ON THE TRACE MAP OF LUBIN-TATE FORMAL GROUPS AND A RESULT OF LANG-TATE

CHUANGXUN CHENG AND CHENG NIU

Abstract. Let p be a prime number, E be an elliptic curve over $\mathbb{Q}_p$ with good supersingular reduction, and C be a principal homogeneous space of $E/\mathbb{Q}_p$ with period p^n. In this paper we give a sufficient condition for extensions $F/\mathbb{Q}_p$ so that $C(F) \neq \emptyset$. In particular, we show that a totally ramified abelian extension $F/\mathbb{Q}_p$ splits C if $[F : \mathbb{Q}_p]$ is sufficiently large. Moreover, in case $n = 1$, we show that a degree p extension $F/\mathbb{Q}_p$ splits C if and only if $v_F(\mathcal{D}_{F/\mathbb{Q}_p}) = 2p - 1$. This is an analogy and also a complement of a result of Lang-Tate on splitting fields of principal homogeneous spaces of abelian varieties.

1. Introduction

Let E/K be an elliptic curve over a field K and $\mathrm{WC}(E/K)$ be the Weil-Châtelet group of E/K. If C/K is a principal homogeneous space of E/K, let $[C] \in \mathrm{WC}(E/K)$ be the corresponding class. The *period* of C is the order of $[C]$ in the group $\mathrm{WC}(E/K)$. The *index* of C is the smallest positive integer d such that there is a K-rational divisor of degree d on C. We denote the period of C by $P(C)$ and the index by $I(C)$. By the Riemann-Roch theorem, the index of C equals the smallest degree of splitting fields of C (cf. [6, Page 670]). Here a field extension L/K is a *splitting field* of C if $C(L) \neq \emptyset$.

It is well known that $P(C)$ divides $I(C)$ and that $P(C)$ and $I(C)$ have the same prime factors (cf. [6, Proposition 5]). In general the exact difference between $P(C)$ and $I(C)$ is still a mystery (cf. [1, 2, 10]). Yet if K is a local field with mixed characteristic, Lichtenbaum [7] (see also [10, Section 5]) showed that $P(C) = I(C)$ for all principal homogeneous spaces of E/K. In this case, a natural question is to characterize the splitting fields of C. As a special case of Lang-Tate [6, Theorem 1, Corollary 1], we have the following result: If E/K has good reduction, $P(C) = m$ and $(m, p) = 1$, where p is the characteristic of the residue field of K, then L is a splitting field of C if and only if m divides the ramification index of L/K. In particular, a degree m extension is a splitting field of C if and only if it is totally ramified.

The proof of Lang-Tate is based on the Néron-Ogg-Shafarevich criterion and the key ingredient is the isomorphism $E[m] \cong \widetilde{E}[m]$, where $\widetilde{E}$ is the special fiber of E. This argument breaks down if $p \mid m$. In this paper, we consider a special case where $m = p^n$ and $E/\mathbb{Q}_p$ has good supersingular reduction. One shall see that the $p \mid m$ situation is more subtle. For a finite extension $F/\mathbb{Q}_p$ with maximal ideal $\mathcal{M}_F$, denoted by $\mathcal{D}_{F/\mathbb{Q}_p}$ the

2010 *Mathematics Subject Classification.* 11G07, 11G20, 11S31.

Key words and phrases. elliptic curve, Lubin-Tate formal group, principal homogeneous space, local Tate duality, splitting field.

The authors are supported by NSFC 11701272 and NSFC 12071221.

difference of the extension $F/\mathbb{Q}_p$ and $v_F(\mathcal{D}_{F/\mathbb{Q}_p})$ the exponent of $\mathcal{M}_F$ in $\mathcal{D}_{F/\mathbb{Q}_p}$. The main result of the paper is as follows.

Theorem 1.1. *Let E be an elliptic curve over $\mathbb{Q}_p$ with good supersingular reduction, $C/\mathbb{Q}_p$ be a principal homogeneous space of $E/\mathbb{Q}_p$, and F be a totally ramified extension of $\mathbb{Q}_p$. The following statements hold.*

(1) *Suppose that $P(C) = p^n$. Let $t \geq n$ be an integer. If $F/\mathbb{Q}_p$ has degree $[F : \mathbb{Q}_p] = p^{2t-1}$ and $v_F(\mathcal{D}_{F/\mathbb{Q}_p}) \geq p^{2t-1}(n+t) - p^{2t-2}$, then F is a splitting field of C; if $F/\mathbb{Q}_p$ has degree $[F : \mathbb{Q}_p] = p^{2t}$ and $v_F(\mathcal{D}_{F/\mathbb{Q}_p}) \geq p^{2t}(n+t)$, then F is a splitting field of C.*

(2) *Suppose that $P(C) = p^n$ and $[F : \mathbb{Q}_p] = p^s$ with $s \geq n$. If F is a splitting field of C, then $v_F(\mathcal{D}_{F/\mathbb{Q}_p}) \geq p^s(n+1) - \lfloor \frac{p^s}{p^2-1} \rfloor - 1$. Here $\lfloor r \rfloor$ is the largest integer that is $\leq r$.*

(3) *Suppose that $P(C) = p$ and $[F : \mathbb{Q}_p] = p$, then F is a splitting field of C if and only if $v_F(\mathcal{D}_{F/\mathbb{Q}_p}) = 2p - 1$.*

(4) *Suppose that $P(C) = p^2$ and $[F : \mathbb{Q}_p] = p^2$, then F is a splitting field of C if and only if $v_F(\mathcal{D}_{F/\mathbb{Q}_p}) = 3p^2 - 2$ and $v_p(\mathrm{Tr}_{L/\mathbb{Q}_{p^2}}(-px + x^{p^2})) \geq 4$ for any uniformizer x of L, where $\mathbb{Q}_{p^2}$ is the unramified quadratic extension of $\mathbb{Q}_p$, v_p is the valuation on $\mathbb{Q}_{p^2}$ with $v_p(p) = 1$, and $L = F\mathbb{Q}_{p^2}$ is the composition of F and $\mathbb{Q}_{p^2}$.*

Notation and conventions. In the following, K denotes a finite extension of $\mathbb{Q}_p$ and $G_K = \mathrm{Gal}(\bar{K}/K)$ denotes the absolute Galois group of K. Let $\mathcal{O}_K$ be the integer ring of K, $\mathcal{M}_K$ the maximal ideal of $\mathcal{O}_K$, k the residue field of $\mathcal{O}_K$, and v_K the normalized valuation on K such that $v_K(K^*) = \mathbb{Z}$. Let $e_K = v_K(p)$ be the ramification index of K. For a field extension L/K, let $\mathcal{O}_L$, $\mathcal{M}_L$, l, v_L, e_L be the corresponding objects associated with L. Denoted by $\mathcal{D}_{L/K}$ the difference of the extension L/K and $v_L(\mathcal{D}_{L/K})$ the exponent of $\mathcal{M}_L$ in $\mathcal{D}_{L/K}$. Denoted by $e_{L/K}$ the ramification index of L/K.

All formal groups in this paper are one-dimensional. We refer to [14, Chap. 4] for notions and basic properties of dimension one formal groups.

For $r \in \mathbb{R}$, denoted by $\lfloor r \rfloor$ the largest integer that is $\leq r$.

Outline of the proof. We explain the strategy of the proof. Let E/K be an elliptic curve and C/K a principal homogeneous space of E/K with period m. By the canonical isomorphism $\mathrm{WC}(E/K) \cong H^1(G_K, E(\bar{K}))$, C corresponds to an element in $H^1(G_K, E(\bar{K}))$ with order m and we denote it by $[C]$. Via the local Tate duality (cf. [9, Chap. 1, Section 3] and [11]), $[C]$ corresponds to an element $f_C \in \mathrm{Hom}(E(K), \mathbb{Q}/\mathbb{Z})$ with image $\frac{1}{m}\mathbb{Z}/\mathbb{Z}$. The local Tate duality also gives us a commutative diagram

$$\begin{array}{ccc} H^1(G_K, E) & \xrightarrow{\cong} & \mathrm{Hom}(E(K), \mathbb{Q}/\mathbb{Z}) \\ {\scriptstyle \mathrm{Res}_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{Tr}^*_{L/K}} \\ H^1(G_L, E) & \xrightarrow{\cong} & \mathrm{Hom}(E(L), \mathbb{Q}/\mathbb{Z}). \end{array}$$

Here $\mathrm{Tr}^*_{L/K}$ is the dual of the natural trace map $\mathrm{Tr}_{L/K} : E(L) \to E(K)$. The following conditions are equivalent.

(1) L is a splitting field of C/K.

(2) $[C]$ is in the kernel of $\mathrm{Res}_{L/K} : H^1(G_K, E) \to H^1(G_L, E)$.

(3) f_C is in the kernel of $\mathrm{Tr}^*_{L/K} : \mathrm{Hom}(E(K), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(E(L), \mathbb{Q}/\mathbb{Z})$.

Assume that E/K has good reduction and denoted by $\widetilde{E}/k$ the special fiber. Let $\widehat{E}/\mathcal{O}_K$ be the formal group associated with E. We have a short exact sequence (cf. [14, Chap. 7])

$$0 \to \widehat{E}(\mathcal{M}_K) \to E(K) \to \widetilde{E}(k) \to 0.$$

Assume that $m = p^n$ and E has good supersingular reduction, then $\widetilde{E}[p^n]$ is trivial and for any L/K

$$\mathrm{Hom}(E(L), \mathbb{Q}/\mathbb{Z})[p^n] \cong \mathrm{Hom}(\widehat{E}(\mathcal{M}_L), \mathbb{Q}/\mathbb{Z})[p^n].$$

Therefore L is a splitting field of C/K if and only if the restriction $f_C|_{\widehat{E}(\mathcal{M}_K)}$ is in the kernel of

$$\widehat{\mathrm{Tr}}^*_{L/K} : \mathrm{Hom}(\widehat{E}(\mathcal{M}_K), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\widehat{E}(\mathcal{M}_L), \mathbb{Q}/\mathbb{Z}).$$

Here $\widehat{\mathrm{Tr}}^*_{L/K}$ is the dual of the trace map $\widehat{\mathrm{Tr}}_{L/K} : \widehat{E}(\mathcal{M}_L) \to \widehat{E}(\mathcal{M}_K)$.

Finally, assume further that $K = \mathbb{Q}_p$, then after base change to the integer ring $\mathbb{Z}_{p^2}$ of the unramified quadratic extension $\mathbb{Q}_{p^2}$ of $\mathbb{Q}_p$, $\widehat{E}$ is isomorphic to the Lubin-Tate formal group (cf. [4, Proposition 8.6]). Then one could prove the theorem by computing the trace map $\widehat{\mathrm{Tr}}_{L/K}$.

2. The trace map of the Lubin-Tate formal groups

Let $\mathcal{F}$ be a formal group over K. Let $\log_{\mathcal{F}}$ and $\exp_{\mathcal{F}}$ be the associated formal logarithm and formal exponential. The following result is well known (cf. [14, Theorem 6.4]).

Lemma 2.1. *With the notation as above, the following properties hold.*

(1) *The formal logarithm induces a homomorphism*

$$\log_{\mathcal{F}} : \mathcal{F}(\mathcal{M}_K) \to K,$$

where the group law on K is additive.

(2) *Let $r > e_K/(p-1)$ be an integer. The formal logarithm induces an isomorphism*

$$\log_{\mathcal{F}} : \mathcal{F}(\mathcal{M}_K^r) \to \widehat{\mathbb{G}}_a(\mathcal{M}_K^r).$$

Here $\widehat{\mathbb{G}}_a$ is the additive group. The inverse is given by the formal exponential $\exp_{\mathcal{F}}$.

(3) *Let L/K be a finite extension. The following diagram is commutative*

$$\begin{array}{ccc} \mathcal{F}(\mathcal{M}_L) & \xrightarrow{\log_{\mathcal{F}}} & L \\ {\scriptstyle \widehat{\mathrm{Tr}}_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{Tr}_{L/K}} \\ \mathcal{F}(\mathcal{M}_K) & \xrightarrow{\log_{\mathcal{F}}} & K. \end{array}$$

As we shall use it repeatedly, we recall the following result on the usual trace map of extensions of local fields (cf. [12, Chap. 5, Lemma 4]).

Lemma 2.2. *Let L/K be a finite extension with ramification index $e_{L/K}$, $\mathrm{Tr}_{L/K} : L \to K$ be the trace map, $a \in \mathbb{Z}_{\geq 0}$. We have*

$$\mathrm{Tr}_{L/K}(\mathcal{M}_L^a) = \mathcal{M}_K^{\lfloor \frac{a + v_L(\mathcal{D}_{L/K})}{e_{L/K}} \rfloor}.$$

In particular, if L/K is unramified, then $\mathrm{Tr}_{L/K}(\mathcal{M}_L^a) = \mathcal{M}_K^a$.

Lemma 2.3. *Let L/K be an unramified extension. The trace map $\widehat{\mathrm{Tr}}_{L/K} : \mathcal{F}(\mathcal{M}_L) \to \mathcal{F}(\mathcal{M}_K)$ induces a surjection $\widehat{\mathrm{Tr}}_{L/K} : \mathcal{F}(\mathcal{M}_L^a) \to \mathcal{F}(\mathcal{M}_K^a)$ for $a \in \mathbb{Z}_{\geq 1}$.*

Proof. As L/K is unramified, by checking the valuation of $\widehat{\mathrm{Tr}}_{L/K}(x)$ one sees that $\widehat{\mathrm{Tr}}_{L/K}$ sends $\mathcal{F}(\mathcal{M}_L^a)$ into $\mathcal{F}(\mathcal{M}_K^a)$. If $a > e_K/(p-1)$, the claim follows from Lemma 2.1(2)(3) and Lemma 2.2. Now consider the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{F}(\mathcal{M}_L^a) & \longrightarrow & \mathcal{F}(\mathcal{M}_L^{a-1}) & \longrightarrow & \mathcal{F}(\mathcal{M}_L^{a-1}/\mathcal{M}_L^a) \cong \mathcal{M}_L^{a-1}/\mathcal{M}_L^a \cong l & \longrightarrow & 0 \\ & & \downarrow \widehat{\mathrm{Tr}}_{L/K} & & \downarrow \widehat{\mathrm{Tr}}_{L/K} & & \downarrow \mathrm{Tr}_{l/k} & & \\ 0 & \longrightarrow & \mathcal{F}(\mathcal{M}_K^a) & \longrightarrow & \mathcal{F}(\mathcal{M}_K^{a-1}) & \longrightarrow & \mathcal{F}(\mathcal{M}_K^{a-1}/\mathcal{M}_K^a) \cong \mathcal{M}_K^{a-1}/\mathcal{M}_K^a \cong k & \longrightarrow & 0, \end{array}$$

and note that $\mathrm{Tr}_{l/k} : l \to k$ is surjective, if the claim holds for a, then it holds for $a-1$. The lemma then follows by induction. □

Fix a uniformizer π_K of K and denoted by q the cardinality of k. Let $\mathcal{F} = \mathrm{LT}_{\mathcal{O}_K}$ be the Lubin-Tate formal group over $\mathcal{O}_K$. Let $[\cdot] : \mathcal{O}_K \to \mathrm{End}(\mathcal{F})$ be the $\mathcal{O}_K$-module structure on $\mathcal{F}$. With out loss of generality, we may assume that $[\pi_K](T) = \pi_K T + T^q$. We refer to [13] for basic properties of Lubin-Tate formal groups.

Lemma 2.4. *Let $\mathcal{F}$ be the Lubin-Tate formal group as above. The following statements hold.*

1. $\log_{\mathcal{F}}(T) = \lim_{n\to\infty} \frac{[\pi_K^n](T)}{\pi_K^n}$.
2. *Let L be a finite extension of K. The trace map $\widehat{\mathrm{Tr}}_{L/K} : \mathcal{F}(\mathcal{M}_L) \to \mathcal{F}(\mathcal{M}_K)$ is $\mathcal{O}_K$-equivariant, i.e.*
$$\widehat{\mathrm{Tr}}_{L/K}([a]x) = [a]\widehat{\mathrm{Tr}}_{L/K}(x), \text{ for all } a \in \mathcal{O}_K,\ x \in \mathcal{M}_L.$$
3. *The formal logarithm is $\mathcal{O}_K$-equivariant, i.e. $\log_{\mathcal{F}}([a](T)) = a \cdot \log_{\mathcal{F}}(T)$ for any $a \in \mathcal{O}_K$.*
4. *If $q \geq 3$, then $\log_{\mathcal{F}} : \mathcal{F}(\mathcal{M}_K) \to K$ induces an isomorphism $\log_{\mathcal{F}} : \mathcal{F}(\mathcal{M}_K^a) \cong \widehat{\mathbb{G}}_a(\mathcal{M}_K^a)$ for any $a \in \mathbb{Z}_{\geq 1}$.*

Proof. Statement (1) is just [3, Lemma 1]. Statement (2) follows from the commutativity of the Galois action and the $\mathcal{O}_K$-action.

Statement (3) follows from Lubin's comments in [16] and we restate it here. Let $\mathrm{Prelog}_{\mathcal{F}}$ be the set of power series $g(T) \in K[[T]]$ such that $g(\mathcal{F}(x,y)) = g(x) + g(y)$. If $g \in \mathrm{Prelog}_{\mathcal{F}}$, then $\lambda g \in \mathrm{Prelog}_{\mathcal{F}}$ for any $\lambda \in K$.

If $0 \neq g \in \mathrm{Prelog}_{\mathcal{F}}$ and the first nonzero term of g is aT^m, then by definition $a(x+y)^m \equiv ax^m + ay^m$ modulo terms with degree $\geq (m+1)$. Hence we must have $m = 1$. Therefore if there exists a nonzero element in $\mathrm{Prelog}_{\mathcal{F}}$, the map $\mathrm{Prelog}_{\mathcal{F}} \to K$ ($g \mapsto g'(0)$) is an isomorphism. To prove statement (2), it then suffices to check that $\log_{\mathcal{F}}([a](T))$ and $a \cdot \log_{\mathcal{F}}(T)$ have the same derivative at 0, which is obviously true.

For statement (4), as $q \geq 3$, one has $v_K(\frac{[\pi_K](x)}{\pi_K}) = v_K(x)$ for any $x \in \mathcal{M}_K$. By induction, we have $v_K(\frac{[\pi_K^n](x)}{\pi_K^n}) = v_K(x)$ for any $x \in \mathcal{M}_K$. Therefore, by statement (1), $v_K(\log_{\mathcal{F}}(x)) = v_K(x)$ and $\log_{\mathcal{F}}$ is injective. Moreover, as $\log_{\mathcal{F}}$ is $\mathcal{O}_K$-equivariant, $\log_{\mathcal{F}}(\mathcal{M}_K^a) = \mathcal{M}_K^b$ for some $b \in \mathbb{Z}$. Then b must be a by $v_K(\log_{\mathcal{F}}(x)) = v_K(x)$ and the claim holds. □

Lemma 2.5. *Let L/K be a finite extension with ramification index $e_{L/K}$. If $r > \frac{e_{L/K}}{q-1}$, then $[\pi_K]\mathcal{F}(\mathcal{M}_L^r) = \mathcal{F}(\mathcal{M}_L^{r+e_{L/K}})$.*

Proof. It suffices to show that for any $y \in \mathcal{M}_L^{r+e_{L/K}}$, there exists at least one $x \in \mathcal{M}_L^r$ such that $\pi_K x + x^q = y$.

Let π_L be a uniformizer of L and $\pi_K = \pi_L^{e_{L/K}} u$, where $u \in \mathcal{O}_L^\times$ is a unit. Write $y = \pi_L^{r+e_{L/K}} v$, we need to show that there exists $x = \pi_L^r X$ such that

$$\pi_L^{r+e_{L/K}} uX + \pi_L^{rq} \cdot X^q = \pi_L^{r+e_{L/K}} v.$$

Equivalently, we need to solve the equation

$$uX + \pi_L^{rq-(r+e_{L/K})} X^q = v. \tag{2.1}$$

Modulo π_L, the equation $\bar{u}X = \bar{v}$ has a solution in $\mathcal{O}_L/\pi_L\mathcal{O}_L$. By Hensel's lemma, equation (2.1) has a solution in $\mathcal{O}_L$ and the lemma follows. □

Proposition 2.6. *Let $\mathcal{F}$ be the Lubin-Tate formal group over $\mathcal{O}_K$ and L/K be a finite extension with ramification index $e_{L/K}$. Let $\mathrm{Tr} := \mathrm{Tr}_{L/K} : L \to K$ be the trace map, $\widehat{\mathrm{Tr}} := \widehat{\mathrm{Tr}}_{L/K} : \mathcal{F}(\mathcal{M}_L) \to \mathcal{F}(\mathcal{M}_K)$ be the trace map with respect to the Lubin-Tate formal group law. Then the diagram*

$$\begin{array}{ccc} \mathcal{F}(\mathcal{M}_L) & \xrightarrow{\log_{\mathcal{F}}} & L \\ \widehat{\mathrm{Tr}}\Big\downarrow & & \Big\downarrow \mathrm{Tr} \\ \mathcal{F}(\mathcal{M}_K) & \xrightarrow{\log_{\mathcal{F}}} & K \end{array} \tag{2.2}$$

is commutative and $\mathcal{O}_K$-equivariant. Moreover,

(1) *if $r > \frac{e_{L/K}}{q-1}$ is an integer, then $\log_{\mathcal{F}} \circ \widehat{\mathrm{Tr}}(\mathcal{F}(\mathcal{M}_L^r)) = \mathcal{M}_K^{\lfloor \frac{r+v_L(\mathcal{D}_{L/K})}{e_{L/K}} \rfloor}$;*
(2) *if $r < \frac{e_{L/K}}{q-1}$ is a positive integer, then $\log_{\mathcal{F}} \circ \widehat{\mathrm{Tr}}(\mathcal{F}(\mathcal{M}_L^r)) \subset \mathcal{M}_K^{\lfloor \frac{rq^a+v_L(\mathcal{D}_{L/K})}{e_{L/K}} \rfloor - a}$, where a is the smallest integer which satisfies $rq^a > \frac{e_{L/K}}{q-1}$;*
(3) *if $r = \frac{e_{L/K}}{q-1} \geq 2$ is an integer, then*

$$\mathcal{M}_K^{\lfloor \frac{r+1+v_L(\mathcal{D}_{L/K})}{e_{L/K}} \rfloor} \subset \log_{\mathcal{F}} \circ \widehat{\mathrm{Tr}}(\mathcal{F}(\mathcal{M}_L^r)) \subset \mathcal{M}_K^{\lfloor \frac{r-q+v_L(\mathcal{D}_{L/K})}{e_{L/K}} \rfloor}.$$

Proof. The commutativity of the diagram follows from Lemma 2.1 and the $\mathcal{O}_K$-equivariance follows from Lemma 2.4.

If $r > \frac{e_{L/K}}{q-1}$, we choose an integer n such that $r + ne_{L/K} > \frac{e_L}{p-1}$. Then

$$\log_{\mathcal{F}} \circ \widehat{\mathrm{Tr}}([\pi_K^n]\mathcal{F}(\mathcal{M}_L^r)) = \log_{\mathcal{F}}([\pi_K^n]\widehat{\mathrm{Tr}}(\mathcal{F}(\mathcal{M}_L^r))) = \pi_K^n(\log_{\mathcal{F}} \circ \widehat{\mathrm{Tr}}\mathcal{F}(\mathcal{M}_L^r)).$$

On the other hand, we have

$$
\begin{aligned}
\mathrm{Tr}\circ\log_{\mathcal{F}}([\pi_K^n]\mathcal{F}(\mathcal{M}_L^r)) &= \mathrm{Tr}\circ\log_{\mathcal{F}}(\mathcal{F}(\mathcal{M}_L^{r+ne_{L/K}})) \qquad \text{(by Lemma 2.5)}\\
&= \mathrm{Tr}(\mathcal{M}_L^{r+ne_{L/K}}) \qquad \text{(by Lemma 2.1(2))}\\
&= \mathcal{M}_K^{\lfloor\frac{r+ne_{L/K}+v_L(\mathcal{D}_{L/K})}{e_{L/K}}\rfloor} \qquad \text{(by Lemma 2.2)}\\
&= \mathcal{M}_K^{\lfloor\frac{r+v_L(\mathcal{D}_{L/K})}{e_{L/K}}\rfloor+n}.
\end{aligned}
\tag{2.3}
$$

Therefore, $\log_{\mathcal{F}}\circ\widehat{\mathrm{Tr}}(\mathcal{F}(\mathcal{M}_L^r)) = \mathcal{M}_K^{\lfloor\frac{r+v_L(\mathcal{D}_{L/K})}{e_{L/K}}\rfloor}$.

If $r < \frac{e_{L/K}}{q-1}$, then for any $x\in\mathcal{M}_L^r$, $v_L([\pi_K](x)) = v_L(\pi_K x + x^q) = qv_L(x)$. Thus $[\pi_K]\mathcal{F}(\mathcal{M}^r)\subset\mathcal{F}(\mathcal{M}^{qr})$. Let a be the smallest integer which satisfies $rq^a > \frac{e_{L/K}}{q-1}$, then we have

$$\mathrm{Tr}\circ\log_{\mathcal{F}}([\pi_K^a]\mathcal{F}(\mathcal{M}_L^r))\subset\mathrm{Tr}\circ\log_{\mathcal{F}}(\mathcal{F}(\mathcal{M}_L^{rq^a})).$$

By statement (1), $\mathrm{Tr}\circ\log_{\mathcal{F}}(\mathcal{F}(\mathcal{M}_L^{rq^a})) = \mathcal{M}_K^{\lfloor\frac{rq^a+v_L(\mathcal{D}_{L/K})}{e_{L/K}}\rfloor}$. Since $\log_{\mathcal{F}}\circ\widehat{\mathrm{Tr}}([\pi_K^a]\mathcal{F}(\mathcal{M}_L^r)) = \pi_K^a(\log_{\mathcal{F}}\circ\widehat{\mathrm{Tr}}\mathcal{F}((\mathcal{M}_L^r)))$, we obtain

$$\log_{\mathcal{F}}\circ\widehat{\mathrm{Tr}}(\mathcal{F}(\mathcal{M}_L^r))\subset\mathcal{M}_K^{\lfloor\frac{rq^a+v_L(\mathcal{D}_{L/K})}{e_{L/K}}\rfloor-a}.$$

If $r = \frac{e_{L/K}}{q-1}\geq 2$ is an integer, applying statement (1) to $\mathcal{M}_L^{r+1}$ and statement (2) to $\mathcal{M}_L^{r-1}$, statement (3) follows from

$$\log_{\mathcal{F}}\circ\widehat{\mathrm{Tr}}(\mathcal{F}(\mathcal{M}_L^{r+1}))\subset\log_{\mathcal{F}}\circ\widehat{\mathrm{Tr}}(\mathcal{F}(\mathcal{M}_L^r))\subset\log_{\mathcal{F}}\circ\widehat{\mathrm{Tr}}(\mathcal{F}(\mathcal{M}_L^{r-1})).$$

□

3. The trace map of elliptic curves over local fields

3.1. **Basic properties of the trace map: good reduction case.** Let E/K be an elliptic curve with good reduction. Let $\widetilde{E}/k$ be the special fiber and $\widehat{E}/\mathcal{O}_K$ be the formal group attached to E. Let L/K be a finite extension and $\mathrm{Tr}_{L/K}: E(L)\to E(K)$ be the trace map. Let $\widehat{\mathrm{Tr}}_{L/K}:\widehat{E}(\mathcal{M}_L)\to\widehat{E}(\mathcal{M}_K)$ be the trace map on the formal part and $\widetilde{\mathrm{Tr}}_{l/k}:\widetilde{E}(l)\to\widetilde{E}(k)$ be the trace map on the special fiber. The following result is clear.

Lemma 3.1. *With the notation as above and denoted by $e_{L/K}$ the ramification index of L/K, then the diagram*

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \widehat{E}(\mathcal{M}_L) & \longrightarrow & E(L) & \longrightarrow & \widetilde{E}(l) & \longrightarrow & 0\\
 & & \downarrow{\scriptstyle\widehat{\mathrm{Tr}}_{L/K}} & & \downarrow{\scriptstyle\mathrm{Tr}_{L/K}} & & \downarrow{\scriptstyle e_{L/K}\widetilde{\mathrm{Tr}}_{l/k}} & & \\
0 & \longrightarrow & \widehat{E}(\mathcal{M}_K) & \longrightarrow & E(K) & \longrightarrow & \widetilde{E}(k) & \longrightarrow & 0
\end{array}
\tag{3.1}
$$

is commutative.

If l/k is a finite extension of finite fields, A is an abelian variety over k, then by a result of Lang [5], the trace map $\widetilde{\mathrm{Tr}}_{l/k} : A(l) \to A(k)$ is always surjective. We then obtain the following result.

Lemma 3.2. *If L/K is unramified, then $\mathrm{Tr}_{L/K} : E(L) \to E(K)$ is surjective.*

Proof. If L/K is unramified, in diagram (3.1), the map $\widehat{\mathrm{Tr}}_{L/K}$ is surjective by Lemma 2.3, the map $e_{L/K}\widetilde{\mathrm{Tr}}_{l/k} = \widetilde{\mathrm{Tr}}_{l/k}$ is surjective by the result of Lang [5], the lemma then follows. □

Combining Lemma 3.2 and the local Tate duality, we obtain the following result.

Corollary 3.3. *If L/K is unramified, then the restriction map $\mathrm{Res}_{L/K} : \mathrm{WC}(E/K) \to \mathrm{WC}(E/L)$ is injective.*

Remark 3.4.
(1) By the virtue of Corollary 3.3, while discussing splitting fields of a principal homogeneous space, we may restrict to totally ramified extensions.
(2) Let C/K be a principal homogeneous space with period m and $(p, m) = 1$. Then the associated morphism $f_C : E(K) \to \mathbb{Q}/\mathbb{Z}$ corresponds to a surjection $f_C : E(K)/mE(K) \to \frac{1}{m}\mathbb{Z}/\mathbb{Z}$. Note that $\widehat{E}$ has no m-torsion and $E[m](L) \cong \widetilde{E}[m](l)$ for all L/K, then L/K is a splitting field of C/K if and only if
$$f_C \circ e_{L/K}\widetilde{\mathrm{Tr}}_{l/k} : E(l)/mE(l) \to E(k)/mE(k) \to \frac{1}{m}\mathbb{Z}/\mathbb{Z}$$
is trivial, i.e. if and only if $m | e_{L/K}$. This is the translation of Lang-Tate's argument in terms of trace map via the local Tate duality.

3.2. **Proof of Theorem 1.1.** In the following, $E/\mathbb{Q}_p$ is an elliptic curve with good supersingular reduction.

Lemma 3.5. *Let E be an elliptic curve defined over $\mathbb{Q}_p$ with good supersingular reduction. Then over the integer ring of the unramified quadratic extension of $\mathbb{Q}_p$, the formal group $\widehat{E}$ is isomorphic to the Lubin-Tate formal group $\mathcal{F}$ with parameter $-p$.*

Proof. This is [4, Proposition 8.6]. □

Let $C/\mathbb{Q}_p$ be a homogeneous space of $E/\mathbb{Q}_p$ with $P(C) = p^n$. By the local Tate duality, C corresponds to a homomorphism $f_C : E(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z}$ with $\mathrm{ord}(f) = p^n$. Restricted to the subgroup $\widehat{E}(p\mathbb{Z}_p)$, we get a homomorphism $\widehat{f}_C : \widehat{E}(p\mathbb{Z}_p) \to \mathbb{Q}/\mathbb{Z}$.

Lemma 3.6. *With the notation as above, $\mathrm{ord}(\widehat{f}_C) = \mathrm{ord}(f_C) = p^n$ and $F/\mathbb{Q}_p$ is a splitting field of C if and only if $\widehat{f}_C \circ \widehat{\mathrm{Tr}}_{F/\mathbb{Q}_p} = 0$.*

Proof. As $\widetilde{E}$ is supersingular, it has no p^n-torsion and $p^n : \widetilde{E}(k) \to \widetilde{E}(k)$ is an isomorphism. Then we have an isomorphism $\widehat{E}(p\mathbb{Z}_p)/p^n\widehat{E}(p\mathbb{Z}_p) \cong E(\mathbb{Q}_p)/p^nE(\mathbb{Q}_p)$, and the lemma is clear. □

We say that F is a *splitting field* of a morphism $\widehat{f} : \widehat{E}(p\mathbb{Z}_p) \to \mathbb{Q}/\mathbb{Z}$ if $\widehat{f} \circ \widehat{\mathrm{Tr}}_{F/\mathbb{Q}_p} = 0$. By Lemma 3.6, if $\widehat{f} = \widehat{f}_C$, this is equivalent to the fact that F is a splitting field of C.

Let K be the unramified quadratic extension of $\mathbb{Q}_p$, $\mathcal{F}$ be the Lubin-Tate formal group over $\mathcal{O}_K$ with parameter $\pi_K = -p$, F be a totally ramified extension of $\mathbb{Q}_p$, and $L = KF$

be the composition of K and F. By Lemma 3.5, we have an isomorphism of formal groups $\widehat{E}\times\mathcal{O}_K\cong\mathcal{F}$. The diagram

$$\begin{array}{ccccc} & & \mathcal{F}(\mathcal{M}_L)\cong\widehat{E}(\mathcal{M}_L) & & \\ & \swarrow^{\widehat{\mathrm{Tr}}_{L/K}} & & \searrow^{\widehat{\mathrm{Tr}}_{L/F}} & \\ \mathcal{F}(\mathcal{M}_K)\cong\widehat{E}(\mathcal{M}_K) & & & & \widehat{E}(\mathcal{M}_F) \\ & \searrow_{\widehat{\mathrm{Tr}}_{K/\mathbb{Q}_p}} & & \swarrow_{\widehat{\mathrm{Tr}}_{F/\mathbb{Q}_p}} & \\ & & \widehat{E}(p\mathbb{Z}_p) & & \end{array} \tag{3.2}$$

is commutative.

Lemma 3.7. *With the notation as above,* $\log_{\widehat{E}}$ *induces an isomorphism between* $\widehat{E}(p\mathbb{Z}_p)$ *and* $p\mathbb{Z}_p$.

Proof. If $p\geq 3$, this follows from Lemma 2.1(2). Assume that $p=2$. Since $\widehat{\mathrm{Tr}}_{K/\mathbb{Q}_p}(\widehat{E}(\mathcal{M}_K))=\widehat{E}(p\mathbb{Z}_p)$ by Lemma 2.3, $\log_{\widehat{E}}(\widehat{E}(\mathcal{M}_K))=\log_{\mathcal{F}}(\mathcal{F}(\mathcal{M}_K))=\mathcal{M}_K$ by Lemma 2.4(4), we have

$$\begin{aligned}\log_{\widehat{E}}(\widehat{E}(p\mathbb{Z}_p))&=\log_{\widehat{E}}\circ\widehat{\mathrm{Tr}}_{K/\mathbb{Q}_p}(\widehat{E}(\mathcal{M}_K))\\ &=\mathrm{Tr}_{K/\mathbb{Q}_p}\circ\log_{\widehat{E}}(\widehat{E}(\mathcal{M}_K))=\mathrm{Tr}_{K/\mathbb{Q}_p}(\mathcal{M}_K)=p\mathbb{Z}_p.\end{aligned}$$

The map $\log_{\widehat{E}}:\widehat{E}(p\mathbb{Z}_p)\to p\mathbb{Z}_p$ is surjective. Consider the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \widehat{E}(p^2\mathbb{Z}_p) & \longrightarrow & \widehat{E}(p\mathbb{Z}_p) & \longrightarrow & \widehat{E}(p\mathbb{Z}_p)/\widehat{E}(p^2\mathbb{Z}_p)\cong\mathbb{F}_p & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\log_{\widehat{E}}} & & \downarrow{\scriptstyle\log_{\widehat{E}}} & & \downarrow{\scriptstyle\widetilde{\log}_{\widehat{E}}} & & \\ 0 & \longrightarrow & p^2\mathbb{Z}_p & \longrightarrow & p\mathbb{Z}_p & \longrightarrow & p\mathbb{Z}_p/p^2\mathbb{Z}_p\cong\mathbb{F}_p & \longrightarrow & 0, \end{array}$$

the first vertical arrow is an isomorphism by Lemma 2.1(2), so the third vertical arrow $\widetilde{\log}_{\widehat{E}}$ is surjective, hence it is also an isomorphism. Therefore the middle vertical arrow is an isomorphism and the lemma follows. □

Remark 3.8. Let p be a prime number and $E/\mathbb{Q}$ be an elliptic curve with good supersingular reduction at p. Then $E(\mathbb{Q})[p]$ is trivial by Lemma 3.7. The nontrivial part of this statement is the $p=2$ case as in Lemma 3.7. One could also prove this (for $p=2$) via direct computation using formulas in [14, Appendix A].

Proposition 3.9. *With the notation as above, if* $\widehat{f}:\widehat{E}(p\mathbb{Z}_p)\to\mathbb{Q}/\mathbb{Z}$ *has* $\mathrm{ord}(\widehat{f})=p^n$, *then* F *is a splitting field of* $\widehat{f}$ *if and only if* $\log_{\mathcal{F}}\circ\widehat{\mathrm{Tr}}_{L/K}(\mathcal{F}(\mathcal{M}_L))\subset\mathcal{M}_K^{n+1}$.

Proof. By Lemma 3.7, $\log_{\widehat{E}}:\widehat{E}(p\mathbb{Z}_p)\to\widehat{\mathbb{G}}_a(p\mathbb{Z}_p)$ is an isomorphism. Note that a homomorphism $f:p\mathbb{Z}_p\to\mathbb{Q}/\mathbb{Z}$ has order p^n if and only if $\mathrm{Ker}\,f=p^{1+n}\mathbb{Z}_p$. Hence $\mathrm{ord}(\widehat{f})=p^n$ if and only if $\mathrm{Ker}(\widehat{f})=\exp_{\widehat{E}}(p^{1+n}\mathbb{Z}_p)=\widehat{E}(p^{n+1}\mathbb{Z}_p)$.

Since L/F is unramified, by Lemma 2.3, $\widehat{\mathrm{Tr}}_{L/F}:\widehat{E}(\mathcal{M}_L)\to\widehat{E}(\mathcal{M}_F)$ is surjective. Hence

$$\widehat{\mathrm{Tr}}_{L/\mathbb{Q}_p}(\widehat{E}(\mathcal{M}_L))=\widehat{\mathrm{Tr}}_{F/\mathbb{Q}_p}\circ\widehat{\mathrm{Tr}}_{L/F}(\widehat{E}(\mathcal{M}_L))=\widehat{\mathrm{Tr}}_{F/\mathbb{Q}_p}(\widehat{E}(\mathcal{M}_F)).$$

On the other hand, we have the following commutative diagram:

$$\begin{array}{ccc} \mathcal{F}(\mathcal{M}_L) \cong \widehat{E}(\mathcal{M}_L) & \xrightarrow{\log_{\mathcal{F}}=\log_{\widehat{E}}} & L \\ \widehat{\mathrm{Tr}}_{L/K}\downarrow & & \downarrow \mathrm{Tr}_{L/K} \\ \mathcal{F}(\mathcal{M}_K) \cong \widehat{E}(\mathcal{M}_K) & \xrightarrow{\log_{\mathcal{F}}=\log_{\widehat{E}}} & K \\ \widehat{\mathrm{Tr}}_{K/\mathbb{Q}_p}\downarrow & & \downarrow \mathrm{Tr}_{K/\mathbb{Q}_p} \\ \widehat{E}(p\mathbb{Z}_p) & \xrightarrow{\log_{\widehat{E}}} & \mathbb{Q}_p. \end{array} \tag{3.3}$$

By Lemma 2.4, $\mathrm{Tr}_{L/K} \circ \log_{\mathcal{F}}(\mathcal{F}(\mathcal{M}_L))$ is an $\mathcal{O}_K$-submodule of $\mathcal{M}_K$ and assume that it is $\mathcal{M}_K^a$ for some positive integer a. Since $K/\mathbb{Q}_p$ is unramified, $\mathrm{Tr}_{K/\mathbb{Q}_p}(\mathcal{M}_K^a) = (p\mathbb{Z}_p)^a$. Therefor, for a morphism $\widehat{f} : \widehat{E}(p\mathbb{Z}_p) \to \mathbb{Q}/\mathbb{Z}$ with $\mathrm{ord}(\widehat{f}) = p^n$, we have the following equivalences

$$\begin{aligned} F \text{ splits } \widehat{f} &\iff \widehat{\mathrm{Tr}}_{F/\mathbb{Q}_p}(\widehat{E}(\mathcal{M}_F)) \subset \widehat{E}((p\mathbb{Z}_p)^{1+n}) \\ &\iff \widehat{\mathrm{Tr}}_{L/\mathbb{Q}_p}(\widehat{E}(\mathcal{M}_L)) \subset \widehat{E}((p\mathbb{Z}_p)^{1+n}) \\ &\iff \log_{\widehat{E}} \circ \widehat{\mathrm{Tr}}_{L/\mathbb{Q}_p}(\widehat{E}(\mathcal{M}_L)) \subset (p\mathbb{Z}_p)^{1+n} \\ &\iff \log_{\widehat{E}} \circ \widehat{\mathrm{Tr}}_{L/K}(\widehat{E}(\mathcal{M}_L)) \subset \mathcal{M}_K^{1+n} \\ &\iff \log_{\mathcal{F}} \circ \widehat{\mathrm{Tr}}_{L/K}(\mathcal{F}(\mathcal{M}_L)) \subset \mathcal{M}_K^{1+n}. \end{aligned}$$

The proposition follows. □

Proof of Theorem 1.1. We use the same notation as above, i.e. K is the unramified quadratic extension of $\mathbb{Q}_p$, F is a totally ramified extension of $\mathbb{Q}_p$, $L = KF$ is the composition field, $\mathcal{F}/\mathcal{O}_K$ is the Lubin-Tate formal group with parameter $\pi_K = -p$. As L/F is an unramified extension, we have $v_L(\mathcal{D}_{L/K}) = v_F(\mathcal{D}_{F/\mathbb{Q}_p})$. Let $\widehat{f}_C : \widehat{E}(p\mathbb{Z}_p) \to \mathbb{Q}/\mathbb{Z}$ be the homomorphism associated with C. Recall that $q = p^2$ is the cardinality of the residue field of K.

(1) Assume that $[F : \mathbb{Q}_p] = p^{2t-1}$ and $v_F(\mathcal{D}_{F/\mathbb{Q}_p}) \geq p^{2t-1}(n + t) - p^{2t-2}$. As $a = t - 1$ is the smallest integer such that $q^a > e_{L/K}/(q - 1)$, by Proposition 2.6(2),

$$\log_{\mathcal{F}} \circ \widehat{\mathrm{Tr}}_{L/K}(\mathcal{F}(\mathcal{M}_L)) \subset \mathcal{M}_K^{\lfloor \frac{q^{t-1}+v_L(\mathcal{D}_{L/K})}{e_{L/K}} \rfloor -(t-1)} \subset (\mathcal{M}_K)^{n+1}.$$

Hence F is a splitting field of C by Proposition 3.9.

Assume that $[F : \mathbb{Q}_p] = p^{2t}$ and $v_F(\mathcal{D}_{F/\mathbb{Q}_p}) \geq p^{2t}(n+t)$. As $a = t$ is the smallest integer such that $q^a > e_{L/K}/(q - 1)$, by Proposition 2.6(2),

$$\log_{\mathcal{F}} \circ \widehat{\mathrm{Tr}}_{L/K}(\mathcal{F}(\mathcal{M}_L)) \subset \mathcal{M}_K^{\lfloor \frac{q^{t}+v_L(\mathcal{D}_{L/K})}{e_{L/K}} \rfloor -t} \subset (\mathcal{M}_K)^{n+1}.$$

Hence F is a splitting field of C by Proposition 3.9.

(2) If F with $[F : \mathbb{Q}_p] = p^s$ is a splitting field of C, then by Proposition 3.9, we have

$$\log_{\mathcal{F}} \circ \widehat{\mathrm{Tr}}_{L/K}(\mathcal{F}(\mathcal{M}_L)) \subset (\mathcal{M}_K)^{n+1}.$$

Let $r > \frac{e_{L/K}}{q-1}$ be an integer. Then by Proposition 2.6(1),

$$\log_{\mathcal{F}} \circ \widehat{\mathrm{Tr}}_{L/K}(\mathcal{F}(\mathcal{M}_L^r)) = \mathcal{M}_K^{\lfloor \frac{r+v_L(\mathcal{D}_{L/K})}{e_{L/K}} \rfloor} \subset \log_{\mathcal{F}} \circ \widehat{\mathrm{Tr}}_{L/K}(\mathcal{F}(\mathcal{M}_L)) \subset (\mathcal{M}_K)^{n+1}.$$

In particular, we may take $r = \lfloor \frac{p^s}{p^2-1} \rfloor + 1$ and the claim follows.

(3) This follows from (1) and (2).

(4) By statement (2), if F is a splitting field of C, then $v_F(\mathcal{D}_{F/\mathbb{Q}_p}) \geq 3p^2 - 2$. On the other hand, we know that $v_F(\mathcal{D}_{F/\mathbb{Q}_p}) \leq 3p^2 - 1$ (cf. [12, Chap. 3, Proposition 13]). We first show that those F with $v_F(\mathcal{D}_{F/\mathbb{Q}_p}) = 3p^2 - 1$ do not split C.

By Proposition 3.9, it suffices to show that $\log_{\mathcal{F}} \circ \widehat{\mathrm{Tr}}_{L/K}(\mathcal{F}(\mathcal{M}_L)) = \mathcal{M}_K^2$. Let x be a uniformizer of L. By the following Lemma 3.10(1), $v_K(\mathrm{Tr}_{L/K}(\frac{[\pi_K^n]x}{\pi_K^n})) = 2$. The claim follows from Proposition 2.6(2) and the identity

$$\begin{aligned} v_K(\log_{\mathcal{F}} \circ \widehat{\mathrm{Tr}}_{L/K}(x)) &= v_K(\mathrm{Tr}_{L/K}(\lim_{n\to\infty} \frac{[\pi_K^n]x}{\pi_K^n})) \\ &= \lim_{n\to\infty} v_K(\mathrm{Tr}_{L/K}(\frac{[\pi_K^n]x}{\pi_K^n})) = 2. \end{aligned}$$

Now assume that $v_F(\mathcal{D}_{F/\mathbb{Q}_p}) = 3p^2-2$. If F splits C, then $\log_{\mathcal{F}} \circ \widehat{\mathrm{Tr}}_{L/K}(\mathcal{F}(\mathcal{M}_L)) \subset \mathcal{M}_K^3$. Therefore for any $x \in L$ a uniformizer, $\lim_n (v_K(\mathrm{Tr}_{L/K}([\pi_K^n]x)) - n) \geq 3$. From equation (3.4) in the proof of Lemma 3.10, this shows that $v_K(\mathrm{Tr}_{L/K}(\pi_K x + x^q)) \geq 4$. For the converse, it suffices to show that $\log_{\mathcal{F}} \circ \widehat{\mathrm{Tr}}_{L/K}(\mathcal{F}(\mathcal{M}_L)) = \mathcal{M}_K^3$. Note that $\log_{\mathcal{F}} \circ \widehat{\mathrm{Tr}}(\mathcal{F}(\mathcal{M}_L^2)) = \mathcal{M}_K^3$ by Proposition 2.6(1), it suffices to check that for any uniformizer $x \in L$,

$$\log_{\mathcal{F}} \circ \widehat{\mathrm{Tr}}_{L/K}(x) = \mathrm{Tr}_{L/K}(\log_{\mathcal{F}}(x)) \in \mathcal{M}_K^3.$$

This follows from Lemma 3.10(2) and we complete the proof. □

Lemma 3.10. *Let $K = \mathbb{Q}_{p^2}$ be the quadratic unramified extension of $\mathbb{Q}_p$ and L/K be a totally ramified extension with degree p^2.*

(1) *If $v_L(\mathcal{D}_{L/K}) = 3p^2 - 1$, then for any uniformizer x of L and any $n \geq 1$,*

$$v_K(\mathrm{Tr}_{L/K}([\pi_K^n]x)) = n + 2.$$

(2) *If $v_L(\mathcal{D}_{L/K}) = 3p^2 - 2$, then for any uniformizer x of L and any $n \geq 1$,*

$$v_K(\mathrm{Tr}_{L/K}([\pi_K^n]x)) \geq \min\{n - 1 + v_K(\mathrm{Tr}_{L/K}(\pi_K x + x^q)),\ n + 3\}.$$

Proof. Let x be a uniformizer of L. Let $f(T) \in K[T]$ be the minimal polynomial of x. Then $f(T)$ is an Eisenstein polynomial with degree $q = p^2$. Assume that $f(T) = T^q + a_1 T^{q-1} + \cdots + a_{q-1}T + a_q$. Write $[\pi_K^n]x = \pi_K^n x + \pi_K^{n-1} x^q + \pi_K^n y$ with $v_L(y) \geq 2$, then

$$\begin{aligned} \mathrm{Tr}_{L/K}([\pi_K^n]x) &= \mathrm{Tr}_{L/K}(\pi_K^n x + \pi_K^{n-1} x^q + \pi_K^n y) \\ &= \mathrm{Tr}_{L/K}(\pi_K^n x) + \mathrm{Tr}_{L/K}(\pi_K^{n-1} x^q) + \mathrm{Tr}_{L/K}(\pi_K^n y) \\ &= \pi_K^{n-1} \mathrm{Tr}_{L/K}(x^q) + \pi_K^n \mathrm{Tr}_{L/K}(x) + \pi_K^n \mathrm{Tr}_{L/K}(y). \end{aligned} \tag{3.4}$$

If $v_L(\mathcal{D}_{L/K}) = 3p^2 - 1$, then $\operatorname{Tr}_{L/K} \mathcal{M}_L = \mathcal{M}_K^3$, the last two terms in equation (3.4) have valuation $\geq n+3$. Moreover

$$\begin{aligned} -\operatorname{Tr}_{L/K}(x^q) &= \operatorname{Tr}_{L/K}(a_1 x^{q-1} + \cdots + a_{q-1}x + a_q) \\ &= a_1 \operatorname{Tr}_{L/K}(x^{q-1}) + \cdots + a_{q-1} \operatorname{Tr}_{L/K}(x) + q a_q. \end{aligned}$$

Therefore $v_K(\operatorname{Tr}_{L/K}(x^q)) = v_K(qa_q) = 3$. The statement (1) follows.

If $v_L(\mathcal{D}_{L/K}) = 3p^2 - 2$, then $\operatorname{Tr}_{L/K} \mathcal{M}_L^2 = \mathcal{M}_K^3$. From equation (3.4), we have

$$\begin{aligned} v_K(\operatorname{Tr}_{L/K}([\pi_K^n]x)) &\geq \min\{v_K(\pi_K^{n-1} \operatorname{Tr}_{L/K}(x^q) + \pi_K^n \operatorname{Tr}_{L/K}(x)),\ v_K(\pi_K^n \operatorname{Tr}_{L/K}(y))\} \\ &\geq \min\{n - 1 + v_K(\operatorname{Tr}_{L/K}(\pi_K x + x^q)),\ n+3\}. \end{aligned}$$

The statement (2) follows. □

Remark 3.11. In Theorem 1.1(4), assume that $v_F(\mathcal{D}_{L/K}) = 3p^2 - 2$. Let $f(T) = T^q + a_1 T^{q-1} + \cdots + a_{q-1}T + a_q$ be the Eisenstein polynomial for x. Note that in this case $v_K(a_1) = 2$ and $v_K(a_{q-1}) \geq 3$ (cf. [12, Chap. 3, Proposition 13 and its remarks]), then $\operatorname{Tr}_{L/K}(-px + x^q) \equiv -qa_q + pa_1 \pmod{\mathcal{M}_K^4}$. The condition $v_K(\operatorname{Tr}_{L/K}(-px + x^q)) \geq 4$ is equivalent to $v_K(-pa_q + a_1) \geq 3$.

Remark 3.12 (On the existence of abelian splitting fields). Let $E/\mathbb{Q}_p$ be an elliptic curve with good supersingular reduction. We could apply Theorem 1.1 to show that a principal homogeneous space $C/\mathbb{Q}_p$ of $E/\mathbb{Q}_p$ with period p^n has abelian splitting fields. For positive integer a, denoted by ζ_a the primitive a-th root of unity $e^{2\pi i/a}$.

If $p \geq 3$, for a fixed integer m, $\mathbb{Q}_p$ has only one totally ramified abelian field extension $F(m)$ with $[F(m) : \mathbb{Q}_p] = p^m$ and $\mathbb{Q}_p \subset F(m) \subset \mathbb{Q}_p(\zeta_{p^{m+1}})$. By [12, Chap. 4, Proposition 18], we know the ramification groups of $\operatorname{Gal}(\mathbb{Q}_p(\zeta_{p^{m+1}})/\mathbb{Q}_p)$. Via [12, Chap. 4, Proposition 14] and Herbrand's Theorem [12, Chap. 4, Proposition 14], we can determine the upper numbering ramification groups of $\operatorname{Gal}(F(m)/\mathbb{Q}_p)$. By computing the lower numbering ramification groups and applying [12, Chap. 4, Proposition 4], we obtain $v_{F(m)}(\mathcal{D}_{F(m)/\mathbb{Q}_p}) = (m+1)p^m - \frac{p^m - 1}{p-1} - 1$.

Suppose that $P(C) = p^n$. Then $F(m)$ is a splitting field of C if $\lfloor \frac{q^a + v_F(\mathcal{D}_{F(m)/\mathbb{Q}_p})}{e_{F(m)/\mathbb{Q}_p}} \rfloor - a \geq 1 + n$, where a is the smallest integer which satisfies $q^a > \frac{e_{F(m)/\mathbb{Q}_p}}{q-1}$. Let $m = 2n$, then $a = n$ and

$$\begin{aligned} \lfloor \frac{q^a + v_{F(2n)}(\mathcal{D}_{F(2n)/\mathbb{Q}_p})}{e_{F(2n)/\mathbb{Q}_p}} \rfloor - n &= \lfloor \frac{p^{2n} + (2n+1)p^{2n} - \frac{p^{2n}-1}{p-1} - 1}{p^{2n}} \rfloor - n \\ &= 2n + 1 - n = n + 1. \end{aligned}$$

Hence $F(2n)$ is a splitting field of C. One also sees that for a principal homogeneous space C with $P(C) = p^n$, there is no abelian splitting field F of C with $[F : \mathbb{Q}_p] = p^n$.

If $p = 2$, for a fixed integer m, $\mathbb{Q}_2$ has two totally ramified abelian extension $L_i(m)$ with $[L_i(m) : \mathbb{Q}_2] = 2^m$ $(i = 1,\ 2)$. They are subfields of $\mathbb{Q}(\zeta_{2^{m+2}})$. Note that $\operatorname{Gal}(\mathbb{Q}(\zeta_{2^{m+2}})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^m\mathbb{Z}$, let L_1 be the cyclic extension. Using the same method as above, one can compute $v_{L_1(m)}(\mathcal{D}_{L_1(m)/\mathbb{Q}_2}) = (m+1)2^m - 1$ and $v_{L_2(m)}(\mathcal{D}_{L_2(m)/\mathbb{Q}_2}) = m \cdot 2^m$. Suppose that $P(C) = 2^n$, then $L_1(2n-1)$ and $L_2(2n)$ are splitting fields of C.

Remark 3.13. We note that in other cases, one could also use the trace map to study the splitting fields of a principal homogeneous space. If E/K has good ordinary reduction, we have the computation in [8, Section 4]. If E/K has multiplicative bad reduction, then via the Tate curve, $E(L) \cong L^\times/q^{\mathbb{Z}}$ and the trace map $E(L) \to E(K)$ is induced from the norm map $L^\times \to K^\times$ (cf. [15, Chap. 5]).

References

[1] P. Clark. *There are genus one curves of every index over every number field.* J. Reine Angew. Math. 594 (2006), 201-206.
[2] P. Clark, S. Sharif. *Period, index and potential. III.* Algebra Number Theory 4 (2010), no. 2, 151-174.
[3] L. Fourquaux. *Applications $\mathbb{Q}_p$-linéaires, continues et Galois-équivariantes de $\mathbb{C}_p$ dans lui-même.* J. Number Theory 129 (2009), 1246-1255.
[4] S. Kobayashi. *Iwasawa theory for elliptic curves at supersingular primes.* Invent. Math. 152 (2003), no. 1, 1-36.
[5] S. Lang. *Algebraic groups over finite fields.* Amer. J. Math. 78 (1956), 555-563.
[6] S. Lang, J. Tate. *Principal homogeneous space over abelian varieties.* Amer. J. Math. 80(1958), 659-684.
[7] S. Lichtenbaum. *The period-index problem for elliptic curves.* Amer. J. Math. 90(1968), 1209-1223.
[8] B. Mazur. *Rational points of abelian varieties with values in towers of number fields.* Invent. Math. 18 (1972), 183-266.
[9] J. S. Milne. *Arithmetic Duality Theorem.* BookSurge, LLC, Charleston, SC, 2006.
[10] C. O'neil. *The period-index obstruction for elliptic curves.* J. Number Theory 95 (2002), no. 2, 329-339.
[11] J. Tate. WC *groups over p-adic fields.* Seminaire Bourbaki 10, (1957), No. 156, Paris.
[12] J. P. Serre. *Local Fields.* Graduate Texts in Mathematics, Vol. 67, Springer-Verlag, New York, 1979.
[13] J. P. Serre. *Local class field theory.* In the book Algebraic Number Theory Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich Academic Press, London; Thompson Book Co., Inc., Washington, DC, 1967. 128-161.
[14] J. H. Silverman. *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics, Vol. 106, Springer-Verlag, New York, 1986.
[15] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics, Vol. 151, Springer-Verlag, New York, 1994.
[16] `https://math.stackexchange.com/questions/3644403/logarithm-and-lubin-tate-formal-group`. Discussion on Logarithm and Lubin-Tate formal group.

Department of Mathematics, Nanjing University, Nanjing 210093, China
E-mail address: `cxcheng@nju.edu.cn`

Department of Mathematics, Nanjing University, Nanjing 210093, China
E-mail address: `chengniu@smail.nju.edu.cn`