Journal of Number Theory 129 (2009) 1773–1785

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Explicit construction of self-dual integral normal bases for the square-root of the inverse different ☆

Erik Jarl Pickett

Mathématiques, École Polytechnique Fédérale de Lausanne, 1015 Lausanne, Switzerland

ARTICLE INFO

Article history:
Received 31 July 2008
Revised 29 January 2009
Available online 17 April 2009
Communicated by John S. Hsia

Keywords:
Local field
Galois module
Self-dual
Normal basis
Lubin–Tate
Formal group
Inverse different
Trace form
Dwork's power series

ABSTRACT

Let K be a finite extension of $\mathbb{Q}_p$, let L/K be a finite abelian Galois extension of odd degree and let $\mathfrak{O}_L$ be the valuation ring of L. We define $A_{L/K}$ to be the unique fractional $\mathfrak{O}_L$-ideal with square equal to the inverse different of L/K. For p an odd prime and $L/\mathbb{Q}_p$ contained in certain cyclotomic extensions, Erez has described integral normal bases for $A_{L/\mathbb{Q}_p}$ that are self-dual with respect to the trace form. Assuming $K/\mathbb{Q}_p$ to be unramified we generate odd abelian weakly ramified extensions of K using Lubin–Tate formal groups. We then use Dwork's exponential power series to explicitly construct self-dual integral normal bases for the square-root of the inverse different in these extensions.

1. Introduction

Let K be a finite extension of $\mathbb{Q}_p$ and let $\mathfrak{O}_K$ be the valuation ring of K with unique maximal ideal $\mathfrak{P}_K$ and residue field k. We let L/K be a finite Galois extension of odd degree with Galois group G and let $\mathfrak{O}_L$ be the integral closure of $\mathfrak{O}_K$ in L. From [12, IV §2, Proposition 4], this means that the different, $\mathfrak{D}_{L/K}$, of L/K will have an even valuation, and so we define $A_{L/K}$ to be the unique fractional ideal such that

$$A_{L/K} = \mathfrak{D}_{L/K}^{-1/2}.$$

☆ Part of this work was completed when the author was at the University of Manchester, studying for a PhD under the supervision of M.J. Taylor.

E-mail address: erikjarl.pickett@epfl.ch.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2009.02.012

We let $T_{L/K}: L \times L \to K$ be the symmetric non-degenerate K-bilinear form associated to the trace map (i.e., $T_{L/K}(x, y) = Tr_{L/K}(xy)$) which is G-invariant in the sense that $T_{L/K}(g(x), g(y)) = T_{L/K}(x, y)$ for all g in G.

In [1] Bayer-Fluckiger and Lenstra prove that for an odd extension of fields, L/K, of characteristic not equal to 2, then $(L, T_{L/K})$ and (KG, l) are isometric as K-forms, where $l: KG \times KG \to K$ is the bilinear extension of $l(g, h) = \delta_{g,h}$ for $g, h \in G$. This is equivalent to the existence of a self-dual normal basis generator for L, i.e., an $x \in L$ such that $L = KG.x$ and $T_{L/K}(g(x), h(x)) = \delta_{g,h}$.

If $M \subset KG$ is a free $\mathfrak{O}_K G$-lattice, and is self-dual with respect to the restriction of l to $\mathfrak{O}_K G$, then Fainsilber and Morales have proved that if $|G|$ is odd, then $(M, l) \cong (\mathfrak{O}_K G, l)$ (see [6, Corollary 4.7]). The square-root of the inverse different, $A_{L/K}$, is a Galois module that is self-dual with respect to the trace form. From [4, Theorem 1], we know that $A_{L/K}$ is a free $\mathfrak{O}_K G$-module if and only if L/K is at most weakly ramified, i.e., if the second ramification group is trivial. We know that if $[L:K]$ is odd, then $(L, T_{L/K}) \cong (KG, l)$. Therefore, if $[L:K]$ is odd, $(A_{L/K}, T_{L/K})$ is isometric to $(\mathfrak{O}_K G, l)$ if and only if L/K is at most weakly ramified. Equivalently, there exists a self-dual integral normal basis generator for $A_{L/K}$ if and only if L/K is weakly ramified.

We remark that this problem has not been solved in the global setting. Erez and Morales show in [5] that, for an odd tame abelian extension of $\mathbb{Q}$, a self-dual integral normal basis does exist for the square-root of the inverse different. However, in [13], Vinatier gives an example of a non-abelian tamely ramified extension, $N/\mathbb{Q}$, where such a basis for $A_{N/\mathbb{Q}}$ does not exist.

We now assume K is a finite unramified extension of $\mathbb{Q}_p$ of degree d. We fix a uniformising parameter, π, and let $q = p^d = |k|$. We define $K_{\pi,n}$ to be the unique field obtained by adjoining to K the $[\pi^n]$-division points of a Lubin–Tate formal group associated to π. We note that $K_{\pi,n}/K$ is a totally ramified abelian extension of degree $q^{n-1}(q-1)$. In Section 2 we choose $\pi = p$ and prove that the pth roots of unity are contained in the field $K_{p,1}$, therefore any abelian extension of exponent p above $K_{p,1}$ will be a Kummer extension.

Let $\gamma^{p-1} = -p$. In [2, §5], Dwork introduces the exponential power series,

$$E_\gamma(X) = \exp\bigl(\gamma X - \gamma X^p\bigr),$$

where the right-hand side is to be thought of as the power series expansion of the exponential function. In [10] Lang presents a proof that $E_\gamma(X)|_{X=\eta}$ converges p-adically if $v_p(\eta) \geqslant 0$ and also that $E_\gamma(X)|_{X=1}$ is equal to a primitive pth root of unity. In Section 3 we use Dwork's power series to construct a set $\{e_0, \dots, e_{d-1}\} \subset K_{p,1}$ such that $K_{p,2} = K_{p,1}(e_0^{1/p}, \dots, e_{d-1}^{1/p})$. In Section 3 we use these elements to obtain very explicit constructions of self-dual integral normal basis generators for $A_{M/K}$ where M/K is any Galois extension of degree p contained in $K_{p,2}$.

When $K = \mathbb{Q}_p$ and $\pi = p$ the nth Lubin–Tate extensions are the cyclotomic extensions obtained by adjoining p^nth roots of unity to K. Hence the study of the Lubin–Tate extensions, $K_{p,n}$, can be thought of as a generalisation of cyclotomy theory. In [3] Erez studies a weakly ramified p-extension of $\mathbb{Q}$ contained in the cyclotomic field $\mathbb{Q}(\zeta_{p^2})$ where ζ_{p^2} is a p^2th root of unity. He constructs a self-dual normal basis for the square-root of the inverse different of this extension. It turns out that the weakly ramified extension studied by Erez is, in fact, a special case of the extensions studied in Section 3 and the self-dual normal basis generator that he constructs is the corresponding basis generator we have generated using Dwork's power series, so this work generalises results in [3].

2. Kummer generators

The construction of abelian Galois extensions of local fields using Lubin–Tate formal groups is standard in local class field theory. For a detailed account see, for example, [9] or [11]. We include a brief overview for the convenience of the reader and to fix some notation.

Let K be a finite extension of $\mathbb{Q}_p$, contained in a fixed algebraic closure $\bar{K}$. Let π be a uniformising parameter for $\mathfrak{O}_K$ and let $q = |\mathfrak{O}_K/\mathfrak{P}_K|$ be the cardinality of the residue field. We let $f(X) \in X\mathfrak{O}_K[\![X]\!]$ be such that

$$f(X) \equiv \pi X \mod \deg 2, \quad \text{and} \quad f(X) \equiv X^q \mod \pi.$$

We now let $F_f(X,Y) \in \mathfrak{O}_K[\![X,Y]\!]$ be the unique formal group which admits f as an endomorphism. This means $F_f(f(X), f(Y)) = f(F_f(X,Y))$ and that $F_f(X,Y)$ satisfies some identities that correspond to the usual group axioms, see [11, §3.2] for full details. For $a \in \mathfrak{O}_K$, there exists a unique formal power series, $[a]_f(X) \in X\mathfrak{O}_K[\![X]\!]$, that commutes with f such that $[a]_f(X) \equiv aX \bmod \deg 2$. We can use the formal group, F_f, and the formal power series, $[a]_f$, to define an $\mathfrak{O}_K$-module structure on $\mathfrak{P}^c_{\bar{K}} = \bigcup_L \mathfrak{P}_L$, where the union is taken over all finite Galois extensions L/K where $L \subseteq \bar{K}$. We are going to look at the π^n-torsion points of this module. We let $E_{f,n} = \{x \in \mathfrak{P}^c_{\bar{K}}\colon\ [\pi^n]_f(x) = 0\}$ and $K_{\pi,n} = K(E_{f,n})$. We remark that the set $E_{f,n}$ depends on the choice of the polynomial f but due to a property of the formal group (see [11, §3.3, Proposition 4]), $K_{\pi,n}$ depends only on the uniformising parameter π. The extensions $K_{\pi,n}/K$ are totally ramified abelian extensions. If we let $K = \mathbb{Q}_p$ we can let $\pi = p$ and $f(X) = (X+1)^p - 1$. We then see that $K_{p,n} = \mathbb{Q}_p(\zeta_{p^n})$ where ζ_{p^n} is a primitive p^nth root of unity.

We now let K be an unramified extension of $\mathbb{Q}_p$ of degree d. We note that $q = p^d$ and that we can take $\pi = p$. We can then let $f(X) = X^q + pX$ and note that $K_{p,1} = K(\beta)$ where $\beta^{q-1} = -p$. If we let $\gamma = \beta^{(q-1)/(p-1)}$ then $\gamma^{p-1} = -p$ and $K(\gamma) \subseteq K_{p,1}$. From now on we will let $K(\gamma) = K'$. We will use Dwork's exponential power series to construct Kummer generators for $K_{p,2}$ over $K_{p,1}$.

Definition 1. Let $\gamma^{p-1} = -p$. We define Dwork's exponential power series as

$$E_\gamma(X) = \exp(\gamma X - \gamma X^p),$$

where the right-hand side is to be thought of as the power series expansion of the exponential function.

From [10, Chapter 14 §2], we know that $E_\gamma(X)|_{X=x}$ converges p-adically when $v_p(x) \geqslant 0$ and that $E_\gamma(X) \equiv 1 + \gamma X \bmod \gamma^2$. We know then that $E_\gamma(X)|_{X=1} \neq 1$. We now raise Dwork's power series to the power p and see

$$\begin{aligned}\exp(\gamma X - \gamma X^p)^p &= \exp(p(\gamma X - \gamma X^p)) \\ &= \exp(\gamma pX - \gamma pX^p) \\ &= \exp(\gamma pX)\exp(-\gamma pX^p).\end{aligned}$$

As $\exp(p\gamma X)|_{X=x}$ converges when $v_p(x) \geqslant 0$ we can evaluate both sides at $X = 1$ and see $(\exp(\gamma X - \gamma X^p)^p)|_{X=1} = \exp(\gamma pX)|_{X=1}\exp(-\gamma pX^p)|_{X=1} = 1$. Therefore, $E_\gamma(X)|_{X=1}$ is equal to a primitive pth root of unity. This implies that $K' = K(\gamma) = K(\zeta_p)$.

Let ζ_{q-1} be a primitive $(q-1)$th root of unity. From [8, Theorem 25], we know K is uniquely defined and is equal to $\mathbb{Q}_p(\zeta_{q-1})$. From [8, Theorem 23] we then know that $\mathfrak{O}_K = \mathbb{Z}_p[\zeta_{q-1}]$. We now define $\{a_i\colon\ 0 \leqslant i \leqslant d-1\}$ to be a $\mathbb{Z}_p$-basis for $\mathfrak{O}_K$ where $a_0 = 1$ and each a_i is a $(q-1)$th root of unity. We also define $e_i = E_\gamma(X)|_{X=a_i}$ and let $\mathcal{K}_2 = K_{p,1}(e_0^{1/p}, e_1^{1/p}, \dots, e_{d-1}^{1/p})$. We will now show that $\mathcal{K}_2 = K_{p,2}$.

Lemma 2. *$N_{\mathcal{K}_2/K}(\mathcal{K}_2^*) = \langle\pi\rangle \times (1 + \mathfrak{P}_K^2)$ for some uniformising parameter, π of $\mathfrak{O}_K$.*

Proof. As $E_\gamma(X) \equiv 1 + \gamma X \bmod \gamma^2$ we see that $e_i \equiv 1 + \gamma a_i \bmod \gamma^2$. We define $\mathcal{E}$ to be the set

$$\mathcal{E} = \langle e_i\colon\ 0 \leqslant i \leqslant d-1\rangle(\mathfrak{O}^\times_{K(\gamma)})^p / (\mathfrak{O}^\times_{K(\gamma)})^p$$

with multiplicative group structure. We have an isomorphism of groups $\mathcal{E} \xrightarrow{\simeq} (\mathfrak{P}_K)/(p\mathfrak{P}_K)$, using the additive group structure of $(\mathfrak{P}_K)/(p\mathfrak{P}_K)$, which sends e_i to a_i. We remark that here $p\mathfrak{P}_K = \mathfrak{P}_K^2$. From our selection of the set $\{a_i\colon\ 0 \leqslant i \leqslant d-1\}$ as a basis for $\mathfrak{O}_K$ we know that the e_i must be linearly independent (multiplicatively) over $\mathbb{F}_p$. Therefore, we know that $\mathrm{Gal}(\mathcal{K}_2/K_{p,1})$ must be isomorphic to $\prod_{i=1}^d C_p$. From standard theory (see [11, §3]), we know $\mathrm{Gal}(K_{p,2}/K_{p,1}) \cong \mathfrak{P}_K/\mathfrak{P}_K^2$, which is also isomorphic to $\prod_{i=1}^d C_p$. Therefore, $\mathrm{Gal}(\mathcal{K}_2/K) \cong \mathrm{Gal}(K_{p,2}/K) \cong C_{q-1} \times \prod_{i=1}^d C_p$.

The extensions $\mathcal{K}_2/K$ and $K_{p,2}/K$ are both finite abelian extensions of local fields. By the Artin symbol, (see [14, Appendix, Theorem 7]), we know that

$$K^\times/N_{K_{p,2}/K}\left(K_{p,2}^\times\right) \cong \mathrm{Gal}(K_{p,2}/K) \quad \text{and} \quad K^\times/N_{\mathcal{K}_2/K}\left(\mathcal{K}_2^\times\right) \cong \mathrm{Gal}(\mathcal{K}_2/K),$$

and so

$$K^\times/N_{K_{p,2}/K}\left(K_{p,2}^\times\right) \cong K^\times/N_{\mathcal{K}_2/K}\left(\mathcal{K}_2^\times\right).$$

From [9, Proposition 5.16] we know that $N_{K_{p,2}/K}(K_{p,2}^\times) = \langle p\rangle \times (1+\mathfrak{P}_K^2)$. As $K^\times$ is an abelian group we must then have $N_{\mathcal{K}_2/K}(\mathcal{K}_2^\times) \cong \langle p\rangle \times (1+\mathfrak{P}_K^2)$.

It is straightforward to check that $\mathcal{K}_2/K$ is totally ramified. Therefore, from [7, IV §3], we know that $K^\times/N_{\mathcal{K}_2/K}(\mathcal{K}_2^\times) = \mathfrak{O}_K^\times/N_{\mathcal{K}_2/K}(\mathfrak{O}_{\mathcal{K}_2}^\times)$ ($\cong C_{q-1} \times \prod_{i=1}^d C_p$). The group $\mathfrak{O}_K^\times \cong C_{q-1} \times (1+\mathfrak{P}_K)$, so we know that

$$(1+\mathfrak{P}_K)/N_{\mathcal{K}_2/K}\left(\mathfrak{O}_{\mathcal{K}_2}^\times\right) \cong \prod_{i=1}^d C_p.$$

As $K/\mathbb{Q}_p$ is unramified and $p > 2$, the logarithmic power series gives us an isomorphism of groups, log: $1+\mathfrak{P}_K \cong \mathfrak{P}_K$ ($\cong \bigoplus_{i=0}^{d-1} \mathbb{Z}_p$), using the multiplicative structure of $1+\mathfrak{P}_K$ and the additive structure of $\mathfrak{P}_K$, see [7, Chapter IV, Example 1.4] for full details. The maximal p-elementary abelian quotient of $\bigoplus_{i=1}^d \mathbb{Z}_p$ is given by $\bigoplus_{i=1}^d \mathbb{Z}_p/\bigoplus_{i=1}^d p\mathbb{Z}_p \cong \prod_{i=1}^d C_p$ and the unique subgroup that gives this quotient is $\bigoplus_{i=1}^d p\mathbb{Z}_p$. We then have $\mathfrak{P}_K/p\mathfrak{P}_K \cong \prod_{i=1}^d C_p$ and using the logarithmic isomorphism we see $(1+\mathfrak{P}_K)/(1+\mathfrak{P}_K)^p \cong \prod_{i=1}^d C_p$. This means that $(1+\mathfrak{P}_K)^p$ is the unique subgroup of $1+\mathfrak{P}_K$ that gives the maximal p-elementary abelian quotient. As above we have $(1+\mathfrak{P}_K)^p = 1+\mathfrak{P}_K^2$ and therefore,

$$N_{\mathcal{K}_2/K}\left(\mathfrak{O}_{\mathcal{K}_2}^\times\right) = 1+\mathfrak{P}_K^2.$$

Let Π be a uniformising parameter for $\mathcal{K}_2$. As $\mathcal{K}_2/K$ is totally ramified, $N_{\mathcal{K}_2/K}(\Pi) = \pi$ must be a uniformising parameter of K. Since $N_{\mathcal{K}_2/K}(\mathcal{K}_2^\times)$ is a group under multiplication we know that $\langle\pi\rangle$ must be a subgroup. We have already seen that $(1+\mathfrak{P}_K^2)$ is a subgroup, so as $N_{\mathcal{K}_2/K}(\mathcal{K}_2^\times)$ is abelian, we must have

$$\langle\pi\rangle \times \left(1+\mathfrak{P}_K^2\right) \subseteq N_{\mathcal{K}_2/K}\left(\mathcal{K}_2^\times\right).$$

The subgroups $\langle\pi\rangle \times (1+\mathfrak{P}_K^2)$ and $N_{\mathcal{K}_2/K}(\mathcal{K}_2^\times)$ both have the same finite index in $K^\times$, therefore we must have equality. □

To prove the next lemma we will use some properties of the pth Hilbert pairing for a field that contains the pth roots of unity. For full definitions and proofs see [7, Chapter IV]. We include the properties we will need for the convenience of the reader.

Definition 3. Let L be a field of characteristic 0 with fixed separable algebraic closure $\bar{L}$ and let μ_p be the group of pth roots of unity in $\bar{L}$. Let $\mu_p \subseteq L$. We define the pth Hilbert symbol of L as

$$(,)_{p,L} : L^\times \times L^\times \longrightarrow \mu_p,$$
$$(a,b) \longmapsto \frac{(A_L(a))(b^{1/p})}{b^{1/p}},$$

where $A_L : L^\times \longrightarrow \mathrm{Gal}(L^{ab}/L)$ is the Artin map of L (see [9, Chapter 6, §3] for details).

In [7, Chapter IV, Proposition 5.1] it is proved that if L'/L is a finite Galois extension of local fields, then the Hilbert symbol satisfies the following conditions.

(1) $(a,b)_{p,L} = 1$ if and only if $a \in N_{L(b^{1/p})/L}(L(b^{1/p})^\times)$, and $(a,b)_{p,L} = 1$ if and only if $b \in N_{L(a^{1/p})/L}(L(a^{1/p})^\times)$,
(2) $(a,b)_{p,L'} = (N_{L'/L}(a), b)_{p,L}$ for $a \in L'^\times$ and $b \in L^\times$,
(3) $(a, 1-a)_{p,L} = 1$ for all $1 \neq a \in L^\times$,
(4) $(a,b)_{p,L} = (b,a)^{-1}_{p,L}$.

Lemma 4.

$$p \in N_{\mathcal{K}_2/K}(\mathcal{K}_2^*).$$

Proof. First we show that $(e_i, \zeta_p - 1)_{p,K'} = 1$ for all $0 \leqslant i \leqslant d-1$.

Recall that $K' = K(\zeta_p)$ and consider the field extension $K'/\mathbb{Q}_p(\zeta_p)$. This is an unramified extension of degree d. As $\zeta_p - 1 \in \mathbb{Q}_p(\zeta_p)$, we can use property 2 of the Hilbert symbol to show $(e_i, \zeta_p - 1)_{p,K'} = (N_{K'/\mathbb{Q}_p(\zeta_p)}(e_i), \zeta_p - 1)_{p,\mathbb{Q}_p(\zeta_p)}$. Recall that $e_i = E_\gamma(X)|_{X=a_i}$ where the set $\{a_i\colon\ 0 \leqslant i \leqslant p-1\}$ forms a basis for $\mathfrak{O}_K$ over $\mathbb{Z}_p$, all the a_i are (p^d-1)th roots of unity and $a_0 = 1$. The action of the Galois group $\mathrm{Gal}(K/\mathbb{Q}_p)$ on each a_i (which will be the same as the action of $\mathrm{Gal}(K'/\mathbb{Q}_p(\zeta_p))$ will be generated by the Frobenius element,

$$\phi_{K/\mathbb{Q}_p} : a_i \mapsto a_i^p.$$

We know that $E_\gamma(X)|_{X=x}$ converges when $v_p(x) \geqslant 0$. As $a_i^{p^k} \in \mathfrak{O}_K^\times$, we have that $E_\gamma(X)|_{X=a_i^{p^k}}$ converges for all $k \in \mathbb{Z}$. Therefore $E_\gamma(X^{p^k})|_{X=a_i}$ must converge and

$$\phi^k_{K/\mathbb{Q}_p}(e_i) = E_\gamma\big(X^{p^k}\big)\big|_{X=a_i},$$

where $\phi^k_{K/\mathbb{Q}_p}$ is the Frobenius element, $\phi_{K/\mathbb{Q}_p}$, applied k times. We can now make the following derivation.

$$\begin{aligned} N_{K'/\mathbb{Q}_p(\zeta_p)}(e_i) &= \prod_{g \in \mathrm{Gal}(K'/\mathbb{Q}_p(\zeta_p))} g(e_i) = \prod_{k=0}^{d-1} \phi^k_{K/\mathbb{Q}_p}(e_i) \\ &= \prod_{k=0}^{d-1} E_\gamma\big(X^{p^k}\big)\big|_{X=a_i} = \prod_{k=0}^{d-1} \exp\big(\gamma X^{p^k} - \gamma X^{p^{k+1}}\big)\big|_{X=a_i} \\ &= \exp\big(\big(\gamma X - \gamma X^p\big) + \big(\gamma X^p - \gamma X^{p^2}\big) + \cdots + \big(\gamma X^{p^{d-1}} - X^{p^d}\big)\big)\big|_{X=a_i} \\ &= \exp\big(\gamma X - \gamma X^{p^d}\big)\big|_{X=a_i}. \end{aligned}$$

We now consider raising to the power p and see

$$\begin{aligned}\exp\bigl(\gamma X-\gamma X^{p^d}\bigr)^p&=\exp\bigl(p\bigl(\gamma X-\gamma X^{p^d}\bigr)\bigr)\\&=\exp\bigl(p\gamma X-p\gamma X^{p^d}\bigr)\\&=\exp(p\gamma X)\exp\bigl(-p\gamma X^{p^d}\bigr).\end{aligned}$$

The power series $\exp(p\gamma X)|_{X=x}$ will converge when $v_p(x)\geqslant 0$ so we can evaluate at $X=a_i$ and see, $(N_{K'/\mathbb{Q}_p(\zeta_p)}(e_i))^p=1$. Therefore $N_{K'/\mathbb{Q}_p(\zeta_p)}(e_i)$ is a pth root of unity for all $0\leqslant i\leqslant d-1$. If $N_{K'/\mathbb{Q}_p(\zeta_p)}(e_i)=1$ then $(N_{K'/\mathbb{Q}_p(\zeta_p)}(e_i),1-\zeta_p)_{p,\mathbb{Q}_p(\zeta_p)}=(1,1-\zeta_p)_{p,\mathbb{Q}_p(\zeta_p)}=1$, so we now assume $N_{K'/\mathbb{Q}_p(\zeta_p)}(e_i)$ is a primitive pth root of unity. From property 3 of the Hilbert symbol we know that $(\zeta_p,1-\zeta_p)_{p,\mathbb{Q}_p(\zeta_p)}=1$. We know that for $1\leqslant k\leqslant p-1$, then $\mathbb{Q}_p(\zeta_p)(\zeta_p^{1/p})=\mathbb{Q}_p(\zeta_p)(\zeta_p^{k/p})$, and so from property 1 of the Hilbert symbol we know that $(\zeta_p^k,1-\zeta_p)_{p,\mathbb{Q}_p(\zeta_p)}=1$. This means that $(e_i,1-\zeta_p)_{p,K'}=1$ for all $0\leqslant i\leqslant d-1$. We now let $\xi_i\in K'(e_i^{1/p})$ be such that $N_{K'(e_i^{1/p})/K'}(\xi_i)=1-\zeta_p$. As p is odd, $N_{K'(e_i^{1/p})/K'}(-\xi_i)=\zeta_p-1$, and therefore

$$(e_i,\zeta_p-1)_{p,K'}=1$$

for all $0\leqslant i\leqslant d-1$.

Next we show that $\zeta_p-1\in N_{\mathcal{K}_2/K'}(\mathcal{K}_2^\times)$. We have just shown that $\zeta_p-1\in N_{K'(e_0^{1/p})/K'}(K'(e_0^{1/p})^\times)$. We assume, for induction, that

$$\zeta_p-1\in N_{K'(e_0^{1/p},\dots e_j^{1/p})/K'}\bigl(K'\bigl(e_0^{1/p},\dots e_j^{1/p}\bigr)^\times\bigr)$$

for some $0\leqslant j\leqslant p-1$. Let $\eta\in K'(e_0^{1/p},\dots,e_j^{1/p})^\times$ be such that $N_{K'(e_0^{1/p},\dots e_j^{1/p})/K'}(\eta)=\zeta_p-1$. As $e_{j+1}\in K'$ we can make the following derivation:

$$\begin{aligned}(\eta,e_{j+1})_{p,K'(e_0^{1/p},\dots,e_j^{1/p})}&=\bigl(N_{K'(e_0^{1/p},\dots,e_j^{1/p})/K'}(\eta),e_{j+1}\bigr)_{p,K'}\\&=(\zeta_p-1,e_{j+1})_{p,K'}\\&=(e_{j+1},\zeta_p-1)_{p,K'}^{-1}=1.\end{aligned}$$

Therefore,

$$\eta\in N_{K'(e_0^{1/p},\dots,e_{j+1}^{1/p})/K'(e_0^{1/p},\dots,e_j^{1/p})}\bigl(K'\bigl(e_0^{1/p},\dots,e_{j+1}^{1/p}\bigr)^\times\bigr),$$

and so

$$(\zeta_p-1)\in N_{K'(e_0^{1/p},\dots,e_{j+1}^{1/p})/K'}\bigl(K'\bigl(e_0^{1/p},\dots,e_{j+1}^{1/p}\bigr)^\times\bigr).$$

By induction on j we see that $(\zeta_p-1)\in N_{\mathcal{K}_2/K'}(\mathcal{K}_2^\times)$.

Finally we note that the minimal polynomial of ζ_p-1 over K is $f(X)=((X+1)^p-1)/X$. The constant term in $f(X)$ is equal to p and K' is the splitting field of $f(X)$. Therefore, as $[K':K]$ is even, $N_{K'/K}(\zeta_p-1)=p$. The norm map is transitive, so we know that $p\in N_{\mathcal{K}_2/K}(\mathcal{K}_2^\times)$. □

Theorem 5.

$$K_{p,2}=K_{p,1}\bigl(e_0^{1/p},e_1^{1/p},\dots,e_{d-1}^{1/p}\bigr).$$

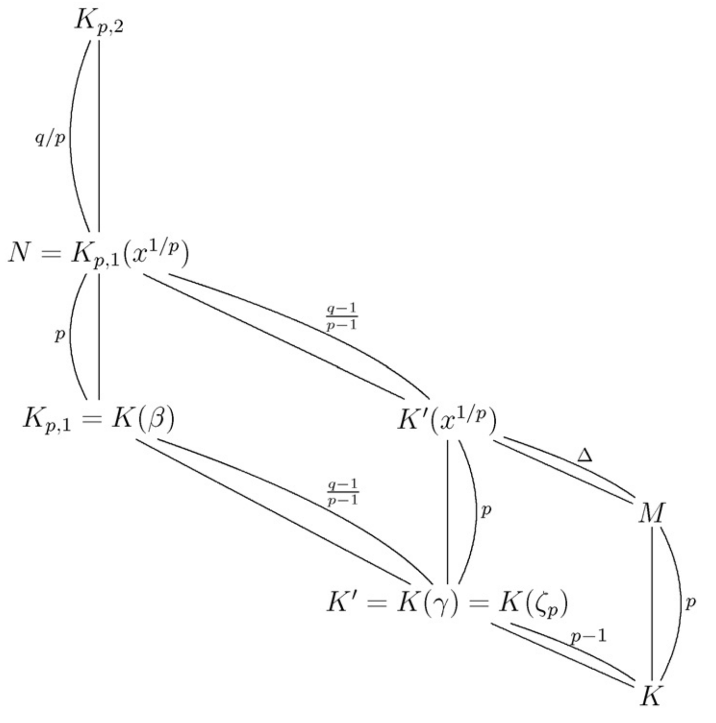

Fig. 1. Abelian extensions of K.

Proof. From Lemma 2 we know that $N_{\mathcal{K}_2/K}(\mathcal{K}_2^\times) = \langle\pi\rangle \times 1 + \mathfrak{P}_K^2$ where $\pi = up$ for some $u \in \mathfrak{O}_K^\times$. From Lemma 4 we know that $p \in N_{\mathcal{K}_2/K}(\mathcal{K}_2^\times)$ and therefore that $N_{\mathcal{K}_2/K}(\mathcal{K}_2^\times) = \langle p\rangle \times 1 + \mathfrak{P}_K^2$. From [9, Proposition 5.16], we know that $N_{K_{p,2}/K}(K_{p,2}^\times) = \langle p\rangle \times (1 + \mathfrak{P}_K^2)$. As $\mathcal{K}_2/K$ and $K_{p,2}/K$ are both finite abelian extensions of local fields contained in $\bar{K}$ and $N_{K_{p,2}/K}(K_{p,2}^\times) = N_{\mathcal{K}_2/K}(\mathcal{K}_2^\times)$, from [14, Appendix, Theorem 9], we know that $\mathcal{K}_2 = K_{p,2}$. □

3. Explicit self-dual normal bases for $A_{M/K}$

We begin this section by describing the intermediate fields of $K_{p,2}/K$ that we are going to study. The extension $K_{p,2}/K_{p,1}$ is a totally ramified abelian extension of degree q. There will be $(q-1)/(p-1)$ intermediate fields, N_j such that $[K_{p,2} : N_j] = q/p$ and $[N_j : K_{p,1}] = p$. The pth roots of unity are contained in $K_{p,1}$, so for each j, the extension $N_j/K_{p,1}$ will be a Kummer extension. We recall that $\{a_i\colon\ 0 \leqslant i \leqslant d-1\}$ is a $\mathbb{Z}_p$-basis for $\mathfrak{O}_K$ where $a_0 = 1$ and all the a_i are $(q-1)$th roots of unity. We have shown that $K_{p,2} = K(e_0^{1/p}, e_1^{1/p}, \ldots e_{d-1}^{1/p})$, where the $e_i = E_\gamma(X)|_{X=a_i}$. Therefore each $N_j = K_{p,1}(x_j^{1/p})$ for $x_j = \prod_{i=0}^{d-1} e_i^{n_i}$ for some $0 \leqslant n_i \leqslant p-1$, not all zero. We now note that for all $x = \prod_{i=0}^{d-1} e_i^{n_i}$ as above, we have $x \in K'(= K(\gamma) = K(\zeta_p))$. Therefore $K'(x_j^{1/p})$ is the unique extension of K' of degree p contained in N_j. There is also a unique extension of K of degree p contained in N_j, we shall call this extension M_j and let $\mathrm{Gal}(K'(x_j^{1/p})/M_j) = \Delta_j$. From now on we will drop the subscript for N_j, x_j, M_j and Δ_j as the following results do not depend on which $x_j = \prod_{i=0}^{d-1} e_i^{n_i}$ we pick. To clarify, we will describe these extensions in Fig. 1.

We also let $\mathrm{Gal}(K'(x^{1/p})/K') = G$, and as all the groups we are dealing with are abelian we will use an abuse of notation and write $\mathrm{Gal}(M/K) = G$ and $\mathrm{Gal}(K'/K) = \Delta$.

Let $A_{M/K}=\mathfrak{D}_{M/K}^{-1/2}$ be the square-root of the inverse different of M/K. The aim now is to show that $(1+Tr_\Delta(x^{1/p}))/p$ is a self-dual normal basis for $A_{M/K}$.

We remark that if $K=\mathbb{Q}_p$, then $K'=K_{p,1}$, $N_1=K_{p,2}=K'(x^{1/p})$ and the only choice for x is $E_\gamma(X)|_{X=1}=\zeta_p$. In [3] Erez shows that in this case $(1+Tr_\Delta(\zeta_p^{1/p}))/p$ does indeed give a self-dual normal basis for $A_{M/K}$. So the situation we describe generalises the work in [3].

Before we proceed to the main results of this section we must make some basic calculations about the field extensions to be studied.

Lemma 6.

$$v_M(A_{M/K})=1-p.$$

Proof. We first calculate the ramification groups of $K_{p,2}/K_{p,1}$. We recall that $f(X)=X^q+pX$. If we let $u\in\mu_{q-1}\cup\{0\}(=k)$, clearly $[u](X)=uX$ and $[up](X)=u[p](X)$. Let α be a primitive $[p^2]$-division point for $F_f(X,Y)$. We see that

$$\begin{aligned} f\big([up+1](\alpha)\big) &= f\big(F\big(u[p](\alpha),\alpha\big)\big) \\ &= F\big(f\big(u[p](\alpha)\big), f(\alpha)\big) \\ &= F\big(uf^2(\alpha), f(\alpha)\big) \\ &= f(\alpha). \end{aligned}$$

Therefore $[up+1](\alpha)$ is another primitive $[p^2]$-division point and the Galois conjugates of α over $K_{p,1}$ are given by $[up+1](\alpha)$ for $u\in\mu_{q-1}\cup\{0\}$.

Given $f(X)\in\mathfrak{O}_K[X]$ such that $f(X)\equiv pX \bmod \deg 2$ and $f(X)\equiv X^q \bmod p$, the standard proof in the literature of the existence of a formal group $F(X,Y)\in\mathfrak{O}_K[\![X,Y]\!]$ such that F commutes with f uses an iterative process for calculating F_f. See, for example, [11, §3.5, Proposition 5] or [9, III, Proposition 3.12]. The ith iteration calculates $F(X,Y) \bmod \deg(i+1)$ and passage to the inductive limit gives $F(X,Y)$. We will use this process to calculate the first few terms of $F(X,Y)$.

We will let $F^i(X,Y)\equiv F(X,Y) \bmod \deg(i+1)$ and define E_i to be the ith error term, i.e., $E_i=f(F^{i-1}(X,Y))-F^{i-1}(f(X),f(Y)) \bmod \deg(i+1)$. From [11, §3.5, Proposition 5] we then have

$$F^{i+1}(X,Y)=F^i(X,Y)-\frac{E_i}{p(1-p^{i-1})}.$$

$F(X,Y)$ is a formal group, so $F^1(X,Y)=X+Y$. We then see

$$\begin{aligned} f\big(F^1(X,Y)\big)-F^1\big(f(X),f(Y)\big) &= (X+Y)^q+p(X+Y)-\big(X^q+pX+Y^q+pY\big) \\ &= \sum_{i=1}^{q-1}\binom{q}{i}X^iY^{q-i}. \end{aligned}$$

So the error terms will be $E_i=0$ for $2\leqslant i\leqslant q-1$ and $E_q=\sum_{i=1}^{q-1}\binom{q}{i}X^iY^{q-i}$. From [11, §3.5, Proposition 5], we then get

$$F(X,Y)\equiv X+Y-\frac{\sum_{i=1}^{q-1}\binom{q}{i}X^iY^{q-i}}{p(1-p^{q-1})} \mod \deg(q+1).$$

We now substitute $X=\alpha$ and $Y=u[p](X)=u(\alpha^q+p\alpha)$ into our expression for $F(X,Y)$ and see that

$$[1+up](\alpha)\equiv\alpha+u\big(\alpha^q+p\alpha\big)-\frac{\sum_{i=1}^{q-1}\binom{q}{i}\alpha^i(u(\alpha^q+p\alpha))^{q-i}}{p(1-p^{q-1})}\bmod\alpha^{q+1}$$
$$\equiv(1+up)\alpha+\left(u-\frac{\sum_{i=1}^{q-1}(up)^{q-i}\binom{q}{i}}{p(1-p^{q-1})}\right)\alpha^q\bmod\alpha^{q+1}.$$

Let $\Gamma=\mathrm{Gal}(K_{p,2}/K_{p,1})$. We know that α is a uniformising parameter for $\mathfrak{O}_{K_{p,2}}$ and that $p\in\mathfrak{P}_{K_{p,2}}^{q(q-1)}$. An element $s\in\Gamma$ is in the ith ramification group (with the lower numbering), Γ_i, if and only if $s(\alpha)/\alpha\equiv1\bmod\mathfrak{P}_{K_{p,2}}^i$, see [12, IV §2, Proposition 5]. We have shown that for $1\neq s\in\Gamma$ then $s(\alpha)/\alpha\equiv1+u\alpha^{q-1}\bmod\mathfrak{P}_{K_{p,2}}^q$. Therefore, $\Gamma=\Gamma_i$ for $0\leqslant i\leqslant(q-1)$ and $\Gamma_q=\{1\}$.

To calculate the ramification groups of $N/K_{p,1}$ we need to change the numbering of the ramification groups of $K_{p,2}/K_{p,1}$ from lower numbering to upper numbering. From [12, IV §3] we have $\Gamma^{-1}=\Gamma$, $\Gamma^0=\Gamma_0$ and $\Gamma^{\phi(m)}=\Gamma_m$ where $\phi(m)=\frac{1}{|\Gamma_0|}\sum_{i=1}^m|\Gamma_i|$. A straightforward calculation then shows that the upper numbering is actually the same as the lower numbering. From [12, IV §3, Proposition 14] we then know that $\mathrm{Gal}(N/K_{p,1})=\mathrm{Gal}(N/K_{p,1})^i$ for $0\leqslant i\leqslant(q-1)$. and $\mathrm{Gal}(N/K_{p,1})^q=\{1\}$ and switching back to the lower numbering we have $\mathrm{Gal}(N/K_{p,1})=\mathrm{Gal}(N/K_{p,1})_i$ for $0\leqslant i\leqslant(q-1)$. and $\mathrm{Gal}(N/K_{p,1})_q=\{1\}$.

From [12, IV §2, Proposition 4], we have the formula,

$$v_N(\mathfrak{D}_{N/K_{p,1}})=\sum_{i\geqslant0}\big(\big|\mathrm{Gal}(N/K_{p,1})_i\big|-1\big),$$

and so $v_N(\mathfrak{D}_{N/K_{p,2}})=q(p-1)$. The extensions N/M and $K_{p,1}/K$ are both totally, tamely ramified extensions of degree $q-1$, so from the formula above we know that $v_N(\mathfrak{D}_{N/M})=v_{K_{p,1}}(\mathfrak{D}_{K_{p,1}/K})=q-2$. From [8, III.2.15] we know, for a separable tower of fields $L''\supseteq L'\supseteq L$, the differents of these field extensions are linked by the formula $\mathfrak{D}_{L''/L}=\mathfrak{D}_{L''/L'}\mathfrak{D}_{L'/L}$. We therefore have $v_M(\mathfrak{D}_{M/K})=2(p-1)$, and so $v_M(A_{M/K})=1-p$. □

Remark 7. We remark that this lemma implies that M/K is weakly ramified.

We now prove a very useful result that makes finding self-dual integral normal bases much easier.

Lemma 8. *Let a be an element of $A_{L/K}$ that is self-dual with respect to the trace form, (i.e., $T_{L/K}(g(a),h(a))=\delta_{g,h}$ for all $g,h\in G$), then $A_{L/K}=\mathfrak{O}_K[G].a$.*

Proof. Let $a\in A_{L/K}$ be as given. The square-root of the inverse different, $A_{L/K}$, is a fractional $\mathfrak{O}_L$-ideal stable under the action of the Galois group, G, therefore $\mathfrak{O}_K[G].a\subseteq A_{L/K}$.

The inclusion of $\mathfrak{O}_K$-lattices, $\mathfrak{O}_K[G].a\subseteq A_{L/K}$, means that $A_{L/K}^D\subseteq(\mathfrak{O}_K[G].a)^D$ where D denotes the $\mathfrak{O}_K$-dual taken with respect to the trace form. As $A_{L/K}=A_{L/K}^D$, we have $A_{L/K}\subseteq(\mathfrak{O}_K[G].a)^D$. We know that $\mathfrak{O}_K[G].a$ is $\mathfrak{O}_K$-free on the basis $\{g(a)\colon g\in G\}$, so $(\mathfrak{O}_K[G].a)^D$ is $\mathfrak{O}_K$-free on the dual basis with respect to the trace form, which is $\{g(a)\colon g\in G\}$. Therefore $(\mathfrak{O}_K[G].a)^D=\mathfrak{O}_K[G].a$ and $A_{L/K}\subseteq\mathfrak{O}_K[G].a$, and so $A_{L/K}=\mathfrak{O}_K[G].a$. □

For each $x=\prod_{i=0}^{d-1}e_i^{n_i}$ with $0\leqslant n_i\leqslant p-1$ not all zero, we know that there exists $u\in\mathfrak{O}_K^\times$ such that $x\equiv1+u\gamma\bmod\gamma^2$. The element γ is a uniformising parameter for $\mathfrak{O}_{K'}$, therefore, $x\in\mathfrak{O}_{K'}^\times$ and $x-1$ will also be a uniformising parameter for $\mathfrak{O}_{K'}$. Using the binomial theorem we note that $(x^{1/p}-1)^p=x-1+py$ where $v_{K'(x^{1/p})}(y)\geqslant0$. Therefore $v_{K'(x^{1/p})}((x^{1/p}-1)^p)=p$ and $v_{K'(x^{1/p})}(x^{1/p}-1)=1$, so $x^{1/p}-1$ is a uniformising parameter for $\mathfrak{O}_{K'(x^{1/p})}$.

Lemma 9.

$$\frac{1+Tr_{\Delta}(x^{1/p})}{p} \in A_{M/K}.$$

Proof. We have just shown that $x^{1/p}-1$ is a uniformising parameter for $\mathfrak{O}_{K'(x^{1/p})}$. As $K'(x^{1/p})/M$ is a totally, tamely ramified extension, we know that $Tr_{\Delta}(x^{1/p}-1) \in \mathfrak{P}_M$ so $v_M(Tr_{\Delta}(x^{1/p}-1)) \geqslant 1$. We know that

$$Tr_{\Delta}\big(x^{1/p}-1\big) = Tr_{\Delta}\big(x^{1/p}\big) - (p-1) = \big(1+Tr_{\Delta}\big(x^{1/p}\big)\big) - p.$$

Therefore, $v_M(1+Tr_{\Delta}(x^{1/p})) \geqslant 1$ and $v_M(\frac{1+Tr_{\Delta}(x^{1/p})}{p}) \geqslant 1-p$. Since $v_M(A_{M/K}) = 1-p$, we must have $\frac{1+Tr_{\Delta}(x^{1/p})}{p} \in A_{M/K}$. $\square$

Lemma 10. *Let $x = \prod_{i=0}^{d-1} e_i^{n_i}$ for some $n_i \in \mathbb{Z}^+$, and let $\delta \in \Delta = \mathrm{Gal}(K'(x^{1/p})/M)$. Let $\delta : \gamma \mapsto \chi(\delta)\gamma$ with $\chi(\delta) \in \mu_{p-1}$, then $\delta(x) = x^{\chi(\delta)}$.*

Proof. As $\chi(\delta)^p = \chi(\delta)$, for all $\delta \in \Delta$ we have the following equality:

$$\exp\big(\chi(\delta)\gamma X - \chi(\delta)\gamma X^p\big) = \exp\left(\big(\chi(\delta)\gamma X\big) + \frac{(\chi(\delta)\gamma X)^p}{p}\right).$$

As $\chi(\delta)$ is a unit we know, from [10, Chapter 14, §2] that $\exp((\chi(\delta)\gamma X) + \frac{(\chi(\delta)\gamma X)^p}{p})|_{X=y}$ will converge when $v_p(y) \geqslant 0$. Therefore, $\exp(\chi(\delta)\gamma X - \chi(\delta)\gamma X^p)|_{X=a_i}$ will converge. We can now make the following derivation:

$$\begin{aligned}\big(E_{\gamma}(X)|_{X=a_i}\big)^{\chi(\delta)} &= \big(\exp\big(\gamma X - \gamma X^p\big)\big|_{X=a_i}\big)^{\chi(\delta)} \\ &= \exp\big(\chi(\delta)\big(\gamma X - \gamma X^p\big)\big)\big|_{X=a_i} \\ &= \exp\big(\chi(\delta)\gamma X - \chi(\delta)\gamma X^p\big)\big|_{X=a_i}.\end{aligned}$$

As a_i is fixed by all $\delta \in \Delta$ we see that

$$\delta\big(\gamma X - \gamma X^p\big)\big|_{X=a_i} = \big(\delta(\gamma)X - \delta(\gamma)X^p\big)\big|_{X=a_i} = \big(\chi(\delta)\gamma X - \chi(\delta)\gamma X^p\big)\big|_{X=a_i}.$$

As $\exp(\chi(\delta)\gamma X - \chi(\delta)\gamma X^p)|_{X=a_i}$ converges we must then have

$$\begin{aligned}\exp\big(\chi(\delta)\gamma X - \chi(\delta)\gamma X^p\big)\big|_{X=a_i} &= \exp\big(\delta(\gamma)X - \delta(\gamma)X^p\big)\big|_{X=a_i} \\ &= \delta\big(\exp\big(\gamma X - \gamma X^p\big)\big|_{X=a_i}\big) \\ &= \delta\big(E_{\gamma}(X)|_{X=a_i}\big).\end{aligned}$$

Therefore, $\delta(e_i) = (e_i)^{\chi(\delta)}$ for all $0 \leqslant i \leqslant (d-1)$, which means $\delta(x) = x^{\chi(\delta)}$. $\square$

Lemma 11. *Let $g \in \mathrm{Gal}(M/K)$, then*

$$T_{M/K}\left(\frac{1+Tr_{\Delta}(x^{1/p})}{p}, g\left(\frac{1+Tr_{\Delta}(x^{i/p})}{p}\right)\right) = \delta_{1,g}.$$

Proof. First we observe that $Tr_G(x^{i/p}) = \sum_{g\in G} g(x^{i/p}) = x^{1/p}\sum_{j=0}^{p-1}\zeta_p^{ij} = 0$ for all $p \mid i$. The trace map is transitive, so $Tr_G(Tr_\Delta(x^{i/p})) = Tr_\Delta(Tr_G(x^{i/p})) = Tr_\Delta(0) = 0$ for $p \mid i$. We make the following derivation:

$$\begin{aligned}
&Tr_G\left(\left(\frac{1+Tr_\Delta(x^{1/p})}{p}\right)g\left(\frac{1+Tr_\Delta(x^{1/p})}{p}\right)\right)\\
&\quad= Tr_G\left(\left(\frac{1+Tr_\Delta(x^{1/p})}{p}\right)\left(\frac{1+g(Tr_\Delta(x^{1/p}))}{p}\right)\right)\\
&\quad= Tr_G\left(\frac{1+Tr_\Delta(x^{1/p})+g(Tr_\Delta(x^{1/p}))+Tr_\Delta(x^{1/p})g(Tr_\Delta(x^{1/p}))}{p^2}\right)\\
&\quad= Tr_G\left(\frac{1+Tr_\Delta(x^{1/p})g(Tr_\Delta(x^{1/p}))}{p^2}\right)\\
&\quad= \frac{p+Tr_G(Tr_\Delta(x^{1/p})g(Tr_\Delta(x^{1/p})))}{p^2}.
\end{aligned}$$

The right-hand side of this equation equals 1 if and only if $Tr_G(Tr_\Delta(x^{1/p})g(Tr_\Delta(x^{1/p}))) = (p-1)p$, and it equals 0 if and only if $Tr_G(Tr_\Delta(x^{1/p})g(Tr_\Delta(x^{1/p}))) = -p$. Therefore it is sufficient to show

$$Tr_G\big(Tr_\Delta\big(x^{1/p}\big)g\big(Tr_\Delta\big(x^{1/p}\big)\big)\big) = \begin{cases}(p-1)p & \text{if } g=\mathrm{id},\\ -p & \text{if } g\neq \mathrm{id}.\end{cases}$$

From Lemma 10 we know that $\delta(x) = x^{\chi(\delta)}$. This means that $\delta(x^{1/p}) = \zeta_\delta x^{\chi(\delta)/p}$ for some $\zeta_\delta \in \mu_p$. We know that $\mu_{p-1} \subset \mathbb{Z}_p^\times$ so we can write $\chi(\delta) \equiv j(\delta) \bmod p$, for some $1 \leqslant j(\delta) \leqslant (p-1)$ and note that $j(\delta) = j(\delta')$ if and only if $\delta = \delta'$. We can therefore define a set of constants $\{\lambda_{j(\delta)} \in \mathfrak{O}_{K'}\colon\ \delta \in \Delta\}$ such that $\delta(x^{1/p}) = \lambda_{j(\delta)}x^{j(\delta)/p}$. We now define $\sigma \in \Delta$ to be the involution such that $\chi(\sigma) = -1$ and $j(\sigma) = p-1$ and note that $\sigma(\zeta_p) = \zeta_p^{-1}$. We consider the double action of σ on $x^{1/p}$. We have $\sigma(x^{1/p}) = \zeta_\sigma x^{\chi(\sigma)/p} = \zeta_\sigma x^{-1/p}$, so

$$\begin{aligned}
\sigma^2\big(x^{1/p}\big) &= \sigma(\zeta_\sigma)\sigma\big(x^{-1/p}\big)\\
&= \zeta_\sigma^{-1}\sigma\big(x^{1/p}\big)^{-1}\\
&= \zeta_\sigma^{-1}\big(\zeta_\sigma x^{-1/p}\big)^{-1}\\
&= \zeta_\sigma^{-2}x^{1/p}.
\end{aligned}$$

As σ is an involution, $x^{1/p} = \zeta_\sigma^{-2}x^{1/p}$, so we have $\zeta_\sigma = 1$. Therefore, $\sigma(x^{1/p}) = x^{-1/p} = (1/x)x^{(p-1)/p}$, and so $\lambda_{p-1} = 1/x$.

For $g \in G$ we know that $g(x^{1/p}) = \zeta^i x^{1/p}$ for some $0 \leqslant i \leqslant p-1$ with $i = 0$ when $g = id$. Using this notation we make the following derivation:

$$\begin{aligned}
Tr_G\big(Tr_\Delta\big(x^{1/p}\big)g\big(Tr_\Delta\big(x^{1/p}\big)\big)\big) &= Tr_G\left(\left(\sum_{\xi\in\Delta}\xi\big(x^{1/p}\big)\right)\left(g\left(\sum_{\eta\in\Delta}\eta\big(x^{1/p}\big)\right)\right)\right)\\
&= Tr_G\left(\sum_{\xi\in\Delta}\sum_{\eta\in\Delta}\xi\big(x^{1/p}\big)g\big(\eta\big(x^{1/p}\big)\big)\right)
\end{aligned}$$

$$
\begin{aligned}
&= Tr_G\left(\sum_{\xi\in\Delta}\sum_{\eta\in\Delta}\xi\big(x^{1/p}\big)\eta g\big(x^{1/p}\big)\right) \quad \text{as } G\times\Delta \text{ is abelian}\\
&= Tr_G\left(\sum_{\xi\in\Delta}\sum_{\delta\in\Delta}\xi\big(x^{1/p}\big)\xi\delta g\big(x^{1/p}\big)\right) \quad \text{where } \delta=\xi^{-1}\eta\\
&= Tr_G\left(\sum_{\xi\in\Delta}\xi\left(\sum_{\delta\in\Delta}\big(x^{1/p}\big)\delta g\big(x^{1/p}\big)\right)\right)\\
&= Tr_{G\times\Delta}\left(\sum_{\delta\in\Delta}\big(x^{1/p}\big)\delta g\big(x^{1/p}\big)\right)\\
&= \sum_{\delta\in\Delta} Tr_{G\times\Delta}\big(\big(x^{1/p}\big)\delta g\big(x^{1/p}\big)\big)\\
&= \sum_{\delta\in\Delta} Tr_{G\times\Delta}\big(\big(x^{1/p}\big)\delta\big(\zeta_p^i\big(x^{1/p}\big)\big)\big)\\
&= \sum_{\delta\in\Delta} Tr_{G\times\Delta}\big(\big(x^{1/p}\big)\delta\big(x^{1/p}\big)\delta\big(\zeta_p^i\big)\big)\\
&= \sum_{\delta\in\Delta} Tr_{G\times\Delta}\big(\big(x^{1/p}\big)\big(\lambda_{j(\delta)}x^{j(\delta)/p}\big)\zeta_p^{ij(\delta)}\big)\\
&= \sum_{j=1}^{p-1} Tr_{G\times\Delta}\big(\big(x^{1/p}\big)\big(\lambda_j x^{j/p}\big)\zeta_p^{ij}\big)\\
&= \sum_{j=1}^{p-1} Tr_{G\times\Delta}\big(\big(x^{(j+1)/p}\big)\lambda_j\zeta_p^{ij}\big).
\end{aligned}
$$

Now $Tr_{G\times\Delta}((x^{(j+1)/p})\lambda_j\zeta_p^{ij}) = Tr_\Delta(\lambda_j\zeta_p^{ij}(Tr_G(x^{(j+1)/p})))$ as $\lambda_j, \zeta_p^{ij} \in K'$ and we saw above that $Tr_G(x^{(j+1)/p}) = 0$ apart from when $j = p-1$. Using this and that fact that $\lambda_{p-1} = 1/x$ we see that

$$
\begin{aligned}
Tr_G\big(Tr_\Delta\big(x^{1/p}\big)g\big(Tr_\Delta\big(x^{1/p}\big)\big)\big) &= Tr_\Delta\big((1/x)\zeta_p^{i(p-1)}\big(Tr_G(x)\big)\big)\\
&= pTr_\Delta\big(\zeta^{-i}\big).
\end{aligned}
$$

Therefore,

$$
Tr_G\big(Tr_\Delta\big(x^{1/p}\big)g\big(Tr_\Delta\big(x^{1/p}\big)\big)\big) = \begin{cases} (p-1)p & \text{if } g=\mathrm{id},\\ -p & \text{if } g\neq \mathrm{id}\end{cases}
$$

as required. □

Theorem 12. *For all $x_j = \prod_{i=0}^{d-1} e_i^{n_i}$ with $0 \leqslant n_i \leqslant p-1$ not all zero,*

$$
\frac{1+Tr_{\Delta_j}(x_j^{1/p})}{p}
$$

is a self-dual normal basis generator for $A_{M_j/K}$.

Proof. From Lemma 9 we know that $(1 + Tr_{\Delta_j}(x_j^{1/p}))/p \in A_{M/K}$. From Lemma 11 we know that

$$T_{M/K}\left(\frac{1 + Tr_{\Delta_j}(x_j^{1/p})}{p}, g\left(\frac{1 + Tr_{\Delta_j}(x_j^{1/p})}{p}\right)\right) = \delta_{1,g}$$

for all $g \in \mathrm{Gal}(M/K)$. Therefore, using Lemma 8 we know that $(1 + Tr_{\Delta_j}(x_j^{1/p}))/p$ is a self-dual normal basis generator for $A_{M_j/K}$. □

Remark 13.

(1) We remark that for every Galois extension, M'/K, of degree p contained in $K_{p,2}$ we can construct a self-dual normal basis generator for $A_{M'/K}$ in this way.
(2) Let $\mathcal{M} = \prod_j M_j$ be the compositum of the field extensions M_j for all j ($\mathcal{M}$ is actually equal to $\prod_{x_j \in \{e_i:\ 0 \leqslant i \leqslant d-1\}} M_i$). This is a weakly ramified extension of K of degree q. The product $\prod_{i=0}^{q-1}(1 + Tr_\Delta(e_i^{1/p}))/(p)$ is then a self-dual element in $\mathcal{M}$ and seems like the obvious choice for a self-dual integral normal basis generator for $A_{\mathcal{M}/K}$. However $v_{\mathcal{M}}(A_{\mathcal{M}/K}) = 1 - q$, and so $\prod_{i=0}^{q-1}(1 + Tr_\Delta(e_i^{1/p}))/(p) \notin A_{\mathcal{M}/K}$ so generalisation up to $\mathcal{M}$ is not as straight forward as one might hope.

Acknowledgments

The author would like to thank his PhD supervisor, Martin Taylor, for all his advice and support. The author would also like to thank the referee for bringing to his attention the paper of Fainsilber and Morales referenced in the introduction.

References

[1] E. Bayer-Fluckiger, H.W. Lenstra, Forms in odd degree extensions and self-dual normal bases, Amer. J. Math. 112 (1990) 359–373.
[2] B. Dwork, On the zeta functions of a hypersurface. II, Ann. of Math. 2 (80) (1964) 227–299.
[3] B. Erez, The Galois structure of the trace form in extensions of odd prime degree, J. Algebra 118 (1988) 438–446.
[4] B. Erez, The Galois structure of the square root of the inverse different, Math. Z. 20 (1991) 239–255.
[5] B. Erez, J. Morales, The Hermitian structure of rings of integers in odd degree Abelian extensions, J. Number Theory 40 (1992) 92–104.
[6] L. Fainsilber, J. Morales, An injectivity result for Hermitian forms over local orders, Illinois J. Math. 43 (2) (1999) 391–402.
[7] I.B. Fesenko, S.V. Vostokov, Local Fields and Their Extensions, second ed., Amer. Math. Soc., 2002.
[8] A. Fröhlich, M.J. Taylor, Algebraic Number Theory, Cambridge University Press, 1991.
[9] K. Iwasawa, Local Class Field Theory, Oxford University Press, 1986.
[10] S. Lang, Cyclotomic Fields II, Springer-Verlag, New York, 1980.
[11] J.P. Serre, Local class field theory, in: J.W.S. Cassels, A. Fröhlich (Eds.), Algebraic Number Theory, Academic Press, London, 1967.
[12] J.P. Serre, Corps Locaux, Hermann, Paris, 1968.
[13] S. Vinatier, Sur la Racine Carrée de la Codifférente, J. Théor. Nombres Bordeaux 15 (2003) 393–410.
[14] L.C. Washington, Introduction to Cyclotomic Fields, Grad. Texts in Math., vol. 83, Springer-Verlag, New York, 1982.