Lubin-Tate theory

Peter Schneider

Course at Münster in 2017, **Version 29.12.2017**

The first three chapters develop the formalism of Lubin-Tate formal group laws. We do this in a slightly generalized way as suggested by de Shalit in [DeS]. In the fourth chapter we construct the Coleman norm operator. The final chapter then is devoted to a complete account of the reciprocity isomorphism of local class field theory. The only further ingredient which we will use for this is the basic theory of the higher ramification subgroups, as can be found, for example, in [Ser]. But we do include a complete proof of the Hasse-Arf theorem, which is crucially needed. In all we follow the outline in [Yos] but give quite a bit more details.

Contents

1 Formal group laws

ec:group-laws

We recall that a (one dimensional) commutative formal group law over a commutative ring A is a formal power series $F(X,Y) \in A[[X,Y]]$ in two variables with coefficients in A such that:

- $F(X,0) = X$ and $F(0,Y) = Y$ (hence $F(X,Y) = X + Y +$ higher terms),
- $F(X,F(Y,Z)) = F(F(X,Y),Z)$, and
- $F(X,Y) = F(Y,X)$.

Furthermore, a homomorphism $h : F \to G$ between two such formal group laws F and G is a formal power series $h(X) \in A[[X]]$ such that $h(0) = 0$ and $h(F(X,Y)) = G(h(X), h(Y))$. Of course, h is called an isomorphism if there exists a homomorphism $h^{-1} : G \to F$ such that $h(h^{-1}(X)) = X = h^{-1}(h(X))$.

formal-iso *Exercise* 1.1. The formal power series $h(X) = c_1X + \dots$ has an inverse h^{-1} if and only if $c_1 \in A^\times$.

Exercise. The set $\mathrm{Hom}_A(F,G)$ of homomorphisms from F to G is an abelian group with respect to the addition $(h_1 + h_2)(X) := G(h_1(X), h_2(X))$ with zero element 0. The abelian group $\mathrm{End}_A(F) := \mathrm{Hom}_A(F,F)$ is a (possibly noncommutative) ring with respect to the multiplication $(h_1 \cdot h_2)(X) := h_1(h_2(X))$ with unit element X.

ormal-inverse **Lemma 1.2.** *The formal group law $F(X,Y)$ has a "formal inverse" in the sense that there is a unique formal power series $\iota_F(X) \in A[[X]]$ such that*

$$\iota_F(X) = -X + \textit{higher terms} \qquad \textit{and} \qquad F(X, \iota_F(X)) = 0$$

Proof. We construct inductively a unique sequence $(\iota_j(X))_{j\geq 1}$ of polynomials in $XA[X]$ such that $\deg \iota_j(X) \leq j$ and

$$F(X, \iota_j(X)) \equiv 0 \mod X^{j+1}A[[X]] \,.$$

Obviously, we have to put $\iota_1(X) := -X$. Suppose that $\iota_j(X)$ has been constructed already. Then

$$F(X, \iota_j(X)) \equiv c_{j+1}X^{j+1} \mod X^{j+2}A[[X]]$$

for a unique $c_{j+1} \in A$. We define $\iota_{j+1}(X) := \iota_j(X) - c_{j+1}X^{j+1}$. Then

$$F(X, \iota_{j+1}(X)) = F(X, \iota_j(X) - c_{j+1}X^{j+1}) \equiv F(X, \iota_j(X)) - c_{j+1}X^{j+1} \equiv 0 \mod X^{j+2}A[[X]] \,.$$

It follows that $\iota_F(X) := -X - \sum_{j\geq 2} c_jX^j \in A[[X]]$ satisfies the equation $F(X, \iota_F(X)) = 0$. □

Example. The multiplicative formal group law is $\widehat{\mathbb{G}}_m(X,Y) := X + Y + XY = (1+X)(1+Y) - 1$. Its formal inverse is $\iota_{\widehat{\mathbb{G}}_m}(X) = -\frac{X}{X+1} = \sum_{i\geq 1}(-1)^iX^i$.

Suppose now that $A = o_L$ is the ring of integers of a complete nonarchimedean field L. Any commutative formal group law F over o_L gives rise to actual abelian groups in the following way. Let K be any complete nonarchimedean extension field of L (which includes the requirement that the absolute value of K extends the one of L), and let $\mathfrak{m}_K$ denote the maximal ideal of its ring of integers. For any two $x, y \in \mathfrak{m}_K$ the series $x +_F y := F(x,y)$ converges with limit in $\mathfrak{m}_K$. One easily checks that $(\mathfrak{m}_K, +_F)$ is an abelian group in which the inverse of x is given by $\iota_F(x)$. Moreover, any $h \in \mathrm{End}_{o_L}(F)$ induces the endomorphism $x \mapsto h(x)$ of $(\mathfrak{m}_K, +_F)$.

Example. For the multiplicative formal group the abelian group $(\mathfrak{m}_K, +_{\widehat{\mathbb{G}}_m})$ is isomorphic, by sending x to $1 + x$, to the subgroup $1 + \mathfrak{m}_K$ of $K^\times$.

2 Relative Lubin-Tate group laws

sec:LT

From now on we put ourselves into the following setting. We fix a local field $(L, |\ |)$ with ring of integers o_L, maximal ideal $\mathfrak{m}_L$ and residue field k_L of characteristic $p > 0$. We let E_0 be any not necessarily unramified extension field of L, and we denote by $(E, |\ |)$ its completion. The extension E_0/L is the union of finite unramified extensions E_i/L. Any prime element π in o_L remains a prime element in each E_i, therefore in E_0, and hence in the ring of integers o_E in E, i.e., the maximal ideal $\mathfrak{m}_E$ in o_E satisfies $\mathfrak{m}_E = \pi o_E$. The residue field k_E of E is also the residue field of E_0 and is a possibly infinite Galois extension of k_L. Its Galois group is topologically generated by the Frobenius automorphism $\varphi_{k_L}(\bar{a}) = \bar{a}^q$ where $q := |k_L|$. Since the restriction map induces an isomorphism

$$\mathrm{Gal}(E_0/L) \xrightarrow{\cong} \mathrm{Gal}(k_E/k_L)$$

the preimage of φ_{k_L} is a well defined Galois automorphism $\varphi := \varphi_L$ of E_0/L. Any Galois automorphism of E_0/L respects the absolute value and hence extends by continuity to an automorphism of the extension E/L. We will denote the extension of $\varphi = \varphi_L$ to E by the same letters.

hi-invariants

Lemma 2.1. $\{a \in E : \varphi(a) = a\} = L$.

Proof. For any finite subextension $L \subseteq E_i \subseteq E_0$ let q_i denote the cardinality of the residue field k_i of E_i. The group μ_i of roots of unity of order dividing $q_i - 1$ is contained in E_i, and $\mu_i \cup \{0\}$ is a set of representatives for the cosets in k_i. Hence $\mu := \{0\} \cup \bigcup_i \mu_i$ is a set of representatives for the cosets in $k_E = o_E/\mathfrak{m}_E$. The point about this set μ is that it is invariant under the automorphism φ with $\{\zeta \in \mu : \varphi(\zeta) = \zeta\} \subseteq L$. On the other hand we fix a prime element π in o_L which also is a prime element in o_E. Any $a \in o_E$ has a unique convergent expansion $a = \sum_{j=0}^{\infty} \zeta_j \pi^j$ with $\zeta_j \in \mu$. We have $\varphi(a) = a$ if and only if φ fixes each coefficient ζ_j if and only if each coefficient ζ_j lies in o_L, i.e., a lies in o_L. □

For any $m \in \mathbb{Z}$ and any formal power series $F(X_1, \ldots, X_n) = \sum_{i_1,\ldots,i_n \geq 0} c_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}$ in $o_E[[X_1, \ldots, X_n]]$ we define the formal power series

$${}^{\varphi^m}F(X_1, \ldots, X_n) = \sum_{i_1,\ldots,i_n \geq 0} \varphi^m(c_{i_1,\ldots,i_n}) X_1^{i_1} \ldots X_n^{i_n} \ .$$

The following facts are easy to check:

- ${}^{\varphi^m}(F + G) = {}^{\varphi^m}F + {}^{\varphi^m}G$.
- ${}^{\varphi^m}(F(H_1, \ldots, H_n)) = {}^{\varphi^m}F({}^{\varphi^m}H_1, \ldots, {}^{\varphi^m}H_n)$.
- If F is a commutative formal group law over o_E, then ${}^{\varphi^m}F$ is a commutative formal group law as well.

Definition 2.2. *Let π be a prime element in o_E. A Frobenius power series (for π) is a formal power series $\phi(X) \in o_E[[X]]$ such that*

$$\phi(X) = \pi X + \textit{higher terms} \qquad \textit{and} \qquad \phi(X) \equiv X^q \mod \pi o_E[[X]] \ .$$

Example. 1) $\phi(X) = \pi X + X^q$.

2) If $L = \mathbb{Q}_p$ and $\pi = p$ then $\phi(X) = (1+X)^p - 1$.

Remark. It follows from the Weierstrass preparation theorem (cf. [B-CA] VII.3.8 Prop. 6) that for any Frobenius power series $\phi(X)$ there is a polynomial $\Phi(X) \in o_E[X]$ of degree q such that $\Phi(X) \equiv X^q \bmod \pi o_E[X]$ and a unit $u(X) \in o_E[[X]]^\times$ such that $\phi(X) = \Phi(X) \cdot u(X)$.

solve **Lemma 2.3.** *Let $a \in \mathfrak{m}_E$; for any $y \in o_E$ there is a unique $x \in o_E$ such that $a\varphi(x) - x = y$.*

Proof. The series $x := -\sum_{j\geq 0}(\prod_{\nu=0}^{j-1}\varphi^\nu(a))\varphi^j(y)$ converges in o_E. It is easily checked to be a solution of the equation in question. On the other hand suppose that $a\varphi(x) - x = 0$ for some $x \in o_E$. Then $|a||x| = |a||\varphi(x)| = |x|$. Since $|a| < 1$ it follows that $x = 0$. □

linear-term **Lemma 2.4.** *Let $\phi(X)$ and $\psi(X)$ be two Frobenius power series for the prime elements π and π', respectively, and let $F_1(X_1, \ldots, X_n) = a_1X_1 + \ldots + a_nX_n \in o_E[X_1, \ldots, X_n]$ be any linear polynomial such that $\pi a_i = \pi'\varphi(a_i)$ for any $1 \leq i \leq n$; then there exists a unique formal power series $F(X_1, \ldots, X_n) \in o_E[[X_1, \ldots, X_n]]$ such that*

$$F = F_1 + \textit{terms of degree} \geq 2 \qquad \textit{and} \qquad \phi(F(X_1, \ldots, X_n)) = {}^\varphi F(\psi(X_1), \ldots, \psi(X_n)) \ .$$

Proof. We begin by constructing inductively a sequence of polynomials $F_i(X_1, \ldots, X_n) \in o_E[X_1, \ldots, X_n]$ for $i \geq 1$ such that

$$F_i = F_1 + \text{terms of degree} \geq 2 \qquad \text{and}$$

nductive-cond (1) $$\phi(F_i(X_1, \ldots, X_n)) \equiv {}^\varphi F_i(\psi(X_1), \ldots, \psi(X_n)) \mod \langle X_1, \ldots, X_n\rangle^{i+1} \ .$$

Here $\langle X_1, \ldots, X_n\rangle$ denotes the ideal in $o_E[[X_1, \ldots, X_n]]$ generated by the variables. Of course, for F_1 we take the given linear polynomial. It satisfies

$$\phi(F_1) = \phi(a_1X_1 + \ldots + a_nX_n) \equiv \pi a_1X_1 + \ldots + \pi a_nX_n \mod \langle X_1, \ldots, X_n\rangle^2$$

and

$${}^\varphi F_1(\psi, \ldots, \psi) =$$
$$\varphi(a_1)\psi(X_1) + \ldots + \varphi(a_n)\psi(X_n) \equiv \varphi(a_1)\pi'X_1 + \ldots + \varphi(a_n)\pi'X_n \mod \langle X_1, \ldots, X_n\rangle^2 \ ,$$

which implies (1) for $i = 1$. Now we suppose that F_i has been constructed already. Using (1) we may write

$$\phi(F_i(X_1, \ldots, X_n)) \equiv {}^\varphi F_i(\psi(X_1), \ldots, \psi(X_n)) + E_{i+1}(X_1, \ldots, X_n) \mod \langle X_1, \ldots, X_n\rangle^{i+2} \ ,$$

where $E_{i+1}(X_1, \ldots, X_n)$ is a homogeneous polynomial of degree $i+1$. We observe that

$$\begin{aligned}\phi(F_i(X_1, \ldots, X_n)) &\equiv F_i(X_1, \ldots, X_n)^q \equiv {}^\varphi F_i(X_1^q, \ldots, X_n^q) \\ &\equiv {}^\varphi F_i(\psi(X_1), \ldots, \psi(X_n)) \mod \pi o_E[[X_1, \ldots, X_n]] \ ,\end{aligned}$$

which implies that $E_{i+1} \in \pi o_E[X_1, \ldots, X_n]$. Write

$$\pi^{-1}E_{i+1} = \sum_M y_M M$$

with $y_M \in o_E$ and where M runs over all monomials of degree $i+1$. According to Lemma 2.3 we find, for any M, a unique $x_M \in o_E$ such that $\frac{(\pi')^{i+1}}{\pi}\varphi(x_M) - x_M = y_M$. We define the homogeneous polynomial $H_{i+1} := \sum_M x_M M$ of degree $i+1$. By construction it satisfies

$$(\pi')^{i+1} \cdot {}^{\varphi}H_{i+1} = \pi H_{i+1} + E_{i+1}$$

and is uniquely determined by this equation. We put

$$F_{i+1} := F_i + H_{i+1} \ .$$

Then

$$\begin{aligned}
\phi(F_{i+1}) = \phi(F_i + H_{i+1}) &\equiv \phi(F_i) + \pi H_{i+1} \\
&\equiv {}^{\varphi}F_i(\psi, \ldots, \psi) + E_{i+1} + \pi H_{i+1} \\
&\equiv {}^{\varphi}F_i(\psi, \ldots, \psi) + (\pi')^{i+1} \cdot {}^{\varphi}H_{i+1} \\
&\equiv {}^{\varphi}F_i(\psi, \ldots, \psi) + {}^{\varphi}H_{i+1}(\psi, \ldots, \psi) \\
&\equiv {}^{\varphi}F_{i+1}(\psi, \ldots, \psi) \mod \langle X_1, \ldots, X_n \rangle^{i+2}
\end{aligned}$$

which implies (1) for $i+1$. It follows that the formal power series

$$F := F_1 + \sum_{i \geq 2} H_i$$

has the desired properties.

For the uniqueness let us suppose that the formal power series F has the asserted properties. We write $F = F_1 + \sum_{i \geq 2} \tilde{H}_i$ with uniquely determined homogeneous polynomials $\tilde{H}_i$ of degree i. By going through the above inductive argument again one sees that these $\tilde{H}_i$ necessarily coincide with the earlier H_i. □

LT-1 **Proposition 2.5.** *For any Frobenius power series $\phi(X)$ there is a unique commutative formal group law $F_\phi(X,Y)$ over o_E such that $\phi : F_\phi \longrightarrow {}^{\varphi}(F_\phi)$ is a homomorphism of formal group laws.*

Proof. By applying Lemma 2.4 with $\psi = \phi$ and $F_1 = X + Y$ we obtain a unique formal power series $F_\phi(X,Y)$ such that

$$F_\phi(X,Y) = X + Y + \text{terms of degree} \geq 2 \ ,$$

and $\phi : F_\phi \longrightarrow {}^{\varphi}(F_\phi)$ is a homomorphism. For the associativity of F_ϕ we consider the two formal power series

$$H_1 := F_\phi(F_\phi(X,Y), Z) \qquad \text{and} \qquad H_2 := F_\phi(X, F_\phi(Y,Z)) \ .$$

Both have the same linear term $X + Y + Z$ and both satisfy

$$\phi(H_i(X,Y,Z)) = {}^{\varphi}H_i(\phi(X), \phi(Y), \phi(Z)) \ .$$

The uniqueness part of the assertion of Lemma 2.4 therefore implies $H_1 = H_2$. For the commutativity of F_ϕ we similarly consider $H_1 := F_\phi(X,Y)$ and $H_2 := F_\phi(Y,X)$, which both

have the same linear term $X+Y$ and satisfy $\phi(H_i(X,Y)) = {}^{\varphi}H_i(\phi(X),\phi(Y))$. Hence again the uniqueness in Lemma 2.4 implies $H_1 = H_2$.

Finally we consider $F(X) := F_\phi(X,0) = X + \sum_{i\geq 2} c_i X^i$. Setting $Y = Z = 0$ in the associativity law we obtain

$$F(X) = F(F(X)) = F(X) + \sum_{i\geq 2} c_i F(X)^i \quad \text{and hence} \quad \sum_{i\geq 2} c_i F(X)^i = 0\ .$$

Since the first term in $F(X)^i$ is X^i we deduce inductively that $c_i = 0$ for any $i \geq 2$. This shows that $F_\phi(X,0) = X$. A similar argument gives that also $F_\phi(0,Y) = Y$. □

Definition 2.6. *F_ϕ is called the relative (to the extension E/L) Lubin-Tate (formal) group law of the Frobenius power series ϕ.*

In the case $E = L$ we simply speak of the Lubin-Tate group law F_ϕ. Note that then $\phi \in \mathrm{End}_{o_L}(F_\phi)$.

Example. 1) F_ϕ for $\phi(X) = \pi X + X^q$ is called the *special* Lubin-Tate group law of π.

2) If $L = \mathbb{Q}_p$, $\pi = p$, and $\phi(X) = (1+X)^p - 1$ then $F_\phi = \widehat{\mathbb{G}}_m$ (which for $p \neq 2$ is not special).

rem:Frob-LT **Remark 2.7.** *If ϕ is a Frobenius power series for the prime element π then ${}^{\varphi}\phi$ is a Frobenius power series for $\varphi(\pi)$ and $F_{({}^{\varphi}\phi)} = {}^{\varphi}(F_\phi)$.*

Suppose that ϕ and ψ are Frobenius power series for the prime elements π and ϖ, respectively. We introduce the additive subgroup

$$o_E^{\pi,\varpi} := \{a \in o_E : \pi a = \varpi\varphi(a)\}$$

of o_E. For three prime elements π, ϖ, and ϖ' we have

f:mult (2) $$o_E^{\pi,\varpi} \cdot o_E^{\varpi,\varpi'} \subseteq o_E^{\pi,\varpi'} \qquad \text{and} \qquad o_E^{\pi,\pi} = o_L$$

(cf. Lemma 2.1). In particular, $o_E^{\pi,\varpi}$ is an o_L-submodule of o_E. Let $a \in o_E^{\pi,\varpi}$ be any element. By applying Lemma 2.4 with $F_1 = aX$ we obtain a unique formal power series $[a]_{\phi,\psi}(X) \in o_E[[X]]$ such that

$$[a]_{\phi,\psi}(X) = aX + \text{higher terms} \qquad \text{and} \qquad \phi([a]_{\phi,\psi}(X)) = {}^{\varphi}[a]_{\phi,\psi}(\psi(X))\ .$$

We obviously have $[1]_{\phi,\phi} = X$ and, if $E = L$, then $[\pi]_{\phi,\phi} = \phi$.

LT-2 **Proposition 2.8.** *Let ϕ, ψ,and ψ' be Frobenius power series for the prime elements π, ϖ, and ϖ', respectively. The map*

$$\begin{aligned} o_E^{\pi,\varpi} &\longrightarrow \mathrm{Hom}_{o_E}(F_\psi, F_\phi) \\ a &\longmapsto [a]_{\phi,\psi} \end{aligned}$$

is a well defined injective homomorphism of abelian groups satisfying

$$[a]_{\phi,\psi}([b]_{\psi,\psi'}(X)) = [ab]_{\phi,\psi'}(X) \qquad \text{for any } a \in o_E^{\pi,\varpi} \text{ and } b \in o_E^{\varpi,\varpi'}.$$

In particular, $[\ ]_\phi := [\ ]_{\phi,\phi} : o_L \longrightarrow \mathrm{End}_{o_E}(F_\phi)$ is an injective homomorphism of rings.

Proof. We consider the formal power series

$$H_1(X,Y) := F_\phi([a]_{\phi,\psi}(X), [a]_{\phi,\psi}(Y)) \qquad \text{and} \qquad H_2(X,Y) := [a]_{\phi,\psi}(F_\psi(X,Y)) \ .$$

They both have the same linear term $aX + aY$. Moreover, we compute

$$\begin{aligned}\phi(H_1(X,Y)) &= \phi(F_\phi([a]_{\phi,\psi}(X), [a]_{\phi,\psi}(Y))) = {}^\varphi F_\phi(\phi([a]_{\phi,\psi}(X)), \phi([a]_{\phi,\psi}(Y))) \\ &= {}^\varphi F_\phi({}^\varphi[a]_{\phi,\psi}(\psi(X)), {}^\varphi[a]_{\phi,\psi}(\psi(Y))) = {}^\varphi H_1(\psi(X), \psi(Y))\end{aligned}$$

and

$$\begin{aligned}\phi(H_2(X,Y)) &= \phi([a]_{\phi,\psi}(F_\psi(X,Y))) = {}^\varphi[a]_{\phi,\psi}(\psi(F_\psi(X,Y))) \\ &= {}^\varphi[a]_{\phi,\psi}({}^\varphi F_\psi(\psi(X), \psi(Y))) = {}^\varphi H_2(\psi(X), \psi(Y)) \ .\end{aligned}$$

Therefore the uniqueness in Lemma 2.4 implies $H_1 = H_2$. This means that

$$[a]_{\phi,\psi} : F_\psi \longrightarrow F_\phi$$

is a homomorphism. The fact that $a \mapsto [a]_{\phi,\psi}$ is additive and multiplicative in the asserted sense follows again, similarly as above, by using the uniqueness in Lemma 2.4. Finally the injectivity is clear, since the linear term of $[a]_{\phi,\psi}$ is aX. □

LT-3 **Corollary 2.9.** *For any two Frobenius power series ϕ and ψ for the **same** prime element there exists an isomorphism $F_\psi \xrightarrow{\cong} F_\phi$.*

Proof. Choose any $a \in o_L^\times$ and take $[a]_{\phi,\psi}$ and $[a^{-1}]_{\psi,\phi}$. □

This corollary can be strengthened in the case where E is maximally large, i.e., where k_E is algebraically closed. The reason is the following fact.

H1 **Lemma 2.10.** *Suppose that k_E is algebraically closed; then the map*

$$\begin{aligned} o_E^\times &\longrightarrow o_E^\times \\ u &\longmapsto u^{-1}\varphi(u)\end{aligned}$$

is surjective.

Proof. We fix a prime element $\varpi \in o_L$. Let $y \in o_E^\times$. We construct inductively a sequence $(u_n)_{n\geq 1}$ in $o_E^\times$ such that

$$u_n^{-1}\varphi(u_n) \equiv y \mod \varpi^n o_E \qquad \text{and} \qquad u_{n+1} \equiv u_n \mod \varpi^n o_E \quad \text{for any } n \geq 1.$$

Then $u := \lim_{n\to\infty} u_n$ is defined, lies in $o_E^\times$, and satisfies $u^{-1}\varphi(u) = y$.

First of all we observe that, since k_E is algebraically closed, the maps

$$\begin{aligned} k_E^\times &\longrightarrow k_E^\times \\ \bar{u} &\longmapsto \bar{u}^{-1}\varphi_{k_E}(\bar{u}) = \bar{u}^{q-1}\end{aligned} \qquad \text{and} \qquad \begin{aligned} k_E &\longrightarrow k_E \\ \bar{a} &\longmapsto \varphi_{k_E}(\bar{a}) - \bar{a} = \bar{a}^q - \bar{a}\end{aligned}$$

are surjective. By the surjectivity of the left hand map we find a $u_1 \in o_E^\times$ such that $u_1^{-1}\varphi(u_1) \equiv y \mod \varpi o_E$. Suppose that $u_1, \ldots, u_n$ have been constructed. Then $u_n^{-1}\varphi(u_n) - y \in \varpi^n o_E$ and hence

$$\frac{y}{u_n^{-1}\varphi(u_n)} = 1 + \varpi^n b \quad \text{for some } b \in o_E.$$

By the surjectivity of the right hand map above we find an $a \in o_E$ such that

$$\varphi(a) - a \equiv b \mod \varpi o_E \ .$$

Then

$$1 + \varpi^n \varphi(a) \equiv 1 + \varpi^n(a+b) \equiv (1+\varpi^n a)(1+\varpi^n b) \mod \varpi^{n+1} o_E \ .$$

We now define $u_{n+1} := u_n(1+\varpi^n a)$, which lies in $o_E^\times$. We compute

$$u_{n+1}^{-1}\varphi(u_{n+1}) - y \equiv \frac{\varphi(u_n)(1+\varpi^n\varphi(a))}{u_n(1+\varpi^n a)} - y \equiv \frac{\varphi(u_n)(1+\varpi^n b)}{u_n} - y \equiv 0 \mod \varpi^{n+1} o_E$$

and

$$u_{n+1} - u_n = u_n \varpi^n a \in \varpi^n o_E \ .$$

□

LT-4 **Proposition 2.11.** *Suppose that k_E is algebraically closed; for any two Frobenius power series ϕ and ψ (for possibly different prime elements π and ϖ) there exists an isomorphism $F_\psi \xrightarrow{\cong} F_\phi$.*

Proof. As $\varpi^{-1}\pi \in o_E^\times$ we may apply Lemma 2.10 in order to see that the set $o_E^{\pi,\varpi}$ contains a unit $u \in o_E^\times$. Then u^{-1} lies in $o_E^{\varpi,\pi}$. Hence $[u]_{\phi,\psi}$ is an isomorphism as required with inverse and $[u^{-1}]_{\psi,\phi}$. □

From this we can deduce a sharpening of Cor. 2.9 provided the extension E/L is finite. We first need further notation.

Given any Frobenius power series ϕ we define inductively, for any $n \geq 1$, the power series ϕ_n by $\phi_1(X) := \phi(X)$ and $\phi_{n+1}(X) := {}^{\varphi^n}\phi(\phi_n(X)) = {}^{\varphi}\phi_n(\phi(X))$. They satisfy

:phi-iterated (3)
$$\begin{aligned} &\phi_n(F(X,Y) = {}^{\varphi^n}F(\phi_n(X), \phi_n(Y)) \quad \text{and} \\ &\phi_n([a]_\phi(X)) = {}^{\varphi^n}[a]_\phi(\phi_n(X)) \quad \text{for any } a \in o_L. \end{aligned}$$

We let E^{max} denote the completion of a maximal unramified extension of L which contains E.

descent **Proposition 2.12.** *Let ϕ and ψ be two Frobenius power series for the prime elements π and ϖ, respectively, and suppose that E/L is a finite extension of degree d; we then have:*

i. $\phi_d = [\mathrm{Norm}_{E/L}(\pi)]_\phi$;

ii. if $\mathrm{Norm}_{E/L}(\pi) = \mathrm{Norm}_{E/L}(\varpi)$ *then* $o_{E^{max}}^{\pi,\varpi} = o_E^{\pi,\varpi}$;

iii. for any $a \in o_{E^{max}}^{\pi,\varpi}$ *we have* ${}^{\varphi^d}[a]_{\phi,\psi} = [a\,\mathrm{Norm}_{E/L}(\frac{\pi}{\varpi})]_{\phi,\psi}$.

Proof. i. We have $\mathrm{Gal}(E/L) = \{\mathrm{id}, \varphi, \ldots, \varphi^{d-1}\}$. Hence

$$\phi_d(X) = \varphi^{d-1}(\pi)\cdots\varphi(\pi)\pi X + \text{ higher terms } = \mathrm{Norm}_{E/L}(\pi)X + \text{ higher terms } .$$

Moreover we have $\phi(\phi_d(X)) = {}^{\varphi^d}\phi(\phi_d(X)) = {}^{\varphi}\phi_d(\phi(X))$. The uniqueness in Lemma 2.4 therefore implies that

$$\phi_d = [\mathrm{Norm}_{E/L}(\pi)]_\phi \ .$$

ii. Let $a \in o_{E^{max}}^{\pi,\varpi}$, so that $\pi a = \varpi\varphi(a)$. It follows that $\varphi^i(\pi)\varphi^i(a) = \varphi^i(\varpi)\varphi^{i+1}(a)$ and then by induction that

$$\varphi^i(\pi)\cdots\varphi(\pi)\pi a = \varphi^i(\varpi)\cdots\varphi(\varpi)\varpi\varphi^{i+1}(a)$$

for any $i \geq 0$. For $i = d-1$ we obtain $\mathrm{Norm}_{E/L}(\pi)a = \mathrm{Norm}_{E/L}(\varpi)\varphi^d(a)$. Our assumption therefore implies that $\varphi^d(a) = a$. Lemma 2.1 then tells us that $a \in o_E$.

iii. By i. we have $\phi_d = [\mathrm{Norm}_{E/L}(\pi)]_\phi$ and $\psi_d = [\mathrm{Norm}_{E/L}(\varpi)]_\psi$. Moreover, an obvious generalization of (3) gives $\phi_d([a]_{\phi,\psi}(X)) = {}^{\varphi^d}[a]_{\phi,\psi}(\psi_d(X))$. We deduce that

$$\begin{aligned}
{}^{\varphi^d}[a]_{\phi,\psi}(\psi_d(X)) &= [\mathrm{Norm}_{E/L}(\pi)]_\phi([a]_{\phi,\psi}(X)) = [\mathrm{Norm}_{E/L}(\pi)a]_{\phi,\psi}(X) \\
&= [a\,\mathrm{Norm}_{E/L}(\pi)]_{\phi,\psi}(X) = [a\,\mathrm{Norm}_{E/L}(\tfrac{\pi}{\varpi})]_{\phi,\psi}([\mathrm{Norm}_{E/L}(\varpi)]_\psi(X)) \\
&= [a\,\mathrm{Norm}_{E/L}(\tfrac{\pi}{\varpi})]_{\phi,\psi}(\psi_d(X))\ .
\end{aligned}$$

The assertion follows by applying Lemma 4.1 (which, in particular, says that the procedure of inserting a fixed Frobenius power series into any power series is injective) successively with the Frobenius power series $\psi, {}^{\varphi}\psi, \ldots, {}^{\varphi^{d-1}}\psi$. □

LT-5 **Corollary 2.13.** *Let ϕ and ψ be two Frobenius power series for the prime elements π and ϖ, respectively, and suppose that E/L is a finite extension; if* $\mathrm{Norm}_{E/L}(\pi) = \mathrm{Norm}_{E/L}(\varpi)$ *then there exists an isomorphism $F_\psi \xrightarrow{\cong} F_\phi$.*

Proof. By viewing F_ϕ and F_ψ as Lubin-Tate group laws over the ring of integers $o_{E^{max}}$ in E^{max} we may apply Prop. 2.11 and obtain a unit $u \in o_{E^{max}}^\times \cap o_{E^{max}}^{\pi,\varpi}$ such that $[u]_{\phi,\psi} : F_\psi \xrightarrow{\cong} F_\phi$ is an isomorphism over $o_{E^{max}}$. But according to Prop. 2.12.ii the unit u lies, in fact, in $o_E^\times \cap o_E^{\pi,\varpi}$. Hence $[u]_{\phi,\psi}$ is an isomorphism over o_E. □

3 Lubin-Tate extensions

:LT-extension

We keep the setting of the previous section, and we fix a prime element π of o_E as well as a Frobenius power series ϕ for π. Let $F := F_\phi$ denote the corresponding Lubin-Tate group law. We also fix an algebraic closure $\overline{E}$ of E and put $\mathfrak{M} := \{a \in \overline{E} : |a| < 1\}$. As explained above we have, for any finite subextension $E \subseteq K \subseteq \overline{E}$, the abelian group $(\mathfrak{m}_K, +_F)$. Since $\mathfrak{M} = \bigcup_K \mathfrak{m}_K$ we also have the abelian group $(\mathfrak{M}, +_F)$. In fact, it follows from Prop. 2.8 that each $(\mathfrak{m}_K, +_F)$ and hence also $(\mathfrak{M}, +_F)$ is an o_L-module via the multiplication

$$\begin{aligned}
o_L \times \mathfrak{M} &\longrightarrow \mathfrak{M} \\
(a, z) &\longmapsto [a]_\phi(z)\ .
\end{aligned}$$

For any $n \geq 1$ we introduce the subset

$$\mathcal{F}_n := \{z \in \mathfrak{M} : \phi_n(z) = 0\}$$

of $\overline{E}$. Of course, we have $\mathcal{F}_1 \subseteq \mathcal{F}_2 \subseteq \ldots \subseteq \mathcal{F}_n \subseteq \ldots$. It follows from (3) that each $\mathcal{F}_n$ is an o_L-submodule of $(\mathfrak{M}, +_F)$. By adjoining these subsets to E we obtain the tower of algebraic extensions

f:L (4) $$E \subseteq E_1 := E(\mathcal{F}_1) \subseteq \ldots \subseteq E_n := E(\mathcal{F}_n) \subseteq \ldots \subseteq E_\infty := \bigcup_n E_n \subseteq \overline{E}\ .$$

Example. Let $E = L = \mathbb{Q}_p$, $\pi = p$, and $\phi(X) = (1+X)^p - 1$ so that $F_\phi = \widehat{\mathbb{G}}_m$. Then

$$\mathcal{F}_n = \{\zeta - 1 : \zeta^{p^n} = 1\} \qquad \text{and} \qquad L_n = L(\{\zeta : \zeta^{p^n} = 1\}) \ .$$

indep **Remark 3.1.** *The extensions E_n and E_∞ only depend on π and not on the choice of ϕ. If E/L is finite then they only depend on $\mathrm{Norm}_{E/L}(\pi)$. If k_E is algebraically closed then they are also independent of the choice of π.*

Proof. Let ψ be a second Frobenius power series for the prime element ϖ and put $\mathcal{F}'_n := \{z \in \mathfrak{M} : \psi_n(z) = 0\}$ and $E'_n := E(\mathcal{F}'_n)$. By Cor. 2.9 (assuming that $\pi = \varpi$), by Cor. 2.13 (assuming that E/L is finite and $\mathrm{Norm}_{E/L}(\pi) = \mathrm{Norm}_{E/L}(\varpi)$), or by Prop. 2.11 (assuming that k_E is algebraically closed) we find a unit $u \in o_E^{\pi,\varpi} \cap o_E^\times$ such that $[u]_{\phi,\psi} : F_\psi \xrightarrow{\cong} F_\phi$ is an isomorphism. The defining condition on the power series $[u]_{\phi,\psi}$ implies inductively that we have

$$\phi_n([u]_{\phi,\psi}(X)) = {}^{\varphi^n}[u]_{\phi,\psi}(\psi_n(X))$$

for any $n \geq 1$. It follows that $[u]_{\phi,\psi}(\mathcal{F}'_n) \subseteq \mathcal{F}_n$. Repeating this argument with the inverse isomorphism $[u^{-1}]_{\psi,\phi}$ we see that we actually have the equality $[u]_{\phi,\psi}(\mathcal{F}'_n) = \mathcal{F}_n$. Since $E(z)$ is complete we have $E([b]_{\phi,\psi}(z)) \subseteq E(z)$ for any $z \in \mathcal{F}'_n$. Hence $E_n \subseteq E'_n$. Again by symmetry we then must have $E_n = E'_n$.
Addendum: Using Prop. 2.8 we see that the bijection $[u]_{\phi,\psi} : \mathcal{F}'_n \xrightarrow{\cong} \mathcal{F}_n$ is an isomorphism of o_L-modules. □

separable **Lemma 3.2.** *For any $z \in \mathfrak{M}$ the polynomial $\pi X + X^q - z$ is separable and its q different zeros again lie in $\mathfrak{M}$.*

Proof. Let $y \in \overline{E}$ be a zero of $\pi X + X^q - z$. If y also is a zero of the derivative $\pi + qX^{q-1}$ then $|y|^{q-1} = |\frac{\pi}{q}| \geq 1$ and hence $|y| \geq 1$. In order to establish the assertion it therefore suffices to prove that the assumption that $|y| \geq 1$ leads to a contradiction. But in this case $|\pi y| < |y| \leq |y^q|$ which would imply $|z| = |\pi y + y^q| = |y^q| \geq 1$. □

free **Proposition 3.3.** *$\mathcal{F}_n$, for any $n \geq 1$, is a free $o_L/\mathfrak{m}_L^n$-module of rank one.*

Proof. Because of the isomorphism in the Addendum to Remark 3.1 it suffices to consider the special Lubin-Tate group law for π. We therefore assume that $\phi(X) = \pi X + X^q$. First of all we observe that it follows from Lemma 3.2 that $\mathcal{F}_n$ has the cardinality $q^n = |o_L/\mathfrak{m}_L^n|$. Consider any element z in the o_L-module $\mathcal{F}_n$. Its annihilator ideal $\{a \in o_L : [a]_\phi(z) = 0\}$ must be of the form $\mathfrak{m}_L^{n_z}$ for some integer $n_z \geq 0$. We have $q^{n_z} = |o_L/\mathfrak{m}_L^{n_z}| \leq |\mathcal{F}_n| = q^n$ and hence $n_z \leq n$. It follows that $\mathcal{F}_n$ is an $o_L/\mathfrak{m}_L^n$-module. Fixing a prime element $\varpi \in o_L$ we, in particular, deduce from this that

$$\mathcal{F}_n \subseteq \{z \in \mathfrak{M} : [\varpi^n]_\phi(z) = 0\}.$$

At this point we invoke the Weierstrass division theorem (cf. [B-CA] VII.3.8 Prop. 5) which implies that the power series $\phi_n(X)$ divides the power series $[\varpi^n]_\phi(X)$ in the ring $o_E[[X]]$, i.e., we find a unique power series $g_n \in o_E[[X]]$ such that $[\varpi^n]_\phi = \phi_n g_n$. It follows that $\varpi^n = \varphi^{n-1}(\pi) \cdots \varphi(\pi)\pi g_n(0)$, which shows that $g_n(0) \in o_E^\times$. Because of this latter property the power series g_n can not have any zeros in $\mathfrak{M}$. We conclude that we have equality $\mathcal{F}_n = \{z \in$

$\mathfrak{M} : [\varpi^n]_\phi(z) = 0\}$. We now pick an element $z_n \in \mathcal{F}_n \setminus \mathcal{F}_{n-1}$ and consider the homomorphism of o_L-modules

$$\begin{aligned} o_L/\mathfrak{m}_L^n o_L &\longrightarrow \mathcal{F}_n \\ a + \mathfrak{m}_L^n &\longmapsto [a]_\phi(z_n) \ . \end{aligned}$$

It is injective since $[\varpi^{n-1}]_\phi(z_n) \neq 0$. But both sides have the same cardinality q^n. So it must be an isomorphism. □

finite-ext **Corollary 3.4.** *E_n/E, for any $n \geq 1$, is a finite separable extension.*

Proof. By Remark 3.1 we may assume that $\phi(X) = \pi X + X^q$. Then, as noted already at the beginning of the proof of Prop. 3.3, the Lemma 3.2 implies that $\mathcal{F}_n$ is the zero set of the separable polynomial ϕ_n of degree q^n. □

Any automorphism $\sigma \in \mathrm{Aut}(\overline{E}/E)$ respects the absolute value of $\overline{E}$. This implies

$$\begin{aligned} &\sigma(F_\phi(z_1, z_2)) = F_\phi(\sigma(z_1), \sigma(z_2)) \qquad \text{for any } z_1, z_2 \in \mathfrak{M}, \\ &\sigma(\phi_n(z)) = \phi_n(\sigma(z)) \qquad \text{for any } n \geq 1 \text{ and any } z \in \mathfrak{M}, \text{ and} \\ &\sigma([a]_\phi(z)) = [a]_\phi(\sigma(z)) \qquad \text{for any } a \in o_L \text{ and any } z \in \mathfrak{M}. \end{aligned}$$

It follows that the group $\mathrm{Aut}(\overline{E}/E)$ acts via

$$\begin{aligned} \mathrm{Aut}(\overline{E}/E) \times \mathcal{F}_n &\longrightarrow \mathcal{F}_n \\ (\sigma, z) &\longmapsto \sigma(z) \end{aligned}$$

$o_L/\mathfrak{m}_L^n$-linearly on $\mathcal{F}_n$. In particular, the extensions E_n/E are Galois. Furthermore, using Prop. 3.3 we see that for any $\sigma \in \mathrm{Gal}(E_n/E)$ there is a unique element $\chi_{E/L,n}(\sigma) \in (o_L/\mathfrak{m}_L^n)^\times$ such that

f:chi-n (5) $$\sigma(z) = [\chi_{E/L,n}(\sigma)]_\phi(z) \qquad \text{for any } z \in \mathcal{F}_n$$

(note that the abuse of notation on the right hand side is justified since $[a]_\phi(z)$ only depends on a mod $\mathfrak{m}_L^n$).

LT-char **Proposition 3.5.** *For any $n \geq 1$ the extension E_n/E is finite Galois and*

$$\chi_{E/L,n} : \mathrm{Gal}(E_n/E) \xrightarrow{\cong} (o_L/\mathfrak{m}_L^n)^\times$$

is an isomorphism of groups. Furthermore, we have:

i. E_n/E is totally ramified of degree $(q-1)q^{n-1}$.

ii. If $z \in \mathcal{F}_n$ is any generator of $\mathcal{F}_n$ as an $o_L/\mathfrak{m}_L^n$-module then:

a) $E_n = E(z)$,

b) z generates the ring of integers o_{E_n} in E_n as an o_E-algebra,

c) z is a prime element of o_{E_n},

d) if $\phi(X) = \pi X + X^q$ then $\mathrm{Norm}_{E_n/E}(-z) = \varphi^{n-1}(\pi)$.

Proof. We have seen already that E_n/E is finite Galois. The multiplicativity of $\chi_{E/L,n}$ is an easy computation which is left to the reader. Any $\sigma \in \ker(\chi_{E/L,n})$ fixes every $z \in \mathcal{F}_n$ and therefore fixes E_n. This shows the injectivity of the map in question. For its surjectivity we note that $o_L^\times/1+\mathfrak{m}_L \cong k_L^\times$ and $1+\mathfrak{m}_L^i/1+\mathfrak{m}_L^{i+1} \cong k_L^+$, for $i \geq 1$, have cardinality $q-1$ and q, respectively. We deduce that $(o_L/\mathfrak{m}_L^n)^\times$ has cardinality $(q-1)q^{n-1}$. It therefore suffices to show that $[E_n : E] = (q-1)q^{n-1}$.

Because of Remark 3.1 we may assume for this that $\phi(X) = \pi X + X^q$. We pick an element $z \in \mathcal{F}_n \setminus \mathcal{F}_{n-1}$, which then is, by Prop. 3.3, a generator of the $o_L/\mathfrak{m}_L^n$-module $\mathcal{F}_n$. Since $E(z) \subseteq E_n$ is complete, it follows that $\mathcal{F}_n \subseteq E(z)$ and hence that $E_n = E(z)$. The element z is a zero of the polynomial ϕ_n but not of ϕ_{n-1} (put $\phi_0(X) := X$). Hence it is a zero of

$$\frac{\phi_n(X)}{\phi_{n-1}(X)} = \frac{{}^{\varphi^{n-1}}\phi(\phi_{n-1}(X))}{\phi_{n-1}(X)} = \frac{\varphi^{n-1}(\pi)\phi_{n-1}(X) + \phi_{n-1}(X)^q}{\phi_{n-1}(X)} = \phi_{n-1}(X)^{q-1} + \varphi^{n-1}(\pi) \ .$$

The congruence

$$\phi_{n-1}(X)^{q-1} + \varphi^{n-1}(\pi) \equiv X^{q^{n-1}(q-1)} \mod \pi o_E[X]$$

shows that z is a zero of an Eisenstein and hence irreducible polynomial of degree $(q-1)q^{n-1}$. We immediately deduce the assertion ii.d). But it also follows (cf. [CF] Chap. I.6 Thm. 1) that E_n/E is totally ramified of degree $(q-1)q^{n-1}$ and that ii.b) and c) hold true.

Going back to a general ϕ we observe that the isomorphism $\mathcal{F}'_n \xrightarrow{\cong} \mathcal{F}_n$ in the Addendum to Remark 3.1 preserves absolute values. This shows that z always is a prime element. Hence ii.a) and b) follow from [CF] Chap. I.6 Thm. 1(ii). □

The isomorphisms $\chi_{E/L,n}$ in Prop. 3.5 fit into the commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(E_{n+1}/E) & \xrightarrow[\cong]{\chi_{E/L,n+1}} & (o_L/\mathfrak{m}_L^{n+1})^\times \\ \Big\downarrow{\scriptstyle \text{restriction}} & & \Big\downarrow{\scriptstyle \text{pr}} \\ \mathrm{Gal}(E_n/E) & \xrightarrow[\cong]{\chi_{E/L,n}} & (o_L/\mathfrak{m}_L^n)^\times. \end{array}$$

By passing to the projective limit with respect to n we therefore obtain the isomorphism

f:LT-char (6) $$\chi_{E/L} : \mathrm{Gal}(E_\infty/E) \xrightarrow{\cong} o_L^\times \ .$$

char-indep **Remark 3.6.** *The isomorphisms $\chi_{E/L,n}$ and $\chi_{E/L}$ have the same independence properties, which were stated in Remark 3.1 for the extensions E_n/E and E_∞/E.*

Proof. We consider the isomorphism $[u]_{\phi,\psi} : \mathcal{F}'_n \xrightarrow{\cong} \mathcal{F}_n$ in the Addendum to Remark 3.1. For $\sigma \in \mathrm{Gal}(E_n/E)$ and $z' \in \mathcal{F}'_n$ we compute

$$\begin{aligned} [u]_{\phi,\psi}(\sigma(z')) &= \sigma([u]_{\phi,\psi}](z')) = [\chi_{L/E,n}(\sigma)]_\phi([u]_{\phi,\psi}(z')) = [\chi_{L/E,n}(\sigma)u]_{\phi,\psi}(z')) \\ &= [u]_{\phi,\psi}([\chi_{E/L,n}(\sigma)]_\psi(z')) \ , \end{aligned}$$

where the second equality uses the characterizing property of $\chi_{E/L,n}$ with respect to $\mathcal{F}_n$. It follows that $\sigma(z') = [\chi_{E/L,n}(\sigma)]_\psi(z')$. This says that $\chi_{E/L,n}$ also satisfies the characterizing property with respect to $\mathcal{F}'_n$. □

The extensions E_n/E have a very explicit higher ramification theory. Let us fix an $n \geq 1$ and abbreviate $\Gamma_n := \mathrm{Gal}(E_n/E)$. We also fix a generator z_n of $\mathcal{F}_n$ as an $o_L/\mathfrak{m}_L^n$-module, which is a prime element of the ring of integers o_{E_n} in E_n by Prop. 3.5.ii.c). For any $i \geq 0$, the ith ramification subgroup of Γ_n is defined to be

$$\Gamma_{n,i} := \{\sigma \in \Gamma_n : \sigma(x) \equiv x \bmod z_n^{i+1} o_{E_n} \text{ for any } x \in o_{E_n}\}.$$

We have $\Gamma_{n,0} = \Gamma_n$, since E_n/E is totally ramified by Prop. 3.5.i, and

:ram-subgroup (7) $$\Gamma_{n,i} = \{\sigma \in \Gamma_n : \sigma(z_n) - z_n \in z_n^{i+1} o_{E_n}\}$$

by Prop. 3.5.ii.b).

lower-ram **Proposition 3.7.** *i.* $\Gamma_{n,0} = \Gamma_n = \mathrm{Gal}(E_n/E)$ *and* $\Gamma_{n,1} = \mathrm{Gal}(E_n/E_1)$.

ii. For $1 \leq m \leq n$ *and* $q^{m-1} \leq i < q^m$ *we have* $\Gamma_{n,i} = \mathrm{Gal}(E_n/E_m)$.

iii. For $i \geq q^{n-1}$ *we have* $\Gamma_{n,i} = 1$.

Proof. i. We already have observed the first part of the assertion. For the second part we recall that, quite generally, $\Gamma_{n,1}$ is a p-group whereas the index $[\Gamma_{n,0} : \Gamma_{n,1}]$ is prime to p (cf. [Ser] IV§2 Cor.s 1 and 3). Using Prop. 3.5.i we then see that necessarily $\Gamma_{n,1} = \mathrm{Gal}(E_n/E_1)$.

ii. and iii. Let $1 \neq \sigma \in \Gamma_{n,1}$ be any element, and let $1 \leq m = m(\sigma) < n$ denote the maximal integer such that $\sigma \in \mathrm{Gal}(E_n/E_m)$. Using Prop. 3.5.ii.b) and c) we see that $z_m := [\pi]_\phi^{n-m}(z_n)$ is a prime element of o_{E_m} and that m is maximal such that $\sigma(z_m) = z_m$. It follows that $[\pi]_\phi^{n-m}(\sigma(z_n)) = \sigma([\pi]_\phi^{n-m}(z_n)) = \sigma(z_m) = z_m$ and hence that

$$\sigma(z_n) = F_\phi(z_n, \tilde{z}_{n-m}) = z_n + \tilde{z}_{n-m} + \sum_{r,s \geq 1} c_{r,s} z_n^r \tilde{z}_{n-m}^s$$

for some generator $\tilde{z}_{n-m}$ of $\mathcal{F}_{n-m}$ and elements $c_{r,s} \in o_E$. The generator $\tilde{z}_{n-m}$ is a prime element of $o_{E_{n-m}}$ and therefore lies in $z_n^{q^m} o_{E_n}$. It follows that

$$\sigma(z_n) - z_n \in z_n^{q^m} o_{E_n} \setminus z_n^{q^m+1} o_{E_n} \ .$$

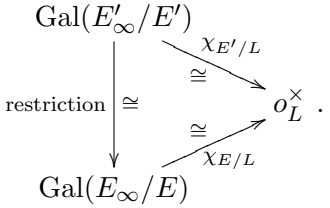
Using (7) we deduce that $\sigma \in \Gamma_{n,q^m-1} \setminus \Gamma_{n,q^m}$, or equivalently, that $\sigma \in \Gamma_{n,i}$ if and only if $i < q^{m(\sigma)}$. It immediately follows that $\Gamma_{n,q^{n-1}} = 1$. Moreover, if $1 \leq q^{m'-1} \leq i < q^{m'} \leq q^{n-1}$ then we obtain (with the convention that $m(1) = n$)

$$\Gamma_{n,i} = \{\sigma \in \Gamma_{n,1} : m(\sigma) \geq m'\} = \mathrm{Gal}(E_n/E_{m'}) \ .$$

□

let $L \subseteq E_0 \subseteq E_0'$ be two unramified extensions with completions $E \subseteq E'$. Since the automorphism φ of E' restricts to the automorphism φ of E, our Lubin-Tate group law F_ϕ for the prime element π over o_E also is a Lubin-Tate group law over $o_{E'}$ (for the same prime element). Hence we have the corresponding totally ramified Galois extension E'_∞/E' and the homomorphism $\chi_{E'/L}$. The following assertion is straightforward.

rem:base **Remark 3.8.** *We have* $E'_\infty = E_\infty E'$ *together with the commutative diagram of isomorphisms*



4 The Coleman norm operator

sec:Coleman

Again we keep the setting and the notations of the previous two sections.

Remark. In the following we will use systematically the fact that the procedure of inserting a power series with a constant coefficient in $\mathfrak{m}_E$ into another power series is well defined. Let $f(X) = \sum_{i=0}^{\infty} c_i X^i$ be an arbitrary power series in $o_E[[X]]$ and let $g(X) \in \pi o_E[[X]] + X o_E[[X]]$. The binomial formula implies that $g(X)^{2i} \in \pi^i o_E[[X]] + X^i o_E[[X]]$ for any $i \geq 0$. Choose $h_i, \tilde{h}_i \in o_E[[X]]$ such that $c_{2i} g(X)^{2i} + c_{2i+1} g(X)^{2i+1} = \pi^i h_i(X) + X^i \tilde{h}_i(X)$. We obtain

$$f(X) = \sum_{i=0}^{\infty} \pi^i h_i(X) + \sum_{i=0}^{\infty} X^i \tilde{h}_i(X) \ .$$

The left sum converges coefficientwise and the right sum exists algebraically.

bij **Lemma 4.1.** *The map*

$$\begin{aligned} o_E[[X]] &\xrightarrow{\cong} \{g \in o_E[[X]] : g(F(X,z)) = g(X) \text{ for any } z \in \mathcal{F}_1\} \\ f(X) &\longmapsto f(\phi(X)) \end{aligned}$$

is bijective.

Proof. Since $f(\phi(F(X,z))) = f({}^{\varphi}F(\phi(X), \phi(z))) = f({}^{\varphi}F(\phi(X), 0)) = f(\phi(X))$ for $z \in \mathcal{F}_1$, the map is well defined.

For its injectivity it suffices to show this injectivity in $o_E/\pi^n o_E[[X]]$ for any $n \geq 1$. For $n = 1$ the map becomes $f(X) \mapsto f(X^q)$ whose injectivity is obvious. By induction we assume that we know the injectivity already for some n. We now show the injectivity for $n+1$. Suppose that $f(\phi(X)) = \pi^{n+1} g(X)$. The induction hypothesis implies that $f = \pi^n f'$ and hence that $f'(\phi(X)) = \pi g(X)$. The injectivity for $n = 1$ then says that $f' = \pi f''$ and hence that $f = \pi^{n+1} f''$.

For the surjectivity let $g_0 := g$ be any power series in the right hand side. Then $g(0) = g(F(0,z)) = g(z)$ for any $z \in \mathcal{F}_1$. We see that $\mathcal{F}_1$ lies in the zero set of $g(X) - g(0)$. So, again by the Weierstrass division theorem (note that ϕ has reduced order q in the sense of [B-CA] VII.3.8), we find a power series $g_1 \in o_E[[X]]$ such that $g - g(0) = \phi \cdot g_1$. Since $\phi(F(X,z)) = \phi(z)$ (cf. the beginning of the proof) we must have $g_1(F(X,z)) = g_1(X)$ for any $z \in \mathcal{F}_1$ as well. Repeating this reasoning for g_1 we find inductively a sequence of power series $g_i \in o_E[[X]]$ such that

$$g_i(X) - g_i(0) = g_{i+1}(X) \cdot \phi(X) \qquad \text{for any } i \geq 0.$$

We deduce that

$$g(X) = \sum_{i=0}^{\infty} g_i(0) \phi(X)^i$$

and, setting $f(X) := \sum_{i=0}^{\infty} g_i(0) X^i$, that $g(X) = f(\phi(X))$. □

Consider any power series $g \in o_E[[X]]$ and define

$$\tilde{g}(X) := \prod_{z \in \mathcal{F}_1} g(F(X,z)) \ .$$

Each factor is a power series in $o_{E_1}[[X]]$. But the coefficients of their product $\tilde{g}(X)$ are fixed by the Galois group $\mathrm{Gal}(E_1/E)$ which permutes the $z \in \mathcal{F}_1$. We see that $\tilde{g} \in o_E[[X]]$. For any $y \in \mathcal{F}_1$ we compute

$$\begin{aligned}\tilde{g}(F(X,z)) &= \prod_{z\in\mathcal{F}_1} g(F(F(X,y),z)) \\ &= \prod_{z\in\mathcal{F}_1} g(F(X,y+_F z)) = \prod_{z\in\mathcal{F}_1} g(F(X,z)) \\ &= \tilde{g}(X)\ .\end{aligned}$$

This shows that $\tilde{g}$ lies in the right hand side of the bijection in Lemma 4.1. Hence there is a unique power series $\mathcal{N}(g) \in o_E[[X]]$ such that $\mathcal{N}(g)(\phi(X)) = \tilde{g}(X)$. This defines a map

$$\mathcal{N}(g) : o_E[[X]] \longrightarrow o_E[[X]]\ ,$$

which called the Coleman norm operator. By construction this map is multiplicative, i.e., we have

$$\mathcal{N}(g_1 g_2) = \mathcal{N}(g_1)\mathcal{N}(g_2) \qquad \text{for any } g_1, g_2 \in o_E[[X]].$$

For a constant $c \in o_E$ we have $\mathcal{N}(c) = c^q$. In particular, $\mathcal{N}$ restricts to a homomorphism $o_E[[X]]^\times \to o_E[[X]]^\times$.

Example. The computation $\mathcal{N}(\phi)(\phi(X)) = \prod_{z\in\mathcal{F}_1} \phi(F(X,z)) = \prod_{z\in\mathcal{F}_1} {}^{\varphi}F(\phi(X),\phi(z)) = \phi(X)^q$ shows that $\mathcal{N}(\phi) = X^q$.

We put $\mathcal{N}^{(0)} := \mathrm{id}$ and, for any $n \geq 1$, we define inductively the maps

$$\mathcal{N}^{(n)}(g) := {}^{\varphi}(\mathcal{N}^{(n-1)}({}^{\varphi^{-1}}(\mathcal{N}(g)))) \qquad \text{for } g \in o_E[[X]].$$

In particular, $\mathcal{N}^{(1)} = \mathcal{N}$. Each $\mathcal{N}^{(n)}$ restricts to an endomorphism of $o_E[[X]]^\times$.

In the following we choose and fix, for technical convenience, an extension of the automorphism φ of E/L to an automorphism of $\overline{E}$ which, for simplicity, also will be denoted by φ.

exact-seq **Lemma 4.2.** *We have, for any $n \geq 1$, the exact sequence of o_L-modules.*

$$0 \longrightarrow \mathcal{F}_1 \xrightarrow{\subseteq} \mathcal{F}_{n+1} \xrightarrow{z\mapsto\varphi^{-1}(\phi(z))} \mathcal{F}_n \longrightarrow 0\ .$$

Proof. First of all we check that the map $z \mapsto \varphi^{-1}(\phi(z))$ is well defined. Let $z \in \mathcal{F}_{n+1}$. By the definition of ϕ_{n+1} we have $0 = \phi_{n+1}(z) = {}^{\varphi}\phi_n(\phi(z))$. Hence $\phi(z)$ is a zero of ${}^{\varphi}\phi_n(X)$ in $\mathfrak{m}_{E_{n+1}}$. In particular, the element $\varphi^{-1}(\phi(z))$ is well defined in $\overline{E}$. But it also follows that $\varphi^{-1}(\phi(z))$ is a zero of $\phi_{n+1}(X)$ and hence lies in $\mathcal{F}_n$.

Since $\phi : F \to {}^{\varphi}F$ is a homomorphism we obtain

$$\begin{aligned}\phi(y+_F z) &= {}^{\varphi}F(\phi(y),\phi(z)) = \varphi(F(\varphi^{-1}(\phi(y)),\varphi^{-1}(\phi(z)))) \\ &= \varphi(\varphi^{-1}(\phi(y)) +_F \varphi^{-1}(\phi(z)))\ .\end{aligned}$$

Hence our map $z \mapsto \varphi^{-1}(\phi(z))$ is a homomorphism of abelian groups. Its kernel obviously is $\mathcal{F}_1$. By comparing cardinalities (cf. Prop. 3.3) we see that it is surjective. Finally we compute

$$[a]_\phi(\varphi^{-1}(\phi(z))) = \varphi^{-1}({}^{\varphi}[a]_\phi(\phi(z))) = \varphi^{-1}(\phi([a]_\phi(z)))$$

for any $a \in o_L$. Hence our map is o_L-linear. □

N-n **Proposition 4.3.** *For any $n \geq 1$ and any $g \in o_E[[X]]$ we have*

$$\mathcal{N}^{(n)}(g)(\phi_n) = \prod_{z \in \mathcal{F}_n} g(F(X,z)) \ .$$

Proof. We argue by induction with respect to n. In case $n = 1$ the assertion is the defining equality for $\mathcal{N}(g)$. Suppose that we have shown the assertion for some $n \geq 1$. Let $R \subseteq \mathcal{F}_{n+1}$ be a set of representatives for the cosets in $\mathcal{F}_{n+1}/\mathcal{F}_1$. We note that, by Lemma 4.2, the map $z \mapsto \varphi^{-1}(\phi(z))$ restricts to a bijection $R \xrightarrow{\sim} \mathcal{F}_n$; this will be subsequently used in the fifth equality. We now compute

$$\begin{aligned}
\prod_{z \in \mathcal{F}_{n+1}} g(F(X,z)) &= \prod_{z \in R} \prod_{y \in \mathcal{F}_1} g(F(X, z +_F y)) = \prod_{z \in R} \prod_{z \in \mathcal{F}_1} g(F(F(X,z),y)) \\
&= \prod_{z \in R} \mathcal{N}(g)(\phi(F(X,z))) = \prod_{z \in R} \mathcal{N}(g)({}^{\varphi}F(\phi(X),\phi(z))) \\
&= \prod_{z \in \mathcal{F}_n} \mathcal{N}(g)({}^{\varphi}F(\phi(X),\varphi(z))) = \prod_{z \in \mathcal{F}_n} \mathcal{N}(g)({}^{\varphi}(F({}^{\varphi^{-1}}\phi(X),z))) \\
&= {}^{\varphi}\Big(\prod_{z \in \mathcal{F}_n} {}^{\varphi^{-1}}(\mathcal{N}(g))(F({}^{\varphi^{-1}}\phi(X),z)) \Big) \\
&= {}^{\varphi}\Big(\mathcal{N}^{(n)}({}^{\varphi^{-1}}(\mathcal{N}(g)))(\phi_n({}^{\varphi^{-1}}\phi(X))) \Big) \\
&= \mathcal{N}^{(n+1)}(g)({}^{\varphi}(\phi_n({}^{\varphi^{-1}}\phi(X)))) = \mathcal{N}^{(n+1)}(g)({}^{\varphi}\phi_n(\phi(X))) \\
&= \mathcal{N}^{(n+1)}(g)(\phi_{n+1}(X)) \ .
\end{aligned}$$

In the eighth equality we have used the induction hypothesis. □

N-properties **Lemma 4.4.** *For any $g \in o_E[[X]]$ and any $n \geq 1$ we have:*

i. $\mathcal{N}(g) \equiv {}^{\varphi}g \bmod \pi o_E[[X]]$*;*

ii. if $g \equiv 1 \bmod \pi^n o_E[[X]]$ *then* $\mathcal{N}^{(j)}(g) \equiv 1 \bmod \pi^{n+j} o_E[[X]]$ *for any* $j \geq 0$*;*

iii. if $g \in o_E[[X]]^{\times}$ *then* $\frac{\mathcal{N}^{(n)}(g)}{{}^{\varphi}(\mathcal{N}^{(n-1)}(g))} \equiv 1 \bmod \pi^n o_E[[X]]$.

Proof. i. Since $\mathcal{F}_1 \subseteq \mathfrak{m}_{E_1}$ we have $\mathcal{N}(g)(X^q) \equiv \mathcal{N}(g)(\phi(X)) \equiv \prod_{z \in \mathcal{F}_1} g(F(X,0)) \equiv g(X)^q \equiv {}^{\varphi}g(X^q) \bmod \mathfrak{m}_{E_1} o_{E_1}[[X]]$. Hence $\mathcal{N}(g)(X^q) \equiv {}^{\varphi}g(X^q) \bmod \pi o_E[[X]]$.

ii. Write $g = 1 + \pi^n h$ with $h \in o_E[[X]]$. Then

$$\begin{aligned}
\mathcal{N}(g)(\phi(X)) &= \prod_{z \in \mathcal{F}_1} (1 + \pi^n h(F(X,z))) \equiv (1 + \pi^n h(X))^q \\
&\equiv \sum_{j=0}^{q} \binom{q}{j} \pi^{jn} h(X)^j \equiv 1 \mod \pi^n \mathfrak{m}_{E_1} o_{E_1}[[X]] \ .
\end{aligned}$$

Hence $(\mathcal{N}(g) - 1)(\phi(X)) \in \pi^n \mathfrak{m}_{E_1} o_{E_1}[[X]] \cap o_E[[X]] = \pi^{n+1} o_E[[X]]$. But the injectivity part of Lemma 4.1 was shown modulo each $\pi^n o_E[[X]]$. It follows that $\mathcal{N}(g) - 1 \in \pi^{n+1} o_E[[X]]$. A simple induction with respect to j gives the assertion in general.

iii. From i. we have $\frac{\mathcal{N}(g)}{\varphi g} \equiv 1 \bmod \pi o_E[[X]]$, which is the case $n = 1$ of the assertion. Moreover, by applying ii. to $\frac{\varphi^{-1}(\mathcal{N}(g))}{g} \equiv 1 \bmod \pi o_E[[X]]$ and $j = n-1$ we obtain

$$\frac{\varphi^{-1}(\mathcal{N}^{(n)}(g))}{\mathcal{N}^{(n-1)}(g)} = \frac{\mathcal{N}^{(n-1)}(\varphi^{-1}(\mathcal{N}(g))}{\mathcal{N}^{(n-1)}(g)} = \mathcal{N}^{(n-1)}(\frac{\varphi^{-1}(\mathcal{N}(g))}{g}) \equiv 1 \bmod \pi^n o_E[[X]] \ ,$$

which is equivalent to the assertion. □

5 Local class field theory

sec:LCFT

As before we fix a local field L with ring of integers o_L, maximal ideal $\mathfrak{m}_L$ and residue field k_L of characteristic $p > 0$. Let $q := |k_L|$ and let $v_L : L^\times \twoheadrightarrow \mathbb{Z}$ denote the normalized discrete valuation of L.

5.1 Norm groups

c:norm-groups

In this section we let E/L be a finite unramified extension of degree d with ring of integers o_E, maximal ideal $\mathfrak{m}_E$, residue field k_E, and normalized discrete valuation $v_E : E^\times \twoheadrightarrow \mathbb{Z}$. The Galois group $\mathrm{Gal}(E/L)$ is generated by the Frobenius automorphism $\varphi = \varphi_L$, which modulo $\mathfrak{m}_E$ is the qth-power map.

norm-surj

Lemma 5.1. *i. The trace map* $\mathrm{Trace}_{k_E/k_L} : k_E \longrightarrow k_L$ *is surjective.*

ii. The norm map $\mathrm{Norm}_{k_E/k_L} : k_E^\times \longrightarrow k_L^\times$ *is surjective.*

Proof. i. The trace map is k_L-linear. Hence it suffices to show that it is nonzero. Otherwise we have

$$0 = \sum_{\sigma \in \mathrm{Gal}(k_E/k_L)} \sigma(a) = a + a^q + \ldots + a^{q^{d-1}} \qquad \text{for any } a \in k_E.$$

Hence all q^d elements of k_E are zeros of the polynomial $X + X^q + \ldots + X^{q^{d-1}}$ of degree q^{d-1}. This is a contradiction.

ii. We have

$$\mathrm{Norm}_{k_E/k_L}(a) = a \cdot a^q \cdots a^{q^{d-1}} = a^{1+q+\ldots+q^{d-1}} = a^{\frac{q^d-1}{q-1}} \qquad \text{for any } a \in k_E.$$

Obviously the map

$$k_E^\times \cong \mathbb{Z}/(q^d-1)\mathbb{Z} \xrightarrow{\frac{q^d-1}{q-1}\cdot} \mathbb{Z}/(q-1)\mathbb{Z} \cong k_L^\times$$

is surjective. □

norm-surj-2

Proposition 5.2. *The norm map* $\mathrm{Norm}_{E/L} : o_E^\times \longrightarrow o_L^\times$ *is surjective.*

Proof. Let $y \in o_L^\times$. We construct inductively a sequence $(x_i)_{i \geq 1}$ in $o_E^\times$ such that

$$\mathrm{Norm}_{E/L}(x_i) - y \in \mathfrak{m}_L^i \quad \text{and} \quad x_{i+1} - x_i \in \mathfrak{m}_E^i$$

for any $i \geq 1$. The right hand condition says that $(x_i)_i$ is a Cauchy sequence and therefore converges to some $x \in o_E^\times$. The norm is a product of continuous Galois automorphisms and therefore is continuous. Hence

$$\mathrm{Norm}_{E/L}(x) - y = \lim_{i\to\infty} \mathrm{Norm}_{E/L}(x_i) - y = 0 \ ,$$

where the latter equality follows from the left hand condition.

Since Galois automorphisms preserve absolute values the norm map satisfies $\mathrm{Norm}_{E/L}(1+\mathfrak{m}_E^i) \subseteq (1+\mathfrak{m}_E^i) \cap o_L = 1+\mathfrak{m}_L^i$. It induces the norm map

$$\mathrm{Norm}_{k_E/k_L} : k_E^\times = o_E^\times/1+\mathfrak{m}_E \longrightarrow o_L^\times/1+\mathfrak{m}_L = k_L^\times$$

as well as homomorphisms

$$\mathrm{Norm} : (1+\mathfrak{m}_E^i)/(1+\mathfrak{m}_E^{i+1}) \longrightarrow (1+\mathfrak{m}_L^i)/(1+\mathfrak{m}_L^{i+1})$$

for any $i \geq 1$. The first one is surjective by Lemma 5.1.ii. Hence we find an element $x_1 \in o_E^\times$ such that $\mathrm{Norm}_{E/L}(x_1) \in y(1+\mathfrak{m}_L) \subseteq y+\mathfrak{m}_L$. Suppose that $x_i \in o_E^\times$, for some $i \geq 1$, has been constructed. Then $\frac{y}{\mathrm{Norm}_{E/L}(x_i)} \in 1+\mathfrak{m}_L^i$. Let ϖ be prime element in o_L and hence in o_E. We have the commutative diagram

$$\begin{array}{ccc} (1+\mathfrak{m}_E^i)/(1+\mathfrak{m}_E^{i+1}) & \xrightarrow{\cong} & k_E \\ \Big\downarrow{\scriptstyle \mathrm{Norm}} & & \Big\downarrow{\scriptstyle \mathrm{Trace}_{k_E/k_L}} \\ (1+\mathfrak{m}_L^i)/(1+\mathfrak{m}_L^{i+1}) & \xrightarrow{\cong} & k_L, \end{array}$$

where the horizontal isomorphisms are given by $1+\varpi^i a \longleftrightarrow a$. Since the right hand trace map is surjective by Lemma 5.1.i we find an $x'_{i+1} \in 1+\mathfrak{m}_E^i$ such that $\mathrm{Norm}_{E/L}(x'_{i+1}) \in \frac{y}{\mathrm{Norm}_{E/L}(x_i)}(1+\mathfrak{m}_L^{i+1})$. We put $x_{i+1} := x'_{i+1}x_i$. Then

$$x_{i+1} \in x_i + \mathfrak{m}_E^i \qquad \text{and} \qquad \mathrm{Norm}_{E/L}(x_{i+1}) \in y + \mathfrak{m}_L^{i+1} \ .$$

□

norm-unr **Corollary 5.3.** $\mathrm{Norm}_{E/L}(E^\times) = v_L^{-1}(d\mathbb{Z})$.

Proof. If ϖ is a prime element in o_L then, by Prop. 5.2, we have

$$\mathrm{Norm}_{E/L}(E^\times) = \mathrm{Norm}_{E/L}(o_E^\times) \cdot \mathrm{Norm}_{E/L}(\varpi)^{\mathbb{Z}} = o_L^\times \varpi^{d\mathbb{Z}} \ .$$

□

We choose a prime element π of o_E together with a Frobenius power series ϕ for π. As before $F = F_\phi$ denotes the corresponding Lubin-Tate group law. We use the same notations as in sections 2 and 3 for the objects F gives rise to, most importantly the o_L-modules $\mathcal{F}_n$ and the totally ramified extensions E_n/E.

norm-En **Proposition 5.4.** $\mathrm{Norm}_{E_n/L}(E_n^\times) \subseteq (1+\mathfrak{m}_L^n)\,\mathrm{Norm}_{E_n/L}(\pi)$ *for any* $n \geq 1$.

Proof. By Remark 3.1 we may assume that F is the special Lubin-Tate group law of π. Let z_n be a generator of the o_L-module $\mathcal{F}_n$. From Prop. 3.5.ii we know:

1. z_n is a prime element in o_{E_n} with $\mathrm{Norm}_{E_n/E}(-z_n) = \varphi^{d-1}(\pi)$. In particular,

$$\mathrm{Norm}_{E_n/L}(-z_n) = \mathrm{Norm}_{E/L}(\varphi^{d-1}(\pi)) = \mathrm{Norm}_{E/L}(\pi) \ .$$

2. Any element in o_{E_n} is of the form $g(z_n)$ for some polynomial $g(X) \in o_E[X]$.

By 1. it suffices for our assertion to show that $\mathrm{Norm}_{E_n/L}(o_{E_n}^\times) \subseteq 1 + \mathfrak{m}_L^n$. Let therefore $x \in o_{E_n}^\times$ be any element. By 2. we have $x = g(z_n)$ for some $g(X) \in o_E[X]$. Since $g(0) \neq 0$ we have $g(X) \in o_E[[X]]^\times$. We therefore may use the Coleman norm operator in order to define $x_i := \mathcal{N}^{(i)}(g)(0) \in o_E^\times$ for any $i \geq 0$. Prop. 4.3 tells us that

$$x_i = \prod_{z \in \mathcal{F}_i} g(z) \ .$$

We compute

$$\begin{aligned} \mathrm{Norm}_{E_n/E}(x) &= \prod_{\sigma \in \mathrm{Gal}(E_n/E)} \sigma(g(z_n)) = \prod_\sigma g(\sigma(z_n)) \\ &= \prod_{z \in \mathcal{F}_n \setminus \mathcal{F}_{n-1}} g(z) = \frac{x_n}{x_{n-1}} \ . \end{aligned}$$

Moreover, Lemma 4.4.iii implies $\frac{x_n}{\varphi(x_{n-1})} \in 1 + \mathfrak{m}_E^n$. We conclude that

$$\begin{aligned} \mathrm{Norm}_{E_n/L}(x) &= \mathrm{Norm}_{E/L}(\frac{x_n}{x_{n-1}}) = \mathrm{Norm}_{E/L}(\frac{x_n}{\varphi(x_{n-1})}) \\ &\in \mathrm{Norm}_{E/L}(1 + \mathfrak{m}_E^n) \cap o_L \subseteq (1 + \mathfrak{m}_E^n) \cap o_L = 1 + \mathfrak{m}_L^n \ . \end{aligned}$$

□

norm-closed **Lemma 5.5.** *For any finite extension E'/E the subgroup $\mathrm{Norm}_{E'/E}(E'^\times)$ is closed in $E^\times$.*

Proof. We observe that, for any element $a \in E^\times$ with $v_E(a) = m$, the subgroup $o_E^\times a^{\mathbb{Z}} = v_E^{-1}(m\mathbb{Z})$ is open and hence closed in $E^\times$. We apply this to $a := \mathrm{Norm}_{E'/E}(\pi')$ for some prime element π' of $o_{E'}$. Then

$$\mathrm{Norm}_{E'/E}(E'^\times) = \mathrm{Norm}_{E'/E}(o_{E'}^\times) \times a^{\mathbb{Z}} \subseteq o_E^\times \times a^{\mathbb{Z}} \ .$$

But $\mathrm{Norm}_{E'/E}(o_{E'}^\times)$ is compact since $o_{E'}^\times$ is compact and the norm is continuous. □

norm-ramified **Corollary 5.6.** *Let $\tilde{E}/E$ be a totally ramified algebraic extension which contains E_∞, and let $\mathcal{E}(\tilde{E}/L)$ denote the set of all intermediate extensions $L \subseteq L' \subseteq \tilde{E}$ which are finite over L. We then have*

$$\bigcap_{L' \in \mathcal{E}(\tilde{E}/L)} \mathrm{Norm}_{L'/L}(L'^\times) = \mathrm{Norm}_{E/L}(\pi)^{\mathbb{Z}} \ .$$

Proof. Let us abbreviate $N(\tilde{E}/L) := \bigcap_{L' \in \mathcal{E}(\tilde{E}/L)} \mathrm{Norm}_{L'/L}(L'^\times)$. Since obviously $N(\tilde{E}/L) \subseteq N(E_\infty/L) \subseteq \bigcap_{n \geq 1} \mathrm{Norm}_{E_n/L}(E_n^\times)$ it follows from Prop. 5.4 that the left hand side of the asserted equality is contained in the right hand side. Since $\mathrm{Norm}_{E/L}(\pi)$ is the only element in the right hand side of discrete valuation d it suffices for the reverse inclusion to show

that the left hand side contains some element of discrete valuation d. Using the equality $v_L \circ \mathrm{Norm}_{E/L} = d \cdot v_E$ this clearly reduces further to the following statement:

Let $\tilde{E}/E$ be any totally ramified algebraic extension; then $v_E^{-1}(1) \cap N(\tilde{E}/E) \neq \emptyset$.

We have $v_E^{-1}(1) = \pi o_E^\times$, which is compact. Each intersection $\pi o_E^\times \cap \mathrm{Norm}_{E'/E}(E'^\times)$, for $E' \in \mathcal{E}(\tilde{E}/E)$, is a closed subset of $\pi o_E^\times$ by Lemma 5.5. Hence it suffices to show that finite intersections $\pi o_E^\times \cap \mathrm{Norm}_{E_1'/E}(E_1'^\times) \cap \ldots \cap \mathrm{Norm}_{E_r'/E}(E_r'^\times)$ are nonempty. But the intersection of finitely many norm subgroups $\mathrm{Norm}_{E_j'/E}(E_j'^\times)$ contains the norm subgroup $\mathrm{Norm}_{E'/E}(E'^\times)$ of the composite $E' := E_1' \cdots E_r'$. The intersection $\pi o_E^\times \cap \mathrm{Norm}_{E'/E}(E'^\times)$ contains the norm of a prime element of $o_{E'}$, which is a prime element of o_E since E'/E is totally ramified. □

5.2 The reciprocity map

c:reciprocity

In the following all algebraic extensions of L are considered in a fixed algebraic closure $\overline{L}$ of L. First of all there is the maximal unramified extension L^{ur}/L. Its Galois group $\mathrm{Gal}(L^{ur}/L) \cong \hat{\mathbb{Z}}$ is topologically generated by the Frobenius automorphism $\varphi = \varphi_L$. Let $\widehat{L^{ur}}$ denote the completion of L^{ur} (taken inside the completion of $\overline{L}$), to which φ extends by continuity.

completion

Lemma 5.7. $\widehat{L^{ur}} \cap \overline{L} = L^{ur}$.

Proof. The discrete valuation v_L of L extends to the discrete valuation of $\widehat{L^{ur}}$, which we therefore also denote by v_L. Suppose now that $y \in \widehat{L^{ur}} \setminus L^{ur}$ is algebraic over L^{ur}. Then y is algebraic over some finite unramified extension L' of L. The finite extension $L'(y)/L'$ cannot be unramified since it is not contained in L^{ur}. Therefore its ramification index e satisfies $e > 1$, and we have $v_L(L'^\times) = \frac{1}{e}\mathbb{Z}$. But on the other hand $v_L(L'^\times) \subseteq v_L(\widehat{L^{ur}}^\times) = \mathbb{Z}$. This is a contradiction. □

Next we consider a nonzero element $x \in \mathfrak{m}_L$, let $d := v_L(x)$, and denote by $E = L_0^{(x)}$ the unramified extension of L of degree d. The Galois group $\mathrm{Gal}(L_0^{(x)}/L)$ is the unique quotient of order d of $\mathrm{Gal}(L^{ur}/L)$. According to Cor. 5.3 there is a prime element π of o_E such that $\mathrm{Norm}_{E/L}(\pi) = x$. We choose a Frobenius power series ϕ for π and then have the corresponding Lubin-Tate group law $F = F_\phi$ with its o_L -modules $\mathcal{F}_n = \{z \in \mathfrak{M} : \phi_n(z) = 0\}$. By Cor. 2.13 the extensions

$$L_n^{(x)} := E = E(\mathcal{F}_n) \quad \text{for } n \geq 1 \text{ and} \quad L_\infty^{(x)} := \bigcup_{n \geq 1} L_n^{(x)} = E_\infty$$

only depend on the element x. They are totally ramified over $E = L_0^{(x)}$ by Prop. 3.5.i. In particular, we have $L_\infty^{(x)} \cap L^{ur} = L_0^{(x)}$. From Prop. 3.5 we also know that $L_\infty^{(x)}/L_0^{(x)}$ is Galois with the isomorphism

$$\chi_{L,x} := \chi_{E/L} : \mathrm{Gal}(L_\infty^{(x)}/L_0^{(x)}) \xrightarrow{\cong} o_L^\times \ .$$

Again, by Remark 3.6, this isomorphism depends at most on x.

Galois

Proposition 5.8. *i. The extension $L_\infty^{(x)}/L$ is Galois.*

ii. The field $L^{LT} := L_\infty^{(x)} L^{ur}$, which is a Galois extension of L, does not depend on the choice of x.

Proof. i. We already know from Cor. 3.4 that the extension in question is separable. Let σ now be any automorphism of the separable algebraic closure of L. Then $\sigma(E) = E$ and hence $\sigma|E = \varphi^m$ for some $m \geq 0$. We see that ${}^\sigma\phi$ is a Frobenius power series for the prime element $\sigma(\pi)$ and $F_{{}^\sigma\phi} = {}^\sigma(F_\phi)$ and $({}^\sigma\phi)_n = {}^\sigma(\phi_n)$ for any $n \geq 0$. Hence

$$\sigma(\mathcal{F}_n) = \sigma(\{z : \phi_n(z) = 0\}) = \{z : ({}^\sigma\phi)_n(z) = 0\} =: \mathcal{F}'_n \ .$$

Since $\mathrm{Norm}_{E/L}(\sigma(\pi)) = \mathrm{Norm}_{E/L}(\pi)$ we conclude from Remark 3.1 that

$$E_n = E(\mathcal{F}_n) = E(\mathcal{F}'_n) = E(\sigma(\mathcal{F}_n)) = \sigma(E(\mathcal{F}_n)) = \sigma(E_n) \ .$$

This shows that the E_n/L and hence E_∞/L are Galois.

ii. For any $n \geq 1$ the composite $L_n^{(x)}\widehat{L^{ur}}$ is a finite extension of $\widehat{L^{ur}}$ and hence is complete. Therefore, the completion of $L_n^{(x)}L^{ur}$ on the one hand is contained in $L_n^{(x)}\widehat{L^{ur}}$, but on the other hand also contains this latter field. We see that $L_n^{(x)}\widehat{L^{ur}}$ is the completion of $L_n^{(x)}L^{ur}$. Since $L_n^{(x)}L^{ur}$ is the maximal unramified extension of $L_n^{(x)}$ we may apply Lemma 5.7 for the base field $L_n^{(x)}$ and obtain that

$$L_n^{(x)}\widehat{L^{ur}} \cap \overline{L} = L_n^{(x)}L^{ur} \ .$$

View the two Lubin-Tate group laws used for x and y, respectively, over the ring of integers in $\widehat{L^{ur}}$. Remark 3.1 tells us that $L_n^{(x)}\widehat{L^{ur}} = L_n^{(y)}\widehat{L^{ur}}$ for any $n \geq 1$. The above equation then implies that $L_n^{(x)}L^{ur} = L_n^{(y)}L^{ur}$. □

We now introduce the injective "reciprocity" homomorphism

$$\begin{aligned} rec_{L,x} : v_L^{-1}(d\mathbb{Z}) = o_L^\times x^{\mathbb{Z}} &\longrightarrow \mathrm{Gal}(L_\infty^{(x)}/L_0^{(x)}) \times \mathrm{Gal}(L^{ur}/L_0^{(x)}) = \mathrm{Gal}(L_\infty^{(x)}L^{ur}/L_0^{(x)}) \\ &\qquad\qquad \subseteq \mathrm{Gal}(L^{LT}/L) \\ ux^j &\longmapsto (\chi_{L,x}^{-1}(u), \varphi_L^{-dj}) \ . \end{aligned}$$

compatibility

Theorem 5.9. *For any nonzero elements $x, y \in \mathfrak{m}_L$ such that $v_L(y)$ divides $d := v_L(x)$ we have*

$$rec_{L,y}|v_L^{-1}(d\mathbb{Z}) = rec_{L,x} \ .$$

Proof. First we consider the case where $d = v_L(x) = v_L(y)$. Then $E := L_0^{(x)} = L_0^{(y)}$ and $E^{max} = \widehat{L^{ur}}$ in earlier notation. Let ϖ be a prime element of o_E such that $\mathrm{Norm}_{E/L}(\varpi) = y$ and choose a Frobenius power series ψ for ϖ with the corresponding o_L-modules $\mathcal{F}'_n := \{z \in \mathfrak{M} : \psi_n(z) = 0\}$. According to the Addendum to Remark 3.1 there exists a unit $u \in o_{E^{max}}^{\pi,\varpi}$ such that $[u]_{\phi,\psi} : \mathcal{F}'_n \xrightarrow{\cong} \mathcal{F}_n$ is a bijection for any $n \geq 1$. Let $v := \frac{x}{y} = \mathrm{Norm}_{E/L}(\frac{\pi}{\varpi}) \in o_L^\times$. The key equation, which was established in Prop. 2.12.iii, for the present purpose is

$${}^{\varphi^d}[u]_{\phi,\psi} = [uv]_{\phi,\psi} \ .$$

The automorphism $rec_{L,x}(x)$ is equal to φ^{-d} on L^{ur} and is the identity on $L_n^{(x)}$. The automorphism $rec_{L,y}(x) = rec_{L,y}(vy)$ is equal to φ^{-d} on L^{ur} and is determined on $L_n^{(y)}$ by

$$rec_{L,y}(x)(z') = [v]_\psi(z') \qquad \text{for any } z' \in \mathcal{F}'_n.$$

We need to compute the action of $rec_{L,y}(x)$ on $L_n^{(x)}$, i.e., on $\mathcal{F}_n$. Let $z \in \mathcal{F}_n$ and write $z = [u]_{\phi,\psi}(z')$ for a (unique) $z' \in \mathcal{F}'_n$. We now compute

$$\begin{aligned} rec_{L,y}(x)(z) &= rec_{L,y}(vy)([u]_{\phi,\psi}(z')) \\ &= {}^{\varphi^{-d}}[u]_{\phi,\psi}([v]_\psi(z')) = {}^{\varphi^{-d}}[u]_{\phi,\psi}({}^{\varphi^{-d}}[v]_\psi(z')) \\ &= {}^{\varphi^{-d}}[uv]_{\phi,\psi}(z') = [u]_{\phi,\psi}(z') \\ &= z \ . \end{aligned}$$

At this point we have shown that $rec_{L,x}(x) = rec_{L,y}(x)$. If $x' \in \mathfrak{m}_L$ is a third nonzero element such that $v_L(x') = d$ then it follows that

$$rec_{L,x}(x') = rec_{L,x'}(x') = rec_{L,y}(x') \ .$$

But any element in $v_L^{-1}(d\mathbb{Z})$ can be written as a finite product of elements in $v_L^{-1}(d\mathbb{Z})$ which have discrete valuation d or $-d$. We conclude that

$$rec_{L,x} = rec_{L,y} \ .$$

In order to deduce from this case our general assertion it suffices to consider the case where $y = \varpi$ is a prime element of o_L and $x = \varpi^d$. Then $L_0^{(\varpi)} = L$ and $[L_0^{(\varpi^d)} : L] = d$. Since $\mathrm{Norm}_{L_0^{(\varpi^d)}/L}(\varpi) = \varpi^d$ we may take for both, y and x, the same Lubin-Tate group law over o_L for the prime element ϖ, viewed over o_L for y and over the unramified extension of L of degree d for x. We then have $L_n^{(x)} = L_n^{(y)} L_0^{(x)}$ and $\chi_{L,x}^{-1}(-)|L_\infty^{(y)} = \chi_{L,y}^{-1}(-)$ by Remark 3.8. Hence it follows from the definition that $rec_{L,y}|v_L^{-1}(d\mathbb{Z}) = rec_{L,x}$. □

For a prime element element ϖ of o_L we put $rec_L := rec_{L,\varpi}$. By Thm. 5.9 this map is independent of the choice of ϖ, is an injective homomorphism

$$rec_L : L^\times \longrightarrow \mathrm{Gal}(L^{LT}/L) \ ,$$

and satisfies:

- $rec_L|v_L^{-1}(v_L(x)\mathbb{Z}) = rec_{L,x}$ for any nonzero $x \in \mathfrak{m}_L$;
- $rec_L(x)|L_\infty^{(x)} = \mathrm{id}$ for any nonzero $x \in \mathfrak{m}_L$;
- $rec_L(x)|L^{ur} = \varphi_L^{-v_L(x)}$ for any nonzero $x \in L^\times$.

The image of rec_L is the *Weil group*

$$W(L^{LT}/L) := \{\sigma \in \mathrm{Gal}(L^{LT}/L) : \sigma|L^{ur} \in \varphi_L^{\mathbb{Z}}\},$$

which is dense in $\mathrm{Gal}(L^{LT}/L)$. We also point out that the group $\mathrm{Gal}(L^{LT}/L)$ is abelian.

norm-ramified **Remark 5.10.** *Let $\tilde{E}/L_\infty^{(x)}$ be a totally ramified algebraic extension; then*

$$N(\tilde{E}/L) := \bigcap_{L' \in \mathcal{E}(\tilde{E}/L)} \mathrm{Norm}_{L'/L}(L'^\times) = x^{\mathbb{Z}} \ .$$

Proof. This is a reformulation of Cor. 5.6. □

base-change **Theorem 5.11.** *For any finite extension M/L we have*

i. $L^{LT} \subseteq M^{LT}$*:*

ii. the diagram

$$\begin{array}{ccc} M^\times & \xrightarrow{rec_M} & \mathrm{Gal}(M^{LT}/M) \\ {\scriptstyle \mathrm{Norm}_{M/L}}\downarrow & & \downarrow{\scriptstyle \text{restriction}} \\ L^\times & \xrightarrow{rec_L} & \mathrm{Gal}(L^{LT}/L) \end{array}$$

is commutative.

Proof. We consider a prime element x of o_M and choose an extension of $rec_M(x) = rec_{M,x}(x) \in \mathrm{Gal}(M^{LT}/M)$ to an automorphism of the separable algebraic closure L^{sep} of L. Let $E_\sigma \subseteq L^{sep}$ denote the fixed field of this automorphism σ. By definition we have

$$M_\infty^{(x)} \subseteq E_\sigma,\ E_\sigma \cap M^{ur} = M,\ \text{and, in particular, } E_\sigma/M_\infty^{(x)} \text{ is totally ramified.}$$

Therefore Remark 5.10 tells us that

$$N(E_\sigma/M) = x^{\mathbb{Z}},\ \text{and hence that } N(E_\sigma/L) = \mathrm{Norm}_{M/L}(x)^{\mathbb{Z}}.$$

Let $M_0 := M \cap L^{ur}$ denote the inertia subfield of the extension M/L. We have $\sigma|L^{ur} = \varphi_M^{-1}|L^{ur} = \varphi_L^{-[M_0:L]}$. Hence there exists a (unique) $y \in \mathfrak{m}_L$ such that $v_L(y) = [M_0 : L]$ and $rec_L(y) = \sigma|L^{LT}$. Then

$$M_0 = L_0^{(y)},\ \sigma|L_\infty^{(y)} = rec_L(y)|L_\infty^{(y)} = \mathrm{id},\ \text{and hence } L_\infty^{(y)} \subseteq E_\sigma.$$

Moreover, $E_\sigma \cap L^{ur} = M \cap L^{ur} = M_0 = L_0^{(y)}$, which implies that $E_\sigma/L_\infty^{(y)}$ is totally ramified. Therefore we may apply Remark 5.10 again and obtain this time that

$$N(E_\sigma/L) = y^{\mathbb{Z}}\ .$$

Since $v_L(y) = [M_0 : L] = v_L(\mathrm{Norm}_{M/L}(x))$ comparing the two computations gives that

$$y = \mathrm{Norm}_{M/L}(x)\ .$$

We have $L_\infty^{(y)} \subseteq \bigcup_\sigma E_\sigma = M_\infty^{(x)}$ with σ running over all possible extensions. From this and $M^{ur} = ML^{ur}$ we deduce that $L^{LT} \subseteq M^{LT}$. We further conclude that

$$rec_M(x)|L^{LT} = \sigma|L^{LT} = rec_L(y) = rec_L(\mathrm{Norm}_{M/L}(x))$$

for any prime element x of o_M. But these prime elements generate the group $M^\times$. This establishes the commutative diagram in our assertion. □

unique **Corollary 5.12.** *i. There is a unique homomorphism $rec_L : L^\times \longrightarrow \mathrm{Gal}(L^{LT}/L)$ such that*

a) If ϖ is a prime element of o_L then $rec_L(\varpi)|L^{ur} = \varphi_L^{-1}$;

b) if $L \subseteq M \subseteq L^{LT}$ is an intermediate finite extension then $rec_L(\mathrm{Norm}_{M/L}(M^\times)) = \{\mathrm{id}\}$.

ii. If M/L is any finite extension then rec_L induces an isomorphism

$$L^\times/\operatorname{Norm}_{M/L}(M^\times) \xrightarrow{\cong} \operatorname{Gal}((M\cap L^{LT})/L)\ .$$

Proof. i. By construction we have $rec_L(\varpi)|L^{ur} = rec_{L,\varpi}(\varpi)|L^{ur} = \varphi_L^{-1}$. Part b) is immediate from Thm. 5.11.ii.

Let now rec'_L be a second map which satisfies a) and b). Using again that the prime elements of o_L generate $L^\times$ it suffices to pick one such prime element ϖ and to show that $rec'_L(\varpi) = rec_L(\varpi)$. By a) both sides restrict to φ_L^{-1} on L^{ur}. By construction $rec_L(\varpi) = rec_{L,\varpi}(\varpi)$ restricts to the identity on $L_\infty^{(\varpi)}$. According to Prop. 3.5.ii.d) (for $\varpi \in E = L$) the element ϖ is a norm from $L_n^{(\varpi)}$ for any $n \geq 1$. It therefore follows from b) that $rec'_L(\varpi)|L_\infty^{(\varpi)} =$ id as well.

ii. Thm, 5.11.ii implies that rec_L induces an isomorphism

$$L^\times/\operatorname{Norm}_{M/L}(M^\times) \xrightarrow{\cong} W(L^{LT}/L)/\text{ image of } W(M^{LT}/M)\ .$$

Furthermore we have the commutative diagram

$$\begin{array}{ccc}
W(M^{LT}/M) & \xrightarrow{\subseteq} & \operatorname{Gal}(M^{LT}/M) \\
\downarrow{\scriptstyle \text{restriction}} & & \downarrow{\scriptstyle \text{restriction}} \\
W(L^{LT}/L) & \xrightarrow{\subseteq} & \operatorname{Gal}(L^{LT}/L) \\
\downarrow & & \downarrow{\scriptstyle \text{pr}} \\
\operatorname{Gal}((M\cap L^{LT})/L) & = & \operatorname{Gal}((M\cap L^{LT})/L) \\
\downarrow & & \downarrow \\
0 & & 0.
\end{array}$$

The right column is exact by Galois theory. The upper square is cartesian. In the left column the lower map is surjective by the density of the Weil group in the Galois group. It follows that the left column is exact as well. □

further-prop

Proposition 5.13. *i. Let $L \subseteq M, M_1, M_2 \subseteq L^{LT}$ be intermediate extensions which are finite over L. We then have:*

a. The extension M/L is Galois with abelian Galois group, and rec_L induces an isomorphism

$$L^\times/\operatorname{Norm}_{M/L}(M^\times) \xrightarrow{\cong} \operatorname{Gal}(M/L)\ .$$

b. $\operatorname{Norm}_{M_1/L}(M_1^\times) \subseteq \operatorname{Norm}_{M_2/L}(M_2^\times)$ if and only if $M_2 \subseteq M_1$.

c. $\operatorname{Norm}_{M_1M_2/L}((M_1M_2)^\times) = \operatorname{Norm}_{M_1/L}(M_1^\times) \cap \operatorname{Norm}_{M_2/L}(M_2^\times)$.

d. $\operatorname{Norm}_{M_1\cap M_2/L}((M_1\cap M_2)^\times) = \operatorname{Norm}_{M_1/L}(M_1^\times)\cdot \operatorname{Norm}_{M_2/L}(M_2^\times)$.

ii. For any closed subgroup $N \subseteq L^\times$ of finite index there is a unique intermediate extension $L \subseteq M \subseteq L^{LT}$ such that $N = \operatorname{Norm}_{M/L}(M^\times)$.

Proof. This is left to the reader as an exercise. □

5.3 Reminder of ramification subgroups

ram-subgroups

We quickly go through the formalism of ramification subgroups. For proofs we refer to [Ser] Chap. IV.

Let M/L be a finite Galois extension with Galois group $G := \mathrm{Gal}(M/L)$. The ramification subgroups of G (in the lower numbering) are defined by

$$G_i := \{\sigma \in G : \sigma(x) \equiv x \bmod \mathfrak{m}_M^{i+1} \text{ for any } x \in o_M\}$$

for any integer $i \geq 0$. They form a decreasing sequence of normal subgroups with the property that $G_i = \{1\}$ for sufficiently big i.

On the other hand, in the group of units $o_M^\times$ we have the decreasing sequence of subgroups

$$U_M^{(0)} := o_M^\times \quad \text{and} \quad U_M^{(i)} := \{x \in o_M^\times : x \equiv 1 \bmod \mathfrak{m}_M^i\} \quad \text{for } i \geq 1.$$

Gi/Gi+1

Proposition 5.14. *If M/L is totally ramified then, for any $i \geq 0$, we have:*

i. $G_i = \{\sigma \in G : v_M(\sigma(\pi_M) - \pi_M) > i\}$;

ii. the map

$$\begin{aligned} G_i/G_{i+1} &\longrightarrow U_M^{(i)}/U_M^{(i+1)} \\ \sigma &\longmapsto \frac{\sigma(\pi_M)}{\pi_M} U_M^{(i+1)} \end{aligned}$$

is a well defined injective homomorphism, which does not depend on the choice of the prime element π_M.

We remind the reader that totally ramified extensions M/L have the additional property that $o_M = o_L[\pi_M]$. This fact immediately implies that first assertion of the above lemma.

For later purposes we add the following observation.

ineq

Remark 5.15. *For any $\sigma \in G_1$ and any $a \in M^\times$ we have $v_M(\sigma(a) - a) > v_M(a)$.*

Proof. By multiplying a by some appropriate element in $L^\times$ it suffices to consider the case where $a \in o_M \setminus \{0\}$. For these a we proceed by induction with respect to $v_M(a)$. If $v_M(a) \leq 1$ then the assertion holds by the definition of G_1. Now suppose that a satisfies the assertion and consider the element $a\pi_M$. We compute

$$\begin{aligned} v_M(\sigma(a\pi_M) - a\pi_M) &= v_M((\sigma(a) - a)\sigma(\pi_M) + a(\sigma(\pi_M) - \pi_M)) \\ &\geq \min(v_M(\sigma(a) - a) + v_M(\sigma(\pi_M)), v_M(a) + v_M(\sigma(\pi_M) - \pi_M)) \\ &> v_M(a) + 1 = v_M(a\pi_M) \ . \end{aligned}$$

□

Let $L \subseteq K \subseteq M$ be an intermediate extension. We then obviously have

$$\mathrm{Gal}(M/K)_i = G_i \cap \mathrm{Gal}(M/K) \ .$$

Suppose now that K/L is Galois as well. Is there a similar formula which computes the ramification subgroups $\mathrm{Gal}(K/L)_i$ form the G_i? There is, but it requires an explicit change of indices.

We first extend the definition of the subgroups G_i to arbitrary real indices $z \geq 1$ by

$$G_{-1} := G \quad \text{and} \quad G_z := G_{\lceil z \rceil} \ ,$$

where $\lceil z \rceil$ denotes the smallest integer $\geq z$. Note that in case, that M/L is totally ramified, we simply have

f:Gz (8) $$G_z = \{\sigma \in G : v_M(\sigma(\pi_M) - \pi_M) \geq z + 1\}.$$

We now introduce the change of indices function $\phi : [-1, \infty) \longrightarrow \mathbb{R}$ by

$$\phi(y) := \phi_{M/L}(y) := \int_0^y \frac{1}{[G_0 : G_z]} dz \ ,$$

using the convention that $[G_0 : G_{-1}] := [G_{-1} : G_0]^{-1}$. Its basic properties are as follows.

hi-properties **Proposition 5.16.** *a) ϕ is continuous, piecewise linear, strictly increasing, and concave.*

b) $\phi(y) = y$ for $y \in [-1, 0]$.

c) $\phi(i) = \frac{1}{|G_0|}(|G_1| + \ldots + |G_i|)$ for any integer $i \geq 1$.

d) If M/L is totally ramified then $\phi(y) = [\frac{1}{|G|} \sum_{\sigma \in G} \min(y + 1, v_M(\sigma(\pi_M) - \pi_M))] - 1$.

We see that, in particular, ϕ is a homeomorphism of the interval $[-1, \infty)$ onto itself. Therefore the homeomorphism $\psi(z) := \psi_{M/L}(z)$ inverse to ϕ exists and is a continuous, piecewise linear, strictly increasing, and convex function $\psi : [-1, \infty) \longrightarrow \mathbb{R}$. The ramification subgroups in the upper numbering now are defined by

$$G^z := G_{\psi(z)} \qquad \text{for any } z \geq -1.$$

The following properties are obvious:

- $G_z = G^{\phi(z)}$.
- $G^z = G_z$ for any $z \in [-1, 0]$, and $G^z = \{1\}$ for sufficiently big z.
- $G^{z_1} \supseteq G^{z_2}$ if $z_1 \leq z_2$.

We consider now an intermediate extension $L \subseteq K \subseteq M$ which we assume to also be Galois over L. Then $N := \mathrm{Gal}(M/K)$ is a normal subgroup of G, and $G/N = \mathrm{Gal}(K/L)$. The main facts, which we need, are the following.

G/N **Proposition 5.17.** *i. $\phi_{M/L} = \phi_{K/L} \circ \phi_{M/K}$ and $\psi_{M/L} = \psi_{M/K} \circ \psi_{K/L}$.*

ii. $G_z N/N = (G/N)_{\phi_{M/K}(z)}$ for any $z \geq -1$.

iii. $(G/N)^z = G^z N/N$ for any $z \geq -1$.

compositum **Corollary 5.18.** *Let M_1/L and M_2/L be two finite Galois extensions, and let $z \geq 0$; if $\mathrm{Gal}(M_1/L)^z = \mathrm{Gal}(M_2/L)^z = \{1\}$ then $\mathrm{Gal}(M_1M_2/L)^z = \{1\}$ as well.*

Proof. Let $G := \mathrm{Gal}(M_1M_2/L)$ and $N_i := \mathrm{Gal}(M_1M_2/M_i)$. Using Prop. 5.17.iii we obtain $G^z N_i/N_i = (G/N_i)^z = \mathrm{Gal}(M_i/L)^z = \{1\}$. It follows that $G^z \subseteq N_1 \cap N_2 = \{1\}$. □

We finish this survey by making the upper numbering explicit in the case of the Lubin-Tate extensions E_n/E, where E/L is a finite unramified extension, from section 3. It follows from Prop. 3.7 that, for any $m \geq 1$, the function $\phi = \phi_{E_n/E}$ is linear in the interval $(q^{m-1}-1, q^m-1)$ with slope $\frac{1}{|\operatorname{Gal}(E_m/E)|} = \frac{1}{(q-1)q^{m-1}}$. Hence the inverse function ψ is linear in the interval $(m-1, m)$ with $\psi(m) = q^m - 1$. We conclude that

$$\operatorname{Gal}(E_n/E)^z = \operatorname{Gal}(E_n/E_m) \quad \text{for } -1 \leq m-1 < z \leq m.$$

In particular we have

f:LT-trivial

$$\operatorname{Gal}(E_n/E)^n = \{1\} \ . \tag{9}$$

sec:Hasse-Arf

5.4 The Hasse-Arf theorem

Again let M/L be a finite Galois extension with Galois group $G := \operatorname{Gal}(M/L)$. The goal of this section is to establish the following result.

Hasse-Arf

Theorem 5.19. *Suppose that G is abelian, and let $m \geq 0$ be an integer such that $G_m \neq G_{m+1}$; then $\phi_{M/L}(m)$ is an integer as well.*

Remark. An equivalent formulation of the above Theorem using the upper numbering is the following: Suppose that G is abelian; any $z \geq 0$ such that $G^z \neq G^{z+\epsilon}$ for any $\epsilon > 0$ is an integer. The condition on z is equivalent to $G_{\psi_{M/L}(z)} \neq G_{\psi_{M/L}(z)+\delta}$ for any $\delta > 0$, in which case $m := \psi_{M/L}(z)$ necessarily has to be an integer. It remains to note that $z = \phi_{M/L}(m)$.

The proof requires some preparation.

ab

Lemma 5.20. *Under the assumptions of Thm. 5.19 we have that m is divisible by $[G_0 : G_1]$.*

Proof. It suffices to treat any $m \geq 1$. By Prop. 5.14 we have the composite homomorphism

$$\begin{aligned} \theta : G_m/G_{m+1} \to U_M^{(m)}/U_M^{m+1)} &\xrightarrow{\cong} \mathfrak{m}_M^m/\mathfrak{m}_M^{m+1} \\ \sigma G_{m+1} &\longrightarrow \frac{\sigma(\pi_M)}{\pi_M} - 1 \bmod \mathfrak{m}_M^{m+1} \ , \end{aligned}$$

which is injective and independent of the choice of π_M. Let $\sigma \in G_m$ and $\tau \in G$ be arbitrary elements. Since G_m is normal in G we have $\tau\sigma\tau^{-1} \in G_m$. Using the prime element $\tau^{-1}(\pi_M)$ we have

$$\theta(\sigma) = \frac{\sigma\tau^{-1}(\pi_M)}{\tau^{-1}(\pi_M)} - 1 \bmod \mathfrak{m}_M^{m+1} \ .$$

On the other hand, using the prime element π_M we obtain

$$\theta(\tau\sigma\tau^{-1}) = \frac{\tau\sigma\tau^{-1}(\pi_M)}{\pi_M} - 1 \bmod \mathfrak{m}_M^{m+1} = \tau(\theta(\sigma)) \ .$$

We temporarily write $\theta(\sigma) = b\pi_M^m \bmod \mathfrak{m}_M^{m+1}$ for some $b \in o_M$. We also assume from now on that $\tau \in G_0$ so that $\tau(b) \equiv b \bmod \mathfrak{m}_M$. Setting $u_\tau := \frac{\tau(\pi_M)}{\pi_M} \in o_M^\times$ we have $\tau(b\pi_M^m) \equiv bu_\tau^m\pi_M^m \equiv u_\tau^m(b\pi_M^m) \bmod \mathfrak{m}_M^{m+1}$. We deduce that

$$\theta(\tau\sigma\tau^{-1}) = \tau(\theta(\sigma)) = u_\tau^m\theta(\sigma) \ .$$

Now we use that G is abelian. Then $\tau\sigma\tau^{-1} = \sigma$ and hence $\theta(\sigma) = u_\tau^m \theta(\sigma)$. Since $\mathfrak{m}_M^m/\mathfrak{m}_M^{m+1}$ is a vector space over $o_M/\mathfrak{m}_M = k_M$, this means that either $\theta(\sigma) = 0$ or that the order of u_τ viewed in $k_M^\times$ divides m. Choosing $\sigma \in G_m \setminus G_{m+1}$ we guarantee that $\theta(\sigma) \neq 0$. Hence the second condition must hold. But $\tau \mapsto u_\tau$ induces an injective map $G_0/G_1 \to k_M^\times$. Hence this second condition is equivalent to the order of τG_1 in G_0/G_1 dividing m. It remains to choose τ such that τG_1 generates the cyclic group G_0/G_1, and we obtain that $[G_0 : G_1]$ divides m. □

In order to state the key technical fact let us fix an automorphism $\sigma \in G_1 \setminus \{1\}$ and let us denote by $H := \langle\sigma\rangle$ the subgroup in G which σ generates. By Prop. 5.14.ii the subgroup G_1 is a p-group. Hence $H \cong \mathbb{Z}/p^j\mathbb{Z}$ for some $j \geq 1$. We will determine the ramification subgroups $H_m = H \cap G_m$ in terms of the numbers

$$\ell_\nu := v_M(\sigma^{p^\nu}(\pi_M) - \pi_M) \qquad \text{for } \nu \geq 0$$

(with the convention that $\ell_\nu = \infty$ for $\nu \geq j$).

expansion **Remark 5.21.** *Any element $x \in M$ has a convergent expansion $x = \sum_{i=v_M(x)}^{\infty} x_i$ such that each x_i either is zero or satisfies $v_M(x_i) = i$ and $v_M(\sigma(x_i) - x_i) = i - 1 + v_M(\sigma^i(\pi_M) - \pi_M)$.*

Proof. We recall the following general fact. For each integer i we choose an element $\pi_i \in M$ such that $v_M(\pi_i) = i$. We also fix a set of representatives $\mathcal{R} \subseteq (o_M^{G_0})^\times$ for the elements in $k_M^\times$. Then any $x \in M$ has a unique convergent expansion $x = \sum_{i=v_M(x)}^{\infty} c_i\pi_i$ with $c_i \in \mathcal{R} \cup \{0\}$.

In our situation we make the following specific choice for the π_i. Let $\pi_0 := 1$; if $i > 0$ then we take $\pi_i := \prod_{\ell=0}^{i-1} \sigma^\ell(\pi_M)$; for $i < 0$ we define $\pi_i := \pi_{-i}^{-1}$. Suppose that $c_i \neq 0$. Then $v_M(c_i\pi_i) = v_M(\pi_i) = i$ and

$$\begin{aligned} v_M(\sigma(c_i\pi_i) - c_i\pi_i) &= v_M(c_i\pi_i) + v_M\Big(\frac{\sigma(c_i\pi_i)}{c_i\pi_i} - 1\Big) \\ &= i + v_M\Big(\frac{\sigma(\pi_i)}{\pi_i} - 1\Big) = i + v_M\Big(\frac{\sigma^i(\pi_M)}{\pi_M} - 1\Big) \quad \text{for } i > 0\ , \end{aligned}$$

resp.

$$\begin{aligned} v_M(\sigma(c_i\pi_i) - c_i\pi_i) &= i + v_M\Big(\frac{\sigma(\pi_i)}{\pi_i} - 1\Big) = i + v_M\Big(\frac{\sigma^{-i}(\pi_M)^{-1}}{\pi_M^{-1}} - 1\Big) \\ &= i + v_M\Big(\frac{\pi_M}{\sigma^{-i}(\pi_M)} - 1\Big) = i + v_M\Big(\frac{\sigma^{-i}(\sigma^i(\pi_M))}{\sigma^{-i}(\pi_M)} - 1\Big) \\ &= i + v_M\Big(\frac{\sigma^i(\pi_M)}{\pi_M} - 1\Big) \quad \text{for } i < 0\ . \end{aligned}$$

□

trivial **Remark 5.22.** *For any $y \in M^\times$ we have $v_M(\sum_{i=0}^{p-1} \sigma^i(y)) > v_M(y)$.*

Proof. We know from Remark 5.15 that $v_M((\sigma - 1)(y)) > v_M(y)$ and then, a fortiori, that $v_M((\sigma - 1)^{p-1}(y)) > v_M(y)$. Next we note that in the polynomial ring $\mathbb{F}_p[X]$ we have the identity $\sum_{i=0}^{p-1} X^i = \frac{X^p - 1}{X - 1} = (X - 1)^{p-1}$. Hence, viewing the group ring $\mathbb{F}_p[H]$ as a quotient of

$\mathbb{F}_p[X]$ by sending X to σ, we deduce the equality $\sum_{i=0}^{p-1}\sigma^i = (\sigma-1)^{p-1}$ in $\mathbb{F}_p[H]$. The action of H on yo_M induces an action

$$\mathbb{F}_p[H] \times yo_M/pyo_M \longrightarrow yo_M/pyo_M \ .$$

It follows that $\sum_{i=0}^{p-1}\sigma^i(y) = (\sigma-1)^{p-1}(y) \bmod pyo_M$ and therefore that $v_M(\sum_{i=0}^{p-1}\sigma^i(y)) \geq \min(v_M((\sigma-1)^{p-1}(y)), 1+v_M(y)) > v_M(y)$. □

Sen **Proposition 5.23.** *i. Let $1 \leq \nu \leq j$; we have $\ell_{\nu-1} < \ell_\nu$, and $H_m = \langle\sigma^{p^\nu}\rangle$ for any $\ell_{\nu-1} \leq m < \ell_\nu$.*

ii. For any $\nu \geq 0$ and any integer $a \in \mathbb{Z}\setminus\{0\}$ prime to p we have $v_M(\sigma^{ap^\nu}(\pi_M)-\pi_M) = \ell_\nu$.

iii. For $1 \leq \nu < j$ we have $\ell_{\nu-1} \equiv \ell_\nu \bmod p^\nu$.

Proof. i. Let $\tau := \sigma^{p^{\nu-1}} \in H_1 \setminus \{1\}$. Then $\sum_{i=0}^{p-1}\tau^i(\sigma^{p^{\nu-1}}-1) = \sigma^{p^\nu}-1$. Hence $\ell_{\nu-1} < \ell_\nu$ follows from Remark 5.22 applied with τ and $a := \sigma^{p^{\nu-1}}(\pi_M)-\pi_M$. For the second part of the assertion note that $H_m = \langle\sigma^{p^\nu}\rangle$ if and only if $\langle\sigma^{p^\nu}\rangle \subseteq H_m$ and $\langle\sigma^{p^{\nu-1}}\rangle \not\subseteq H_m$. But Prop. 5.14.i implies that $\langle\sigma^{p^\nu}\rangle \subseteq H_m$ (if and only if $\sigma^{p^\nu} \in H_m$) if and only if $\ell_\nu > m$, and correspondingly that $\langle\sigma^{p^{\nu-1}}\rangle \not\subseteq H_m$ if and only if $\ell_{\nu-1} \leq m$.

ii. For $\nu \geq j$ both sides are equal to ∞. Suppose therefore that $\nu < j$. Using i. we see that $\langle\sigma^{p^\nu}\rangle = H_{\ell_\nu - 1}$ and $H_{\ell_\nu} = \langle\sigma^{p^{\nu+1}}\rangle$. It follows that $\sigma^{ap^\nu} \in H_{\ell_{\nu-1}} \setminus H_{\ell_\nu}$, which, by Prop. 5.14.i again, means that $v_M(\sigma^{ap^\nu}(\pi_M)-\pi_M) = \ell_\nu$.

iii. We will proceed by induction with respect to ν. More precisely we view the assertion as a claim about pairs in the set $\{(\sigma',\nu') : \sigma' \in G_1 \setminus \{1\},\ 1 \leq \nu' < v_p(\mathrm{ord}(\sigma'))\}$. Here and in the following $v_p := v_{\mathbb{Q}_p}$ denotes the p-adic valuation and $\mathrm{ord}(\sigma')$ the order of the element σ'. We assume that the claim has been proved already for all pairs (σ',ν') such that either $v_p(\mathrm{ord}(\sigma')) < j$ or $\sigma' = \sigma$ and $\nu' < \nu$. Note that the claim is empty if $v_p(\mathrm{ord}(\sigma')) = 1$. We now prove the claim for the pair (σ,ν).

Step 1: We show that the integers $\ell_{\nu-1}$ and $b + v_M(\sigma^b(\pi_M)-\pi_M)$ for $b \in \mathbb{Z}\setminus\{0\}$ and $v_p(b) < \nu$ are pairwise different.

Let $b, b' \in \mathbb{Z}\setminus\{0\}$ with $v_p(b), v_p(b') < \nu$. According to ii. we have

$$v_M(\sigma^b(\pi_M)-\pi_M) = \ell_{v_p(b)} \quad \text{and} \quad v_M(\sigma^{b'}(\pi_M)-\pi_M) = \ell_{v_p(b')} \ .$$

The induction hypothesis implies that

$$\ell_{v_p(b)} \equiv \ell_{\nu-1} \bmod p^{v_p(b)+1} \quad \text{and} \quad \ell_{v_p(b')} \equiv \ell_{\nu-1} \bmod p^{v_p(b')+1} \ .$$

On the one hand it follows that $\ell_{\nu-1} - v_M(\sigma^b(\pi_M)-\pi_M) \equiv 0 \bmod p^{v_p(b)+1}$. But $b \not\equiv 0 \bmod p^{v_p(b)+1}$. Hence $\ell_{\nu-1} \neq b + v_M(\sigma^b(\pi_M)-\pi_M)$. On the other hand let us assume that

$$b + v_M(\sigma^b(\pi_M)-\pi_M) = b' + v_M(\sigma^{b'}(\pi_M)-\pi_M) \ .$$

We then have

$$b'-b = v_M(\sigma^b(\pi_M)-\pi_M) - v_M(\sigma^{b'}(\pi_M)-\pi_M) = \ell_{v_p(b)} - \ell_{v_p(b')} \equiv 0 \bmod p^{\min(v_p(b),v_p(b'))+1}.$$

This is impossible if $v_p(b) \neq v_p(b')$ since then $\min(v_p(b),v_p(b')) = v_p(b-b')$. Hence $v_p(b) = v_p(b')$ and therefore $v_M(\sigma^b(\pi_M)-\pi_M) = \ell_{v_p(b)} = \ell_{v_p(b')} = v_M(\sigma^{b'}(\pi_M)-\pi_M)$. It follows that $b = b'$.

Step 2: We may assume $j \geq 2$. Put $s := \ell_{\nu-1} - \ell_\nu$, which is nonzero by i. We have to show that $v_p(s) \geq \nu$. If $\nu = 1$ then obviously $v_p(s) \geq \nu - 1$. If $\nu > 1$ then we may apply the induction hypothesis with σ^p and obtain $v_p(s) \geq \nu - 1$ as well. We therefore assume $v_p(s) = \nu - 1$ in the following and derive a contradiction.

Using the proof of Remark 5.21 with σ^p we obtain an element $z := \pi_s \in M^\times$ such that $v_M(z) = s$ and $v_M(\sigma^p(z) - z) = s - 1 + v_M(\sigma^{ps}(\pi_M) - \pi_M)$. Since $v_p(ps) = \nu$ we conclude from ii. that $v_M(\sigma^{ps}(\pi_M) - \pi_M) = \ell_\nu$. Hence we have

$$v_M(z) = s \quad \text{and} \quad v_M(\sigma^p(z) - z) = s - 1 + \ell_\nu = \ell_{\nu-1} - 1 \ .$$

We define $y := \sum_{i=0}^{p-1} \sigma^i(z)$ and have

$$v_M(y) > v_M(z) = s \text{ (by Remark 5.22) and} \quad v_M(\sigma(y) - y) = v_M(\sigma^p(z) - z) = \ell_{\nu-1} - 1 \ .$$

Applying Remark 5.21 we obtain an expansion $y = \sum_{i \geq v_M(y)} y_i$ such that either $y_i = 0$ or $v_M(y_i) = i$ and $v_M(\sigma(y_i) - y_i) = i - 1 + v_M(\sigma^i(\pi_M) - \pi_M)$.

Finally we put $x := \sigma(y) - y$, which has the expansion $x = \sum_{i \geq v_M(y)} x_i$ with $x_i := \sigma(y_i) - y_i$. We have $v_M(x) = \ell_{\nu-1} - 1$, and, if $y_i \neq 0$, then x_i satisfies $v_M(x_i) = i - 1 + v_M(\sigma^i(\pi_M) - \pi_M)$. The above Step 1 implies that the integers $v_M(x)$ and $v_M(x_i)$ for $v_p(i) < \nu$ are pairwise different. It follows that

$$v_M(x - \sum_{v_p(i) < \nu} x_i) \leq v_M(x) = \ell_{\nu-1} - 1 < \ell_{\nu-1} \ .$$

Now consider any $i \geq v_M(y)$ such that $y_i \neq 0$ and $v_p(i) \geq \nu$. Then

$$\begin{aligned} v_M(x_i) &= i - 1 + v_M(\sigma^i(\pi_M) - \pi_M) \\ &= i - 1 + \ell_{v_p(i)} \\ &\geq i - 1 + \ell_\nu \\ &\geq v_M(y) - 1 + \ell_\nu > s - 1 + \ell_\nu = \ell_{\nu-1} - 1 \ , \end{aligned}$$

using ii. and i. in the second and third line, respectively. It follows that $v_M(\sum_{v_p(i) \geq \nu} x_i) \geq \ell_{\nu-1}$, which is the wanted contradiction. □

cor:Sen **Corollary 5.24.** *There exist integers $c_0, \ldots, c_{j-1} \geq 1$ such that, for $0 \leq \nu \leq j-1$, we have $|H_m| = p^{j-\nu}$ if and only if $\sum_{i=0}^{\nu-1} c_i p^i \leq m < \sum_{i=0}^{\nu} c_i p^i$.*

Proof. According to Prop. 5.23.i/iii we find integers $c_0, \ldots, c_{j-1} \geq 1$ such that $\ell_\nu = c_0 + c_1 p + \ldots + c_{\nu-1} p^{\nu-1} + c_\nu p^\nu$ for any $0 \leq \nu < j$. Moreover, Prop. 5.23.i also says that

$$\begin{aligned} |H| = |H_1| = \ldots = |H_{\ell_0 - 1}| &= p^j \ , \\ |H_{\ell_0}| = \ldots = |H_{\ell_1 - 1}| &= p^{j-1} \ , \\ &\vdots \\ |H_{\ell_{j-2}}| = \ldots = |H_{\ell_{j-1} - 1}| &= p \ , \\ |H_{\ell_{j-1}}| = \ldots = |\{1\}| &= 1 \ . \end{aligned}$$

For the first line use Prop. 5.14.i observing that $\ell_0 = v_M(\sigma(\pi_M) - \pi_M)$. □

Proof of Thm. 5.19: The assertion is trivial if $M = L$. We therefore suppose in the following that $G \neq \{1\}$.

Step 1: We assume that $G = G_1$. Then G is an abelian p-group. Suppose first that $G \cong \mathbb{Z}/p^j\mathbb{Z}$ is cyclic. Then Cor. 5.24 implies that

$$m = (\sum_{i=0}^{\nu} c_i p^i) - 1 \quad \text{for some } 0 \leq \nu \leq j-1 \text{ and some integers } c_0, \ldots, c_\nu \geq 1.$$

Using Prop. 5.16.c in the first equality and again Cor. 5.24 in the second one, we compute

$$\begin{aligned} \phi_{M/L}(m) &= \frac{1}{|G|}(|G_1| + \ldots |G_m|) \\ &= \frac{1}{p^j}(p^j \cdot (c_0 - 1)p^0 + p^{j-1} \cdot c_1 p^1 + \ldots + p^{j-\nu} \cdot c_\nu p^\nu) \\ &= c_0 - 1 + c_1 + \ldots + c_\nu \ . \end{aligned}$$

The result is a positive integer as claimed.

Now suppose that $G = G_1$ is arbitrary. Writing G/G_{m+1} as a product of cyclic groups we find a cyclic factor group H of G such that the image of G_m, resp. of G_{m+1}, in H is nontrivial, resp. is trivial. Setting $z := \phi_{M/L}(m)$ this means, using Prop. 5.17.iii, that $H^z \neq H^{z+\epsilon}$ for any $\epsilon > 0$. In view of the Remark after Thm. 5.19 we then deduce from the cyclic case, which we have established above, that z is an integer.

Step 2: Now let G be any abelian group. Since $\phi_{M/L}(0) = 0$ we assume that $m \geq 1$. If $L \subseteq M_0 := M^{G_0} \subseteq M$ denotes the inertia subfield then $\phi_{M/L} = \phi_{M/M_0}$. Hence we will assume that $M = M_0$, i.e., that M/L is totally ramified. Next consider $L \subseteq M_1 := M^{G_1} \subseteq M$ with $\mathrm{Gal}(M_1/L) = G/G_1$. With M/L also M_1/L is totally ramified, so that $\mathrm{Gal}(M_1/L)_0 = \mathrm{Gal}(M_1/L)$. On the other hand, using Prop. 5.14.ii, we see first that the order of G/G_1 is prime to p (whereas G_1 is a p-group) and then that therefore $\mathrm{Gal}(M_1/L)_1 = \{1\}$. We conclude that $\phi_{M_1/L}(y) = \frac{y}{[G:G_1]}$ for any $y \geq 0$. By Prop. 5.17.i we have $\phi_{M/L} = \phi_{M_1/L} \circ \phi_{M/M_1}$. It follows that

$$\phi_{M/L}(m) = \frac{\phi_{M/M_1}(m)}{[G : G_1]} \ .$$

Since $G_m \subseteq G_1 = \mathrm{Gal}(M/M_1)$ we know from Step 1 that $\phi_{M/M_1}(m)$ is a positive integer. Hence it remains to show that $\phi_{M/M_1}(m)$ is divisible by $[G : G_1]$.

Lemma 5.20 implies that, for any $i \geq 1$ such that

$$G_i = \mathrm{Gal}(M/M_1)_i \neq \mathrm{Gal}(M/M_1)_{i+1} = G_{i+1} \ ,$$

we have that $[G : G_1]$ divides i. Let

$$\mathrm{Gal}(M/M_1) = G_1 = \ldots = G_{i_1} \neq G_{i_1+1} = \ldots = G_{i_r} \neq G_{i_r+1} = \ldots = G_m \neq G_{m+1}$$

with $1 \leq i_1 < \ldots < i_r < m$. It follows that $[G : G_1]$ divides

$$i_1|G_{i_1}| + (i_2 - i_1)|G_{i_2}| + \ldots (m - i_r)|G_m| = \sum_{i=1}^{m} |\,\mathrm{Gal}(M/M_1)_i| = \sum_{i=1}^{m} |(G_1)_i| \ .$$

Since $[G : G_1]$ and $|G_1|$ are coprime we deduce that $[G : G_1]$ divides $\phi_{M/M_1}(m) = \frac{\sum_{i=1}^{m} |(G_1)_i|}{|G_1|}$ (cf. Prop. 5.16.c).

This finishes the proof of Thm. 5.19.

order **Corollary 5.25.** *Suppose that M/L is totally ramified with abelian Galois group G; then $[G : G^m]$ divides $(q-1)q^{m-1}$ for any integer $m \geq 1$.*

Proof. We have $G^m = G_{\psi_{M/L}(m)}$. Hence, if $n-1 < \psi_{M/L}(m) \leq n$, then $G^m = G_n$. Consider the decomposition

$$[G : G^m] = [G : G_n] = [G : G_1] \cdot [G_1 : G_2] \cdot \ldots \cdot [G_{n-1} : G_n] \ .$$

It follows from Prop. 5.14.ii that $[G : G_1]$ divides $q-1$ and that $[G_i : G_{i+1}]$ divides q for any integer $i \geq 1$. On the other hand Thm. 5.19 tells us that, if $G_i \neq G_{i+1}$ for some $1 \leq i \leq n-1$, then $\phi_{M/L}(i) \in \mathbb{Z}$. But, as

$$1 \leq \phi_{M/L}(i) \leq \phi_{M/L}(n-1) < \phi_{M/L}(\psi_{M/L}(m)) = m \ ,$$

the latter can happen at most $m-1$ times. □

subsec:max-ab

5.5 The maximal abelian extension

The final result, which in view of Cor. 5.12 determines the maximal abelian extension of L, is the following.

max-ab **Theorem 5.26.** *Every finite abelian extension of L (inside $\overline{L}$) is contained in L^{LT}.*

Proof. Let L^{ab}/L denote the maximal abelian extension of L. We already know from section 5.2 that $L^{LT} \subseteq L^{ab}$. Let ϖ be a prime element in o_L, choose an automorphism $\sigma \in \mathrm{Gal}(L^{ab}/L)$ such that $\sigma|L^{LT} = rec_L(\varpi)$, and let $E \subseteq L^{ab}$ denote the fixed field of σ. We recall from the paragraph before Remark 5.6 that:

(a) $rec_L(\varpi)|L^{ur} = \varphi_L^{-1}$ and hence $E \cap L^{ur} = L$.

(b) $rec_L(\varpi)|L_\infty^{(\varpi)} = \mathrm{id}$ and hence $L_\infty^{(\varpi)} \subseteq E$.

Step 1: We show that $L^{ab} = EL^{ur}$. Of course, EL^{ur} is contained in L^{ab}. Consider the restriction map

$$\mathrm{Gal}(L^{ab}/E) \longrightarrow \mathrm{Gal}(L^{ur}/L) \cong \hat{\mathbb{Z}} \ .$$

By (a) the automorphism σ is mapped to the topological generator φ_L^{-1} of $\mathrm{Gal}(L^{ur}/L)$. Hence the map is surjective. On the other hand, any intermediate extension $E \subseteq F \subseteq L^{ab}$ finite over E has a cyclic Galois group generated by $\sigma|F$. This implies that F is uniquely determined by its degree $[F : E]$ and then that $\mathrm{Gal}(L^{ab}/E) \cong \hat{\mathbb{Z}}$ is topologically generated by σ. It follows that the above map is an isomorphism and therefore that $EL^{ur} = L^{ab}$.

Step 2: We show that $L_\infty^{(\varpi)} = E$. Since $L^{LT} = L_\infty^{(\varpi)} L^{ur}$ this together with Step 1 then proves that $L^{LT} = EL^{ur} = L^{ab}$. By (b) it suffices to check that $E \subseteq L_\infty^{(\varpi)}$. Let $L \subseteq M \subseteq E$ be any intermediate extension finite over L. It is totally ramified by (a). Let the integer $m \geq 1$ be sufficiently large such that $\mathrm{Gal}(M/L)^m = \{1\}$. We have $\mathrm{Gal}(L_m^{(\varpi)}/L)^m = \{1\}$ by (9). Hence $\mathrm{Gal}(ML_m^{(\varpi)}/L)^m = \{1\}$ by Cor. 5.18. Since $ML_m^{(\varpi)} \subseteq E$ by (b) the composite extension $ML_m^{(\varpi)}/L$ is totally ramified. It then follows from Cor. 5.25 that the degree $[ML_m^{(\varpi)} : L]$ divides $(q-1)q^{m-1}$. But $(q-1)q^{m-1} = [L_m^{(\varpi)} : L]$ according to Prop. 3.5.i. This implies $M \subseteq L_m^{(\varpi)}$. □

References

[B-CA] Bourbaki N.: *Commutative Algebra*. Hermann 1972

[CF] Cassels J.W.S., Fröhlich A.: *Algebraic Number Theory*. Academic Press 1967

[Col] Coleman R.: *Division Values in Local Fields*. Invent. math. 53, 91-116 (1979)

[DeS] de Shalit E.: *Relative Lubin-Tate groups*. Proc. AMS 95, 1-4 (1985)

[Ser] Serre J.-P.: *Local Fields*. Springer 1979

[Yos] Yoshida T.: *Local class field theory via Lubin-Tate theory*. Annales de la Faculté des Sciences de Toulouse, Ser. 6, 17-2, 411-438 (2008)