Generating the root of the codifferent by values of elliptic functions

Cornelius Greither

26th May, 2016

Abstract

It is well known that the square root $A_{L/K}$ of the codifferent in a weakly ramified G-Galois extension of p-adic fields is a free $\mathfrak{O}_K[G]$-module. We will also assume that L/K is totally ramified. Then G is elementary p-abelian. The case $K = \mathbb{Q}_p$ is nice and simple: here G is at most cyclic of order p, L is "essentially" the degree p subfield of $\mathbb{Q}(\zeta_{p^2})$, and Erez gave a generator of $A_{L/K}$ in terms of ζ_{p^2}. More general constructions were given by Pickett-Vinatier and by the author. They are still very cyclotomic in spirit, using Kummer extensions. New work of Pickett-Thomas involves formal groups. So it is tempting to look around for a construction that combines both aspects: globality, and the use of algebraic groups. We try to do this in a very modest case: K is unramified quadratic over $\mathbb{Q}_p$, and G is bi-cyclic of order p^2 (which is the largest possible for such K). We pick the elliptic curve $E : y^2 = x^3 + x$ defined over $\mathbb{Q}$, and we restrict to $p \equiv 3 \pmod 4$, so $K = \mathbb{Q}(i)$. Note that E has complex multiplication with $\mathbb{Z}[i]$. We do find a local generator for $A_{L/K}$ with global origin: it comes from division values of an appropriate elliptic function on E. It is an important feature of our approach that the extension L/K is the completion of an abelian extension of $\mathbb{Q}(i)$ which has the same Galois group G and is unramified outside p. So far we haven't succeeded in finding a global generator. Indeed, the generators which we exhibit fail to generate the root of the global codifferent at certain primes (of course finite in number), and we do not yet understand the nature and origin of those bad primes.

0 The starting point

Let $p \neq 2$ be prime, K be an extension of $\mathbb{Q}_p$, and L/K a G-Galois extension. Assume that L/K is weakly ramified (that is, $G_2 = \{1\}$). Assume further (for simplicity) that L/K is totally ramified. Then

$$G \cong \frac{G_0}{G_2} \cong \frac{G}{G_2} \text{ is elementary abelian.}$$

Let $A = A_{L/K} = \mathcal{D}_{L/K}^{-1/2}$ be the square root of the inverse different. It is well known that A is free over $\mathfrak{O}_K[G]$. Any $x \in A$ with $v_L(x) = 1 - [L : K]$ is a generator. If $K/\mathbb{Q}_p$ is unramified then there exists a maximal extension L/K with all the above quantities, and by local class field theory we have

$$\begin{array}{cccccc} & G & \cong & \dfrac{1 + p\mathfrak{O}_K}{1 + p^2\mathfrak{O}_K} & \cong & \left(\dfrac{\mathfrak{O}_K}{p}, +\right) \\ \text{via} & & & 1 + pu & \leftarrow\!\shortmid & u. \end{array}$$

Given K, the extension L is not quite unique, but writing K^{nr} for the maximal unramified extension of K, we at least have that $LK^{\mathrm{nr}}/K^{\mathrm{nr}}$ is unique.

For $K = \mathbb{Q}_p$, L is the degree p subfield of $M = \mathbb{Q}_p(\zeta_{p^2})$. In this situation, Erez showed that $A_{L/K}$ is generated by

$$x_L = \frac{1}{p}\left(\mathrm{Tr}_{M/L}(\zeta_{p^2}) + 1\right).$$

In the case that $K/\mathbb{Q}_p$ is unramified and L'/K is a cyclic subextension of L/K, Pickett gave a generator $x = x_{L'}$ of $A_{L'/K}$ that is self-dual: $\mathrm{Tr}_{L'/K}(x^\sigma x^\tau) = \delta_{\sigma,\tau}$.

Here is a very brief overview of relevant results:

Author(s)	Allow $K/\mathbb{Q}_p$ ramified	Allow L'/K noncyclic	Give self-dual basis
Pickett	—	—	✓
G.	✓	—	✓
G.	—	✓	—
Pickett-Thomas	✓	✓	—

1 The goal and the setting

We would like to combine two aspects: globality, and the use of algebraic groups. Choose $K = \mathbb{Q}_p(i)$, $p \equiv 3 \pmod 4$, $E : y^2 = x^3 + x$. This elliptic curve has complex multiplication by $\mathbb{Z}[i]$:

$$\begin{aligned} [i]x &= -x \\ [i]y &= iy. \end{aligned}$$

Construct L/K weakly ramified bicyclic as follows. Adopt the following global notation:

$$\begin{tikzcd}
 & \tilde K(p^2) \arrow[dd, dash, "p^2"] \\
\tilde L \arrow[ur, dash] \arrow[dd, dash] & \\
 & \tilde K(p) \\
\mathbb{Q}(i) = \tilde K \arrow[ur, dash, "(p^2-1)/4"'] &
\end{tikzcd}$$

Here $\tilde K(p)$, $\tilde K(p^2)$ denote the ray class fields of conductors p, p^2 respectively, and $\tilde L/\tilde K$ is totally and weakly ramified. The corresponding local setup is obtained by completing these objects at p, giving

$$\begin{tikzcd}
 & M \arrow[dd, dash] \\
L \arrow[ur, dash] \arrow[dd, dash] & \\
 & K_1 \\
K \arrow[ur, dash] &
\end{tikzcd}$$

We have

$$\begin{array}{rclcl} E(\mathbb{C}) & = & \mathbb{C}\big/\Lambda & \to & \{(x,y) \mid y^2 = x^3 + x\} \\ & & z & \mapsto & (\wp(z), \wp'(z)) \qquad\qquad = \ (X(z), Y(z)), \text{ say.} \end{array}$$

Now we have the deep fact that $\tilde{K}(p^2) = K(X^2(\beta))$ with β a primitive p^2-division point on $E(\mathbb{C})$. We can describe the Galois action:

$$\begin{array}{rccc} & \mathrm{Gal}(\tilde{K}(p^2)/\tilde{K}) & = & \left(\mathbb{Z}[i]/p^2\right)\Big/\mu_4 \\ & \sigma_u & \leftarrow\!\shortmid & \overline{u}, \\ \text{and} & \sigma_u\left(X^2(\beta)\right) & = & X^2(u\beta). \end{array}$$

Idea: In order to find a generator of $A_{L/K}$, try

$$x = \frac{1}{p}\left(\mathrm{Tr}_{M/L}(D(\beta)) + c\right),$$

for some elliptic function D in $\mathbb{Q}(X^2)$ and c some integer chosen to make the valuation of x correct.

We cannot let D be X^2 itself: $X^2(\beta)$ is not p-integral. We cannot take $D = X^{-2}$ either: $X^{-2}(\beta)$ *is* p-integral and congruent to 0 modulo $\mathfrak{p}_L$, and we can take $c = 0$, but then we need $\mathrm{Tr}_{L/K}(x) \sim p$, and we find that $\mathrm{Tr}_{L/K}(x) \sim p^2$.

We take $D(z) = \dfrac{X^2(z)+1}{X^2(z)-1}$.

2 A distribution relation for D

Proposition 1. *For all $z \in \mathbb{C}$ and all $m \in \mathbb{Z}$ such that $m \equiv 3 \pmod 4$, we have*

$$\sum_{\alpha \in E[m]} D(z+\alpha) = -mD(mz).$$

The *proof* is omitted here.

We now let $y = D(\beta)$ for a chosen $\beta \in E[p^2] - E[p]$, so β is a primitive p^2-division point.

Lemma 2. *$y \in \mathfrak{O}_M[1/2]$ and $y \equiv 1 \pmod{\mathfrak{p}_M}$.*

Sketch Proof. $q \nmid 2p$, so E is still an elliptic curve modulo q. The zeroes of $X^2(z) - 1$ are in $E[4]$. Hence $X^2(\beta) - 1$ is not zero. Moreover

$$y = \frac{1 + X^{-2}(\beta)}{1 - X^{-2}(\beta)},$$

and $X^{-2}(\beta) \in \mathfrak{p}_M$. □

3 A trace formula, and the main result

Recall $\beta \in E[p^2] - E[p]$ and $y = D(\beta)$.

Proposition 3. $\mathrm{Tr}_{M/K}(y) = p\frac{p+1}{4}$.

Proof.

$$\begin{aligned}
\mathrm{Tr}_{M/K_1}(y) &= \sum_{u \in \mathfrak{O}_K/p} D(\beta)^{\sigma_{1+pu}} \\
&= \sum_{u \in \mathfrak{O}_K/p} D((1+pu)\beta) \\
&= \sum_{u \in \mathfrak{O}_K/p} D(\beta + pu\beta) \\
&= \sum_{\alpha \in E[p]} D(\beta + \alpha) \\
&= -pD(p\beta) \quad \text{by Prop. 1.}
\end{aligned}$$

Let $\gamma = p\beta$. We still need to prove that:

$$\mathrm{Tr}_{K_1/K} D(\gamma) = -\frac{p+1}{4}.$$

We have:

$$\sum_{\alpha \in E[p]} D(0+\alpha) = -pD(p \cdot 0) = -p,$$

and also

$$\begin{aligned}
\sum_{\alpha \in E[p]} D(0+\alpha) &= D(0) + \sum_{\substack{\alpha \in E[p] \\ \alpha \neq 0}} D(\alpha) \\
&= 1 + 4\mathrm{Tr}_{K_1/K} D(\gamma).
\end{aligned}$$

Rearranging this gives the result. □

Now let $x_0 = \mathrm{Tr}_{M/L}(y) + \frac{p+1}{4}$ and $x = \frac{1}{p}x_0$.

Theorem 4.

1) $x_0 \in \mathfrak{p}_L$*;*

2) $\mathrm{Tr}_{L/K}(x_0) \sim p$*;*

3) (Main result) *The element x generates $A_{L/K}$ over $\mathfrak{O}_K[G]$.*

Proof. Part (1): We have $y \equiv 1 \pmod{\mathfrak{p}_M}$, and $\mathrm{Tr}_{M/L}(y) \equiv \frac{p^2-1}{4} \pmod{\mathfrak{p}_L}$, so

$$x_0 \equiv \frac{p^2-1}{4} + \frac{p+1}{4} \equiv 0 \pmod{\mathfrak{p}_L}.$$

Part (2): We calculate

$$\begin{aligned}
\mathrm{Tr}_{L/K}(x_0) &= \mathrm{Tr}_{M/K}(y) + p^2\frac{p+1}{4} \\
&= p\frac{p+1}{4} + p^2\frac{p+1}{4} \qquad \text{by Prop. 3} \\
&= p\frac{(p+1)^2}{4}.
\end{aligned}$$

Part (3): We know $x \in A$ since $v_L(x_0) \geq 1$, and $v_L(x) \geq 1 - [L : K]$. We want equality to hold. If not, we would have $v_L(x_0) \geq 2$, but then we may apply the usual formula that describes, in terms of the different, how the valuation behaves under taking the trace, and we get that $\mathrm{Tr}_{L/K}(x_0)$ would be divisible by p^2, contradicting part (2). □

4 What can we say besides Theorem 4?

The element x comes from a global construction. It seems natural to ask the following questions.

1) *Does x generate $A_{\tilde{L}/\tilde{K}}$ globally (maybe outside 2)?*

2) *Is the generator x self-dual (i.e. $\mathrm{Tr}_{L/K}(x^\sigma x^\tau) = \delta_{\sigma,\tau}$)?*

3) *What do we get by numerical verification?*

As of now, we have the following answers to offer.

Concerning 3): We did the primes 3, 7, 11, 19, 23, and everything checks out as it should, which is reassuring.

Concerning 1) and 2): In general, the answer is No. Let us look at the trace matrix $T = (\mathrm{Tr}(x^\sigma \tau^\tau))_{\sigma,\tau\in G}$ (recall that we can identify G with $\mathbb{F}_{p^2} \cong \mathbb{Z}[i]/p$). Self-duality would mean that $T = I$, x being a generator over $q \nmid 2p$ would mean that $\det(T)$ is a unit at q.

For $p = 3$ we get:

$$T = \begin{pmatrix}
4 & 2 & 2 & 2 & 1 & 1 & 2 & 1 & 1 \\
\vdots & \ddots & & & & & & & \vdots \\
\vdots & & \ddots & & & & & & \vdots \\
\vdots & & & \ddots & & & & & \vdots
\end{pmatrix}$$

where the column indices correspond to the enumeration $0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i$ of the field $\mathbb{F}_9$. We find in this case that $\det(T) = 2^{12}$, so indeed x is a global generator outside 2.

However, for $p = 7$, $\det(T)$ contains the prime factors $2, 13, 67, 2267$. We have no arithmetic explanation for these "bad" primes. The next step would be a systematic search for an elliptic function that works better than D. For this, presumably an in-depth study of elliptic resolvents is necessary.

Acknowledgments: The author would like to cordially thank Griff Elder for all the work he put into the organization of the Omaha 2016 workshop, and also Paul Truman for producing

this very nice typeset version, from the notes he took of my talk given as an old-fashioned white-board lecture.