Lectures on Complete Discrete Valuation Fields

1: Discrete Valuation Fields

(1.1). Valuations. One can generalize the properties of the p-adic valuation v_p and proceed to the concept of valuation. Let Γ be an additively written totally ordered abelian group. Add to Γ a formal element $+\infty$ with the properties $a \leqslant +\infty$, $+\infty \leqslant +\infty$, $a + (+\infty) = +\infty$, $(+\infty) + (+\infty) = +\infty$, for each $a \in \Gamma$; denote $\Gamma' = \Gamma \cup \{+\infty\}$.

A map $v: F \to \Gamma'$ with the properties

$$v(\alpha) = +\infty \Leftrightarrow \alpha = 0$$
$$v(\alpha\beta) = v(\alpha) + v(\beta)$$
$$v(\alpha + \beta) \geqslant \min(v(\alpha), v(\beta))$$

is said to be a *valuation* on F; in this case F is said to be a valuation field. The map v induces a homomorphism of $F^\times$ to Γ and its value group $v(F^\times)$ is a totally ordered subgroup of Γ. If $v(F^\times) = \{0\}$, then v is called the *trivial valuation*. It is easy to show that $v(-1) = 0$, and if $v(\alpha) < v(\beta)$, then

$$v(\alpha) \geqslant \min(v(\alpha + \beta), v(-\beta)) \geqslant \min(v(\alpha), v(\beta)) = v(\alpha);$$

thus, if $v(\alpha) \neq v(\beta)$ then $v(\alpha + \beta) = \min(v(\alpha), v(\beta))$.

(1.2). Basic Objects. Let $\mathcal{O}_v = \{\alpha \in F : v(\alpha) \geqslant 0\}$, $\mathcal{M}_v = \{\alpha \in F : v(\alpha) > 0\}$. Then $\mathcal{M}_v$ coincides with the set of non-invertible elements of $\mathcal{O}_v$. Therefore, $\mathcal{O}_v$ is a local ring with the unique *maximal ideal* $\mathcal{M}_v$; $\mathcal{O}_v$ is called the *ring of integers* (with respect to v), and the field $\overline{F}_v = \mathcal{O}_v/\mathcal{M}_v$ is called the *residue field*, or residue class field. The image of an element $\alpha \in \mathcal{O}_v$ in $\overline{F}_v$ is denoted by $\overline{\alpha}$, it is called the *residue* of α in $\overline{F}_v$. The set of invertible elements of $\mathcal{O}_v$ is a multiplicative group $U_v = \mathcal{O}_v - \mathcal{M}_v$, it is called the *group of units*.

LEMMA. *Assume that* $\mathrm{char}(F) \neq \mathrm{char}(\overline{F}_v)$. *Then* $\mathrm{char}(F) = 0$ *and* $\mathrm{char}(\overline{F}_v) = p > 0$.

Proof. Suppose that $\mathrm{char}(F) = p \neq 0$. Then $p = 0$ in F and therefore in $\overline{F}_v$. Hence $p = \mathrm{char}(\overline{F}_v)$. □

(1.3). EXAMPLES OF VALUATIONS AND VALUATION FIELDS.

1. A valuation v on F is said to be *discrete* if the totally ordered group $v(F^\times)$ is isomorphic to the naturally ordered group $\mathbb{Z}$.

For a prime p and a non-zero integer m let $k = v_p(m)$ be the maximal integer such that p^k divides m. Extend v_p to rational numbers putting $v_p(m/n) = v_p(m) - v_p(n)$; $v_p(0) = +\infty$. The p-adic valuation v_p is a discrete valuation with the ring of integers

$$\mathcal{O}_{v_p} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, \quad n \text{ is relatively prime to } p \right\}.$$

The residue field $\overline{\mathbb{Q}}_{v_p}$ is a finite field of order p.

2. Let $F = K(X)$. For an irreducible polynomial $p(X)$ define $v_{p(X)}$ similarly to v_p above. The map $v_{p(X)}$ is a discrete valuation with the ring of integers

$$\mathcal{O}_{v_{p(X)}} = \left\{ \frac{f(X)}{g(X)} : f(X), g(X) \in K[X], g(X) \text{ is relatively prime to } p(X) \right\}$$

and the residue field is $K[X]/p(X)K[X]$ which is a finite algebraic extension of K.

The field F has another discrete valuation trivial on K: $v_\infty(f) = -\deg(f)$, its residue field is K.

(1.4). Discrete valuations. A field F is said to be a *discrete valuation field* if it admits a nontrivial discrete valuation v (see Example 1 in (1.3)). An element $\pi \in \mathcal{O}_v$ is said to be a *prime element* (*uniformizing element*) if $v(\pi)$ generates the group $v(F^\times)$. Without loss of generality we shall often assume that the homomorphism $v: F^\times \to \mathbb{Z}$ is *surjective.*

LEMMA. *Let F be a discrete valuation field, and π be a prime element. Then the ring of integers $\mathcal{O}_v$ is a principal ideal ring, and every proper ideal of $\mathcal{O}_v$ can be written as $\pi^n\mathcal{O}_v$ for some $n > 0$. In particular, $\mathcal{M}_v = \pi\mathcal{O}_v$. The intersection of all proper ideals of $\mathcal{O}_v$ is the zero ideal.*

Each element $\alpha \in F^\times$ can be uniquely written as $\pi^n\varepsilon$ for some $n \in \mathbb{Z}$ and $\varepsilon \in U_v$.

Proof. Let I be a proper ideal of $\mathcal{O}_v$. Then there exists $n = \min\{v(\alpha) : \alpha \in I\}$ and hence $\pi^n\varepsilon \in I$ for some unit ε. It follows that $\pi^n\mathcal{O}_v \subset I \subset \pi^n\mathcal{O}_v$ and $I = \pi^n\mathcal{O}_v$. If α belongs to the intersection of all proper ideals $\pi^n\mathcal{O}_v$ in $\mathcal{O}_v$, then $v(\alpha) = +\infty$, i.e., $\alpha = 0$.

Let $n = v(\alpha)$. Then $\alpha\pi^{-n} \in U_v$ and $\alpha = \pi^n\varepsilon$ for $\varepsilon \in U_v$. If $\pi^n\varepsilon_1 = \pi^m\varepsilon_2$, then $n + v(\varepsilon_1) = m + v(\varepsilon_2)$. As $\varepsilon_1, \varepsilon_2 \in U_v$, we deduce $n = m$, $\varepsilon_1 = \varepsilon_2$. □

(1.5). Completion. Completion of a discrete valuation field is an object which is easier to work with than with the original field.

Let F be a field with a discrete valuation v (as usual, $v(F^\times) = \mathbb{Z}$). F is a metric space with respect to the norm $|\alpha| = (1/2)^{v(\alpha)}$. So one can introduce the notion of a fundamental sequence: a sequence $(\alpha_n)_{n\geqslant 0}$ of elements of F is called a fundamental sequence if for every real c there is $n(c) \geqslant 0$ such that $v(\alpha_n - \alpha_m) \geqslant c$ for $m, n \geqslant n(c)$.

If (α_n) is a fundamental sequence then for every integer r there is n_r such that for all $n, m \geqslant n_r$ we have $v(\alpha_n - \alpha_m) \geqslant r$. We can assume $n_1 \leqslant n_2 \leqslant \ldots$. If for every r there is $n'_r \geqslant n_r$ such that $v(\alpha_{n'_r}) \neq v(\alpha_{n'_r+1})$, then $v(\alpha_{n'_r}) \geqslant r$ and $v(\alpha_n) \geqslant r$ for $n \geqslant n'_r$, and hence $\lim v(\alpha_n) = +\infty$. Otherwise $\lim v(\alpha_n)$ is finite.

LEMMA. *The set A of all fundamental sequences forms a ring with respect to componentwise addition and multiplication. The set of all fundamental sequences $(\alpha_n)_{n\geqslant 0}$ with $\alpha_n \to 0$ as $n \to +\infty$ forms a maximal ideal M of A. The field A/M is a discrete valuation field with its discrete valuation $\widehat{v}$ defined by $\widehat{v}((\alpha_n)) = \lim v(\alpha_n)$ for a fundamental sequence $(\alpha_n)_{n\geqslant 0}$.*

Proof. A sketch of the proof is as follows. It suffices to show that M is a maximal ideal of A. Let $(\alpha_n)_{n\geqslant 0}$ be a fundamental sequence with $\alpha_n \nrightarrow 0$ as $n \to +\infty$. Hence, there is an $n_0 \geqslant 0$ such that $\alpha_n \neq 0$ for $n \geqslant n_0$. Put $\beta_n = 0$ for $n < n_0$ and $\beta_n = \alpha_n^{-1}$ for $n \geqslant n_0$. Then $(\beta_n)_{n\geqslant 0}$ is a fundamental sequence and $(\alpha_n)(\beta_n) \in (1) + M$. Therefore, M is maximal. □

(1.6). A discrete valuation field F is called a *complete discrete valuation field* if every fundamental sequence $(\alpha_n)_{n\geqslant 0}$ is convergent, i.e., there exists $\alpha = \lim \alpha_n \in F$ with respect to v. A field $\widehat{F}$ with a discrete valuation $\widehat{v}$ is called a *completion* of F if it is complete, $\widehat{v}|_F = v$, and F is a dense subfield in $\widehat{F}$ with respect to $\widehat{v}$.

PROPOSITION. *Every discrete valuation field has a completion which is unique up to an isomorphism over F.*

Proof. We verify that the field A/M with the valuation $\widehat{v}$ is a completion of F. F is embedded in A/M by the formula $\alpha \to (\alpha) \mod M$. For a fundamental sequence $(\alpha_n)_{n\geqslant 0}$ and real c, let $n_0 \geqslant 0$ be such that $v(\alpha_n - \alpha_m) \geqslant c$ for all $m, n \geqslant n_0$. Hence, for $\alpha_{n_0} \in F$ we have $\widehat{v}((\alpha_{n_0}) - (\alpha_n)_{n\geqslant 0}) \geqslant c$, which shows that F is dense in A/M. Let $((\alpha_n^{(m)})_n)_m$ be a fundamental sequence in A/M with respect to $\widehat{v}$. Let $n(0)$, $n(1)$, ... be an increasing sequence of integers such that $v(\alpha_{n_2}^{(m)} - \alpha_{n_1}^{(m)}) \geqslant m$ for $n_1, n_2 \geqslant n(m)$. Then $(\alpha_{n(m)}^{(m)})_m$ is a fundamental sequence in F and it is the limit of $((\alpha_n^{(m)})_n)_m$ with respect to $\widehat{v}$ in A/M. Thus, we obtain the existence of the completion A/M, $\widehat{v}$.

If there are two completions $\widehat{F}_1$, $\widehat{v}_1$ and $\widehat{F}_2$, $\widehat{v}_2$, then we put $f(\alpha) = \alpha$ for $\alpha \in F$ and extend this homomorphism by continuity from F, as a dense subfield in $\widehat{F}_1$, to $\widehat{F}_1$. It is easy to verify that the extension $\widehat{f}\colon \widehat{F}_1 \to \widehat{F}_2$ is an isomorphism and $\widehat{v}_2 \circ \widehat{f} = \widehat{v}_1$. □

We shall denote the completion of the field F with respect to v by $\widehat{F}_v$ or simply $\widehat{F}$.

1.7. Examples of complete valuation fields. 1. The completion of $\mathbb{Q}$ with respect to v_p of (1.3) is denoted by $\mathbb{Q}_p$ and is called the *field of p-adic numbers*. Certainly, the completion of $\mathbb{Q}$ with respect to the absolute value $\|\cdot\|_\infty$ of (1.1) is $\mathbb{R}$. Embeddings of $\mathbb{Q}$ in $\mathbb{Q}_p$ for all prime p and in $\mathbb{R}$ is a tool to solve various problems over $\mathbb{Q}$. An example is the *Minkowski–Hasse* Theorem: an equation $\sum a_{ij}X_iX_j = 0$ for $a_{ij} \in \mathbb{Q}$ has a nontrivial solution in $\mathbb{Q}$ if and only if it admits a nontrivial solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all prime p.

The ring of integers of $\mathbb{Q}_p$ is denoted by $\mathbb{Z}_p$ and is called the ring of *p-adic integers*. The residue field of $\mathbb{Q}_p$ is the finite field $\mathbb{F}_p$ consisting of p elements.

2. The completion of $K(X)$ with respect to v_X is the formal power series field $K((X))$ of all formal series $\sum_{-\infty}^{+\infty} \alpha_n X^n$ with $\alpha_n \in K$ and $\alpha_n = 0$ for almost all negative n. The ring of integers with respect to v_X is $K[[X]]$, that is, the set of all formal series $\sum_0^{+\infty} \alpha_n X^n$, $\alpha_n \in K$. Its residue field may be identified with K.

(1.8). Representatives. For simplicity, we will often omit the index v in notations U_v, $\mathcal{O}_v$, $\mathcal{M}_v$, $\overline{F}_v$. We fix a prime element π of F.

A set R is said to be a *set of representatives* for a valuation field F if $R \subset \mathcal{O}$, $0 \in R$ and R is mapped bijectively on $\overline{F}$ under the canonical map $\mathcal{O} \to \mathcal{O}/\mathcal{M} = \overline{F}$. Denote by $\mathrm{rep}\colon \overline{F} \to R$ the inverse bijective map. For a set S denote by $(S)_n^{+\infty}$ the set of all sequences $(a_i)_{i\geqslant n}$, $a_i \in S$. Let $(S)_{-\infty}^{+\infty}$ denote the union of increasing sets $(S)_n^{+\infty}$ where $n \to -\infty$.

The additive group F has a natural filtration

$$\cdots \supset \pi^i\mathcal{O} \supset \pi^{i+1}\mathcal{O} \supset \ldots.$$

The factor filtration of this filtration is easy to calculate: $\pi^i\mathcal{O}/\pi^{i+1}\mathcal{O} \xrightarrow{\sim} \overline{F}$.

LEMMA. *Let F be a complete field with respect to a discrete valuation v. Let $\pi_i \in F$ for each $i \in \mathbb{Z}$ be an element of F with $v(\pi_i) = i$. Then the map*

$$\mathrm{Rep}\colon (\overline{F})_{-\infty}^{+\infty} \to F, \quad (a_i)_{i\in\mathbb{Z}} \mapsto \sum_{-\infty}^{+\infty} \mathrm{rep}(a_i)\pi_i$$

is a bijection. Moreover, if $(a_i)_{i\in\mathbb{Z}} \neq (0)_{i\in\mathbb{Z}}$ then $v(\mathrm{Rep}(a_i)) = \min\{i : a_i \neq 0\}$.

Proof. The map Rep is well defined, because for almost all $i < 0$ we get $\mathrm{rep}(a_i) = 0$ and the series $\sum \mathrm{rep}(a_i)\pi_i$ converges in F. If $(a_i)_{i\in\mathbb{Z}} \neq (b_i)_{i\in\mathbb{Z}}$ and

$$n = \min\{i \in \mathbb{Z} : a_i \neq b_i\},$$

then $v(a_n\pi_n - b_n\pi_n) = n$. Since $v(a_i\pi_i - b_i\pi_i) > n$ for $i > n$, we deduce that

$$v(\mathrm{Rep}(a_i) - \mathrm{Rep}(b_i)) = n.$$

Therefore Rep is injective.

In particular, $v(\mathrm{Rep}(a_i)) = \min\{i : a_i \neq 0\}$. Further, let $\alpha \in F$. Then $\alpha = \pi^n\varepsilon$ with $n \in \mathbb{Z}$, $\varepsilon \in U$. We also get $\alpha = \pi_n\varepsilon'$ for some $\varepsilon' \in U$. Let a_n be the image of ε' in $\overline{F}$; then $a_n \neq 0$ and $\alpha_1 = \alpha - \mathrm{rep}(a_n)\pi_n \in \pi^{n+1}\mathcal{O}$. Continuing in this way for α_1, we obtain a convergent series $\alpha = \sum \mathrm{rep}(a_i)\pi_i$. Therefore, Rep is surjective. □

COROLLARY. *We often take $\pi_n = \pi^n$. Therefore, by the preceding Lemma, every element $\alpha \in F$ can be uniquely expanded as*

$$\boxed{\alpha = \sum_{-\infty}^{+\infty} \theta_i\pi^i, \qquad \theta_i \in R \quad \text{and} \quad \theta_i = 0 \quad \text{for almost all } i < 0}$$

DEFINITION. If $\alpha - \beta \in \pi^n\mathcal{O}$, we write $\alpha \equiv \beta \mod \pi^n$.

(1.9). Units. The group $1 + \pi\mathcal{O}$ is called the *group of principal units* U_1 and its elements are called *principal units*. Introduce also *higher groups of units*: $U_i = 1 + \pi^i\mathcal{O}$ for $i \geqslant 1$.

The multiplicative group $F^\times$ has a natural filtration $F^\times \supset U \supset U_1 \supset U_2 \supset \ldots$. We describe the factor filtration of the introduced filtration on $F^\times$.

PROPOSITION. *Let F be a discrete valuation field. Then*

(1) *The choice of a prime element π ($1 \in \mathbb{Z} \to \pi \in F^\times$) induces an isomorphism $F^\times \simeq U \times \mathbb{Z}$.*

(2) *The canonical map $\mathcal{O} \to \mathcal{O}/\mathcal{M} = \overline{F}$ induces the surjective homomorphism*

$$\lambda_0\colon U \to \overline{F}^\times, \quad \varepsilon \mapsto \overline{\varepsilon};$$

λ_0 maps U/U_1 isomorphically onto $\overline{F}^\times$.

(3) *The map*

$$\lambda_i\colon U_i \to \overline{F}, \qquad 1 + \alpha\pi^i \mapsto \overline{\alpha}$$

for $\alpha \in \mathcal{O}$ induces the isomorphism λ_i of U_i/U_{i+1} onto $\overline{F}$ for $i \geqslant 1$.

Proof. (2) The kernel of λ_0 coincides with U_1 and λ_0 is surjective. (3) The induced map $U_i/U_{i+1} \to \overline{F}$ is a homomorphism, since

$$(1 + \alpha_1\pi^i)(1 + \alpha_2\pi^i) = 1 + (\alpha_1 + \alpha_2)\pi^i + \alpha_1\alpha_2\pi^{2i}.$$

This homomorphism is bijective, since $\lambda_i(1 + \mathrm{rep}(\overline{\alpha})\pi^i) = \overline{\alpha}$. □

COROLLARY. *Let l be not divisible by* $\mathrm{char}(\overline{F})$. *Raising to the lth power induces an automorphism of U_i/U_{i+1} for $i \geqslant 1$. If F is complete, then the group U_i for $i \geqslant 1$ is uniquely l-divisible.*

Proof. If $\varepsilon = 1 + \alpha\pi^i$ with $\alpha \in \mathcal{O}$, then $\varepsilon^l \equiv 1 + l\alpha\pi^i \mod \pi^{i+1}$. Absence of nontrivial l-torsion in the additive group $\overline{F}$ implies the first property. It also shows that U_i has no nontrivial l-torsion.

For an element $\eta = 1 + \beta\pi^i$ with $\beta \in \mathcal{O}^\times$ we have $\eta = (1 + l^{-1}\beta\pi^i)^l\eta_1$ with $\eta_1 \in U_{i+1}$. Applying the same argument to η_1 and so on, we get an lth root of η in F in the case of complete F. □

(1.10). Raising to pth power. Let $\mathrm{char}(\overline{F}) = p > 0$. Lemma (1.2) shows that either $\mathrm{char}(F) = p$ or $\mathrm{char}(F) = 0$. We shall study the operation of raising to the pth power. Denote this homomorphism by

$$\uparrow p\colon \alpha \to \alpha^p.$$

The first and simplest case is $\mathrm{char}(F) = p$.

PROPOSITION. *Let* $\mathrm{char}(F) = \mathrm{char}(\overline{F}) = p > 0$. *Then the homomorphism $\uparrow p$ maps U_i injectively into U_{pi} for $i \geqslant 1$. For $i \geqslant 1$*

$$\boxed{(1 + \alpha\pi^i)^p \equiv 1 + \alpha^p\pi^{pi} \mod \pi^{pi+1}, \quad \alpha \in \mathcal{O}_F}$$

Proof. Since $(1 + \alpha\pi^i)^p = 1 + \alpha^p\pi^{pi}$ and there is no nontrivial p-torsion in $\overline{F}^\times$ and $F^\times$, the assertion follows.

COROLLARY. *Let F be a field of characteristic $p > 0$ and let $\overline{F}$ be perfect, i.e $\overline{F} = \overline{F}^p$. Then $\uparrow p$ maps the quotient group U_i/U_{i+1} isomorphically onto the quotient group U_{pi}/U_{pi+1} for $i \geqslant 1$.*

We now consider the case of $\mathrm{char}(F) = 0$, $\mathrm{char}(\overline{F}) = p > 0$. As $p = 0$ in the residue field $\overline{F}$, we conclude that $p \in \mathcal{M}$ and, therefore, for the surjective discrete valuation v of F we get $v(p) = e \geqslant 1$.

DEFINITION. The number $e = e(F) = v(p)$ is called *the absolute ramification index of F*.

Let π be a prime element in F. Let R be a set of representatives, and let $\overline{\theta}_0 \in \overline{F}$ be the element of $\overline{F}$ uniquely determined by the relation $p - \theta_0\pi^e \in \pi^{e+1}\mathcal{O}$.

PROPOSITION. *Let F be a discrete valuation field of characteristic zero with residue field of positive characteristic p. Then the homomorphism $\uparrow p$ maps U_i to U_{pi} for $i \leqslant e/(p-1)$, and U_i to U_{i+e} for $i \geqslant e/(p-1)$. Moreover, for $\alpha \in \mathcal{O}^\times$*

$$\boxed{(1 + \alpha\pi^i)^p \equiv 1 + \alpha^p\pi^{pi} \mod \pi^{pi+1}, \quad \textit{if } i < e/(p-1), \quad (1)}$$

$$\boxed{(1+\alpha\pi^i)^p \equiv 1+(\alpha^p+\theta_0\alpha)\pi^{pi} \mod \pi^{pi+1}, \quad \text{if } i = e/(p-1) \in \mathbb{Z}, \quad (2)}$$

$$\boxed{(1+\alpha\pi^i)^p \equiv 1+\theta_0\alpha\pi^{i+e} \mod \pi^{i+e+1}, \quad \text{if } i > e/(p-1), \quad (3)}$$

The induced homomorphisms on the quotient filtration are injective in cases (1), (3) *and surjective in case* (3).

If a primitive pth root ζ_p of unity is contained in F, then $v(1-\zeta_p) = e/(p-1)$ and the kernel of the induced homomorphisms in case (2) *is of order p.*

If F is complete, then $U_{e+i} = U_i^p$ for $i \geqslant e/(p-1)$. If F is complete and $e/(p-1) \in \mathbb{Z}$, then the homomorphism in (2) *is injective iff there is no nontrivial p-torsion in $F^\times$.*

Proof. Let $1+\alpha \in U_i$. We get

$$(1+\alpha)^p = 1 + p\alpha + \frac{p(p-1)}{2}\alpha^2 + \cdots + p\alpha^{p-1} + \alpha^p$$

and $v(p\alpha) = e+i$, $v\big(\frac{p(p-1)}{2}\alpha^2\big) = e+2i, \ldots,$ $v(p\alpha^{p-1}) = e+(p-1)i$, $v(\alpha^p) = pi$, so

$$\begin{aligned} v((1+\alpha)^p - 1) &= v(\alpha^p + p\alpha), && \text{if} \quad v(\alpha^p) \neq v(p\alpha), \\ v((1+\alpha)^p - 1) &\geqslant v(\alpha^p + p\alpha), && \text{otherwise.} \end{aligned}$$

Note $v(\alpha^p) \leqslant v(p\alpha)$ if and only if $i \leqslant e/(p-1)$. For a unit α we obtain the first statement of the proposition.

Further, the homomorphism $\uparrow p$ is an isomorphism in case (3) and injective in case (1).

Assume that $\zeta_p \in F$. From the previous $v(1-\zeta_p) = e/(p-1)$ and $e/(p-1) \in \mathbb{Z}$. Therefore, the homomorphism $\overline{\alpha} \mapsto \overline{\alpha}^p + \overline{\theta}_0\overline{\alpha}$ is not injective. Its kernel $\sqrt[p-1]{-\overline{\theta}_0}\,\mathbb{F}_p$ in this case is of order p.

If F is complete, then due to surjectivity of the homomorphisms in case (3) for $i > e/(p-1)$ we get $U_i = U_{i+1}U_{i-e}^p = U_{i+2}U_{i-e}^p = \cdots = U_{i-e}^p$. Now let $e/(p-1)$ be an integer. Assume that the horizontal homomorphism in case (2) is not injective. Let $\overline{\alpha}_0 \in \overline{F}$ satisfy the equation $\overline{\alpha}_0^p + \overline{\theta}_0\overline{\alpha}_0 = 0$. Then $(1+\alpha_0\pi^{e/(p-1)})^p \in U_j$ for some $j > pe/(p-1)$. Therefore $(1+\alpha_0)\pi^{e/(p-1)})^p = \varepsilon_1^p$ for some $\varepsilon_1 \in U_{e/(p-1)+1}$. Thus, $(1+\alpha_0)\pi^{e/(p-1)})\varepsilon_1^{-1} \in U_{e/(p-1)}$ is a primitive pth root of unity. □

COROLLARY. *Let F be a complete discrete valuation field.*

If $\mathrm{char}(F) = 0$, *then $F^{\times n}$ is an open subgroup in $F^\times$ for $n \geqslant 1$. If* $\mathrm{char}(F) = p > 0$, *then $F^{\times n}$ is an open subgroup in $F^\times$ if and only if n is relatively prime to p.*

F contains finitely many roots of unity of order a power of p.

Proof. If $\mathrm{char}(\overline{F}) = 0$, then we get $U_1 \subset F^{\times n}$ for $n \geqslant 1$. It means that $F^{\times n}$ is open. If $\mathrm{char}(\overline{F}) = p$, then $U_1 \subset F^{\times n}$ for $(n,p) = 1$ and $F^{\times n}$ is open. In this case, if $\mathrm{char}(F) = p$, then $1+\pi^i \notin F^{\times p}$ for $(i,p) = 1$. Then $F^{\times p}$ is not open. If $\mathrm{char}(F) = 0$, then we obtain $U_i \subset F^{\times p^m}$ when $i > pe/(p-1) + (m-1)e$. Therefore $F^{\times n}$ is open for $n \geqslant 1$. □

This corollary demonstrates that for complete discrete valuation fields of characteristic 0 with residue field of characteristic p the topological properties are closely related with the algebraic ones. The case $\mathrm{char}(F) = p$ is very different.

(1.11). Product representation. Now we deduce a multiplicative analog of the expansion in the corollary of (1.8).

PROPOSITION (HENSEL). *Let F be a complete discrete valuation field. Let R be a set of representatives. Then for $\alpha \in F^\times$ there exist uniquely determined $n \in \mathbb{Z}$, $\theta_i \in R$ for $i \geqslant 0$, $\theta_0 \in R^\times$, such that α can be expanded in the convergent product*

$$\boxed{\alpha = \pi^n \theta_0 \prod_{i \geqslant 1} (1 + \theta_i \pi^i)}$$

Proof. The existence and uniqueness of n and θ_0 immediately follow. Assume that $\varepsilon \in U_m$, then find $\theta_m \in R$ with $\varepsilon(1 + \theta_m \pi^m)^{-1} \in U_{m+1}$. Proceeding by induction, we obtain an expansion of α in a convergent product. If there are two such expansions $\prod(1 + \theta_i \pi^i) = \prod(1 + \theta_i' \pi^i)$, then the residues $\overline{\theta}_i$, $\overline{\theta_i'}$ coincide in $\overline{F}$. Thus, $\theta_i = \theta_i'$. □

(1.12). $\mathbb{Z}_p$-Structure of The Group of Principal Units. Everywhere in this section F is a complete discrete valuation field with residue field of positive characteristic p.

If $\varepsilon \in U_1$ then $\varepsilon^{p^n} \to 1$ as $n \to +\infty$. This enables us to define

$$\varepsilon^a = \lim_{n \to \infty} \varepsilon^{a_n} \qquad \text{if} \quad \lim_{n \to \infty} a_n = a \in \mathbb{Z}_p, \quad a_n \in \mathbb{Z}.$$

LEMMA. *Let $\varepsilon \in U_1$, $a \in \mathbb{Z}_p$. Then $\varepsilon^a \in U_1$ is well defined and $\varepsilon^{a+b} = \varepsilon^a \varepsilon^b$, $\varepsilon^{ab} = (\varepsilon^a)^b$, $(\varepsilon\eta)^a = \varepsilon^a \eta^a$ for $\varepsilon, \eta \in U_1$, $a, b \in \mathbb{Z}_p$. The multiplicative group U_1 is a $\mathbb{Z}_p$-module under the operation of raising to a power. Moreover, the structure of the $\mathbb{Z}_p$-module U_1 is compatible with the topologies of $\mathbb{Z}_p$ and U_1.*

Proof. Assume that $\lim a_n = \lim b_n$; hence $a_n - b_n \to 0$ as $n \to +\infty$ and $\lim \varepsilon^{a_n - b_n} = 1$. A map $\mathbb{Z}_p \times U_1 \to U_1$ ($(a, \varepsilon) \to \varepsilon^a$) is continuous with respect to the p-adic topology on $\mathbb{Z}_p$ and the discrete valuation topology on U_1. This argument can be applied to verify the other assertions of the lemma. □

PROPOSITION. *Let F be of characteristic p with perfect residue field. Let R be a set of representatives, and let R_0 be a subset of it such that the residues of its elements in $\overline{F}$ form a basis of $\overline{F}$ as a vector space over $\mathbb{F}_p$. Let an index-set J numerate the elements of R_0. Let v_p be the p-adic valuation.*

Then every element $\alpha \in U_1$ can be uniquely represented as a convergent product

$$\boxed{\alpha = \prod_{\substack{(i,p)=1 \\ i>0}} \prod_{j \in J} (1 + \theta_j \pi^i)^{a_{ij}}, \quad \theta_j \in R_0, a_{ij} \in \mathbb{Z}_p}$$

and the sets $J_{i,c} = \{j \in J : v_p(a_{ij}) \leqslant c\}$ are finite for all $c \geqslant 0$, $(i, p) = 1$.

Proof. We first show that the element α can be written modulo U_n for $n \geqslant 1$ in the desired form with $a_{ij} \in \mathbb{Z}$. Proceeding by induction, it will suffice to consider an element $\varepsilon \in U_n$ modulo U_{n+1}. Let $\varepsilon \equiv 1 + \theta\pi^n \mod U_{n+1}$, $\theta \in R$. If $(n, p) = 1$, then one can find $\theta_1, \ldots, \theta_m \in R_0$ and $b_1, \ldots, b_m \in \mathbb{Z}$ such that $1 + \theta\pi^n \equiv \prod_{k=1}^m (1 + \theta_k \pi^n)^{b_k} \mod U_{n+1}$ for some m. If $n = p^s n'$ with an integer n', $(n', p) = 1$, then one can find $\theta_1, \ldots, \theta_m \in R_0$ and

$b_1, \dots, b_m \in \mathbb{Z}$ such that $1 + \theta\pi^n \equiv \prod_{k=1}^{m}(1 + \theta_k\pi^{n'})^{p^s b_k} \mod U_{n+1}$ for some m. Now due to the continuity we get the desired expression for $\alpha \in U_1$ with the above conditions on the sets $J_{i,c}$.

Assume that there is a convergent product for 1 with $\theta_j,\ a_{ij}$. Let $(i_0, p) = 1$ and $j_0 \in J$ be such that $n = p^{v_p(a_{i_0 j_0})} i_0 \leqslant p^{v_p(a_{ij})} i$ for all $(i, p) = 1,\ j \in J$. Then the choice of R_0 imply $\prod(1 + \theta_j\pi^i)^{a_{ij}} \notin U_{n+1}$, which concludes the proof. □

COROLLARY. *The group U_1 has a free topological basis $1 + \theta_j\pi^i$ where where $\theta_j \in R_0$, $(i, p) = 1$.*

If $e = v(p)$ is divisible by $p - 1$, let $\psi\colon \overline{F} \to \overline{F}$ be the map $\overline{\alpha} \mapsto \overline{\alpha}^p + \overline{\theta}_0\overline{\alpha}$. Then raising to the pth power in case (2) of the proposition in (1.10) is described by ψ.

PROPOSITION. *Let F be of characteristic 0 with perfect residue field of characteristic p.*

Let R be a set of representatives and let R_0 (resp. R_0') be a subset of it such that the residues of its elements in $\overline{F}$ form a basis of $\overline{F}$ as a vector space over $\mathbb{F}_p$ (resp. are $\mathbb{F}_p$-generators of $\overline{F}/\psi(\overline{F})$). Let the index-set J (resp. J') numerate the elements of R_0 (resp. R_0'). Let

$$I = \{i : i \in \mathbb{Z}, 1 \leqslant i < pe/(p-1), (i, p) = 1\}.$$

Then every element $\alpha \in U_1$ can be represented as a convergent product

$$\boxed{\alpha = \prod_{i \in I}\prod_{j \in J}(1 + \theta_j\pi^i)^{a_{ij}} \prod_{j \in J'}(1 + \eta_j\pi^{pe/(p-1)})^{a_j}, \quad \theta_j \in R_0, \eta_j \in R_0', a_{ij}, a_j \in \mathbb{Z}_p}$$

(*the second product occurs when $e/(p-1)$ is an integer*) *and the sets*

$$J_{i,c} = \{j \in J : v_p(a_{ij}) \leqslant c\}, \quad J_c' = \{j \in J' : v_p(a_j) \leqslant c\}$$

are finite for all $c \geqslant 0,\ i \in I$.

Proof. We shall show how to obtain the required form for $\varepsilon \in U_n$ modulo U_{n+1}. Let $\varepsilon = 1 + \theta\pi^n \mod U_{n+1},\ \theta \in R$. There are four cases to consider:

(1) $n \in I$. One can find $\theta_1, \dots, \theta_m \in R_0$ and $b_1, \dots, b_m \in \mathbb{Z}$ satisfying the congruence $1 + \theta\pi^n \equiv \prod_{k=1}^{m}(1 + \theta_k\pi^n)^{b_k} \mod U_{n+1}$ for some m.

(2) $n < pe/(p-1)$, $n = p^s n'$ with $n' \in I$. Then there exist $\theta_1, \dots, \theta_m \in R_0,\ b_1, \dots, b_m \in \mathbb{Z}$ such that

$$1 + \theta\pi^n \equiv \prod_{k=1}^{m}(1 + \theta_k\pi^{n'})^{p^s b_k} \mod U_{n+1} \quad \text{for some } m\,.$$

(3) $e/(p-1) \in \mathbb{Z},\ n = pe/(p-1)$. The definition of R_0' imply that if $n = p^s n'$ with $n' \in I$, then there exist $\theta_1, \dots, \theta_m \in R_0,\ \eta_1, \dots, \eta_r \in R_0',\ b_1, \dots, b_m,\ c_1, \dots, c_r \in \mathbb{Z}$ such that

$$1 + \theta\pi^n \equiv \prod_{k=1}^{m}(1 + \theta_k\pi^{n'})^{p^s b_k} \prod_{l=1}^{r}(1 + \eta_l\pi^n)^{c_l} \mod U_{n+1} \quad \text{for some } m, r\,.$$

(4) $n > pe/(p-1)$. If $d = \min\{d : n - de \leqslant pe/(p-1)\}$ and $n' = n - de$, then

$$1 + \theta\pi^n \equiv (1 + \theta'\pi^{n'})^{p^d} \mod U_{n+1} \quad \text{for some } \theta' \in R.$$

Now applying the arguments of the preceding cases to $1+\theta'\pi^{n'}$, we can write $1+\theta\pi^n \mod U_{n+1}$ in the required form. □

COROLLARY. *Let F be of characteristic 0 with perfect residue field of characteristic p.*

(1) *If F does not contain nontrivial pth roots of unity then the representation in the proposition is unique. Therefore the elements of the proposition form a topological basis of $U_{1,F}$.*
(2) *If F contains a nontrivial pth root of unity, let r be the maximal integer such that F contains a primitive p^rth root of unity. Then the numbers a_{ij}, a_j of the proposition are determined uniquely modulo p^r. Therefore the elements of the proposition form a topological basis of $U_{1,F}/U_{1,F}^{p^r}$.*
(3) *If the residue field of F is finite then U_1 is the direct sum of a free $\mathbb{Z}_p$-module of rank ef and the torsion part.*

Proof. (1) If $\zeta_p \notin F$ then all horizontal homomorphisms of the diagrams in the second Proposition of (1.10) are injective.

(2) Argue by induction on r. Write a primitive p^rth root ζ_{p^r} in the form

$$\zeta_{p^r} = \prod_{i\in I}\prod_{j\in J}(1+\theta_j\pi^i)^{c_{ij}} \prod_{j\in J'}(1+\eta_j\pi^{pe/(p-1)})^{c_j}$$

and raise the right hand side to the p^rth power which demonstrates the non-uniqueness.

Now if

$$1 = \prod_{i\in I}\prod_{j\in J}(1+\theta_j\pi^i)^{a_{ij}} \prod_{j\in J'}(1+\eta_j\pi^{pe/(p-1)})^{a_j}$$

then we deduce that $a_{ij} = pb_{ij}, a_j = pb_j$ with p-adic integers b_{ij}, b_j. Then

$$\prod_{i\in I}\prod_{j\in J}(1+\theta_j\pi^i)^{b_{ij}} \prod_{j\in J'}(1+\eta_j\pi^{pe/(p-1)})^{b_j}$$

is a pth root of unity, and so is equal to

$$\Big(\prod_{i\in I}\prod_{j\in J}(1+\theta_j\pi^i)^{c_{ij}} \prod_{j\in J'}(1+\eta_j\pi^{pe/(p-1)})^{c_j}\Big)^{p^{r-1}c}$$

for some integer c. Now by the induction assumption all $b_{ij} - p^{r-1}cc_{ij}, b_j - p^{r-1}cc_j$ are divisible by p^{r-1}. Thus, all a_{ij}, a_j are divisible by p^r.

(3) If the residue field of F is finite then U_1 is a module of finite type over the principal ideal domain $\mathbb{Z}_p$, so by the structure theorem on such modules it is a direct sum of a free module and a finite torsion module. If a primitive pth root of unity is in F, then the kernel of ψ is of order p. Hence $|\overline{F} : \psi(\overline{F})| = p$, since $\overline{F}$ is finite. The cardinality of I is equal to $e = [pe/(p-1)] - [[pe/(p-1)]/p]$. □

2: Extensions of Complete Fields

(2.1). Henselian Property. Let A be a commutative ring. For two polynomials $f(X) = a_nX^n + \dots a_0$, $g(X) = b_mX^m + \dots + b_0$ their resultant is the determinant of the matrix

$$\begin{pmatrix} a_n & a_{n-1} & \dots & a_0 & & & \\ & a_n & a_{n-1} & \dots & a_0 & & \\ & & \ddots & \ddots & \ddots & \ddots & \\ & & & a_n & a_{n-1} & \dots & a_0 \\ b_m & a_{m-1} & \dots & b_0 & & & \\ & b_m & b_{m-1} & \dots & b_0 & & \\ & & \ddots & \ddots & \ddots & \ddots & \\ & & & b_m & b_{m-1} & \dots & b_0 \end{pmatrix}.$$

This determinant $R(f,g)$ is zero iff f and g have a common root; in general $R(f,g) = ff_1 + gg_1$ for some polynomials $f_1, g_1 \in A[X]$. If $f(X) = a_n \prod_{i=1}^{n}(X - \alpha_i)$, $g(X) = b_m \prod_{j=1}^{m}(X - \beta_j)$, then their resultant $R(f,g)$ is $a_n^m b_m^n \prod_{i,j}(\alpha_i - \beta_j)$. In particular, $R(X - a, g(X)) = g(a)$.

If $f, g \in \mathcal{O}[X]$ then $R(f,g) \in \mathcal{O}$. We shall use the following properties of the resultant: if $f \equiv f \mod \mathcal{M}[X]$ then $R(f,g) \equiv R(f_1,g) \mod \mathcal{M}$; if $R(f,g) \in \mathcal{M}^s \setminus \mathcal{M}^{s+1}$ then $\mathcal{M}^s[X] \subset f\mathcal{O}[X] + g\mathcal{O}[X]$.

Let F be a complete discrete valuation field with the ring of integers $\mathcal{O}$, the maximal ideal $\mathcal{M}$, and the residue field $\overline{F}$. For a polynomial $f(X) = a_nX^n + \dots + a_0 \in \mathcal{O}[X]$ we will denote the polynomial $\overline{a}_nX^n + \dots + \overline{a}_0$ by $\overline{f}(X) \in \overline{F}[X]$. We will write

$$f(X) \equiv g(X) \mod \mathcal{M}^m$$

if $f(X) - g(X) \in \mathcal{M}^m[X]$.

PROPOSITION. *Let g_0, h_0, f be polynomials over $\mathcal{O}$ such that* $\deg f = \deg g_0 + \deg h_0$ *and the leading coefficient of f coincides with that of g_0h_0. Let*

$$R(g_0,h_0) \notin \mathcal{M}^{s+1}, \quad f \equiv g_0h_0 \mod \mathcal{M}^{2s+1}$$

for an integer $s \geqslant 0$.

Then there exist polynomials $g(X), h(X)$ such that

$$f = gh, \qquad \deg g = \deg g_0, \quad \deg h = \deg h_0, \quad g \equiv g_0 \mod \mathcal{M}^{s+1}, h \equiv h_0 \mod \mathcal{M}^{s+1}.$$

Proof. We first construct polynomials $g_i(X), h_i(X) \in \mathcal{O}[X]$ with the following properties: $\deg(g_i - g_0) < \deg g_0$, $\deg(h_i - h_0) < \deg h_0$

$$g_i(X) \equiv g_{i-1}(X) \mod \mathcal{M}^{i+s}, \quad h_i(X) \equiv h_{i-1}(X) \mod \mathcal{M}^{i+s},$$
$$f(X) \equiv g_i(X)h_i(X) \mod \mathcal{M}^{i+2s+1}.$$

Proceeding by induction, we can assume that the polynomials $g_j(X), h_j(X)$, for $j \leqslant i-1$, have been constructed. For a prime element π put

$$g_i(X) = g_{i-1}(X) + \pi^{i+s}G_i(X), \quad h_i(X) = h_{i-1}(X) + \pi^{i+s}H_i(X)$$

with $G_i(X), H_i(X) \in \mathcal{O}[X]$, $\deg G_i(X) < \deg g_0(X)$, $\deg H_i(X) < \deg h_0(X)$. Then

$$g_i(X)h_i(X) - g_{i-1}(X)h_{i-1}(X) \equiv \pi^{i+s}\big(g_{i-1}(X)H_i(X) + h_{i-1}(X)G_i(X)\big) \mod \mathcal{M}^{i+2s+1}.$$

Since by the induction assumption $f(X) - g_{i-1}(X)h_{i-1}(X) = \pi^{i+2s}f_1(X)$ for a suitable $f_1(X) \in \mathcal{O}[X]$ of degree smaller than that of f, we deduce that it suffices for $G_i(X)$, $H_i(X)$ to satisfy the congruence $\pi^s f_1(X) \equiv g_{i-1}(X)H_i(X) + h_{i-1}(X)G_i(X) \mod \mathcal{M}^{s+1}$..

However, $R(g_{i-1}(X), h_{i-1}(X)) \equiv R(g_0(X), h_0(X)) \not\equiv 0 \mod \mathcal{M}^{s+1}$. Then the properties of the resultant imply the existence of polynomials $\widetilde{G}_i$, $\widetilde{H}_i$ satisfying the congruence. Write $\widetilde{G}_i = g_{i-1}q + G_{i-1}$ with polynomial G_{i-1} of degree smaller than that of g_{i-1}. Then it is easy to see that the degree of $H_i = \widetilde{H}_i + qh_{i-1}$ is smaller that the degree of h_{i-1}. The polynomials G_i, H_i are the required ones.

Now put $g(X) = \lim g_i(X)$, $h(X) = \lim h_i(X)$ and get $f(X) = g(X)h(X)$. □

The following statement is often called Hensel Lemma; it was proved by *K. Hensel* for p-adic numbers and by *K. Rychlík* for complete valuation fields.

COROLLARY 1. *Let f, g_0, h_0 be monic polynomials with coefficients in $\mathcal{O}$. Let $\overline{f} = \overline{g}_0\overline{h}_0$ and suppose that $\overline{g}_0, \overline{h}_0$ are relatively prime in $\overline{F}[X]$. Then there exist monic polynomials g, h with coefficients in $\mathcal{O}$, such that*

$$f(X) = g(X)h(X), \quad \overline{g}(X) = \overline{g}_0(X), \ \overline{h}(X) = \overline{h}_0(X).$$

Proof. We have $R(f_0(X), g_0(X)) \notin \mathcal{M}$ and we can apply the previous proposition for $s = 0$. The polynomials $g(X)$ and $h(X)$ may be assumed to be monic, as it follows from the proof of the proposition. □

Valuation fields satisfying the assertion of Corollary 1 are said to be *Henselian.* Corollary 1 demonstrates that complete discrete valuation fields are Henselian.

COROLLARY 2. *Let $f(X)$ be a monic polynomial with coefficients in $\mathcal{O}$. Let*

$$f(\alpha_0) \in \mathcal{M}^{2s+1}, \quad f'(\alpha_0) \notin \mathcal{M}^{s+1}$$

for some $\alpha_0 \in \mathcal{O}$ and integer $s \geqslant 0$. Then there exists $\alpha \in \mathcal{O}$ such that $\alpha - \alpha_0 \in \mathcal{M}^{s+1}$ and $f(\alpha) = 0$.

Proof. Put $g_0(X) = X - \alpha_0$ and write $f(X) = f_1(X)(X - \alpha_0) + \delta$ with $\delta \in \mathcal{O}$. Then $\delta \in \mathcal{M}^{2s+1}$. Put $h_0(X) = f_1(X) \in \mathcal{O}[X]$. Hence $f(X) \equiv g_0(X)h_0(X) \mod \mathcal{M}^{2s+1}$ and $f'(\alpha_0) = h_0(\alpha_0) \notin \mathcal{M}^{s+1}$. Hence $R(g_0(X), h_0(X)) \notin \mathcal{M}^{s+1}$, and the proposition implies the existence of polynomials $g(X), h(X) \in \mathcal{O}[X]$ such that $g(X) = X - \alpha, \alpha \equiv \alpha_0 \mod \mathcal{M}^{s+1}$, and $f(X) = g(X)h(X)$. □

EXAMPLE. If the residue field of F is finite $\mathbb{F}_q$, then for every $a \in \mathbb{F}_q^\times$ the polynomial $f(X) = X^{q-1} - 1$ has a root α such that $\overline{\alpha} = a$. So one has *multiplicative representatives* of $\mathbb{F}_q$ consisting of 0 and all roots of unity in F of order dividing $q-1$ (or, equivalently, all roots of unity in F of order prime to p).

COROLLARY 3. *For every positive integer m there is n such that $1 + \mathcal{M}^n \subset F^{\times m}$.*

Proof. Put $f_a(X) = X^m - a$ with $a \in 1+\mathcal{M}^n$. Let $m \in \mathcal{M}^s \setminus \mathcal{M}^{s+1}$. Then $f_a'(1) \in \mathcal{M}^s \setminus \mathcal{M}^{s+1}$. Therefore for every $a \in 1+\mathcal{M}^{2s+1}$ the polynomial $f_a(X)$ has a root $\alpha \equiv 1 \mod \mathcal{M}^{s+1}$ due to Corollary 2. □

LEMMA. *Let $f(X) = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_0$ be an irreducible polynomial with coefficients in F. Then the condition $\alpha_0 \in \mathcal{O}$ implies $\alpha_i \in \mathcal{O}$ for $0 \leqslant i \leqslant n-1$.*

Proof. Assume that $\alpha_0 \in \mathcal{O}$ and that j is the maximal such that $v(\alpha_j) = \min_{0\leqslant i\leqslant n-1} v(\alpha_i)$. If $\alpha_j \notin \mathcal{O}$, then put

$$\begin{aligned} f_1(X) &= \alpha_j^{-1} f(X), \\ g_0(X) &= X^j + \alpha_j^{-1}\alpha_{j-1}X^{j-1} + \cdots + \alpha_j^{-1}\alpha_0, \\ h_0(X) &= \alpha_j^{-1}X^{n-j} + 1 \end{aligned}$$

We have $\overline{f}_1(X) = \overline{g}_0(X)\overline{h}_0(X)$, and $\overline{g}_0(X), \overline{h}_0(X)$ are relatively prime. Therefore, by the proposition $f_1(X)$ and $f(X)$ are not irreducible. □

(2.2). e and f. Let F be a field and L an extension of F with a valuation $w: L \to \Gamma'$. Then w induces the valuation $w_0 = w|_F: F \to \Gamma'$ on F. In this context L/F is said to be an *extension of valuation fields*. The group $w_0(F^\times)$ is a totally ordered subgroup of $w(L^\times)$ and the index of $w_0(F^\times)$ in $w(L^\times)$ is called the *ramification index* $e(L/F, w)$. The ring of integers $\mathcal{O}_{w_0}$ is a subring of the ring of integers $\mathcal{O}_w$ and the maximal ideal $\mathcal{M}_{w_0}$ coincides with $\mathcal{M}_w \cap \mathcal{O}_{w_0}$. Hence, the residue field $\overline{F}_{w_0}$ can be considered as a subfield of the residue field $\overline{L}_w$. Therefore, if α is an element of $\mathcal{O}_{w_0}$, then its residue in the field $\overline{F}_{w_0}$ can be identified with the image of α as an element of $\mathcal{O}_w$ in the field $\overline{L}_w$. We shall denote this image of α by $\overline{\alpha}$. The degree of the extension $\overline{L}_w/\overline{F}_{w_0}$ is called the *intertia degree* $f(L/F, w)$. An immediate consequence is the following lemma.

LEMMA. *Let L be an extension of F and let w be a valuation on L. Let $L \supset M \supset F$ and let w_0 be the induced valuation on M. Then*

$$\begin{aligned} e(L/F, w) &= e(L/M, w)\, e(M/F, w_0), \\ f(L/F, w) &= f(L/M, w)\, f(M/F, w_0). \end{aligned}$$

(2.3). Extension of Discrete Valuation. Assume that L/F is a finite extension and w_0 is a discrete valuation. Let elements $\alpha_1, \ldots, \alpha_e \in L^\times$ for natural $e \leqslant e(L/F, w)$ be such that $w(\alpha_1) + w(F^\times), \ldots, w(\alpha_e) + w(F^\times)$ are distinct in $w(L^\times)/w(F^\times)$. If $\sum_{i=1}^e c_i\alpha_i = 0$ holds with $c_i \in F$, then, as $w(c_i\alpha_i)$ are all distinct, we get $w\left(\sum_{i=1}^e c_i\alpha_i\right) = \min_{1\leqslant i\leqslant e} w(c_i\alpha_i)$ and so $c_i = 0$ for $1 \leqslant i \leqslant e$. This shows that $\alpha_1, \ldots, \alpha_e$ are linearly independent over F and hence $e(L/F, w)$ is finite. Let π be a prime element with respect to w_0. Then we deduce that there are only a finite number of positive elements in $w(L^\times)$ which are $\leqslant w(\pi)$. Consider the smallest positive element in $w(L^\times)$. It generates the group $w(L^\times)$, and we conclude that w is a discrete valuation. Thus, we have proved the following result.

LEMMA. *Let L/F be a finite extension and w_0 discrete for a valuation w on L. Then w is discrete.*

(2.4). e, f **for Complete Fields.** Let F and L be fields with discrete valuations v and w respectively and $F \subset L$. The valuation w is said to be an *extension of the valuation* v, if $w_0 = cv$ for a positive c. We shall write $w|v$ and use the notations $e(w|v), f(w|v)$ instead of $e(L/F, w), f(L/F, w)$. If $\alpha \in F$ then $w(\alpha) = e(w|v)v(\alpha)$.

LEMMA. *Let L be a finite extension of F of degree n; then*

$$e(w|v)f(w|v) \leqslant n.$$

Proof. Let $e = e(w|v)$ and let f be a positive integer such that $f \leqslant f(w|v)$. Let $\theta_1, \ldots, \theta_f$ be elements of $\mathcal{O}_w$ such that their residues in $\overline{L}_w$ are linearly independent over $\overline{F}_v$. It suffices to show that $\{\theta_i \pi_w^j\}$ are linearly independent over F for $1 \leqslant i \leqslant f, 0 \leqslant j \leqslant e-1$. Assume that

$$\sum_{i,j} c_{ij}\theta_i \pi_w^j = 0$$

for $c_{ij} \in F$ and not all $c_{ij} = 0$.

Multiplying the coefficients c_{ij} by a suitable power of π_v, we may assume that $c_{ij} \in \mathcal{O}_v$ and not all $c_{ij} \in \mathcal{M}_v$. Note that if $\sum_i c_{ij}\theta_i \in \mathcal{M}_w$, then $\sum_i \overline{c}_{ij}\overline{\theta}_i = 0$ and so $c_{ij} \in \mathcal{M}_v$. Therefore, there exists an index j such that $\sum_i c_{ij}\theta_i \notin \mathcal{M}_w$. Let j_0 be the minimal such index. Then $j_0 = w(\sum c_{ij}\theta_i \pi_w^j)$, which is impossible. We conclude that all $c_{ij} = 0$. Hence, $ef \leqslant n$ and $e(w|v)f(w|v) \leqslant n$. □

EXAMPLE. Let $\widehat{F}$ be the completion of F with the discrete valuation $\widehat{v}$. Then $e(\widehat{v}|v) = 1, f(\widehat{v}|v) = 1$. Note that if F is not complete, then $|\widehat{F} : F| \neq e(\widehat{v}|v)f(\widehat{v}|v)$. On the contrary, in the case of complete discrete valuation fields we have

PROPOSITION. *Let L be an extension of F and let F, L be complete with respect to discrete valuations v, w. Let $w|v, f = f(w|v)$ and $e = e(w|v) < \infty$. Let $\pi_w \in L$ be a prime element with respect to w and $\theta_1, \ldots, \theta_f$ elements of $\mathcal{O}_w$ such that their residues form a basis of $\overline{F}_w$ over $\overline{F}_v$. Then $\{\theta_i \pi_w^j\}$ is a basis of the F-space L and of the $\mathcal{O}_v$-module $\mathcal{O}_w$, with $1 \leqslant i \leqslant f, 0 \leqslant j \leqslant e-1$. If $f < \infty$, then L/F is a finite extension of degree $n = ef$.*

Proof. Let R be a set of representatives for F. Then the set

$$R' = \Big\{\sum_{i=1}^{f} a_i\theta_i : a_i \in R \text{ and almost all } a_i = 0\Big\}$$

is the set of representatives for L. For a prime element π_v with respect to v put $\pi_m = \pi_v^k \pi_w^j$, where $m = ek + j, 0 \leqslant j < e$. Using Corollary (1.8) we obtain that an element $\alpha \in L$ can be expressed as a convergent series

$$\alpha = \sum_m \eta_m \pi_m \qquad \text{with} \quad \eta_m \in R'.$$

Writing

$$\eta_m = \sum_{i=1}^{f} \eta_{m,i}\theta_i \qquad \text{with} \quad \eta_{m,i} \in R,$$

we get

$$\alpha = \sum_{i,j} \Big(\sum_{k} \eta_{ek+j,i} \pi_v^k \Big) \theta_i \pi_w^j .$$

Thus, α can be expressed as $\sum \rho_{i,j} \theta_i \pi_w^j$ with

$$\rho_{i,j} = \sum_{k} \eta_{ek+j,i} \pi_v^k \in F, \quad 1 \leqslant i \leqslant f, 0 \leqslant j \leqslant e-1.$$

By the proof of the previous lemma this expression for α is unique. We conclude that $\{\theta_i \pi_w^j\}$ form a basis of L over F and of $\mathfrak{O}_w$ over $\mathfrak{O}_v$. □

(2.5). Uniqueness of Extension of Discrete Valuation From a Complete Field. Further we shall assume that $v(F^\times) = \mathbb{Z}$ for a discrete valuation v. Then $e(w|v) = |\mathbb{Z} : w(F^\times)|$ for an extension w of v.

THEOREM. *Let F be a complete field with respect to a discrete valuation v and L a finite extension of F. Then there is precisely one extension w on L of the valuation v and $w = \frac{1}{f} v \circ N_{L/F}$ with $f = f(w|v)$. The field L is complete with respect to w.*

Proof. Let $w' = v \circ N_{L/F}$. First we verify that w' is a valuation on L. It is clear that $w'(\alpha) = +\infty$ if and only if $\alpha = 0$ and $w'(\alpha\beta) = w'(\alpha) + w'(\beta)$. Assume that $w'(\alpha) \geqslant w'(\beta)$ for $\alpha, \beta \in L^\times$, then

$$w'(\alpha + \beta) = w'(\beta) + w'\Big(1 + \frac{\alpha}{\beta}\Big)$$

and it suffices to show that if $w'(\gamma) \geqslant 0$, then $w'(1+\gamma) \geqslant 0$. Let

$$f(X) = X^m + a_{m-1} X^{m-1} + \cdots + a_0$$

be the monic irreducible polynomial of γ over F. Then we get $(-1)^m a_0 = N_{F(\gamma)/F}(\gamma)$ and if $s = |L : F(\gamma)|$, then $((-1)^m a_0)^s = N_{L/F}(\gamma)$. We deduce that $v(a_0) \geqslant 0$, and making use of (2.1), we get $v(a_i) \geqslant 0$ for $0 \leqslant i \leqslant m-1$. Now

$$(-1)^m N_{F(\gamma)/F}(1+\gamma) = f(-1) = (-1)^m + a_{m-1}(-1)^{m-1} + \cdots + a_0,$$

hence

$$v\left(N_{F(\gamma)/F}(1+\gamma)\right) \geqslant 0 \quad \text{and} \quad v\left(N_{L/F}(1+\gamma)\right) \geqslant 0,$$

i.e., $w'(1+\gamma) \geqslant 0$. Thus, we have shown that w' is a valuation on L.

Let $n = |L : F|$; then $w'(\alpha) = nv(\alpha)$ for $\alpha \in F^\times$. Hence, the valuation $(1/n)w'$ is an extension of v to L (note that $(1/n)w'(L^\times) \neq \mathbb{Z}$ in general). Let $e = e(L/F, (1/n)w')$; e is finite. Put $w = (e/n)w' : L^\times \to \mathbb{Q}$, hence $w(L^\times) = w(\pi_w)\mathbb{Z} = \mathbb{Z}$ with a prime element π_w with respect to w. Therefore, $w = (e/n)\, v \circ N_{L/F}$ is at once a discrete valuation on L and an extension of v.

Let $\gamma_1, \ldots, \gamma_n$ be a basis of the F-vector space L. By induction on r, $1 \leqslant r \leqslant n$, we shall show that

$$\sum_{i=1}^{r} a_i^{(m)} \gamma_i \to 0, \quad m \to \infty \Longleftrightarrow a_i^{(m)} \to 0 \quad m \to \infty \quad \text{for } i = 1, \ldots, r$$

where $a_i^{(m)} \in F$.

The left arrow and the case $r = 1$ are clear. For the induction step we can assume that $a_i^{(m)} \not\to 0$ for each $i = 1, \ldots, r$. Therefore we can assume that $v(a_i^{(m)})$ is bounded for $i = 1, \ldots, r$. Hence

$$\gamma_1 + \sum_{i=2}^{r} b_i^{(m)}\gamma_i = \left(a_1^{(m)}\right)^{-1} \sum_{i=1}^{r} a_i^{(m)}\gamma_i \to 0,$$

where $b_i^{(m)} = (a_1^{(m)})^{-1} a_i^{(m)}$. Then

$$\sum_{i=2}^{r}(b_i^{(m)} - b_i^{(m+1)}) = \sum_{i=2}^{r} b_i^{(m)}\gamma_i - \sum_{i=2}^{r} b_i^{(m+1)}\gamma_i \to 0,$$

and the induction hypothesis shows that $b_i^{(m)} - b_i^{(m+1)} \to 0$ for $i = 2, \ldots, r$. Thus, each $(b_i^{(m)})_m$ converges to, say, $b_i \in F$. Finally, the sequence $\gamma_1 + \sum_{i=2}^{r} b_i^{(m)}\gamma_i$ converges both to 0 and to $\gamma_1 + \sum_{i=2}^{r} b_i\gamma_i$, so $0 = \gamma_1 + \sum_{i=2}^{r} b_i\gamma_i$ which contradicts the choice of γ_i.

Similarly one shows that a sequence $\sum_{i=1}^{r} a_i^{(m)}\gamma_i$ is fundamental if and only if $a_i^{(m)}$ is fundamental for each $i = 1, \ldots, r$.

Thus, the completeness of F implies the completeness of its finite extension L with respect to any extension of v. We also have the uniqueness of the extension.

□

COROLLARY. *Let L be a finite Galois extension of F. Then $w \circ \sigma = w$ for the discrete valuation w on L and $\sigma \in \mathrm{Gal}(L/F)$. If π is a prime element in L, then $\sigma\pi$ is a prime element and $\sigma\mathcal{O}_w = \mathcal{O}_w$, $\sigma\mathcal{M}_w = \mathcal{M}_w$.*

LEMMA. *Let L/F be a finite extension. Let $\alpha \in \mathcal{O}_w$ and let $f(X)$ be the monic irreducible polynomial of α over F. Then $f(X) \in \mathcal{O}_v[X]$. Conversely, let $f(X)$ be a monic polynomial with coefficients in $\mathcal{O}_v$. If $\alpha \in L$ is a root of $f(X)$, then $\alpha \in \mathcal{O}_w$.*

Proof. It is well known that $\beta = \alpha^{p^m}$ is separable over F for some $m \geqslant 0$. Let M be a finite Galois extension of F with $\beta \in M$. Then, in fact, $\beta \in \mathcal{O}$ and the monic irreducible polynomial $g(X)$ of β over F can be written as

$$g(X) = \prod_{i=1}^{r}(X - \sigma_i\beta), \quad \sigma_i \in \mathrm{Gal}(M/F),\ \sigma_1 = 1.$$

By the previous corollary we get $\sigma_i\beta \in \mathcal{O}$. Hence we obtain $g(X) \in \mathcal{O}_v[X]$ and $f(X) = g\left(X^{p^m}\right) \in \mathcal{O}_v[X]$. If $\alpha \in L$ is a root of the polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}_v[X]$ and $\alpha \notin \mathcal{O}_w$, then $1 = -a_{n-1}\alpha^{-1} - \cdots - a_0\alpha^{-n} \in \mathcal{M}_w$, contradiction. Thus, $\alpha \in \mathcal{O}_w$. □

(2.6). Types of Ramified Extensions. From now on F is a complete discrete valuation field.

Let L/F be an algebraic extension. If v_L is the unique discrete valuation on L which extends the valuation $v = v_F$ on F, then we shall write $e(L|F), f(L|F)$ instead of $e(v_L|v_F)$, $f(v_F|v_F)$. We shall write $\mathcal{O}$ or $\mathcal{O}_F, \mathcal{M}$ or $\mathcal{M}_F, U$ or U_F, π or $\pi_F, \overline{F}$ for the ring of integers

$\mathcal{O}_v$, the maximal ideal $\mathcal{M}_v$, the group of units U_v, a prime element π_v with respect to v, and the residue field $\overline{F}_v$, respectively.

A finite extension L of a complete discrete valuation field F is called *unramified* if $\overline{L}/\overline{F}$ is a separable extension of the same degree as L/F. A finite extension L/F is called *totally ramified* if $f(L|F) = 1$. A finite extension L/F is called *tamely ramified* if $\overline{L}/\overline{F}$ is a separable extension and $p \nmid e(L|F)$ where $p = \mathrm{char}(\overline{F}) > 0$. A finite extension L/F is called *totally ramified* if $\overline{L} = \overline{F}$. A finite extension L/F is called *wildly totally ramified* if $\overline{L} = \overline{F}$ and the degree of L/F is a power of $p = \mathrm{char}(F)$.

(2.7). Unramified Extensions. If L/F is unramified then we deduce From Lemma (2.4) that $e(L|F) = 1$, $f(L|F) = |L : F|$.

PROPOSITION.

(1) *Let L/F be an unramified extension, and $\overline{L} = \overline{F}(\theta)$ for some $\theta \in \overline{L}$. Let $\alpha \in \mathcal{O}_L$ be such that $\overline{\alpha} = \theta$. Then $L = F(\alpha)$, and L is separable over F, $\mathcal{O}_L = \mathcal{O}_F[\alpha]$; θ is a simple root of the polynomial $\overline{f}(X)$ irreducible over $\overline{F}$, where $f(X)$ is the monic irreducible polynomial of α over F.*

(2) *Let $f(X)$ be a monic polynomial over $\mathcal{O}_F$, such that its residue is a monic separable polynomial over $\overline{F}$. Let α be a root of $f(X)$ in F^{alg}, and let $L = F(\alpha)$. Then the extension L/F is unramified and $\overline{L} = \overline{F}(\theta)$ for $\theta = \overline{\alpha}$.*

Proof. (1) By the preceding lemma $f(X) \in \mathcal{O}_F[X]$. We have $f(\alpha) = 0$ and $\overline{f}(\overline{\alpha}) = 0$, $\deg f(X) = \deg \overline{f}(X)$. Furthermore,

$$|L : F| \geqslant |F(\alpha) : F| = \deg f(X) = \deg \overline{f}(X) \geqslant |\overline{F}(\theta) : \overline{F}| = |L : F|.$$

It follows that $L = F(\alpha)$ and θ is a simple root of the irreducible polynomial $\overline{f}(X)$. Therefore, $\overline{f}'(\theta) \neq 0$ and $f'(\alpha) \neq 0$, i.e., α is separable over F. Thus, $\mathcal{O}_L = \mathcal{O}_F[\alpha]$.

(2) Since the residue of f is separable, it is separable too. Let $f(X) = \prod_{i=1}^{n} f_i(X)$ be the decomposition of $f(X)$ into irreducible monic factors in $F[X]$. Then every root of $f(X)$ is in the ring of integers of any finite Galois extension of F which contains all of them; and therefore $f_i(X) \in \mathcal{O}_F[X]$. Suppose that α is a root of $f_1(X)$. Then $g_1(X) = \overline{f}_1(X)$ is a monic separable polynomial over $\overline{F}$. The Henselian property of F implies that $g_1(X)$ is irreducible over $\overline{F}$. We get $\alpha \in \mathcal{O}_L$. Since $\theta = \overline{\alpha} \in \overline{L}$, we obtain $\overline{L} \supset \overline{F}(\theta)$ and

$$\deg f_1(X) = |L : F| \geqslant |\overline{L} : \overline{F}| \geqslant |\overline{F}(\theta) : \overline{F}| = \deg g_1(X) = \deg f_1(X).$$

Thus, $\overline{L} = \overline{F}(\theta)$, and L/F is unramified. □

COROLLARY.

(1) *If $L/F, M/L$ are unramified, then M/F is unramified.*

(2) *If L/F is unramified, M is an algebraic extension of F and M is the discrete valuation field with respect to the extension of the valuation of F, then ML/M is unramified.*

(3) *If $L_1/F, L_2/F$ are unramified, then L_1L_2/F is unramified.*

Proof. (1) follows from the multiplicativity of the ramification index. To verify (2) let $L = F(\alpha)$ with $\alpha \in \mathcal{O}_L$, $f(X) \in \mathcal{O}_F[X]$ as in the first part of the proposition. Then $\alpha \notin \mathcal{M}_L$ because $\overline{L} = \overline{F}(\overline{\alpha})$. Observing that $ML = M(\alpha)$, we denote the irreducible monic polynomial

of α over M by $f_1(X)$. By the Henselian property of M we obtain that $\overline{f}_1(X)$ is a power of an irreducible polynomial over $\overline{M}$. However, $\overline{f}_1(X)$ divides $\overline{f}(X)$, hence $\overline{f}_1(X)$ is irreducible separable over $\overline{M}$. Applying the second part of the proposition, we conclude that ML/M is unramified.

(3) follows from (1) and (2). □

An algebraic extension L of F is called *unramified* if $L/F, \overline{L}/\overline{F}$ are separable extensions and $e(w|v) = 1$, where v is the discrete valuation on F, and w is the unique extension of v on L.

The third assertion of the Corollary shows that the compositum of all finite unramified extensions of F in a fixed algebraic closure F^{alg} of F is unramified. This extension is not a complete field in general, but a Henselian discrete valuation field. It is called the *maximal unramified extension* F^{ur} of F. Its maximality implies $\sigma F^{\text{ur}} = F^{\text{ur}}$ for any automorphism of the separable closure F^{sep} over F. Thus, F^{ur}/F is Galois.

PROPOSITION.

(1) *Let L/F be an unramified extension and let $\overline{L}/\overline{F}$ be a Galois extension. Then L/F is Galois.*

(2) *Let L/F be an unramified Galois extension. Then $\overline{L}/\overline{F}$ is Galois. For an automorphism $\sigma \in \text{Gal}(L/F)$ let $\overline{\sigma}$ be the automorphism in $\text{Gal}(\overline{L}/\overline{F})$ satisfying the relation $\overline{\sigma}\overline{\alpha} = \overline{\sigma\alpha}$ for every $\alpha \in \mathcal{O}_L$. Then the map $\sigma \to \overline{\sigma}$ induces an isomorphism of $\text{Gal}(L/F)$ onto $\text{Gal}(\overline{L}/\overline{F})$.*

Proof. (1) It suffices to verify the first assertion for a finite unramified extension L/F. Let $\overline{L} = \overline{F}(\theta)$ and let $g(X)$ be the irreducible monic polynomial of θ over $\overline{F}$. Then

$$g(X) = \prod_{i=1}^{n}(X - \theta_i),$$

with $\theta_i \in \overline{L}, \theta_1 = \theta$. Let $f(X)$ be a monic polynomial over $\mathcal{O}_F$ of the same degree as $g(X)$ and $\overline{f}(X) = g(X)$. The Henselian property implies

$$f(X) = \prod_{i=1}^{n}(X - \alpha_i),$$

with $\alpha_i \in \mathcal{O}_L, \overline{\alpha}_i = \theta_i$. The first proposition above shows that $L = F(\alpha_1)$, and we deduce that L/F is Galois.

(2) Note that the automorphism $\overline{\sigma}$ is well defined. Indeed, if $\beta \in \mathcal{O}_L$ with $\overline{\beta} = \overline{\alpha}$, then $\sigma(\alpha - \beta) \in \mathcal{M}_L$ and $\overline{\sigma\alpha} = \overline{\sigma\beta}$. It suffices to verify the second assertion for a finite unramified Galois extension L/F. Let $\alpha, \theta, f(X)$ be as in the first part of the first proposition. Since all roots of $f(X)$ belong to L, we obtain that all roots of $\overline{f}(X)$ belong to $\overline{L}$ and $\overline{L}/\overline{F}$ is Galois. The homomorphism $\text{Gal}(L/F) \to \text{Gal}(\overline{L}/\overline{F})$ defined by $\sigma \to \overline{\sigma}$ is surjective because the condition $\overline{\sigma}\theta = \theta_i$ implies $\sigma\alpha = \alpha_i$ for the root α_i of $f(X)$ with $\overline{\alpha}_i = \theta_i$. Since $\text{Gal}(L/F)$, $\text{Gal}(\overline{L}/\overline{F})$ are of the same order, we conclude that $\text{Gal}(L/F)$ is isomorphic to $\text{Gal}(\overline{L}/\overline{F})$. □

COROLLARY. *The residue field of F^{ur} coincides with the separable closure $\overline{F}^{\text{sep}}$ of $\overline{F}$ and* $\text{Gal}(F^{\text{ur}}/F) \simeq \text{Gal}(\overline{F}^{\text{sep}}/\overline{F})$.

Proof. Let $\theta \in \overline{F}^{\text{sep}}$, let $g(X)$ be the monic irreducible polynomial of θ over $\overline{F}$, and $f(X)$ as in the second part of the first proposition. Let $\{\alpha_i\}$ be all the roots of $f(X)$ and $L = F(\{\alpha_i\})$. Then $L \subset F^{\text{ur}}$ and $\theta = \overline{\alpha}_i \in \overline{F^{\text{ur}}}$ for a suitable i. Hence, $\overline{F^{\text{ur}}} = \overline{F}^{\text{sep}}$. □

(2.8). Maximal Unramified Field. Let L be an algebraic extension of F, and let L be a discrete valuation field with perfect residue field. We will assume that $F^{\text{alg}} = L^{\text{alg}}$.

PROPOSITION. *Let L be an algebraic extension of F and let L be a discrete valuation field. Then $L^{\text{ur}} = LF^{\text{ur}}$, $L_0 = L \cap F^{\text{ur}}$ is the maximal unramified subextension of F which is contained in L, and L/L_0 is totally ramified.*

Proof. We have $L^{\text{ur}} \supset LF^{\text{ur}}$. Since the residue field of LF^{ur} coincides with the residue field of F^{ur}, we deduce $L^{\text{ur}} = LF^{\text{ur}}$. An unramified subextension of F in L is contained in L_0, and L_0/F is unramified. □

PROPOSITION. *Let L be a finite Galois extension of F and let L_0/F be the maximal unramified subextension in L/F. Then L_0/F and $\overline{L}_0/\overline{F}$ are Galois, and the map $\sigma \to \overline{\sigma}$ defined in the second proposition of* (2.7) *induces the surjective homomorphism*

$$\text{Gal}(L/F) \to \text{Gal}(L_0/F) \to \text{Gal}(\overline{L}_0/\overline{F}) = \text{Gal}(\overline{L}/\overline{F}).$$

The extension L^{ur}/F is Galois and $\text{Gal}(L^{\text{ur}}/L_0) \simeq \text{Gal}(L^{\text{ur}}/L) \times \text{Gal}(L^{\text{ur}}/F^{\text{ur}})$, $\text{Gal}(L^{\text{ur}}/F^{\text{ur}}) \simeq \text{Gal}(L/L_0)$, $\text{Gal}(L^{\text{ur}}/L) \simeq \text{Gal}(F^{\text{ur}}/L_0)$.

Proof. Let $\sigma \in \text{Gal}(L/F)$. Then σL_0 is unramified over F, hence $L_0 = \sigma L_0$ and L_0/F is Galois. The surjectivity of the homomorphism $\text{Gal}(L/F) \to \text{Gal}(\overline{L}_0/\overline{F})$ follows from the second proposition of (2.7). Since L/F and F^{ur}/F are Galois extensions, we obtain that LF^{ur}/F is a Galois extension. Then $L^{\text{ur}} = LF^{\text{ur}}$ by the previous proposition. The remaining assertions are easily deduced by Galois theory. □

(2.9). Tamely Ramified Extensions.

PROPOSITION.

(1) *Let L be a finite tamely ramified extension of F, and let L_0/F be the maximal unramified subextension in L/F. Then $L = L_0(\pi)$ and $\mathcal{O}_L = \mathcal{O}_{L_0}[\pi]$ with a prime element π in L satisfying the equation $X^e - \pi_0 = 0$ for some prime element π_0 in L_0, where $e = e(L|F)$.*

(2) *Let L_0/F be a finite unramified extension, $L = L_0(\alpha)$ with $\alpha^e = \beta \in L_0$. Let $p \nmid e$ if $p = \text{char}(\overline{F}) > 0$. Then L/F is separable tamely ramified.*

Proof. (1) (2.8) shows that L/L_0 is totally ramified. Let π_1 be a prime element in L_0, then $\pi_1 = \pi_L^e \varepsilon$ for a prime element π_L in L and $\varepsilon \in U_L$. Since $\overline{L} = \overline{L}_0$, there exists $\eta \in \mathcal{O}_{L_0}$ such that $\overline{\eta} = \overline{\varepsilon}$. Hence $\pi_1 \eta^{-1} = \pi_L^e \rho$ for the principal unit $\rho = \varepsilon \eta^{-1} \in \mathcal{O}_L$. For the polynomial $f(X) = X^e - \rho$ we have $f(1) \in \mathcal{M}_L$, $f'(1) = e$. Now Corollary 2 of (2.1) shows the existence of an element $\nu \in \mathcal{O}_L$ with $\nu^e = \rho$, $\overline{\nu} = 1$. Therefore, $\pi = \pi_1 \eta^{-1}$, $\pi_0 = \pi_L \nu$ are the elements desired for the first part of the Proposition.

(2) Let $\beta = \pi_1^a \varepsilon$ for a prime element π_1 in L_0 and a unit $\varepsilon \in U_{L_0}$. The polynomial $g(X) = X^e - \overline{\varepsilon}$ is separable in $\overline{L}_0[X]$ and we can apply the Henselian property to $f(X) = X^e - \varepsilon$

and a root $\eta \in F^{\text{sep}}$ of $f(X)$. We deduce that $L_0(\eta)/L_0$ is unramified and hence it suffices to verify that M/M_0 for $M = L(\eta), M_0 = L_0(\eta)$, is tamely ramified. We get $M = M_0(\alpha_1)$ with $\alpha_1 = \alpha\eta^{-1}$, $\alpha_1^e = \pi_1^a$. Put $d = \text{g.c.d.}(e, a)$. Then $M \subset M_0(\alpha_2, \zeta)$ with $\alpha_2^{e/d} = \pi_1^{a/d}$ and a primitive eth root ζ of unity. Since the extension $M_0(\zeta)/M_0$ is unramified (this can be verified by the same arguments as above), π_1 is a prime element in $M_0(\zeta)$. Let v be the discrete valuation on $M_0(\alpha_2, \zeta)$. Then $(a/d)v(\pi_1) \in (e/d)\mathbb{Z}$ and $v(\pi_1) \in (e/d)\mathbb{Z}$, because a/d and e/d are relatively prime. This shows that $e\big(M_0(\alpha_2, \zeta) \mid M_0(\zeta)\big) \geqslant e/d$. However, $|M_0(\zeta, \alpha_2) : M_0(\zeta)| \leqslant e/d$, and we conclude that $M_0(\zeta, \alpha_2)/M_0(\zeta)$ is tamely and totally ramified. Thus, $M_0(\zeta, \alpha_2)/M_0$ and M/M_0 are tamely ramified extensions. □

COROLLARY.

(1) *If $L/F, M/L$ are tamely ramified, then M/F is separable tamely ramified.*
(2) *If L/F is tamely ramified, M/F is an algebraic extension, and M is discrete, then ML/M is tamely ramified.*
(3) *If $L_1/F, L_2/F$ are tamely ramified, then L_1L_2/F is tamely ramified.*

Proof. It is carried out similarly to (2.8). To verify (2) one can find the maximal unramified subextension L_0/F in L/F. Then it remains to show that ML/ML_0 is tamely ramified. Put $L = L_0(\pi)$ with $\pi^e = \pi_0$. Then we get $ML = ML_0(\pi)$, and the second part of the proposition yields the required assertion. □

(2.10). Totally Ramified Extensions. A polynomial

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \quad \text{over } \mathcal{O}$$

is called an *Eisenstein polynomial* if

$$a_0, \ldots, a_{n-1} \in \mathcal{M}, \quad a_0 \notin \mathcal{M}^2.$$

PROPOSITION.

(1) *The Eisenstein polynomial $f(X)$ is irreducible over F. If α is a root of $f(X)$, then $F(\alpha)/F$ is a totally ramified extension of degree n, α is a prime element in $F(\alpha)$, $\mathcal{O}_{F(\alpha)} = \mathcal{O}_F[\alpha]$.*
(2) *Let L/F be a separable totally ramified extension of degree n, and let π be a prime element in L. Then π is a root of an Eisenstein polynomial over F of degree n.*

Proof. (1) Let α be a root of $f(X)$, $L = F(\alpha)$, $e = e(L|F)$. Then

$$nv_L(\alpha) = v_L\Big(\sum_{i=0}^{n-1} a_i\alpha^i\Big) \geqslant \min_{0\leqslant i\leqslant n-1} \left(ev_F(a_i) + iv_L(\alpha)\right),$$

where v_F and v_L are the discrete valuations on F and L. It follows that $v_L(\alpha) > 0$. Since $ev_F(a_0) < ev_F(a_i) + iv_L(\alpha)$ for $i > 0$, one has $nv_L(\alpha) = ev_F(a_0) = e$. Then $v_L(\alpha) = 1, n = e, f = 1$, and $\mathcal{O}_L = \mathcal{O}_F[\alpha]$.
(2) Let π be a prime element in L. Then $L = F(\pi)$. Let

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

be the irreducible polynomial of π over F. Then $n = e$ and $nv_L(\pi) = \min_{0\leqslant i\leqslant n-1}\big(nv_F(a_i) + i\big)$, hence $v_F(a_i) > 0$, and $n = nv_F(a_0)$, $v_F(a_0) = 1$. □

(2.11). Ramification Groups. Let L be a finite Galois extension of F, $G = \mathrm{Gal}(L/F)$. Put

$$G_i = \left\{\sigma \in G : \sigma\alpha - \alpha \in \mathfrak{M}_L^{i+1} \text{ for all } \alpha \in \mathfrak{O}_L\right\}, \qquad i \geqslant -1.$$

Then $G_{-1} = G$ by Lemma (2.11) and G_{i+1} is a subset of G_i.

Let v_L be the discrete valuation of L. For a real number x define

$$G_x = \left\{\sigma \in G : v_L(\sigma\alpha - \alpha) \geqslant x + 1 \text{ for all } \alpha \in \mathfrak{O}_L\right\}.$$

Certainly each of G_x is equal to G_i with the least integer $i \geqslant x$.

LEMMA. *G_i are normal subgroups of G.*

Proof. Let $\sigma \in G_i, \alpha \in \mathfrak{O}_L$. Then $\sigma\alpha - \alpha \in \mathfrak{M}_L^{i+1}$. Hence $\alpha - \sigma^{-1}(\alpha) \in \sigma^{-1}(\mathfrak{M}_L^{i+1}) = \mathfrak{M}_L^{i+1}$ by Lemma (2.11), i.e., $\sigma^{-1} \in G_i$. Let $\sigma, \tau \in G_i$. Then

$$\sigma\tau(\alpha) - \alpha = \sigma(\tau(\alpha) - \alpha) + \sigma(\alpha) - \alpha \in \mathfrak{M}_L^{i+1},$$

i.e., $\sigma\tau \in G_i$. Furthermore, let $\sigma \in G_i, \tau \in G$. Then $\tau(\alpha) \in \mathfrak{O}_L$ for $\alpha \in \mathfrak{O}_L$ and $\sigma(\tau\alpha) - \tau\alpha \in \mathfrak{M}_L^{i+1}$, $\tau^{-1}\sigma\tau(\alpha) - \alpha \in \mathfrak{M}_L^{i+1}$, $\tau^{-1}\sigma\tau \in G_i$. □

The groups G_x are called (*lower*) *ramification groups* of $G = \mathrm{Gal}(L/F)$.

PROPOSITION. *Let L be a finite Galois extension of F, and let $\overline{L}$ be a separable extension of $\overline{F}$. Then $G_0 = \mathrm{Gal}(L/L_0)$ and the i th ramification groups of G_0 and G coincide for $i \geqslant 0$. Moreover,*

$$G_i = \left\{\sigma \in G_0 : \sigma\pi - \pi \in \mathfrak{M}_L^{i+1}\right\}$$

for a prime element π in L, and $G_i = \{1\}$ for sufficiently large i.

Proof. Note that $\sigma \in G_0$ if and only if $\overline{\sigma} \in \mathrm{Gal}(\overline{L}/\overline{F})$ is trivial. Then G_0 coincides with the kernel of the homomorphism $\mathrm{Gal}(L/F) \to \mathrm{Gal}(\overline{L}/\overline{F})$. The first proposition of (2.11) and the second proposition of (2.7) imply that this kernel is equal to $\mathrm{Gal}(L/L_0)$. Since G_i is a subgroup of G_0 for $i \geqslant 0$, we deduce the assertion about the i th ramification group of G_0. We get $\mathfrak{O}_L = \mathfrak{O}_{L_0}[\pi]$. Let $\alpha = \sum_{i=0}^{n} a_i\pi^i$ be an expansion of $\alpha \in \mathfrak{O}_L$ with coefficients in $\mathfrak{O}_{L_0}$. As $\sigma a_i = a_i$ for $\sigma \in G_0$ it follows that

$$\sigma\alpha - \alpha = \sum_{i=0}^{n} a_i\left(\sigma(\pi^i) - \pi^i\right).$$

Now we deduce the description of G_i, since $\sigma(\pi^i) - \pi^i \in G_i$. If $i \geqslant \max\{v_L(\sigma\pi - \pi) : \sigma \in G\}$, then $G_i = \{1\}$. □

The group G_0 is called the *inertia group* of G, and the field L_0 is called the *inertia subfield* of L/F.

PROPOSITION. *Let L be a finite Galois extension of F, $\overline{L}$ a separable extension of $\overline{F}$, and π a prime element in L. Introduce the maps*

$$\psi_0 : G_0 \longrightarrow \overline{L}^{\times}, \quad \psi_i : G_i \longrightarrow \overline{L} \quad (i > 0)$$

by the formulas $\psi_i(\sigma) = \lambda_i(\sigma\pi/\pi)$. Then ψ_i is a homomorphism with the kernel G_{i+1} for $i \geqslant 0$.

Proof. The proof follows from the congruence

$$\frac{\sigma\tau(\pi)}{\pi} = \sigma\left(\frac{\tau\pi}{\pi}\right)\cdot\frac{\sigma\pi}{\pi} \equiv \frac{\tau\pi}{\pi}\cdot\frac{\sigma\pi}{\pi} \mod U_{i+1}$$

for $\sigma, \tau \in G_i$. The kernel of ψ_i consists of those automorphisms $\sigma \in G_i$, for which $\sigma\pi/\pi \in 1 + \mathfrak{M}_L^{i+1}$, i.e., $\sigma\pi - \pi \in \mathfrak{M}_L^{i+2}$. □

COROLLARY 1. *Let L be a finite Galois extension of F, and $\overline{L}$ a separable extension of $\overline{F}$. If* $\mathrm{char}(\overline{F}) = 0$, *then $G_1 = \{1\}$ and G_0 is cyclic. If* $\mathrm{char}(\overline{F}) = p > 0$, *then the group G_0/G_1 is cyclic of order relatively prime to p, G_i/G_{i+1} are abelian p-groups, and G_1 is the maximal p-subgroup of G_0.*

Proof. The previous proposition permits us to transform the assertions of this corollary into the following: a finite subgroup in $\overline{L}^\times$ is cyclic (of order relatively prime to $\mathrm{char}(\overline{L})$ when $\mathrm{char}(\overline{L}) \neq 0$); there are no nontrivial finite subgroups in the additive group of $\overline{L}$ if $\mathrm{char}(\overline{L}) = 0$; if $\mathrm{char}(\overline{L}) = p > 0$ then a finite subgroup in $\overline{L}$ is a p-group. □

COROLLARY 2. *Let L be a finite Galois extension of F and $\overline{L}$ a separable extension of $\overline{F}$. Then the group G_1 coincides with* $\mathrm{Gal}(L/L_1)$, *where L_1/F is the maximal tamely ramified subextension in L/F.*

Proof. The extension L_1/L_0 is totally ramified by the first proposition of (2.11) and is the maximal subextension in L/L_0 of degree relatively prime with $\mathrm{char}(\overline{F})$. Now Corollary 1 implies $G_1 = \mathrm{Gal}(L/L_1)$. □

COROLLARY 3. *Let L be a finite Galois extension of F and $\overline{L}$ a separable extension of $\overline{F}$. Then G_0 is a solvable group. If, in addition, $\overline{L}/\overline{F}$ is a solvable extension, then L/F is solvable.*

Proof. It follows from Corollary 1. □

(2.12). The Norm Map for Cyclic Extensions. Let F be a local field and L its Galois extension of prime degree n. Then there are four possible cases:

L/F is unramified;
L/F is tamely and totally ramified;
L/F is totally ramified of degree $p = \mathrm{char}(\overline{F}) > 0$;

LEMMA. *Let L/F be a separable extension of prime degree n, $\gamma \in \mathfrak{M}_L$. Then*

$$N_{L/F}(1+\gamma) = 1 + N_{L/F}(\gamma) + \mathrm{Tr}_{L/F}(\gamma) + \mathrm{Tr}_{L/F}(\delta)$$

with some $\delta \in \mathfrak{O}_L$ such that $v_L(\delta) \geqslant 2v_L(\gamma)$ ($N_{L/F}$ and $\mathrm{Tr}_{L/F}$ are the norm and the trace maps, respectively).

Proof. Recall that for distinct embeddings σ_i of L over F into the algebraic closure of F, $1 \leqslant i \leqslant n$, one has

$$N_{L/F}\alpha = \prod_{i=1}^{n}\sigma_i(\alpha), \quad \mathrm{Tr}_{L/F}\,\alpha = \sum_{i=1}^{n}\sigma_i(\alpha), \qquad \alpha \in L.$$

Hence

$$N_{L/F}(1+\gamma) = \prod_{i=1}^{n}(1+\sigma_i(\gamma)) = 1 + \sum_{i=1}^{n}\sigma_i(\gamma) + \left(\sum_{i=1}^{n}\sigma_i\right)\left(\sum_{1\leqslant j\leqslant n}\gamma\sigma_j(\gamma)+\cdots\right) + \prod_{i=1}^{n}\sigma_i(\gamma).$$

For $\delta = \sum_{1\leqslant j\leqslant n}\gamma\sigma_j(\gamma)+\cdots$ we get $v_L(\delta) \geqslant 2v_L(\gamma)$. □

Our nearest purpose is to describe the action of the norm map $N_{L/F}$ with respect to the filtration on $L^\times$ and $F^\times$.

PROPOSITION. *Let L/F be an unramified extension of degree n. Then a prime element π_F in F is a prime element in L. Let $U_{i,L} = 1+\pi_F^i\mathcal{O}_L$, $U_{i,F} = 1+\pi_F^i\mathcal{O}_F$. Then the following diagrams are commutative:*

$$\begin{array}{ccc} L^\times & \xrightarrow{v_L} & \mathbb{Z} \\ {\scriptstyle N_{L/F}}\downarrow & & \downarrow{\scriptstyle \times n} \\ F^\times & \xrightarrow{v_F} & \mathbb{Z} \end{array} \qquad \begin{array}{ccc} U_L & \xrightarrow{\lambda_{0,L}} & \overline{L}^\times \\ {\scriptstyle N_{L/F}}\downarrow & & \downarrow{\scriptstyle N_{\overline{L}/\overline{F}}} \\ U_F & \xrightarrow{\lambda_{0,F}} & \overline{F}^\times \end{array} \qquad \begin{array}{ccc} U_{i,L} & \xrightarrow{\lambda_{i,L}} & \overline{L} \\ {\scriptstyle N_{L/F}}\downarrow & & \downarrow{\scriptstyle \mathrm{Tr}_{\overline{L}/\overline{F}}} \\ U_{i,F} & \xrightarrow{\lambda_{i,F}} & \overline{F} \end{array}$$

Proof. The commutativity of the first two diagrams is easy. The preceding Lemma shows that

$$N_{L/F}(1+\theta\pi_F^i) = 1 + (\mathrm{Tr}_{L/F}\,\theta)\pi_F^i + (N_{L/F}\theta)\pi_F^{pi} + \mathrm{Tr}_{L/F}(\delta)$$

with $v_L(\delta) \geqslant 2i$ and, consequently, $v_F\,\mathrm{Tr}_{L/F}(\delta) \geqslant 2i$. Thus, we get

$$N_{L/F}(1+\theta\pi_F^i) \equiv 1 + (\mathrm{Tr}_{L/F}\,\theta)\pi_F^i \mod \pi_F^{i+1}$$

and the commutativity of the third diagram. □

COROLLARY. *In the case under consideration $N_{L/F}U_{1,L} = U_{1,F}$.*

PROPOSITION. *Let L/F be a totally and tamely ramified cyclic extension of degree n. Then for some prime element π_L in L, the element $\pi_F = \pi_L^n$ is prime in F and $\overline{F} = \overline{L}$. Let $U_{i,L} = 1+\pi_L^i\mathcal{O}_L$, $U_{i,F} = 1+\pi_F^i\mathcal{O}_F$. Then the following diagrams*

$$\begin{array}{ccc} L^\times & \xrightarrow{v_L} & \mathbb{Z} \\ {\scriptstyle N_{L/F}}\downarrow & & \downarrow{\scriptstyle \mathrm{id}} \\ F^\times & \xrightarrow{v_F} & \mathbb{Z} \end{array} \qquad \begin{array}{ccc} U_L & \xrightarrow{\lambda_{0,L}} & \overline{L}^\times \\ {\scriptstyle N_{L/F}}\downarrow & & \downarrow{\scriptstyle \uparrow n} \\ U_F & \xrightarrow{\lambda_{0,F}} & \overline{F}^\times \end{array} \qquad \begin{array}{ccc} U_{ni,L} & \xrightarrow{\lambda_{ni,L}} & \overline{L} = \overline{F} \\ {\scriptstyle N_{L/F}}\downarrow & & \downarrow{\scriptstyle \times\overline{n}} \\ U_{i,F} & \xrightarrow{\lambda_{i,F}} & \overline{F} \end{array}$$

are commutative, where id *is the identity map, $\uparrow n$ takes an element to its nth power, $\times\overline{n}$ is the multiplication by $\overline{n} \in \overline{F}$, $i \geqslant 1$. Moreover, $N_{L/F}U_{i,L} = N_{L/F}U_{i+1,L}$ if $n \nmid i$.*

Proof. Since $\pi_L^n = \pi_F$ and L/F is Galois, then $\mathrm{Gal}(L/F)$ is cyclic of order n and $\sigma(\pi_L) = \zeta\pi_L$ for a generator σ of $\mathrm{Gal}(L/F)$, where ζ is a primitive nth root of unity, $\zeta \in F$.

It is easy to see that the first diagram is commutative.

Corollary in (2.5) shows that $\overline{\sigma(\alpha)} = \overline{\alpha}$ for $\sigma \in \mathrm{Gal}(L/F)$, $\alpha \in \mathcal{O}_L$, and we get the commutativity of the second diagram.

If $j = ni$, then $1 + \theta\pi_L^j \in F$ for $\theta \in \mathcal{O}_F$, and

$$N_{L/F}(1 + \theta\pi_L^j) = (1 + \theta\pi_F^i)^n \equiv 1 + n\theta\pi_F^i \mod \pi_F^{i+1}.$$

We deduce $U_{i,F} = U_{i,F}^n = N_{L/F}U_{ni,L}$

Finally, $X^n - 1 = \prod_{j=0}^{n-1}(X - \zeta^j)$, therefore for $n \nmid i$ and for $\theta \in \mathcal{O}_F$ one has

$$N_{L/F}(1 + \theta\pi_L^i) = \prod_{j=0}^{n-1}(1 + \zeta^j\theta\pi_L^i) = 1 - (-\theta)^n\pi_F^i.$$

Thus $N_{L/F}U_{i,L} = N_{L/F}U_{i+1,L}$. □

COROLLARY. *In the case under consideration $N_{L/F}U_{1,L} = U_{1,F}$. If $\overline{F}$ is algebraically closed then $N_{L/F}L^\times = F^\times$.*

Now we treat *the most complicated case* where L/F is a totally ramified Galois extension of degree $p = \mathrm{char}(\overline{F}) > 0$. In this case $\mathcal{O}_L = \mathcal{O}_F[\pi_L]$, $L = F(\pi_L)$ for a prime element π_L in L, and $\overline{L} = \overline{F}$. Let σ be a generator of $\mathrm{Gal}(L/F)$, then $\sigma(\pi_L)/\pi_L \in U_L$. One can write $\sigma(\pi_L)/\pi_L = \theta\varepsilon$ with $\theta \in U_F, \varepsilon \in 1 + \mathfrak{M}_L$. Then

$$\sigma^2(\pi_L)/\pi_L = \sigma(\theta\varepsilon)\cdot\theta\varepsilon = \theta^2\varepsilon\cdot\sigma(\varepsilon),$$

and

$$1 = \sigma^p(\pi_L)/\pi_L = \theta^p\varepsilon\cdot\sigma(\varepsilon)\cdot\ \cdots\ \cdot\sigma^{p-1}(\varepsilon).$$

This shows that $\theta^p \in 1 + \mathfrak{M}_L$ and $\theta \in 1 + \mathfrak{M}_F$, because raising to the pth power is an injective homomorphism of $\overline{F}$. Thus, we obtain $\sigma(\pi_L)/\pi_L \in 1 + \mathfrak{M}_L$. Put

$$\frac{\sigma(\pi_L)}{\pi_L} = 1 + \eta\pi_L^s \qquad \text{with} \quad \eta \in U_L,\ s = s(L|F) \geqslant 1. \tag{$*$}$$

Note that s does not depend on the choice of the prime element π_L and of the generator σ of $G = \mathrm{Gal}(L/F)$. Indeed, we have

$$\frac{\sigma^i(\pi_L)}{\pi_L} \equiv 1 + i\eta\pi_L^s \mod \pi_L^{s+1} \qquad \text{and} \qquad \frac{\sigma(\rho)}{\rho} \equiv 1 \mod \pi_L^{s+1}$$

for an element $\rho \in U_L$. We also deduce that

$$\frac{\sigma(\alpha)}{\alpha} \in U_{s,L}$$

for every element $\alpha \in L^\times$. This means that $G = G_s$, $G_{s+1} = \{1\}$.

LEMMA. *Let $f(X) = X^p + a_{p-1}X^{p-1} + \cdots + a_0$ be the irreducible polynomial of π_L over F. Then*

$$\mathrm{Tr}_{L/F}\left(\frac{\pi_L^j}{f'(\pi_L)}\right) = \begin{cases} 0 & \text{if} \quad 0 \leqslant j \leqslant p-2, \\ 1 & \text{if} \quad j = p-1. \end{cases}$$

Proof. Since $\sigma^i(\pi_L)$ for $0 \leqslant i \leqslant p-1$ are all the roots of the polynomial $f(X)$, we get

$$\frac{1}{f(X)} = \sum_{i=0}^{p-1} \frac{1}{f'\big(\sigma^i(\pi_L)\big)\,\big(X - \sigma^i(\pi_L)\big)}.$$

Putting $Y = X^{-1}$ and performing the calculations in the field $F((Y))$, we consequently deduce

$$f(X) = Y^{-p}(1 + a_{p-1}Y + \cdots + a_0 Y^p),$$
$$\frac{1}{f(X)} = \frac{Y^p}{1 + a_{p-1}Y + \cdots + a_0 Y^p} \equiv Y^p \mod Y^{p+1},$$
$$\frac{1}{X - \sigma^i(\pi_L)} = \frac{Y}{1 - \sigma^i(\pi_L)Y} = \sum_{j \geqslant 0} \sigma^i(\pi_L^j) Y^{j+1}$$

(because $1/(1-Y) = \sum_{i \geqslant 0} Y^i$ in $F((Y))$). Hence

$$\sum_{j \geqslant 0} \sum_{i=0}^{p-1} \frac{\sigma^i(\pi_L^j) Y^{j+1}}{f'\big(\sigma^i(\pi_L)\big)} \equiv Y^p \mod Y^{p+1},$$

or

$$\mathrm{Tr}_{L/F}\left(\frac{\pi_L^j}{f'(\pi_L)}\right) = \sum_{i=0}^{p-1} \frac{\sigma^i(\pi_L^j)}{f'\big(\sigma^i(\pi_L)\big)} = \begin{cases} 0 & \text{if} \quad 0 \leqslant j \leqslant p-2, \\ 1 & \text{if} \quad j = p-1, \end{cases}$$

as desired. □

PROPOSITION. *Let* $[a]$ *denote the maximal integer* $\leqslant a$. *For an integer* $i \geqslant 0$ *put* $j(i) = s + 1 + \big[(i - 1 - s)/p\big]$. *Then*

$$\mathrm{Tr}_{L/F}(\pi_L^i \mathcal{O}_L) = \pi_F^{j(i)} \mathcal{O}_F.$$

Proof. One has $f'(\pi_L) = \prod_{i=1}^{p-1} \big(\pi_L - \sigma^i(\pi_L)\big)$ and $\sigma^i(\pi_L)/\pi_L \equiv 1 + i\eta\pi_L^s \mod \pi_L^{s+1}$. Then

$$f'(\pi_L) = (p-1)!(-\eta)^{p-1} \pi_L^{(p-1)(s+1)} \varepsilon$$

with some $\varepsilon \in 1 + \mathfrak{M}_L^{(p-1)(s+1)+1}$. Since $\overline{F} = \overline{L}$, for a prime element π_F in F one has the representation $\pi_F = \pi_L^p \varepsilon'$ with $\varepsilon' \in U_L$. The previous lemma implies

$$\mathrm{Tr}_{L/F}\left(\pi_L^{j+s+1} \varepsilon_{j+s+1}\right) = \begin{cases} 0 & \text{if} \quad 0 \leqslant j < p-1, \\ \pi_F^{s+1} & \text{if} \quad j = p-1 \end{cases}$$

for $\varepsilon_{j+s+1} = (\varepsilon')^{s+1} / \big((p-1)!(-\eta)^{p-1}\varepsilon\big)$. Since $\mathrm{Tr}_{L/F}(\pi_F^i \alpha) = \pi_F^i \mathrm{Tr}_{L/F}(\alpha)$ we can choose the units ε_{j+s+1}, for every integer j, such that $\mathrm{Tr}_{L/F}(\pi_L^{j+s+1} \varepsilon_{j+s+1}) = 0$ if $p \nmid (j+1)$ and $= \pi_F^{s+(j+1)/p}$ if $p | (j+1)$. Thus, since the $\mathcal{O}_F$-module $\pi_L^i \mathcal{O}_L$ is generated by $\pi_L^j \varepsilon_j$, $j \geqslant i$, we conclude that $\mathrm{Tr}_{L/F}(\pi_L^i \mathcal{O}_L) = \pi_F^{j(i)} \mathcal{O}_F$. □

PROPOSITION. *Let L/F be a totally ramified Galois extension of degree $p = \mathrm{char}(\overline{F}) > 0$. Let π_L be a prime element in L. Then $\pi_F = N_{L/F}\pi_L$ is a prime element in F. Let $U_{i,L} = 1 + \pi_L^i \mathcal{O}_L, U_{i,F} = 1 + \pi_F^i \mathcal{O}_F$. Then the following diagrams are commutative:*

$$\begin{array}{ccc} L^\times & \xrightarrow{v_L} & \mathbb{Z} \\ {\scriptstyle N_{L/F}}\downarrow & & \downarrow{\scriptstyle \mathrm{id}} \\ F^\times & \xrightarrow{v_F} & \mathbb{Z} \end{array} \qquad \begin{array}{ccc} U_L & \xrightarrow{\lambda_{0,L}} & \overline{L}^\times \\ {\scriptstyle N_{L/F}}\downarrow & & \downarrow{\scriptstyle \uparrow p} \\ U_F & \xrightarrow{\lambda_{0,F}} & \overline{F}^\times \end{array}$$

$$\begin{array}{ccc} U_{i,L} & \xrightarrow{\lambda_{i,L}} & \overline{L} = \overline{F} \\ {\scriptstyle N_{L/F}}\downarrow & & \downarrow{\scriptstyle \uparrow p} \\ U_{i,F} & \xrightarrow{\lambda_{i,F}} & \overline{F} \end{array} \qquad \begin{array}{ccc} U_{s,L} & \xrightarrow{\lambda_{s,L}} & \overline{L} = \overline{F} \\ {\scriptstyle N_{L/F}}\downarrow & & \downarrow{\scriptstyle \overline{\theta} \mapsto \overline{\theta}^p - \overline{\eta}^{p-1}\overline{\theta}} \\ U_{s,F} & \xrightarrow{\lambda_{s,F}} & \overline{F} \end{array} \qquad \begin{array}{ccc} U_{s+pi,L} & \xrightarrow{\lambda_{s+pi,L}} & \overline{L} = \overline{F} \\ {\scriptstyle N_{L/F}}\downarrow & & \downarrow{\scriptstyle \times(-\overline{\eta}^{p-1})} \\ U_{s+i,F} & \xrightarrow{\lambda_{s+i,F}} & \overline{F} \end{array}$$

where $1 \leqslant i < s$ in the third diagram and $i > 0$ is the last diagram.

Moreover, $N_{L/F}(U_{s+i,L}) = N_{L/F}(U_{s+i+1,L})$ for $i > 0, p \nmid i$.

Proof. The commutativity of the first and the second diagrams is easy.

To treat the remaining diagrams, put $\varepsilon = 1 + \theta\pi_L^i$ with $\theta \in U_L$. Then, by the first lemma, we get

$$N_{L/F}\varepsilon = 1 + N_{L/F}(\theta)\pi_F^i + \mathrm{Tr}_{L/F}(\theta\pi_L^i) + \mathrm{Tr}_{L/F}(\theta\delta)$$

with $v_L(\delta) \geqslant 2i$. The previous proposition implies that

$$v_F\left(\mathrm{Tr}_{L/F}(\pi_L^i)\right) \geqslant s + 1 + \left[\frac{i-1-s}{p}\right], \; v_F\left(\mathrm{Tr}_{L/F}(\delta)\right) \geqslant s + 1 + \left[\frac{2i-1-s}{p}\right]$$

and for $i < s$

$$v_F\left(\mathrm{Tr}_{L/F}(\pi_L^i)\right) \geqslant i + 1, \quad v_F\left(\mathrm{Tr}_{L/F}(\delta)\right) \geqslant i + 1.$$

Therefore, the third diagram is commutative.

Further, using $(*)$, write

$$1 = N_{L/F}\left(\frac{\sigma(\pi_L)}{\pi_L}\right) \equiv 1 + N_{L/F}(\eta)\pi_F^s + \mathrm{Tr}_{L/F}(\eta\pi_L^s) \mod \pi_F^{s+1}.$$

We deduce that

$$\mathrm{Tr}_{L/F}(\eta\pi_L^s) \equiv -N_{L/F}(\eta)\pi_F^s \mod \pi_F^{s+1}.$$

Since $N_{L/F}(\eta) \equiv \eta^p \mod \pi_L$ in view of $U_L \subset U_F U_{1,L}$, we conclude that

$$N_{L/F}(1 + \theta\eta\pi_L^s) - 1 - \eta^p\pi_F^s(\theta^p - \theta) \in \pi_L^{ps+1}\theta\mathcal{O}_L$$

for $\theta \in \mathcal{O}_F$. This implies the commutativity of the fourth (putting $\theta \in \mathcal{O}_F$) and the fifth (when $\theta \in \pi_F^i\mathcal{O}_F$) diagrams.

Finally, if $p \nmid i, \theta \in \mathcal{O}_F$, then

$$\frac{\sigma(1 + \theta\pi_L^i)}{1 + \theta\pi_L^i} \equiv 1 + i\theta\eta\pi_L^{i+s} \mod \pi_L^{i+s+1}.$$

This means that $N_{L/F}(1 + i\theta\eta\pi_L^{i+s}) \in N_{L/F}U_{s+i+1,L}$ and
$N_{L/F}(U_{s+i,L}) = N_{L/F}(U_{s+i+1,L})$. □

REMARK. Compare the behaviour of the norm map with the behaviour of raising to the pth power in Proposition (1.10).

COROLLARY. $U_{s+1,F} = N_{L/F}U_{s+1,L}$.
If $\overline{F}$ is algebraically closed then $N_{L/F}L^\times = F^\times$.

Proof. It follows immediately from the last diagram of the proposition, since the multiplication by $(-\overline{\eta})^{p-1}$ is an isomorphism of the additive group $\overline{F}$. □

3: Local Class Field Theory

This section focuses on complete discrete valuation fields with finite residue field.

3.1. Useful Results on Local Fields with Finite Residue Field

(3.1.1). Structures. Let F be a local field with finite residue field $\overline{F} = \mathbb{F}_q$, $q = p^f$ elements. Since $\mathrm{char}(\mathbb{F}_q) = p$, F is of characteristic 0 or of characteristic p.

In the first case $v(p) > 0$ for the discrete valuation v in F, hence the restriction of v on $\mathbb{Q}$ is equivalent to the p-adic valuation (by Ostrowski's Theorem). Then we can view the field $\mathbb{Q}_p$ of p-adic numbers as a subfield of F. Let $e = v(p) = e(F)$ be the absolute ramification index of F. Then F is a finite extension of $\mathbb{Q}_p$ of degree $n = ef$. Such a field was called a *local number field.*

In the second case F is isomorphic (with respect to the field structure and the discrete valuation topology) to the field of formal power series $\mathbb{F}_q((X))$ with prime element X, since the multiplicative representatives of the residue field form a finite subfield of F. Such a field was called a *local functional field.*

LEMMA. *F is a locally compact topological space with respect to the discrete valuation topology. The ring of integers $\mathcal{O}$ and the maximal ideal $\mathcal{M}$ are compact. The multiplicative group $F^\times$ is locally compact, and the group of units U is compact.*

Proof. Assume that $\mathcal{O}$ is not compact. Let $(V_i)_{i\in I}$ be a covering by open subsets in $\mathcal{O}$, i.e., $\mathcal{O} = \cup V_i$, such that $\mathcal{O}$ isn't covered by a finite union of V_i. Let π be a prime element of $\mathcal{O}$. Since $\mathcal{O}/\pi\mathcal{O}$ is finite, there exists an element $\theta_0 \in \mathcal{O}$ such that the set $\theta_0 + \pi\mathcal{O}$ is not contained in the union of a finite number of V_i. Similarly, there exist elements $\theta_1, \ldots, \theta_n \in \mathcal{O}$ such that $\theta_0 + \theta_1\pi + \cdots + \theta_n\pi^n + \pi^{n+1}\mathcal{O}$ is not contained in the union of a finite number of V_i. However, the element $\alpha = \lim_{n\to+\infty} \sum_{m=0}^{n} \theta_m\pi^m$ belongs to some V_i, a contradiction. Hence, $\mathcal{O}$ is compact and U, as the union of $\theta + \pi\mathcal{O}$ with $\overline{\theta} \neq 0$, is compact. □

(3.1.2). Galois Extensions.

LEMMA. *The Galois group of every finite extension of F is solvable.*

Proof. Follows from (2.11).

PROPOSITION. *For every $n \geqslant 1$ there exists a unique unramified extension L of F of degree n: $L = F(\mu_{q^n-1})$. The extension L/F is cyclic and the maximal unramified extension F^{ur} of F is a Galois extension.* $\mathrm{Gal}(F^{\mathrm{ur}}/F)$ *is isomorphic to $\widehat{\mathbb{Z}}$ and topologically generated by an automorphism φ_F such that*

$$\varphi_F(\alpha) \equiv \alpha^q \mod \mathcal{M}_{F^{\mathrm{ur}}} \qquad \text{for } \alpha \in \mathcal{O}_{F^{\mathrm{ur}}}.$$

The automorphism φ_F is called the Frobenius automorphism of F.

Proof. First we note that, by (2.1) F contains the group μ_{q-1} of $(q-1)$th roots of unity which coincides with the set of nonzero multiplicative representatives of $\overline{F}$ in $\mathcal{O}$. Moreover, the unit group U_F is isomorphic to $\mu_{q-1} \times U_{1,F}$.

The field $\mathbb{F}_q$ has the unique extension $\mathbb{F}_{q^n}$ of degree n, which is cyclic over $\mathbb{F}_q$. (2.7) shows that there is a unique unramified extension L of degree n over F and hence $L = F(\mu_{q^n-1})$.

Now let E be an unramified extension of F and $\alpha \in E$. Then $F(\alpha)/F$ is of finite degree. Therefore, F^{ur} is contained in the union of all finite unramified extensions of F. We have

$$\mathrm{Gal}(F^{\mathrm{ur}}/F) \simeq \varprojlim \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \widehat{\mathbb{Z}}.$$

It is well known that $\mathrm{Gal}(\mathbb{F}_q^{\mathrm{sep}}/\mathbb{F}_q)$ is topologically generated by the automorphism σ such that $\sigma(a) = a^q$ for $a \in \mathbb{F}_q^{\mathrm{sep}}$. Hence, $\mathrm{Gal}(F^{\mathrm{ur}}/F)$ is topologically generated by the Frobenius automorphism φ_F. □

REMARK. If $\theta \in \mu_{q^n-1}$, then

$$\varphi_F(\theta) \equiv \theta^q \mod \mathcal{M}_L$$

and $\varphi_F(\theta) \in \mu_{q^n-1}$. The uniqueness of the multiplicative representative for $\overline{\theta}^q \in \overline{F}$ implies now that $\varphi_F(\theta) = \theta^q$.

(3.1.3). EXAMPLE. Let ζ_{p^m} be a primitive p^m th root of unity. Put $\mathbb{Q}_p^{(m)} = \mathbb{Q}_p(\zeta_{p^m})$. Then

$$v_{\mathbb{Q}_p^{(m)}}(\zeta_{p^m}) = 0$$

and ζ_{p^m} belongs to the ring of integers of $\mathbb{Q}_p^{(m)}$. Let

$$f_m(X) = \frac{X^{p^m}-1}{X^{p^{m-1}}-1} = X^{(p-1)p^{m-1}} + X^{(p-2)p^{m-1}} + \cdots + 1.$$

Then ζ_{p^m} is a root of $f_m(X)$, and hence $|\mathbb{Q}_p^{(m)} : \mathbb{Q}_p| \leqslant (p-1)p^{m-1}$. The elements $\zeta_{p^m}^i$, $0 < i < p^m, p \nmid i$, are roots of $f_m(X)$. Hence

$$f_m(X) = \prod_{\substack{p \nmid i \\ 0<i<p^m}} (X - \zeta_{p^m}^i) \quad \text{and} \quad p = f_m(1) = \prod_{\substack{p \nmid i \\ 0<i<p^m}} (1 - \zeta_{p^m}^i).$$

However,

$$(1-\zeta_{p^m}^i)(1-\zeta_{p^m})^{-1} = 1+\zeta_{p^m}+\cdots+\zeta_{p^m}^{i-1}$$

belongs to the ring of integers of $\mathbb{Q}_p^{(m)}$. For the same reason, $(1-\zeta_{p^m})(1-\zeta_{p^m}^i)^{-1}$ belongs to the ring of integers of $\mathbb{Q}_p^{(m)}$. Thus, $(1-\zeta_{p^m}^i)(1-\zeta_{p^m})^{-1}$ is a unit and $p=(1-\zeta_{p^m})^{p^{m-1}(p-1)}\varepsilon$ for some unit ε. Therefore, $e(\mathbb{Q}_p^{(m)}|\mathbb{Q}_p)\geqslant(p-1)p^{m-1}$, and $\mathbb{Q}_p^{(m)}$ is a cyclic totally ramified extension with the prime element $1-\zeta_{p^m}$, and of degree $(p-1)p^{m-1}$ over $\mathbb{Q}_p$. In particular,

$$\mathcal{O}_{\mathbb{Q}_p^{(m)}} = \mathcal{O}_{\mathbb{Q}_p}[1-\zeta_{p^m}] = \mathcal{O}_{\mathbb{Q}_p}[\zeta_{p^m}].$$

(3.1.4). The Group of Principal Units. If $\mathrm{char}(F)=p$, then Proposition (6.2) Ch. I shows that every element $\alpha\in U_1$ can be uniquely expressed as the convergent product

$$\alpha=\prod_{\substack{p\nmid i\\ i>0}}\prod_{j\in J}(1+\theta_j\pi_i)^{a_{ij}},$$

where the index-set J numerates f elements in $\mathcal{O}_F$, such that their residues form a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$, and the elements θ_j belong to this set of f elements; π_i are elements of $\mathcal{O}_F$ with $v(\pi_i)=i$, and $a_{ij}\in\mathbb{Z}_p$. Thus, U_1 has the infinite topological basis $1+\theta_j\pi_i$.

Now let $\mathrm{char}(F)=0$. Every element $\alpha\in U_1$ can be expressed as a convergent product

$$\alpha=\prod_{i\in I}\prod_{j\in J}(1+\theta_j\pi_i)^{a_{ij}}\omega_*^a$$

where $I=\{1\leqslant i<pe/(p-1),\ p\nmid i\}$, $e=e(F)$; the index-set J numerates f elements in $\mathcal{O}_F$, such that their residues form a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$, and the elements θ_j belong to this set of f elements; π_i are elements of $\mathcal{O}_F$ with $v(\pi_i)=i$, and $a_{ij}\in\mathbb{Z}_p$.

If a primitive pth root of unity does not belong to F, then $\omega_*=1, a=0$ and the above expression for α is unique; U_1 is a free $\mathbb{Z}_p$-module of rank $n=ef=|F:\mathbb{Q}_p|$.

If a primitive pth root of unity belongs to F, then $\omega_*=1+\theta_*\pi_{pe/(p-1)}$ is a principal unit such that $\omega_*\notin F^{\times p}$, and $a\in\mathbb{Z}_p$. In this case the above expression for α is not unique. U_1 is isomorphic to the product of n copies of $\mathbb{Z}_p$ and the p-torsion group μ_{p^r}, where $r\geqslant 1$ is the maximal integer such that $\mu_{p^r}\subset F$.

LEMMA. *If* $\mathrm{char}(F)=0$, *then* $F^{\times n}$ *is an open subgroup of finite index in* $F^\times$ *for* $n\geqslant 1$. *If* $\mathrm{char}(F)=p$, *then* $F^{\times n}$ *is an open subgroup of finite index in* $F^\times$ *for* $p\nmid n$. *If* $\mathrm{char}(F)=p$ *and* $p|n$, *then* $F^{\times n}$ *is not open and is not of finite index in* $F^\times$.

Proof. It follows (1.9) and (1.10) and the previous considerations.

(3.1.5). The Norm Groups. Now we have a look at the norm group $N_{L/F}(L^\times)$ for a finite extension L of F. Recall that the norm map

$$N_{\mathbb{F}_{q'}/\mathbb{F}_q}:\mathbb{F}_{q'}^\times\longrightarrow\mathbb{F}_q^\times$$

is surjective when $\mathbb{F}_{q'}\supset\mathbb{F}_q$.

Let L/F be a finite unramified extension. Then (2.12) implies that $N_{L/F}U_L=U_F$ in the case of an unramified extension L/F and $N_{L/F}L^\times=\langle\pi^n\rangle\times U_F$, where π is a prime element in F, $n=|L:F|$. This means, in particular, that $F^\times/N_{L/F}L^\times$ is a cyclic group of order n

in this case. Conversely, every subgroup of finite index in $F^\times$ that contains U_F coincides with the norm group $N_{L/F}L^\times$ for a suitable unramified extension L/F.

Let L/F be a totally and tamely ramified Galois of degree n. (2.12) shows that

$$N_{L/F}U_{1,L} = U_{1,F}, \quad \pi \in N_{L/F}L^\times,$$

for a suitable prime element π in F (e.g. such that $L = F(\sqrt[n]{-\pi})$, and $\theta \in N_{L/F}L^\times$ for $\theta \in U_F$ if and only if $\overline{\theta} \in \mathbb{F}_q^{\times n}$. Since L/F is Galois, we get $\mu_n \subset F^\times$ and $n|(q-1)$. Hence, the subgroup $\mathbb{F}_q^{\times n}$ is of index n in $\mathbb{F}_q^\times$, and the quotient group $\mathbb{F}_q^\times/\mathbb{F}_q^{\times n}$ is cyclic. We conclude that

$$N_{L/F}L^\times = \langle\pi\rangle \times \langle\theta\rangle \times U_{1,F}$$

with an element $\theta \in U_F$, such that its residue $\overline{\theta}$ generates $\mathbb{F}_q^\times/\mathbb{F}_q^{\times n}$. So $F^\times/N_{L/F}L^\times$ is cyclic of order n. Conversely, every subgroup of index n relatively prime to $\mathrm{char}(\overline{F})$ coincides with the norm group $N_{L/F}L^\times$ for a suitable cyclic extension L/F.

Let L/F be a totally ramified Galois extension L/F of degree p. The right vertical homomorphism of the fourth diagram in the last proposition of (2.12) $\overline{\theta} \to \overline{\theta}^p - \overline{\eta}^{p-1}\overline{\theta}$ has kernel of order p; therefore its cokernel is also of order p. Let $\theta_* \in U_F$ be such that $\overline{\theta}_*$ does not belong to the image of this homomorphism. Since $\overline{F}$ is perfect, we deduce that $1+\theta_*\pi_F^s \notin N_{L/F}U_{1,L}$. The other diagrams imply that $F^\times/N_{L/F}L^\times$ is a cyclic group of order p and generated by $1+\theta_*\pi_F^s \mod N_{L/F}L^\times$. If $\mathrm{char}(F) = 0$, then $s \leqslant pe/(p-1)$, where $e = e(F)$, and if $p|s$ then $s = pe/(p-1)$ and a primitive pth root of unity ζ_p belongs to F, and $L = F(\sqrt[p]{\pi})$ for a suitable prime element π in F. In this case $F^\times/N_{L/F}L^\times$ is generated by $\omega_* \mod N_{L/F}L^\times$.

(3.1.6). Completion of F^{ur}. The field F^{ur} is a Henselian discrete valuation field with algebraically closed residue field and its completion $\mathcal{F}$ is a local field with algebraically closed residue field $\mathbb{F}_q^{\mathrm{sep}}$.

Let R be the set of multiplicative representatives of the residue field of $\mathcal{F}$ if its characteristic is p. R is the union of all sets $\mu_{q^n-1}, n \geqslant 1$ (which coincides with the set of all roots of unity of order relatively prime to p) and of 0.

Let $\mathcal{L}$ be a finite separable extension of $\mathcal{F}$. Since the residue field of $\mathcal{F}$ is algebraically closed, $\mathcal{L}/\mathcal{F}$ is totally ramified.

LEMMA. *The norm maps*

$$N_{\mathcal{L}/\mathcal{F}}: \mathcal{L}^\times \to \mathcal{F}^\times, \quad N_{\mathcal{L}/\mathcal{F}}: U_{\mathcal{L}} \to U_{\mathcal{F}}$$

are surjective.

Proof. Since the Galois group of $\mathcal{L}/\mathcal{F}$ is solvable, it suffices to consider the case of a Galois extension of prime degree l. Certainly, the norm of a prime element of $\mathcal{L}$ is a prime element of $\mathcal{F}$. The surjectivity of the norm maps follows from (2.12). □

(3.1.7). Augmentation Group $U(\mathcal{L}/\mathcal{F})$.

DEFINITION. For a finite Galois extension $\mathcal{L}/\mathcal{F}$ denote by $U(\mathcal{L}/\mathcal{F})$ the subgroup of $U_{1,\mathcal{L}}$ generated by $u^{\sigma-1}$ where u runs through all elements of $U_{1,\mathcal{L}}$ and σ runs through all elements of $\mathrm{Gal}(\mathcal{L}/\mathcal{F})$.

Every unit in $U_{\mathcal{L}}$ can be factorized as $\theta\varepsilon$ with $\theta \in R^{\times}$, $\varepsilon \in U_{1,\mathcal{L}}$ Since $\theta^{\sigma-1} = 1$ we deduce that $U(\mathcal{L}/\mathcal{F})$ coincides with the subgroup of $U_{\mathcal{L}}$ generated by $u^{\sigma-1}$, $u \in U_{\mathcal{L}}$, $\sigma \in \mathrm{Gal}(\mathcal{L}/\mathcal{F})$.

PROPOSITION. *Let $\mathcal{L}$ be a finite Galois extension of $\mathcal{F}$. For a prime element π of $\mathcal{L}$ define*

$$\ell\colon \mathrm{Gal}(\mathcal{L}/\mathcal{F}) \to U_{\mathcal{L}}/U(\mathcal{L}/\mathcal{F}), \quad \ell(\sigma) = \pi^{\sigma-1} \mod U(\mathcal{L}/\mathcal{F}).$$

The map ℓ is a homomorphism which does not depend on the choice of π. It induces a monomorphism $\ell\colon \mathrm{Gal}(\mathcal{L}/\mathcal{F})^{\mathrm{ab}} \to U_{\mathcal{L}}/U(\mathcal{L}/\mathcal{F})$ where for a group G the notation G^{ab} stands for the maximal abelian quotient of G.

The sequence

$$1 \to \mathrm{Gal}(\mathcal{L}/\mathcal{F})^{\mathrm{ab}} \xrightarrow{\ell} U_{\mathcal{L}}/U(\mathcal{L}/\mathcal{F}) \xrightarrow{N_{\mathcal{L}/\mathcal{F}}} U_{\mathcal{F}} \to 1$$

is exact.

Proof. Since $\pi^{\tau-1}$ belongs to $U_{\mathcal{L}}$, we deduce that $(\pi^{\tau-1})^{\sigma-1} \in U(\mathcal{L}/\mathcal{F})$ and

$$\pi^{\sigma\tau-1} \equiv \pi^{\tau-1}\pi^{\sigma-1} \mod U(\mathcal{L}/\mathcal{F}).$$

Thus, the map ℓ is a homomorphism. It does not depend on the choice of π, since $(\pi\varepsilon)^{\sigma-1} \equiv \pi^{\sigma-1} \mod U(\mathcal{L}/\mathcal{F})$.

Surjectivity of the norm map has already been proved.

Suppose first that $\mathrm{Gal}(\mathcal{L}/\mathcal{F})$ is cyclic with generator σ. The kernel of $N_{\mathcal{L}/\mathcal{F}}$ coincides with $\mathcal{L}^{\times\sigma-1}$. Since ℓ is a homomorphism, we have $\pi^{\sigma^m-1} \equiv (\pi^{\sigma-1})^m \mod U(\mathcal{L}/\mathcal{F})$. So we deduce that $\mathcal{L}^{\times\sigma-1}$ is equal to the product of $U(\mathcal{L}/\mathcal{F})$ and the image of ℓ. This shows the exactness in the middle term.

Note that $u^{\sigma^m-1} = (u^{1+\sigma+\cdots+\sigma^{m-1}})^{\sigma-1}$, so $U(\mathcal{L}/\mathcal{F}) = U_{\mathcal{L}}^{\sigma-1}$. If $\pi^{\sigma^m-1} \in U(\mathcal{L}/\mathcal{F})$, then $(\pi^{\sigma-1})^m = u^{\sigma-1}$ for some $u \in U_{\mathcal{L}}$. Hence $\pi^m u^{-1}$ belongs to $\mathcal{F}$ and therefore $|L:F|$ divides m and $\sigma^m = 1$. This shows the injectivity of ℓ.

Now in the general case we use the solvability of $\mathrm{Gal}(\mathcal{L}/\mathcal{F})$ and argue by induction. Let $\mathcal{M}/\mathcal{F}$ be a Galois cyclic subextension of $\mathcal{L}/\mathcal{F}$ such that $\mathcal{L} \neq \mathcal{M} \neq \mathcal{F}$. Put $\pi_M = N_{\mathcal{L}/\mathcal{M}}\pi$. Since $N_{\mathcal{L}/\mathcal{M}}\colon U_{\mathcal{L}} \to U_{\mathcal{M}}$ is surjective, we deduce that $N_{\mathcal{L}/\mathcal{M}}U(\mathcal{L}/\mathcal{F}) = U(\mathcal{M}/\mathcal{F})$.

Let $N_{\mathcal{L}/\mathcal{F}}u = 1$ for $u \in U_{\mathcal{L}}$. Then by the induction hypothesis there is $\tau \in \mathrm{Gal}(\mathcal{L}/\mathcal{F})$ such that $N_{\mathcal{L}/\mathcal{M}}u = \pi_M^{\tau-1}\eta$ with $\eta \in U(\mathcal{M}/\mathcal{F})$. Write $\eta = N_{\mathcal{L}/\mathcal{M}}\xi$ with $\xi \in U(\mathcal{L}/\mathcal{F})$. Then $u^{-1}\pi^{\tau-1}\xi$ belongs to the kernel of $N_{\mathcal{L}/\mathcal{M}}$ and therefore by the induction hypothesis can be written as $\pi^{\sigma-1}\rho$ with $\sigma \in \mathrm{Gal}(\mathcal{L}/\mathcal{M})$, $\rho \in U(\mathcal{L}/\mathcal{M})$. Altogether, $u \equiv \pi^{\sigma\tau-1} \mod U(\mathcal{L}/\mathcal{F})$ which shows the exactness in the middle term.

To show the injectivity of ℓ assume that $\pi^{\sigma-1} \in U(\mathcal{L}/\mathcal{F})$. Then $\pi_M^{\sigma-1} \in U(\mathcal{M}/\mathcal{F})$ and by the previous considerations of the cyclic case σ acts trivially on $\mathcal{M}$. So σ belongs to $\mathrm{Gal}(\mathcal{L}/\mathcal{M})$. Now the maximal abelian extension of $\mathcal{F}$ in $\mathcal{L}$ is the compositum of all cyclic extensions $\mathcal{M}$ of $\mathcal{F}$ in $\mathcal{L}$. Since σ acts trivially on each $\mathcal{M}$, we conclude that ℓ is injective. □

(3.1.8). $\varphi - 1$ Acting on $\mathcal{F}^{\times}$. For every n every element $\alpha \in \mathcal{F}$ can be uniquely expanded as

$$\alpha = \sum_{a \leqslant i} \theta_i \pi^i, \qquad \theta_i \in R,$$

where π is a prime element in F.

Since $\varphi: F^{\mathrm{ur}} \to F^{\mathrm{ur}}$ is continuous, it has exactly one extension $\varphi: \mathcal{F} \to \mathcal{F}$ which acts as $\sum_{i \geqslant a} \theta_i \pi^i \mapsto \sum_{i \geqslant a} \theta_i^q \pi^i$.

We shall study the action of φ^{-1} on the multiplicative group.

LEMMA. *The kernel of the homomorphism* $\mathcal{F}^\times \to \mathcal{F}^\times, \quad \alpha \mapsto \alpha^{\varphi-1}$ *is equal to* F *and the image is* $U_{\mathcal{F}}$; $U_{n,\mathcal{F}}^{\varphi-1} = U_{n,\mathcal{F}}$ *for every* $n \geqslant 1$.

Proof. For $\alpha = \sum_{i \geqslant a} \theta_i \pi^i \in \mathcal{F}$ with $\theta_i \in R$ the condition $\varphi(\alpha) = \alpha$ implies that $\overline{\varphi}(\overline{\theta}_i) = \overline{\theta}_i$ for $i \geqslant a$. Hence, $\overline{\theta}_i$ belongs to the residue field of F and $\alpha \in F$. Similarly one shows the exactness of the sequence in the central term $U_{n,\mathcal{F}}/U_{n+m,\mathcal{F}}$.

Let $\varepsilon \in U_{\mathcal{F}}$. We shall show the existence of a sequence $\beta_n \in U_{\mathcal{F}}$ such that $\varepsilon \equiv \beta_n^{\varphi-1}$ mod $U_{n+1,\mathcal{F}}$ and $\beta_{n+1}\beta_n^{-1} \in U_{n+1,\mathcal{F}}$.

Let $\varepsilon = \theta\varepsilon_0$ with $\theta \in R^\times$, $\varepsilon_0 \in U_{1,\mathcal{F}}$. Let $\rho \in R^\times$ be such that $\rho^{q-1} = \theta$. Then $\rho^{\varphi-1} = \theta$; put $\beta_0 = \rho$.

Now assume that the elements $\beta_0, \beta_1, \ldots, \beta_n \in U_{\mathcal{F}}$ have already been constructed. Define the element $\theta_{n+1} \in R$ from the congruence

$$\varepsilon^{-1}\beta_n^{\varphi-1} \equiv 1 + \theta_{n+1}\pi^{n+1} \mod \pi^{n+2}.$$

There is an element $\eta_{n+1} \in R$ such that

$$\varphi(\eta_{n+1}) - \eta_{n+1} + \theta_{n+1} = \eta_{n+1}^q - \eta_{n+1} + \theta_{n+1} \equiv 0 \mod \pi.$$

Now put $\beta_{n+1} = \beta_n(1 + \eta_{n+1}\pi^{n+1})$. Then $\varepsilon^{-1}\beta_{n+1}^{\varphi-1} \in U_{n+2,\mathcal{F}}$ and $\beta_{n+1}\beta_n^{-1} \in U_{n+1,\mathcal{F}}$.

There exists $\beta = \lim \beta_n \in U_{\mathcal{F}}$, and $\beta^{\varphi-1} = \varepsilon$. When $\varepsilon \in U_{n,\mathcal{F}}$ the element β can be chosen in $U_{n,\mathcal{F}}$ as well. □

Let L/F be a finite Galois totally ramified extension. The extension $L^{\mathrm{ur}}/F^{\mathrm{ur}}$ is Galois with the group isomorphic to that of L/F. We may assume that the completion of F^{ur} is a subfield of the completion of L^{ur}.

The extension $\mathcal{L}/\mathcal{F}$ is totally ramified of the same degree as L/F. From (2.7) and (2.8) we deduce that the extension $\mathcal{L}/\mathcal{F}$ is Galois with the group isomorphic to that of L/F.

PROPOSITION. *Let* $\gamma \in \mathcal{L}^\times$ *be such that* $\gamma^{\varphi-1} \in U(\mathcal{L}/\mathcal{F})$. *Then* $N_{\mathcal{L}/\mathcal{F}}\gamma$ *belongs to the group* $N_{L/F}L^\times$.

Proof. We have $\gamma^{\varphi-1} = \prod \varepsilon_j^{\tau_j - 1}$ for some $\varepsilon_j \in U_{\mathcal{L}}$ and $\tau_j \in \mathrm{Gal}(\mathcal{L}/\mathcal{F})$. By the previous proposition we have $\varepsilon_j = \eta_j^{\varphi-1}$ for some $\eta_j \in U_{\mathcal{L}}$. So $(\gamma^{-1}\prod \eta_j^{\tau_j - 1})^{\varphi-1} = 1$ and $\gamma^{-1}\prod \eta_j^{\tau_j - 1} = a$ with $a \in L^\times$. Then $N_{\mathcal{L}/\mathcal{F}}\gamma = N_{L/F}a^{-1} \in N_{L/F}L^\times$. □

3.2. The Neukirch Map

(3.2.1). Let L be a finite Galois extension of F. Then $L^{\mathrm{ur}} = LF^{\mathrm{ur}}$. Recall that $\mathrm{Gal}(F^{\mathrm{ur}}/F)$ consists of $\widehat{\mathbb{Z}}$-powers of φ_F.

DEFINITION. Put $\mathrm{Frob}(L/F) = \{\widetilde{\sigma} \in \mathrm{Gal}(L^{\mathrm{ur}}/F) : \widetilde{\sigma}|_{F^{\mathrm{ur}}} \text{ is a positive integer power of } \varphi_F\}$.

PROPOSITION. *The set* $\mathrm{Frob}(L/F)$ *is closed with respect to multiplication; it is not closed with respect to inversion and* $1 \notin \mathrm{Frob}(L/F)$.

The fixed field Σ *of* $\widetilde{\sigma} \in \mathrm{Frob}(L/F)$ *is of finite degree over* F, $\Sigma^{\mathrm{ur}} = L^{\mathrm{ur}}$, *and* $\widetilde{\sigma}$ *is the Frobenius automorphism of* Σ.

Thus, the set $\mathrm{Frob}(L/F)$ *consists of the Frobenius automorphisms* φ_Σ *of finite extensions* Σ *of* F *in* L^{ur} *with* $\mathrm{Gal}(L^{\mathrm{ur}}/\Sigma) \simeq \widehat{\mathbb{Z}}$.

The map $\mathrm{Frob}(L/F) \longrightarrow \mathrm{Gal}(L/F), \quad \widetilde{\sigma} \mapsto \widetilde{\sigma}|_L$ *is surjective.*

Proof. The first assertion is obvious.

Since $F \subset \Sigma \subset L^{\mathrm{ur}}$ we deduce that $F^{\mathrm{ur}} \subset \Sigma^{\mathrm{ur}} \subset L^{\mathrm{ur}}$. The Galois group of L^{ur}/Σ is topologically generated by $\widetilde{\sigma}$ and isomorphic to $\widehat{\mathbb{Z}}$, therefore it does not have nontrivial closed subgroups of finite order. So the group $\mathrm{Gal}(L^{\mathrm{ur}}/\Sigma^{\mathrm{ur}})$ being a subgroup of the finite group $\mathrm{Gal}(L^{\mathrm{ur}}/F^{\mathrm{ur}})$ should be trivial. So $L^{\mathrm{ur}} = \Sigma^{\mathrm{ur}}$.

Put $\Sigma_0 = \Sigma \cap F^{\mathrm{ur}}$. This field is the fixed field of $\widetilde{\sigma}|_{F^{\mathrm{ur}}} = \varphi_F^m$, therefore $|\Sigma_0 : F| = m$ is finite. We deduce that

$$|\Sigma : \Sigma_0| = |\Sigma^{\mathrm{ur}} : F^{\mathrm{ur}}| = |L^{\mathrm{ur}} : F^{\mathrm{ur}}| = |L : L_0|$$

is finite. Thus, Σ/F is a finite extension.

Now $\widetilde{\sigma}$ is a power of φ_Σ and $\varphi_\Sigma|_{F^{\mathrm{ur}}} = \varphi_F^{|\Sigma_0:F|}|_{F^{\mathrm{ur}}} = \varphi_F^m|_{F^{\mathrm{ur}}} = \widetilde{\sigma}|_{F^{\mathrm{ur}}}$. Therefore, $\widetilde{\sigma} = \varphi_\Sigma$. Certainly, the Frobenius automorphism φ_Σ of a finite extension Σ of F in L^{ur} with $\mathrm{Gal}(L^{\mathrm{ur}}/\Sigma) \simeq \widehat{\mathbb{Z}}$ belongs to $\mathrm{Frob}(L/F)$.

Denote by $\widetilde{\varphi}$ an extension in $\mathrm{Gal}(L^{\mathrm{ur}}/F)$ of φ_F. Let $\sigma \in \mathrm{Gal}(L/F)$, then $\sigma|_{L_0}$ is equal to φ_F^n for some positive integer n. Hence $\sigma^{-1}\widetilde{\varphi}^n|_L$ acts trivially on L_0, and so $\tau = \sigma\widetilde{\varphi}^{-n}|_L$ belongs to $\mathrm{Gal}(L/L_0)$. Let $\widetilde{\tau} \in \mathrm{Gal}(L^{\mathrm{ur}}/F^{\mathrm{ur}})$ be such that $\widetilde{\tau}|_L = \tau$. Then for $\widetilde{\sigma} = \widetilde{\tau}\widetilde{\varphi}^n$ we deduce that $\widetilde{\sigma}|_{F^{\mathrm{ur}}} = \varphi_F^n$ and $\widetilde{\sigma}|_L = \tau\widetilde{\varphi}^n|_L = \sigma$. Then the element $\widetilde{\sigma} \in \mathrm{Frob}(L/F)$ is mapped to $\sigma \in \mathrm{Gal}(L/F)$. □

(3.2.2). DEFINITION. Let L/F be a finite Galois extension. Introduce

$$\boxed{\widetilde{\Upsilon}_{L/F}\colon \mathrm{Frob}(L/F) \longrightarrow F^\times/N_{L/F}L^\times, \quad \widetilde{\sigma} \mapsto N_{\Sigma/F}\pi_\Sigma \mod N_{L/F}L^\times}$$

where Σ is the fixed field of $\widetilde{\sigma} \in \mathrm{Frob}(L/F)$ and π_Σ is any prime element of Σ.

LEMMA. *The map* $\widetilde{\Upsilon}_{L/F}$ *is well defined. If* $\widetilde{\sigma}|_L = \mathrm{id}_L$ *then* $\widetilde{\Upsilon}_{L/F}(\widetilde{\sigma}) = 1$.

Proof. Let π_1, π_2 be prime elements in Σ. Then $\pi_1 = \pi_2\varepsilon$ for a unit $\varepsilon \in U_\Sigma$. Let E be the compositum of Σ and L. Since $\Sigma \subset E \subset \Sigma^{\mathrm{ur}}$, the extension E/Σ is unramified. From (3.1.5) we know that $\varepsilon = N_{E/\Sigma}\eta$ for some $\eta \in U_E$. Hence

$$N_{\Sigma/F}\pi_1 = N_{\Sigma/F}(\pi_2\varepsilon) = N_{\Sigma/F}\pi_2 \cdot N_{\Sigma/F}(N_{E/\Sigma}\eta) = N_{\Sigma/F}\pi_2 \cdot N_{L/F}(N_{E/L}\eta).$$

We obtain that $N_{\Sigma/F}\pi_1 \equiv N_{\Sigma/F}\pi_2 \mod N_{L/F}L^\times$.

If $\widetilde{\sigma}|_L = \mathrm{id}_L$ then $L \subset \Sigma$ and therefore $N_{\Sigma/F}\pi_\Sigma \in N_{L/F}L^\times$. □

(3.2.3). The definition of the Neukirch map is very natural from the point of view of the well known principle that a prime element in an unramified extension should correspond to the Frobenius automorphism (see Theorem (3.2.4) below) and the functorial property of the reciprocity map (see (3.2.5) and (3.3.4)) which forces the reciprocity map $\Upsilon_{L/F}$ to be defined as it is.

Already at this stage one can prove that the map $\widetilde{\Upsilon}_{L/F}\colon \mathrm{Frob}(L/F) \longrightarrow F^\times/N_{L/F}L^\times$ induces the Neukirch homomorphism

$$\Upsilon_{L/F}\colon \mathrm{Gal}(L/F) \longrightarrow F^\times/N_{L/F}L^\times.$$

In other words, $\widetilde{\Upsilon}_{L/F}(\widetilde{\sigma})$ does not depend on the choice of $\widetilde{\sigma} \in \mathrm{Frob}(L/F)$ which extends $\sigma \in \mathrm{Gal}(L/F)$, and moreover, $\widetilde{\Upsilon}_{L/F}(\widetilde{\sigma}_1)\widetilde{\Upsilon}_{L/F}(\widetilde{\sigma}_2) = \widetilde{\Upsilon}_{L/F}(\widetilde{\sigma_1\sigma_2})$.

We will choose a different route, which is a little longer but perhaps is more satisfying.

The plan is the following: first we easily show the existence of $\Upsilon_{L/F}$ for unramified extensions and even prove that it is an isomorphism. Then we deduce some functorial properties of $\widetilde{\Upsilon}_{L/F}$. To treat the case of totally ramified extensions in the next section, we introduce the Hazewinkel homomorphism $\Psi_{L/F}$ which acts in the opposite direction to $\Upsilon_{L/F}$. Calculating composites of the latter with $\Psi_{L/F}$ we shall deduce the existence of $\Upsilon_{L/F}$ which is expressed by the commutative diagram

$$\begin{array}{ccc} \mathrm{Frob}(L/F) & \xrightarrow{\widetilde{\Upsilon}_{L/F}} & F^\times/N_{L/F}L^\times \\ \downarrow & & \mathrm{id}\downarrow \\ \mathrm{Gal}(L/F) & \xrightarrow{\Upsilon_{L/F}} & F^\times/N_{L/F}L^\times. \end{array}$$

Then using $\Psi_{L/F}$ we prove that $\Upsilon_{L/F}$ is a homomorphism and that its abelian part

$$\Upsilon^{\mathrm{ab}}_{L/F}\colon \mathrm{Gal}(L/F)^{\mathrm{ab}} \to F^\times/N_{L/F}L^\times$$

is an isomorphism.

Then we treat the general case of abelian extensions and then Galois extensions reducing it to the two cases described above and using functorial properties of $\widetilde{\Upsilon}_{L/F}$. This route not only establishes the existence of $\Upsilon_{L/F}$, but also implies its isomorphism properties.

(3.2.4). THEOREM. *Let L be an unramified extension of F of finite degree.*

Then $\widetilde{\Upsilon}_{L/F}(\widetilde{\sigma})$ does not depend on the choice of $\widetilde{\sigma}$ for $\sigma \in \mathrm{Gal}(L/F)$. It induces an isomorphism $\Upsilon_{L/F}\colon \mathrm{Gal}(L/F) \longrightarrow F^\times/N_{L/F}L^\times$ and

$$\Upsilon_{L/F}\big(\varphi_F|_L\big) \equiv \pi_F \mod N_{L/F}L^\times$$

for a prime element π_F in F.

Proof. Since L/F is unramified, σ is equal to φ_F^n sor some $n \geqslant 1$. Let $m = |L : F|$. Then $\widetilde{\sigma}$ must be in the form φ_F^d with $d = n + lm > 0$ for some integer l. The fixed field Σ of $\widetilde{\sigma}$ is

the unramified extension of F of degree d. We can take π_F as a prime element of Σ. Then

$$\widetilde{\Upsilon}_{L/F}(\widetilde{\sigma}) = N_{\Sigma/F}\pi_F = \pi_F^d \equiv \pi_F^n \mod N_{L/F}L^\times,$$

since $\pi_F^m = N_{L/F}\pi_F$. Thus, $\widetilde{\Upsilon}_{L/F}(\widetilde{\sigma})$ does not depend on the choice of $\widetilde{\sigma}$.

It is now clear that $\Upsilon_{L/F}$ is a homomorphism and it sends φ_F to $\pi_F \mod N_{L/F}L^\times$. Results of (3.1.5) show that $\pi_F \mod N_{L/F}L^\times$ generates the group $F^\times/N_{L/F}L^\times$ which is cyclic of order $|L:F|$. Hence, $\Upsilon_{L/F}$ is an isomorphism. □

(3.2.5). Now we describe first functorial properties of $\widetilde{\Upsilon}_{L/F}$.

LEMMA. *Let M/F be a finite separable extension and let L/M be a finite Galois extension, $\sigma \in \mathrm{Gal}(F^{\mathrm{sep}}/F)$. Then the diagram of maps*

$$\begin{array}{ccc} \mathrm{Frob}(L/M) & \xrightarrow{\widetilde{\Upsilon}_{L/M}} & M^\times/N_{L/M}L^\times \\ {\scriptstyle \sigma^*}\downarrow & & \downarrow{\scriptstyle \sigma} \\ \mathrm{Frob}(\sigma L/\sigma M) & \xrightarrow{\widetilde{\Upsilon}_{\sigma L/\sigma M}} & (\sigma M)^\times/N_{\sigma L/\sigma M}(\sigma L)^\times \end{array}$$

is commutative; here $\sigma^*(\widetilde{\tau}) = \sigma\widetilde{\tau}\sigma^{-1}|_{\sigma L^{\mathrm{ur}}}$ for $\widetilde{\tau} \in \mathrm{Frob}(L/M)$.

Proof. If Σ is the fixed field of $\widetilde{\tau}$, then $\sigma\Sigma$ is the fixed field of $\sigma\widetilde{\tau}\sigma^{-1}$. For a prime element π in Σ, the element $\sigma\pi$ is prime in $\sigma\Sigma$. Since $N_{\sigma\Sigma/\sigma M}(\sigma\pi) = \sigma N_{\Sigma/M}\pi$, the proof is completed. □

PROPOSITION. *Let M/F and E/L be finite separable extensions, and let L/F and E/M be finite Galois extensions. Then the diagram of maps*

$$\begin{array}{ccc} \mathrm{Frob}(E/M) & \xrightarrow{\widetilde{\Upsilon}_{E/M}} & M^\times/N_{E/M}E^\times \\ \downarrow & & \downarrow{\scriptstyle N^*_{M/F}} \\ \mathrm{Frob}(L/F) & \xrightarrow{\widetilde{\Upsilon}_{L/F}} & F^\times/N_{L/F}L^\times \end{array}$$

is commutative. Here the left vertical homomorphism is the restriction $\widetilde{\sigma}|_{L^{\mathrm{ur}}}$ of $\widetilde{\sigma} \in \mathrm{Frob}(E/M)$ and the right vertical homomorphism is induced by the norm map $N_{M/F}$.

The left vertical map is surjective if $M = F$.

Proof. Indeed, if $\widetilde{\sigma} \in \mathrm{Frob}(E/M)$ then for $\widetilde{\tau} = \widetilde{\sigma}|_{L^{\mathrm{ur}}} \in \mathrm{Gal}(L^{\mathrm{ur}}/F)$ we deduce that $\widetilde{\tau}|_{F^{\mathrm{ur}}} = \widetilde{\sigma}|_{F^{\mathrm{ur}}}$ is a positive power of φ_F, i.e., $\widetilde{\tau} \in \mathrm{Frob}(L/F)$. Let Σ be the fixed field of $\widetilde{\sigma}$. Then $\mathrm{T} = \Sigma \cap L^{\mathrm{ur}}$ is the fixed field of $\widetilde{\tau}$. The extension Σ/T is totally ramified, since $L^{\mathrm{ur}} = \mathrm{T}^{\mathrm{ur}}$ and so $\mathrm{T} = \Sigma \cap \mathrm{T}^{\mathrm{ur}}$. Hence for a prime element π_Σ in Σ the element $\pi_{\mathrm{T}} = N_{\Sigma/\mathrm{T}}\pi_\Sigma$ is prime in T and we get $N_{\mathrm{T}/F}\pi_{\mathrm{T}} = N_{\Sigma/F}\pi_\Sigma = N_{M/F}(N_{\Sigma/M}\pi_\Sigma)$.

If $M = F$, then the left vertical map is surjective, since every extension of $\widetilde{\sigma} \in \mathrm{Frob}(L/F)$ to $\mathrm{Gal}(E^{\mathrm{ur}}/F)$ belongs to $\mathrm{Frob}(E/F)$. □

COROLLARY. *Let M/F be a Galois subextension in a finite Galois extension L/F. Then the diagram of maps*

$$\begin{array}{ccccc} \mathrm{Frob}(L/M) & \longrightarrow & \mathrm{Frob}(L/F) & \longrightarrow & \mathrm{Frob}(M/F) \\ \downarrow \widetilde{\Upsilon}_{L/M} & & \downarrow \widetilde{\Upsilon}_{L/F} & & \downarrow \widetilde{\Upsilon}_{M/F} \\ M^\times/N_{L/M}L^\times & \xrightarrow{N^*_{M/F}} & F^\times/N_{L/F}L^\times & \longrightarrow & F^\times/N_{M/F}M^\times \longrightarrow 1 \end{array}$$

is commutative; *here the central homomorphism of the lower exact sequence is induced by the identity map of $F^\times$.*

Proof. An easy consequence of the preceding Proposition. □

3.3. The Hazewinkel Homomorphism

(3.3.1). Let L be a finite Galois totally ramified extension of F. The Galois group of the extension $\mathcal{L}/\mathcal{F}$ is isomorphic to $\mathrm{Gal}(L/F)$.

DEFINITION. Let φ be the continuous extension on $\mathcal{L}$ of the Frobenius automorphism φ_L. Let π be a prime element of $\mathcal{L}$. Let E be the maximal abelian extension of F in L. For $\alpha \in F^\times$ by Lemma (3.1.6) there is $\beta \in \mathcal{L}^\times$ such that $\alpha = N_{\mathcal{L}/\mathcal{F}}\beta$. Then $N_{\mathcal{L}/\mathcal{F}}\beta^{\varphi-1} = \alpha^{\varphi-1} = 1$ and by Proposition (3.1.7)

$$\beta^{\varphi-1} \equiv \pi^{1-\sigma} \mod U(\mathcal{L}/\mathcal{F})$$

for some $\sigma \in \mathrm{Gal}(\mathcal{L}/\mathcal{F})$ which is uniquely determined as an element of $\mathrm{Gal}(\mathcal{E}/\mathcal{F})$ where $\mathcal{E} = E\mathcal{F}$. Define the *Hazewinkel* (*reciprocity*) *homomorphism*

$$\boxed{\Psi_{L/F}: F^\times/N_{L/F}L^\times \longrightarrow \mathrm{Gal}(L/F)^{\mathrm{ab}}, \quad \alpha \mapsto \sigma|_E, \quad \alpha = N_{\mathcal{L}/\mathcal{F}}\beta, \quad \beta^{\varphi-1} \equiv \pi^{1-\sigma}}$$

LEMMA. *The map $\Psi_{L/F}$ is well defined and is a homomorphism.*

Proof. First, independence on the choice of π follows from Proposition (3.1.7). So we can assume that $\pi \in L$.

If $\alpha = N_{\mathcal{L}/\mathcal{F}}\gamma$ then $\gamma\beta^{-1}$ belongs to the kernel of $N_{\mathcal{L}/\mathcal{F}}$. Therefore by Proposition (3.1.7) $\gamma\beta^{-1} = \pi^{\tau-1}\xi$ with $\xi \in U(\mathcal{L}/\mathcal{F})$. Then $\gamma^{\varphi-1} = \beta^{\varphi-1}\xi^{\varphi-1} \equiv \beta^{\varphi-1} \mod U(\mathcal{L}/\mathcal{F})$ which proves correctness of the definition.

If $N_{\mathcal{L}/\mathcal{F}}(\beta_1) = \alpha_1$ and $N_{\mathcal{L}/\mathcal{F}}(\beta_2) = \alpha_2$, then we can choose $\beta_1\beta_2$ for $\alpha_1\alpha_2$ and then from Proposition (3.1.7) we deduce that $\Psi_{L/F}$ is a homomorphism. □

REMARKS.

1. Since L/F is totally ramified, the norm of a prime element of L is a prime element of F. So $F^\times/N_{L/F}L^\times = U_F/N_{L/F}U_L$. Moreover, if L/F is a totally ramified p-extension (i.e. its degree is a power of p), then $F^\times/N_{L/F}L^\times = U_{1,F}/N_{L/F}U_{1,L}$, since all multiplicative representatives are pth powers.

2. The Hazewinkel homomorphism can be defined for every finite Galois extension, but it has the simplest form for totally ramified extensions.

(3.3.2). Now we prove that $\Psi_{L/F}$ is inverse to $\Upsilon^{\mathrm{ab}}_{L/F}$.

THEOREM. *Let L/F be a finite Galois totally ramified extension. Let E/F be the maximal abelian subextension of L/F. Then*

(1) *For every $\widetilde{\sigma} \in \mathrm{Frob}(L/F)$*

$$\Psi_{L/F}\big(\widetilde{\Upsilon}_{L/F}(\widetilde{\sigma})\big) = \widetilde{\sigma}|_E.$$

(2) *Let $\alpha \in F^\times$ and let $\widetilde{\sigma} \in \mathrm{Frob}(L/F)$ be such that $\widetilde{\sigma}|_E = \Psi_{L/F}(\alpha)$. Then*

$$\widetilde{\Upsilon}_{L/F}(\widetilde{\sigma}) \equiv \alpha \mod N_{L/F}L^\times.$$

Therefore, $\Psi_{L/F}$ is an isomorphism, $\widetilde{\Upsilon}_{L/F}(\widetilde{\sigma})$ does not depend on the choice of $\widetilde{\sigma}$ for $\sigma \in \mathrm{Gal}(L/F)$ and induces the Neukirch homomorphism

$$\Upsilon_{L/F}\colon \mathrm{Gal}(L/F) \longrightarrow F^\times/N_{L/F}L^\times.$$

The latter induces an isomorphism $\Upsilon^{\mathrm{ab}}_{L/F}$ between the groups $\mathrm{Gal}(L/F)^{\mathrm{ab}} = \mathrm{Gal}(E/F)$ and $F^\times/N_{L/F}L^\times$, which is inverse to $\Psi_{L/F}$.

Proof. *To show* (1) note at first that $\mathrm{Gal}(L^{\mathrm{ur}}/F)$ is isomorphic to $\mathrm{Gal}(L^{\mathrm{ur}}/L) \times \mathrm{Gal}(L^{\mathrm{ur}}/F^{\mathrm{ur}})$ and so $\widetilde{\sigma}$ is equal to $\sigma\varphi^m$ for some positive integer m and $\sigma \in \mathrm{Gal}(L^{\mathrm{ur}}/F^{\mathrm{ur}})$. Let π_Σ be a prime element of the fixed field Σ of $\widetilde{\sigma}$. Since π_Σ is a prime element of $\Sigma^{\mathrm{ur}} = L^{\mathrm{ur}}$ we have $\pi_\Sigma = \pi\varepsilon$ for some $\varepsilon \in U_{L^{\mathrm{ur}}}$, where π is a prime element of L. Therefore $\pi^{1-\sigma} = \varepsilon^{\sigma\varphi^m-1}$.

Let $\Sigma_0 = \Sigma \cap F^{\mathrm{ur}}$, then $|\Sigma_0 : F| = m$. Then $N_{\Sigma/F} = N_{\Sigma_0/F} \circ N_{\Sigma/\Sigma_0}$ and N_{Σ/Σ_0} acts as $N_{\Sigma^{\mathrm{ur}}/\Sigma_0^{\mathrm{ur}}} = N_{L^{\mathrm{ur}}/F^{\mathrm{ur}}} = N_{\mathcal{L}/\mathcal{F}}$, $N_{\Sigma_0/F}$ acts as $1 + \varphi + \cdots + \varphi^{m-1}$. We have

$$N_{\Sigma/F}\pi_\Sigma = N_{L^{\mathrm{ur}}/F^{\mathrm{ur}}}\varepsilon_1\, N_{L^{\mathrm{ur}}/F^{\mathrm{ur}}}\pi^m, \quad \text{where } \varepsilon_1 = \varepsilon^{1+\varphi+\cdots+\varphi^{m-1}}.$$

So $\alpha = N_{\Sigma/F}\pi_\Sigma \equiv N_{L^{\mathrm{ur}}/F^{\mathrm{ur}}}\varepsilon_1 \mod N_{L/F}L^\times$ and $\Psi_{L/F}(\alpha)$ can be calculated by looking at $\varepsilon_1^{\varphi-1}$. We deduce $\varepsilon_1^{\varphi-1} = \varepsilon^{\varphi^m-1} \equiv \varepsilon^{\sigma\varphi^m-1} = \pi^{1-\sigma} = \pi^{1-\widetilde{\sigma}} \mod U(\mathcal{L}/\mathcal{F})$. This proves (1).

To show (2) let $\alpha = N_{\mathcal{L}/\mathcal{F}}\beta$ and $\beta^{\varphi-1} \equiv \pi^{1-\sigma} \mod U(\mathcal{L}/\mathcal{F})$ with $\sigma \in \mathrm{Gal}(L/F)$. Then again $\widetilde{\sigma} = \sigma\varphi^m$ and similarly to the previous $\widetilde{\Upsilon}_{L/F}(\widetilde{\sigma}) = N_{\Sigma/F}\pi_\Sigma \equiv N_{L^{\mathrm{ur}}/F^{\mathrm{ur}}}\varepsilon_1 \mod N_{L/F}L^\times$ and $\varepsilon_1^{\varphi-1} \equiv \pi^{1-\sigma} \equiv \beta^{\varphi-1} \mod U(\mathcal{L}/\mathcal{F})$. From the second proposition of (3.1.9) applied to $\gamma = \varepsilon_1\beta^{-1}$ we deduce that $N_{\mathcal{L}/\mathcal{F}}\gamma$ belongs to $N_{L/F}L^\times$ and therefore $N_{\mathcal{L}/\mathcal{F}}\varepsilon_1 \equiv N_{\mathcal{L}/\mathcal{F}}\beta = \alpha \mod N_{L/F}L^\times$ which proves (2).

Now from (1) we deduce the surjectivity of $\Psi_{L/F}$. From (2) and Lemma in (3.2.2) by taking $\widetilde{\sigma} = \varphi$, so that $\widetilde{\sigma}|_E = \mathrm{id}_E = \Psi_{L/F}(\alpha)$, we deduce that $\alpha \in N_{L/F}L^\times$, i.e. $\Psi_{L/F}$ is injective. Hence $\Psi_{L/F}$ is an isomorphism. Now from (1) we conclude that $\widetilde{\Upsilon}_{L/F}$ does not depend on the choice of a lifting $\widetilde{\sigma}$ of $\sigma \in \mathrm{Gal}(L/F)$ and therefore determines the map $\Upsilon_{L/F}$.

Since we can take $\widetilde{\sigma_1\sigma_2} = \widetilde{\sigma}_1\widetilde{\sigma}_2$, from (1) we deduce that $\Upsilon_{L/F}$ is a homomorphism.

Proposition (3.2.1) and (2) show that this homomorphism is surjective. From (1) we deduce that its kernel is contained in $\mathrm{Gal}(L/E)$. The latter coincides with the kernel, since the image of $\Upsilon_{L/F}$ is abelian. □

COROLLARY. *For $\sigma \in \mathrm{Gal}(L/F)$ there exists $\eta \in \mathcal{L}^\times$ such that $\eta^{\varphi-1} = \pi^{1-\sigma}$. Then $\varepsilon = N_{\mathcal{L}/\mathcal{F}}\eta$ belongs to $F^\times$ and $\Upsilon_{L/F}(\sigma) = N_{\mathcal{L}/\mathcal{F}}\eta$.*

Conversely, for every $\varepsilon \in F^\times$ *there exists* $\eta \in \mathcal{L}^\times$ *such that*

$$\varepsilon \equiv N_{\mathcal{L}/\mathcal{F}}\eta \mod N_{L/F}L^\times, \qquad \eta^{\varphi-1} = \pi^{1-\sigma} \quad \textit{for some } \sigma \in \mathrm{Gal}(\mathcal{L}/\mathcal{F}).$$

Then $\Psi_{L/F}(\varepsilon) = \sigma|_E$.

Proof. We can assume that η is a unit, since $\pi^{\varphi-1} = 1$. Denote by the same notation σ the element of $\mathrm{Gal}(\mathcal{L}/\mathcal{F})$ which corresponds to σ. Let Σ be the fixed field of $\widetilde{\sigma} = \sigma\varphi$. Applying the lemma of (3.1.8) to the continuous extension to $\mathcal{L}$ of the Frobenius automorphism $\widetilde{\sigma}$ we deduce that there is $\rho \in U_{\mathcal{L}}$ such that $\rho^{\sigma\varphi-1} = \pi^{1-\sigma}$. Now

$$\pi^{1-\sigma\varphi} = \pi^{1-\sigma} = \rho^{\sigma\varphi-1},$$

so $\pi\rho$ belongs to the fixed field of $\widetilde{\sigma}$ in $\mathcal{L}$ which by the lemma of (3.1.8) equals to the fixed field Σ of $\widetilde{\sigma}$ in L^{ur}. The element $\pi_\Sigma = \pi\rho$ is a prime element of Σ. Note that $(\rho\eta^{-1})^{\varphi-1} = \rho^{\varphi-1}\pi^{\sigma-1} = (\rho^{1-\sigma})^{\varphi} \in U(\mathcal{L}/\mathcal{F})$; hence from the proposition of (3.1.8) we deduce that $N_{\mathcal{L}/\mathcal{F}}\rho \equiv N_{\mathcal{L}/\mathcal{F}}\eta \mod N_{L/F}L^\times$. Finally,

$$N_{\Sigma/F}\pi_\Sigma \equiv N_{\mathcal{L}/\mathcal{F}}\rho \equiv N_{\mathcal{L}/\mathcal{F}}\eta \mod N_{L/F}L^\times.$$

To prove the second assertion use the first assertion and the congruence supplied by the Theorem: $\varepsilon \equiv \Upsilon_{L/F}(\sigma) \mod N_{L/F}L^\times$ where $\sigma \in \mathrm{Gal}(L/F)$ is such that $\sigma|_E = \Psi_{L/F}(\varepsilon)$. □

The Theorem demonstrates that for a finite Galois totally ramified extension L/F in the definition of the Neukirch map one can fix the choice of Σ as the field invariant under the action of $\sigma\varphi$.

(3.3.3). The following Lemma will be useful in the proof of the main theorem.

LEMMA. *Let* L/F *be a finite abelian extension. Then there is a finite unramified extension* M/L *such that* M *is an abelian extension of* F, M *is the compositum of an unramified extension* M_0 *of* F *and an abelian totally ramified extension* K *of* F. *For every such* M *we have* $N_{M/F}M^\times = N_{K/F}K^\times \cap N_{M_0/F}M_0^\times$.

Proof. Since L/F is abelian, the extension LF^{ur} is an abelian extension of F. Let $\widetilde{\varphi} \in \mathrm{Gal}(LF^{\mathrm{ur}}/F)$ be an extension of φ_F. Let K be the fixed field of $\widetilde{\varphi}$. Then $K \cap F^{\mathrm{ur}} = F$, so K is an abelian totally ramified extension of F. The compositum M of K and L is an unramified extension of L, since $K^{\mathrm{ur}} = L^{\mathrm{ur}}$. The field M is an abelian extension of F and $\mathrm{Gal}(M/F) \simeq \mathrm{Gal}(M/K) \times \mathrm{Gal}(M/M_0)$.

Now the left hand side of the formula of the Lemma is contained in the right hand side $\mathcal{N}$. We have $\mathcal{N} \cap U_F \subset N_{K/F}U_K \subset N_{M/F}U_M$, since $U_K \subset N_{M/K}U_M$. If π_M is a prime element of M, then $N_{M/F}\pi_M \in \mathcal{N}$. Then $v_F(N_{M/F}\pi_M)\mathbb{Z} = v_F(N_{M_0/F}M_0^\times)$. So every $\alpha \in \mathcal{N}$ can be written as $\alpha = N_{M/F}\pi_M^m\varepsilon$ with $\varepsilon \in \mathcal{N} \cap U_F$ and some m. Thence $\mathcal{N}$ is contained in $N_{M/F}M^\times$ and we have $\mathcal{N} = N_{M/F}M^\times$. □

Now we state and prove the first main theorem of local class field theory.

THEOREM. *Let* L/F *be a finite Galois extension. Let* E/F *be the maximal abelian subextension of* L/F.

Then $\Psi_{L/F}$ *is an isomorphism,* $\widetilde{\Upsilon}_{L/F}(\widetilde{\sigma})$ *does not depend on the choice of* $\widetilde{\sigma}$ *for* $\sigma \in \mathrm{Gal}(L/F)$ *and induces the Neukirch* (*reciprocity*) *homomorphism*

$$\Upsilon_{L/F}\colon \mathrm{Gal}(L/F) \longrightarrow F^{\times}/N_{L/F}L^{\times}.$$

The latter induces an isomorphism $\Upsilon^{\mathrm{ab}}_{L/F}$ *between* $\mathrm{Gal}(L/F)^{\mathrm{ab}} = \mathrm{Gal}(E/F)$ *and* $F^{\times}/N_{L/F}L^{\times}$ (*which is inverse to* $\Psi_{L/F}$ *for totally ramified extensions*).

Proof. *First*, we consider the case of an abelian extension L/F such that L is the compositum of the maximal unramified extension L_0 of F in L and an abelian totally ramified extension K of F. Then by the previous lemma $N_{L/F}L^{\times} = N_{K/F}K^{\times} \cap N_{L_0/F}L_0^{\times}$. From Proposition (3.2.5) applied to surjective maps

$$\mathrm{Frob}(L/F) \to \mathrm{Frob}(L_0/F) \quad \text{and} \quad \mathrm{Frob}(L/F) \to \mathrm{Frob}(K/F),$$

and from Theorem (3.2.4) and Theorem (3.3.2) we deduce that $\widetilde{\Upsilon}_{L/F}$ does not depend on the choice of $\widetilde{\sigma}$ modulo $N_{K/F}K^{\times} \cap N_{L_0/F}L_0^{\times}$, therefore, modulo $N_{L/F}L^{\times}$. So we get the map $\Upsilon_{L/F}$.

Now from Proposition (3.2.5) and Theorem (3.2.4), Theorem (3.3.2) we deduce that $\Upsilon_{L/F}$ is a homomorphism modulo $N_{K/F}K^{\times} \cap N_{L_0/F}L_0^{\times}$, so it is a homomorphism modulo $N_{L/F}L^{\times}$. It is injective, since if $\Upsilon_{L/F}(\sigma) \in N_{L/F}L^{\times}$, then σ acts trivially on L_0 and K, and so on L. Its surjectivity follows from the commutative diagram of Corollary in (3.2.5).

Second, we consider the case of an arbitrary finite abelian extension L/F. By the previous Lemma and the preceding arguments there is an unramified extension M/L such that the map $\widetilde{\Upsilon}_{M/F}$ induces the isomorphism $\Upsilon_{M/F}$. The map $\mathrm{Frob}(M/F) \to \mathrm{Frob}(L/F)$ is surjective and we deduce using Proposition (3.2.5) that $\widetilde{\Upsilon}_{L/F}$ induces the well defined map $\Upsilon_{L/F}$, which is a surjective homomorphism. If $\sigma \in \mathrm{Gal}(M/F)$ is such that $\Upsilon_{L/F}(\sigma) = 1$, then from the commutative diagram of Corollary in (3.2.5) and surjectivity of Υ for every finite abelian extension we deduce that $\Upsilon_{M/F}(\sigma) = \Upsilon_{M/F}(\tau)$ for some $\tau \in \mathrm{Gal}(M/L)$. The injectivity of $\Upsilon_{M/F}$ now implies that $\sigma = \tau$ acts trivially on L.

Finally, we consider the general case of a finite Galois extension where we argue by induction on the degree of L/F. We can assume that L/F is not an abelian extension.

Every $\sigma \in \mathrm{Gal}(L/F)$ belongs to the cyclic subgroup of $\mathrm{Gal}(L/F)$ generated by it, and by what has already been proved and by Proposition in (3.2.5) $\widetilde{\Upsilon}_{L/F}(\widetilde{\sigma})$ does not depend on the choice of $\widetilde{\sigma}$ and therefore determines the map $\Upsilon_{L/F}$.

Since $\mathrm{Gal}(L/F)$ is solvable, we conclude similarly to the second case above using the induction hypothesis that $\Upsilon_{L/F}$ is surjective. In the next several paragraphs we shall show that $\Upsilon_{L/F}(\mathrm{Gal}(L/E)) = 1$. Due to surjectivity of Υ this implies that the map $N^{\times}_{E/F}$ in the diagram of Corollary (3.2.5) (where we put $M = E$) is zero. Since $\Upsilon_{E/F}$ is an isomorphism we see from the diagram of the Corollary that $\Upsilon_{L/F}$ is a surjective homomorphism with kernel $\mathrm{Gal}(L/E)$.

So it remains to prove that $\Upsilon_{L/F}$ maps every element of the derived group $\mathrm{Gal}(L/E)$ to 1. Since $\mathrm{Gal}(L/F)$ is solvable, we have $E \neq F$. Proposition (3.2.5) shows that $\Upsilon_{L/F}(\rho) = N^{\times}_{E/F}(\Upsilon_{L/E}(\rho))$ for every $\rho \in \mathrm{Gal}(L/E)$. Since by the induction assumption $\Upsilon_{L/E}$ is a homomorphism, it suffices to show that

$$\Upsilon_{L/F}(\tau\sigma\tau^{-1}\sigma^{-1}) = N^{\times}_{E/F}(\Upsilon_{L/E}(\tau\sigma\tau^{-1}\sigma^{-1})) = 1$$

for every $\sigma, \tau \in \mathrm{Gal}(L/F)$. To achieve that we use Lemma (3.2.5) and the induction hypothesis.

Suppose that the subgroup $\mathrm{Gal}(L/K)$ of $G = \mathrm{Gal}(L/F)$ generated by $\mathrm{Gal}(L/E)$ and τ is not equal to G. Then from the induction hypothesis and Lemma (3.2.5)

$$\Upsilon_{L/K}(\tau\sigma\tau^{-1}\sigma^{-1}) = \Upsilon_{L/K}(\tau)\Upsilon_{L/K}(\sigma\tau^{-1}\sigma^{-1}) = \Upsilon_{L/K}(\tau)^{1-\sigma},$$

and so

$$\Upsilon_{L/F}(\tau\sigma\tau^{-1}\sigma^{-1}) = N^{\times}_{K/F}\left(\Upsilon_{L/K}(\tau)^{1-\sigma}\right) = 1.$$

In the remaining case the image of τ generates $\mathrm{Gal}(E/F)$. Hence $\sigma = \tau^m\rho$ for some $\rho \in \mathrm{Gal}(L/E)$ and integer m. We deduce $\tau\sigma\tau^{-1}\sigma^{-1} = \tau^m(\tau\rho\tau^{-1}\rho^{-1})\tau^{-m}$ and similarly to the preceding

$$\Upsilon_{L/F}(\tau^m(\tau\rho\tau^{-1}\rho^{-1})\tau^{-m}) = \Upsilon_{L/F}(\tau\rho\tau^{-1}\rho^{-1}) = N^{\times}_{E/F}\left(\Upsilon_{L/E}(\rho)^{\tau-1}\right) = 1.$$

□

COROLLARY.

(1) *Let L/F be a finite Galois extension and let E/F be the maximal abelian subextension in L/F. Then $N_{L/F}L^{\times} = N_{E/F}E^{\times}$.*
(2) *Let L/F be a finite abelian extension, and M/F a subextension in L/F. Then $\alpha \in N_{L/M}L^{\times}$ if and only if $N_{M/F}\alpha \in N_{L/F}L^{\times}$.*

Proof. The first assertion follows immediately from the theorem. The second assertion follows the diagram of the corollary in (3.2.5) (with Frob being replaced with Gal) in which the homomorphism $N^{\times}_{M/F}$ is injective due to the theorem. □

(3.3.4). We now list functorial properties of the homomorphism $\Upsilon_{L/F}$. Immediately from the previous theorem and (3.2.5) we deduce the following

PROPOSITION.

(1) *Let M/F be a finite separable extension and let L/M be a finite Galois extension, $\sigma \in \mathrm{Gal}(F^{\mathrm{sep}}/F)$. Then the diagram*

$$\begin{array}{ccc} \mathrm{Gal}(L/M) & \xrightarrow{\Upsilon_{L/M}} & M^{\times}/N_{L/M}L^{\times} \\ {\scriptstyle \sigma^*}\downarrow & & \downarrow{\scriptstyle \sigma} \\ \mathrm{Gal}(\sigma L/\sigma M) & \xrightarrow{\Upsilon_{\sigma L/\sigma M}} & (\sigma M)^{\times}/N_{\sigma L/\sigma M}(\sigma L)^{\times} \end{array}$$

is commutative.

(2) *Let $M/F, E/L$ be finite separable extensions, and let L/F and E/M be finite Galois extensions. Then the diagram*

$$\begin{array}{ccc} \mathrm{Gal}(E/M) & \xrightarrow{\Upsilon_{E/M}} & M^{\times}/N_{E/M}E^{\times} \\ \downarrow & & \downarrow{\scriptstyle N^{\times}_{M/F}} \\ \mathrm{Gal}(L/F) & \xrightarrow{\Upsilon_{L/F}} & F^{\times}/N_{L/F}L^{\times} \end{array}$$

is commutative.

3.4. The Reciprocity Map

In this section we define and describe properties of the reciprocity map

$$\Psi_F: F^\times \longrightarrow \mathrm{Gal}(F^{\mathrm{ab}}/F)$$

using the Neukirch map $\Upsilon_{L/F}$ studied in the previous sections.

(3.4.1). The homomorphism inverse to $\Upsilon_{L/F}$ induces the surjective homomorphism

$$(\cdot\,, L/F): F^\times \longrightarrow \mathrm{Gal}(L/F)^{\mathrm{ab}}.$$

It coincides with $\Psi_{L/F}$ for totally ramified extensions.

Denote the maximal abelian extension of F in F^{sep} by F^{ab}.

PROPOSITION. *Let H be a subgroup in $\mathrm{Gal}(L/F)^{\mathrm{ab}}$, and let M be the fixed field of H in $L \cap F^{\mathrm{ab}}$. Then $(\cdot, L/F)^{-1}(H) = N_{M/F}M^\times$.*

Let L_1, L_2 be abelian extensions of finite degree over F, and let $L_3 = L_1L_2$, $L_4 = L_1 \cap L_2$. Then

$$N_{L_3/F}L_3^\times = N_{L_1/F}L_1^\times \cap N_{L_2/F}L_2^\times, \quad N_{L_4/F}L_4^\times = N_{L_1/F}L_1^\times\, N_{L_2/F}L_2^\times.$$

The field L_1 is a subfield of the field L_2 if and only if $N_{L_2/F}L_2^\times \subset N_{L_1/F}L_1^\times$; in particular, $L_1 = L_2$ if and only if $N_{L_1/F}L_1^\times = N_{L_2/F}L_2^\times$.

If a subgroup N in $F^\times$ contains a norm subgroup $N_{L/F}L^\times$ for some finite Galois extension L/F, then N itself is a norm subgroup.

Proof. The first assertion follows immediately from (3.3.3) and (3.3.4). Put $H_i = \mathrm{Gal}(L_3/L_i)$, $i = 1, 2$. Then

$$\begin{aligned} N_{L_3/F}L_3^\times &= (\cdot, L_3/F)^{-1}(1) = (\cdot, L_3/F)^{-1}(H_1 \cap H_2) \\ &= (\cdot, L_3/F)^{-1}(H_1) \cap (\cdot, L_3/F)^{-1}(H_2) = N_{L_1/F}L_1^\times \cap N_{L_2/F}L_2^\times, \\ N_{L_4/F}L_4^\times &= (\cdot, L_3/F)^{-1}(H_1H_2) = (\cdot, L_3/F)^{-1}(H_1)(\cdot, L_3/F)^{-1}(H_2) \\ &= N_{L_1/F}L_1^\times N_{L_2/F}L_2^\times. \end{aligned}$$

If $L_1 \subset L_2$, then $N_{L_2/F}L_2^\times \subset N_{L_1/F}L_1^\times$. Conversely, if $N_{L_2/F}L_2^\times \subset N_{L_1/F}L_1^\times$, then $N_{L_1L_2/F}(L_1L_2)^\times$ coincides with $N_{L_2/F}L_2^\times$, and Theorem (3.3.3) shows that the extension L_1L_2/F is of the same degree as L_2/F, hence $L_1 \subset L_2$.

Finally, if $N \supset N_{L/F}L^\times$, then $N = N_{M/F}M^\times$, where M is the fixed field of $(N, L/F)$. □

Passing to the projective limit, we get

$$\Psi_F: F^\times \longrightarrow \varprojlim F^\times/N_{L/F}L^\times \longrightarrow \varprojlim \mathrm{Gal}(L/F)^{\mathrm{ab}} = \mathrm{Gal}(F^{\mathrm{ab}}/F)$$

where L runs through all finite Galois (or all finite abelian) extensions of F. The homomorphism Ψ_F is called *the reciprocity map.*

(3.4.2). THEOREM. *The reciprocity map is well defined.*

Its image is dense in $\mathrm{Gal}(F^{\mathrm{ab}}/F)$*, and its kernel coincides with the intersection of all norm subgroups* $N_{L/F}L^{\times}$ *in* $F^{\times}$ *for finite Galois* (*or finite abelian*) *extensions* L/F.

If L/F *is a finite Galois extension and* $\alpha \in F^{\times}$*, then the automorphism* $\Psi_F(\alpha)$ *acts trivially on* $L \cap F^{\mathrm{ab}}$ *if and only if* $\alpha \in N_{L/F}L^{\times}$.

The restriction of $\Psi_F(\alpha)$ *on* F^{ur} *coincides with* $\varphi_F^{v_F(\alpha)}$ *for* $\alpha \in F^{\times}$.

Let L *be a finite separable extension of* F*, and let* σ *be an automorphism of* $\mathrm{Gal}(F^{\mathrm{sep}}/F)$. *Then the diagrams*

$$\begin{array}{ccc} L^{\times} & \xrightarrow{\Psi_L} & \mathrm{Gal}(L^{\mathrm{ab}}/L) \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma^*} \\ (\sigma L)^{\times} & \xrightarrow{\Psi_{\sigma L}} & \mathrm{Gal}\left((\sigma L)^{\mathrm{ab}}/\sigma L\right) \end{array}$$

$$\begin{array}{ccc} L^{\times} & \xrightarrow{\Psi_L} & \mathrm{Gal}(L^{\mathrm{ab}}/L) \\ \downarrow{\scriptstyle N_{L/F}} & & \downarrow \\ F^{\times} & \xrightarrow{\Psi_F} & \mathrm{Gal}\left(F^{\mathrm{ab}}/F\right) \end{array}$$

are commutative, where $\sigma^{\times}(\tau) = \sigma\tau\sigma^{-1}$*, the right vertical homomorphism of the second diagram is the restriction.*

Proof. Let $L_1/F, L_2/F$ be finite extensions and $L_1 \subset L_2$. Then Proposition (3.3.4) shows that the restriction of the automorphism

$$(\alpha, L_2/F) \in \mathrm{Gal}(L_2/F)^{\mathrm{ab}}$$

on the field $L_1 \cap F^{\mathrm{ab}}$ coincides with $(\alpha, L_1/F)$ for an element $\alpha \in F^{\times}$. This means that Ψ_F is well defined.

The condition $\alpha \in N_{L/F}L^{\times}$ is equivalent $(\alpha, L/F) = 1$ and the last relation means that $\Psi_F(\alpha)$ acts trivially on $L \cap F^{\mathrm{ab}}$.

Hence, the kernel of Ψ_F is equal to $\bigcap N_{L/F}L^{\times}$, where L runs through all finite Galois extensions of F. Since $\Psi_F(F^{\times})|_L = \mathrm{Gal}(L/F)$ for a finite abelian extension L/F, we deduce that $\Psi(F^{\times})$ is dense in $\mathrm{Gal}(F^{\mathrm{ab}}/F)$.

Theorem (3.2.4) shows that $\Psi_F(\pi_F)|_{F^{\mathrm{ur}}} = \varphi_F$ for a prime element π_F in F. Hence, $\Psi_F(\alpha)|_{F^{\mathrm{ur}}} = \varphi_F^{v_F(\alpha)}$ and $\Psi_F(U_F)|_{F^{\mathrm{ur}}} = 1$.

The commutativity of the diagrams follow from Propositions (3.3.4) and (3.3.5). □

3.5. The Existence Theorem

(3.5.1). PROPOSITION. *Let* L *be a finite separable extension of* F. *Then the norm map*

$$N_{L/F}\colon L^{\times} \to F^{\times}$$

is continuous and $N_{L/F}L^{\times}$ *is an open subgroup of finite index in* $F^{\times}$.

Proof. Let E/F be a finite Galois extension with $L \subset E$. Then, by Theorem (3.4.2), $N_{E/F}E^\times$ is of finite index in $F^\times$. The Galois group of the extension E/F is solvable. Therefore, in order to show that $N_{L/F}L^\times$ is open, it suffices to verify that the norm map for a cyclic extension of prime degree transforms open subgroups to open subgroups. This follows from the description of the behavior of the norm map in (2.13). The same description of the norm map implies that the pre-image $N^{-1}_{M/F}$ of an open subgroup is an open subgroup for a cyclic extension M/F. Therefore, the pre-image $N^{-1}_{E/F}$ of an open subgroup N in $F^\times$ is an open subgroup in $E^\times$. Since $N^{-1}_{L/F}(N) \supset N_{E/L}\big(N^{-1}_{E/F}(N)\big)$, we obtain that $N^{-1}_{L/F}(N)$ is open in $L^\times$ and $N_{L/F}$ is continuous. □

(3.5.2). THEOREM ("EXISTENCE THEOREM"). *There is a one-to-one correspondence between open subgroups of finite index in $F^\times$ and the norm subgroups of finite abelian extensions: $N \leftrightarrow N_{L/F}L^\times$. This correspondence is an order reversing bijection between the lattice of open subgroups of finite index in $F^\times$ (with respect to the intersection $N_1 \cap N_2$ and the product N_1N_2) and the lattice of finite abelian extensions of F (with respect to the intersection $L_1 \cap L_2$ and the compositum L_1L_2).*

Proof. We verify that an open subgroup N of finite index in $F^\times$ coincides with the norm subgroup $N_{L/F}L^\times$ of some finite abelian extension L/F. It suffices to verify that N contains the norm subgroup $N_{L/F}L^\times$ of some finite separable extension L/F. Indeed, in this case N contains $N_{E/F}E^\times$, where E/F is a finite Galois extension, $E \supset L$. Then by Proposition (3.4.1) we deduce that $N = N_{M/F}M^\times$, where M is the fixed field of $(N, E/F)$ and M/F is abelian.

Assume char$(F) \nmid n$, where n is the index of N in $F^\times$. If $\mu_n \subset F^\times$, then the Kummer theory implies that $F^{\times n} = N_{L/F}L^\times$ for the abelian extension L/F, where $L = F(\sqrt[n]{F})$. Since $F^{\times n}$ is of finite index in $F^\times$, the extension L/F is finite. Then $N_{L/F}L^\times \subset N$. If μ_n is not contained in $F^\times$, then put $F_1 = F(\mu_n)$. By the same arguments, $F_1^{\times n} = N_{L/F_1}L^\times$ for some finite abelian extension L/F_1. Then $N_{L/F}L^\times \subset F^{\times n} \subset N$.

Assume now that char$(F) = p$. We will show by induction on $m \geqslant 1$ that any open subgroup N of index p^m in $F^\times$ contains a norm subgroup. This is true for $m = 1$, as follows from the theory of Artin–Schreier extensions. Now let $m > 1$, and let N_1 be an open subgroup of index p^{m-1} in $F^\times$ such that $N \subset N_1$. By the induction assumption, $N_1 \supset N_{L_1/F}L_1^\times$. The subgroup $N \cap N_{L_1/F}L_1^\times$ is of index 1 or p in $N_{L_1/F}L_1^\times$. In the first case $N \supset N_{L_1/F}L_1^\times$, and in the second case let L/L_1 be a finite separable extension with $N^{-1}_{L_1/F}\left(N \cap N_{L_1/F}L_1^\times\right) \supset N_{L/L_1}L^\times$; then $N \supset N_{L/F}L^\times$.

For an open subgroup N of index np^m in $F^\times$ with $p \nmid n$ we now take open subgroups N_1 and N_2 of indices n and p^m, respectively, in $F^\times$ such that $N \subset N_1, N_2$. Then $N = N_1 \cap N_2 \supset N_{L_1/F}L_1^\times \cap N_{L_2/F}L_2^\times \supset N_{L_1L_2/F}(L_1L_2)^\times$ and we have proved the desired assertion for N.

Finally, Proposition (3.4.1) implies all remaining assertions. □

COROLLARY. *The reciprocity map Ψ_F is injective and continuous.*

Proof. By Theorem (3.4.2) the preimage $\Psi_F^{-1}(G)$ of an open subgroup G of the group $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ coincides with $N_{L/F}L^\times$, where L is the fixed field of G. Hence, $\Psi_F^{-1}(G)$ is

open and Ψ_F is continuous. Since the intersection of all norm subgroups coincides with the intersection of all open subgroups of finite index in $F^\times$, we conclude that Ψ_F is injective. □

REMARK. One may omit the word "open" in the Theorem if $\mathrm{char}(F) = 0$.

DEFINITION. The field L, which is an abelian extension of finite degree over F, with the property $N_{L/F}L^\times = N$ is called the *class field* of the subgroup $N \subset F^\times$.

(3.5.3). Now we will generalize Theorem (3.5.2) for abelian (not necessarily finite) extensions of F. For an abelian extension L/F, we put

$$N_{L/F}L^\times = \bigcap_M N_{M/F}M^\times,$$

where M runs through all finite subextensions of F in L. Then the norm subgroup $N_{L/F}L^\times$, as the intersection of closed subgroups, is closed in $F^\times$. Theorem (3.4.2) implies that $N_{L/F}L^\times = \bigcap_M \Psi_F^{-1}\big(\mathrm{Gal}(F^{\mathrm{ab}}/M)\big) = \Psi_F^{-1}\big(\mathrm{Gal}(F^{\mathrm{ab}}/L)\big)$. Moreover, for a closed subgroup N in $F^\times$ denote the topological closure of $\Psi_F(N)$ in $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ by $G_{(N)}$. In other words, $G_{(N)}$ coincides with the intersection of all open subgroups H in $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ with $H \supset \Psi_F(N)$. If an element $\alpha \in F^\times$ belongs to $\Psi_F^{-1}(G_{(N)})$, then the automorphism $\Psi_F(\alpha)$ acts trivially on the fixed field of an open subgroup H with $H \supset \Psi_F(N)$. From Theorem (3.4.2) we deduce that $\alpha \in \bigcap_M N_{M/F}M^\times$, where M corresponds to H. We conclude that $N = N_{L/F}L^\times$ for the fixed field L of $G_{(N)}$ (or of $\Psi_F(N)$).

THEOREM. *The correspondence $L \to N_{L/F}L^\times$ is an order reversing bijection between the lattice of abelian extensions of F and the lattice of closed subgroups in $F^\times$. The quotient group $F^\times/N_{L/F}L^\times$ is isomorphic to a dense subgroup in* $\mathrm{Gal}(L/F)$.

Proof. It remains to use the injectivity of Ψ_F and the arguments in the proof of Proposition (3.4.2) and Theorem (3.5.2) (replacing the word "open" by "closed"). □

(3.5.4). Let L/F be a finite abelian extension, and L_0 be the maximal unramified subextension of F in L. Theorem (3.4.2) shows that $\Psi_F(U_F)|_L \subset \mathrm{Gal}(L/L_0)$. Conversely, if $\sigma \in \mathrm{Gal}(L/L_0)$ and $\sigma = \Psi_F(\alpha)|_L$ for $\alpha \in F^\times$, then Theorem (3.4.2) implies that $v_F(\alpha) = 0$, i.e., $\alpha \in U_F$. Hence $\Psi_F(U_F)|_L = \mathrm{Gal}(L/L_0)$. The extension L^{ur}/F is abelian, and we similarly deduce that $\Psi_F(U_F)|_{L^{\mathrm{ur}}} = \mathrm{Gal}(L^{\mathrm{ur}}/F^{\mathrm{ur}})$. Since U_F is compact and Ψ_F is continuous, the group $\Psi_F(U_F)$ is closed and equal to $\mathrm{Gal}(F^{\mathrm{ab}}/F^{\mathrm{ur}})$.

Let π be a prime element in F and $\Psi_F(\pi) = \varphi$. Then $\varphi|_{F^{\mathrm{ur}}} = \varphi_F$, and for the fixed field F_π of φ we get

$$F_\pi \cap F^{\mathrm{ur}} = F, \quad F_\pi F^{\mathrm{ur}} = F^{\mathrm{ab}}$$

(the second equality can be deduced by the same arguments as in the proof of Proposition (3.2.1). The prime element π belongs to the norm group of every finite subextension L/F of F_π/F. The group $\mathrm{Gal}(F^{\mathrm{ab}}/F_\pi)$ is mapped isomorphically onto $\mathrm{Gal}(F^{\mathrm{ur}}/F)$ and the group $\mathrm{Gal}(F_\pi/F)$ is isomorphic $\mathrm{Gal}(F^{\mathrm{ab}}/F^{\mathrm{ur}})$. The latter group is often denoted by I_F and called the *inertia subgroup* of $G_F^{\mathrm{ab}} = \mathrm{Gal}(F^{\mathrm{ab}}/F)$.

We have

$$\mathrm{Gal}(F^{\mathrm{ab}}/F) \simeq \mathrm{Gal}(F_\pi/F) \times \mathrm{Gal}(F^{\mathrm{ur}}/F), \qquad \mathrm{Gal}(F_\pi/F) \simeq U_F, \mathrm{Gal}(F^{\mathrm{ur}}/F) \simeq \widehat{\mathbb{Z}}$$

and

$$\Psi_F(F^\times) = \langle\varphi\rangle \times \mathrm{Gal}(F^{\mathrm{ab}}/F^{\mathrm{ur}}),$$

where $\langle\varphi\rangle$ is the cyclic group generated by φ. We observe that the distinction between $F^\times$ and $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ is the same as that between $\mathbb{Z}$ and $\widehat{\mathbb{Z}}$. So if we define the group $\widehat{F}^\times$ as $\varprojlim F^\times/U$ where U runs over all open subgroups of finite index in $F^\times$, then $\widehat{F}^\times = U_F \times \widehat{\mathbb{Z}}$ and the reciprocity map Ψ_F extends to the isomorphism (and homeomorphism of topological spaces)

$$\widehat{\Psi}_F\colon \widehat{F}^\times \longrightarrow \mathrm{Gal}(F^{\mathrm{ab}}/F) = G_F^{\mathrm{ab}}.$$

Define

$$\Upsilon_F = \widehat{\Psi}_F^{-1}\colon \mathrm{Gal}(F^{\mathrm{ab}}/F) \longrightarrow \widehat{F}^\times.$$

Then Υ_F maps I_F homeomorphically onto U_F.

The field F_π can be explicitly generated by roots of iterated powers of the isogeny of a formal *Lubin–Tate group* associated to π.

3.6. Comments on other approaches to the local reciprocity map

(3.6.1). The approaches of Hazewinkel and Neukirch for local fields with finite residue field can be developed without using each other; but each of them has to go through some "unpleasant" lemmas.

In characteristic p there is a very elegant elementary approach by *Y. Kawada* and *I. Satake* which employs Artin–Schreier–Witt theory.

(3.6.2). The maximal abelian totally ramified extension of $\mathbb{Q}_p$ coincides with $\mathbb{Q}_p(\mu_{p^\infty})$ where μ_{p^∞} is the group of all roots of order a power of p. By using formal Lubin–Tate groups associated to a prime element π one can similarly construct the field F_π of (3.5.5). Due to explicit results on the extensions generated by roots of iterated powers of the isogeny of the formal group, one can develop an explicit class field theory for local fields with finite residue field. Disadvantage of this approach is that it is not apparently generalizable to local fields with infinite residue field.

(3.6.3). All other approaches prove and use the fact (or its equivalent) that for the *Brauer group* of a local field F there is a (canonical) isomorphism

$$\mathrm{inv}_F\colon \mathrm{Br}(F) \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

Historically this is the first approach due to *H. Hasse*.

Recall that the Brauer group of a field K is the group of equivalence classes of central simple algebras over K. A finite dimensional algebra A over K is called central simple if there exists a finite Galois extension L/K such that the algebra viewed over L isomorphic to a matrix algebra over L (in this case A is said to split over L). A central simple algebra A over K is isomorphic to $M_m(D)$ where D is a division algebra with centre K, $m \geqslant 1$. Two

central simple algebras A, A' are said to be equivalent if the associated division algebras are isomorphic over K. The group structure of $\mathrm{Br}(K)$ is given by the class of the tensor product of representatives.

A standard way to prove the assertion about $\mathrm{Br}(F)$ is the show that every central simple algebra over F splits over some finite unramified extension of F, and then using $\mathrm{Gal}(F^{\mathrm{ur}}/F) \simeq \mathrm{Gal}(\mathbb{F}_q^{\mathrm{sep}}/\mathbb{F}_q)$ reduce the calculation to the fact that the group of continuous characters $\mathrm{X}_{\mathbb{F}_q}$ of $G_{\mathbb{F}_q}$ is canonically (due to the canonical Frobenius automorphism) isomorphic with $\mathbb{Q}/\mathbb{Z}$.

Now let a character $\chi \in \mathrm{X}_F = \mathrm{Hom}_c(G_F, \mathbb{Q}/\mathbb{Z})$ correspond to a cyclic extension L/F of degree n with generator σ such that $\chi(\sigma) = 1/n$. For every element $\alpha \in F^\times$ there is a so called cyclic algebra $A_{\alpha,\chi}$ defined as $\oplus_{i=0}^{n-1} L\beta^i$ where $\beta^n = \alpha$, $a\beta = \beta \cdot \sigma(a)$ for every $a \in L$. We have a pairing

$$F^\times \times \mathrm{X}_F \longrightarrow \mathbb{Q}/\mathbb{Z}, \quad (\alpha, \chi) \mapsto \mathrm{inv}_F([A_{\alpha,\chi}]).$$

This pairing induces then a homomorphism

$$F^\times \longrightarrow \mathrm{Gal}(F^{\mathrm{ab}}/F) = \mathrm{Hom}(\mathrm{X}_F, \mathbb{Q}/\mathbb{Z}).$$

Then one proves that this homomorphism possesses all nice properties, i.e. establishes local class field theory.

The just described approach does not require cohomological tools and was known before the invention of those.

(3.6.4). Using cohomology groups one can perhaps simplify the proofs in the approach described in (3.6.3). From our point of view the exposition of class field theory for local fields with finite residue field given in this chapter is the most appropriate for a beginner; at a later stage the cohomological approach can be mastered. The real disadvantage of the cohomological approach is its unexplicitness whereas the approach in this chapter in addition to quite an explicit nature can be easily extended to many other situations.

If L is a finite Galois extension of F then one has an exact sequence

$$1 \to H^2(\mathrm{Gal}(L/F), L^\times) \to \mathrm{Br}(F) \to \mathrm{Br}(L) \to 1$$

and $\mathrm{Br}(F)$ is the union of classes of algebras which split over L (i.e. the image of all $H^2(\mathrm{Gal}(L/F), L^\times)$ for all finite Galois extensions L/F). So inv_F induces a canonical isomorphism

$$\mathrm{inv}_{L/F} \colon H^2(\mathrm{Gal}(L/F), L^\times) \xrightarrow{\sim} \frac{1}{|L:F|}\mathbb{Z}/\mathbb{Z}.$$

Denote the element which is mapped to $1/|L:F|$ by $u_{L/F}$. If $\widehat{H}^r$ stands for the modified *Tate's cohomology group*, then the cup product with $u_{L/F}$ induces an isomorphism

$$\widehat{H}^r(\mathrm{Gal}(L/F), \mathbb{Z}) \xrightarrow{\sim} \widehat{H}^{r+2}(\mathrm{Gal}(L/F), L^\times).$$

For $r = 0$ we have

$$\mathrm{Gal}(L/F)^{\mathrm{ab}} = \widehat{H}^0(\mathrm{Gal}(L/F), \mathbb{Z}) \xrightarrow{\sim} \widehat{H}^2(\mathrm{Gal}(L/F), L^\times) = F^\times/N_{L/F}L^\times$$

which leads to the analog of Theorems (3.3.3) and (3.4.2). Certainly the last isomorphism in much more explicit form is $\Upsilon^{\mathrm{ab}}_{L/F}$.

Using cohomology groups one can interpret the pairing $F^\times \times \mathrm{X}_F \longrightarrow \mathbb{Q}/\mathbb{Z}$ of the previous subsection as arising from the cup product

$$H^0(\mathrm{Gal}(L/F), L^\times) \times H^2(\mathrm{Gal}(L/F), \mathbb{Z}) \to H^2(\mathrm{Gal}(L/F), L^\times)$$

and the border homomorphism $H^1(\mathrm{Gal}(L/F), \mathbb{Q}/\mathbb{Z}) \to H^2(\mathrm{Gal}(L/F), \mathbb{Z})$ associated to the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0.$$

For a field K one can try to axiomatize those properties of its cohomology groups which are sufficient to get a reciprocity map from $K^\times$ to G_K^{ab}, as it is well known this leads to the notion of class formation.

(3.6.5). Assume that F is of characteristic zero with finite residue field of characteristic p. For $n \geqslant 1$ the p^n-component of the pairing $F^\times \times \mathrm{X}_F \longrightarrow \mathbb{Q}/\mathbb{Z}$ defined in (3.6.3) is a pairing

$$H^1(G_F, \mu_{p^n}) \times H^1(G_F, \mathbb{Z}/p^n\mathbb{Z}) \to H^2(G_F, \mu_{p^n}).$$

If for every n one knows that this pairing is a perfect pairing, and the right hand side is a cyclic group of order p^n, then one deduces the p-part of class field theory of the field F.

More generally, for a finitely generated $\mathbb{Z}_p$-module M equipped with the action of G_F and annihilated by p^n define $M^\times(1) = \mathrm{Hom}(M, \mu_{p^n})$. The previous pairing can be generalized to the pairing given by the cup product

$$H^i(G_F, M) \times H^{2-i}(G_F, M^\times(1)) \to H^2(G_F, \mu_{p^n}).$$

By *Tate local duality* it is a perfect pairing of finite groups. So, if one can establish Tate local duality independently of local class field theory, then one obtains another approach to the p-part of local class field theory in characteristic zero.

J.-M. Fontaine's theory of $\Phi - \Gamma$-modules was used by *L. Herr* to relate $H^i(G_F, M)$ with cohomology groups of a simple complex of $\Phi - \Gamma$-modules. Then Tate local duality can be established by working with the complex above and this provides another approach to the p-part of local class field theory.

Exercises

1. Go through the proof of (1.6).

2. Go through the proofs of (1.12).

3. Multiplicative Representatives.

Assume that $\mathrm{char}(\overline{F}) = p > 0$. Let $a \in \overline{F}$. An element $\alpha \in \mathcal{O}$ is said to be a *multiplicative representative* (*Teichmüller representative*) of a if $\overline{\alpha} = a$ and $\alpha \in \bigcap_{m \geqslant 0} F^{p^m}$. This definition is justified by the following Proposition.

PROPOSITION. *An element $a \in \overline{F}$ has a multiplicative representative if and only if $a \in \bigcap_{m \geqslant 0} \overline{F}^{p^m}$. A multiplicative representative for such a is unique. If a and b have the multiplicative representatives α and β, then $\alpha\beta$ is the multiplicative representative of ab.*

Proof. We need the following Lemma.

LEMMA. *Let $\alpha, \beta \in \mathcal{O}$ and $v(\alpha - \beta) \geqslant m$, $m > 0$. Then $v(\alpha^{p^n} - \beta^{p^n}) \geqslant n + m$.*

Proof. Put $\alpha = \beta + \pi^m\gamma$; then $\alpha^p = \beta^p + p\beta^{p-1}\pi^m\gamma + \cdots + p\beta(\pi^m\gamma)^{p-1} + \pi^{pm}\gamma^p$, and as $v(p) \geqslant 1$ (recall $\mathrm{char}(\overline{F}) = p$), we have $v(p\beta^{p-1}\pi^m\gamma) \geqslant m + 1, \ldots, v(\pi^{pm}\gamma^p) \geqslant m + 1$, and $\alpha^p - \beta^p \in \pi^{m+1}\mathcal{O}$. Now the required assertion follows by induction. □

To prove the first assertion of the Proposition, suppose that $a \in \bigcap_{m \geqslant 0} \overline{F}^{p^m}$. Since $\overline{F}$ has no nontrivial p-torsion, there exist unique elements $a_m \in \overline{F}$ satisfying the equations $a_m^{p^m} = a$. Let $\beta_m \in \mathcal{O}$ be such that $\overline{\beta}_m = a_m$. Then $\overline{\beta_{m+1}^p} = \overline{\beta}_m$ and $v(\beta_{m+1}^p - \beta_m) \geqslant 1$. The previous lemma implies $v(\beta_{m+1}^{p^{n+1}} - \beta_m^{p^n}) \geqslant n + 1$. Hence, the sequence $(\beta_m^{p^{m-n}})_{m \geqslant n}$ is fundamental. It has the limit $\alpha_n = \lim \beta_m^{p^{m-n}} \in \mathcal{O}$. We see that $\alpha_n^{p^n} = \alpha_0$ for $n \geqslant 0$ and $\overline{\alpha}_0 = a$, i.e., α_0 is a multiplicative representative of a. Conversely, if $a \in \overline{F}$ has a multiplicative representative α, then $\overline{\alpha} \in \bigcap_{m \geqslant 0} \overline{F}^{p^m}$.

Furthermore, if α and β are multiplicative representatives of $a \in \overline{F}$, then writing $\alpha = \alpha_m^{p^m}, \beta = \beta_m^{p^m}$ for some $\alpha_m, \beta_m \in \mathcal{O}$, we have $\overline{\alpha}_m^{p^m} = \overline{\beta}_m^{p^m}$ and $\overline{\alpha}_m = \overline{\beta}_m$ because of the injectivity of $\uparrow p^m$ in $\overline{F}$. Now the previous lemma implies $v(\alpha - \beta) \geqslant m + 1$, hence $\alpha = \beta$.

Finally, if α and β are the multiplicative representatives of a and b, then $\overline{\alpha\beta} = ab$ and $\alpha\beta \in \bigcap_{m \geqslant 0} F^{p^m}$. Therefore, $\alpha\beta$ is the multiplicative representative of ab. □

Denote the set of multiplicative representatives in $\mathcal{O}$ by $\mathcal{R}$.

COROLLARY 1. *If $\overline{F}$ is perfect* (*i.e. F is a local field*) *then every element of $\overline{F}$ has its multiplicative representative in $\mathcal{R}$. The map $r\colon \overline{F} \to \mathcal{R}$ induces an isomorphism $\overline{F}^{\times} \xrightarrow{\sim} \mathcal{R} \setminus \{0\}$. The correspondence $r\colon \overline{F} \to \mathcal{R}$ is called the Teichmüller map.*

If $\overline{F}$ is finite then $\mathcal{R} \setminus \{0\}$ is a cyclic group of order equal to $|\overline{F}| - 1$.

COROLLARY 2. *Let* $\operatorname{char}(F) = p$. *If α, β are the multiplicative representatives of $a, b \in \overline{F}$, then $\alpha + \beta$ is the multiplicative representative of $a + b$.*

Proof. Let $\alpha = \alpha_m^{p^m}, \beta = \beta_m^{p^m}$. Then $\alpha + \beta = (\alpha_m + \beta_m)^{p^m}$, hence $\alpha + \beta \in \bigcap_{m \geqslant 0} F^{p^m}$ and $\overline{\alpha + \beta} = a + b$. □

4. Go through the proof of (2.9) and (2.10).

5. Go through (2.11).

6. Go through the proofs of (2.12).

7. Structure theorems for complete discrete valuation fields. Let F be a complete discrete valuation field with perfect residue field.

There are three possible cases: two equal-characteristic cases, when $\operatorname{char}(F) = \operatorname{char}(\overline{F}) = 0$ or $\operatorname{char}(F) = \operatorname{char}(\overline{F}) = p > 0$, and one mixed-characteristic case, when $\operatorname{char}(F) = 0, \operatorname{char}(\overline{F}) = p > 0$.

LEMMA 1. *The ring of integers $\mathcal{O}_F$ contains a nontrivial field M if and only if* $\operatorname{char}(F) = \operatorname{char}(\overline{F})$.

Proof. Since $M \cap \mathcal{M}_F = (0)$, M is mapped isomorphically onto the field $\overline{M} \subset \overline{F}$, therefore $\operatorname{char}(F) = \operatorname{char}(\overline{F})$. Conversely, let A be the subring in $\mathcal{O}_F$ generated by 1. Then A is a field if $\operatorname{char}(F) = p$, and $A \cap \mathcal{M}_F = (0)$ if $\operatorname{char}(\overline{F}) = 0$. Hence, the quotient field of A is the desired one. □

A field $M \subset \mathcal{O}_F$, that is mapped isomorphically onto the residue field $\overline{F} = \overline{M}$ is called a *coefficient field* in $\mathcal{O}_F$. Such a field, if it exists, is a set of representatives of $\overline{F}$ in $\mathcal{O}_F$. (1.8) implies that in this case F is isomorphic (algebraically and topologically) to the field $M((X))$: a prime element π in F corresponds to X. Note that this isomorphism depends on the choice of a coefficient field (which is sometimes unique, see Proposition 2 below) and the choice of a prime element of F.

We shall show below that a coefficient field exists in an equal-characteristic case.

The simplest case is that of $\operatorname{char}(F) = \operatorname{char}(\overline{F}) = 0$.

PROPOSITION 1. *Let* $\operatorname{char}(\overline{F}) = 0$. *Then there exists a coefficient field in $\mathcal{O}_F$. A coefficient field can be selected in infinitely many ways if and only if $\overline{F}$ is not algebraic over $\mathbb{Q}$.*

Proof. Let M be a maximal subfield in $\mathcal{O}_F$, in other words, M be not contained in any other larger subfield of $\mathcal{O}_F$. We assert that $\overline{M} = \overline{F}$, i.e., M is a coefficient field. Indeed, if $\theta \in \overline{F}$ is algebraic over $\overline{M}$, then θ is separable over $\overline{M}$ and we can apply the Henselian property to find an element $\alpha \in \mathcal{O}_F$ which is algebraic over M and such that $\overline{\alpha} = \theta$. Since $M(\alpha) = M$, by the maximality of M, we get $\alpha \in M, \theta \in \overline{M}$. Furthermore, let $\theta \in \overline{F}$ be transcendental over $\overline{M}$.

Let $\alpha \in \mathcal{O}_F$ be such that $\overline{\alpha} = \theta$. Then α is not algebraic over M, because if $\sum_{i=0}^{n} a_i \alpha^i = 0$ with $a_i \in M$, then $\sum_{i=0}^{n} \overline{a}_i \theta^i = 0$. Hence, $\overline{a}_i = 0$ and $a_i = 0$ (M is mapped isomorphically onto $\overline{M}$). By the same reason $M[\alpha] \cap \mathcal{M} = (0)$. Hence, the quotient field $M(\alpha)$ is contained in $\mathcal{O}_F$ and $M \neq M(\alpha)$, contradiction. Thus, we have been convinced ourselves in the existence of a coefficient field.

If $\overline{F}$ is not algebraic over $\mathbb{Q}$, let $\alpha \in \mathcal{O}_F$ be an element transcendental over the prime subfield $\mathbb{Q}$ in $\mathcal{O}_F$. Then the maximal subfield in $\mathcal{O}_F$, which contains $\mathbb{Q}(\alpha + a\varepsilon)$ with $\varepsilon \in \mathcal{M}_F, a \in \mathbb{Q}$, is a coefficient field. If $\overline{F}$ is algebraic over $\mathbb{Q}$, then M is algebraic over $\mathbb{Q}$ and is uniquely determined by our previous constructions. □

PROPOSITION 2. *Let* $\mathrm{char}(F) = p$. *Then a coefficient field exists and is unique*; *it coincides with the set of multiplicative representatives of* $\overline{F}$ *in* $\mathcal{O}_F$.

Proof. Convince yourself. □

We conclude with the case of mixed-characteristic: $\mathrm{char}(F) = 0$, $\mathrm{char}(\overline{F}) = p$. with the residue field $\overline{F}$ isomorphic to K. Here is an analog:

PROPOSITION 3. *Let* F *be a complete discrete valuation field of characteristic 0 with residue field* K *of characteristic* p. *Let* K_1 *be any extension of* K. *Then there exists a complete discrete valuation field* F_1 *which is an extension of* F, *such that* $e(F_1|F) = 1$ *and* $\overline{F}_1 = K_1$.

Proof. It is suffices to consider two cases: $K_1 = K(a)$ is an algebraic extension over K and $K_1 = K(y)$ is a transcendental extension over K. If, in addition, in the first case K_1/K is separable, then let $g(X)$ be the monic irreducible polynomial of a over K, and let $f(X)$ be a monic polynomial over the ring of integers of K such that $\overline{f}(X) = g(X)$. By the Hensel Lemma (1.2) there exists a root α of $f(X)$ such that $\overline{\alpha} = a$. Then $F_1 = F(\alpha)$ is the desired extension of F. Next, if $a^p = b \in K$ and β is an element in the ring of integers of F such that $\overline{\beta} = b$, then $F_1 = F(\alpha)$ is the desired extension of F for $\alpha^p = \beta$. Finally, in the case of transcendental extension let w be defined as $w(f(y)) = \min_{m \leqslant i \leqslant k} v(\alpha_i)$ for $f(y) = \sum_{i=m}^{k} \alpha_i y^i \in F[y]$ with $\alpha_m \neq 0$, $m \leqslant k$. Extending w to $F(y)$ we obtain the discrete valuation w with residue field K_1. □

COROLLARY. *There exists a complete discrete valuation field of characteristic 0 with any given residue field of characteristic* p *and the absolute index of ramification is equal to 1.*

Proof. One can set $F = \mathbb{Q}_p$ and apply the Proposition. □

8. Hasse–Herbrand function. Let F be a complete discrete valuation field with perfect residue field.

PROPOSITION. *Let the residue field* $\overline{F}$ *be infinite. Let* L/F *be a finite Galois extension,* $N = N_{L/F}$. *Then there exists a unique function*

$$h = h_{L/F} \colon \mathbb{N} \to \mathbb{N}$$

such that $h(0) = 0$ *and*

$$NU_{h(i),L} \subset U_{i,F}, \quad NU_{h(i),L} \not\subset U_{i+1,F}, \quad NU_{h(i)+1,L} \subset U_{i+1,F}.$$

Proof. The uniqueness of h follows immediately. Indeed, for $j > h(i)$ $NU_{j,L} \subset U_{i+1,F}$, hence if $\widetilde{h}$ is another function with the required properties, then $\widetilde{h}(i) \leqslant h(i), h(i) \leqslant \widetilde{h}(i)$, i.e., $h = \widetilde{h}$.

As for the existence of h, we first consider the case of an unramified extension L/F. (2.12) shows that in this case $h(i) = i$ (because $N_{\overline{L}/\overline{F}}(\overline{L}^{\times}) \neq 1$ and $\mathrm{Tr}_{\overline{L}/\overline{F}}\,\overline{L} = \overline{F}$).

The next case to consider is a totally ramified cyclic extension L/F of prime degree. In this case the map $N_{L/F}$ is determined by some nonzero polynomials over $\overline{L}$. The image of $\overline{L}$ under the action of such a polynomial is not zero since $\overline{L}$ is infinite. Hence, we obtain

$$h(i) = |L : F|i,$$

if L/F is totally tamely ramified, and

$$h(i) = \begin{cases} i, & i \leqslant s, \\ s(1-p) + pi, & i \geqslant s, \end{cases}$$

if L/F is totally ramified of degree $p = \mathrm{char}(\overline{F}) > 0$.

Now we consider the general case. Note that if we have the functions $h_{L/M}$ and $h_{M/F}$ for the Galois extensions $L/M, M/F$, then for the extension L/F one can put $h_{L/F} = h_{L/M} \circ h_{M/F}$. Indeed,

$$N_{L/F}U_{h_{L/F}(i),L} \subset N_{M/F}U_{h_{M/F}(i),M} \subset U_{i,F}.$$

Furthermore, the behavior of $N_{L/F}$ is determined by some nonzero polynomials (the composition of the polynomials for $N_{L/M}$ and $N_{M/F}$, the existence of which can be assumed by induction). Hence

$$N_{L/F}U_{h_{L/F}(i),L} \not\subset U_{i+1,F}.$$

Since

$$N_{L/F}U_{h_{L/F}(i)+1,L} \subset N_{M/F}U_{h_{M/F}(i)+1,M} \subset U_{i+1,M},$$

we deduce that $h = h_{L/F}$ is the desired function.

In the general case we put $h_{L/F} = h_{L/L_0}$ for $L_0 = L \cap F^{\mathrm{ur}}$ and determine h_{L/L_0} by induction using solvability of L/L_0. □

To treat the case of finite residue fields we need

LEMMA. *Let L/F be a finite separable totally ramified extension. Then for an element $\alpha \in L$ we get*

$$N_{L/F}(\alpha) = N_{\widehat{L^{\mathrm{ur}}}/\widehat{F^{\mathrm{ur}}}}(\alpha)$$

where $\widehat{F^{\mathrm{ur}}}$ is the completion of F^{ur}, $\widehat{L^{\mathrm{ur}}} = L\widehat{F^{\mathrm{ur}}}$.

Proof. Let $L = F(\pi_L)$ with a prime element π_L in L, and let $\alpha \in L$. Let

$$\alpha\pi_L^i = \sum_{j=0}^{n-1} c_{ij}\pi_L^j \quad \text{with } c_{ij} \in F, 0 \leqslant i \leqslant n-1, n = |L : F|.$$

Then $N_{L/F}(\alpha) = \det(c_{ij})$. Since $L^{\mathrm{ur}} = F^{\mathrm{ur}}(\pi_L)$ and

$$|L^{\mathrm{ur}} : F^{\mathrm{ur}}| = e(L^{\mathrm{ur}}|F^{\mathrm{ur}}) = e(L^{\mathrm{ur}}|F) = e(L|F) = |L : F|,$$

we get

$$N_{L^{\mathrm{ur}}/F^{\mathrm{ur}}}(\alpha) = \det(c_{ij}) = N_{L/F}(\alpha).$$

Finally, let E/F^{ur} be a finite totally ramified Galois extension with $E \supset L^{\mathrm{ur}}$. Let $G = \mathrm{Gal}(E/F^{\mathrm{ur}})$, $H = \mathrm{Gal}(E/L^{\mathrm{ur}})$, and let G be the disjoint union of $\sigma_i H$ with $\sigma_i \in G, 1 \leqslant i \leqslant |L^{\mathrm{ur}} : F^{\mathrm{ur}}|$. Then

$$N_{L^{\mathrm{ur}}/F^{\mathrm{ur}}}(\alpha) = \prod \sigma_i(\alpha) = N_{\widehat{L^{\mathrm{ur}}}/\widehat{F^{\mathrm{ur}}}}(\alpha),$$

because G and H are isomorphic to $\mathrm{Gal}(\widehat{E}/\widehat{F^{\mathrm{ur}}})$ and $\mathrm{Gal}(\widehat{E}/\widehat{L^{\mathrm{ur}}})$. □

This Lemma shows that for a finite totally ramified Galois extension L/F the functions $h_{L/F}$ and $h_{\widehat{L^{\mathrm{ur}}}/\widehat{F^{\mathrm{ur}}}}$ coincide. Now, if L/F is a finite Galois extension, we put

$$h_{L/F} = h_{L/L_0} = h_{\widehat{L^{\mathrm{ur}}}/\widehat{F^{\mathrm{ur}}}}.$$

In particular, if $\overline{F}$ is finite we put $h_{L/F} = h_{\widehat{L^{\mathrm{ur}}}/\widehat{F^{\mathrm{ur}}}}$ (the residue field of $\widehat{F^{\mathrm{ur}}}$ is infinite as the separable closure of a finite field).

It is useful to extend this function to real numbers. For unramified extension, or tamely totally ramified extension of prime degree, or totally ramified extension of degree $p = \mathrm{char}(\overline{F}) > 0$ put

$$h_{L/F}(x) = x, \quad h_{L/F}(x) = |L : F|x, \quad h_{L/F}(x) = \begin{cases} x, & x \leqslant s, \\ s(1-p) + px, & x \geqslant s \end{cases}$$

for real $x \geqslant 0$ respectively. Using the solvability of L/L_0 (Corollary 3 of (4.4) Ch. II) and the equality $h_{L/F} = h_{L/M} \circ h_{M/F}$ define now $h_{L/F}(x)$ as the composite of the functions for a tower of cyclic subextensions in L/L_0.

THEOREM. *Thus defined function $h_{L/F}: [0, +\infty) \to [0, +\infty)$ is independent on the choice of a tower of subfields. The function $h_{L/F}$ is called the Hasse–Herbrand function of L/F. It is piecewise linear, continuous and increasing.*

Proof. It suffices to show that if M_1/M, M_2/M are cyclic extensions of prime degree, then

$$(*) \qquad h_{E/M_1} \circ h_{M_1/M} = h_{E/M_2} \circ h_{M_2/M}$$

where $E = M_1 M_2$.

Note that each of $h_{M_1/M}(x)$, $h_{M_2/M}(x)$ has at most one point at which its derivate is not continuous. Therefore there are at most two points at which the function of the left (resp. right) hand side of $(*)$ has discontinuous derivative. By looking at graphs of the functions it is obvious that at such points the derivative strictly increases and there is at most one such noninteger point for at most one of the composed functions of the left hand side and the right hand side of $(*)$. At this point (if it exists) the derivative jumps from p to p^2.

From the uniqueness in the preceding proposition we deduce that the left and right hand sides of $(*)$ are equal at all nonnegative integers. Thus, elementary calculus shows that the left and right hand sides of $(*)$ are equal at all nonnegative real numbers. □

9. Selfduality of local fields with finite residue field. Let F be a local field with finite residue field. Prove that there is a nontrivial character $\psi: F \to \mathbb{C}^\times$ and that every character ψ' of F is of the form $x \mapsto \psi(ax)$ for a uniquely defined $a \in F$. This means that the additive group of F is selfdual. It is one of the first observations which lead to the theory of *J. Tate* and *K. Iwasawa* on harmonic analysis interpretation of the zeta function.

[Hint: For a local functional field $\mathbb{F}_q((X))$ let $m: \mathbb{F}_p \to \mathbb{Z}/p \to \mathbb{C}^\times$ be induced by $a + p\mathbb{Z} \to \exp(2\pi i a/p)$, define

$$\psi: \sum a_i X^i \to m\left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} a_{-1}\right).$$

For $\alpha \in \mathbb{Q}_p^\times$ let $r(\alpha) \in \mathbb{Z}$ be such that $r(\alpha) \equiv \alpha p^n \mod p^n$ where $n = -v_p(\alpha)$. Define

$$\psi_{\mathbb{Q}_p}: \alpha \to \exp(2\pi i r(\alpha)/p^n).$$

For a local number field F define

$$\psi = \psi_{\mathbb{Q}_p} \circ \mathrm{Tr}_{F/\mathbb{Q}_p}.$$

To show the second part for a charater ψ' find a as $\sum \theta_i \pi^i$ constructing θ_i step by step.]

10. Go through details of (3.3.3).

11. Go through details of (3.4).

12. Go through details of (3.5).

13. The reciprocity map and Hasse–Arf theorem.

THEOREM. *Let L/F be a finite abelian extension, $G = \mathrm{Gal}(L/F)$. Denote by h the Hasse–Herbrand function $h_{L/F}$. Put $U_{-1,F} = F^\times$, $U_{0,F} = U_F$, and $h(-1) = -1$. Then for every integer $n \geqslant -1$ the reciprocity map $\Psi_{L/F}$ maps the quotient group $U_{n,F}N_{L/F}L^\times/N_{L/F}L^\times$ isomorphically onto the ramification group $G(n) = G_{h(n)}$ and $U_{n,F}N_{L/F}L^\times/U_{n+1,F}N_{L/F}L^\times$ isomorphically onto $G_{h(n)}/G_{h(n)+1}$.*

Thus $G_{h(n)+1} = G_{h(n+1)}$ for integer n; this is called the Hasse–Arf theorem.

Proof. Let L_0 be the maximal unramified extension of F in L. We know from Exercise 8 that $h_{L/F} = h_{L/L_0}$, and from section 1 that the norm $N_{L_0/F}$ maps U_{n,L_0} onto $U_{n,F}$ for $n \geqslant 0$. Using the second commutative diagram of (3.4.2) (for $E = L, M = F, L = L_0$) we can therefore assume that L/F is totally ramified and $n \geqslant 0$.

We use the notations of Corollary (3.3.2), so $\mathcal{F}$ and $\mathcal{L}$ are complete fields. Let $\sigma \in G_{h(n)}$, then $\pi^{1-\sigma}$ belongs to $U_{h(n),L}$. Let $\eta \in \mathcal{L}^\times$ be such that $\eta^{\varphi-1} = \pi^{1-\sigma}$. The first proposition of (3.1.8) shows that η can be chosen in $U_{h(n),\mathcal{L}}$. Now from Corollary (3.3.2) and the previous Exercise we deduce that $\Upsilon_{L/F}(\sigma) = \varepsilon = N_{\mathcal{L}/\mathcal{F}}(\eta)$ belongs to $U_{n,F}N_{L/F}L^\times$. So $\Upsilon(G_{h(n)}) \subset U_{n,F}N_{L/F}L^\times$. Similarly, we establish that $\Upsilon(G_{h(n)+1}) \subset U_{n+1,F}N_{L/F}L^\times$.

Conversely, let ε belong to $U_{n,F}N_{L/F}L^\times$. For the abelian extension L/F we will prove below a stronger assertion than that in Corollary (3.3.2):

> there exists $\eta \in U_{\mathcal{L}}$ such that $\varepsilon \equiv N_{\mathcal{L}/\mathcal{F}}(\eta) \mod N_{L/F}L^\times$ and $\eta^{\varphi-1} = \pi^{1-\sigma}$ for some $\sigma \in \mathrm{Gal}(\mathcal{L}/\mathcal{F})$. For every such η we have $\eta^{\varphi-1} \in U_{h(n),\mathcal{L}}$.

From this assertion we deduce that $\Psi(U_{n,F}N_{L/F}L^\times) \subset G_{h(n)}$. Hence $\Psi(U_{n,F}N_{L/F}L^\times) = G_{h(n)}$ and $\Upsilon_{L/F}(G_{h(n)+1}) = \Upsilon_{L/F}(G_{h(n+1)})$, so $G_{h(n)+1} = G_{h(n+1)}$.

It remains to prove the assertion by induction on the degree of L/F. If $n = 0$, the assertion is obvious, so we assume that $n > 0$. If $\mathrm{Gal}(L/F)$ is of prime order with generator τ, then from Corollary (3.3.2) we know that there is $\eta \in U_{\mathcal{L}}$ such that $\varepsilon \equiv N_{\mathcal{L}/\mathcal{F}}(\eta) \mod N_{L/F}L^{\times}$ and $\eta^{\varphi-1} = \pi^{1-\tau^m}$ for some integer m. So $j = v_{\mathcal{L}}(\eta^{\varphi-1} - 1) = v_{\mathcal{L}}(\pi^{1-\tau^m} - 1)$. If $\tau^m = 1$ then the assertion is obvious, so assume that $\tau^m \neq 1$. From (2.12) we know that $U_{j+1,F} \subset N_{L/F}L^{\times}$. If $N_{\mathcal{L}/\mathcal{F}}(\eta)$ belongs to $U_{j+1,F}$, then $\Psi_{L/F}(N_{\mathcal{L}/\mathcal{F}}(\eta))$ is 1, not τ^m, a contradiction. Therefore, $v_F(N_{\mathcal{L}/\mathcal{F}}(\eta) - 1) = j = h_{L/F}(j)$.

For the induction step let M/F be a subextension of L/F such that $\mathrm{Gal}(L/M)$ is of prime degree l with generator τ. By Corollary (3.3.2) there is $\eta \in U_{\mathcal{L}}$ such that $\varepsilon \equiv N_{\mathcal{L}/\mathcal{F}}(\eta) \mod N_{L/F}L^{\times}$ and $\eta^{\varphi-1} = \pi^{1-\sigma}$. By the induction hypothesis $N_{\mathcal{L}/\mathcal{M}}\eta^{\varphi-1}$ belongs to $U_{h_{M/F}(n),\mathcal{M}}$. By the first proposition of (3.1.8) the latter group is $^{\varphi-1}$-divisible, and therefore from the same proposition we deduce that $N_{\mathcal{L}/\mathcal{M}}\eta^{\varphi-1} = \rho u$ with $\rho \in U_{h_{M/F}(n),\mathcal{M}}$ and $u \in U_M$. According to the definition of the Hasse–Herbrand function in Exercise 8 there is $\xi \in U_{h_{L/F}(n),\mathcal{L}}$ such that $N_{\mathcal{L}/\mathcal{M}}(\xi) = \rho$. Then $\xi^{\varphi-1} = \pi^{1-\sigma}\alpha$ for some α in the kernel of $N_{\mathcal{L}/\mathcal{M}}$.

Let τ be a generator of $\mathrm{Gal}(L/M)$. Using Proposition (3.1.7) we deduce that $\alpha \equiv \pi^{1-\tau^m} \mod U(\mathcal{L}/\mathcal{M})$ and so $\xi^{\varphi-1} = \pi^{1-\sigma\tau^m}\gamma^{1-\tau}$ for an appropriate $\gamma \in U_{\mathcal{L}}$ and some integer m. By the first proposition of (3.1.8) there is $\delta \in U_{\mathcal{L}}$ such that $\delta^{\varphi-1} = \gamma^{1-\tau}$. Then $\eta^{\varphi-1} = \pi^{\sigma\tau^m-1}$ where $\eta = \xi\delta^{-1}$. All we need to show is that $\gamma^{\tau-1}$ belongs to $U_{h(n),\mathcal{L}}$. If it does not, then $j = v_{\mathcal{L}}(\gamma^{\tau-1} - 1) = v_L(\pi^{1-\sigma\tau^m} - 1) > 0$. Let $s = s(L|M)$ as defined in (2.12). Since γ is a unit, from (2.12) we deduce that $j - s$ is prime to p. On the other hand, the following Lemma implies that j is congruent to s modulo p, a contradiction. □

LEMMA. *Let L/F be a finite Galois extension with separable residue field extension. Let $\sigma \in G_i \setminus G_{i+1}$ and $\tau \in G_j \setminus G_{j+1}$ with $i, j \geqslant 1$. Then $\sigma\tau\sigma^{-1}\tau^{-1} \in G_{i+j+1}$ and $i \equiv j$ mod p.*

Proof. Let π_L be a prime element of L. Then

$$\frac{\sigma\pi_L}{\pi_L} = 1 + \alpha\pi_L^i, \quad \frac{\tau\pi_L}{\pi_L} = 1 + \beta\pi_L^j \qquad \text{with } \alpha, \beta \in \mathcal{O}_L^{\times}.$$

Therefore

$$\begin{aligned}\sigma\tau\pi_L &= \sigma\pi_L + (\sigma\beta)(\sigma\pi_L)^{j+1} \\ &\equiv \pi_L + \alpha\pi_L^{i+1} + \beta\pi_L^{j+1} + (j+1)\alpha\beta\pi_L^{i+j+1} \mod \mathcal{M}_L^{i+j+2}.\end{aligned}$$

Hence $(\sigma\tau - \tau\sigma)\pi_L \equiv (j-i)\alpha\beta\pi_L^{i+j+1} \mod \mathcal{M}_L^{i+j+2}$. Substituting instead of π_L the other prime element $\sigma^{-1}\tau^{-1}\pi_L$ of L we deduce that

$$\frac{\sigma\tau\sigma^{-1}\tau^{-1}\pi_L}{\pi_L} \equiv 1 + (j-i)\alpha\beta\pi_L^{i+j} \mod \mathcal{M}_L^{i+j+1}.$$

Now if j is the maximal ramification number of L/F, then $G_{j+1} = \{1\}$. Therefore the last formula in the previous paragraph shows that every positive ramification number i of L/F is congruent to j modulo p. Therefore every two positive ramification number of L/F are congruent to each other modulo p. Finally, from the same formula we deduce that $\sigma\tau\sigma^{-1}\tau^{-1} \in G_{i+j+1}$. □

14. The Hilbert symbol. Let F be a local field with finite residue field $\overline{F}$. Let the group μ_n of all nth roots of unity in the separable closure F^{sep} be contained in F and let $p \nmid n$ if $\text{char}(F) = p$.

The *norm residue symbol* or *Hilbert symbol* or *Hilbert pairing* $(\cdot,\cdot)_n : F^\times \times F^\times \to \mu_n$ is defined by the formula

$$(\alpha,\beta)_n = \gamma^{-1}\Psi_F(\alpha)(\gamma), \quad \text{where } \gamma^n = \beta, \gamma \in F^{\text{sep}}.$$

If $\gamma' \in F^{\text{sep}}$ is another element with $\gamma'^n = \beta$, then $\gamma^{-1}\gamma' \in \mu_n$ and

$$\gamma'^{-1}\Psi_F(\alpha)(\gamma') = \gamma^{-1}\Psi_F(\alpha)(\gamma).$$

Hence the Hilbert symbol is well defined.

PROPOSITION 1. *The norm residue symbol possesses the following properties:*

(1) $(\cdot,\cdot)_n$ *is bilinear*;
(2) $(1-\alpha,\alpha)_n = 1$ *for* $\alpha \in F^\times, \alpha \neq 1$ (*Steinberg property*);
(3) $(-\alpha,\alpha)_n = 1$ *for* $\alpha \in F^\times$;
(4) $(\alpha,\beta)_n = (\beta,\alpha)_n^{-1}$;
(5) $(\alpha,\beta)_n = 1$ *if and only if* $\alpha \in N_{F(\sqrt[n]{\beta})/F} F(\sqrt[n]{\beta})^\times$ *and if and only if* $\beta \in N_{F(\sqrt[n]{\alpha})/F} F(\sqrt[n]{\alpha})^\times$;
(6) $(\alpha,\beta)_n = 1$ *for all* $\beta \in F^\times$ *if and only if* $\alpha \in F^{\times n}$,
$(\alpha,\beta)_n = 1$ *for all* $\alpha \in F^\times$ *if and only if* $\beta \in F^{\times n}$;
(7) $(\alpha,\beta)_{nm}^m = (\alpha,\beta)_n$ *for* $m \geqslant 1, \mu_{nm} \subset F^\times$;
(8) $(\alpha,\beta)_{n,L} = (N_{L/F}\alpha,\beta)_{n,F}$ *for* $\alpha \in L^\times, \beta \in F^\times$, *where* $(\cdot,\cdot)_{n,L}$ *is the Hilbert symbol in* L, $(\cdot,\cdot)_{n,F}$ *is the Hilbert symbol in* F, *and* L *is a finite separable extension of* F;
(9) $(\sigma\alpha,\sigma\beta)_{n,\sigma L} = \sigma(\alpha,\beta)_{n,L}$, *where* L/F *is finite separable,* $\sigma \in \text{Gal}(F^{\text{sep}}/F)$, *and* $\mu_n \subset L^\times$ *but not necessarily* $\mu_n \subset F^\times$.

Proof. (1): For $\gamma \in F^{\text{sep}}, \gamma^n = \beta$ we get

$$\begin{aligned}\gamma^{-1}\Psi_F(\alpha_1\alpha_2)(\gamma) &= \Psi_F(\alpha_1)\big(\gamma^{-1}\Psi_F(\alpha_2)(\gamma)\big)\cdot\big(\gamma^{-1}\Psi_F(\alpha_1)(\gamma)\big)\\ &= \big(\gamma^{-1}\Psi_F(\alpha_2)(\gamma)\big)\big(\gamma^{-1}\Psi_F(\alpha_1)(\gamma)\big),\end{aligned}$$

since $\Psi_F(\alpha_1)$ acts trivially on $(\alpha_2,\beta)_n \in \mu_n$. We also obtain

$$\begin{aligned}(\alpha,\beta_1\beta_2)_n &= \big(\gamma_1^{-1}\gamma_2^{-1}\Psi_F(\alpha)(\gamma_1\gamma_2)\big) = \big(\gamma_1^{-1}\Psi_F(\alpha)(\gamma_1)\big)\big(\gamma_2^{-1}\Psi_F(\alpha)(\gamma_2)\big)\\ &= (\alpha,\beta_1)_n(\alpha,\beta_2)_n.\end{aligned}$$

for $\gamma_1,\gamma_2 \in F^{\text{sep}}$, $\gamma_1^n = \beta_1, \gamma_2^n = \beta_2$.
(5),(2),(3),(4): $(\alpha,\beta)_n = 1$ if and only if $\Psi_F(\alpha)$ acts trivially on $F(\sqrt[n]{\beta})$ and if and only if $\big($by Theorem (3.4.2)$\big)$ $\alpha \in N_{F(\sqrt[n]{\beta})/F} F(\sqrt[n]{\beta}))^\times$.

Let $m|n$ be the maximal integer for which $\alpha \in F^{\times m}$. Then $F(\sqrt[n]{\alpha})/F$ is of degree nm^{-1}. Let $\alpha = \alpha_1^m$ with $\alpha_1 \in F^\times$ and let ζ_n be a primitive nth root of unity. Then for

$\delta \in F^{\text{sep}}, \delta^n = \alpha$, we get

$$1-\alpha = \prod_{i=1}^{m}(1-\zeta_n^i\delta) = \prod_{i=1}^{n}\prod_{j=1}^{nm^{-1}}\left(1-\zeta_n^i\zeta_{nm^{-1}}^j\delta\right)$$
$$= N_{F(\sqrt[n]{\alpha})/F}\left(\prod_{i=1}^{m}\left(1-\zeta_n^i\delta\right)\right) \in N_{F(\sqrt[n]{\alpha})/F}F(\sqrt[n]{\alpha})^{\times}.$$

Hence, $(1-\alpha,\alpha)_n = 1$. Further, $-\alpha = (1-\alpha)(1-\alpha^{-1})^{-1}$ for $\alpha \neq 0, \alpha \neq 1$. This means that $(-\alpha,\alpha)_n = (1-\alpha,\alpha)_n(1-\alpha^{-1},\alpha^{-1})_n^{-1} = 1$. Moreover,

$$1 = (-\alpha\beta,\alpha\beta)_n = (-\alpha,\alpha)_n(\alpha,\beta)_n(\beta,\alpha)_n(-\beta,\beta)_n = (\alpha,\beta)_n(\,be,\alpha)_n,$$

i.e., $(\alpha,\beta)_n = (\beta,\alpha)_n^{-1}$.

Finally, if $(\alpha,\beta)_n = 1$, then $(\beta,\alpha)_n = 1$, which is equivalent to

$$\beta \in N_{F(\sqrt[n]{\alpha})/F}F(\sqrt[n]{\alpha})^{\times}.$$

(6): Let $\beta \in F^{\times n}$; then $(\alpha,\beta)_n = 1$ for all $\alpha \in F^{\times}$. Let $\beta \notin F^{\times n}$, then $L = F(\sqrt[n]{\beta}) \neq F$, and L/F is a nontrivial abelian extension. By Theorem (3.4.2) the subgroup $N_{L/F}L^{\times}$ does not coincide with $F^{\times}$. If we take an element $\alpha \in F^{\times}$ such that $\alpha \notin N_{L/F}L^{\times}$ then, by property (5), we get $(\alpha,\beta)_n \neq 1$.

(7): For $\gamma \in F^{\text{sep}}, \gamma^{nm} = \beta$, one has

$$(\alpha,\beta)_{nm}^m = \left(\gamma^{-1}\Psi_F(\alpha)(\gamma)\right)^m = \left(\gamma^{-m}\Psi_F(\alpha)(\gamma^m)\right) = (\alpha,\beta)_n,$$

because $(\gamma^m)^n = \beta$.

(8): Theorem (3.4.2) shows that

$$(\alpha,\beta)_{n,L} = \gamma^{-1}\Psi_L(\alpha)(\gamma) = \gamma^{-1}\Psi_F\left(N_{L/F}(\alpha)\right)(\gamma) = \left(N_{L/F}\alpha,\beta\right)_{n,F},$$

where $\gamma \in F^{\text{sep}}, \gamma^n = \beta$.

(9): Theorem (3.4.2) shows that for $\gamma \in F^{\text{sep}}, \gamma^n = \beta$,

$$(\sigma\alpha,\sigma\beta)_{n,\sigma L} = \sigma\left(\gamma^{-1}\Psi_L(\alpha)(\gamma)\right) = \sigma(\alpha,\beta)_{n,L}.$$

□

COROLLARY. *The Hilbert symbol induces the nondegenerate pairing*

$$(\,\cdot,\cdot)_n : F^{\times}/F^{\times n} \times F^{\times}/F^{\times n} \longrightarrow \mu_n.$$

The Kummer theory asserts that abelian extensions L/F of exponent n ($\mu_n \subset F^{\times}, p \nmid n$ if $\text{char}(F) = p$) are in one-to-one correspondence with subgroups $\text{B}_L \subset F^{\times}$, such that $\text{B}_L \supset F^{\times n}$, $L = F(\sqrt[n]{\text{B}_L}) = F(\gamma_i : \gamma_i^n \in \text{B}_L)$ and the group $\text{B}_L/F^{\times n}$ is dual to $\text{Gal}(L/F)$.

THEOREM. *Let $\mu_n \subset F^{\times}, p \nmid n$, if $\text{char}(F) = p$. Let* A *be a subgroup in $F^{\times}$ such that $F^{\times n} \subset \text{A}$. Denote its orthogonal complement with respect to the Hilbert symbol $(\,\cdot,\cdot)_n$ by* $\text{B} = \text{A}^{\perp}$, *i.e.,*

$$\text{B} = \{\beta \in F^{\times} : (\alpha,\beta)_n = 1 \quad \textit{for all } \alpha \in \text{A}\}.$$

Then $\text{A} = N_{L/F}L^{\times}$, *where $L = F(\sqrt[n]{\text{B}})$ and $A = B^{\perp}$.*

Proof. Recall that $F^{\times n}$ is of finite index in $F^\times$.

Let B be a subgroup in $F^\times$ with $F^{\times n} \subset \mathrm{B}$ and $|\mathrm{B} : F^{\times n}| = m$. Let $\mathrm{A} = \mathrm{B}^\perp$. Then $\Psi_F(\alpha)$, for $\alpha \in \mathrm{A}$, acts trivially on $F(\sqrt[n]{\beta})$ for $\beta \in \mathrm{B}$. This means that $\Psi_F(\alpha)$ acts trivially on $L = F(\sqrt[n]{\mathrm{B}})$ and, by Theorem (3.4.2), $\alpha \in N_{L/F}L^\times$. Hence

$$\mathrm{A} \subset N_{L/F}L^\times.$$

Conversely, if $\alpha \in N_{L/F}L^\times$, then $\Psi_F(\alpha)$ acts trivially on $F(\sqrt[n]{\beta}) \subset L$ and

$$\alpha \in N_{F(\sqrt[n]{\beta})/F}F(\sqrt[n]{\beta})^\times$$

for every $\beta \in \mathrm{B}$. Property (5) of the previous proposition shows that $(\alpha, \beta)_n = 1$ and hence $N_{L/F}L^\times \subset \mathrm{A}$. Thus, $\mathrm{A} = N_{L/F}L^\times$.

Furthermore, to complete the proof it suffices to verify that a subgroup A in $F^\times$ with $F^{\times n} \subset \mathrm{A}$ coincides with $(\mathrm{A}^\perp)^\perp$. Restricting the Hilbert symbol on $\mathrm{A} \times F^\times$ we obtain that it induces the nondegenerate pairing $\mathrm{A}/F^{\times n} \times F^\times/\mathrm{A}^\perp \to \mu_n$. The theory of finite abelian groups implies that the order of $\mathrm{A}/F^{\times n}$ coincides with the order of $F^\times/\mathrm{A}^\perp$. Similarly, one can verify that the order of $\mathrm{A}^\perp/F^{\times n}$ is the same as that of $F^\times/(\mathrm{A}^\perp)^\perp$, and hence the order of $F^\times/\mathrm{A}^\perp$ equals the order of $(\mathrm{A}^\perp)^\perp/F^{\times n}$. From $\mathrm{A} \subset (\mathrm{A}^\perp)^\perp$ we deduce that $\mathrm{A} = (\mathrm{A}^\perp)^\perp$. □

The problem to find explicit formulas for the norm residue symbol originates from Hilbert. In the case under consideration the challenge is to find a formula for the Hilbert symbol $(\alpha, \beta)_n$ in terms of the elements α, β of the field F. This problem is very complicated when $p|n$. Nevertheless, there is a simple answer when $p \nmid n$.

PROPOSITION. *Let n be relatively prime with p and $\mu_n \subset F^\times$. Then*

$$(\alpha, \beta)_n = t(\alpha, \beta)^{(q-1)/n},$$

where q is the cardinality of the residue field $\overline{F}$ and

$$t\colon F^\times \times F^\times \longrightarrow \mu_{q-1}$$

is the tame symbol: $t(\alpha, \beta)$ is the multiplicative representative of the residue of

$$\beta^{v_F(\alpha)}\alpha^{-v_F(\beta)}(-1)^{v_F(\alpha)v_F(\beta)}.$$

Proof. Note that the elements of the group μ_n, for $p \nmid n$, are isomorphically mapped onto the subgroup in the multiplicative group $\mathbb{F}_q^\times$. Hence, $n|(q-1)$. Note also that the prime elements generate $F^\times$. Indeed, if $\alpha = \pi^a\varepsilon$ with $\varepsilon \in U_F$, then $\alpha = \pi_1\pi^{a-1}$ for the prime element $\pi_1 = \pi\varepsilon$, when $a \neq 1$, and $\alpha = \pi_2$ for the prime element $\pi_2 = \pi\varepsilon$, when $a = 1$. Using properties (1) and (7) of the Hilbert symbol it suffices to verify that $t(\pi, \beta) = (\pi, \beta)_{q-1}$ for $\beta \in F^\times$.

Let $\beta = (-\pi)^a\theta\varepsilon$ with $a = v_F(\beta), \theta \in \mu_{q-1}, \varepsilon \in U_{1,F}$. Then, as $t(\pi, -\pi) = 1, t(\pi, \varepsilon) = 1$, we obtain $t(\pi, \beta) = t(\pi, \theta) = \theta$. Property (3) of the Hilbert symbol shows that $(\pi, -\pi)_{q-1} = 1$. Since the group $U_{1,F}$ is $(q-1)$-divisible, $(\pi, \varepsilon)_{q-1} = 1$. Finally, since the extension $F(\sqrt[n]{\theta})/F$ is unramified, so for $\eta \in F^{\mathrm{sep}}, \eta^{q-1} = \theta$,

$$(\pi, \theta)_{q-1} = \eta^{-1}\Psi_F(\pi)(\eta) = \eta^{-1}\varphi_F(\eta) = \eta^{q-1} = \theta.$$

We conclude that $(\pi, \beta)_{q-1} = \theta = t(\pi, \beta)$. □

15. Local Kroneker–Weber theorem.

Read (3.1.3).

Let ζ_1 be a primitive $(p^n - 1)$ th root of unity, let ζ_2 be a primitive p^m th root of unity, and $L_1 = \mathbb{Q}_p(\zeta_1), L_2 = \mathbb{Q}_p(\zeta_2)$. Show that

$$N_{L_1/\mathbb{Q}_p} L_1^\times = \langle p^n \rangle \times U_{\mathbb{Q}_p}, \qquad N_{L_2/\mathbb{Q}_p} L_2^\times = \langle p \rangle \times U_{m,\mathbb{Q}_p}.$$

Prove the local Kronecker–Weber Theorem: every finite abelian extension of $\mathbb{Q}_p$ is contained in a cyclotomic field $\mathbb{Q}_p(\zeta_n)$ for a suitable primitive n th root of unity.