of \mathbb{Q}_p , and f_0 the residue degree of K .

Assume that the lower ramification number v of $K(\pi)/K$, is a positive integer not divisible by p .

Then $K(\pi)/K$ is normal if and only if:

There exists ψ a $(p^{f_0} - 1)$ -th root of unity of K , such that

$$(p - \bar{v}) a_{p-\bar{v}} \equiv (-1)^{v+1-((v-\bar{v})/p)} \psi^{p-1} a_0^{v-((v-\bar{v})/p)} \text{ modulo } \tau^{v+1-((v-\bar{v})/p)}. \quad (2.9)$$

(τ being a uniformizer of K .)

The following little lemma will be necessary:

Lemma 2.4. Let $K(\pi)/K$ be a cyclic wildly ramified extension of degree p , K being a finite extension of \mathbb{Q}_p and π a uniformizer of $K(\pi)$.

Then there exists a suitable uniformizer τ of K such that:

$N(\pi) \equiv \tau \text{ modulo } \tau^{v+1}$, where $N(\pi)$ is the norm of π in the extension $K(\pi)/K$ and v (an integer strictly positive) is the lower ramification number of $K(\pi)/K$.

Proof. Since the extension is cyclic, then for any generator σ of $\text{gal}(K(\pi)/K)$, we have $\sigma^i(\pi) \equiv \pi + i\xi\pi^{v+1} \text{ modulo } \pi^{v+2}$ for $1 \leq i \leq p-1$ with ξ a suitable root of unity of $K(\pi)$.

Take for example $\pi' = \pi + \pi^{v+1}$. Then $\frac{\sigma(\pi)}{\pi'} = \frac{1+\xi\pi^v+\dots}{1+\pi^v}$. Hence $\frac{\sigma(\pi)}{\pi'} \in U_{K(\pi)}^v$, where $U_{K(\pi)}^v$ is the subgroup of units z of $K(\pi)$ such that $z-1 \equiv 0 \text{ modulo } \pi^v$.

Furthermore we know that $U_K^1 \supseteq N_{K(\pi)/K}(U_{K(\pi)}^1)$ and $N_{K(\pi)/K}(U_{K(\pi)}^1)$ is a subgroup of index p of U_K^1 in the case that $K(\pi)/K$ is normal and totally ramified.

By use of the Herbrand function ψ (see [7] ch:IV §.3 page 73) we get $\psi(v) = v$ (see [7] ch:V §.3 page 83). By Proposition:4 of [7] (ch:V §.3 page 84), we have $U_K^v \supseteq N_{K(\pi)/K}(U_{K(\pi)}^v)$. Therefore we can affirm that $N_{K(\pi)/K}(\pi)/N_{K(\pi)/K}(\pi') \in U_K^v$. By taking $N_{K(\pi)/K}(\pi') = \tau$, the result follows. \square

Consequences:

In this case we easily can notice the following:

- 1.) From the expression of the lower ramification number v , we have $v \equiv p - i_0 \text{ modulo } p$.
- 2.) Since $v_K(a_i) \geq v_K(a_{i_0}) = n_0$, for any $1 \leq i \leq p-1$, we can deduce that: $v_K(a_i) \geq v - \lfloor \frac{v}{p} \rfloor$, for any $1 \leq i \leq p-1$, where $\lfloor \alpha \rfloor$ is the greater integer less or equal to α .

Indeed, $1 \leq i_0 \leq p-1$ thus $\frac{v+i_0}{p} - 1 < \frac{v}{p}$; (we know that $\frac{v+i_0}{p}$ is integer) hence we have:
 $\frac{v+i_0}{p} - 1 \leq \lfloor \frac{v}{p} \rfloor$ and then $n_0 = v - (\frac{v+i_0}{p} - 1) \geq v - \lfloor \frac{v}{p} \rfloor$.

• 3.) According to the lemma 2.4 above we have that: $a_0 \equiv \tau$ modulo τ^{v+1} , for some suitable uniformizer τ .

Note: If $v \neq 1$, it is not true that $a_0 \equiv \tau$ modulo τ^{v+1} for any uniformizer τ of K .

Example:

Consider $f(X) = X^3 + 3X^2 + 3$ as a polynomial of $\mathbb{Q}_3[X]$ with $f(\pi) = 0$. f is an Eisenstein polynomial, and the ramification number of the extension $\mathbb{Q}_3(\pi)/\mathbb{Q}_3$ is 1. Although the integrity of the ramification number the extension is not normal.

Now the discriminant of f and that of the extension $\mathbb{Q}_3(\pi)/\mathbb{Q}_3$ is, $-567 = (9\sqrt{-7})^2$, the splitting field of f over \mathbb{Q}_3 is $\mathbb{Q}_3(\pi, \sqrt{-7})$. $\mathbb{Q}_3(\sqrt{-7})/\mathbb{Q}_3$ is a quadratic extension generated by a root of $X^2 + 7$ and $X^2 + 7 \equiv X^2 + 1$ modulo 3. Furthermore, $X^2 + 1$ being irreducible in $\mathbb{Z}/3\mathbb{Z}[X]$, so the residue degree of $\mathbb{Q}_3(\sqrt{-7})/\mathbb{Q}_3$ is 2. That is $\mathbb{Q}_3(\sqrt{-7})/\mathbb{Q}_3$ is unramified and contains ζ_{3^2-1} a 8-th root of unity. Then we have that f is still Eisenstein as polynomial of $\mathbb{Q}_3(\sqrt{-7})[X]$.

Therefore, the formula

$$i_0 a_{i_0} \equiv (-1)^{n_0+1} \psi^{p-1} a_0^{n_0} \text{ modulo } \tau^{n_0+1}. \quad (2.10)$$

is satisfied.

Indeed $p = 3$, $i_0 = 2$, $a_{i_0} = a_0 = 3$, and $n_0 = 1$, also it suffices to take $\tau = 3$, and $\zeta_{3^2-1} = i$ hence we get $6 \equiv -3$ modulo 9.

Then we can say that $\mathbb{Q}_3(\pi, \sqrt{-7})/\mathbb{Q}_3(\sqrt{-7})$ is normal which is a foregone conclusion.

2.2.2. *Second case.* In this case we have: $i_0 = p$, $v = \frac{ep}{p-1}$, and $v(a_i) \geq (e+1)p$ for $1 \leq i \leq p-1$.

Furthermore we verify that the coefficient b_1 of $g(X) = f(X + \pi) = \sum_{t=0}^p b_t X^t$, has the valuation $v(b_1) = (p-1)(v+1)$.

Therefore from congruence (2.3) we have that the extension is normal if and only if:

- 1.) v is integer.
- 2.)

$$\frac{b_1}{\pi^{v(b_1)}} \equiv -\psi^{p-1} \text{ modulo } \pi. \quad (2.11)$$

that is:

- 1.) $(p-1)$ divides e .
- 2.)

$$\frac{p\pi^{p-1}}{\pi^{p(e+1)-1}} \equiv -\psi^{p-1} \text{ modulo } \pi. \quad (2.12)$$

We prove the following Lemma:

Lemma 2.5. *For every $w \in K$, with $v(w) > 0$, the number $1 + w$ is a $(p-1)$ -th power of some element of K .*

Proof. The assertion comes from the fact that $X^{p-1} - 1 - w = 0$, has a root in K .

Indeed by passage to the residue classes we get the equation $X^{p-1} - 1 = 0$, which completely splits in the residue field of K , then Hensel's Lemma ends the proof. \square

Therefore, the congruence (2.12) is equivalent to:

$$-p(-\alpha_0\tau)^{-e} = \psi^{p-1}(1+w), \text{ with } w \in K \text{ and } v(w) > 0.$$

Therefore (2.12) holds if, $-p$ is a $(p-1)$ -th power of some element of K .

Conversely, if $-p = z^{(p-1)}$, with $z \in K$, then we can write $z = (-\alpha_0\tau)^{e_1} (1+y)\psi$, where $e_1 = \frac{e}{p-1}$, $y \in K$ with $v(y) > 1$, and ψ is a $(p^{f_0} - 1)$ -th root of unity of K , hence (2.12) holds.

On the other hand, it is well known that the extension arising from Q_p by adjoining a primitive p -th root of unity equals the last one obtained by adjoining a $(p-1)$ -th root of $-p$, see ([1]ch:III, exercise:7 page 74), ie: $Q_p(\xi_p) = Q_p(\sqrt[p-1]{-p})$.

Then we can state the result:

Theorem 2.6. *Let f be an Eisenstein polynomial of degree p ; $f(\pi) = 0$; the coefficients of which are integer in K , a finite extension of Q_p . Assume that:*

- 1.) $(p-1)$ divides e .
- 2.) The lower ramification number of $K(\pi)/K$ is $v = \frac{ep}{(p-1)}$, (it is also integer).

Then: $K(\pi)/K$ is normal if and only if $-p$ is $p-1$ -th power in K .

(That is if and only if K contains the p -th roots of unity).

In such case $K(\pi)/K$ is a cyclic Kummer extension.

3. COMPUTATION OF SOME REDUITES

Let K be a finite extension of Q_p containing no primitive p -th root of unity, in his article [2] M.Krasner established an equivalence relationship between the different Eisenstein polynomials of a same given degree, with coefficients in K . In the sense that two Eisenstein polynomials f_1 and f_2 belong to the same equivalence class if and only if $K(\pi_1) = K(\pi_2)$ with $f_1(\pi_1) = f_2(\pi_2) = 0$. Furthermore he puts and answers the question:

"Under what conditions on their coefficients two Eisenstein polynomials are equivalent?"

Unfortunately the said article is in an old way (1938) written and contains some typing mistakes. Naturally, M.Krasner is in all innocence of the mistakes. Curiously, when asking some specialists (some of them having been Krasner's students) about the Reduite, I couldn't obtain any answer. I had the feeling that nobody has read this article. It seems that everybody knows that M.Krasner has discovered the Reduite, but none can calculate it.

Indeed, M.Krasner in ([2] Theorem:I, ch:10, page: 164) proved the existence of some privileged representative of an equivalence class that he called Reduite. Then he described it as far as possible.

A Reduite of a given Eisenstein polynomial, in Krasner's sense, is an equivalent polynomial having a minimal number of nonzero coefficients, furthermore the nonzero coefficients have a finite $\bar{\pi}$ -adic Hensel expansion with a minimal number of nonzero terms, with respect to a uniformizer $\bar{\pi}$ of K .

Note that a Reduite is not unique. Indeed it especially depends on the chosen uniformizer $\bar{\pi}$ of K .

Starting by an Eisenstein polynomial:

$$f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 = 0, a_i \in K,$$

he wrote $a_i = \sum_{t=1}^{\infty} \gamma_t^{(i)} \bar{\pi}^t$ with $\gamma_t^{(i)}$ a $p^{f_0} - 1$ -th root of unity, f_0 being the residue degree of K .

Then he made the following reordering of terms:

$$f(X) = X^n + \sum_{t=n+1}^{\infty} \gamma_{\lfloor \frac{t}{n} \rfloor}^{(t-n\lfloor \frac{t}{n} \rfloor)} \bar{\pi}^{\lfloor \frac{t}{n} \rfloor} X^{t-n\lfloor \frac{t}{n} \rfloor} + \gamma_1^{(0)} \bar{\pi}.$$

$\lfloor \alpha \rfloor$ being the greater integer less or equal to α .

For the special and remarkable case when $K(\pi)/K$ is galois of prime degree p with the lower ramification number v , he explicitly calculated the said Reduite (see [2] ch:10, page 168), that is:

$$X^p + \sum_{p+v(p-1) \leq i < p(v+1); p \nmid i} \gamma_{\lfloor \frac{i}{p} \rfloor}^{(i-p\lfloor \frac{i}{p} \rfloor)} \bar{\pi}^{\lfloor \frac{i}{p} \rfloor} X^{i-p\lfloor \frac{i}{p} \rfloor} + \gamma_1^{(0)} \bar{\pi} + \gamma_{v+1}^{(0)} \bar{\pi}^{v+1}.$$

(Note that in the said article, a typing mistake slipped out in this formula, the term $\gamma_1^{(0)} \bar{\pi}$ was missing.)

Through the variable changes: $t = i - p\lfloor \frac{i}{p} \rfloor$ and $j = \lfloor \frac{i}{p} \rfloor = \frac{i-t}{p}$, the form of the Reduite above becomes:

$$X^p + \sum_{t=p-v+p\lfloor \frac{v}{p} \rfloor}^{p-1} \sum_{j=v-\lfloor \frac{v}{p} \rfloor}^v \gamma_j^{(t)} \bar{\pi}^j X^t + \gamma_1^{(0)} \bar{\pi} + \gamma_{v+1}^{(0)} \bar{\pi}^{v+1}.$$

\bar{v} being the integer belonging to $\{1, 2, \dots, p-1\}$ such that $v \equiv \bar{v}$ modulo p .

It is easy to see that $p - v + p\lfloor \frac{v}{p} \rfloor = p - \bar{v}$.

By taking into consideration the consequence 2) of theorem (2.2) this Reduite can be written, with respect to the initial coefficients of f , as follows:

$$X^p + \sum_{t=p-\bar{v}}^{p-1} \bar{a}_t^{(v)} X^t + \bar{a}_0, \text{ with } \bar{a}_t^{(v)} \equiv a_t \text{ modulo } \bar{\pi}^{v+1}, \bar{a}_0 = \gamma_1^{(0)} \bar{\pi} + \gamma_{v+1}^{(0)} \bar{\pi}^{v+1}, \text{ when the expansion of } a_0 \text{ is } a_0 = \sum_{i=1}^{\infty} \gamma_i^{(0)} \bar{\pi}^i.$$

That is by choosing a suitable uniformizer $\bar{\pi}$ such that $a_0 \equiv \xi \bar{\pi}$ modulo $\bar{\pi}^{v+1}$ with ξ a suitable root of unity; see consequence 3) of theorem (2.2); we can say that:

the Reduite of f is:

$$X^p + \sum_{t=p-\bar{v}}^{p-1} \bar{a}_t^{(v)} X^t + \bar{a}_0^{(v+1)}, \text{ with } \bar{a}_t^{(v)} \equiv a_t \text{ modulo } \bar{\pi}^{v+1}, \bar{a}_0^{(v+1)} \equiv a_0 \text{ modulo } \bar{\pi}^{v+2}.$$

To sum up the Reduite of an Eisenstein polynomial of degree p defining a normal (=cyclic) extension is simply its reduction, as described above, with respect to a suitable uniformizer.

And as is has been told above in the definition of the reduite, "the reduite is not unique since it depends essentially of the chosen uniformizer."

In this case, when already knowing the form of the Reduite, and by choosing a suitable uniformizer $\bar{\pi}$ such that $a_0 \equiv \xi \bar{\pi}$ modulo $\bar{\pi}^{v+1}$, with ξ a suitable root of unity, it is easy to verify that effectively f and its Reduite define the same extension, by means of a simple and classical proof.

Indeed, using the current notations, consider the Eisenstein polynomial, $f(X) = \sum_{i=0}^p a_i X^i$, with coefficients in K a finite extension of \mathbb{Q}_p , and set $f(\pi) = 0$, such that $K(\pi)/K$ is normal.

Denote by g the reduite of f as calculated above. Write π_0 for a root of g and $\pi = \pi_1, \pi_2, \dots, \pi_p$; the various roots of f . Then compute the following expression $f(\pi_0) - g(\pi_0) = f(\pi_0)$, in two different ways:

$$f(\pi_0) = \prod_{i=1}^p (\pi_0 - \pi_i), \text{ and } f(\pi_0) - g(\pi_0) = \pi_0^p - \pi_0^p + \sum_{i=1}^{p-1} \alpha_i \pi_0^i + \alpha_0.$$

Where $\alpha_i = a_i - \bar{a}_i^{(v)}$ for $p - \bar{v} \leq i \leq p - 1$, and $\alpha_0 = a_0 - \bar{a}_0^{(v+1)}$, since we have $\alpha_0 \equiv 0$ modulo $\bar{\pi}^{v+2}$, and $\alpha_i \equiv 0$ modulo $\bar{\pi}^{v+1}$. v being the ramification number of $K(\pi)/K$.

Then according to the normalized valuation of $K(\pi)$:

$$v(\alpha_0) \geq p(v+2) \text{ and } v(\alpha_i \pi_0^i) \geq p(v+1) + i \text{ for } 1 \leq i \leq p-1.$$

So we get $v(f(\pi_0) - g(\pi_0)) = v(\prod_{i=1}^p (\pi_0 - \pi_i)) \geq p(v+1) + 1$, thus there exists at least one i , $1 \leq i \leq p$, such that $v(\pi_0 - \pi_i) \geq v+1 + \frac{1}{p} > v+1$, then Krasner's Lemma ends the proof.

So we have the result:

Theorem 3.1. *Let $f(X) = \sum_{i=0}^p a_i X^i$ be an Eisenstein polynomial of degree p (p being any odd prime number), with coefficients in K , a finite extension of \mathbb{Q}_p , $f(\pi) = 0$. Assume that $K(\pi)/K$ is normal having a lower ramification number v not divisible by p . Then $K(\pi)/K$ can be generated by a root of the Reduite of f namely the polynomial:*

$X^p + \sum_{t=p-\bar{v}}^{p-1} \bar{a}_t^{(v)} X^t + \bar{a}_0^{(v+1)}$, with $\bar{a}_t^{(v)} \equiv a_t$ modulo $\bar{\pi}^{v+1}$, and $\bar{a}_0^{(v+1)} \equiv a_0$ modulo $\bar{\pi}^{v+2}$.
For $\bar{\pi}$ a uniformizer of K such that: $a_0 \equiv \xi \bar{\pi}$ modulo $\bar{\pi}^{v+1}$, with ξ a suitable root of unity.

Note:

In the special case when the lower ramification number $v \equiv 1$ modulo p , which is manifestly the case if the base field $K = Q_p$, we have $i_0 = p - 1$, in the formula (2.9) so $n_0 p = v(p - 1) + 1$, then (2.9) becomes:

$$(p - 1)a_{p-1} \equiv (-1)^{v+1 - ((v-1)/p)} \psi^{p-1} a_0^{v - ((v-1)/p)} \text{ modulo } \bar{\pi}^{v+1 - ((v-1)/p)}. \quad (3.1)$$

Then for the Reduite we must take:

$$\bar{a}_{p-1}^{(v)} \equiv a_{p-1} \text{ modulo } \bar{\pi}^{v+1}, \text{ that is } \bar{a}_{p-1}^{(v)} = \sum_{t=v - ((v-1)/p)}^v \gamma_t^{(p-1)} \bar{\pi}^t.$$

Hence the Reduite is the following trinomial polynomial:

$$X^p + \left(\sum_{t=v - ((v-1)/p)}^v \gamma_t^{(p-1)} \bar{\pi}^t \right) X^{p-1} + (\gamma_1^{(0)} \bar{\pi} + \gamma_{v+1}^{(0)} \bar{\pi}^{v+1}),$$

with the normality condition that: $\gamma_{v - ((v-1)/p)}^{(p-1)} = (-1)^{v - ((v-1)/p)} \psi^{p-1} (\gamma_1^{(0)})^{v - ((v-1)/p)}$.

That is, if $K = Q_p$:

$$X^p + \gamma_1^{(p-1)} \bar{\pi} X^{p-1} + (\gamma_1^{(0)} \bar{\pi} + \gamma_2^{(0)} \bar{\pi}^2),$$

with the normality condition that: $\gamma_1^{(p-1)} = -\gamma_1^{(0)}$.

So, we can deduce the following result:

Corollary 3.2. *Let p be any odd prime number. Every cyclic totally ramified extension of degree p over Q_p is generated by a root of an Eisenstein polynomial in the form:*

$$X^p + pX^{p-1} + (p - 1)p + dp^2, \text{ with } d \text{ an integer verifying } 0 \leq d \leq p - 1.$$

It is noteworthy that we get exactly p Reduites relative to the different p cyclic totally ramified extension of degree p of Q_p which meets the number computed by Safarevic (1.3).

Particularly let us determine the reduite of the wild ramified subextension $Q_p(\pi)$ of $Q_p(\tau_{p^2})$, where τ_{p^2} is a primitive p^2 -th root of unity.

Consider g a generator of $(Z/p^2Z)^*$, and $\alpha \equiv g^p$ modulo p^2 , we can take $\pi = \prod_{i=1}^{p-1} (1 - \tau_{p^2}^{\alpha_i})$, with $\alpha_1 = \alpha$, and $\alpha_i \equiv \alpha^i$ modulo p^2 , as primitive generator of the said extension.

Since $\pi = N_{Q_p(\tau_{p^2})/Q_p(\pi)} (1 - \tau_{p^2})$, we get $N_{Q_p(\pi)/Q_p}(\pi) = p$, that is $a_0 = -p \equiv (p - 1)(p + p^2)$ modulo p^3 , thus the reduite relative to the wild ramified subextension $Q_p(\pi)$ of $Q_p(\tau_{p^2})$, is $X^p + pX^{p-1} + (p - 1)(p + p^2)$ therefore we have the result:

Corollary 3.3. *Let p be any odd prime number. Then the wild ramified subextension of $Q_p(\tau_{p^2})$ where τ_{p^2} is a primitive p^2 -th root of unity can be generated by the roots of the polynomial:*
 $X^p + pX^{p-1} + (p - 1)(p + p^2)$.

Examples:

As numerical evidence we calculate the Reduites relative to the following extensions K/Q_p :

1. K/Q_p is the wild ramified subextension of $Q_p(\tau_{p^2})$; τ_{p^2} is a primitive p^2 -th root of unity :

- For $p = 3$, consider the minimal polynomial f_3 of $\pi = (1 - \tau_9)(1 - \tau_9^{-1})$, with τ_9 a primitive 9-th

root of unity over Q_3 . Then

$$\begin{aligned}
f_3(X) &= X^3 - 6X^2 + 9X - 3 \\
&\equiv X^3 + 21X^2 + 9X + 24 \\
&\equiv X^3 + (3 + 2 \cdot 3^2)X^2 + 9X + 2(3 + 3^2) \pmod{27}.
\end{aligned} \tag{3.2}$$

So, as reduite we can take: $X^3 + 3X^2 + 2(3 + 3^2)$.

• For $p = 5$, consider the minimal polynomial f_5 of $\pi = (1 - \tau_{25})(1 - \tau_{25}^{-1})(1 - \tau_{25}^7)(1 - \tau_{25}^{-7})$ with τ_{25} a primitive 25-th root of unity over Q_5 . Then

$$\begin{aligned}
f_5(X) &= X^5 - 20X^4 + 100X^3 - 125X^2 + 50X - 5 \\
&\equiv X^5 + 105X^4 + 100X^3 + 50X + 120 \\
&\equiv X^5 + (5 + 4 \cdot 5^2)X^4 + 100X^3 + 50X + 4(5 + 5^2) \pmod{125}.
\end{aligned} \tag{3.3}$$

So, as reduite we can take: $X^5 + 5X^4 + 4(5 + 5^2)$.

• For $p = 7$, consider the minimal polynomial f_7 of $\pi = (1 - \tau_{49})(1 - \tau_{49}^{-1})(1 - \tau_{49}^{18})(1 - \tau_{49}^{-18})(1 - \tau_{49}^{19})(1 - \tau_{49}^{-19})$ with τ_{49} a primitive 49-th root of unity over Q_7 . Then

$$\begin{aligned}
f_7(X) &= X^7 - 42X^6 + 539X^5 - 2401X^4 + 3773X^3 - 1470X^2 + 196X - 7 \\
&\equiv X^7 + 301X^6 + 196X^5 + 245X^2 + 196X + 336 \\
&\equiv X^7 + (7 + 6 \cdot 7^2)X^6 + 196X^5 + 245X^2 + 196X + 6(7 + 7^2) \pmod{343}.
\end{aligned} \tag{3.4}$$

So, as reduite we can take: $X^7 + 7X^6 + 6(7 + 7^2)$.

• For $p = 11$, consider the minimal polynomial f_{11} of $\pi = (1 - \tau_{121})(1 - \tau_{121}^{-1})(1 - \tau_{121}^3)(1 - \tau_{121}^{-3})(1 - \tau_{121}^{27})(1 - \tau_{121}^{-27})(1 - \tau_{121}^{40})(1 - \tau_{121}^{-40})(1 - \tau_{121}^{112})(1 - \tau_{121}^{-112})$ with τ_{121} a primitive 121-th root of unity over Q_{11} . Then

$$\begin{aligned}
f_{11}(X) &\equiv X^{11} + 979X^{10} + 726X^9 + 847X^8 + 726X^6 + 726X^4 + 242X^3 + 605X + 1320 \\
&\equiv X^{11} + (11 + 8 \cdot 11^2)X^{10} + 726X^9 + 847X^8 + 726X^6 \\
&\quad + 726X^4 + 242X^3 + 605X + 10(11 + 11^2) \pmod{1331}.
\end{aligned} \tag{3.5}$$

So, as reduite we can take: $X^{11} + 11X^{10} + 10(11 + 11^2)$.

• For $p = 13$, consider the minimal polynomial f_{13} of $\pi = (1 - \tau_{169})(1 - \tau_{169}^{-1})(1 - \tau_{169}^{80})(1 - \tau_{169}^{-80})(1 - \tau_{169}^{147})(1 - \tau_{169}^{-147})(1 - \tau_{169}^{99})(1 - \tau_{169}^{-99})(1 - \tau_{169}^{146})(1 - \tau_{169}^{-146})(1 - \tau_{169}^{150})(1 - \tau_{169}^{-150})$ with τ_{169} a primitive 169-th root of unity over Q_{13} .

Then

$$\begin{aligned}
f_{13}(X) &\equiv X^{13} + 1703X^{12} + 2028X^{11} + 1352X^{10} + 338X^9 + 2028X^8 + 338X^7 \\
&\quad + 338X^4 + 845X^3 + 1859X^2 + 1183X + 2184 \\
&\equiv X^{13} + (13 + 10 \cdot 13^2) X^{12} + 2028X^{11} + 1352X^{10} + 338X^9 + 2028X^8 + 338X^7 \\
&\quad + 338X^4 + 845X^3 + 1859X^2 + 1183X + 12(13 + 13^2) \pmod{2197}.
\end{aligned} \tag{3.6}$$

So, as reduite we can take: $X^{13} + 13X^{12} + 12(13 + 13^2)$.

Q_p having exactly p cyclic totally ramified extensions of degree p , in the following example we determine the $(p - 1)$ other extensions by means of Eisenstein polynomials.

2. The $(p - 1)$ other cyclic totally ramified extensions K/Q_p of degree p :

By use of the following program, through the software Pari, for the case $p = 7$ we have determined $p - 1$ various Eisenstein polynomials corresponding respectively to the said extensions.

The input of the program for the case $p = 7$:

```

Phi49 = polcyclo(49, z);
Phi29 = polcyclo(29, w);
zeta49 = Mod(z, Phi49);
zeta29 = Mod(w, Phi29);
Eta = 1 + zeta49 + zeta49^(-1) + zeta49^(18) + zeta49^(-18) + zeta49^(19) + zeta49^(-19);
Lambda = zeta29 + zeta29^(-1) + zeta29^(12) + zeta29^(-12);
c = vector(7, a, 3^(a - 1) %49);
d = vector(7, b, 2^(b - 1) %29);
conjugate(X, g) = {local(Y);
Y = lift(X, z);
Y = subst(Y, z, z^(c[g[1]]%7 + 1))};
Y* = Mod(1, Phi49);
Y = lift(Y, w);
Y = subst(Y, w, w^(d[[2]]%7 + 1));
Y* = Mod(1, Phi29);
return(Y);
}
Tr(X, g) = sum(i = 0, 6, conjugate(X, i*g));
N(X, g) = prod(i = 0, 6, conjugate(X, i*g));
subfield(i) = lift(lift(N(x - Tr(Eta * Lambda, [i, 1]), [1, 0])));
for(i = 1, 6, print(subfield(i)));

```

And by similar programs, Mutatis Mutandis, for the cases $p = 3$ and $p = 5$. I have got the following outputs .

The output of the program for the case $p = 3$:

$$\begin{aligned}
f_1(X) &= X^3 + 3X^2 - 18X - 48 \\
&\equiv X^3 + 3X^2 + 9X + 6 \pmod{27}.
\end{aligned} \tag{3.7}$$

So, as reduite we can take: $X^3 + 3X^2 + 2.3 + 0.3^2$.

$$\begin{aligned}
f_2(X) &= X^3 + 3X^2 - 18X + 15 \\
&\equiv X^3 + 3X^2 + 9X + 15 \pmod{27}.
\end{aligned} \tag{3.8}$$

So, as reduite we can take: $X^3 + 3X^2 + 2.3 + 1.3^2$.

The output of the program for the case $p = 5$:

$$\begin{aligned}
f_1(X) &= X^5 + 5X^4 - 100X^3 - 375X^2 + 225X + 1145 \\
&\equiv X^5 + 5X^4 + 25X^3 + 100X + 20 \pmod{125}.
\end{aligned} \tag{3.9}$$

So, as reduite we can take: $X^5 + 5X^4 + 4.5 + 0.5^2$.

$$\begin{aligned}
f_2(X) &= X^5 + 5X^4 - 100X^3 + 175X^2 + 225X + 45 \\
&\equiv X^5 + 5X^4 + 25X^3 + 50X^2 + 100X + 45 \pmod{125}.
\end{aligned} \tag{3.10}$$

So, as reduite we can take: $X^5 + 5X^4 + 4.5 + 1.5^2$.

$$\begin{aligned}
f_3(X) &= X^5 + 5X^4 - 100X^3 - 100X^2 + 1600X + 320 \\
&\equiv X^5 + 5X^4 + 25X^3 + 25X^2 + 100X + 70 \pmod{125}.
\end{aligned} \tag{3.11}$$

So, as reduite we can take: $X^5 + 5X^4 + 4.5 + 2.5^2$.

$$\begin{aligned}
f_4(X) &= X^5 + 5X^4 - 100X^3 - 925X^2 - 2525X - 2155 \\
&\equiv X^5 + 5X^4 + 25X^3 + 75X^2 + 100X + 95 \pmod{125}.
\end{aligned} \tag{3.12}$$

So, as reduite we can take: $X^5 + 5X^4 + 4.5 + 3.5^2$.

The output of the program for the case $p = 7$:

$$\begin{aligned}
f_1(X) &= X^7 + 7X^6 - 588X^5 - 5243X^4 + 33124X^3 + 84672X^2 - 35721X - 5103 \\
&\equiv X^7 + 7X^6 + 98X^5 + 245X^4 + 196X^3 + 294X^2 + 294X + 42 \pmod{343}.
\end{aligned} \tag{3.13}$$

So, as reduite we can take: $X^7 + 7X^6 + 6.7 + 0.7^2$.

$$\begin{aligned}
f_2(X) &= X^7 + 7X^6 - 588X^5 - 2401X^4 + 33124X^3 - 54586X^2 - 35721X + 65947 \\
&\equiv X^7 + 7X^6 + 98X^5 + 196X^3 + 294X^2 + 294X + 91 \pmod{343}.
\end{aligned} \tag{3.14}$$

So, as reduite we can take: $X^7 + 7X^6 + 6.7 + 1.7^2$.

$$\begin{aligned} f_3(X) &= X^7 + 7X^6 - 588X^5 + 3283X^4 + 21756X^3 - 85848X^2 - 354025x - 280777 \\ &\equiv X^7 + 7X^6 + 98X^5 + 196X^4 + 147X^3 + 245X^2 + 294X + 140 \pmod{343}. \end{aligned} \quad (3.15)$$

So, as reduite we can take: $X^7 + 7X^6 + 6.7 + 2.7^2$.

$$\begin{aligned} f_4(X) &= X^7 + 7X^6 - 588X^5 - 980X^4 + 72912X^3 + 84672X^2 - 1517824X + 874496 \\ &\equiv X^7 + 7X^6 + 98X^5 + 49X^4 + 196X^3 + 294X^2 + 294X + 189 \pmod{343}. \end{aligned} \quad (3.16)$$

So, as reduite we can take: $X^7 + 7X^6 + 6.7 + 3.7^2$.

$$\begin{aligned} f_5(X) &= X^7 + 7X^6 - 588X^5 - 5243X^4 + 21756X^3 + 152880X^2 - 354025X - 476875 \\ &\equiv X^7 + 7X^6 + 98X^5 + 245X^4 + 147X^3 + 245X^2 + 294X + 238 \pmod{343}. \end{aligned} \quad (3.17)$$

So, as reduite we can take: $X^7 + 7X^6 + 6.7 + 4.7^2$.

$$\begin{aligned} f_6(X) &= X^7 + 7X^6 - 588X^5 - 2401X^4 + 101332X^3 + 192668X^2 - 5049009X + 4687039 \\ &\equiv X^7 + 7X^6 + 98X^5 + 147x^3 + 245X^2 + 294X + 287 \pmod{343}. \end{aligned} \quad (3.18)$$

So, as reduite we can take: $X^7 + 7X^6 + 6.7 + 5.7^2$.

Sketch of calculus:

In this Sketch, by use of the reduite, we prove the equivalence (in Krasner's sens) between two Eisenstein polynomials defining normal extensions over Q_7 , that is generating the same extension over Q_7 .

Let f_0 be the minimal polynomial (of Eisenstein) of π_0 :

$$\begin{aligned} f_0(X) &= X^7 - 42X^6 + 10584X^4 - 762048X^2 - 2286144X + 1959552 \\ &\equiv X^7 + 301X^6 + 294X^4 + 98X^2 + 294X + 336 \\ &\equiv X^7 + (7 + 6.7^2)X^6 + 294X^4 + 98X^2 + 294X + 6(7 + 7^2) \pmod{343}. \end{aligned} \quad (3.19)$$

Hence we can take as corresponding reduite of f_0 the polynomial $X^7 + 7X^6 + 6(7 + 7^2)$.

With respect to 3.4 $Q_7(\pi_0)$, is the wildly ramified subextension of $Q_7(\tau_{49})$.

On the other hand, consider the polynomial:

$$\begin{aligned} f_1(X) &= X^7 - 35X^6 + 6125X^4 - 306250X^2 - 765625X + 546875 \\ &\equiv X^7 + 308X^6 + 294X^4 + 49X^2 + 294X + 133 \\ &\equiv X^7 + 2(7 + 3.7^2)X^6 + 294X^4 + 49X^2 + 294X + (5.7 + 2.7^2) \pmod{343}. \end{aligned} \quad (3.20)$$

and call π_1 a root of it. Since 4 is the inverse of 2 modulo 7, write $\pi_2 = 4\pi_1$ and let f_2 be the minimal polynomial of π_2 over Q_7 , we have:

$Tr(\pi_1) = 35$, and $Tr(\pi_2) = 4Tr(\pi_1) = 140 \equiv 42 \equiv -7 \pmod{7^2}$, where $Tr(\cdot)$ is the trace with

respect to Q_7 .

Furthermore we have:

$N(\pi_1) = -546875$, and $N(\pi_2) = 4^7 N(\pi_1)$, so $N(\pi_2) \equiv (16384)N(\pi_1) \equiv -263.133 \equiv 7 \pmod{7^3}$, that is: $-N(\pi_2) \equiv 336 \equiv 6(7 + 7^2) \pmod{7^3}$, where $N(\cdot)$ is the norm with respect to Q_7 .

In consequence the reduite relative to f_2 is $X^7 + 7X^6 + 6(7 + 7^2)$.

f_0 and f_2 having the same reduite, hence we can deduce that they are equivalent that is

$$Q_7(\pi_0) = Q_7(\pi_2) = Q_7(\pi_1).$$

Acknowledgment:

I thank the referee very much for his important remarks as well as the staff of Scientiae Mathematicae Japonicae for the care they have taken to achieve the publication of this article.

REFERENCES

- [1] N. KOBLIZ..... P-adic Numbers, P-adic Analysis and Zeta functions.
Second edition 1984
Springer Verlag, Berlin, Newyork,
- [2] M.KRASNER..... Sur la primitivité des corps p-adiques, Mathematica Cluj 13
(1937) pages 72-191
- [3] A. LBEKKOURI..... On the construction of normal wildly ramified extensions
over Q_p $p \neq 2$, Arch. Math. 93 (2009), 331-344
- [4] I.R.SAFAREVIC..... On p-extensions, Amer. Math. Soc. Transl. (2) 4.(1954)
- [5] O. ORE..... Abriss einer arithmetischen Theorie der galoischen
Körper, Teil 1, Math. Annalen 100 (1928) pages 650-673
- [6] O. ORE..... Abriss einer arithmetischen Theorie der galoischen
Teil 2, Math. Annalen 102 (1930) pages 283-304
- [7] J.P. SERRE..... Local fields, Springer 1979

communicated by *Noburo Ishii*

Retiring professor/ BP : 10507 Casa-Bandoeng 20002 Casablanca - Morocco

E – mail : lbekkouri_akram1@hotmail.com