POWER CLASSES OF AN EXTENSION OF DEGREE p OF A $\mathfrak{p}$-ADIC FIELD AS FILTERED GALOIS MODULE

MAURIZIO MONGE

ABSTRACT. Let K be a $\mathfrak{p}$-adic field, and let L/K be a totally ramified Galois cyclic extension of degree p. We describe the structure of the group of p-th power classes ${}^{L^\times}/{}_{(L^\times)^p}$ considered as a Galois module and a filtered abelian group simultaneously. In particular we explain how it is possible to derive explicitly the indecomposable factors of the group ${}^{U_{i,L}(L^\times)^p}/{}_{(L^\times)^p}$ of power classes represented by the i-th unit group $U_{i,L}$ of L, for $i \geq 0$.

1. Introduction

Let K be a $\mathfrak{p}$-adic field, that is a finite extension of the rational $\mathfrak{p}$-adic field $\mathbb{Q}_p$, and let L/K be a totally ramified Galois cyclic extension of degree p, with $G = \mathrm{Gal}(L/K)$. If L (and hence K) contains a primitive p-th root of the unity let's fix one of them once for all and denote it by ζ_p. For any field F and a subset $X \subseteq F^\times$, or element $x \in F$, we will denote by $[X]_F$ and by $[x]_F$ the image under the map of reduction modulo p-th powers $F^\times \to {}^{F^\times}/{}_{(F^\times)^p}$. For a $\mathfrak{p}$-adic field F we put $e_F = e(F/\mathbb{Q}_p)$ and $f_F = f(F/\mathbb{Q}_p)$ for the absolute ramification index and inertia degree, and $U_i = U_{i,F}$ for the i-th group of principal units, we refer to [FV02, Ser79] for these standard definitions as well as for ramification theory and local class field theory.

By local class field theory, or by Kummer theory when $\zeta_p \in L$, we have that the module $[L^\times]_L = {}^{L^\times}/{}_{(L^\times)^p}$ describes the maximal p-elementary abelian extension of L. One cyclic extension F/L of degree p correspond to a subspace $N = [N_{F/L}(F^\times)]_L$ of codimension 1 of $[L^\times]_L$ by local class field theory (resp. Δ of dimension 1 such that $F = L(\Delta^{1/p})$ by Kummer theory, when $\zeta_p \in L$). Local class field theory gives an isomorphism ${}^{L^\times}/{}_{N_{F/L}(F^\times)} \to \mathrm{Gal}(F/L)$ mapping $U_{i,L}$ to the i-th ramification subgroup, and the ramification break of the extension F/L is given in local class field theory by the biggest integer i such that $[U_i]_L \not\subseteq N$. Via Kummer theory the ramification break is instead obtained as ${}^{pe_K}/{}_{p-1} - i$, where i is the biggest integer such that $[U_i]_L \supseteq N$. It is the index of a class α such that $F = L(\alpha^{1/p})$ in the filtration $[U_i]_L$, an invariant which is also known as "defect" and whose connection with the ramification break is well known, see [Wym69, §4] for more details.

On the other hand any elementary abelian p-extension of L is Galois over K if and only if the corresponding quotient in $[L]_L$ by local class field theory (resp. submodule by Kummer theory) is a module under the action of $\mathrm{Gal}(L/K)$, and consequently the normal closure over K of the extension F/L corresponds to the biggest submodule contained in N by local class field theory (resp. to the module generated by Δ by Kummer theory if $\zeta_p \in L$). We refer to the [Wat94, MS05] for a comprehensive study of the possible Galois groups of the normal closure of a tower formed by two cyclic extensions of degree p.

Let C_p be the cyclic group of order p, the indecomposable modules over the group algebra $\mathbb{F}_p[C_p]$ are classified by their composition length which can be any

Date: November 6, 2011.

positive integer $\leq p$, and each module generated by one element is indecomposable. Consequently if we know the factorization in indecomposables of ${}^{[L^\times]_L}/{}_{[U_{i+1}]_L}$ and of ${}^{[L^\times]_L}/{}_{[U_i]_L}$ for some i depending on the ramification break of F/L (resp. of $[U_i]_L$ and $[U_{i+1}]_L$ with Kummer theory) we can give precise bounds on the length of the module spawn over $\mathbb{F}_p[G]$ for $G = \mathrm{Gal}(L/K)$, deriving information about the Galois group of the normal closure of F over K in dependence of the ramification break.

This connection between ramification numbers and the Galois theoretic structure motivates the present paper, where we study the interaction of these two different structures and look for an explicit description of $[L^\times]_L$ as filtered Galois module. While it is hard to write an explicit formula giving the factorization of $[U_i]_L$ into indecomposables, we describe how it is possible to obtain inductively such a decomposition.

The multiplicative group $L^\times$ of a local field as abstract Galois module was studied by Borevic in [Bor65] and subsequent papers, while Mináč-Schultz-Swallow gave in [MS03, MSS06] a description of $[L^\times]_L$ for a field extension of p-th power degree in a very general setting. In [Pak84] it was determined by Pak the structure of U_i as a $\mathbb{Z}_p[G]$-module in characteristic p.

In [Gor82] it was obtained an arithmetical description by generators and relations of a Galois group of a local field which is extension of a cyclic group of order p with abelian kernel, under some additional hypothesis on the ramification number of the cyclic extension and on the p-th roots of the unity contained in the field. Such description is quite complicated, but it shows that the knowledge of the ramification break of the cyclic extension and of the roots of the unity contained in the field is generally sufficient to determine almost uniquely the ramification subgroups, and could certainly be used to recover a decomposition of the $[U_i]_L$ in indecomposable $\mathbb{F}_p[G]$-modules via class field theory. We give in this note a result where this structure is clearly evidenced.

2. Structure of $[L^\times]_L$ as filtered module

Let $M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \dots$ be a finitely generated filtered vector space over $\mathbb{F}_p$, we will say that a basis $\{x_j\}_{1\leq j\leq m}$ is *adapted to the filtration* if for each i the elements x_j that are contained in M_i generate M_i. If $M'' \subseteq M' \subseteq M$ are submodules, we call *natural filtration* of the subquotient $\tilde{M} = {}^{M'}/{}_{M''}$ the filtration obtained putting

$$\tilde{M}_i = {}^{(M_i \cap M')M''}/{}_{M''} = {}^{M_i M''}/{}_{M''} \cap {}^{M'}/{}_{M''}$$

for each $i \leq 0$, thanks to the last equality we have that the filtration obtained restricting to M' and then quotienting by M'' is equal to the filtration obtained quotienting by M'' first, and then restricting to ${}^{M'}/{}_{M''}$.

Let now L/K be a cyclic Galois extension of degree p with $G = \mathrm{Gal}(L/K)$ generated by the fixed element σ and having unique ramification break s. This is the unique integer such that for each uniformizing element π of L we have

$$\frac{\sigma(\pi)}{\pi} = 1 + \eta\pi^s + \mathcal{O}(\pi^{s+1}),$$

for a suitable unit η.

We take M to be the group of p-th power classes $[L^\times]_L$ with the natural filtration obtained putting $M_0 = M$ and $M_i = [U_i]_L$. Put $I_L = {}^{pe_k}/{}_{p-1}$ for convenience, so that M_{I_L} is the last non-zero element of the filtration when $\zeta_p \in L$ and is 0 when $\zeta_p \notin L$.

For $x \in M$ we will denote $x^{(r)} = x^{(\sigma-1)^r}$, note that $x^{(p)}$ is always 0 being $(\sigma - 1)^p = 0$. Put $\ell(x)$ to be the length of the module generated by x, $\partial(x)$ its index in the filtration, that is the superior extremum of the i such that $x \in M_i$, and put $\Gamma(x)$ to be the biggest index of the elements $x+y$, for all y generating a module of smaller length than x, and which we will call *essential index*.

Recall that the radical of $\mathbb{F}_p[G]$ is generated by $\sigma-1$, and that for each $0 \le i \le p$ the i-th socle and radical are

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

Let $m = [K : \mathbb{Q}_p]$. We will now show that assuming a technical condition in one very special case we have the following structure theorem.

Theorem 1. *The module M is the direct sum of m indecomposable modules of maximal length p generated by elements $a_1, \dots, a_m$, plus depending on the structure of L/K*

(A) a trivial module of dimension 1 generated by an element c, when $\zeta_p \notin K$,

(B) an indecomposable module of length 2 generated by an element b, when $\zeta_p \in K$ but $\zeta_p \notin N_{L/K}(L^\times)$, and in this case let's assume additionally that

$$s > I_L/(p-1),$$

(C) a trivial module of dimension 2 generated by elements b, c, when $\zeta_p \in N_{L/K}(L^\times)$.

The modules generated by the different generators provide a factorization of M into indecomposables. Furthermore for fixed $0 \le k < p$ the set all possible elements $g^{(r)} \in \mathrm{soc}^{k+1}(M) \setminus \mathrm{soc}^k(M)$ obtained for g in the set of generator and some integer $r \ge 0$ gives a basis of ${}^{\mathrm{soc}^{k+1}(M)}/_{\mathrm{soc}^k(M)}$ which is adapted to the filtration as a subquotient.

The basis obtained is such that for each generator g we have

$$\Gamma(g^{(i)}) = \Gamma(g^{(i-1)}) + s$$

for all $0 < i < \ell(g)$ with at most one exception. For the generators a_i we have

$$\Gamma(a_i) = \psi_{L/K}(j) \qquad \Gamma(a_i^{(p-1)}) = I_L - \psi_{L/K}(I_K - j)$$

for some j, if we put $N = {}^{N_{L/K}(L^\times)((L^\times)^p \cap K^\times)}/_{(L^\times)^p \cap K^\times}$ with the natural filtration of subquotient of $[K^\times]_K$ we have that the j appearing in the above expression are those such that $N_j \supsetneq N_{j+1}$, each appearing $\dim_{\mathbb{F}_p}({}^{N_j}/_{N_{j+1}})$ times.

For b (when present), and putting $c = b^{(1)}$ in case (B)*, we have*

$$\Gamma(b) = I_L - \psi_{L/K}(\min\{ps, s+e_K\}), \qquad \Gamma(c) = I_L - \psi_{L/K}(I_K - s).$$

We prove first a helper lemma regarding how the filtration has to be translated under the map $[K^\times]_K \to [L^\times]_L$ induced by the natural inclusion $K^\times \to L^\times$.

Lemma 1. *Consider the module $M = {}^{K^\times}/_{K^\times \cap (L^\times)^p}$ with the filtration induced as a quotient of $[K^\times]_K$, that is induced by the reduction of the $U_{i,K}$. Consider the injection $\iota : M \to [L^\times]_L$, where as usual $[L^\times]_L$ is equipped with the filtration induced by the $U_{i,L}$. Then for each $x \in M$ we have $\partial(\iota(x)) = I_L - \psi_{L/K}(I_K - \partial(x))$.*

This is a slight rework of [NQD76, Prop. 3.2.2], but since we are working with ${}^{K^\times}/_{K^\times \cap (L^\times)^p}$ rather than with $[K^\times]_K$ we don't have to exclude any value of $\partial(x)$. We refer to the characterization of ramification breaks in terms of the defects as proved in [Wym69, §4, Theo. 11 and 12], these results hold even when $\zeta_p \notin L$, considering that taking the compositum with a tamely ramified extension both the defects and the ramification numbers are multiplied by a constant.

Proof. If $\zeta_p \in K$, let Δ be the preimage in $[K]_K$ of the module generated by x in M. It is a subspace of dimension 2 of $[K]_K$, and for each subspace, generated by κ say, we have a subextension $K(\kappa^{1/p})$ of $K(\Delta^{1/p})$ with ramification break $I_K - \partial(\kappa)$, those breaks run over all the upper ramification breaks of $K(\Delta^{1/p})/K$ being it an abelian elementary p-extension. Taking a representative in $[K^\times]_K$ of x with biggest possible index in the filtration of $[K^\times]_K$ we have that the only upper break we can have additionally to the break s of L/K is $I_K - \partial(x)$, when this is different from s. On the other hand $K(\Delta^{1/p})/L$ has ramification break at $I_L - \partial(\iota(x))$, and hence an additional upper ramification break of L/K has to be equal to $\phi_{L/K}(I_L - \partial(\iota(x)))$ if this quantity is not s. Applying $\psi_{L/K}$ to the equality

$$I_K - \partial(x) = I_L - \partial(\iota(x))$$

we obtain the Lemma. The case with $\zeta_p \notin K$ is even easier, considering that taking the compositum with ζ_p has the effect of multiplying the defect and ramification numbers by a constants. □

Let's recall that $\mathrm{soc}^1(M)$ is respectively equal to $[K]_L$ in cases (A) and (B), and to $[K]_L \oplus \langle\delta\rangle$ for some additional class δ in case (C), see for instance [MSS06]. Since M has dimension $pm+1$ in case (A) and $pm+2$ in cases (B) and (C) we obtain immediately information about how it splits into indecomposables, considering that $\mathrm{rad}^{p-1}(M) = [N_{L/K}(L^\times)]_L$ always has dimension m. We will now construct the elements (b and) c generating a direct factor of M, whose complement is free.

The Theorem is very easy to prove when s assumes the biggest possible value I_K (see [FV02, Proposition 2.3]), and in this case we can take as a_i representatives of any filtered basis of M_1/M_{I_K}, and construct suitable elements b, c in M_0 and M_{I_L}. Consequently in the proof we will consider the case of $s < I_K$, which also implies $(p, s) = 1$.

Construction of the elements (b and) c. A representative of a generator of $K^\times/N_{L/K}(L^\times)$ can be found in U_s by local class field theory. Its index in $K^\times/K^\times\cap(L^\times)^p$ will still be s being $K^\times \cap (L^\times)^p \subseteq N_{L/K}(L^\times)$, and the index in $[K^\times]_L$ will be consequently translated to $I_L - \psi_{L/K}(I_K - s)$. Call c its image in $[L^\times]_L$. In case (A) we are done.

In case (C) the Galois embedding problem $C_{p^2} \to C_p$ can be solved for L/K, and let $\delta \in M$ be a class such that $L(\delta^{1/p})/K$ is cyclic of order p^2. Its maximum index depends on the minimal lower ramification break of $L(\delta^{1/p})/L$ over all the extensions that are cyclic of order p^2 over K. The minimal upper break is $\min\{ps, s + e_K\}$ by [Mau71, Mik81], applying $\psi_{L/K}$ we obtain the minimal lower break, and the maximal index of δ will be its complement to I_L. Take such a δ with maximal index as b.

In case (B) if $L = K(\alpha^{1/p})$ consider the class $b = [\alpha^{1/p}]_L$: the p-th roots of the elements in this class give extensions whose normal closure is the non-abelian group of order p^3 and exponent p^2. Indeed $b^{(1)} = [\zeta_p]_L$ being the conjugates of $\alpha^{1/p}$ of the form $\zeta_p^k \alpha^{1/p}$, so the normal closure is obtained as $K(\zeta_p^{1/p}, \alpha^{1/p^2})$ which has group C_{p^2} over $K(\zeta_p^{1/p})$, and group over K which is non-abelian of order p^3 and exponent p^2. For $p \geq 3$ we have that $b \notin \mathrm{rad}^{p-2}(M)$ because the non-abelian group of order p^3 and exponent p^2 is not a quotient of a group obtained as extension of C_p by an indecomposable module of length ≥ 3. Consequently we have that b generates $\mathrm{soc}^2(M)/\mathrm{rad}^{p-2}(M)$. Similarly $b^{(1)}$ generates $\mathrm{soc}^1(M)/\mathrm{rad}^{p-1}(M)$ and we can assume

$$c \equiv b^{(1)} \mod \mathrm{rad}^{p-1}(M).$$

We note that $\partial(b) = \partial([\alpha]_K)$ by the properties of the p-th power map, and consequently $\partial(b) = I_K - s$. Furthermore we have $\partial([\zeta_p]_K) \geq e_K/p-1 = v_K(1-\zeta_p)$, and since ζ_p is not a norm we must have $s \geq \partial([\zeta_p]_K)$ having $U_{\partial_K(\zeta_p)}$ non-trivial image modulo $N_{L/K}(L^\times)$. Consequently being $s \geq e_K/p-1$ we obtain the equality

$$I_K - s = I_L - \psi_{L/K}(\min\{ps, s + e_K\}),$$

so $\partial(b)$ is as stated.

The element c has the biggest possible index for elements generating $\mathrm{soc}^1(M)/\mathrm{rad}^{p-1}(M)$, and similarly for b as generator of $\mathrm{soc}^2(M)/\mathrm{rad}^{p-2}(M)$ when $s > I_K/(p-1)$, because in this case we have $\mathrm{rad}^{p-2}(M) \subset M_{I_K-s+1}$. The case $s \le I_K$ was excluded in the hypotheses of the theorem.

We now show that we can modify b by suitable elements of $\mathrm{rad}^{p-2}(M)$ in order to have exactly $b^{(1)} = c$. Indeed, we are allowed to change b by $x^{(p-2)}$ for any $x \in M_r$, where $r = I_K - (p-1)s$, and the $x^{(p-1)}$ for all $x \in M_r$ generate $\mathrm{rad}^1(M) \cap M_q$ for $q = I_L - \psi_{L/K}(I_K - \phi_{L/K}(r))$ by the properties of the norm map. We are done if we can prove that $\partial(b^{(1)} - c) \ge q$. Note that

$$\phi_{L/K}(r) = \phi_{L/K}(I_K - (p-1)s) = I_K - (p-1)s = r$$

because we have $I_K - (p-1)s \le s$ considering that $s \ge {}^{e_K}/_{p-1}$. We can show that $q \le \partial_L(\zeta_p) = \partial(b^{(1)})$ verifying that

$$I_L - \psi_{L/K}(I_K - [I_K - (p-1)s]) \le I_L - \psi_{L/K}(I_K - \partial_K(\zeta_p)).$$

Being $a \mapsto I_L - \psi_{L/K}(I_K - a)$ a monotonic increasing function of a we have to verify that

$$I_K - (p-1)s \le \partial_K(\zeta_p),$$

or

$$(p-1)s + \partial_K(\zeta_p) \ge I_K$$

which is certainly true being $\partial_K(\zeta_p)$ and s both at least ${}^{e_K}/_{p-1} = {}^{I_K}/_{p}$. Similarly we can prove that

$$q \le \partial(c) = I_L - \psi_{L/K}(I_K - s)$$

with a similar computation with s in the place of $\partial([\zeta_p]_K)$, and we are done.

Construction of the a_i. We will assume inductively that we have built a basis $\{g_i\}$ of a submodule A of M, satisfying the following hypothesis:

(1) M/A is a free $\mathbb{F}_p[G]$-module, and hence projective, and consequently A is a direct factor of M;
(2) let $S^r = \mathrm{soc}^r(M)/\mathrm{soc}^{r-1}(M)$ with the induced filtration for $1 \le r \le p$, then images of the elements $g_i^{(j)} \in \mathrm{soc}^r(M)$ which are contained in $S_k^r \setminus S_{k+1}^r$ should be linearly independent in S_k^r/S_{k+1}^r, for each r and k;
(3) for some k, the g_i are contained in S_k^p and generate S_{k+1}^p.

We point out that the second requirement is equivalent to that of having

$$\Gamma(x) = \min_{c_{i,j} \neq 0} \Gamma(g_i^{(j)})$$

whenever

$$x = \sum_{i,j} c_{i,j} g_i^{(j)},$$

and also to the requirement that for elements $\{g_i^{(j)}\}$ generating modules of the same length and with equal value of $\Gamma(g_i^{(j)})$, then any non-trivial linear combination x has equal value of $\Gamma(x)$.

Let's start with A to be the module generated by b (when present)and c. We will show that such a submodule, equipped with a basis as above, can be extended to a bigger submodule with a basis satisfying the same hypotheses.

Let k be the biggest integer such that $M_k + \mathrm{soc}^{p-1}(M)$ is not contained in $A + \mathrm{soc}^{p-1}(M)$. Then thanks to the inductive hypothesis 3 we have

$$A + \mathrm{soc}^{p-1}(M) \subset M_k + \mathrm{soc}^{p-1}(M).$$

Being $M_k + \mathrm{soc}^{p-1}(M) \supsetneq M_{k+1} + \mathrm{soc}^{p-1}(M)$ we have that $k = \psi_{L/K}(h)$ for some h by [FV02, Proposition 1.5], and let's put

$$\ell = I_L - \psi_{L/K}(I_K - h),$$

so that for each $x \in M_k$ and $\notin M_{k+1} + \mathrm{soc}^{p-1}(M)$ we have $x^{(p-1)} \in M_\ell \setminus M_{\ell+1}$. In other words if $\partial(x) = \Gamma(x) = k$ then $\partial(x^{(p-1)}) = \ell$.

Now being the $\mathbb{F}_p[G]$-module generated by x disjoint from A we certainly have $\mathrm{soc}^1(M) \cap M_\ell \nsubseteq A$. Suppose that for some i the reduction of $A \cap \mathrm{soc}^{i+1}(M)$ modulo $\mathrm{soc}^i(M)$ does not generate the quotient $S^{i+1}_{\ell-si}/S^{i+1}_{\ell-si+1}$: this amounts to saying that

$$(A + M_{\ell-si+1}) \cap \mathrm{soc}^{i+1}(M) + \mathrm{soc}^i(M) \nsupseteq M_{\ell-si} \cap \mathrm{soc}^{i+1}(M) + \mathrm{soc}^i(M). \qquad (1)$$

Assume now x to be in $M_{\ell-si} \cap \mathrm{soc}^{i+1}(M)$ but not in the left hand side, and consider $x^{(1)}$: if we had

$$x^{(1)} \in (A + M_{\ell-s(i-1)+1}) \cap \mathrm{soc}^i(M) + \mathrm{soc}^{i-1}(M)$$

then we would have also

$$x^{(i)} \in (A + M_{\ell+1}) \cap \mathrm{soc}^1(M) = A \cap \mathrm{soc}^1(M).$$

We obtain that $x^{(i)} = y^{(i)}$ for some $y \in A$, so

$$x \in A \cap \mathrm{soc}^{(i+1)}(M) + \mathrm{soc}^i(M),$$

contradicting the choice of x.

Consequently we can consider the biggest let $d < p-1$ such that the (1) hold with $i = d$, and let z be contained in $M_{\ell-sd} \cap \mathrm{soc}^{d+1}(M)$ but not in the left hand side.

If $d = 0$ note that we can always take $z \in A \cap \mathrm{rad}^{p-1}(M)$. If $d = 1$ and in case (B) we have that z cannot generate $\mathrm{soc}^2(M)/\mathrm{rad}^{p-2}(M)$ if $\delta(z) > \delta(b)$, and if $\delta(z) \leq \delta(b)$ subtracting from z a suitable multiple of b we can assure $z \in \mathrm{rad}^{p-2}(M)$, and consequently $z^{(1)} \in \mathrm{rad}^{p-1}(M)$. If $d \geq 2$ we always have $z^{(d)} \in \mathrm{rad}^{p-1}(M)$.

Since $(\sigma - 1)^{p-1}$ is an isomorphism from $M/\mathrm{soc}^1(M)$ to $\mathrm{rad}^{p-1}(M)$ and $z^{(d)} \in \mathrm{rad}^{(p-1)}(M)$ we can find an element $x \in M_k$ such that $x^{(p)} = z^{(d)}$. Since $x^{(p-d)} - z$ has length $d-1$ we have that $\Gamma(x^{p-d}) = \ell - ds$, and in particular $\Gamma(x^{p-i}) = \ell - is$ for all $0 \leq i \leq d$.

We are done if we can show that $\{g_i\} \cup \{x\}$ satisfy the inductive hypotheses. To do so we are reduced to showing that $\Gamma(x^{(i)}+t) = k+(i+1)s$ for each $0 \leq i < p-d$, and for each t which is a combination of elements $g_i^{(j)}$ generating a module of length $p-i$. We will show that this equality holds for each element congruent to x modulo M_{k+1}. Assume this is not the case, and let i be the smallest integer such that we have $\gamma = \Gamma(x^{(i)}+t) > k+(i+1)s$ for some t as above, and assume the representative $x \mod M_{k+1}$ and t to be taken to maximize γ. Let $\gamma = Ap + Bs$ for $0 \leq B < p$, which will still be $\leq \ell - s(p-i-1)$. Then clearly $B \geq i$ or the generate module would have length $> p-i$. If $B > i$ then we could change x by some element in $M_{ap+(b-i)s} \subset M_{k+1}$ increasing γ.

If $B = i$ consider $x^{(p-1)} - t^{(p-i-1)}$: $x^{(p-1)} \in M_\ell \cap \mathrm{soc}^1(M)$ by properties of the norm map, while $t^{(p-i-1)} \in A \cap \mathrm{soc}^1(M) \subset M_\ell$. So we have that $Ap + Bs$ has to be equal to $\ell - s(p-i-1)$, and $x^{(i)} - t$ is an element contained in $M_{\ell-s(p-i-1)} \cap \mathrm{soc}^{p-i}(M) + \mathrm{soc}^{p-i-1}(M)$ but not in

$$(A + M_{\ell-s(p-i-1)+1}) \cap \mathrm{soc}^{p-i}(M) + \mathrm{soc}^{p-i-1}(M),$$

or we would have $x^{(p-1)} - t^{(p-i-1)} \in A$ which is not the case. But this is impossible by the choice of d, which we have taken is $< p-i-1$ but maximal with the property (1).

By induction we obtain a basis of M with the required properties, and the theorem is proved.

References

[Bor65] Zenon Ivanovich Borevich, *On the multiplicative group of cyclic p-extensions of a local field*, Trudy Matematicheskogo Instituta im. VA Steklova **80** (1965), 15–30.

[FV02] Ivan Borisovich Fesenko and Sergei Vladimirovich Vostokov, *Local fields and their extensions*, American Mathematical Society, 2002.

[Gor82] Nikolai L. Gordeev, *Ramification groups of infinite p-extensions of a local field*, Journal of Mathematical Sciences **20** (1982), no. 6, 2566–2595.

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

[Mik81] Hiroo Miki, *on the ramification numbers of cyclic p-extensions over local fields*, Journal für die reine und angewandte Mathematik (1981), 99–115.

[MS03] Ján Mináč and John Swallow, *Galois module structure of pth-power classes of extensions of degree p*, Israel Journal of Mathematics **138** (2003), no. 1, 29–42.

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

[MSS06] Ján Mináč, Andrew Schultz, and John Swallow, *Galois module structure of pth-power classes of cyclic extensions of degree p^n*, Proceedings of the London Mathematical Society **92** (2006), no. 2, 307.

[NQD76] Thong Nguyen-Quang-Do, *Filtration de K^*/K^{*p} et ramification sauvage*, Acta Arith **30** (1976), 323–340.

[Pak84] G. K. Pak, *Filtration of the group of principal units of a local function field as a Galois module*, Journal of Mathematical Sciences **24** (1984), no. 4, 446–448.

[Ser79] Jean-Pierre Serre, *Local fields*, Springer, 1979.

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

[Wym69] Bostwick Frampton Wyman, *Wildly Ramified Gamma Extensions*, American Journal of Mathematics **91** (1969), no. 1, 135.