**Mersenne primes and class field theory**
Jansen, B.J.H.

**Author**: Jansen, Bas
**Title**: Mersenne primes and class field theory
**Date**: 2012-12-18

# Chapter 5

# The Lehmer symbol

In this chapter we state an observation made by Lehmer giving rise to what we will call the *Lehmer symbol* (see [4, §A3, page 9]), which is the main object of study in this thesis. After we have introduced this symbol, we will relate it to the so-called *Frobenius symbol.* In Chapters 7 and 9 properties of the Frobenius symbol will be used to prove properties of the Lehmer symbol.

## Lehmer's observation and the Frobenius symbol

We start with stating Lehmer's observation. Let $p \in \mathbb{Z}_{>2}$ be such that $M_p = 2^p - 1$ is prime, so in particular $p$ is an odd prime. Let $s \in K$ be a starting value for $p$ (see Definition 2.5). Let $(s \bmod M_p)$ be as in Definition 2.4. Define $s_i$ for $i \in \{1, 2, \ldots, p-1\}$ by $s_1 = (s \bmod M_p)$ and $s_{i+1} = s_i^2 - 2$.

**Proposition 5.1.** *Let the assumptions be as above. Then we have* $s_{p-2} = \epsilon(s,p)2^{(p+1)/2}$ *for a unique* $\epsilon(s,p) \in \{-1, +1\}$.

In order to see this, note that by Theorem 2.1 we have $s_{p-1} = 0$. So Proposition 5.1 follows from

$$0 = s_{p-1} = s_{p-2}^2 - 2 = s_{p-2}^2 - 2^{p+1} = (s_{p-2} - 2^{(p+1)/2})(s_{p-2} + 2^{(p+1)/2})$$

and the fact that $M_p$ is prime.

Now we will define $\epsilon(s,p)$ for $s$ in the field $K = \bigcup_{n=1}^{\infty} \mathbb{Q}(\sqrt[n]{2})$ of characteristic zero. Take $s \in K$. Define $P(s)$ by

$$P(s) = \{p \in \mathbb{Z}_{>2} : M_p \text{ is prime and } s \text{ is a starting value for } p\}.$$

**Definition 5.2.** *Let* $s \in K$ *and* $p \in P(s)$*. We define the Lehmer symbol* $\epsilon(s,p)$ *by*

$$\epsilon(s,p) = \epsilon(s \bmod M_p, p).$$

Next we define the Frobenius symbol. Let $F/E$ be a finite Galois extension of number fields with Galois group $G$. Let $\mathfrak{m}$ be a non-zero prime ideal of the ring of integers $\mathcal{O}_E$ of $E$ that is unramified in $F$. Let $\mathfrak{M}$ be a prime ideal of the ring of integers $\mathcal{O}_F$ of $F$ above $\mathfrak{m}$, i.e. $\mathcal{O}_E \cap \mathfrak{M} = \mathfrak{m}$. Let $H$ be a subgroup of $G$. We denote the fixed field of $H$ by $L$.

**Theorem 5.3.** *There is a unique element* $\mathrm{Frob}_{\mathfrak{M}}$ *in $G$ with the property*

$$\forall x \in \mathcal{O}_F\colon \quad \mathrm{Frob}_{\mathfrak{M}}(x) \equiv x^{\#(\mathcal{O}_E/\mathfrak{m})} \bmod \mathfrak{M},$$

*where $\#(\mathcal{O}_E/\mathfrak{m})$ is the number of elements of $\mathcal{O}_E/\mathfrak{m}$. Furthermore the inertia degree of $\mathcal{O}_L \cap \mathfrak{M}$ over $\mathfrak{m}$ is 1 if and only if* $\mathrm{Frob}_{\mathfrak{M}} \in H$.

For a proof of Theorem 5.3 see the next section. We call the unique element $\mathrm{Frob}_{\mathfrak{M}}$ of Theorem 5.3 the *Frobenius symbol* of $\mathfrak{M}$ over $E$. If we want to make the extension $F/E$ explicit, then we denote $\mathrm{Frob}_{\mathfrak{M}}$ by

$$(\mathfrak{M}, F/E) \text{ or } \Big(\frac{\mathfrak{M}}{F/E}\Big).$$

The Galois group $G$ acts transitively on the set of prime ideals of $\mathcal{O}_F$ above $\mathfrak{m}$ and $(\sigma(\mathfrak{M}), F/E) = \sigma(\mathfrak{M}, F/E)\sigma^{-1}$ for any $\sigma \in G$ (see [7, Chapter I, §5]). Therefore the conjugacy class of $(\mathfrak{M}, F/E)$ in $G$ does not depend on the choice of a prime $\mathfrak{M}$ above $\mathfrak{m}$. Hence we can define $(\mathfrak{m}, F/E)$ to be the conjugacy class of $(\mathfrak{M}, F/E)$ in $G$. When it is clear in which extension we work we will denote $(\mathfrak{m}, F/E)$ by $\mathrm{Frob}_{\mathfrak{m}}$.

We will also use the so-called consistency property of the Frobenius symbol. We will state this property in the next proposition. Let $F'$ be a number field such that $E \subset F' \subset F$ and $F'/E$ Galois. Let $\mathfrak{M}'$ be the prime below $\mathfrak{M}$ in $F'$, i.e. $\mathfrak{M}' = \mathfrak{M} \cap F'$.

**Proposition 5.4.** *We have $(\mathfrak{M}, F/E)|_{F'} = (\mathfrak{M}', F'/E)$, where $(\mathfrak{M}, F/E)|_{F'}$ is the restriction of $(\mathfrak{M}, F/E)$ to the field $F'$.*

For a proof of Proposition 5.4 see [7, Chapter X, §1].

Now we relate the Lehmer symbol and the Frobenius symbol. First we recall some notation of Chapter 4. Let $s \in K$ be a potential starting value, let $f_s = x^{16} - sx^8 + 1$ and let $L_s$ be the splitting field of $f_s$ over $\mathbb{Q}(s)$. Define $K_s$ by $K_s = L_s \cap K$ and let $n \in \mathbb{Z}_{>0}$ be such that $K_s = \mathbb{Q}(\sqrt[n]{2})$. Define $K_s'' = K_s(\sqrt{s-2}, \sqrt{-s-2})$. As in Chapter 4 let $G_s = \mathrm{Gal}(L_s/K_s)$ be the Galois group of $L_s$ over $K_s$. Recall that the equivalence relation $\sim$ on $G_s$ is defined by conjugation. Note that the set $\mathrm{Gal}(L_s/K_s'')^{\mathrm{gen}}$ of elements of order 8 in $\mathrm{Gal}(L_s/K_s'')$ is closed under $\sim$.

**Proposition 5.5.** *Let $s \in K$ and let $p \in P(s)$. Then the ideal $(\sqrt[n]{2}^p - 1)$ in $\mathcal{O}_{K_s}$ is prime and unramified in $L_s$. Furthermore we have* $\mathrm{Frob}((\sqrt[n]{2}^p - 1), L_s/K_s) \in \mathrm{Gal}(L_s/K_s'')^{\mathrm{gen}}/\!\sim$.

We prove Proposition 5.5 in the last section of this chapter. Recall the map

$$\lambda_s : \mathrm{Gal}(L_s/K_s'')^{\mathrm{gen}}/{\sim} \to \{+1, -1\}$$

of Chapter 4. We define the map

$$\epsilon_s : P(s) \to \{+1, -1\}$$

by $\epsilon_s : p \mapsto \epsilon(s, p)$ and we define a map

$$\mathrm{Frob} : P(s) \to \mathrm{Gal}(L_s/K_s'')^{\mathrm{gen}}$$

by $p \mapsto \mathrm{Frob}((\sqrt[n]{2}^p - 1), L_s/K_s)$. Note that this map is well-defined by Proposition 5.5.

The following theorem relates the Lehmer symbol to the Frobenius symbol.

**Theorem 5.6.** *Let $s \in K$ be a potential starting value. Then the diagram*

$$\begin{tikzcd}
P(s) \arrow[rr, "\epsilon_s"] \arrow[drr, "\mathrm{Frob}"'] & & \{+1,-1\} \\
& & \mathrm{Gal}(L_s/K_s'')^{\mathrm{gen}}/{\sim} \arrow[u, "\lambda_s"']
\end{tikzcd}$$

*commutes.*

A proof of Theorem 5.6 can be found in the last section of this chapter.

We finish this section with a corollary of Theorem 5.6. First we recall some notation of Chapter 4. The map $r : \mathrm{Gal}(L_s/K_s'')^{\mathrm{gen}}/{\sim} \to \mathrm{Gal}(L_s'/K_s')^{\mathrm{gen}}/{\sim}$ induced by the restriction map $\mathrm{Gal}(L_s/K_s) \to \mathrm{Gal}(L_s'/K_s)$ is bijective. We define the map $\mathrm{Frob}' = r \circ \mathrm{Frob}$ from $P(s)$ to $\mathrm{Gal}(L_s'/K_s')^{\mathrm{gen}}/{\sim}$. Note that the consistency property implies $\mathrm{Frob}'(p) = \mathrm{Frob}((\sqrt[n]{2}^p - 1), L_s'/K_s)$. Recall the map $\lambda_s' : \mathrm{Gal}(L_s'/K_s')^{\mathrm{gen}}/{\sim} \to \{+1, -1\}$ (see Definition 4.6). Now Theorem 5.6 and the definition of $\lambda_s'$ yield the following corollary.

**Corollary 5.7.** *Let $s \in K$ be a potential starting value. Then the diagram*

$$\begin{tikzcd}
P(s) \arrow[rr, "\epsilon_s"] \arrow[drr, "\mathrm{Frob}'"'] & & \{+1,-1\} \\
& & \mathrm{Gal}(L_s'/K_s')^{\mathrm{gen}}/{\sim} \arrow[u, "\lambda_s'"']
\end{tikzcd}$$

*commutes.*

Corollary 5.7 implies that if $p, q \in P(s)$ and $\mathrm{Frob}'(p) = \mathrm{Frob}'(q)$ then $p$ and $q$ have the same Lehmer symbol.

In the next chapter we state well-known properties of the Frobenius symbol. In the case $\mathrm{Gal}(L_s'/K_s)$ is abelian these properties allow us to calculate the Lehmer symbol more efficiently than by direct calculation of $\epsilon_s(p)$.

## Ramification and ramification groups

In this section we introduce decomposition groups and ramification groups. The proposition that we state about these groups will imply Theorem 5.3.

Let $F/E$ be a Galois extension of number fields with Galois group $G$. Let $\mathfrak{M}$ be a non-zero prime ideal of $\mathcal{O}_F$, let $\mathfrak{m} = \mathcal{O}_E \cap \mathfrak{M}$ and let $p \in \mathbb{Z}$ be the prime number below $\mathfrak{M}$, i.e. $(p) = \mathbb{Z} \cap \mathfrak{M}$. We define the decomposition group $G_{\mathfrak{M}}$ of $\mathfrak{M}$ by

$$G_{\mathfrak{M}} = \{\sigma \in G : \sigma(\mathfrak{M}) = \mathfrak{M}\}.$$

Since $\sigma \in G_{\mathfrak{M}}$ leaves $\mathfrak{M}$ fixed and is the identity on $\mathcal{O}_E$, the element $\sigma$ induces an element $\overline{\sigma}$ of $\overline{G}_{\mathfrak{M}} = \mathrm{Gal}((\mathcal{O}_F/\mathfrak{M})/(\mathcal{O}_E/\mathfrak{m}))$. Hence we have a group homomorphism

$$r : G_{\mathfrak{M}} \to \overline{G}_{\mathfrak{M}}.$$

For $n \in \mathbb{Z}_{\geq 0}$ we define the $n$-th ramification group $V_{\mathfrak{M},n}$ of $\mathfrak{M}$ by

$$V_{\mathfrak{M},n} = \{\sigma \in G : \text{for all } x \in \mathcal{O}_F \text{ we have } \sigma(x) \equiv x \bmod \mathfrak{M}^{n+1}\}.$$

Denote the fixed field of $G_{\mathfrak{M}}$ by $D$ and denote the fixed field of $V_{\mathfrak{M},n}$ by $T_n$. Let $L$ be a number field such that $E \subset L \subset F$. In the following proposition we state well-known results about the decomposition group and the ramification groups that we will use in this thesis (see [14, Chapter 1 §7 and §8, Chapter 4]).

**Proposition 5.8.** *We have:*

(i) *the map $r$ is surjective and has kernel $V_{\mathfrak{M},0}$,*
(ii) $\forall \sigma \in G\ \forall n \in \mathbb{Z}_{\geq 0} :\ G_{\sigma(\mathfrak{M})} = \sigma G_{\mathfrak{M}} \sigma^{-1}$ *and* $V_{\sigma(\mathfrak{M}),n} = \sigma V_{\mathfrak{M},n} \sigma^{-1}$,
(iii) $e(\mathcal{O}_L \cap \mathfrak{M}/\mathfrak{m}) = f(\mathcal{O}_L \cap \mathfrak{M}/\mathfrak{m}) = 1$ *if and only if* $L \subset D$,
(iv) $e(\mathcal{O}_L \cap \mathfrak{M}/\mathfrak{m}) = 1$ *if and only if* $L \subset T_0$,
(v) *there is an injective group homomorphism* $V_{\mathfrak{M},0}/V_{\mathfrak{M},1} \to (\mathcal{O}_F/\mathfrak{M})^*$,
(vi) $V_{\mathfrak{M},1} = \{\sigma \in V_{\mathfrak{M},0} :$ *order of $\sigma$ equals $p^n$ for some* $n \in \mathbb{Z}_{\geq 0}\}$.

**Proof of Theorem 5.3.** Let the notation be as in Theorem 5.3. By assumption $\mathfrak{m}$ is unramified in $F$. Now proposition 5.8(iv) implies $T_0 = F$, so $V_0$ is the trivial group. Hence by Proposition 5.8(i) the map $r$ is an isomorphism. We know by the theory of finite fields that there exists a unique element $\overline{\sigma} \in \overline{G}_{\mathfrak{M}}$ defined by $\overline{\sigma} : x \mapsto x^{\#(\mathcal{O}_E/\mathfrak{m})}$ that generates $\overline{G}_{\mathfrak{M}}$. Hence there exists an element $\mathrm{Frob}_{\mathfrak{M}} \in G$ that has the property described in Theorem 5.3. To prove uniqueness we have to show that every $\sigma \in G$ with the property as described in Theorem 5.3 belongs to $G_{\mathfrak{M}}$. Let $\sigma \in G$ be an element with the property described in Theorem 5.3. Suppose $x \in \mathfrak{M}$. Then we have $\sigma(x) \equiv x^{\#(\mathcal{O}_E/\mathfrak{m})} \equiv 0 \bmod \mathfrak{M}$, so $\sigma(\mathfrak{M}) \subset \mathfrak{M}$. Since $\sigma$ has finite order, we see that $\sigma(\mathfrak{M}) = \mathfrak{M}$. Hence we have $\sigma \in G_{\mathfrak{M}}$. Therefore we conclude that the element $\mathrm{Frob}_{\mathfrak{M}}$ is unique. The second part of Theorem 5.3 follows directly from (iii). □

We finish this section with a proposition that controls the ramification in $L_s/K_s$. Let $\mathfrak{d}_s = \{x \in \mathcal{O}_{K_s} : x \cdot s \in \mathcal{O}_{K_s}\}$ be the denominator ideal of $s \in K$.

**Proposition 5.9.** *Let $s \in K$. If a non-zero prime ideal $\mathfrak{m}$ of $\mathcal{O}_{K_s}$ ramifies in $L_s$ then $\mathfrak{m} \mid 2\mathfrak{d}_s$ or $\mathfrak{m}$ ramifies in $K_s(\sqrt{4-s^2})$.*

**Proof of Proposition 5.9**. We recall from the first section of Chapter 4 that $L_s = K_s(\alpha, \zeta_8)$. If a non-zero prime ideal $\mathfrak{m}$ of $\mathcal{O}_{K_s}$ ramifies then it ramifies in $K_s(\alpha^8, \zeta_8)/K_s$ or in $L_s/K_s(\alpha^8, \zeta_8)$.

By definition of $\alpha$ the element $\alpha^8$ is a zero of the polynomial $x^2 - sx + 1$, hence $K_s(\alpha^8, \zeta_8) = K_s(\sqrt{4-s^2}, \zeta_8)$. In the extension $K_s(\zeta_8)/K_s$ only the prime ideal $(\sqrt[n]{2})$ can ramify, hence if $\mathfrak{m}$ ramifies in $K_s(\alpha^8, \zeta_8)/K_s$ then $\mathfrak{m}|2$ or $\mathfrak{m}$ ramifies in $K_s(\sqrt{4-s^2})/K_s$.

Let $d \in \mathfrak{d}_s$. Then $d \cdot s$ is an element of $\mathcal{O}_K$, so $g = x^2 - dsx + d^2 \in \mathcal{O}_K[x]$. Both $d\alpha^8$ and $d\alpha^{-8}$ are zeros of $g$. Hence it follows that $d\alpha^8, d\alpha^{-8} \in \mathcal{O}_K$. Therefore the zero $d\alpha$ of the polynomial $x^8 - (d\alpha)^8$ is an algebraic integer. Hence if $\mathfrak{m}$ ramifies in $L_s/K_s(\alpha^8, \zeta_8)$ then $\mathfrak{m}|8(d\alpha)^8$ (see [7, Chapter II, §2]). Similarly if $\mathfrak{m}$ ramifies in $L_s/K_s(\alpha^8, \zeta_8)$ then $\mathfrak{m}|8(d\alpha^{-1})^8$. Therefore $\mathfrak{m}$ divides $8(d\alpha)^8 \cdot 8(d\alpha^{-1})^8 = 64d^{16}$, so $\mathfrak{m}|2d$. Hence if $\mathfrak{m}$ ramifies in $L_s/K_s(\alpha^8, \zeta_8)$ then $\mathfrak{m}|2\mathfrak{d}_s$. □

# Relating the symbols

In this section we prove Proposition 5.5 (actually we prove a stronger result, namely Proposition 5.10 below) and Theorem 5.6. Let $s \in K$. Recall the definitions of $L_s$, $L'_s$, $K''_s$, $K'_s$ and $K_s$ of Chapter 4.

**Proposition 5.10.** *Let $s \in K$, take $p \in P(s)$ and set $n = [K_s : \mathbb{Q}]$. Define $\mathfrak{m}_p$ to be the ideal $(\sqrt[n]{2}^p - 1)$ of $\mathcal{O}_{K_s}$. Then we have:*

(i) *$s$ is a potential starting value,*
(ii) *$\mathfrak{m}_p$ is a prime ideal of $\mathcal{O}_{K_s}$ of degree one over $\mathbb{Q}$ unramified in $L_s$,*
(iii) *$\mathrm{Frob}_{\mathfrak{M}_p}$ generates the group $\mathrm{Gal}(L_s/K''_s)$,*
(iv) *$\mathrm{Frob}_{\mathfrak{M}'_p}$ generates the group $\mathrm{Gal}(L'_s/K'_s)$,*

*where $\mathfrak{M}_p$ and $\mathfrak{M}'_p$ are prime ideals of $\mathcal{O}_{L_s}$ and $\mathcal{O}_{L'_s}$ above $\mathfrak{m}_p$ respectively.*

**Proof**. (i) The assumption $p \in P(s)$ implies by definition that $s$ is a starting value for $p$ and that $p$ is odd. Hence $s$ is by Theorem 3.2 a potential starting value.

(ii) By Proposition 4.4 the integer $[K_s : \mathbb{Q}(s)]$ equals 1 or 2. Since $p \in P(s)$, we have $\gcd(p, [\mathbb{Q}(s) : \mathbb{Q}]) = 1$ and $p$ is odd. Hence we have $\gcd(p, [K_s : \mathbb{Q}]) = 1$. Since $n$ is even, we see that the absolute norm of $\sqrt[n]{2}^p - 1$ is $(-1)^n \cdot -M_p = -M_p$. Hence $\mathfrak{m}_p$ is a prime of degree one and the fields $\mathcal{O}_{K_s}/\mathfrak{m}_p$ and $\mathbb{Z}/M_p\mathbb{Z}$ are isomorphic. Since $p \in P(s)$, we can write $s = r/t$ with $r \in R_p$ and $t \in S_p$ (see Definition 2.5). By definition of $R_p$ and $S_p$ there is a positive integer $m \in n\mathbb{Z}$ such that $r, t \in \mathbb{Z}[\sqrt[m]{2}]$ and $p \nmid m$. The prime $\mathfrak{M}_p = (\sqrt[m]{2}^p - 1)$ of $\mathcal{O}_{\mathbb{Q}(\sqrt[m]{2})}$ lies above $\mathfrak{m}_p$. Since $t \in S_p$ and $S_p$ is the inverse image of $(\mathbb{Z}/M_p\mathbb{Z})^*$ under the map $\varphi_p : R_p \to \mathbb{Z}/M_p\mathbb{Z}$ (see Chapter 2), the prime $\mathfrak{M}_p$ does not divide the ideal $(t)$

of $\mathcal{O}_{\mathbb{Q}(\sqrt[m]{2})}$. Hence we have $\mathrm{ord}_{\mathfrak{m}_p}(s) \geq 0$, so $4 - s^2$ maps naturally to $\mathcal{O}_{K_s}/\mathfrak{m}_p$ and $\mathfrak{m}_p$ does not divide the denominator ideal $\mathfrak{d}_s$ of $s$.

Since $s$ is a starting value for $p$, it follows that $4 - s^2$ is a nonzero square in $\mathbb{Z}/M_p\mathbb{Z}$. Therefore $4-s^2$ is a nonzero square in $\mathcal{O}_{K_s}/\mathfrak{m}_p$, so $\mathfrak{m}_p$ splits completely in $K_s(\sqrt{4-s^2})$. Now Proposition 5.9 implies (ii).

(iii) From (ii) it follows that $\mathfrak{m}_p$ is unramified in $L_s$. In the proof of (ii) we showed that $\mathrm{ord}_{\mathfrak{m}_p}(s) \geq 0$. Since $s$ is a starting value for $p$, the elements $s - 2$ and $-s - 2$ are nonzero squares in $\mathbb{Z}/M_p\mathbb{Z}$. Hence the natural images of $s - 2$ and $-s - 2$ are nonzero squares in $\mathcal{O}_{K_s}/\mathfrak{m}_p$. From this it follows that $\mathfrak{m}_p$ splits completely in $K_s'' = K_s(\sqrt{s-2}, \sqrt{-s-2})$. The primes above $\mathfrak{m}_p$ in $K_s''$ are inert in the extension $K_s''(\alpha^4 + \alpha^{-4}) = K_s''(\mathrm{i})$ over $K_s''$ since $\left(\frac{-1}{M_p}\right) = -1$. Now Theorem 5.3 implies that $(\mathfrak{m}_p'', K_s''(\mathrm{i})/K_s'')$ generates $\mathrm{Gal}(K_s''(\mathrm{i})/K_s'')$, where $\mathfrak{m}_p''$ is the prime of $K_s''$ below $\mathfrak{M}_p$. By Proposition 4.2 the extension $L_s/K_s''$ is cyclic of order 8. By Proposition 5.4 the element $(\mathfrak{m}_p'', L_s/K_s'')$ generates $\mathrm{Gal}(L_s/K_s'')$. Since $\mathrm{Gal}(L_s/K_s'')$ is abelian and $\mathfrak{M}_p$ lies above $\mathfrak{m}_p''$, the element $(\mathfrak{m}_p'', L_s/K_s'')$ equals $\mathrm{Frob}_{\mathfrak{M}_p}$. This completes the proof of (iii).

(iv) Take $\mathfrak{M}_p$ above $\mathfrak{M}_p'$. By (iii) we know that $(\mathfrak{M}_p, L_s/K_s)$ generates $\mathrm{Gal}(L_s/K_s'')$. Using Proposition 4.2 and Proposition 5.4 for the extension $K_s \subset L_s' \subset L_s$ yields that $(\mathfrak{M}_p', L_s'/K_s)$ generates $\mathrm{Gal}(L_s'/K_s')$. □

**Proof of Proposition 5.5.** Directly from Proposition 5.10(ii) and (iii). □

**Proof of Theorem 5.6.** Let $\mathcal{O}_{L_s}$ be the ring of integers of $L_s$. Since ring morphisms respect inverting, it follows that Theorem 5.3 can also be applied to elements $x$ in the local ring $(\mathcal{O}_{L_s})_{\mathfrak{M}_p}$, where $\mathfrak{M}_p$ is as above.

Let $p \in P(s)$. Then $(s \bmod M_p) \in \mathbb{Z}/M_p\mathbb{Z}$ is defined. Hence $\alpha$, a root of the polynomial $x^{16} - sx^8 + 1$, is an element of $(\mathcal{O}_{L_s})_{\mathfrak{M}_p}$. By Theorem 5.3 we have

$$\mathrm{Frob}_{\mathfrak{M}_p}(\alpha)\alpha + \mathrm{Frob}_{\mathfrak{M}_p}(\alpha^{-1})\alpha^{-1} = \alpha^{M_p+1} + \alpha^{-(M_p+1)} = (\alpha^8)^{2^{p-3}} + (\alpha^{-8})^{2^{p-3}}$$

in the field $\mathcal{O}_{L_s}/\mathfrak{M}_p$. Recall that

$$s_{i+1} = s_i^2 - 2.$$

From $s_1 = s = \alpha^8 + \alpha^{-8}$ we get $s_{p-2} = (\alpha^8)^{2^{p-3}} + (\alpha^{-8})^{2^{p-3}}$. Note $\zeta_8 \in L_s$ implies that $n$ is even. Hence $\sqrt{2} - 2^{(p+1)/2} = \sqrt{2}(1 - \sqrt{2}^p)$ and $\mathfrak{M}_p \mid (1 - \sqrt[n]{2}^p) \mid (1 - \sqrt{2}^p)$ imply

$$(\alpha^8)^{2^{p-3}} + (\alpha^{-8})^{2^{p-3}} = s_{p-2} = \epsilon(s,p)2^{(p+1)/2} = \epsilon(s,p)\sqrt{2}$$

in the field $\mathcal{O}_{L_s}/\mathfrak{M}_p$. This means that the equality

$$(\mathrm{Frob}_{\mathfrak{M}_p}(\alpha)\alpha + \mathrm{Frob}_{\mathfrak{M}_p}(\alpha^{-1})\alpha^{-1})/\sqrt{2} = \epsilon(s,p)$$

holds in the field $\mathcal{O}_{L_s}/\mathfrak{M}_p$. By Proposition 5.10(iii) the element $[\mathrm{Frob}_{\mathfrak{m}_p}]$ is in the domain of $\lambda_s$. Applying Proposition 4.5 we see that

$$\epsilon_s = \lambda_s \circ \mathrm{Frob}.$$

□