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 $\{e_0, \ldots, e_{d-1}\} \subset K_{p,1}$ 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 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

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