Explicit Construction of Self-Dual Integral Normal Bases for the Square-Root of the Inverse Different

Erik Jarl Pickett

July 5, 2010

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 \( \mathfrak{P}_K \). 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 \cite{13} IV §2 Prop 4, this means that the different, \( D_{L/K} \), of \( L/K \) will have an even valuation, and so we define \( A_{L/K} \) to be the unique fractional ideal such that

\[
A_{L/K} = \mathfrak{O}_{L/K}^{-1/2}.
\]

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 \cite{11} 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 $\mathcal{O}_K G$-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 $(L, T_{L/K}) \cong (K G, l)$. Therefore, if $[L : K]$ is odd, $(A_{L/K}, T_{L/K})$ is isometric to $(\mathcal{O}_K G, l)$ 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, $\pi$, 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 $\pi$. We note that $K_{\pi,n}/K$ is a totally ramified abelian extension of degree $q^n - 1$. In Section 2 we choose $\pi = p$ and prove that the $p$th 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,

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

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 $v_p(\eta) \geq 0$ and also that $E_{\gamma}(X)|_{X = 1}$ is equal to a primitive $p$th root of unity. In Section 2 we use Dwork’s power series to construct a set $\{e_0, \ldots, e_{d-1}\} \subset K_{p,1}$ such that $K_{p,2} = K_{p,1}(e_0^{1/p}, \ldots, e_{d-1}^{1/p})$. 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 $n$th Lubin-Tate extensions are the cyclotomic extensions obtained by adjoining $p^n$th 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 $\zeta_{p^2}$ is a $p^2$th 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 \( \mathbb{Q}_p \). Let \( \pi \) 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

\[
\pi X \equiv f(X) \equiv q X \mod \text{deg } 2; \quad \text{and} \quad f(X) \equiv X^q \mod \pi.
\]

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 [12] 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 \([a]_f(X) \equiv aX \mod \text{deg } 2\). We can use the formal group, \( F_f \), and the formal power series, \([a]_f \), to define an \( \mathfrak{O}_K \)-module structure on \( \mathfrak{P}_K^c = \bigcup_L \mathfrak{P}_L \), where the union is taken over all finite Galois extensions \( L/K \) where \( L \subseteq \bar{K} \). We are going to look at the \( \pi^n \)-torsion points of this module. We let \( E_{f,n} = \{ x \in \mathfrak{P}_K^c : [\pi^n]_f(x) = 0 \} \) 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 Prop. 4), \( K_{\pi,n} \) depends only on the uniformising parameter \( \pi \). 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 \( \zeta_{p^n} \) is a primitive \( p^n \)th 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 \( \beta^{p-1} = -p \). 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 2.1** 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 [12] Chapter 14 §2, we know that \( E_\gamma(X)|_{X=x} \) converges \( p \)-adically when \( v_p(x) \geq 0 \) and that \( E_\gamma(X) \equiv 1 + \gamma X \mod \gamma^2 \). We know then that \( E_\gamma(X)|_{X=1} \neq 1 \). We now raise Dwork’s power series to the power \( p \) and see

\[
\exp(\gamma X - \gamma X^p)^p = \exp(p(\gamma X - \gamma X^p)) = \exp(\gamma p X - \gamma p X^p) = \exp(\gamma p X) \exp(-\gamma p X^p).
\]

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

Let \( \zeta_{q-1} \) 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
Lemma 2.2 \( N_{\mathcal{K}_2/K}(\mathcal{O}_{\mathcal{K}_2}^x) = \langle \pi \rangle \times (1 + \mathfrak{P}_K^2) \) for some uniformizing parameter, \( \pi \) of \( \mathcal{O}_K \).

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

\[
\mathcal{E} = \langle e_i : 0 \leq i \leq d - 1 \rangle \cong \left( \frac{\mathcal{O}_K^x}{\mathcal{O}_K^x(\gamma)} \right)^p / \left( \frac{\mathcal{O}_K^x}{\mathcal{O}_K^x(\gamma)} \right)^p
\]

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

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

\[
K^x/N_{\mathcal{K}_2/K}(\mathcal{O}_{\mathcal{K}_2}^x) \cong \text{Gal}(\mathcal{K}_2/K)\quad \text{and} \quad K^x/N_{\mathcal{K}_{p,2}/K}(\mathcal{O}_{\mathcal{K}_{p,2}}^x) \cong \text{Gal}(\mathcal{K}_2/K),
\]

and so

\[
K^x/N_{\mathcal{K}_2/K}(\mathcal{O}_{\mathcal{K}_2}^x) \cong K^x/N_{\mathcal{K}_{p,2}/K}(\mathcal{O}_{\mathcal{K}_{p,2}}^x).
\]

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

It is straightforward to check that \( \mathcal{K}_2/K \) is totally ramified. Therefore, from [4] IV §3, we know that \( K^x/N_{\mathcal{K}_2/K}(\mathcal{O}_{\mathcal{K}_2}^x) = \mathcal{O}_K^x/N_{\mathcal{K}_2/K}(\mathcal{O}_{\mathcal{K}_2}^x) \cong C_{q-1} \times \prod_{i=1}^d C_p \). The group \( \mathcal{O}_K^x \cong C_{q-1} \times (1 + \mathfrak{P}_K) \), so we know that

\[
(1 + \mathfrak{P}_K)/N_{\mathcal{K}_2/K}(\mathcal{O}_{\mathcal{K}_2}^x) \cong \prod_{i=1}^d C_p.
\]

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,

\[
N_{\mathcal{K}_{p,2}/K}(\mathcal{O}_{\mathcal{K}_{p,2}}^x) = 1 + \mathfrak{P}_K^2.
\]
Let $\Pi$ 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 $< \pi >$ 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

$$< \pi > \times (1 + \mathfrak{P}_K^2) \subseteq N_{\mathcal{K}_2/K}(\mathcal{K}_2^\times).$$

The subgroups $< \pi > \times (1 + \mathfrak{P}_K^2)$ 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 $p$th Hilbert pairing for a field that contains the $p$th 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 2.3** Let $L$ be a field of characteristic 0 with fixed separable algebraic closure $\bar{L}$ and let $\mu_p$ be the group of $p$th roots of unity in $\bar{L}$. Let $\mu_p \subseteq L$. We define the $p$th Hilbert symbol of $L$ as

$$\langle , \rangle_{p,L} : L^\times \times L^\times \longrightarrow \mu_p$$

$$(a, b) \longmapsto (A_L(a))^{(b^{1/p})},$$

where $A_L : L^\times \longrightarrow \text{Gal}(L^{ab}/L)$ 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. $(a, b)_{p,L} = (b, a)_{p,L}^{-1}$.

**Lemma 2.4**

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

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

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 $(\epsilon_i, \zeta_p - 1)_{p,K'} = (N_{K'/\mathbb{Q}_p(\zeta_p)}(\epsilon_i), \zeta_p - 1)_{p,\mathbb{Q}_p(\zeta_p)}$. Recall that $\epsilon_i = E_{\alpha}(X)|_{X = a_i}$ where the set $\{a_i : 0 \leq i \leq p - 1\}$ 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 $\text{Gal}(K'/\mathbb{Q}_p(\zeta_p))$ on each $a_i$ (which will be the same as the action of $\text{Gal}(K'/\mathbb{Q}_p(\zeta_p))$) 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 \( v_p(x) \geq 0 \). As \( a_i^{p^k} \in \Omega_K^\infty \), we have that \( E_\gamma(X)|_{x=a_i^{p^k}} \) converges for all \( k \in \mathbb{Z} \). Therefore \( E_\gamma(X^{p^j})|_{x=a_i} \) must converge and

\[
\phi^k_{K/Q_p}(e_i) = E_\gamma(X^{p^k})|_{x=a_i},
\]

where \( \phi^k_{K/Q_p} \) is the Frobenius element, \( \phi_{K/Q_p} \), applied \( k \) times. We can now make the following derivation:

\[
N_{K'/Q_p(\zeta)}(e_i) = \prod_{g \in \text{Gal}(K'/Q_p(\zeta))} g(e_i) = \prod_{k=0}^{d-1} \phi^k_{K/Q_p}(e_i)
= \prod_{k=0}^{d-1} E_\gamma(X^{p^k})|_{x=a_i} = \prod_{k=0}^{d-1} \exp(\gamma X^{p^k} - \gamma X^{p^{k+1}})|_{x=a_i}
= \exp \left( (\gamma X - \gamma X^p) + (\gamma X^p - \gamma X^{p^2}) + \ldots + (\gamma X^{p^{d-1}} - \gamma X^{p^d}) \right) |_{x=a_i}
= \exp(\gamma X - \gamma X^{p^d})|_{x=a_i}.
\]

We now consider raising to the power \( p \) and see

\[
\exp(\gamma X - \gamma X^{p^d})^p = \exp(p(\gamma X - \gamma X^{p^d}))
= \exp(p\gamma X - p\gamma X^{p^d})
= \exp(p\gamma X) \exp(-p\gamma X^{p^d}).
\]

The power series \( \exp(p\gamma X)|_{x=x} \) will converge when \( v_p(x) \geq 0 \) so we can evaluate at \( X = a_i \) and see, \( (N_{K'/Q_p(\zeta)}(e_i))^p = 1 \). Therefore \( N_{K'/Q_p(\zeta)}(e_i) \) is a \( p \)th root of unity for all \( 0 \leq i \leq d-1 \). If \( N_{K'/Q_p(\zeta)}(e_i) = 1 \) then \( (N_{K'/Q_p(\zeta)}(e_i), 1 - \zeta_p, p_{Q_p(\zeta)} = (1, 1 - \zeta_p, p_{Q_p(\zeta)} = 1) \), so we now assume \( \zeta_p = 1 \). We now let \( \zeta_i \in \text{Gal}(K'/Q_p(\zeta)) \) be such that \( N_{K'(e_i^{1/p})/K}(\zeta_i) = 1 - \zeta_p \). As \( p \) is odd, \( N_{K'(e_i^{1/p})/K}(\zeta_i) = \zeta_p - 1 \), and therefore

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

for all \( 0 \leq i \leq d-1 \).

Next we show that \( \zeta_p - 1 \in N_{K_2/K'}(K_2^\times) \). We have just shown that \( \zeta_p - 1 \in N_{K'(e_i^{1/p})/K'}(K'(e_0^{1/p})^\times) \).

We assume, for induction, that

\[
\zeta_p - 1 \in N_{K'(e_0^{1/p}, \ldots, e_j^{1/p})/K'}(K'(e_0^{1/p}, \ldots, e_j^{1/p})^\times)
\]

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

\[
(\eta, e_{j+1})_{p,K'} = (N_{K'(e_0^{1/p}, \ldots, e_j^{1/p})/K'}(\eta), e_{j+1})_{p,K'}
= (\zeta_p - 1, e_{j+1})_{p,K'}
= (e_{j+1}, \zeta_p - 1)_{p,K'} = 1.
\]
Therefore, 
\[ \eta \in N_{K'((e_0^{1/p}, \ldots, e_{j+1}^{1/p})/K')} N_{\gamma}((e_0^{1/p}, \ldots, e_{j+1}^{1/p}) \times (K'((e_0^{1/p}, \ldots, e_{j+1}^{1/p}) \times K)), \]
and so 
\[ (\zeta_p - 1) \in N_{K'((e_0^{1/p}, \ldots, e_{j+1}^{1/p})/K')} N_{\gamma}((e_0^{1/p}, \ldots, e_{j+1}^{1/p}) \times K)). \]

By induction on \( j \) we see that \((\zeta_p - 1) \in N_{K_2/K}(\zeta_p^{1/p}).\)

Finally we note that the minimal polynomial of \( \zeta_p - 1 \) 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 \( p \in N_{K_2/K}(\zeta_p^{1/p}).\) □

**Theorem 2.5**

\[ K_{p,2} = K_{p,1}(e_0^{1/p}, e_1^{1/p}, \ldots, e_{d-1}^{1/p}) . \]

**Proof.** From Lemma 2.2 we know that \(N_{K_2/K}(\zeta_p^{1/p}) = <\pi > \times 1 + \mathfrak{P}_K^2\) where \( \pi = up \) for some \( u \in \mathcal{O}_K.\) From Lemma 2.4 we know that \(p \in N_{K_2/K}(\zeta_p^{1/p})\) and therefore that \(N_{K_2/K}(\zeta_p^{1/p}) = <\pi > \times 1 + \mathfrak{P}_K^2.\) From [2] Proposition 5.16, we know that \(N_{K_2/K}(\zeta_p^{1/p}) = <\pi > \times (1 + \mathfrak{P}_K^2).\) As \(K_2/K\) and \(K_{p,2}/K\) are both finite abelian extensions of local fields contained in \(K\) and \(N_{K_{p,2}/K}(\zeta_p^{1/p}) = N_{K_2/K}(\zeta_p^{1/p}),\) from [13] Appendix Theorem 9, we know that \(K_2 = K_{p,2}.\) □

## 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 \(p\)th 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 \(\{a_i : 0 \leq i \leq d-1\}\) is a \(Z_p\)-basis for \(\mathcal{O}_K\) 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 \(0 \leq n_i \leq p-1,\) 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 \(\text{Gal}(K'(x_j^{1/p})/M_j) = \Delta_j.\) From now on we will drop the subscript for \(N_j, x_j, M_j\) and \(\Delta_j\) 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 \(\text{Gal}(K'(x^{1/p})/K') = G,\) and as all the groups we are dealing with are abelian we will use an abuse of notation and write \(\text{Gal}(M/K) = G\) and \(\text{Gal}(K'/K) = \Delta.\)

Let \(A_{M/K} = \mathcal{O}_{M/K}^{-1/2}\) 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 \(A_{M/K}\).
Figure 1: Abelian extensions of $K$

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 3.1**

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

**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 $\alpha$ be a primitive $[p^2]$-division point for $F_f(X,Y)$. We see that

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

Given \(f(X) \in \Omega_K[X]\) such that \(f(X) \equiv pX \mod \deg 2\) and \(f(X) \equiv X^q \mod p\), the standard proof in the literature of the existence of a formal group \(F(X,Y) \in \Omega_K[[X,Y]]\) 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 \(i\)th iteration calculates \(F(X,Y) \mod \deg(i + 1)\) 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 \(F^i(X,Y) \equiv F(X,Y) \mod \deg(i + 1)\) and define \(E_i\) to be the \(i\)th error term, i.e., \(E_i = f(F^{i-1}(X,Y)) - F^{i-1}(f(X), f(Y)) \mod \deg(i + 1)\). 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

\[
f(F^{1}(X,Y)) - F^{1}(f(X), f(Y)) = (X + Y)^q + p(X + Y) - (X^q + pX + Y^q + pY) = \sum_{i=1}^{q-1} \binom{q}{i} X^i Y^{q-i}.
\]

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

\[
F(X,Y) \equiv X + Y - \sum_{i=1}^{q-1} \binom{q}{i} X^i Y^{q-i} \mod \deg(q + 1).
\]

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

\[
[1 + up](\alpha) \equiv \alpha + u(\alpha^q + p\alpha) - \sum_{i=1}^{q-1} \binom{q}{i} \frac{u(\alpha^q + p\alpha)^{q-i}}{p(1 - p^{q-1})} \mod \alpha^{q+1}
\]

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

Let \(\Gamma = Gal(K_{p,2}/K_{p,1})\). We know that \(\alpha\) is a uniformising parameter for \(\Omega_{K_{p,2}}\) and that \(p \in \mathfrak{P}_{K_{p,2}}^{q(q-1)}\). An element \(s \in \Gamma\) is in the \(i\)th ramification group (with the lower numbering), \(\Gamma_i\), if and only if \(s(\alpha)/\alpha \equiv 1 \mod \mathfrak{P}_{K_{p,2}}^i\), see [12] IV §2 Prop 5. We have shown that for \(1 \neq s \in \Gamma\) then \(s(\alpha)/\alpha \equiv 1 + u\alpha^{q-1} \mod \mathfrak{P}_{K_{p,2}}^q\). Therefore, \(\Gamma = \Gamma_i\) for \(0 \leq i \leq (q - 1)\) 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 $Gal(N/K_{p,1}) = Gal(N/K_{p,1})^i$ for $0 \leq i \leq (q-1)$, and $Gal(N/K_{p,1})^q = \{1\}$ and switching back to the lower numbering we have $Gal(N/K_{p,1}) = Gal(N/K_{p,1})_i$ for $0 \leq i \leq (q-1)$, and $Gal(N/K_{p,1})_q = \{1\}$.

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

$$v_N(\mathcal{D}_{N/K_{p,1}}) = \sum_{i \geq 0} (|Gal(N/K_{p,1})_i| - 1),$$

and so $v_N(\mathcal{D}_{N/K_{p,2}}) = q(p-1)$. 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 $v_N(\mathcal{D}_{N/M}) = v_{K_{p,1}}(\mathcal{D}_{K_{p,1}/K}) = q-2$. From [5] III.2.15 we know, for a separable tower of fields $L'' \supset L' \supset L$, the different of these field extensions are linked by the formula $\mathcal{D}_{L''/L} = \mathcal{D}_{L'/L} \mathcal{D}_{L/L}$. We therefore have $v_M(\mathcal{D}_{M/K}) = 2(p-1)$, and so $v_M(A_{M/K}) = 1 - p$. \(\square\)

**Remark 3.2** We remark that this lemmama 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 3.3** Let $a$ be an elemmaent 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 $A_{L/K} = \mathcal{D}_K[G].a$.

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

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

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

**Lemma 3.4**

$$\frac{1 + \text{Tr}_{\Delta}(x^{1/p})}{p} \in A_{M/K}.$$
Therefore, we have just shown that \( x^{1/p} - 1 \) is a uniformising parameter for \( \mathcal{O}_{K'(x^{1/p})} \). As \( K'(x^{1/p})/M \) is a totally, tamely ramified extension, we know that \( \text{Tr}_{\Delta}(x^{1/p} - 1) \in \mathfrak{P}_M \) so \( v_M(\text{Tr}_{\Delta}(x^{1/p} - 1)) \geq 1 \). We know that

\[
\text{Tr}_{\Delta}(x^{1/p} - 1) = \text{Tr}_{\Delta}(x^{1/p}) - (p - 1) = (1 + \text{Tr}_{\Delta}(x^{1/p})) - p.
\]

Therefore, \( v_M(1 + \text{Tr}_{\Delta}(x^{1/p})) \geq 1 \) and \( v_M \left( \frac{1 + \text{Tr}_{\Delta}(x^{1/p})}{p} \right) \geq 1 - p \). Since \( v_M(A_{M/K}) = 1 - p \), we must have \( \frac{1 + \text{Tr}_{\Delta}(x^{1/p})}{p} \in A_{M/K} \). \( \square \)

**Lemma 3.5** Let \( x = \prod_{i=0}^{d-1} e_i^{n_i} \) for some \( n_i \in \mathbb{Z}^+ \), and let \( \delta \in \Delta = \text{Gal}(K'(x^{1/p})/M) \). 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:

\[
\exp(\chi(\delta)X - \chi(\delta)^X)^p = \exp \left( (\chi(\delta)X + \frac{(\chi(\delta)^X)^p}{p} \right).
\]

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

\[
(E_{\gamma}(X) \mid_{X=a_i})^{\chi(\delta)} = (\exp(\gamma X - \gamma X^p) \mid_{X=a_i})^{\chi(\delta)}
\]

\[
= \exp(\chi(\delta)(\gamma X - \gamma X^p)) \mid_{X=a_i}
\]

\[
= \exp(\chi(\delta)\gamma X - \chi(\delta)^X) \mid_{X=a_i}.
\]

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

\[
\delta(\gamma X - \gamma X^p) \mid_{X=a_i} = (\delta(\gamma)X - \delta(\gamma)X^p) \mid_{X=a_i} = (\chi(\delta)\gamma X - \chi(\delta)^X) \mid_{X=a_i}.
\]

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

\[
\exp(\chi(\delta)\gamma X - \chi(\delta)^X) \mid_{X=a_i} = \exp(\delta(\gamma)X - \delta(\gamma)X^p) \mid_{X=a_i}
\]

\[
= \delta(\exp(\gamma X - \gamma X^p) \mid_{X=a_i})
\]

\[
= \delta(E_{\gamma}(X) \mid_{X=a_i}.
\]

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

**Lemma 3.6** Let \( g \in \text{Gal}(M/K) \), then

\[
T_{M/K} \left( \frac{1 + \text{Tr}_{\Delta}(x^{1/p})}{p} \cdot g \left( \frac{1 + \text{Tr}_{\Delta}(x^{1/p})}{p} \right) \right) = \delta_{1,g}.
\]
Proof. First we observe that $Tr_G(x^{i/p}) = \sum_{g \in G} g(x^{i/p}) = x^{1/p} \sum_{j=0}^{p-1} g_{ij} = 0$ for all $p \nmid i$. 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 $p \nmid i$. We make the following derivation:

$$Tr_G \left( \left( \frac{1 + Tr_\Delta(x^{1/p})}{p} \right) g \left( \frac{1 + Tr_\Delta(x^{1/p})}{p} \right) \right) = Tr_G \left( \frac{1 + Tr_\Delta(x^{1/p})}{p} \cdot \frac{1 + g(Tr_\Delta(x^{1/p}))}{p} \right) = Tr_G \left( \frac{1 + Tr_\Delta(x^{1/p}) + g(Tr_\Delta(x^{1/p})) + Tr_\Delta(x^{1/p})g(Tr_\Delta(x^{1/p}))}{p^2} \right) = Tr_G \left( \frac{1 + Tr_\Delta(x^{1/p})g(Tr_\Delta(x^{1/p}))}{p^2} \right) = \frac{p + Tr_G(Tr_\Delta(x^{1/p})g(Tr_\Delta(x^{1/p})))}{p^2}.$$ 

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

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

From Lemma 3.5 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 $\chi(\delta) \equiv j(\delta) \mod p$, for some $1 \leq j(\delta) \leq (p - 1)$ and note that $j(\delta) = j(\delta')$ if and only if $\delta = \delta'$. We can therefore define a set of constants $\{\lambda_{j(\delta)} \in \Omega_{K^2} : \delta \in \Delta\}$ such that $\delta(x^{1/p}) = \lambda_{j(\delta)} x^{\chi(\delta)/p}$. 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 $\sigma$ on $x^{1/p}$. We have $\sigma(x^{1/p}) = \zeta_p x^{\chi(\sigma)/p} = \zeta_p x^{1/p}$, so

$$\sigma^2(x^{1/p}) = \sigma(\zeta_p) \sigma(x^{1/p}) = \zeta_p^{-1} \sigma(x^{1/p})^{-1} = \zeta_p^{-1} (\zeta_p x^{1/p})^{-1} = \zeta_p^{-2} x^{1/p}.$$ 

As $\sigma$ is an involution, $x^{1/p} = \zeta_p^{-2} x^{1/p}$, so we have $\zeta_p = 1$. 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 $0 \leq i \leq p - 1$ with $i = 0$ when $g = id$. 

12
Using this notation we make the following derivation:

\[
Tr_G(Tr_\Delta(x^{1/p})g(Tr_\Delta(x^{1/p}))) = Tr_G \left( \sum_{\xi \in \Delta} \xi (x^{1/p}) \right) \left( g(\sum_{\eta \in \Delta} \eta (x^{1/p})) \right) \\
= Tr_G \left( \sum_{\xi \in \Delta} \xi (x^{1/p}) g(\eta (x^{1/p})) \right) \\
= Tr_G \left( \sum_{\xi \in \Delta} \xi (x^{1/p}) \eta g(x^{1/p}) \right) \\
= Tr_G \left( \sum_{\xi \in \Delta} \xi (x^{1/p}) \xi \delta g(x^{1/p}) \right) \\
= Tr_G \left( \sum_{\delta \in \Delta} (x^{1/p}) \delta g(x^{1/p}) \right) \\
= \sum_{\delta \in \Delta} Tr_{G \times \Delta} ((x^{1/p}) \delta g(x^{1/p})) \\
= \sum_{\delta \in \Delta} Tr_{G \times \Delta} ((x^{1/p}) \delta (\zeta^j(x^{1/p}))) \\
= \sum_{\delta \in \Delta} Tr_{G \times \Delta} ((x^{1/p}) \delta (\zeta^i_p)) \\
= \sum_{\delta \in \Delta} Tr_{G \times \Delta} ((x^{1/p}) (\lambda_j \zeta^{j+1/p}) \zeta^{ij}) \\
= \sum_{j=1}^{p-1} Tr_{G \times \Delta} ((x^{j+1/p}) \lambda_j \zeta^{ij}) .
\]

Now \( Tr_{G \times \Delta} ((x^{j+1/p}) \lambda_j \zeta^{ij}) = Tr_\Delta (\lambda_j \zeta^{ij}_p (Tr_G(x^{j+1/p}))) \) as \( \lambda_j, \zeta^{ij}_p \in K' \) 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

\[
Tr_G(Tr_\Delta(x^{1/p})g(Tr_\Delta(x^{1/p}))) = Tr_\Delta(1/x) \zeta^{i(p-1)}(Tr_G(x)) \\
= p Tr_\Delta(\zeta^{-1}).
\]

Therefore,

\[
Tr_G(Tr_\Delta(x^{1/p})g(Tr_\Delta(x^{1/p}))) = \begin{cases} 
(p-1)p & \text{if } fg = id \\
-p & \text{if } fg \neq id
\end{cases}
\]

as required. \qed

**Theorem 3.7** For all \( x_j = \prod_{i=0}^{d-1} a_i^{e_i} \) with \( 0 \leq n_i \leq p - 1 \) 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 3.4 we know that \((1 + Tr_{\Delta_j}(x_j^{1/p}))/p \in A_{M/K}\). From Lemma 3.6 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 \(g \in Gal(M/K)\). Therefore, using Lemma 3.3 we know that \((1 + Tr_{\Delta_j}(x_j^{1/p}))/p\) is a self-dual normal basis generator for \(A_{M_j/K}\).

\[\square\]

**Remark 3.8**

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 \(M = \prod_j M_j\) be the compositum of the field extensions \(M_j\) for all \(j\) (\(M\) is actually equal to \(\prod_{x_j \in \{e_i : 0 \leq i \leq d-1\}} M_i\)). 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 \(A_{M}/K\) and seems like the obvious choice for a self-dual integral normal basis generator for \(A_{M/K}\). However \(v_M(A_{M/K}) = 1 - q\), and so \(\prod_{i=0}^{q-1}(1 + Tr_{\Delta}(e_i^{1/p}))/p \notin A_{M/K}\) so generalisation up to \(M\) is not as straightforward as one might hope.

**References**

[1] E. Bayer-Fluckiger and H. W. Lenstra. Forms in Odd Degree Extensions and Self-Dual Normal Bases. *Amer. J. Math.*, (112):359–373, 1990.

[2] B. Dwork. On the Zeta Functions of a Hypersurface.II. *Ann. of Math.*, 2(80):227–299, 1964.

[3] B. Erez. The Galois Structure of the Trace Form in Extensions of Odd Prime Degree. *J. Algebra*, (118):438–446, 1988.

[4] B. Erez. The Galois Structure of the Square Root of the Inverse Different. *Math.Z.*, (208):239–255, 1991.

[5] B. Erez and J. Morales. The Hermitian Structure of Rings of Integers in Odd Degree Abelian Extensions. *J. of Number Theory*, (40):92–104, 1992.

[6] L. Fainsilber and J. Morales. An Injectivity Result for Hermitian Forms Over Local Orders. *Illinois J. Math.*, 43(2):391–402, 1999.

[7] I. B. Fesenko and S. V. Vostokov. *Local Fields and Their Extensions*. American Mathematical Society, second edition, 2002.
[8] A. Fröhlich and 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 and A. Fröhlich, editors, *Algebraic Number Theory*, London, 1967. Academic Press.

[12] J. P. Serre. *Corps Locaux*. Hermann, Paris, 1968.

[13] S. Vinatier. Sur la Racine Carrée de la Codifférente. *J. Théor. Nombres Bordeaux*, 15:393–410, 2003.

[14] L. C. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.