JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Maurizio MONGE

A characterization of Eisenstein polynomials generating extensions of degree p^2 and cyclic of degree p^3 over an unramified $\mathfrak{p}$-adic field

Tome 26, n$^{\text{o}}$ 1 (2014), p. 201-231.

<http://jtnb.cedram.org/item?id=JTNB_2014__26_1_201_0>

Journal de Théorie des Nombres
de Bordeaux **26** (2014), 201–231

A characterization of Eisenstein polynomials generating extensions of degree p^2 and cyclic of degree p^3 over an unramified $\mathfrak{p}$-adic field

par Maurizio MONGE

Résumé. Soit $p \neq 2$ un nombre premier. Nous obtenons une technique basée sur la théorie du corps de classes local et sur les développements de certains résultants qui permet de retrouver très facilement la caractérisation de Lbekkouri des polynômes d'Eisenstein qui génèrent une extension cyclique totalement ramifiée de degré p^2 sur $\mathbb{Q}_p$, et de l'étendre au cas de corps de base K qui est une extension non ramifiée de $\mathbb{Q}_p$.

Quand un polynôme satisfait un sous-ensemble de ces conditions, la première condition insatisfaite caractérise le groupe de Galois de la clôture normale. Nous obtenons une classification complète des polynômes d'Eisenstein de degré p^2 dont le corps de décomposition est une p-extension, fournissant une description complète du groupe de Galois et de ses sous-groupes de ramification.

Les mêmes méthodes sont utilisées pour donner une caractérisation des polynômes d'Eisenstein de degré p^3 qui génèrent une extension cyclique.

Dans la dernière section, on en déduit une interprétation combinatoire des fonctions symétriques monômiales évaluées aux racines de l'unité, qui apparaissent dans certains développements.

Abstract. Let $p \neq 2$ be a prime. We derive a technique based on local class field theory and on the expansions of certain resultants allowing to recover very easily Lbekkouri's characterization of Eisenstein polynomials generating cyclic wild extensions of degree p^2 over $\mathbb{Q}_p$, and extend it to when the base fields K is an unramified extension of $\mathbb{Q}_p$.

When a polynomial satisfies a subset of such conditions the first unsatisfied condition characterizes the Galois group of the normal closure. We derive a complete classification of Eisenstein polynomials of degree p^2 whose splitting field is a p-extension, providing a full description of the Galois group and its higher ramification subgroups.

Manuscrit reçu le 15 octobre 2012, révisé le 6 juillet 2013, accepté le 3 septembre 2013.
Classification math. 11S05, 11S15.

The same methods are used to give a characterization of Eisenstein polynomials of degree p^3 generating a cyclic extension.

In the last section, we deduce a combinatorial interpretation of monomial symmetric functions evaluated in the roots of the unity, which appear in certain expansions.

1. Introduction

In this paper we introduce a technique which can be used to deduce necessary and sufficient conditions on the coefficients of an Eisenstein polynomial over a $\mathfrak{p}$-adic field for the Galois group of the splitting field to be a prescribed group, when the field is an unramified extension of $\mathbb{Q}_p$ and the polynomial has degree p^2 or p^3. Even when not explicitly stated, the residual characteristic p will always be assumed $\neq 2$.

In [Lbe09], Lbekkouri gave a list of congruence conditions for the coefficients of Eisenstein polynomials of degree p^2 with coefficients in the rational $\mathfrak{p}$-adic field $\mathbb{Q}_p$, and these conditions are satisfied if and only if the generated extension is Galois. Since the multiplicative group $U_{1,\mathbb{Q}_p}$ of 1-units of $\mathbb{Q}_p$ has rank 1 as $\mathbb{Z}_p$-module, and in particular ${}^{U_{1,\mathbb{Q}_p}(\mathbb{Q}_p^\times)^p}\!/\!{}_{(\mathbb{Q}_p^\times)^p} \cong {}^{\mathbb{Z}}\!/\!{}_{p\mathbb{Z}}$, we have by local class field theory that every Galois totally ramified extension of degree p^2 over $\mathbb{Q}_p$ is cyclic. Consequently when the base field is $\mathbb{Q}_p$ the problem is reduced to finding conditions for Eisenstein polynomials of degree p^2 to generate a cyclic extension.

If the base field K is a proper extension of $\mathbb{Q}_p$ a Galois extension of degree p^2 may not be cyclic, so the restriction of considering polynomials that generate cyclic extensions has to be added explicitly. If K is ramified over $\mathbb{Q}_p$ the bare characterization of the possibilities for upper ramification breaks is a non-trivial problem (see [Mau71, Mik81]) and the problem seems to be very difficult for a number of other reasons, so we will only consider fields K that are finite unramified extensions over $\mathbb{Q}_p$, with residual degree $f = f(K/\mathbb{Q}_p) = [K : \mathbb{Q}_p]$. In this setting the problem is still tractable without being a trivial generalization of the case over $\mathbb{Q}_p$, and we will show a technique allowing to handle very easily the case of degree p^2.

When studying the norm map of a wildly ramified extension L/K generated by an Eisenstein polynomial, the Artin-Hasse exponential function comes into play, and we use it to clarify the connection between the image of the norm map and the coefficients of the generating Eisenstein polynomial.

While some of the conditions we deduce are necessary for the splitting field to be a p-extension, the remaining conditions can be tested in their order on a candidate polynomial, and the first one that fails gives information on the Galois group of the splitting field. Taking into account another family of polynomials that can never provide a cyclic extension of degree

p^2, we give a full classification of the polynomials of degree p^2 whose normal closure is a p-extension, providing a complete description of the Galois group of the normal closure with its ramification filtration. See [Cap07] for an abstract classification of all such extensions when the base field is $\mathbb{Q}_p$.

The same methods apply to characterize Eisenstein polynomials of degree p^3 generating a cyclic extension. In this case the characterization is substantially more complicated, but the strategy used in degree p^2 can still be applied in a relatively straightforward way. It should be quite easy to apply the same methods to other abelian groups, and should even be possible to obtain a characterization for some non-abelian group.

In the last section we give a combinatorial interpretation of certain sums of roots of the unity appearing during the proof, it is actually more general than what is needed in the present paper, but it has some interest on its own.

Overview on the general strategy. We give here an overview of our strategy for deducing conditions on coefficients of generating Eisenstein polynomials. Let K be a p-adic field that is unramified over $\mathbb{Q}_p$, $p \neq 2$, so that p is a uniformizing element of K. Let $f(T)$ be an Eisenstein polynomial of degree n say, and π be a root in a fixed algebraic closure. Let $L = K(\pi)$ be the extension generated by π over K.

Let G be an abelian group of order n equal to the degree $[L : K]$. By local class field theory the totally ramified extension L/K is Galois with group isomorphic to G if and only if $N_{L/K}(U_L)$ has index n in U_K, and quotient $U_K/N_{L/K}(U_L)$ isomorphic to G. When n is a power of p the groups U_K and U_L can be replaced with the 1-units $U_{1,K}$ and $U_{1,L}$, so we only need to check whether $U_{1,K}/N_{L/K}(U_{1,L})$ is isomorphic to G.

When G is a cyclic group of order p^k, it turns out that $N = N_{L/K}(U_{1,L})$ should have a special form. In particular, $U_{1,K}/N$ is cyclic of order p^k if and only if there exists a subgroup $V \subseteq \mathcal{O}_k$ that is the preimage of a $\mathbb{F}_p$-subspace $\bar{V}$ of codimension 1 in κ_K (with respect to the canonical projection $\mathcal{O}_k \to \kappa_k$), and

(1) $(N \cap U_{i,K}) \subseteq 1 + p^i V$, for all $1 \leq i \leq k$,
(2) $N \supseteq U_{k+1,K}$.

Note also that if $(U_K : N) \leq n$, then the last condition is automatically satisfied. A similar characterization is possible for general abelian p-groups, but here we will restrict to the case of cyclic group.

If the first condition is verified for $i = 1$, then $N \mod \mathfrak{p}_K^2$ is already sufficient to determine uniquely V. So if N has the requested form for a suitable V, to test whether U_K/N is cyclic of order p^k we can verify whether $N \cap U_{i,K} \subset 1 + p^i V$ for $2 \leq i \leq k$. We will test this condition on $N = N_{L/K}(U_{1,L})$, for an extension L/K.

By the structure of the norm map over local fields (see [FV02, Chap. 3, §3, Prop. 3.1]), we have that if $j = \psi_{L/K}(k)$, then $N_{L/K}(U_{j+1,L}) \subseteq U_{k+1,K}$. Since the above conditions are all stated modulo $U_{k+1,K}$, we can just consider the subgroup of $U_{1,K}/U_{k+1,K}$ generated by elements $N_{L/K}(\alpha_m)$, for a set α_m of generators of $U_{1,L}/U_{j+1,L}$. If each combination that belongs to $U_{i,K}$ turns out to be also in $1 + p^iV$, then the extension is verified to be Galois with group G.

A suitable set of generator is formed by the elements of the form $1+\theta\pi^m$ with $(m,p) = 1$ and $\theta \in U_K$. Consider the group generated by their norms in $U_{1,K}/U_{k+1,K}$. Each norm $N_{K(\pi)/K}(1+\theta\pi^m)$ can be expressed as function of the coefficients of the minimal polynomial of $f(T)$, and in principle the constraints on the structure of $N/U_{k+1,K}$ can be translated into conditions on the coefficients of $f(T)$.

Unluckily the norms $N_{K(\pi)/K}(1+\theta\pi^m)$ have a quite complicated expression in terms of the coefficients. Let $E(x)$ be the Artin-Hasse exponential function, then the elements of the form $E(\theta\pi^m)$ give an alternative set of generators of $U_{1,L}/U_{j+1,L}$, and it turns out that their norms can be expressed rather easily in terms of the coefficients of $f(T)$.

This method can be extended to classify completely the polynomials of degree p^2 whose splitting field is p-extension. In degree p^2, a subset of the condition on the coefficients for the extension to be cyclic will be shown to be equivalent to be satisfied if and only if L/K is decomposable in a double cyclic extension; that is, there exists an intermediate extension F such that L/F and F/K are cyclic of degree p.

This condition is verified if an only if the Galois closure is a p-extension, and the group of the normal closure $\tilde{L}$ satisfies the exact sequence

$$1 \to \mathrm{Gal}(\tilde{L}/F) \to \mathrm{Gal}(\tilde{L}/K) \to \mathrm{Gal}(F/K) \to 1.$$

$\mathrm{Gal}(\tilde{L}/F)$ is a cyclic and indecomposable $\mathrm{Gal}(F/K)$-module of length $\leq p$, and the isomorphism class of the group $\mathrm{Gal}(\tilde{L}/F)$ is identified by the length of $\mathrm{Gal}(\tilde{L}/F)$ as $\mathrm{Gal}(F/K)$-module, and by its exponent (see [MS05, Wat94]).

If K is unramified over $\mathbb{Q}_p$, it turns out that the ramification breaks coincide with those of a cyclic extension of degree p^2 only when $\mathrm{Gal}(\tilde{L}/K)$ has exponent p^2, so under suitable ramification hypotheses the exponent is easily determined. Furthermore, after requesting $N \cap U_{1,K} \subseteq 1 + pV$, the other conditions that characterize the polynomials with group isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ allow more in general to recover the biggest i (if any) such that the condition $N_{L/K}(U_{i,L}) \cap U_{2,K} \subseteq 1 + p^2V$ fails. This i can be related to the length of $\mathrm{Gal}(\tilde{L}/F)$, applying the functorial properties of the reciprocity map.

When L has a suitable intermediate extension, but the ramification breaks do not coincide with those of a cyclic extension, then the problem turns out to be slightly easier, because $\mathrm{Gal}(\tilde{L}/K)$ is always a semidirect product, and the ramification data give almost complete information about the group. In this way we obtain a characterization of all polynomials of degree p^2 whose Galois group is a p-group.

2. Preliminaries

Let K be a $\mathfrak{p}$-adic field, $p \neq 2$. As usual we will denote with $[K^\times]_K$ the group of p-th power classes ${}^{K^\times}\!/\!{}_{(K^\times)^p}$. For integers a, b, we will denote by $[\![a, b]\!]$ the set of integers $a \leq i \leq b$ such that $(i, p) = 1$.

We start computing modulo which power of p an Eisenstein polynomial identifies uniquely the extension it generates (this computation is very well known, see [Kra62] for example): let $f(X) = \sum_{i=0}^{n} f_{n-i} X^i$ and $g(X) = \sum_{i=0}^{n} g_{n-i} X^i$ be Eisenstein polynomials of degree n say, ρ a root of g, $\pi = \pi_1, \pi_2, \ldots$ the roots of f, with π the nearest one to ρ, and put $L = K(\pi)$. Let v be the biggest lower ramification break and $\mathscr{D}_f = f'(\pi)$ be the different, if

$$\left|(f_{n-i} - g_{n-i})\pi^i\right| < \left|\pi^{v+1}\mathscr{D}_f\right|$$

for each $0 \leq i \leq n$, then being

$$f(\rho) = f(\rho) - g(\rho) = \sum_{i=0}^{n} (f_{n-i} - g_{n-i})\, \rho^i$$

we obtain $|f(\rho)| < |\pi^{v+1}\mathscr{D}_f|$. We have

$$\left|(\rho - \pi) \cdot \prod_{i=2}^{n} (\pi - \pi_i)\right| \leq \left|\prod_{i=1}^{n} (\rho - \pi_i)\right| < \left|\pi^{v+1}\mathscr{D}_f\right|,$$

because $|\pi - \pi_i| \leq |\rho - \pi_i|$ for $i \geq 2$, being π the root of f that is nearest to ρ. Consequently $|\rho - \pi| < |\pi^{v+1}|$, which is equal to the minimum of the $|\pi - \pi_i|$, and hence $K(\pi) \subseteq K(\rho)$ by Krasner's lemma, and $K(\rho) = K(\pi)$ having the same degree.

Ramification breaks. Let now K be unramified over $\mathbb{Q}_p$, then $U_{1,K}^{p^i} = U_{i+1,K}$, and consequently by local class field theory the upper ramification breaks of a cyclic p-extension are $1, 2, 3, \ldots$, and the lower ramification breaks are $1, p + 1, p^2 + p + 1, \ldots$.

For an extension of degree p^k having exactly k lower ramification breaks $t_0 < t_1 < \cdots < t_{k-1}$ we can compute $v_L(\mathscr{D}_{L/K})$ as $\sum_{i=1}^{k} (p^i - p^{i-1}) t_{k-i}$, which for a cyclic L/K of degree p^2 or p^3 is $3p^2 - p - 2$ (resp. $4p^3 - p^2 - p - 2$), while $v_L(\pi^{v+1}\mathscr{D}_{L/K})$ is respectively $3p^2 = v_L(p^3)$ and $4p^3 = v_L(p^4)$. Hence we obtain the condition on the precision of the coefficients, which we state in a proposition for convenience:

Proposition 2.1. *Let L/K be a totally ramified cyclic extension of degree $n = p^2$ (resp. $n = p^3$) determined by the Eisenstein polynomial $f(X) = \sum_{i=0}^{n} f_{n-i}X^n$. Then the lower ramification breaks are $1, p+1$ (resp. $1, p+1, p^2+p+1$), $v_L(\mathscr{D}_{L/K})$ is equal to $3p^2-p-2$ (resp. is $4p^3-p^2-p-2$), and the extension is uniquely determined by the classes of $f_n \pmod{p^4}$ and $f_i \pmod{p^3}$ for $0 \le i < n$ (resp. by the classes of $f_n \pmod{p^5}$ and $f_i \pmod{p^4}$ for $0 \le i < n$, for $n = p^3$).*

2.1. Additive polynomials. We will need a few facts about additive polynomials, and in particular formulæ to express in terms of the coefficients that an additive polynomial has range contained in the range of another additive polynomial. We resume what we need in the following

Proposition 2.2. *Let $A(Y) = a_pY^p + a_1Y$ be an additive polynomial in $\kappa_K[Y]$ such that $A'(0) \neq 0$ and all the roots of $A(Y)$ are in κ_K, and let $B(Y) = b_pY^p + b_1Y$, $C(Y) = c_{p^2}Y^{p^2} + c_pY^p + c_1Y$ and $D(Y) = d_{p^3}Y^{p^3} + d_{p^2}Y^{p^2} + d_pY^p + d_1Y$ be any three other additive polynomials in $\kappa_K[Y]$. Then*

- *$B(\kappa_K) \subseteq A(\kappa_K)$ if and only if $b_p = a_p({}^{b_1}/{}_{a_1})^p$, and in this case $B(Y)$ is equal to $A({}^{b_1}/{}_{a_1}Y)$,*
- *$C(\kappa_K) \subseteq A(\kappa_K)$ if and only if $c_p = a_p({}^{c_1}/{}_{a_1})^p + a_1({}^{c_{p^2}}/{}_{a_p})^{1/p}$, and in this case $C(Y)$ can be written as $A(\beta Y^p + {}^{c_1}/{}_{a_1}Y)$ with $\beta = ({}^{c_{p^2}}/{}_{a_p})^{1/p}$ or equivalently $\beta = {}^{c_p}/{}_{a_1} - {}^{a_p}/{}_{a_1}({}^{c_1}/{}_{a_1})^p$.*
- *$D(\kappa_K) \subseteq A(\kappa_K)$ if and only if ${}^{a_1}/{}_{a_p}({}^{d_{p^3}}/{}_{a_p})^{1/p} + ({}^{d_p}/{}_{a_1})^p = {}^{d_{p^2}}/{}_{a_p} + ({}^{a_p}/{}_{a_1})^p({}^{d_1}/{}_{a_1})^{p^2}$.*

Note that being κ_K finite and hence perfect the map $x \mapsto x^p$ is an automorphism, and we just denote by $x \mapsto x^{1/p}$ the inverse automorphism.

Proof. Since $A'(0) \neq 0$ and all the roots of $A(Y)$ are in κ_K we have from the theory of additive polynomials (see [FV02, Chap. 5, §2, Corollary 2.4]) that if $B(\kappa_K) \subseteq A(\kappa_K)$ then $B(Y) = A(G(Y))$ where $G(Y)$ is an additive polynomial, which will be linear considering the degrees, $G(Y) = \alpha Y$ say. Consequently it has to be $B(Y) = a_p\alpha^pY^p + a_1\alpha Y$, and comparing the coefficients we obtain that $\alpha^p = ({}^{b_1}/{}_{a_1})^p$ and should also be equal to ${}^{b_p}/{}_{a_p}$. Similarly if $C(\kappa_K) \subseteq A(\kappa_K)$ it can be written as

$$C(Y) = A(\beta Y^p + \alpha Y) = a_p\beta^pY^{p^2} + (a_p\alpha^p + a_1\beta)Y^p + a_1\alpha Y,$$

and we deduce $\alpha = {}^{c_1}/{}_{a_1}$, $\beta^p = {}^{c_{p^2}}/{}_{a_p}$; and we obtain the condition substituting α, β in $c_p = a_p\alpha^p + a_1\beta$. If $D(\kappa_K) \subseteq A(\kappa_K)$ then $D(Y)$ has to be of the form $A(\gamma Y^{p^2} + \beta Y^p + \alpha Y)$ and hence

$$a_p\gamma^pY^{p^3} + (a_p\beta^p + a_1\gamma)Y^{p^2} + (a_p\alpha^p + a_1\beta)Y^p + a_1\alpha Y,$$

$\alpha = {}^{d_1}/_{a_1}$, $\gamma = ({}^{d_{p^3}}/_{a_p})^{1/p}$, and β^p can be written in two different ways as

$$ {}^{d_{p^2}}/_{a_p} - {}^{a_1}/_{a_p}({}^{d_{p^3}}/_{a_p})^{1/p} = ({}^{d_p}/_{a_1} - {}^{a_p}/_{a_1}({}^{d_1}/_{a_1})^p)^p. $$

The condition is clearly also sufficient. □

The following proposition will also be useful. It gives a criterion to verify if the splitting field of an additive polynomial of degree p^2 is a p-extension (that is, either trivial, or cyclic of degree p), which is slightly easier to test than the condition itself.

Proposition 2.3. *Let $A(Y) = Y^{p^2} + aY^p + bY$ be an additive polynomial in $\kappa_K[Y]$, than the splitting field is a p-extension over κ_K precisely when $A(Y)$ has a root in $\kappa_K^\times$, and $b \in (\kappa_K^\times)^{p-1}$.*

Proof. If the Galois group is a p-group then any non-trivial orbit has cardinality divisible by p, and the action on the roots of $A(Y)$ should have a fixed point other than 0, $\eta \in \kappa_K^\times$ say. If $\beta = \eta^{p-1}$ then the roots of $Y^p - \beta Y$ are a subset of the roots of $A(Y)$. Consequently by [FV02, Chap. 5, §2, Prop. 2.5] $A(Y)$ can be expressed as $B(Y^p - \beta Y)$ for some additive polynomial $B(Y)$, which has to be monic too, $B(Y) = Y^p - \alpha Y$ say. The roots of $B(Y)$ have to be in κ_K or it, and hence $A(Y)$, would generate an extension of order prime with p, and consequently α has to be in $(\kappa_K^\times)^{p-1}$, and $b = \alpha\beta \in (\kappa_K^\times)^{p-1}$ as well.

In the other hand if a root η is in κ_K we can write $A(Y) = B(Y^p - \beta Y)$ for $\beta = \eta^{p-1}$, and replacing Y by ηZ we can consider $B(\eta^p(Z^p - Z))$, and the generated extension is an Artin-Schreier extension over the extension determined by $B(Y)$. Consequently we only need the extension determined by $B(Y)$ to be trivial, and this condition is verified precisely when $b \in (\kappa_K^\times)^{p-1}$. □

2.2. Sum of roots of the unity. Let ζ_ℓ be a primitive ℓ-th root of the unity for some $\ell \geq 1$ (in any suitable field of characteristic 0), we define for each tuple $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r)$ of r integers the sum

$$ \Sigma_\lambda(\ell) = \sum_{\iota = (\iota_1, \dots, \iota_r)} \zeta_\ell^{\iota_1\lambda_1 + \iota_2\lambda_2 + \dots + \iota_r\lambda_r}, $$

where the sum ranges over all the r-tuples $\iota = (\iota_1, \dots, \iota_r)$ such that $0 \leq \iota_i \leq \ell - 1$ for each i, and the ι_i are all different.

We deduce some property of the sums $\Sigma_\lambda(\ell)$ to help expanding the expressions that will appear. For each $\lambda = (\lambda_1, \lambda_2, \dots)$ and integer k put $k\lambda$ for the tuple $(k\lambda_1, k\lambda_2, \dots)$. For integers ℓ, k, m let's define the functions

$$ \delta_{\ell,k}^{[m]} = \begin{cases} \ell & \text{if } \ell \geq m \text{ and } \ell \mid k, \\ 0 & \text{in any other case,} \end{cases} $$

and put $\delta_{\ell,k} = \delta_{\ell,k}^{[1]}$ for short. Then we have

Proposition 2.4. *Assume $(\ell,p)=1$, $\ell>1$. For each tuple λ we have $\Sigma_{p\lambda}(\ell)=\Sigma_{\lambda}(\ell)$. For $k\geq 1$ we have $\Sigma_{(k)}(\ell)=\delta_{\ell,k}$, and $\Sigma_{(k,1)}(\ell)=\delta^{[2]}_{\ell,k+1}$, and if $(k,p)=1$ we also have $\Sigma_{(k,p)}(\ell)=\delta^{[2]}_{\ell,k+p}$ and $\Sigma_{(k,p^2)}(\ell)=\delta^{[2]}_{\ell,k+p^2}$. Furthermore we have $\Sigma_{(1,1,1)}(\ell)=\delta^{[3]}_{\ell,3}$, $\Sigma_{(p,1,1)}(\ell)=\delta^{[3]}_{\ell,p+2}$ and $\Sigma_{(p,p,1)}(\ell)=\delta^{[3]}_{\ell,2p+1}$.*

The proof can be obtained via an easy computation, but we omit it being also an immediate consequence of the more general Lemma 6.1 proved in the last section.

3. Polynomials of degree p^2 generating a cyclic extension

3.1. Conditions on the valuations of coefficients. We deduce now the necessary conditions on the valuations of coefficients for the Galois group to be cyclic of order p^2. Let as above f be an Eisenstein polynomial of order p^2 with coefficients in K unramified over $\mathbb{Q}_p$, $p\neq 2$, π a root in the algebraic closure and $L=K(\pi)$.

By Prop. 2.1 the different $f'(\pi)$ has L-valuation equal to $3p^2-p-2$, so in the expression of $f'(\pi)$ the valuation comes from a term $f_{p+1}X^{p^2-p-1}$ with $v_p(f_{p+1})=2$, we must have $v_p(f_i)\geq 2$ for all $(i,p)=1$, and $v_p(f_i)\geq 3$ if furthermore $i>p+1$.

Since the first ramification break is at 1, coefficient of X^p in the ramification polynomial $f(X+\pi)$ needs to have L-valuation equal to $(p^2-p)\cdot 2=2p^2-2p$ (because p^2-p roots of $f(X+\pi)$ have L-valuation 2). A monomial $f_{p^2-i}(X+\pi)^i$ contributes at most one term $\binom{i}{p}f_{p^2-i}\pi^{i-p}X^p$ in X^p; the valuations of these terms have different remainders modulo the degree p^2, and consequently the smallest valuation of the $\binom{i}{p}f_{p^2-i}\pi^{i-p}$ has to be $2p^2-2p$. The minimum is achieved for $i=p^2-p$ and we must have $v_p(f_p)=1$, while $v_p(f_{pk})\geq 2$ for all $2\leq k\leq p-1$.

We have deduced the following

Condition 3.1. *We must have*

- $v_p(f_p)=1$, *and* $v_p(f_{pi})\geq 2$ *for* $i\in[\![2,p-1]\!]$,
- $v_p(f_i)\geq 2$ *for* $i\in[\![1,p-1]\!]$, $v(f_{p+1})=2$ *and* $v_p(f_i)\geq 3$ *for* $i\in[\![p+2,p^2-1]\!]$.

Turning to 0 all the f_i divisible by p^3 for $i\neq p^2$, a change that preserves the generated extension by Prop. 2.1, $f(X)$ can be written as

(3.1)
$$f(X)=X^{p^2}+\underbrace{f_pX^{p^2-p}+f_{p^2}}_{\overset{\cap}{p\mathcal{O}[X]}}+\underbrace{\sum_{j\in[\![2,p-1]\!]}f_{pj}X^{p^2-pj}+\sum_{k\in[\![1,p+1]\!]}f_kX^{p^2-k}}_{\overset{\cap}{p^2\mathcal{O}[X]}}.$$

3.2. Conditions on the norms of units. Let L be the extension generated by a root π of the polynomial $f(X)$, by local class field theory it is a totally ramified abelian extension precisely when $N_{L/K}(L^\times) \cap U_{1,K} = N_{L/K}(U_{1,L})$ has index p^2 in $U_{1,K}$ and the corresponding quotient is cyclic.

Because $U_{i+1,K} = U_{1,K}^{p^i}$ for each $i \geq 1$, to have a cyclic extension $N_{L/K}(U_{1,L})U_{2,K}$ must have index p in $U_{1,K}$, and $N_{L/K}(U_{1,L}) \cap U_{2,K}$ index p in $U_{2,K}$.

For each $i \geq 0$ we have a natural map $(\times p) : {}^{\mathfrak{p}_K^i}\!/\!_{\mathfrak{p}_K^{i+1}} \to {}^{\mathfrak{p}_K^{i+1}}\!/\!_{\mathfrak{p}_K^{i+2}}$ induced by multiplication by p, and for $i \geq 1$ being $(1+\theta p^i)^p = 1 + \theta p^{i+1} + \mathcal{O}(p^{i+2})$ we have a natural map $(\uparrow p) : {}^{U_{i,K}}\!/\!_{U_{i+1,K}} \to {}^{U_{i+1,K}}\!/\!_{U_{i+2,K}}$ induced by taking p-th powers. The diagram

$$\begin{tikzcd} \mathfrak{p}_K^i/\mathfrak{p}_K^{i+1} \arrow[r, "\times p"] \arrow[d, "\mu_i"'] & \mathfrak{p}_K^{i+1}/\mathfrak{p}_K^{i+2} \arrow[d, "\mu_{i+1}"'] \\ U_{i,K}/U_{i+1,K} \arrow[r, "\uparrow p"] & U_{i+1,K}/U_{i+2,K} \end{tikzcd} , \tag{3.2}$$

where μ_i is induced by $x \mapsto 1 + x$, is commutative.

So if the quotient is cyclic of order p^2 then $N_{L/K}(U_{1,L}) \cap U_{2,K}$ will certainly contain $N_{L/K}(U_{1,L})^p U_{3,K}$, which has index p in $U_{2,K}$, and consequently has to be equal to it. For L/K to be Galois cyclic we need

$$N_{L/K}(U_{1,L}) \subseteq 1 + pV, \qquad N_{L/K}(U_{1,L}) \cap U_{2,K} \subseteq 1 + p^2 V \tag{3.3}$$

for some $V \subset \mathcal{O}_K$ that is preimage of an $\mathbb{F}_p$-subspace of ${}^{\mathcal{O}_K}\!/\!_{\mathfrak{p}_K}$ of codimension 1. Note that V is uniquely determined by $N_{L/K}(U_{1,L})U_{2,K}$ as a subgroup of $U_{1,K}$.

If $i \geq 1$ then $N_{L/K}(U_{i+1,L}) \subseteq U_{\phi_{L/K}(i)+1,K}$ (see [FV02, Chap. 3, §3.3 and §3.4], like in [FV02] we put $U_{x,K} = U_{\lceil x \rceil,K}$ when x is not an integer), in our case this amounts to $N_{L/K}(U_{2,L}) \subseteq U_{2,K}$ and $N_{L/K}(U_{p+2,L}) \subseteq U_{3,K}$.

Consequently, when the correct ramification hypotheses are verified, the extension L/K of degree p^2 will be cyclic if and only if

(1) given a set of elements whose images generate ${}^{U_{1,L}}\!/\!_{U_{2,L}}$, their norms are contained in $1 + pV$ for $V \subset \mathcal{O}_K$ as above, and
(2) given a set of elements whose reduction modulo $U_{p+2,L}$ generates ${}^{U_{1,L}}\!/\!_{U_{p+2,L}}$, each x obtained as combination of said elements and such that $N_{L/K}(x) \in U_{2,K}$ satisfies $N_{L/K}(x) \in 1 + p^2 V$.

3.3. Expression of norms of units. We will take as (redundant) generators of ${}^{U_{1,L}}\!/\!_{U_{p+1,L}}$ the elements of the form $(1 - \theta\pi^\ell)$ for $\ell \in [\![1, p+1]\!]$, plus those of the forms $(1 - \theta\pi)^p$, for $\theta \in \mathcal{O}_K^\times$ that are multiplicative representatives. The generators of the form $(1 - \theta\pi)^p$ can be discarded from the check, considering that we are already requesting $N_{L/K}(1-\theta\pi)\in 1+pV$, so their norm is certainly in $1+p^2V$.

The norm of an element of the form $1-\theta\pi^\ell$ can be expressed as

$$N_{L/K}(1-\theta\pi^\ell)=\prod_{\pi_i|f(\pi_i)=0}(1-\theta\pi_i^\ell)=\mathrm{Res}_X(1-\theta X^\ell,f(X)),$$

where π_i are the roots of $f(X)$ and we denote by Res_X the resultant in X.

For a polynomial $a(X)$ of degree d let's denote by $\tilde{a}(X)$ the conjugate polynomial $X^d a(X^{-1})$. Then for each pair of polynomials $a(X),b(X)$ we have $Res_X(a(X),b(X))=Res_X(\tilde{b}(X),\tilde{a}(X))$.

Consequently $N_{L/K}(1-\theta\pi^\ell)$ can also we written as

$$\mathrm{Res}_X(\tilde{f}(X),X^\ell-\theta)=\prod_{i=0}^{\ell-1}\tilde{f}(\zeta_\ell^i\theta^{1/\ell})$$

for some primitive ℓ-th root of the unity. Expanding of the right hand side, only integral powers of θ will appear, being invariant under the substitution $\theta^{1/\ell}\to\zeta_\ell\theta^{1/\ell}$. In the same way while the terms in the expression belong to $K(\zeta_\ell)$, the result is always in K, and the above expansion should be regarded as a combinatorial trick.

Let's put $T=\theta^{1/\ell}$ and consider it as an indeterminate. From the expression of $f(X)$ in the (3.1), $N_{L/K}(1-\theta\pi^\ell)$ can be expanded as

$$\prod_{i=0}^{\ell-1}\left(1+\underbrace{f_p\zeta_\ell^{ip}T^p+f_{p^2}\zeta_\ell^{ip^2}T^{p^2}}_{\substack{\pitchfork\\ \mathfrak{p}_K}}+\underbrace{\sum_{j\in[\![2,p-1]\!]}f_{pj}\zeta_\ell^{ipj}T^{pj}+\sum_{k\in[\![1,p+1]\!]}f_k\zeta_\ell^{ik}T^k}_{\substack{\pitchfork\\ \mathfrak{p}_K^2}}\right).$$

For each tuple $\lambda=(\lambda_1,\lambda_2,\dots,\lambda_r)$ of r integers put $f_\lambda T^{|\lambda|}$ for the term $\prod_{i=1}^r f_{\lambda_i}T^{\lambda_i}$, that can appear in the expansion of the above product. For each $k\geq 0$ let $m_k(\lambda)$ denote the number of parts λ_i equal to k.

In the term $f_\lambda T^{|\lambda|}$, the coefficient f_k appears at the $m_k(\lambda)$-th power. Such $m_k(\lambda)$ coefficients come from $m_k(\lambda)$ factors of product, and in the i-th factor f_kT^k has a coefficient ζ_ℓ^{ik}, if present. Consequently the coefficient of $f_\lambda T^{|\lambda|}$ in the expansion can be computed over all the ways we can partition the $1,\zeta_\ell,\zeta_\ell^2,\dots$ in sets I_k of cardinality $m_k(\lambda)$, for $k\geq 0$, and computing the sum of $\prod_{k\geq 0,x\in I_k}x^k$, over all possible choices. Note that while computing

$$\Sigma_\lambda(\ell)=\sum_{\iota=(\iota_1,\dots,\iota_r)}\zeta_\ell^{\iota_1\lambda_1+\iota_2\lambda_2+\dots+\iota_r\lambda_r},$$

the $m_k(\lambda)$ parts of λ equal to k correspond to factors of the form $\prod_{x\in I_k}x^k$, and we have one such factor for each *ordered* choice of $m_k(\lambda)$ elements of $1, \zeta_\ell, \zeta_\ell^2, \dots$. Consequently the coefficient of $f_\lambda T^{|\lambda|}$ in the expansion is exactly $\frac{1}{\prod_{k\geq 1} m_k(\lambda)!} \cdot \Sigma_\lambda(\ell)$.

In particular, discarding the terms with valuation ≥ 3 and subtracting 1, the above product can be expanded modulo p^3 as

$$\begin{array}{l} \mathfrak{p}_K \ni \left[\qquad \Sigma_{(p)}(\ell) \cdot f_p T^p + \Sigma_{(p^2)}(\ell) \cdot f_{p^2} T^{p^2} \right. \\ \mathfrak{p}_K^2 \ni \left[\begin{array}{l} +\frac{1}{2}\Sigma_{(p,p)}(\ell) \cdot f_p^2 T^{2p} + \Sigma_{(p^2,p)}(\ell) \cdot f_p f_{p^2} T^{p^2+p} + \frac{1}{2}\Sigma_{(p^2,p^2)}(\ell) \cdot f_{p^2}^2 T^{2p^2} \\ \qquad + \sum\limits_{j\in[\![2,p-1]\!]} \left(\Sigma_{(pj)}(\ell) \cdot f_{pj} T^{pj}\right) + \sum\limits_{k\in[\![1,p+1]\!]} \left(\Sigma_{(k)}(\ell) \cdot f_k T^k\right), \end{array} \right. \end{array}$$

which applying Prop. 2.4 can be rewritten as

$$\begin{array}{l} \mathfrak{p}_K \ni \left[\qquad \delta_{\ell,1} f_p T^p + \delta_{\ell,1} f_{p^2} T^{p^2} \right. \\ \mathfrak{p}_K^2 \ni \left[\begin{array}{l} -\frac{1}{2}\delta_{\ell,2}^{[2]} f_p^2 T^{2p} - \delta_{\ell,p+1}^{[2]} f_p f_{p^2} T^{p^2+p} - \frac{1}{2}\delta_{\ell,2}^{[2]} f_{p^2}^2 T^{2p^2} \\ \qquad + \sum\limits_{j\in[\![2,p-1]\!]} \delta_{\ell,j} f_{pj} T^{pj} + \sum\limits_{k\in[\![1,p+1]\!]} \delta_{\ell,k} f_k T^k. \end{array} \right. \end{array} \tag{3.4}$$

Recall that $\delta_{\ell,1} = 0$, unless $\ell = 1$. For $\ell = 1$, the expansion reduced modulo p^2 tells us that the norms in $U_{1,K}$ are of the form $1 + f_p T^p + f_{p^2} T^{p^2} + \mathcal{O}(p^2)$ for some T. Consequently put $F_p = \overline{f_p/p}$, $F_{p^2} = \overline{f_{p^2}/p}$ and consider the additive polynomial

$$A(Y) = F_{p^2} Y^p + F_p Y \tag{3.5}$$

over the residue field. It defines a linear function, if V is the range $A(\kappa_K)$ then $N_{L/K}(U_{1,L})U_{2,K}$ is contained in $1 + pV$, and V has codimension 1 precisely when the map defined by A has a kernel of dimension 1, that is when $-F_p/F_{p^2}$ is a $(p-1)$-th power (if $K = \mathbb{Q}_p$ we must have $V = 0$ and the condition is $F_{p^2} = -F_p$).

Condition 3.2. *We must have $-F_p/F_{p^2} \in \kappa_K^{p-1}$.*

Now for $\ell \geq 2$ the first part of the expansion (3.4) is 0, and we must check if the remaining part is in $p^2 V$, for each ℓ and each value of $T^\ell = \theta$.

Note that we only consider the ℓ prime with p, we are allowed to do so because all the $\delta_{\ell,i}^{[m]}$ appearing satisfy $(i,p) = 1$. Consequently for $\ell \geq 2$ the expansion can be written as a polynomial $C_\ell(T^\ell) = \ell \sum_{(k,p)=1} c_{k\ell}(T^{k\ell})$, where for each ℓ prime with p we denote by $c_\ell(T^\ell)$ the polynomial of T^ℓ obtained evaluating equation (3.4), but changing the definition of $\delta_{a,b}^{[m]}$ to be 1 if $a = b$, and 0 if $a \neq b$ (so in particular $c_\ell = 0$ if $\ell > p+1$).

Fix $\ell \geq 2$, then $c_\ell(T^\ell)$ can be obtained via Möbius inversion

$$\begin{aligned}\sum_{(k,p)=1} \mu(k) \frac{C_{k\ell}(T^{k\ell})}{k\ell} &= \sum_{(k,p)=1} \left(\mu(k) \cdot \sum_{(j,p)=1} c_{jk\ell}(T^{jk\ell}) \right) \\ &= \sum_{(i,p)=1} \left(c_{i\ell}(T^{i\ell}) \cdot \sum_{k|i} \mu(k) \right)\end{aligned}$$

by change of variable $i = jk$, obtaining $c_\ell(T^\ell)$ by the properties of the Möbius function μ. In view of the isomorphism $\mathfrak{p}_K^2/\mathfrak{p}_K^3 \to U_{2,K}/U_{3,K}$ induced by $x \mapsto 1 + x$ and specializing the argument $T^{k\ell}$ of $C_{k\ell}(T^{k\ell})$ to θ^k we have that

$$1 + \frac{1}{k} C_{k\ell}(\theta^k) \equiv N_{L/K} \left(1 - \theta^k \pi^{k\ell}\right)^{1/k} \pmod{p^3},$$

for each ℓ, k prime with p and each $\theta = T^\ell$. Consequently $1 + \ell \cdot c_\ell(\theta)$ is congruent modulo p^3 to the norm of

$$\prod_{(k,p)=1} \left(1 - \theta^k \pi^{k\ell}\right)^{\mu(k)/k} \equiv E(\theta\pi^\ell) \pmod{\mathfrak{p}_K^3},$$

where $E(x)$ is the Artin-Hasse exponential function (in its original form, according to [FV02, Chap. 3, §9.1]). We can equivalently require all $N_{L/K}(E(\theta\pi^\ell))$ to be in $1 + p^2 V$, for $\ell \in [\![2, p+1]\!]$ and $\theta \in U_K$.

Put $A_\ell(Y) = \overline{c_\ell(Y)/p^2}$, depending on ℓ we obtain

$$\begin{array}{cl} -F_p F_{p^2} Y^p + G_{p+1} Y & \ell = p+1, \\ G_{p\ell} Y^p + G_\ell Y & \ell \in [\![3, p-1]\!], \\ -\frac{1}{2} F_{p^2}^2 Y^{p^2} + \left(G_{2p} - \frac{1}{2} F_p^2\right) Y^p + G_2 Y & \ell = 2, \end{array}$$

where for convenience we have put $G_i = \overline{f_i/p^2}$ for each $i \neq p, p^2$. They are all additive polynomials.

Hence we have obtained the

Condition 3.3. *For each $\ell \in [\![2, p+1]\!]$, it is necessary that $A_\ell(\kappa_K) \subseteq A(\kappa_K)$.*

We are now left to consider the norms of elements of the form $1 + \theta\pi$ but such that $N_{L/K}(1 + \theta\pi) \in U_{2,K}$. This is the case if and only if θ is such that $\theta^{p^2-p} \equiv -f_p/f_{p^2} \pmod{p}$. Consider again the (3.4) for $\ell = 1$, in this case $\sum_{(k,p)=1} c_k(T^k)$ differs from $C_1(T) = N_{L/K}(1 - T\pi) - 1$ by the extra term

$$-\frac{1}{2} f_p^2 T^{2p} - f_p f_{p^2} T^{p^2+p} - \frac{1}{2} f_{p^2}^2 T^{2p^2} = -\frac{1}{2} \left(f_p T^p + f_{p^2} T^{p^2}\right)^2,$$

which is however even contained in $\mathfrak{p}^4$ for $T = \theta$. Since we already required all polynomials $c_k(Y^k)$ to take values in p^2V when $k \geq 2$, our requirement becomes that

$$c_1(\theta) = f_{p^2}\theta^{p^2} + f_p\theta^p + f_1\theta$$

should be contained in p^2V too, for each θ as above. Hence we have the

Condition 3.4. *Let θ be such that $\theta^{p^2-p} \equiv -{}^{f_p}/{}_{f_{p^2}} \pmod{p}$, it is necessary that $\overline{{}^{c_1(\theta)}/{}_{p^2}} \in V$.*

Collecting all the above conditions, and applying Prop. 2.2 to obtain conditions on the coefficients, we obtain the following theorem.

Theorem 3.1. *Let K be an unramified extension of $\mathbb{Q}_p$, $p \neq 2$. The Eisenstein polynomial $f(X) = X^{p^2} + f_1X^{p^2-1} + \cdots + f_{p^2-1}X + f_{p^2}$ determines a cyclic extension of degree p^2 over K if and only if*

(1) $v_p(f_p) = 1$, and $v_p(f_{pi}) \geq 2$ for $i \in [\![2, p-1]\!]$,
(2) $v_p(f_i) \geq 2$ for $i \in [\![1, p-1]\!]$, $v(f_{p+1}) = 2$ and $v_p(f_i) \geq 3$ for $i \in [\![p+2, p^2-1]\!]$,

putting $F_p = \overline{{}^{f_p}/{}_p}$, $F_{p^2} = \overline{{}^{f_{p^2}}/{}_p}$, and $G_i = \overline{{}^{f_i}/{}_{p^2}}$ for all $i \neq p, p^2$ we have

(3) $-{}^{F_p}/{}_{F_{p^2}} \in \kappa_K^{p-1}$,
(4) $G_{p+1}^p = -F_p^{p+1}$,
(5) $G_{p\ell} = F_{p^2}\left({}^{G_\ell}/{}_{F_p}\right)^p$, for all $\ell \in [\![3, p-1]\!]$,
(6) $G_{2p} = F_{p^2}\left({}^{G_2}/{}_{F_p}\right)^p + \frac{1}{2}F_p\left(F_p - F_{p^2}^{1/p}\right)$,

for each θ such that $\bar{\theta}^{p(p-1)} = -{}^{F_p}/{}_{F_{p^2}}$, we have that

(7) $F_{p^2}X^p + F_pX - \overline{\frac{1}{p^2}\left(f_{p^2}\theta^{p^2} + f_p\theta^p\right)} - G_1\bar{\theta}$ has a root in κ_K.

4. Polynomials of degree p^2 whose Galois group is a p-group

In this section we consider different families of polynomials that generate extensions of degree p^2 whose Galois closure is a p-group, and we will begin considering polynomials that satisfy a subset of the conditions stated in Theorem 3.1. We prove a preliminary proposition, first.

4.1. Galois actions in tower of degree p^2. Let K be unramified over $\mathbb{Q}_p$, $p \neq 2$, F/K and L/F totally ramified extensions of degree p such that L/F has ramification break > 1, and F/K has ramification break 1 and is cyclic, with group generated by σ say. In the notation of Theorem 3.1, if L/K is generated by an Eisenstein polynomial having a root π, then the only f_i with $v_p(f_i) = 1$ are f_p and f_{p^2}.

Let π_F be a uniformizing element of F. For some $\theta \in K$ we can write

$$\begin{aligned} \pi_F^{(\sigma-1)} &= 1 - \theta^p \pi_F + \dots \\ &= N_{L/F}(1 - \theta\pi) + \mathcal{O}(\pi_F^2) \end{aligned}$$

by [FV02, Chap. 3, §1, Prop. 1.5], because L/F has ramification break > 1. Assume $\pi_F = N_{L/F}(\pi)$, since $\pi_F^{(\sigma-1)}$ is killed by $N_{F/K}$ and $N_{F/K}(U_{2,F}) \subseteq U_{2,K}$ we have $N_{L/K}(1 - \theta\pi) \in U_{2,K}$, the first part of the expression (3.4) should vanish, for $\ell = 1$ and $T = \theta$. Consequently we have $\bar{\theta}^{p(p-1)} = -{}^{F_p}/{}_{F_{p^2}}$. Its easy to verify that the same holds for any other uniformizer π_F of F, writing it as power series in π_F (and indeed ${}^{F_p}/{}_{F_{p^2}}$ is an invariant of the extension F/K not depending on the choice of the uniformizer π_F, as can be proved using the theory of residual polynomials [Ore28], see also [MP99, GP12]).

We obtain inductively the following proposition.

Proposition 4.1. *For each $1 \leq \ell < p$ we have*

$$\pi_F^{(\sigma-1)^\ell} = 1 - k\theta^{p\ell}\pi_F^\ell + \dots,$$

for some integer k prime with p, where $\bar{\theta}^{p(p-1)} = -{}^{F_p}/{}_{F_{p^2}}$.

4.2. Lower ramification breaks $\boldsymbol{1, p+1}$. We return to the study of the extensions of degree p^2 whose Galois closure is a p-group, considering the first case. Let's keep the hypotheses on the ramification breaks of Theorem 3.1 (and consequently conditions 1 and 2 of the theorem), we will describe the Galois group of the normal closure when not all the remaining conditions are satisfied.

We will also assume condition 3, it is satisfied if and only if L contains a Galois extension of degree p of K, a necessary condition for the normal closure of L/K to be a p-group. Note that this hypothesis is always satisfied for $f(X)$ if K is replaced by a suitable unramified extension.

In view of the proof of Theorem 3.1, the first failing condition among the 4, 5 (for ℓ as big as possible), 6 and 7 in Theorem 3.1 allows to determine the biggest possible ℓ such that $N_{L/K}(U_{\ell,L}) \cap U_{2,K}$ is not contained in $1 + p^2 V$, with V defined as in the proof. We expect this observation to provide information about the Galois group of the normal closure.

Let L/K be totally ramified, and generated by an Eisenstein polynomial of degree p^2 satisfying conditions 1,2 and 3 of Theorem 3.1. Let F be the Galois extension of degree p of K contained in L corresponding to the ramification break 1, then L/F has ramification break $p + 1$.

We need L/F to be Galois: by local class field theory this is the case precisely when the map ${}^{U_{p+1,L}}/{}_{U_{p+2,L}} \to {}^{U_{p+1,F}}/{}_{U_{p+2,F}}$ induced by $N_{L/F}$ is not surjective. Since the map ${}^{U_{p+1,F}}/{}_{U_{p+2,F}} \to {}^{U_{2,K}}/{}_{U_{3,K}}$ induced by $N_{F/K}$ is an isomorphism by [FV02, Chap. 3, §1, Prop. 1.5], we are reduced to study the image of ${}^{U_{p+1,L}}/_{U_{p+2,L}}$ in ${}^{U_{2,K}}/_{U_{3,K}}$. Considering elements of the form $E(\theta\pi^{p+1})$ for $\theta \in \mathcal{O}_K^\times$, by the proof of Theorem 3.1 this map is described by the additive polynomial $A_{p+1}(Y)$, and is non-surjective precisely when ${}^{G_{p+1}}/_{F_p F_{p^2}}$ is in κ_K^{p-1}. Consequently we will always assume the

Condition 4.1. *We require ${}^{G_{p+1}}/_{F_p F_{p^2}} \in \kappa_K^{p-1}$.*

This condition is necessary and sufficient for the Galois closure of L/K to be a p-group, and again is always satisfied if we replace K by a suitable unramified extension.

For an $\mathbb{F}_p[G]$-module M we respectively denote by $\mathrm{soc}^i(M)$ and $\mathrm{rad}^i(M)$ the i-th socle and radical of M. If σ is a generator of G, the radical of $\mathbb{F}_p[G]$ is generated by $\sigma - 1$, and we have

$$\mathrm{rad}^i(M) = M^{(\sigma-1)^i}, \qquad \mathrm{soc}^i(M) = \left\{x : x^{(\sigma-1)^i} = 0\right\}.$$

Let $G = \mathrm{Gal}(F/K)$ and $\tilde{L}$ be the Galois closure of L over K, we want to compute the length of $\mathrm{Gal}(\tilde{L}/F)$ as a $\mathbb{F}_p[G]$-module using the first unsatisfied condition when applying Theorem 3.1, and we will show that such length determines completely $\mathrm{Gal}(\tilde{L}/K)$ in the present case. If $F^{(p)}$ is the maximal abelian elementary p-extension of F, considering $\mathrm{Gal}(F^{(p)}/F)$ as an $\mathbb{F}_p[G]$-module this amounts to computing the smallest m such that $\mathrm{rad}^m(\mathrm{Gal}(F^{(p)}/F))$ is contained in $\mathrm{Gal}(F^{(p)}/L)$.

For $0 \le i \le p$ let's consider the submodules $S_i = \mathrm{soc}^{p-i}(P_F)$ of $P_F = [F^\times]_F$ ($P_F \cong \mathrm{Gal}(F^{(p)}/F)$ canonically, via local class field theory), and let K_i be the class field corresponding to S_i over F. For $0 \le i < p$ we have $[U_{i+1,F}] \subseteq S_i$ and thus the highest upper ramification break of $\mathrm{Gal}(K_i/F)$ is $< p$, and in particular being $p+1$ the unique ramification break of L/F we have that $K_i \not\supseteq L$ for $i < p$. Note also that K_1 is the maximal elementary abelian p-extension of K.

Let K' be the field corresponding to $\mathrm{rad}^1(P_F)$, it is the maximal p-elementary abelian extension of F that is abelian over K, and as such it corresponds to $N_{F/K}(F^\times)^p$ via the class field theory of K (because F corresponds to $N_{F/K}(F^\times)$). Considering the structure of $P_F \cong \mathbb{F}_p[G]^{\oplus f} \oplus \mathbb{F}_p$ as a Galois module we have that

$$rad^i(P_F) = \mathrm{soc}^{p-i}(P_F) \cap \mathrm{rad}^1(P_F) = S_i \cap \mathrm{rad}^1(P_F),$$

for each i, and $rad^i(P_F)$ corresponds to $K'K_i$ via class field theory of F, so we are looking for the smallest m such that $L \subset K'K_m$. Since L and K' are never contained in K_i for $i < p$ and K' has degree p over K_1, this inclusion holds if and only if L and K' generate the same extension over K_m (and $\tilde{L}$ will too, being $K'K_m$ Galois over K). This is the case if and only if $K' \subset LK_m$, and this condition is consequently equivalent to the $\mathbb{F}_p[G]$-module $\mathrm{Gal}(\tilde{L}/F)$ having length $\le m$.

Proposition 4.2. *For each $1 \leq m < p$, $\mathrm{Gal}(\tilde{L}/F)$ has length $\leq m$ if an only if $K' \subset LK_m$.*

We can now show that if $K' \subset LK_m$ for some $m < p$, then $\mathrm{Gal}(\tilde{L}/K)$ cannot be the split extension of $\mathrm{Gal}(F/K)$ by $\mathrm{Gal}(\tilde{L}/F)$. This is essentially a consequence of $\mathrm{Gal}(K_m/K)$ being the quotient of $\mathrm{Gal}(K_{m+1}/K)$ by its socle. Indeed, $\mathrm{Gal}(K_{m+1}/K)$ lives in the exact sequence

$$1 \to {}^{P_F}/_{S_{m+1}} \to \mathrm{Gal}(K_{m+1}/K) \to G \to 1,$$

and all p-th powers in $\mathrm{Gal}(K_{m+1}/K)$ are clearly G-invariant elements of ${}^{P_F}/_{S_{m+1}}$, and hence contained in ${}^{S_m}/_{S_{m+1}}$. It follows that the quotient $\mathrm{Gal}(K_m/K)$ has exponent p since we quotiented out all p-th powers. On the other hand $\mathrm{Gal}(K'/K)$ has exponent p^2 so if $K' \subset LK_m$ then also $\mathrm{Gal}(\tilde{L}K_m/K)$ does, having $\mathrm{Gal}(K_m/K)$ exponent p we would have a contradiction if $\mathrm{Gal}(\tilde{L}/K)$ had exponent p too. If $\mathrm{Gal}(\tilde{L}/F)$ has greatest possible length $m = p$, then there is only one possibility for the isomorphism class, which is the wreath product of two cyclic groups of order p, see [MS05, Wat94].

The above observation can be viewed as the fact that, for $m < p$, K_m is the compositum of all extensions of degree p whose normal closure has group over F of length $\leq m$ as $\mathbb{F}_p[G]$-module, and whose group over K is the semidirect product extension (and hence has exponent p). The extensions of F whose group of the normal closure over K is not the semidirect product and the length is m are obtained taking a subextension of K_mK' that is not contained in K_m, nor in $K_{m-1}K'$.

Now K' is not contained in LK_m precisely when there exist an element in $\mathrm{Gal}(K^{\mathrm{alg}}/K)$ fixing LK_m but not K'; any such element is in $\mathrm{Gal}(K^{\mathrm{alg}}/L)$ and we can consider its projection to $\mathrm{Gal}(L^{\mathrm{ab}}/L)$. Since the image of the Artin map $\Psi_L : L^\times \to \mathrm{Gal}(L^{\mathrm{ab}}/L)$ is dense in $\mathrm{Gal}(L^{\mathrm{ab}}/L)$, we can take such element of the form $\Psi_L(\alpha)$ for some $\alpha \in L^\times$. Having to fix K_1 we will have $N_{L/K}(\alpha) \in (K^\times)^p$ by the functoriality property of the reciprocity map (see [FV02, Chap. 4, Theorem 4.2]), $[N_{L/F}(\alpha)]_F \in S_m$ because K_m is fixed, and $N_{L/K}(\alpha) \notin N_{F/K}(F^\times)^p$ because the action is non-trivial on K'. On the other hand the existence of such an element ensures that $K' \not\subseteq LK_m$.

If L and K are as above, we have proved the following proposition.

Proposition 4.3. *Let $1 \leq m \leq p$ be the smallest possible integer such that for all $\alpha \in L^\times$ satisfying $N_{L/K}(\alpha) \in (K^\times)^p$ and $[N_{L/F}(\alpha)]_F \in S_m$ we have $N_{L/K}(\alpha) \in N_{F/K}(F^\times)^p$. Then $\mathrm{Gal}(\tilde{L}/K)$ is the unique p-group that has exponent p^2 and is an extension of $G = \mathrm{Gal}(F/K)$ by an indecomposable $\mathbb{F}_p[G]$-module of length m.*

We now determine the $(p-m)$-th socle S_m of P_F for each $0 \leq m \leq p$, and deduce the ramification breaks of the normal closure.

Consider the images $V_i = [U_{i,F}]_F$ of the $U_{i,F}$ in P_F for $i \geq 1$, and put $V_0 = P_F$ for convenience. If G is generated by σ say, the radical of $\mathbb{F}_p[G]$ is generated by $(\sigma - 1)$ and we have $V_i^{\sigma-1} \subseteq V_{i+1}$. Since $V_p = V_{p+1}$ and $V_{p+2} = 1$ we have that V_p is killed by $\sigma - 1$, V_{p-1} by $(\sigma-1)^2$ and so on, so that $V_{k+1} \subseteq \operatorname{soc}^{p-k} P_F = S_k$ for $0 \leq k < p$, while clearly $S_p = 0$. Furthermore if π_F is a uniformizing element of F we have $\pi_F^{(\sigma-1)^k} \in V_k \backslash V_{k+1}$ and $\pi_F^{(\sigma-1)^k} \in S_k$ for $0 \leq k < p$, so comparing the dimensions we have that

$$S_k = \langle \pi_F^{(\sigma-1)^k} \rangle + V_{k+1}.$$

If m is like in the proposition and ≥ 2, let $\alpha \in L^\times$ be an element that provides a counterexample to the proposition for $m-1$, and such that $t = v_F(1 - N_{L/F}(\alpha))$ is as big as possible. Then $\psi_{LK_{m-1}/F}(t)$ is the ramification break of $K'LK_{m-1}/LK_{m-1}$, which is also equal to that of $LK'K_{m-1}/K'K_{m-1}$ considering that $K'K_{m-1}/K_{m-1}$ and LK_{m-1}/K_{m-1} have the same ramification break equal to $\psi_{K_{m-1}/F}(p+1)$, and the total set of breaks of $K'LK_{m-1}/K_{m-1}$ has to be preserved. By the definition of S_{m-1} and S_m we have that t can be either $m-1$ or m, unless $m = p$ where t is either $p-1$ or $p+1$.

By local class field theory $K'K_{m-1}/F$ corresponds to the subgroup $A = rad^{m-1}(P_F)$ of P_F, and $LK'K_{m-1}/F$ to another subgroup B with index p in A, and t is the biggest t such that some $x \in V_t \cap A$ has non-trivial image in A/B. Passing to the groups A' and B' of the elements sent by $\sigma - 1$ into A and B respectively, $A' = soc^{p-m+2}(P_F)$ corresponds to K_{m-2}, and B' to $L'K_{m-2}$ where L' is the subfield of $\tilde{L}$ corresponding to $\operatorname{soc}^1(\operatorname{Gal}(\tilde{L}/F))$ as $\mathbb{F}_p[G]$-module. The upper ramification break of the new relative extension is $\psi_{K_{m-2}/F}(s)$ where s is the biggest integer such that some $y \in V_s \cap A'$ is nontrivial in A'/B'. Being $A = rad^{m-1}(P_F)$ each $x \in A \setminus B$ is of the form $x = y^{\sigma-1}$ for some $y \in A' \backslash B'$, so $s = t-1$ unless $t = p+1$ where it becomes $s = p-1$.

Because $\operatorname{Gal}(L'/F)$ has length $m-1$ and the field L'' fixed by $\operatorname{soc}^1(\operatorname{Gal}(L'/L))$ is contained in K_{m-2}, and $V_{m-2} \supseteq A' \supseteq V_{m-1}$, we have that s is also the ramification break of L'/L'' with respect to F, that is the break is $\psi_{L''/F}(s)$. Repeating this observation for $m-1$ steps we have that the upper ramification breaks over F are either $1, 2, \ldots, m-1, p+1$, either $0, 1, \ldots, m-2, p+1$ depending on whether an element $\alpha \in S_{m-1}$ contradicting the proposition for $m-1$ can be found in V_m or not, where for convenience a “ramification break” of 0 indicates an unramified extension.

We proved the

Proposition 4.4. *Let $1 \leq m \leq p$ be like in the Prop. 4.3, if we can find an α such that $N_{L/K}(\alpha) \in (K^\times)^p \setminus N_{F/K}(F^\times)^p$ such that $[N_{L/F}(\alpha)]_F \in V_m \subset S_m$, then the normal closure $\tilde{L}/F$ is totally ramified with breaks $1, 2, \ldots, m-1, p+1$. If not, then $\tilde{L}/F$ has inertia degree p and upper ramification breaks $1, 2, \ldots, m-2, p+1$.*

For an extension determined by an Eisenstein polynomial $f(T)$, we will determined the biggest $1 \leq \ell \leq p-1$ such that the requirements of Prop. 4.3 fail for $\ell = m-1$. For all $\ell = p-1, \ldots, 2, 1$ in descending order, if we cannot find a suitable α with $[N_{L/F}(\alpha)]_F \in V_{\ell+1}$, we inductively test $S_\ell \supset V_{\ell+1}$ (deducing that $\mathrm{Gal}(\tilde{L}/F)$ has length $\ell+1$ and there is an unramified part), and whether $V_\ell \supseteq S_\ell$ (in this case $\mathrm{Gal}(\tilde{L}/F)$ has length ℓ and the extension is totally ramified).

Testing the existence of an α such that $[N_{L/F}(\alpha)]_F \in V_{\ell+1}$ is easy, and is the condition of the theorem connected to $A_{p+1}(Y)$ for $\ell = p-1$, or to $A_{\ell+1}$ if $\ell < p-1$. At the subsequent step we allow $[N_{L/F}(\alpha)]_F$ to be in $S_\ell = \langle \pi_F^{(\sigma-1)^\ell} \rangle + V_{\ell+1}$: by Prop. 4.1 for $\bar{\theta}^{p(p-1)} = -{}^{F_p}/_{F_{p^2}}$ and for some k prime with p we have

$$\begin{aligned} \pi_F^{(\sigma-1)^\ell} &= 1 - k\theta^{p\ell}\pi_F^\ell + \ldots \\ &= N_{L/F}(1 - k\theta^\ell\pi^\ell) + \mathcal{O}(\pi_F^{\ell+1}), \end{aligned}$$

in view of [FV02, Chap. 3, §1, Prop. 1.5] and being ℓ smaller than the ramification break $p+1$. In particular the image of $N_{L/F}(1-\theta^\ell\pi^\ell)$ generates ${}^{S_\ell}/_{V_{\ell+1}}$, and testing the condition for S_ℓ is equivalent to verifying whether $A_\ell(\bar{\theta}^\ell) \in V$.

Note that $A_2(\bar{\theta}^2)$ has the simplified form $G_{2p}\bar{\theta}^{2p} + G_2\bar{\theta}^2$, and testing if $F_{p^2}X^p + F_pX = A_\ell(\bar{\theta}^\ell)$ has solution in κ_K is equivalent to checking, after replacing X by $\bar{\theta}^\ell X$ and dividing by $\bar{\theta}^\ell$, if there are solutions to

$$F_{p^2}(-{}^{F_p}/_{F_{p^2}})^{\ell/p}X^p + F_pX - G_{p\ell}(-{}^{F_p}/_{F_{p^2}})^{\ell/p} - G_\ell = 0.$$

Note that for $\ell = 1$ we just test if $\overline{{}^{c_1(\theta)}/_{p^2}}$ is in V, like in the last condition of Theorem 3.1.

We have the

Theorem 4.1. *Let K be an unramified extension of $\mathbb{Q}_p$, $p \neq 2$. Assume that $f(X)$ satisfies conditions 1, 2, 3 of Theorem 3.1, and keeping the notation assume additionally that*

(1) ${}^{G_{p+1}}/_{F_pF_{p^2}} \in \kappa_K^{p-1}$.

Let L be the extension determined by $f(X)$, $\tilde{L}$ the normal closure over K, and F the unique subextension of degree p contained in L. Then $\mathrm{Gal}(\tilde{L}/K)$ is an extension of $G = \mathrm{Gal}(F/K)$ by the indecomposable $\mathbb{F}_p[G]$-module $M = \mathrm{Gal}(\tilde{L}/F)$, $\mathrm{Gal}(\tilde{L}/K)$ has exponent p^2 and is a non-split extension *unless M has length p. Considering the first of the following conditions that fails for a given polynomial, we obtain depending on the case:*

(I) if $G_{p+1}^p \neq -F_p^{p+1}$, then M has length p and L/F is totally ramified with upper ramification breaks $1, 2, \dots, p-1, p+1$;

assuming equality in the previous condition,

(II) if $G_{p\ell} \neq F_{p^2}\left({}^{G_\ell}/{}_{F_p}\right)^p$ for some $\ell \in [\![3, p-1]\!]$ (that we select as big as possible), or if said equality always holds but $G_{2p} \neq F_{p^2}\left({}^{G_2}/{}_{F_p}\right)^p + \frac{1}{2}F_p\left(F_p - F_{p^2}^{1/p}\right)$ (and in this case we put $\ell = 2$), then let

$$U(X) = F_{p^2}\left(-{}^{F_p}/{}_{F_{p^2}}\right)^{\ell/p}X^p + F_pX - G_{p\ell}\left(-{}^{F_p}/{}_{F_{p^2}}\right)^{\ell/p} - G_\ell;$$

we have that

- *if $U(X)$ has no root in κ_K, then M has length $\ell+1$ and $\tilde{L}/F$ has inertia degree p, and upper ramification breaks $1, 2, \dots, \ell-1, p+1$,*
- *if $U(X)$ has some root in κ_K, then M has length ℓ and $\tilde{L}/F$ is a totally ramified with upper ramification breaks $1, 2, \dots, \ell-1, p+1$;*

assuming equality in all previous conditions, and putting $\bar{\theta}^{p(p-1)} = -{}^{F_p}/{}_{F_{p^2}}$,

(III) if $F_{p^2}X^p + F_pX - \overline{\frac{1}{p^2}\left(f_{p^2}\theta^{p^2} + f_p\theta^p\right)} - G_1\bar{\theta}$ has no root in κ_K, then M has length 2 and $\tilde{L}/F$ has inertia degree p, and upper ramification break $p+1$.

All conditions are satisfied precisely when all requirements of Theorem 3.1 are satisfied, and in this case L/F is Galois cyclic of degree p^2.

4.3. Lower ramification breaks $\mathbf{1}, \boldsymbol{\ell}$, $\mathbf{1} < \boldsymbol{\ell} \leq \boldsymbol{p} - \mathbf{1}$. It turns out that we just worked out the hard case of the classification of all polynomials of degree p^2 whose Galois group is a p-group.

We keep the notation of the previous part of this section. We have classified in Theorem 4.1 all polynomials such that L/F has ramification break at $p+1$ and the normal closure is a p-group, and it turned out that the condition on the ramification break is sufficient to guarantee that the Galois group of the normal closure has exponent p^2. Conversely if the ramification break is $\leq p-1$ then either $L \subset K_m$ for some $m < p$, $\mathrm{Gal}(\tilde{L}/F)$ has length $\leq m$, and $\mathrm{Gal}(\tilde{L}/K)$ is the splitting extension of G; either $\mathrm{Gal}(\tilde{L}/F)$ has length p. In the latter case there is only one possible isomorphism class for $\mathrm{Gal}(\tilde{L}/K)$, which is both a split extension and has exponent p^2, and is isomorphic to the wreath product of two cyclic groups of order p.

As above, let ℓ be the smallest integer such that $[N_{L/F}(L^\times)]_F$ contains $V_{\ell+1}$. The ramification break of L/F is equal to ℓ, and the length of $\mathrm{Gal}(\tilde{L}/K)$ as G-module can be ℓ when the norms also contain S_ℓ, or $\ell+1$ if this is not the case. Since $S_\ell = \langle \pi_F^{(\sigma-1)^\ell} \rangle + V_{\ell+1}$ to resolve this ambiguity we should test whether $[\pi_F^{(\sigma-1)^\ell}]_F \in [N_{L/F}(L^\times)]_F$. Since $\pi_F^{(\sigma-1)^\ell} \in U_{\ell,F}$ and we assumed $N_{L/F}(L^\times) \supset U_{\ell+1,F}$, we can just test whether

$$N_{L/F}(1+\theta\pi^\ell) = \pi_F^{(\sigma-1)^\ell} + \mathcal{O}(p^{\ell+1})$$

for some unit $\theta \in U_K$.

Let's focus in the extension generated by $f(T)$; we start deducing the condition for L/F to be Galois, and will subsequently determine the above length. Factoring (in L) the ramification polynomial $f(X+\pi)$ over the Newton polygon we have that $f(X+\pi) = Xg(X)h(X)$, where $g(X)$ has degree $p-1$ with roots of valuation $\ell+1$ and $h(X)$ degree p^2-p and roots with valuation 2. We can take $g(X)$ to be monic and with roots $\tau^i(\pi)-\pi$, where τ is an automorphism of order p of the normal closure of L over F and $1 \leq i < p$, note that L/F is Galois if and only if $g(X) = X^{p-1}+\dots+g_1X+g_0$ splits into linear factors in L.

If we can write $\tau(\pi)-\pi = \eta\pi^{\ell+1}+\dots$ with $\eta \in U_K$, then $F(\pi) = L$ contains an element that approximates $\tau(\pi)$ better than any other conjugate of $\tau(\pi)$, and consequently $F(\tau(\pi)) \subseteq L$ by Krasner lemma, and it follows that L/F is Galois being $L = F(\pi)$. On the other hand if L/K is Galois we certainly have such an expression for some η. Since

$$g_0 = \prod_{i=1}^{p-1}(\tau^i\pi - \pi) \tag{4.1}$$

$$\equiv \prod_{i=1}^{p-1} i\eta\pi^{\ell+1} \equiv -\eta^{p-1}\pi^{(p-1)(\ell+1)} \tag{4.2}$$

we have that L/F is Galois if and only if $-g_0$ is a $(p-1)$-th power.

The term in X^p of $f(X+\pi)$ is (up to higher order)

$$\binom{p^2-p}{p} f_p\pi^{p^2-2p}X^p = h_0X^p$$

where h_0 is the constant term of $h(X)$, while the term in X is

$$Xf'(\pi) = (p^2-r)f_r\pi^{p^2-r-1}X = g_0h_0X$$

where r should be $p^2-(p-1)\ell+p$ and $v_p(f_r) = 2$, considering that $f'(\pi)$ is the different and has valuation $(p^2-p)\cdot 2 + (p-1)\cdot(\ell+1)$.

Since $\binom{p^2-p}{p} \equiv -1 \pmod{p}$, by the definition of r we have taking the ratio of the coefficients of the monomials above that

$$\begin{aligned}\frac{g_0}{\pi^{(p-1)(\ell+1)}} &= \frac{-rf_r\pi^{(p-1)\ell-p-1}}{-f_p\pi^{p^2-2p}}\cdot\pi^{-(p-1)(\ell+1)}+\dots\\ &= {}^{rf_r}/_{f_p}\cdot\pi^{-p^2}+\dots = -{}^{rf_r}/_{f_pf_{p^2}}+\dots,\end{aligned}$$

being $\pi^{p^2} = -f_0+\dots$.

Since $r \equiv \ell \pmod{p}$ we obtained that $\bar{\eta}^{p-1}$ is equal to $\overline{\ell f_r/f_p f_{p^2}}$, and it is contained in κ_K^{p-1} if and only if g_0 is a $(p-1)$-th power in L. Put again $F_p = \overline{f_p/p}$, $F_{p^2} = \overline{F_{p^2}/p}$ and $G_i = \overline{f_i/p^2}$ for $i \neq p, p^2$.

Condition 4.2. *L/F is Galois if and only if $\ell G_r/F_p F_{p^2}$ is in κ_K^{p-1}, where r is equal to $p^2 - (p-1)\ell + p$.*

We will now determine the exact length of the Galois module. Let's recall from [FV02, Chap. 3, §1, Prop. 1.5] that

$$N_{L/F}(1 + \theta\pi^\ell) = 1 + (\theta^p - \eta^{p-1}\theta)\pi_F^\ell + \dots,$$

while

$$\pi_F^{(\sigma-1)^\ell} = 1 - k\rho^\ell \pi_F^\ell + \dots$$

for $\bar{\rho}^{p-1} = -F_p/F_{p^2}$ and some integer k prime with p, by Prop. 4.1. For a suitable σ we can assume $k = -1$, then we must test the existence of a θ making the above expressions equal modulo $\mathfrak{p}^{\ell+1}$. It follows that the length of $\operatorname{Gal}(\tilde{L}/K)$ is precisely ℓ when $X^p - \ell G_r/F_p F_{p^2} X = \bar{\rho}^\ell$ has solution in κ_K, and $\ell + 1$ if this is not the case. Replacing X by $\bar{\rho}^\ell X$ and dividing by $\bar{\rho}^\ell$ this is equivalent to testing whether

$$(-F_p/F_{p^2})^\ell X^p - \ell G_r/F_p F_{p^2} X - 1 = 0$$

has solution in κ_K.

Consequently we obtain

Theorem 4.2. *Let K be an unramified extension of $\mathbb{Q}_p$, $p \neq 2$. Let $2 \leq \ell \leq p-1$ an let $r = p^2 - (p-1)\ell + p$, and assume that $f(X)$ is an Eisenstein polynomial such that*

1. *$v_p(f_p) = 1$, and $v_p(f_{pi}) \geq 2$ for $i \in [\![2, p-1]\!]$,*
2. *$v_p(f_i) \geq 2$ for $i \in [\![1, r-1]\!]$, $v(f_r) = 2$ and $v_p(f_i) \geq 3$ for $i \in [\![r+1, p^2-1]\!]$,*

and putting $F_p = \overline{f_p/p}$, $F_{p^2} = \overline{f_{p^2}/p}$, $G_i = \overline{f_i/p^2}$ for all $i \neq p, p^2$ we have

3. *$-F_p/F_{p^2} = \bar{\rho}^{p-1}$ for some $\bar{\rho} \in \kappa_K^\times$,*
4. *$\ell G_r/F_p F_{p^2} = \bar{\eta}^{p-1}$ for some $\bar{\eta} \in \kappa_K^\times$.*

Let L be the extension determined by $f(X)$, $\tilde{L}$ the normal closure over K, and F the unique subextension of degree p contained in L. Then $\operatorname{Gal}(\tilde{L}/K)$ is a split extension of $G = \operatorname{Gal}(F/K)$ by the indecomposable $\mathbb{F}_p[G]$-module $M = \operatorname{Gal}(\tilde{L}/F)$. Furthermore for

$$U(X) = (-F_p/F_{p^2})^\ell X^p - \ell G_r/F_p F_{p^2} X - 1$$

we have that

- *if $U(X)$ has no root in κ_K, then M has length $\ell+1$, and $\tilde{L}/F$ has inertia degree p and upper ramification breaks $1, 2, \dots, \ell$,*

- *if $U(X)$ has some root in κ_K, then M has length ℓ, and $\tilde{L}/F$ is totally ramified with upper ramification breaks $1, 2, \dots, \ell$.*

4.4. Lower ramification break 1 (with multiplicity 2). What is left is the easy case for $\ell = 1$, which is studied separately. In this case L/K has 1 as unique ramification break, $v_p(f_1) = 1$ while $v_p(f_i) \geq 2$ for $i \in [\![2, p^2 - 1]\!]$, and consequently put $F_i = \overline{f_i/p}$ for $i = 1, p, p^2$. The map ${}^{U_{1,L}}/_{U_{2,L}} \to {}^{U_{1,K}}/_{U_{2,K}}$ induced by $N_{L/K}$ is described by the additive polynomial $A(Y) = F_{p^2} Y^{p^2} + F_p Y^p + F_1 Y$, and L/K is Galois precisely when $N_{L/K}(U_{1,L}) = 1 + pW$ for a subspace W of codimension 2 in κ_K, that is when $A(Y)$ splits completely in κ_K. On the other hand the normal closure $\tilde{L}/K$ is a p-extension if and only if L becomes abelian elementary over the unique unramified extension of degree p of K, or equivalently if $A(Y)$ splits completely over the unique extension of degree p of κ_K. Applying Prop. 2.3 to the polynomial $A(Y)$ we obtain the following theorem.

Theorem 4.3. *Let K be an unramified extension of $\mathbb{Q}_p$, $p \neq 2$. Assume that $f(X)$ is an Eisenstein polynomial such that*

(1) $v_p(f_p) \leq 1$, and $v_p(f_{pi}) \geq 2$ for $i \in [\![2, p-1]\!]$,
(2) $v_p(f_1) = 1$, and $v(f_i) \geq 2$ for $i \in [\![2, p^2 - 1]\!]$,

and putting $F_i = \overline{f_i/p}$ for $i = 1, p, p^2$

(3) the polynomial $F_{p^2} Y^{p^2} + F_p Y^p + F_1 Y$ has a root in $\kappa_K^\times$, and ${}^{F_1}/_{F_{p^2}} \in (\kappa_K^\times)^{p-1}$.

Let L be the extension determined by $f(X)$, and $\tilde{L}$ be the normal closure over K. Then

- *if $F_{p^2} Y^{p^2} + F_p Y^p + F_1 Y$ does not split completely in κ_K, then L/K has a unique subextension F, $\mathrm{Gal}(\tilde{L}/F)$ has length 2, $\tilde{L}/F$ has inertia degree p and upper ramification break 1, and $\mathrm{Gal}(\tilde{L}/K)$ is a split extension of $\mathrm{Gal}(F/K)$ by $\mathrm{Gal}(\tilde{L}/F)$,*
- *if $F_{p^2} Y^{p^2} + F_p Y^p + F_1 Y$ has all roots in κ_K then L/K is a totally ramified abelian elementary p-extension.*

Theorems 4.1, 4.2 and 4.3 cover all possible ramification breaks of the extension L/F, so they completely describe the Galois groups of polynomials of degree p^2 whose splitting field is a p-extension.

5. Polynomials of degree p^3 generating a cyclic extension

We proceed with the same strategy used for the polynomials of degree p^2, starting from the conditions on the valuations of the coefficients.

Let $f(X) = X^{p^3} + \cdots + f_{p^3-1}X + f_{p^3}$, since the different has now valuation $4p^3 - p^2 - p - 2$ it will come from the monomial $f_{p^2+p+1}X^{p^3-p^2-p-1}$, $v_p(f_{p^2+p+1}) = 3$, $v_p(f_i) \geq 3$ if $(i,p) = 1$ and $v_p(f_i) \geq 4$ if furthermore $i > p^2+p+1$. Let π be a root, the coefficient of the term of degree p of the ramification polynomial $f(X+\pi)$ will have valuation $(p^3 - p^2)\cdot 2 + (p^2 - p)\cdot(p+1) = 3p^3 - p^2 - 2p$ and has to come from a monomial $f_{p^3-i}(X+\pi)^i$ contributing the term $\binom{i}{p} f_{p^3-i}X^p\pi^{i-p}$. We deduce that $i = p^3 - p^2 - p$, $v_p(f_{p^2+p}) = 2$, $v_p(f_{pi}) \geq 2$ for $(i,p) = 1$ and $v_p(f_{pi}) \geq 3$ if furthermore $i \geq p+2$. Similarly, considering the coefficient of the term of degree p^2 of the ramification polygon, which must have valuation $2p^3 - 2p^2$, we obtain that $v_p(f_{p^2}) = 1$ and $v_p(f_{p^2 i}) \geq 2$ for all indices such that $(i,p) = 1$.

Condition 5.1. *We must have*

(1) $v_p(f_{p^2}) = 1$ *and* $v_p(f_{p^2 i}) \geq 2$ *for* $i \in \llbracket 2, p-1 \rrbracket$,
(2) $v_p(f_{pi}) \geq 2$ *for all* $i \in \llbracket 1, p-1 \rrbracket$, $v_p(f_{p^2+p}) = 2$, *and* $v_p(f_{pi}) \geq 3$ *for all* $i \in \llbracket p+1, p^2-1 \rrbracket$,
(3) $v_p(f_i) \geq 3$ *for all* $i \in \llbracket 1, p^2+p-1 \rrbracket$, $v_p(f_{p^2+p+1}) = 3$ *and* $v_p(f_i) \geq 4$ *for all* $i \in \llbracket p^2+p+2, p^3-1 \rrbracket$.

Working like in degree p^2, we require $N_{L/K}(U_{1,L})^{p^{i-1}} \cap U_{i+1,L}$ to be contained in $1 + p^i V$ for $1 \leq i \leq 3$ and some $\mathbb{F}_p$-vector space V, and after determining V we will have to verify the condition on the combinations of the norms of elements of the form $1+\theta\pi^\ell$ for a unit θ, and $1 \leq \ell \leq p^2+p+1$ and $(\ell,p) = 1$.

Let's expand again $\prod_{i=0}^{\ell} \tilde{f}(\zeta_\ell^i T)$ modulo p^4. Taking into account the valuations of the f_i and evaluating directly the $\Sigma_\lambda(\ell)$ via Prop. 2.4, it can be written (ordering terms by increasing valuation) as

$$\text{(5.1)} \quad \mathfrak{p}_K \ni \Big[\quad +\delta_{\ell,1} f_{p^2} T^{p^2} + \delta_{\ell,1} f_{p^3} T^{p^3}$$

$$\text{(5.2)} \quad \mathfrak{p}_K^2 \ni \left[\begin{array}{l} +\frac{1}{2}\delta_{\ell,2}^{[2]} f_{p^2}^2 T^{2p^2} + \delta_{\ell,p+1}^{[2]} f_{p^2} f_{p^3} T^{p^3+p^2} + \frac{1}{2}\delta_{\ell,2}^{[2]} f_{p^3}^2 T^{2p^3} \\ + \sum\limits_{j \in \llbracket 2, p-1 \rrbracket} \delta_{\ell,j} f_{p^2 j} T^{p^2 j} + \sum\limits_{k \in \llbracket 1, p+1 \rrbracket} \delta_{\ell,k} f_{pk} T^{pk} \end{array} \right.$$

$$\mathfrak{p}_K^3 \ni \left[\begin{array}{c} +\frac{1}{3}\delta_{\ell,3}^{[3]} f_{p^2}^3 T^{3p^2} + \delta_{\ell,p+2}^{[3]} f_{p^3} f_{p^2}^2 T^{p^3+2p^2} + \delta_{\ell,2p+1}^{[3]} f_{p^3}^2 f_{p^2} T^{2p^3+p^2} \\ +\frac{1}{3}\delta_{\ell,3}^{[3]} f_{p^3}^3 T^{3p^3} + \sum_{j\in[\![2,p-2]\!]} \delta_{\ell,j+1}^{[2]} f_{p^2} f_{p^2 j} T^{p^2+p^2 j} + \delta_{\ell,1}^{[2]} f_{p^2} f_{p^3-p^2} T^{p^3} \\ + \sum_{k\in[\![1,p+1]\!]} \delta_{\ell,k+p}^{[2]} f_{p^2} f_{pk} T^{p^2+pk} + \sum_{j\in[\![2,p-1]\!]} \delta_{\ell,j+p}^{[2]} f_{p^3} f_{p^2 j} T^{p^3+p^2 j} \\ + \sum_{k\in[\![1,p+1]\!]} \delta_{\ell,k+p^2}^{[2]} f_{p^3} f_{pk} T^{p^3+pk} + \sum_{j\in[\![p+2,p^2-1]\!]} \delta_{\ell,j} f_{pj} T^{pj} \\ + \sum_{k\in[\![1,p^2+p+1]\!]} \delta_{\ell,k} f_k T^k \end{array} \right. \tag{5.3}$$

While this expansion looks scary we can start noticing that because the p-th power map induces an automorphism of multiplicative representatives, considering the expansion modulo p^3 all conditions stated in Theorem 3.1 must be satisfied with f_{pi} in place of f_i. Consequently put $F_i = \overline{f_i/p}$ for $i = p^2, p^3$, $G_i = \overline{g_i/p^2}$ for $i \in p[\![1,p+1]\!]$ or $i \in p^2[\![2,p-1]\!]$, let $A(Y) = F_{p^3}Y^p + F_{p^2}Y$ and put $V = A(\kappa_K)$. Such conditions are satisfied if and only if V has codimension 1 in κ_K and the norms contained in $U_{1,K}$ or $U_{2,K}$ are respectively in $1 + pV$ and $1 + p^2V$, so we will only have to consider the norms in $U_{3,K}$.

Like in degree p^2, for $\ell \geq 2$ the above expression can be written as $D_\ell(\theta) = \ell \cdot \sum_{\ell|k} d_k(\theta^k)$ where the $d_\ell(T^\ell)$ are the polynomial obtained interpreting $\delta_{\ell,i}^{[m]}$ as a Kronecker's delta, and $1+\ell\cdot d_\ell(\theta) \equiv N(E(\theta\pi^\ell)) \pmod{p^4}$. For $\ell = 1$ there are exceptions because $\delta_{\ell,i}^{[m]} = 0$ for $\ell < m$.

The norms contained in $U_{3,K}$ are required to be in $1 + p^3V$, and let's concentrate first on the case of $\ell \in [\![p+2, p^2+p+1]\!]$ so that the norms $N_{L/K}(1+\theta\pi^\ell)$ already live in $U_{3,K}$, and the first few terms of the expansion disappear. For such indices ℓ, $d_\ell(\theta)$ must be in p^3V for each representative θ, and dividing by p^3 we can consider the additive polynomials $A_\ell(Y) = \overline{d_\ell(Y)/p^3}$, which, depending on ℓ, are

$$\begin{array}{cl} -G_{p(\ell-p^2)}F_{p^3}Y^p + H_\ell Y & \ell \in [\![p^2+1, p^2+p+1]\!], \\ H_{p\ell}Y^p + H_\ell Y & \ell \in [\![2p+2, p^2-1]\!], \\ F_{p^3}^2 F_{p^2} Y^{p^2} + (H_{p\ell} - F_{p^2}G_{p(p+1)})Y^p + H_\ell Y & \ell = 2p+1, \\ -F_{p^3}F_{p^2(\ell-p)}Y^{p^2} + (H_{p\ell} - F_{p^2}G_{p(\ell-p)})Y^p + H_\ell Y & \ell \in [\![p+3, 2p-1]\!], \\ (F_{p^3}F_{p^2}^2 - F_{p^3}F_{2p^2})Y^{p^2} + (H_{p\ell} - F_{p^2}G_{2p})Y^p + H_\ell Y & \ell = p+2, \end{array}$$

where we have put $H_k = \overline{f_k/p^3}$ for $k \in [\![1, p^2+p+1]\!]$ and $k \in p[\![p+2, p^2-1]\!]$.

Condition 5.2. *For each $\ell \in [\![p+2, p^2+p+1]\!]$ we require $A_\ell(\kappa_K) \subseteq A(\kappa_K)$.*

For $\ell \leq p+1$ the problem is a bit more complicated because in general the norms of $1-\theta\pi^\ell$ will not be contained in $U_{3,K}$, but a proper combination of norms of elements of this form may be, and we should require it to be in $1+p^3V$. However the elements of the form $N_{L/K}(1-\eta\pi)^p$ for some $\eta \in \mathcal{O}_K^\times$ have norms covering all possible classes in $U_{2,K}/U_{3,K}$, and consequently each $N_{L/K}(1-\theta\pi^\ell)$ can be reduced into $U_{3,K}$ multiplying it by an suitable $N_{L/K}(1-\eta\pi)^p$ for a certain η; we must test whether all such ratios are actually in $1+p^3V$, more complicated combinations will be automatically ensured to be in $1+p^3V$.

Since the map ${}^{\mathfrak{p}_K^2}/_{\mathfrak{p}_K^4} \to {}^{U_{2,K}}/_{U_{4,K}}$ induced by $x \mapsto 1+x$ is still an isomorphism we have that a suitable combination of the of $1+\theta\pi^\ell$ (e.g. via the Artin-Hasse exponential) has norm of the form $1+d_\ell(\theta)$. Depending on $2 \leq \ell \leq p+1$, the remaining term, which we call $g_\ell(Y)$, is

$$\begin{array}{rl}
\left\{-f_{p^3}f_{p^2}Y^{p^2}+f_{p^2+p}Y^p\right\}-f_{p^2}f_pY^p+f_{p+1}Y & \ell=p+1,\\
\left\{f_{p^2\ell}Y^{p^2}+f_{p\ell}Y^p\right\}-f_{p^2}f_{p^2(\ell-1)}Y^{p^2}+f_\ell Y & \ell\in[4,p-1],\\
\left\{f_{3p^2}Y^{p^2}+f_{3p}Y^p\right\}+\tfrac{1}{3}f_{p^3}^3Y^{p^3}+\tfrac{1}{3}f_{p^2}^3Y^{p^2} & \\
-f_{p^2}f_{2p^2}Y^{p^2}+f_3Y & \ell=3,\\
\left\{-\tfrac{1}{2}f_{p^3}^2Y^{p^3}+\left(f_{2p^2}-\tfrac{1}{2}f_{p^2}^2\right)Y^{p^2}+f_{2p}Y^p\right\}+f_2Y & \ell=2,
\end{array}$$

where under braces are the terms that are not identically in $\mathfrak{p}_K^3$. On the other hand

$$N(1+\eta\pi)=1+f_{p^3}\eta^{p^3}+f_{p^2}\eta^{p^2}+f_p\eta^p \mod p^2V$$

and consequently

$$N(1+\eta\pi)^p=1+\left\{pf_{p^3}\eta^{p^3}+pf_{p^2}\eta^{p^2}\right\}+pf_p\eta^p \mod p^3V,$$

where the terms under braces are again those not identically in $\mathfrak{p}_K^3$. Consequently let's consider the polynomial

$$h(Z)=\{pf_{p^3}Z^{p^2}+pf_{p^2}Z^p\}+pf_pZ,$$

for fixed Y we will look for $Z=\phi_\ell(Y)$ such that $g_\ell(Y)-h(\phi_\ell(Y)) \in \mathfrak{p}_K^3$, in order to require it to be in p^3V as well. Since we obtain an additive polynomial when g_ℓ and h are divided by p^2 and reduced to κ_K, for each ℓ we can take a ϕ_ℓ that is the preimage of a suitable additive polynomial with coefficients in κ_K.

The additive polynomials $\overline{{}^{g_\ell(Y)}/_{p^2}}$, which we denote by $B_\ell(Y^p)$ replacing Y^p by Y, are forced to have image contained V, that is the image of $\overline{{}^{h(Y)}/_{p^2}} = A(Y^p)$, and the condition is that $B_\ell(Y)=A(D_\ell(Y))$ for some other additive polynomial $D_\ell(Y)$ whose coefficients can be deduced easily.

In particular, being $A(Y) = F_{p^3}Y^p + F_{p^2}Y$ and $B_\ell(Y)$ the polynomials

$$\begin{array}{cl} -F_{p^2}F_{p^3}Y^p + G_{p^2+p}Y & \ell = p+1, \\ G_{p^2\ell}Y^p + G_{p\ell}Y & \ell \in [3,\ p-1], \\ -\frac{1}{2}F_{p^3}^2 Y^{p^2} + \left(G_{2p^2} - \frac{1}{2}F_{p^2}^2\right) Y^p + G_{2p}Y & \ell = 2, \end{array} \tag{5.4}$$

in view of Prop. 2.2 we can take as $D_\ell(Y)$ the polynomials

$$\begin{array}{cl} G_{p\ell}/F_{p^2}Y & \ell \in [3,\ p+1], \\ -\frac{1}{2}F_{p^3}^{1/p}Y^{p^2} + G_{2p}/F_{p^2}Y & \ell = 2. \end{array} \tag{5.5}$$

Now, $B_\ell(Y^p) = A((D_\ell^{1/p}(Y))^p)$ where $D_\ell^{1/p}(Y)$ is $D_\ell(Y)$ with the map $x \mapsto x^{1/p}$ applied to the coefficients. Given the definitions of $A(Y)$ and $B_\ell(Y)$ in terms of the $h(Y)$ and $g_\ell(Y)$, we can take as $\phi_\ell(Y)$ any lifting of $D_\ell^{1/p}(Y)$ to $\mathcal{O}_K[Y]$.

For $3 \leq \ell \leq p+1$ let's take a $\rho \in \mathcal{O}_K$ such that $\bar{\rho}^p = G_{p\ell}/F_{p^2} = \overline{f_{p\ell}/pf_{p^2}}$, then $D_\ell(Y) = \bar{\rho}^p Y$ and we can take $\phi_\ell(Y) = \rho Y$, and the condition is that all polynomials $\overline{\frac{1}{p^3}(g_\ell(Y) - h(\phi_\ell(Y)))}$ must take values in V. Considering that

$$h(\phi_\ell(Y)) = \left\{pf_{p^3}\rho^{p^2}Y^{p^2} + pf_{p^2}\rho^pY^p\right\} + pf_p\rho Y,$$

depending on ℓ they are

$$\begin{gathered} \overline{\left(-f_{p^3}f_{p^2}/p^3 - f_{p^3}\rho^{p^2}/p^2\right)}Y^{p^2} \\ + \left[\overline{(f_{p^2+p}/p^3 - f_{p^2}\rho^p/p^2)} - F_{p^2}G_p\right] Y^p + (H_{p+1} - G_p\bar{\rho})Y \end{gathered}$$

for $\ell = p+1$,

$$\begin{gathered} \left[\overline{\left(-f_{p^2\ell}/p^3 - f_{p^3}\rho^{p^2}/p^2\right)} - F_{p^2}G_{p^2(\ell-1)}\right] Y^{p^2} \\ +\overline{(f_{p\ell}/p^3 - f_{p^2}\rho^p/p^2)}Y^p + (H_\ell - G_p\bar{\rho})Y, \end{gathered}$$

for $4 \leq \ell = p-1$, and

$$\begin{gathered} \frac{1}{3}F_{p^3}^3Y^{p^3} + \left[\overline{\left(f_{3p^2}/p^3 - f_{p^3}\rho^{p^2}/p^2\right)} + \frac{1}{3}F_{p^2}^3 - F_{p^2}G_{2p^2}\right] Y^{p^2} \\ +\overline{(f_{3p}/p^3 - f_{p^2}\rho^p/p^2)}Y^p + (H_3 - G_p\bar{\rho})Y \end{gathered}$$

for $\ell = 3$.

For $\ell = 2$ let's take $\rho, \tau \in \mathcal{O}_K$ such that $\bar{\rho}^p = G_{p2}/F_{p^2} = \overline{f_{p2}/pf_{p^2}}$ and $\bar{\tau}^{p^2} = -\frac{1}{2}F_{p^3} = -\frac{1}{2}\overline{f_{p^3}/p^3}$. Then $D_\ell(Y) = \bar{\tau}^pY^p + \bar{\rho}^pY$ so that we can take

$\phi_2(Y) = \tau Y^p + \rho Y$, and we have

$$\begin{aligned} h(\phi_2(Y)) &= \Big\{ pf_{p^3}(\tau Y^p + \rho Y)^{p^2} + pf_{p^2}(\tau Y^p + \rho Y)^p \Big\} + pf_p(\tau Y^p + \rho Y) \\ &= pf_{p^3}\tau^{p^3}Y^{p^3} + pf_{p^3}\rho^{p^2}Y^{p^2} + pf_{p^3}\sum_{i=1}^{p-1}\binom{p^2}{ip}\tau^{ip}\rho^{(p-i)p}Y^{ip^2+(p-1)p} + \mathcal{O}(p^4) \\ &\qquad +pf_{p^2}\tau^{p^2}Y^{p^2} + pf_{p^2}\rho^pY^p + pf_{p^2}\sum_{i=1}^{p-1}\binom{p}{i}\tau^i\rho^{(p-i)}Y^{ip+(p-1)} \\ &\qquad\qquad +pf_p\tau Y^p + pf_p\rho Y. \end{aligned}$$

Considering that $\frac{1}{p}\binom{p}{i} \equiv \frac{1}{p}\binom{p^2}{ip} \pmod{p}$ and the terms in the sums can be paired in elements that are $pf_{p^3}\binom{p^2}{ip}Z^p + pf_{p^2}\binom{p}{i}Z$ for $Z = \tau^i\rho^{(p-i)}Y^{ip+(p-1)}$ and hence in p^3V for each Z, it follows that up to some element in p^3V we can write $h(\phi_2(Y))$ as

$$pf_{p^3}\tau^{p^3}Y^{p^3} + (pf_{p^3}\rho^{p^2} + pf_{p^2}\tau^{p^2})Y^{p^2} + (pf_{p^2}\rho^p + pf_p\tau)Y^p + pf_p\rho Y.$$

Consequently up to some element of V the polynomial $\overline{\frac{1}{p^3}(g_2(Y) - h(\phi_2(Y)))}$ is the

$$\overline{\left(-\frac{1}{2}f_{p^3}^2/p^3 - f_{p^3}\tau^{p^3}/p^2\right)}Y^{p^3} + \overline{\left(f_{2p^2}/p^3 - \frac{1}{2}f_{p^2}^2/p^3 - f_{p^3}\rho^{p^2}/p^2 - f_{p^2}\tau^{p^2}/p^2\right)}Y^{p^2} \\ + \left(\overline{(f_{2p}/p^3 - f_{p^2}\rho^p/p^2)} - G_p\tau\right)Y^p + (H_2 - G_p\bar{\rho})\,Y,$$

which is required to take values in V.

One last effort is required: for $\ell = 1$ in the case that $1 - \theta\pi$ has norm in $U_{2,K}$ (and hence in $1 + p^2V$). That is, when θ is such that $A(\bar{\theta}^{p^2}) = 0$, the norm of $(1 - \theta\pi)(1 - \eta\pi)^{-p}$ must be $\in 1 + p^3V$, for all η making said norm in $U_{3,K}$.

Let $\theta = T$ be as required, the terms that disappear because $\ell = 1$ are

$$\frac{1}{2}f_{p^2}^2T^{2p^2} + f_{p^3}f_{p^2}T^{p^3+p^2} + \frac{1}{2}f_{p^3}^2T^{2p^3} = \frac{1}{2}\left(f_{p^2}T^{p^2} + f_{p^3}T^{p^3}\right)^2,$$

then

$$\frac{1}{3}f_{p^2}^3T^{3p^2} + f_{p^3}f_{p^2}^2T^{p^3+2p^2} + f_{p^3}^2f_{p^2}T^{2p^3+p^2} + \frac{1}{3}f_{p^3}^3T^{3p^3} = \\ \frac{1}{3}\left(f_{p^2}T^{p^2} + f_{p^3}T^{p^3}\right)^3,$$

and the sums can be decomposed as sums of $(f_{p^2}T^{p^2} + f_{p^3}T^{p^3})f_{p^2j}T^{p^2j}$ and of $(f_{p^2}T^{p^2} + f_{p^3}T^{p^3})f_{pk}T^{pk}$, and in particular all such terms are in $\mathfrak{p}_K^4$ considering the hypotheses on T.

Consequently such terms can be assumed to be present, and removing the extra terms we already studied (or considering the norm of $E(\theta\pi)$) the remaining terms are

$$w(T) = f_{p^3}T^{p^3} + f_{p^2}T^{p^2} - f_{p^2}f_{p^3-p^2}T^{p^2} + f_pT^p + f_1T.$$

Assume $\overline{\frac{1}{p^2}\left(f_{p^3}\theta^{p^3} + f_{p^3}\theta^{p^2} + f_p\theta^p\right)}$ can be written as $F_{p^3}\bar{\alpha}^{p^2} + F_{p^2}\bar{\alpha}^p$ for some $\bar{\alpha}$, then taking any lift α of $\bar{\alpha}$ we can consider $w(\theta) - h(\alpha)$, which comes from a norm of the required type, and should be in p^3V.

At last, we can state the

Theorem 5.1. *Let K be an unramified extension of $\mathbb{Q}_p$, $p \neq 2$. The Eisenstein polynomial $f(X) = X^{p^3} + f_1X^{p^3-1} + \cdots + f_{p^3-1}X + f_{p^3}$ determines a cyclic extension of degree p^3 over K if and only if*

(1) $v_p(f_{p^2}) = 1$ *and* $v_p(f_{p^2i}) \geq 2$ *for* $i \in \llbracket 2, p-1 \rrbracket$,

(2) $v_p(f_{pi}) \geq 2$ *for all* $i \in \llbracket 1, p-1 \rrbracket$, $v_p(f_{p^2+p}) = 2$, *and* $v_p(f_{pi}) \geq 3$ *for all* $i \in \llbracket p+1, p^2-1 \rrbracket$,

(3) $v_p(f_i) \geq 3$ *for all* $i \in \llbracket 1, p^2+p-1 \rrbracket$, $v_p(f_{p^2+p+1}) = 3$ *and* $v_p(f_i) \geq 4$ *for all* $i \in \llbracket p^2+p+2, p^3-1 \rrbracket$,

putting $F_{p^2} = \overline{f_{p^2}/p}$, $F_{p^3} = \overline{f_{p^3}/p}$, *and* $\overline{G_i = f_i/p^2}$ *for all i in* $p^2\llbracket 2, p-1 \rrbracket$ *or in* $p\llbracket 1, p+1 \rrbracket$ *we have*

(4) $-F_{p^2}/F_{p^3} \in \kappa_K^{p-1}$,

(5) $G_{p(p+1)}^p = -F_{p^2}^{p+1}$,

(6) $G_{p^2\ell} = F_{p^3}\left(G_{\ell p}/F_{p^2}\right)^p$ *for* $\ell \in \llbracket 3, p-1 \rrbracket$,

(7) $G_{2p^2} = F_{p^3}\left(G_{2p}/F_{p^2}\right)^p + \frac{1}{2}F_{p^2}\left(F_{p^2} - F_{p^3}^{1/p}\right)$,

if ρ is such that $\bar{\rho}^{p(p-1)} = -F_{p^2}/F_{p^3}$ *we have (independently of ρ)*

(8) $\overline{\frac{1}{p^2}\left(f_{p^3}\rho^{p^2} + f_{p^2}\rho^p + f_p\rho\right)} = F_{p^3}\alpha^p + F_{p^2}\alpha$ *for some* $\alpha \in \kappa_K$,

putting $H_i = \overline{f_i/p^3}$ *for i in* $\llbracket 1, p^2+p+1 \rrbracket$ *or in* $p\llbracket p+2, p^2-1 \rrbracket$ *we have*

(9) $-G_{p(\ell-p^2)}F_{p^3} = F_{p^3}(H_\ell/F_{p^2})^p$ *for* $\ell \in \llbracket p^2+1, p^2+p+1 \rrbracket$,

(10) $H_{p\ell} = F_{p^3}(H_\ell/F_{p^2})^p$ *for* $\ell \in \llbracket 2p+2, p^2-1 \rrbracket$,

(11) $H_{p(2p+1)} - F_{p^2}G_{p(p+1)} = F_{p^3}(H_{2p+1}/F_{p^2})^p + F_{p^2}(F_{p^3}F_{p^2})^{1/p}$,

(12) $H_{p\ell} - F_{p^2}G_{p(\ell-p)} = F_{p^3}(H_\ell/F_{p^2})^p - F_{p^2}(F_{p^2(\ell-p)})^{1/p}$ *for* $\ell \in \llbracket p+3, 2p-1 \rrbracket$,

(13) $H_{p(p+2)} - F_{p^2}G_{2p} = F_{p^3}(H_{p+2}/F_{p^2})^p + F_{p^2}(F_{p^2}^2 - F_{2p^2})^{1/p}$,

for each $\ell \in \llbracket 3, p+1 \rrbracket$, *let ρ_ℓ be such that* $\bar{\rho}_\ell^p = G_{p\ell}/F_{p^2}$. *Then*

(14) *putting* $P_{p+1} = H_{p+1} - G_p\bar{\rho}_{p+1}$,

$$Q_{p+1} = \overline{(f_{p^2+p}/p^3 - f_{p^2}\rho_{p+1}^p/p^2)} - F_{p^2}G_p, \quad R_{p+1} = \overline{\left(-f_{p^3}f_{p^2}/p^3 - f_{p^3}\rho_{p+1}^{p^2}/p^2\right)},$$

we have $Q_{p+1} = F_{p^3}({}^{P_{p+1}}/{}_{F_{p^2}})^p + F_{p^2}({}^{R_{p+1}}/{}_{F_{p^3}})^{1/p}$,

(15) for each $4 \leq \ell \leq p-1$ *putting* $P_\ell = H_\ell - G_p\bar{\rho}_\ell$,

$$Q_\ell = \overline{({}^{f_{p\ell}}/{}_{p^3} - {}^{f_{p^2}\rho_\ell^p}/{}_{p^2})} - F_{p^2}G_p, \quad R_\ell = \overline{\left(-{}^{f_{p^2\ell}}/{}_{p^3} - {}^{f_{p^3}\rho_\ell^{p^2}}/{}_{p^2}\right)} - F_{p^2}G_{p^2(\ell-1)},$$

we have $Q_\ell = F_{p^3}({}^{P_\ell}/{}_{F_{p^2}})^p + F_{p^2}({}^{R_\ell}/{}_{F_{p^3}})^{1/p}$,

(16) putting $P_3 = H_3 - G_p\bar{\rho}_3$,

$$Q_3 = \overline{({}^{f_{3p}}/{}_{p^3} - {}^{f_{p^2}\rho_3^p}/{}_{p^2})}, \qquad R_3 = \overline{\left({}^{f_{3p^2}}/{}_{p^3} - {}^{f_{p^3}\rho_3^{p^2}}/{}_{p^2}\right)} + \frac{1}{3}F_{p^2}^3 - F_{p^2}G_{2p^2}$$

we have $\frac{1}{3}F_{p^2}(F_{p^3}^2)^{1/p} + F_{p^3}({}^{Q_3}/{}_{F_{p^2}})^p = R_3 + F_{p^3}({}^{F_{p^3}}/{}_{F_{p^2}})^p({}^{P_3}/{}_{F_{p^2}})^{p^2}$,

let $\rho_2, \tau_2 \in \mathcal{O}_K$ *such that* $\bar{\rho}_2^p = {}^{G_{p^2}}/{}_{F_{p^2}}$ *and* $\bar{\tau}_2^{p^2} = -\frac{1}{2}F_{p^3}$. *Then*

(17) putting

$$P_2 = H_2 - G_p\bar{\rho}, \qquad Q_2 = \overline{({}^{f_{2p}}/{}_{p^3} - {}^{f_{p^2}\rho^p}/{}_{p^2})} - G_p\bar{\tau},$$

$$R_2 = \overline{\left({}^{f_{2p^2}}/{}_{p^3} - \frac{1}{2}{}^{f_{p^2}^2}/{}_{p^3} - {}^{f_{p^3}\rho^{p^2}}/{}_{p^2} - {}^{f_{p^2}\tau^{p^2}}/{}_{p^2}\right)}, \ S_2 = \overline{\left(-\frac{1}{2}{}^{f_{p^3}^2}/{}_{p^3} - {}^{f_{p^3}\tau^{p^3}}/{}_{p^2}\right)}$$

we have $F_{p^2}({}^{S_2}/{}_{F_{p^3}})^{1/p} + F_{p^3}({}^{Q_2}/{}_{F_{p^2}})^p = R_2 + F_{p^3}({}^{F_{p^3}}/{}_{F_{p^2}})^p({}^{P_2}/{}_{F_{p^2}})^{p^2}$,

if ρ, ξ *are such that* $\bar{\rho}^{p^2(p-1)} = -{}^{F_{p^2}}/{}_{F_{p^3}}$ *and*

$$\overline{\frac{1}{p^2}\left(f_{p^3}\rho^{p^3} + f_{p^2}\rho^{p^2} + f_p\rho^p\right)} = F_{p^3}\bar{\xi}^{p^2} + F_{p^2}\bar{\xi}^p,$$

(18) we have that

$$\overline{\frac{1}{p^3}\left(f_{p^3}(\rho^{p^3} - \xi^{p^2}) + f_{p^2}(\rho^{p^2} - \xi^p) + f_p(\rho^p - \xi) - f_{p^2}f_{p^3-p^2}\rho^{p^2} + f_1\rho\right)}$$

is also of the form $F_{p^3}\bar{\omega}^p + F_{p^2}\bar{\omega}$ *for some* $\bar{\omega} \in \kappa_K$.

6. Sums of roots of unity

We finally prove the lemma about the $\Sigma_\lambda(\ell)$, it is actually much more than needed but nevertheless is has a nice statement, and could be useful in similar circumstances:

Lemma 6.1. *Let* $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r)$ *be an* r*-tuple, then*

$$\Sigma_\lambda(\ell) = \sum_{\lambda = \sqcup_{j\in J}\lambda^{(j)}} \ell^{\#J} \cdot \prod_{j\in J}(-1)^{\#\lambda^{(j)}-1}(\#\lambda^{(j)} - 1)!$$

where the sum is over all partitions $\lambda = \bigsqcup_{j\in J}\lambda^{(j)}$ *(as set) such that for each* $j \in J$ *the sum* $|\lambda^{(j)}|$ *of the elements in* $\lambda^{(j)}$ *is multiple of* ℓ *and* $\#\lambda^{(j)}$ *is the cardinality of the subset* $\lambda^{(j)}$.

Proof. Let A_0 the set of all possible indices in the sum (with no constraint)

$$A_0 = \{0, 1, \dots, \ell - 1\}^r = \Big\{(\iota_1, \dots, \iota_r) \mid \iota_i \in \{0, 1, \dots, \ell - 1\}, \forall i\Big\},$$

and, for each pair of integers (i, j), let $A_{(i,j)}$ be the subset of of indices $(\iota_1, \dots, \iota_r)$ such that $\iota_i = \iota_j$. For each $A \subseteq A_0$ denote by $\Sigma(A)$ the sum over all the indices in A. By inclusion-exclusion we have that

$$\begin{aligned}\Sigma_\lambda(\ell) &= \Sigma(A_0) - \Sigma(\cup_{(i,j)} A_{(i,j)}) \\ &= \Sigma(A_0) - \sum_{(i,j)} \Sigma(A_{(i,j)}) + \sum_{(i,j) \neq (i',j')} \Sigma(A_{(i,j)} \cap A_{(i',j')}) - \dots\end{aligned}$$

Now let A be the intersection of all the sets $A_{(i_k,j_k)}$ for any collection of pairs

$$P = \{(i_1, j_1), \dots, (i_s, j_s)\}_{s \in S}$$

(indexed by $s \in S$, say). Let's consider the graph with $R = \{1, \dots, r\}$ as vertices and the (i_k, j_k) as edges; splitting R in connected components $R = \sqcup_{t \in T} R_t$ (indexed by $t \in T$, say) we can see that the allowed indices $\iota \in A$ are those constant on each R_t; calling ι_t the value taken on R_t the sum $\Sigma(A)$ becomes

$$\Sigma(A) = \prod_{t \in T} \sum_{\iota_t = 0}^{\ell - 1} \zeta_\ell^{\iota_t (\sum_{r \in R_t} \lambda_r)},$$

and this sum is $\ell^{\# T}$ when all the $\sum_{r \in R_t} \lambda_r$ are multiple of ℓ, and 0 if not. Note that $\Sigma(A)$ appears with sign equal to $(-1)^{\# S}$ in the inclusion-exclusion, so for each partition of R in sets R_t such that the sum of λ_r for $r \in R_t$ is multiple of ℓ we have to consider the all graphs with set of vertices R and such that each R_t is a connected component, and count the number of graphs with an even number of edges minus those with a odd number of edges. Now the total difference is the product of the differences over all the connected components, so we have

$$\Sigma_\lambda(\ell) = \sum_{\lambda = \sqcup_{j \in J} \lambda^{(j)}} \ell^{\# J} \cdot \prod K_{\# \lambda^{(j)}}$$

where for each i we denote by K_i the difference of the numbers of connected graphs on i vertices having an even and odd number of edges.

The difference of the number of connected graphs K_i on i vertices with an even or odd number of vertices can be computed fixing an edge, and considering the graphs obtained adding or removing that edge. Those such that with or without it are connected come in pairs with an even and odd number of edges, the other graphs are obtained connecting two other connected graphs on j and $i-j$ vertices. In particular choosing $j-1$ vertices to make one component with the first vertex of our distinguished edge we obtain

$$K_{i+2} = -\sum_{j=0}^{i} \binom{i}{j} K_{i-j+1} K_{j+1}$$

for $i \geq 0$, and $K_1 = 1$. Calling $G(X)$ the exponential generating function $\sum_{i=0}^{\infty} \frac{K_{i+1}}{i!} X^i$ we obtain that

$$\frac{d}{dX} G(X) = -G(X)^2$$

with the additional condition that $K_1 = 1$, and this equation is clearly satisfied by $1/(1+X)$, which can be the only solution. Consequently $K_{i+1} = (-1)^i \cdot i!$ and the lemma is proved. □

References

[Cap07] L. Caputo, *A classification of the extensions of degree p^2 over $\mathbb{Q}_p$ whose normal closure is a p-extension.* Journal de théorie des nombres de Bordeaux **19** (2007), no. 2, 337–355.

[FV02] I. B. Fesenko and S. V. Vostokov, *Local fields and their extensions.* American Mathematical Society, 2002.

[GP12] C. Greve and S. Pauli, *Ramification polygons, splitting fields, and galois groups of eisenstein polynomials.* International Journal of Number Theory **8** (2012), no. 06, 1401–1424.

[Kra62] M. Krasner, *Nombre des extensions d'un degré donné d'un corps $\mathfrak{p}$-adique.* C. R. Acad. Sc. Paris **254** (1962), 3470–3472, *ibidem* **255** (1962), 224–226, 1682–1684, 2342–2344, 3095–3097.

[Lbe09] A. Lbekkouri, *On the construction of normal wildly ramified extensions over $\mathbb{Q}_p$, ($p \neq 2$).* Archiv der Mathematik **93** (2009), no. 4, 331–344.

[Mau71] E. Maus, *On the jumps in the series of ramifications groups.* Bull. Soc. math. France **25** (1971), 127–133.

[Mik81] H. Miki, *On the ramification numbers of cyclic p-extensions over local fields.* Journal für die Reine und Angewandte Mathematik **328** (1981), 99–115.

[MP99] J. Montes Peral, *Polígonos de newton de orden superior y aplicaciones aritméticas.* Ph.D. thesis, Universitat de Barcelona, 1999.

[MS05] J. Mináč and J. Swallow, *Galois embedding problems with cyclic quotient of order p.* Israel Journal of Mathematics **145** (2005), no. 1, 93–112.

[Ore28] Ö. Ore, *Newtonsche polygone in der theorie der algebraischen körper.* Mathematische Annalen **99** (1928), no. 1, 84–117.

[Wat94] W. C. Waterhouse, *The normal closures of certain Kummer extensions.* Canad. Math. Bull **37** (1994), no. 1, 133–139.

Maurizio Monge
Instituto de Matemática da UFRJ,
Av. Athos da Silveira Ramos 149, Centro de Tecnologia
Bloco C Cidade Universitária
Ilha do Fundão
Caixa Postal 68530 21941-909
Rio de Janeiro - RJ - Brasil
E-mail: `maurizio.monge@im.ufrj.br`