The unit residue group

Dalla Torre, G.

CHAPTER 3

The local norm-residue symbol

We introduce the concept of norm-residue symbol in the case of local fields. Most of the statements in this chapter are well-known. Our main new contribution is Theorem 3.80, which characterizes the norm-residue symbol in an elementary way.

3.1 Topological algebra

We consider groups, rings, and fields endowed with a topology and recall some properties when they are locally compact Hausdorff spaces.

Definition 3.1 (Topological group)**.** A *topological group* is a group $(G, \cdot)$ together with a topology on G such that the group operations

(a) $G \times G \to G,\ (x, y) \mapsto x \cdot y$,

(b) $G \to G,\ x \mapsto x^{-1}$,

are continuous, where $G \times G$ has the product topology.

Remark 3.2. We consider finite groups as topological groups by endowing them with the discrete topology.

Definition 3.3 (Locally compact)**.** A topological space X is *locally compact* if every point of X has a compact neighbourhood.

Definition 3.4 (σ-algebra)**.** A *σ-algebra* on a set X is a non empty collection Σ of subsets of X closed under the formation of complements and countable unions.

Definition 3.5 (Measure)**.** Let X be a set and let Σ be a σ-algebra on X. A *measure* μ on Σ is a function $\mu : \Sigma \to \mathbb{R}_{\geq 0} \cup \{+\infty\}$ such that $\mu(\emptyset) = 0$ and for any sequence $(X_i)_{i \in \mathbb{Z}_{>0}}$ of pairwise disjoint sets in Σ one has

$$\mu\left(\bigcup_{i=1}^{\infty} X_i\right) = \sum_{i=1}^{\infty} \mu(X_i).$$

Definition 3.6 (Left Haar measure)**.** Let G be a locally compact topological group and let $\mathcal{B}$ be the σ-algebra generated by the compact subsets of G. A *left Haar measure* on G is a measure $\mu : \mathcal{B} \to \mathbb{R}_{\geq 0} \cup \{+\infty\}$ with the following properties.

(a) It is not the zero measure.

(b) It is finite on all compact sets $C \in \mathcal{B}$.

(c) It is outer regular on all sets $B \in \mathcal{B}$:

$$\mu(B) = \inf\{\mu(U) : B \subseteq U, \text{ open } U \in \mathcal{B}\}.$$

(d) It is inner regular on all sets $B \in \mathcal{B}$:

$$\mu(U) = \sup\{\mu(C) : C \subseteq B, \text{ compact } C \in \mathcal{B}\}.$$

(e) It is invariant under left translation: for every $g \in G$ and every set $B \in \mathcal{B}$ one has $\mu(gB) = \mu(B)$.

Theorem 3.7 (Weil [75])**.** *Let G be a locally compact Hausdorff group. Then there exists a left Haar measure on G. If μ and ν are two left Haar measures on G, then there is $C \in \mathbb{R}_{>0}$ such that $\nu = C\mu$.*

Proof. We refer to Chapter XI in [23] by Halmos. See Theorem B in Section 58 for the existence and Theorem C in Section 60 for the uniqueness up to a positive constant. □

Remark 3.8. A ring $(R, +, \cdot)$ is assumed to have a multiplicative identity, which we denote by 1.

Definition 3.9 (Topological ring)**.** A *topological ring* is a ring $(R, +, \cdot)$ together with a topology on R such that the ring operations

(a) $R \times R \to R,\ (x, y) \mapsto x + y$,

(b) $R \times R \to R,\ (x, y) \mapsto x \cdot y$

are continuous, where $R \times R$ has the product topology.

Theorem 3.10. *Let R be a ring. Then the set of all invertible elements of R forms a group under multiplication.*

Proof. See Section 1 of Chapter II in [32] by Lang. □

Definition 3.11 (Group of units)**.** Let R be a ring. The *group of units* R^* of R is the group of all invertible elements of R.

Remark 3.12. The topology of a topological ring R, which is often called 'additive topology', induces a topology on the group R^*. This topology does not always render R^* a topological group, because the operation $R^* \to R^*$, $x \mapsto x^{-1}$, is not necessarily continuous with respect to the additive topology. A canonical way to repair this is to give R^* the subset topology coming from the injection

$$R^* \to R \times R,\ x \mapsto (x, x^{-1}),$$

of R^* into the topological product $R \times R$. This topology renders R^* a topological group and the inclusion map $R^* \hookrightarrow R$ is continuous.

The previous remark suggests the following definition of topological field.

Definition 3.13 (Topological field)**.** A *topological field* is a field F that is a topological ring such that the operation

$$F^* \to F^*,\ x \mapsto x^{-1},$$

is continuous with respect to the induced topology on F^*.

Theorem 3.14. *Let F be a locally compact Hausdorff topological ring that is a field. Then F is a topological field.*

Proof. See Section 2.3 of Chapter III in [28] by Iyanaga. □

3.2 Local fields

We recall some basic facts and terminology relative to local fields. We refer to [65] by Serre, to [9] by Cassels and Fröhlich, to [6] by Bourbaki, to [50] and [51] by Neukirch. Since the definitions of some concepts are not uniform, we provide a reference for our reader.

Definition 3.15 (Local field)**.** A *local field* is a non-discrete locally compact Hausdorff topological field.

Local fields have been completely classified by van Dantzig [72] and Pontryagin [55].

Theorem 3.16 (van Dantzig [72], Pontryagin [55])**.** *All of the following are local fields and every local field is isomorphic, as a topological field, to one of the following:*

(a) *the field $\mathbb{R}$ of real numbers;*

(b) *the field $\mathbb{C}$ of complex numbers;*
(c) *a finite field extension of $\mathbb{Q}_p$, the field of p-adic rationals, where p is a prime;*
(d) *the field $\mathbb{F}_q((t))$ of formal Laurent series in one variable t with coefficients in a finite field $\mathbb{F}_q$ of q elements.*

Proof. See Theorem 22 in Section 27 of Chapter 4 in [56] by Pontryagin. □

Definition 3.17 (Normalized absolute value)**.** Let F be a local field. The *normalized absolute value* $|\cdot|_F$ on F is the function

$$|\cdot|_F : F \to \mathbb{R}_{\geq 0}$$

such that for every $\alpha \in F$ the normalized absolute value $|\alpha|_F$ of α is given by the formula

$$|\alpha|_F = \frac{\mu(\alpha X)}{\mu(X)},$$

where μ is a Haar measure on the additive group F and X is any subset of F with $0 < \mu(X) < \infty$.

We will often use only the symbol $|\cdot|$ for the normalized absolute value when the field is understood.

Theorem 3.18. *Let F be a local field and let $|\cdot|_F : F \to \mathbb{R}_{\geq 0}$ be the normalized absolute value on F. Then for all $\alpha, \beta \in F$ one has*

$$|\alpha\beta|_F = |\alpha|_F \cdot |\beta|_F.$$

Proof. The formula follows from Definition 3.17. □

Definition 3.19 (Non-Archimedean and Archimedean local fields)**.** A local field F is *non-Archimedean* if for all $\alpha, \beta \in F$ one has

$$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}.$$

Otherwise, it is *Archimedean*.

The fields of real and complex numbers are Archimedean fields. All local fields that are not isomorphic to any of those two fields are non-Archimedean.

Definition 3.20 (Extension of local fields)**.** An *extension of local fields* is a field extension F/E such that E and F are local fields and the inclusion $E \hookrightarrow F$ is continuous.

Theorem 3.21. *Let F/E be an extension of local fields. Then F/E is a finite field extension.*

Proof. See Theorem 3 in Section 2.4 of Chapter I in [6] by Bourbaki. □

Theorem 3.22. *Let F/E be an extension of local fields and let $|\cdot|_F : F \to \mathbb{R}_{\geq 0}$ and $|\cdot|_E : E \to \mathbb{R}_{\geq 0}$ be the normalized absolute values on F and E, respectively. Then for all $\alpha \in F$ one has*

$$|\alpha|_F = |\,\mathrm{N}_{F/E}\,\alpha|_E.$$

Proof. See Lemma in Section 11 of Chapter II in [9] by Cassels and Fröhlich. □

Theorem 3.23. *Let F be a non-Archimedean local field. Then the set of all elements of F whose normalized absolute value is less than or equal to* 1 *forms a ring under addition and multiplication.*

Proof. The result follows from Theorem 3.18 and Definition 3.19. □

Definition 3.24 (Ring of integers)**.** Let F be a non-Archimedean local field. The *ring of integers* $\mathcal{O}_F$ of F is the ring of all elements of F whose normalized absolute value is less than or equal to 1.

Theorem 3.25. *Let F be a non-Archimedean local field and let $\mathcal{O}_F$ be its ring of integers. Then the set of all elements of F whose normalized absolute value is equal to* 1 *forms the group $\mathcal{O}_F^*$ of invertible elements of $\mathcal{O}_F$ under multiplication.*

Proof. The result follows from Theorem 3.18. □

Definition 3.26 (Group of units)**.** Let F be a non-Archimedean local field and let $\mathcal{O}_F$ be its ring of integers. The *group of units* U_F of $\mathcal{O}_F$ is the group of elements of F whose normalized absolute value is equal to 1.

Remark 3.27. Note the equality $\mathcal{O}_F^* = U_F$. We introduce a different notation in analogy to Definition 3.36.

Theorem 3.28. *Let F be a non-Archimedean local field and let $\mathcal{O}_F$ be its ring of integers. Then $\mathcal{O}_F$ is a local ring with maximal ideal formed by the set of all elements of F whose normalized absolute value is less than* 1*.*

Proof. Theorem 3.18 and Definition 3.19 imply that the set of all elements of F whose normalized absolute value is less than 1 forms an ideal of $\mathcal{O}_F$. Theorem 3.25 shows that this ideal is the unique maximal ideal of $\mathcal{O}_F$. □

Definition 3.29 (Maximal ideal)**.** Let F be a non-Archimedean local field. The *maximal ideal* $\mathfrak{P}_F$ of the ring of integers of F is the additive group of all elements of F whose normalized absolute value is less than 1.

Definition 3.30 (Residue field)**.** Let F be a non-Archimedean local field, let $\mathcal{O}_F$ be the ring of integers of F, and let $\mathfrak{P}_F$ be the maximal ideal of $\mathcal{O}_F$. The *residue field* of F is the quotient $\mathcal{O}_F/\mathfrak{P}_F$.

Theorem 3.31. *Let F be a non-Archimedean local field. Then there exist a unique real number $C \in \mathbb{R}_{>1}$ and a unique surjective group homomorphism $\mathrm{v}_F : F^* \to \mathbb{Z}$ such that for all $\alpha \in F^*$ one has*

$$|\alpha| = C^{-\mathrm{v}_F(\alpha)}.$$

Proof. See Theorem 6 in Section 4 of Chapter I in [76] by Weil. □

Definition 3.32 (Normalized valuation)**.** Let F be a non-Archimedean local field. The *normalized valuation* on F is the function $\mathrm{v}_F : F \to \mathbb{Z} \cup \{+\infty\}$ such that $\mathrm{v}_F(0) = +\infty$ and $\mathrm{v}_F\,|_{F^*}$ equals the surjective group homomorphism $F^* \to \mathbb{Z}$ of Theorem 3.31.

We will often use only the symbol v for the normalized valuation when the field is understood and the symbol v_p for the normalized valuation on the field $\mathbb{Q}_p$ of p-adic rationals.

Definition 3.33 (Prime element)**.** Let F be a non-Archimedean local field. A *prime element* of F is an element in F whose normalized valuation is 1.

Theorem 3.34. *Let F be a non-Archimedean local field. Then the cardinality of its residue field is finite and equals the constant C of* Theorem 3.31.

Proof. See Theorem 6 in Section 4 of Chapter I in [76] by Weil. □

Theorem 3.35. *Let F be a non-Archimedean local field, let $\mathcal{O}_F$ be its ring of integers, and let $\mathfrak{P}_F$ be the maximal ideal of $\mathcal{O}_F$. Then for each $n \in \mathbb{Z}_{>0}$ the $\mathcal{O}_F$-ideal $\mathfrak{P}_F^n$ consists of all elements of F whose normalized valuation is greater than or equal to n.*

Proof. The result follows from Theorem 3.31. □

Definition 3.36 (Higher unit groups)**.** Let F be a non-Archimedean local field and let $\mathfrak{P}_F$ be the maximal ideal of its ring of integers. For each $n \in \mathbb{Z}_{>0}$ the *n-th higher unit group* $U_F^{(n)}$ of the ring of integers of F is the group $1+\mathfrak{P}_F^n$. The *0-th higher unit group* $U_F^{(0)}$ of the ring of integers of F is the group of units U_F.

Theorem 3.37. *Let F be a non-Archimedean local field, let q be the cardinality of its residue field, let U_F be the group of units of the ring of integers of F, and let μ_{q-1} be the group of $q-1$-th roots of unity in F. Then the short sequence*

$$1 \longrightarrow U_F \longrightarrow F^* \xrightarrow{\mathrm{v}} \mathbb{Z} \longrightarrow 1$$

is exact and split, the group μ_{q-1} is cyclic of order $q-1$, and the group U_F has the direct decomposition

$$U_F = \mu_{q-1} \times U_F^{(1)},$$

where $U_F^{(1)}$ is the first higher unit group of the ring of integers of F.

Proof. See Proposition 1.1 of Chapter III in [50] by Neukirch. □

Theorem 3.38. *Let F be a non-Archimedean local field of characteristic 0, let p and q be the characteristic and the cardinality of its residue field, respectively, let U_F be the group of units of the ring of integers of F, let d the degree of the extension $F/\mathbb{Q}_p$, where $\mathbb{Q}_p$ is the field of p-adic rationals, and let $\mathbb{Z}_p$ be the ring of integers of $\mathbb{Q}_p$. Then there exists $a \in \mathbb{Z}_{\geq 0}$ such that there is an isomorphism of topological groups*

$$U_F \cong \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d.$$

Proof. See Proposition 5.7 of Chapter II in [51] by Neukirch. □

Theorem 3.39. *Let p be a prime, let F be a non-Archimedean local field of characteristic p, let q be the cardinality of its residue field, and let U_F be the group of units of the ring of integers of F. Then there is an isomorphism of topological groups*

$$U_F \cong \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}_p^{\mathbb{Z}},$$

where $\mathbb{Z}_p^{\mathbb{Z}}$ is endowed with the product topology.

Proof. See Proposition 5.7 of Chapter II in [51] by Neukirch. □

3.3 Abelian Kummer theory

Definition 3.40 (Exponent of a Galois field extension)**.** The *exponent of a Galois field extension L/K* is the exponent of the Galois group $\mathrm{Gal}(L/K)$.

Definition 3.41 (Abelian field extension)**.** An *abelian field extension* is a Galois field extension L/K such that the Galois group $\mathrm{Gal}(L/K)$ is abelian.

Definition 3.42 (Cyclic field extension)**.** A *cyclic field extension* is a Galois field extension L/K such that the Galois group $\mathrm{Gal}(L/K)$ is cyclic.

Definition 3.43 (Kummer m-extension)**.** Let m be a positive integer. A *Kummer m-extension* is an abelian field extension L/K of exponent dividing m such that the field K contains a primitive m-th root of unity.

Theorem 3.44. *Let m be a positive integer and let K be a field containing a primitive m-th root of unity. Then there is an inclusion preserving bijection*

$$\begin{aligned}\{\textit{Kummer } m\textit{-extensions of } K\}/{\cong_K} &\leftrightarrow \{\textit{subgroups of } K^*/{K^*}^m\},\\ L &\mapsto (L^{*m} \cap K^*)/K^{*m},\\ K(\sqrt[m]{\Delta}) &\hookleftarrow \Delta\end{aligned}$$

Proof. See Theorem 8.2 in Section 8 of Chapter VI in [32] by Lang. □

Remark 3.45. On the Galois group $\mathrm{Gal}(L/K)$ of a Galois field extension L/K we consider the Krull topology. If G is a topological group and H is an abelian topological group, then the set of continuous group homomorphisms $G \to H$ forms an abelian group under pointwise addition. We denote the group of continuous group homomorphisms from G to H by $\mathrm{Hom}(G, H)$.

Definition 3.46 (Compact-open topology)**.** Let X and Y be topological spaces and let $\mathrm{C}(X, Y)$ be the set of continuous functions $X \to Y$. The *compact-open topology* on the set $\mathrm{C}(X, Y)$ is the topology generated by the sets of the form

$$V(K, U) = \{f \in \mathrm{C}(X, Y) : f(K) \subseteq U\},$$

where K ranges over the compact subsets of X and U ranges over the open subsets of Y.

Theorem 3.47. *Let m be a positive integer, let K be a field containing a primitive m-th root of unity, let μ_m be the group of m-th roots of unity in K, let L be a Kummer m-extension of K, and let Δ be the discrete group $(L^{*m} \cap K^*)/K^{*m}$. Then there is a perfect pairing*

$$\begin{aligned}\mathrm{Gal}(L/K) \times \Delta &\to \mu_m,\\ (\sigma, a) &\mapsto \frac{\sigma(\sqrt[m]{a})}{\sqrt[m]{a}},\end{aligned}$$

that is, the map that sends an element $a \in \Delta$ to the character $\sigma \mapsto \frac{\sigma(\sqrt[m]{a})}{\sqrt[m]{a}}$ is a canonical isomorphism of topological groups

$$\Delta \cong \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_m)$$

and the map that sends an automorphism $\sigma \in \mathrm{Gal}(L/K)$ to the character $a \mapsto \frac{\sigma(\sqrt[m]{a})}{\sqrt[m]{a}}$ is a canonical isomorphism of topological groups

$$\mathrm{Gal}(L/K) \cong \mathrm{Hom}(\Delta, \mu_m),$$

where the groups $\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_m)$ and $\mathrm{Hom}(\Delta, \mu_m)$ are endowed with the compact-open topology.

Proof. See Theorem 5.3 of Chapter I in [50] by Neukirch. □

Remark 3.48. Let m be a positive integer and let K be a field containing a primitive m-th root of unity. Within a fixed algebraic closure of K there exists a unique maximal Kummer m-extension $L = K(\sqrt[m]{K^*})$, because L is a Kummer m-extension and all Kummer m-extensions of K are contained in L. By Theorem 3.47 we have a canonical isomorphism of topological groups

$$K^*/K^{*m} \cong \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_m).$$

3.4 Local class field theory

We state the main theorem of local class field theory about the local reciprocity map and some related results. See [50] by Neukirch and Chapter VI in [9] by Cassels and Fröhlich as references.

Theorem 3.49. *Let l/k be an extension of finite fields. The map $\varphi : l \to l$, $x \mapsto x^{\#k}$, is an automorphism of l over k.*

Proof. See Theorem 5.5 in Section 5 of Chapter V in [32] by Lang. □

Definition 3.50 (Frobenius automorphism)**.** Let l/k be an extension of finite fields. The *Frobenius automorphism* of l over k is the automorphism of l that maps any element x in l to $x^{\#k}$.

Theorem 3.51. *Let l/k be an extension of finite fields. Then the extension l/k is Galois and its Galois group* $\mathrm{Gal}(l/k)$ *is cyclic and generated by the Frobenius automorphism of l over k.*

Proof. See Theorem 5.5 in Section 5 of Chapter V in [32] by Lang. □

Definition 3.52 (Unramified extension of non-Archimedean local fields)**.** Let F/E be an extension of non-Archimedean local fields and let $\mathcal{O}_F/\mathfrak{P}_F$ and $\mathcal{O}_E/\mathfrak{P}_E$ be the residue fields of F and E, respectively. The extension F/E is *unramified* if one has

$$[F : E] = [\mathcal{O}_F/\mathfrak{P}_F : \mathcal{O}_E/\mathfrak{P}_E].$$

Theorem 3.53. *Let F/E be an unramified extension of non-Archimedean local fields and let $\mathrm{v}_F : F^* \to \mathbb{Z}$ and $\mathrm{v}_E : E^* \to \mathbb{Z}$ be the normalized valuations on F and E, respectively. Then one has*

$$\mathrm{v}_F\,|_E = \mathrm{v}_E\,.$$

Proof. By definition $\mathrm{v}_F(0) = +\infty = \mathrm{v}_E(0)$. Let $\mathcal{O}_F/\mathfrak{P}_F$ and $\mathcal{O}_E/\mathfrak{P}_E$ be the residue fields of F and E, respectively. Since the extension F/E is unramified, we have

$$[F : E] = [\mathcal{O}_F/\mathfrak{P}_F : \mathcal{O}_E/\mathfrak{P}_E].$$

Using Theorem 3.22 and Theorem 3.34 we get for all $\alpha \in E^*$

$$|\mathcal{O}_F/\mathfrak{P}_F|^{-\mathrm{v}_F(\alpha)} = |\mathcal{O}_E/\mathfrak{P}_E|^{-\mathrm{v}_E(\mathrm{N}_{F/E}\,\alpha)}.$$

Taking the logarithm in base $|\mathcal{O}_E/\mathfrak{P}_E|$ of both sides gives

$$-[F : E]\,\mathrm{v}_F(\alpha) = -\,\mathrm{v}_E(\mathrm{N}_{F/E}\,\alpha).$$

The result follows from the equality $\mathrm{N}_{F/E}\,\alpha = \alpha^{[F:E]}$ for all $\alpha \in E$. □

Theorem 3.54. *Let F/E be an unramified extension of non-Archimedean local fields and let $\mathcal{O}_F/\mathfrak{P}_F$ and $\mathcal{O}_E/\mathfrak{P}_E$ be the residue fields of F and E, respectively. Then the extension F/E is Galois and the map that sends an automorphism in $\mathrm{Gal}(F/E)$ to its induced automorphism in $\mathrm{Gal}((\mathcal{O}_F/\mathfrak{P}_F)/(\mathcal{O}_E/\mathfrak{P}_E))$ by restriction to the rings of integers and reduction modulo the maximal ideals is a canonical isomorphism*

$$\mathrm{Gal}(F/E) \cong \mathrm{Gal}((\mathcal{O}_F/\mathfrak{P}_F)/(\mathcal{O}_E/\mathfrak{P}_E)).$$

Proof. See Corollary of Theorem 1 in Section 7 of Chapter 1 in [9] by Cassels and Fröhlich. □

Definition 3.55 (Frobenius element)**.** Let F/E be an unramified extension of non-Archimedean local fields. The *Frobenius element* $\mathrm{Fr}_{F/E}$ is the automorphism in the Galois group $\mathrm{Gal}(F/E)$ that induces the Frobenius automorphism on the corresponding extension of residue fields.

Theorem 3.56. *Let F/E be an unramified extension of non-Archimedean local fields. Then the Galois group $\mathrm{Gal}(F/E)$ is cyclic and generated by the Frobenius element $\mathrm{Fr}_{F/E}$.*

Proof. By Theorem 3.54 the Galois group $\mathrm{Gal}(F/E)$ is isomorphic to the Galois group of an extension of finite fields, which is, by Theorem 3.51, cyclic and generated by the Frobenius automorphism. □

Theorem 3.57. *Let $\mathcal{L}$ be the category whose objects are local fields and whose morphisms are continuous homomorphisms of fields, let $E \to F$ be a morphism of local fields, and let $\mathrm{N}_{F/E} : F \to E$ be the norm map from F to E. Then there is a unique system of group homomorphisms*

$$r_{F/E} : \mathrm{Gal}(F/E) \to E^*/\,\mathrm{N}_{F/E}\,F^*$$

indexed by all morphisms $E \to F$ in $\mathcal{L}$ with F/E Galois with the following properties.

(a) *For each commutative diagram in* $\mathcal{L}$

$$\begin{array}{ccc} E & \longrightarrow & F \\ \downarrow & & \downarrow \\ K & \longrightarrow & L \end{array}$$

with F/E *and* L/K *Galois, the diagram*

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \xrightarrow{r_{L/K}} & K^*/\,\mathrm{N}_{L/K}\,L^* \\ \Big\downarrow{\scriptstyle \mathrm{res}} & & \Big\downarrow{\scriptstyle \mathrm{N}_{K/E}} \\ \mathrm{Gal}(F/E) & \xrightarrow{r_{F/E}} & E^*/\,\mathrm{N}_{F/E}\,F^* \end{array}$$

commutes, where the map $\mathrm{res} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/E)$ *is given by restricting to* F *the automorphisms of* L *over* K*.*

(b) *If* E *is Archimedean, then the group homomorphism*

$$r_{F/E} : \mathrm{Gal}(F/E) \to E^*/\,\mathrm{N}_{F/E}\,F^*$$

is surjective.

(c) *If* E *is non-Archimedean and the extension* F/E *is unramified, then there is a commutative diagram*

$$\begin{array}{ccc} \mathrm{Gal}(F/E) & \xrightarrow{r_{F/E}} & E^*/\,\mathrm{N}_{F/E}\,F^* \\ \Big\downarrow{\scriptstyle \sim} & & \Big\downarrow{\scriptstyle \mathrm{v}} \\ \mathrm{Gal}((\mathcal{O}_F/\mathfrak{P}_F)/(\mathcal{O}_E/\mathfrak{P}_E)) & \xrightarrow{\sim} & \mathbb{Z}/[F:E]\mathbb{Z} \end{array}$$

where the map

$$\mathrm{Gal}(F/E) \xrightarrow{\sim} \mathrm{Gal}((\mathcal{O}_F/\mathfrak{P}_F)/(\mathcal{O}_E/\mathfrak{P}_E))$$

is the isomorphism of Theorem 3.54*, the vertical map*

$$\mathrm{v} : E^*/\,\mathrm{N}_{F/E}\,F^* \longrightarrow \mathbb{Z}/[F:E]\mathbb{Z}$$

is the group homomorphism induced by the normalized valuation on E *modulo* $[F:E]$*, and the isomorphism*

$$\mathrm{Gal}((\mathcal{O}_F/\mathfrak{P}_F)/(\mathcal{O}_E/\mathfrak{P}_E)) \xrightarrow{\sim} \mathbb{Z}/[F:E]\mathbb{Z}$$

maps the Frobenius automorphism of $\mathcal{O}_F/\mathfrak{P}_F$ *over* $\mathcal{O}_E/\mathfrak{P}_E$ *to the residue class* $1 \bmod [F:E]$*.*

Proof. See Section 2 of Chapter III in [50] by Neukirch. □

Definition 3.58 (Local reciprocity maps)**.** The *local reciprocity maps* are the group homomorphisms $r_{F/E}$ in Theorem 3.57.

Theorem 3.59. *Let F/E be a Galois extension of local fields and let $\mathrm{Gal}(F/E)^{\mathrm{ab}}$ be the abelianization of the Galois group of F over E. Then each local reciprocity map $r_{F/E}$ induces a group isomorphism*

$$\mathrm{Gal}(F/E)^{\mathrm{ab}} \xrightarrow{\sim} E^*/\,\mathrm{N}_{F/E}\,F^*. \tag{3.60}$$

Proof. See Theorem 2.1 in Section 2 of Chapter III in [50] by Neukirch. □

Definition 3.61 (Norm-residue map)**.** Let F/E be a Galois extension of local fields and let $\mathrm{Gal}(F/E)^{\mathrm{ab}}$ be the abelianization of the Galois group of F over E. The *norm-residue map* $\psi_{F/E}$ of the extension F/E is the surjective homomorphism

$$\psi_{F/E} : E^* \to \mathrm{Gal}(F/E)^{\mathrm{ab}}$$

obtained by composing the inverse $E^*/\,\mathrm{N}_{F/E}\,F^* \to \mathrm{Gal}(F/E)^{\mathrm{ab}}$ of the group isomorphism 3.60 with the projection $E^* \to E^*/\,\mathrm{N}_{F/E}\,F^*$.

Remark 3.62. By taking projective limits the norm-residue map gives rise to a norm-residue map for any arbitrary Galois extension F/E of a given local field E. In the particular case of the maximal abelian extension of E we denote by

$$\psi_E : E^* \to G_E^{\mathrm{ab}}$$

the norm-residue map from E^* to the Galois group G_E^{ab} of the maximal abelian extension of E.

Theorem 3.63 (Local existence theorem)**.** *Let E be a local field. A subgroup of E^* is of the form $\mathrm{N}_{F/E}\,F^*$ for some abelian extension F/E of local fields if and only if it is of finite index and open.*

Proof. See Theorem 3 in Section 2.7 of Chapter VI in [9] by Cassels and Fröhlich. □

Theorem 3.64. *Let m be a positive integer, let E be a local field containing a primitive m-th root of unity, and let $F = E(\sqrt[m]{E^*})$ be the maximal Kummer m-extension of E within a fixed algebraic closure of E. Then the extension F/E is finite, one has*

$$\mathrm{N}_{F/E}\,F^* = E^{*m},$$

and the norm-residue map $\psi_{F/E}$ induces an isomorphism

$$E^*/E^{*m} \xrightarrow{\sim} \mathrm{Gal}(F/E).$$

Proof. By Theorem 3.37, Theorem 3.38, and Theorem 3.39 the subgroup E^{*m} of E is of finite index and open. Theorem 3.63 implies that there exists some abelian extension L/E of local fields such that $\mathrm{N}_{L/E}\, L^* = E^{*m}$. By Theorem 3.21 the extension L/E is finite. By Theorem 3.59 the local reciprocity map $r_{L/E}$ gives the isomorphism

$$\mathrm{Gal}(L/E) \xrightarrow{\sim} E^*/E^{*m}.$$

Hence, the norm-residue map $\psi_{F/E}$ induces an isomorphism

$$E^*/E^{*m} \xrightarrow{\sim} \mathrm{Gal}(F/E).$$

Since E^*/E^{*m} is the maximal quotient group of E^* of exponent dividing m, the extension L/E is the maximal Kummer m-extension of E. □

Theorem 3.65 (Norm limitation theorem)**.** *Let E/F be an extension of local fields and let L be the largest abelian extension of F contained in E. Then one has*

$$\mathrm{N}_{E/F}\, E^* = \mathrm{N}_{L/F}\, L^*.$$

Proof. See Proposition 4 in Section 2.6 of Chapter VI in [9] by Cassels and Fröhlich. □

Corollary 3.66. *Let E/F be an extension of local fields and let L be the largest abelian extension of F contained in E. Let $U_E^{(1)}$ and $U_L^{(1)}$ be the first higher unit groups of the rings of integers of E and of L, respectively. Then one has*

$$\mathrm{N}_{E/F}\, U_E^{(1)} = \mathrm{N}_{L/F}\, U_L^{(1)}$$

Proof. Let U_E, U_L, and U_F be the unit groups of the rings of integers of E, of L, and of F, respectively. Since we have $\mathrm{N}_{E/F}\, U_E = (\mathrm{N}_{E/F}\, E^*) \cap U_F$ and $\mathrm{N}_{L/F}\, U_L = (\mathrm{N}_{L/F}\, L^*) \cap U_F$, the result follows from Theorem 3.65 and the direct decompositions of Theorem 3.37. □

3.5 The norm-residue symbol

Given a positive integer m, we introduce the m-th power norm-residue symbol.

Definition 3.67 (m-th power norm-residue symbol)**.** Let m be a positive integer, let F be a local field containing a primitive m-th root of unity, let μ_m be the group of m-th roots of unity in F, and let $\psi_F : F^* \to G_F^{\mathrm{ab}}$ be the norm-residue map. The *m-th power norm-residue symbol* is the map

$$\begin{aligned}(\cdot,\cdot)_{F,m} : F^* \times F^* &\to \mu_m,\\ (a,b) &\mapsto (a,b)_{F,m},\end{aligned}$$

such that for all $a, b \in F^*$ one has

$$(a,b)_{F,m} = \psi_F(a)(\beta)/\beta,$$

where $\beta^m = b$ with β in an algebraic closure of F.

Remark 3.68. The m-th power norm-residue symbol is well-defined. The definition does not depend on the choice of β, because F contains the group of m-th roots of unity.

We will often write only '$(\cdot,\cdot)$' and 'norm-residue symbol' when m and F are understood.

Theorem 3.69. *Let m be a positive integer, let F be a local field containing a primitive m-th root of unity, and let μ_m be the group of m-th roots of unity in F. Then the norm-residue symbol is a pairing*

$$(\cdot,\cdot) : F^* \times F^* \to \mu_m.$$

Proof. Since by Definition 3.61 the norm-residue map is a homomorphism, for all $a, b, c \in F^*$ we get

$$(ac,b) = \frac{\psi(ac)(\beta)}{\beta} = \frac{\psi(a)(\psi(c)(\beta))}{\beta} = \frac{\psi(a)(\beta')}{\beta'}\frac{\psi(c)(\beta)}{\beta} = (a,b)\,(c,b)\,,$$

where $\beta^m = b$ and $\beta' = \psi(c)(\beta)$. Note that $(\beta')^m = b$, because $\psi(c)$ is a field automorphism that is the identity on F. Moreover, if $\gamma^m = c$, we have

$$(a,bc) = \frac{\psi(a)(\beta\gamma)}{\beta\gamma} = \frac{\psi(a)(\beta)}{\beta}\frac{\psi(a)(\gamma)}{\gamma} = (a,b)\,(a,c)\,.$$

Hence, the norm-residue symbol is a pairing. □

Let m be a positive integer and let F be a local field containing a primitive m-th root of unity. Now we want to apply both Kummer theory and local class field theory to the maximal abelian extension of F of exponent dividing m, that is, the field extension $L = F(\sqrt[m]{F^*})$, and to see how we can obtain the norm-residue symbol. By Theorem 3.64 of local class field theory the norm-residue map $\psi_{L/F}$ induces a canonical isomorphism

$$F^*/{F^*}^m \cong \mathrm{Gal}(L/F).$$

Combining this isomorphism and the perfect pairing

$$\begin{aligned} \mathrm{Gal}(L/F) \times F^*/{F^*}^m &\to \mu_m, \\ (\sigma, a) &\mapsto \frac{\sigma(\sqrt[m]{a})}{\sqrt[m]{a}}. \end{aligned}$$

of Theorem 3.47 yields the perfect pairing

$$(\cdot,\cdot) : F^*/F^{*m} \times F^*/F^{*m} \to \mu_m$$
$$(a,b)_m = \psi_{L/F}(a)(\beta)/\beta,$$

where $\beta^m = b$, which is equal to the pairing induced by the norm-residue symbol. We have proved the following theorem.

Theorem 3.70. *Let m be a positive integer, let F be a local field containing a primitive m-th root of unity, and let μ_m be the group of m-th roots of unity in F. Then the norm-residue symbol induces a perfect pairing*

$$(\cdot,\cdot) : F^*/F^{*m} \times F^*/F^{*m} \longrightarrow \mu_m.$$

We will often call the pairing in Theorem 3.70 'norm-residue symbol'.

Theorem 3.71. *Let m be a positive integer and let F be a local field containing a primitive m-th root of unity. Then*

$$[F^* : F^{*m}] = m[U_F : U_F^m] = m^2|m|^{-1} < \infty.$$

Proof. The first equality follows from the exact and split sequence of Theorem 3.37. If the characteristic of F is 0, then Theorem 3.38 gives

$$[U_F : U_F^m] = m|(\mathbb{Z}_p/m\mathbb{Z}_p)|^d = mp^{d\,\mathrm{v}_p(m)},$$

where p is the characteristic of the residue field of F and $d = [F : \mathbb{Q}_p]$. Using Theorem 3.22 we get

$$|m|^{-1} = |\,\mathrm{N}_{F/\mathbb{Q}_p}\, m|^{-1} = |m^d|^{-1} = p^{d\,\mathrm{v}_p(m)}.$$

Hence, we obtain the equality

$$[U_F : U_F^m] = m|m|^{-1}.$$

If the characteristic of F is a prime p, then we have $(m,p) = 1$. Hence, we obtain $|m| = 1$ and $m\mathbb{Z}_p = \mathbb{Z}_p$. The equality

$$[U_F : U_F^m] = m|m|^{-1}$$

follows from Theorem 3.39. □

Lemma 3.72. *Let m be a positive integer, let F be a local field containing a primitive m-th root of unity, and let a and b be elements in F^*. Then one has $(a,b) = 1$ if and only if a is a norm for the extension $F(\beta)/F$, where $\beta^m = b$ with β in an algebraic closure of F.*

Proof. By definition of norm-residue symbol we have

$$(a, b) = \psi_F(a)(\beta)/\beta.$$

Since β is a generator of the extension $F(\beta)/F$, the automorphism $\psi_F(a)$ acts trivially on $F(\beta)$ if and only if we have $(a, b) = 1$. By Theorem 3.59 this is the case if and only if a is in $\mathrm{N}_{F(\beta)/F} F(\beta)^*$. □

Lemma 3.73. *Let m be a positive integer, let K be a field containing a primitive m-th root of unity, and let $a \in K^*$. Then for every $x \in K$ the element $x^m - a$ is a norm from $K(\sqrt[m]{a})$.*

Proof. See Exercise 2.5 in [9] by Cassels and Fröhlich. □

We note that the norm-residue symbol necessarily satisfies the following three relations. We will very often use them.

Theorem 3.74. *Let m be a positive integer, let F be a local field containing a primitive m-th root of unity, let μ_m be the group of m-th roots of unity in F, and let $(\cdot, \cdot) : F^* \times F^* \to \mu_m$ be the norm-residue symbol. Then for all $a, b \in F^*$, $c \in F^* \setminus \{1\}$ the norm-residue symbol satisfies the equalities*

$$(-a, a) = 1 \quad \textit{and} \quad (1 - c, c) = 1$$

and the antisymmetric relation

$$(a, b)(b, a) = 1.$$

Proof. Lemma 3.73 implies that for all $a \in F^*$, $c \in F^* \setminus \{1\}$ the elements $-a$ and $1 - c$ are nonzero norms for $F(\sqrt[m]{a})/F$ and for $F(\sqrt[m]{c})/F$, respectively. By Lemma 3.72 we get the equalities $(-a, a) = 1$ and $(1 - c, c) = 1$. Now the antisymmetric relation follows easily from bilinearity and the first equality:

$$1 = (-ab, ab) = (-a, a)(b, a)(a, b)(-b, b) = (a, b)(b, a).$$ □

Corollary 3.75. *Let m be a positive integer, let F be a local field containing a primitive m-th root of unity, let μ_m be the group of m-th roots of unity in F, and let $(\cdot, \cdot) : F^* \times F^* \to \mu_m$ be the norm-residue symbol. Then for all $a \in F^*$ one has*

$$(-1, a) = (a, a)\,.$$

Proof. For all $a \in F^*$ we get

$$(-1, a) = (-1, a)\,(-a, a) = (a, a)\,,$$

because by Theorem 3.74 we have $(-a, a) = 1$ for all $a \in F^*$. □

Theorem 3.76. *Let m be a positive integer, let n be a positive divisor of m, let F be a local field containing a primitive m-th root of unity, let μ_m and μ_n be the groups of m-th roots of unity in F and of n-th roots of unity in F, respectively, let $(\cdot,\cdot)_{F,m} : F^* \times F^* \to \mu_m$ be the m-th power norm-residue symbol, and let $(\cdot,\cdot)_{F,n} : F^* \times F^* \to \mu_n$ be the n-th power norm-residue symbol. Then one has*

$$(\cdot,\cdot)_{F,n} = (\cdot,\cdot)_{F,m}^{m/n}.$$

Proof. This follows immediately from Definition 3.67. □

Remark 3.77. We will often assume that m is a prime power. In fact, if one has $m = m_1 m_2$ with m_1 and m_2 coprime positive integers, then by Theorem 3.76 and the Chinese remainder theorem the pairing

$$(\cdot,\cdot)_{F,m} : F^* \times F^* \to \mu_m$$

is uniquely determined by the two pairings

$$(\cdot,\cdot)_{F,m_1} : F^* \times F^* \to \mu_{m_1} \quad \text{and} \quad (\cdot,\cdot)_{F,m_2} : F^* \times F^* \to \mu_{m_2}.$$

3.6 A new elementary characterization

In this section we show that the norm-residue symbol can be characterized in an elementary way. The formulation of Theorem 3.80 does not use local class field theory.

Definition 3.78 (Second K-group)**.** Let F be a field. The *second K-group* of F is the group

$$K_2F = (F^* \otimes_{\mathbb{Z}} F^*)/\langle a \otimes b : a + b = 1\rangle.$$

The following theorem about the structure of K_2F is very important from both a theoretical and a computational point of view. The proof of this theorem, as found in [48] by Milnor, was used in [13] by Daberkow to give an algorithm for computing the norm-residue symbol.

Theorem 3.79 (Moore)**.** *Let F be a non-Archimedean local field and let n be the number of roots of unity in F. Then the group K_2F is the direct sum of a cyclic group of order n and a divisible group $(K_2F)^n$.*

Proof. See Theorem A.14 of Appendix in [48] by Milnor. □

In [48] by Milnor elementary arguments show that the group $K_2F/(K_2F)^n$ is cyclic. Local class field theory, in particular the existence of the norm-residue symbol, is used to prove that $K_2F/(K_2F)^n$ is of order n.

Theorem 3.80 (Elementary characterization of the norm-residue symbol)**.** *Let m be a positive integer, let F be a local field containing a primitive m-th root of unity, and let μ_m be the group of m-th roots of unity in F. Then the m-th power norm-residue symbol is the unique pairing*

$$(\cdot,\cdot) : F^* \times F^* \to \mu_m$$

with the following properties.

(a) *If a and b are elements in F^* satisfying the equality $a+b=1$, then one has $(a,b)=1$.*

(b) *If F is non-Archimedean, the elements a and b are in F^*, and the extension $F(\beta)/F$ is unramified, where $\beta^m = b$ with β in an algebraic closure of F, then one has*

$$(a,b) = \mathrm{Fr}^{\mathrm{v}_F(a)}(\beta)/\beta,$$

where Fr *is the Frobenius element in* $\mathrm{Gal}(F(\beta)/F)$ *and* $\mathrm{v}_F : F \to \mathbb{Z} \cup \{+\infty\}$ *is the normalized valuation on F.*

(c) *If F is isomorphic to $\mathbb{R}$, then the map $(\cdot,\cdot)$ is surjective.*

Proof. Firstly, by Theorem 3.69 the norm-residue symbol is a pairing

$$(\cdot,\cdot) : F^* \times F^* \to \mu_m.$$

Secondly, we have to prove that the norm-residue symbol satisfies the three conditions. By Theorem 3.74 we immediately see that the first condition is satisfied. The second and the third properties follow from the explicit expression of the norm-residue maps in these particular cases. In fact, if F is non-Archimedean, the elements a and b are in F^*, and the extension $F(\beta)/F$ is unramified, where $\beta^m = b$ with β in an algebraic closure of F, Property (c) in Theorem 3.57 gives

$$\psi_{F(\beta)/F}(a) = \mathrm{Fr}^{\mathrm{v}_F(a)}$$

and by definition of the norm-residue symbol we get

$$(a,b) = \mathrm{Fr}^{\mathrm{v}_F(a)}(\beta)/\beta.$$

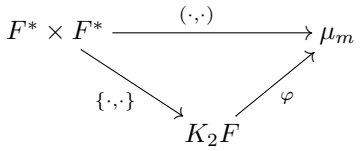
Now we consider the case when F is isomorphic to $\mathbb{R}$. The integer m is equal either to 1 or to 2. If m is 1, then the map $(\cdot,\cdot)$ is trivially surjective. If m is equal to 2, the surjectivity of the norm-residue map $\psi_{\mathbb{R}} : \mathbb{R}^* \to \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ implies

$$(-1,-1) = \psi_{\mathbb{R}}(-1)(\mathrm{i})/\mathrm{i} = -\mathrm{i}/\mathrm{i} = -1,$$

where $\mathrm{i}^2 = -1$ with $\mathrm{i} \in \mathbb{C}$. This proves that the norm-residue symbol is surjective.

Finally, we need to prove the uniqueness of this map. Suppose that F is a non-Archimedean local field. By Definition 3.78 it follows that for any pairing

$(\cdot,\cdot) : F^* \times F^* \to \mu_m$ with the first property there exists one and only one homomorphism $\varphi : K_2F \to \mu_m$ that carries for all $a, b \in F^*$ the image $\{a, b\}$ of (a, b) in K_2F to the norm-residue symbol (a, b). This means that the diagram



commutes. Theorem 3.79 implies that $K_2F/(K_2F)^m$ is a cyclic group of order m. The homomorphism φ has to be trivial on $(K_2F)^m$ and therefore there are only m such homomorphisms.

By Theorem 3.56 the Galois group of an unramified extension of non-Archimedean local field is cyclic and generated by the Frobenius element. If we choose $a, b \in F^*$ such that $\mathrm{v}_F(a) = 1$ and the extension $F(\beta)/F$ is unramified of degree m, where $\beta^m = b$ with β in an algebraic closure of F, then the norm-residue symbol (a, b) is a primitive m-th root of unity. To see that such a b exists, we can consider the unramified extension generated by adjoining to F a root of a polynomial of degree m with coefficients in F that is irreducible over the residue field of F. By Theorem 3.44 of Kummer theory this extension is of the form $F(\beta)/F$, where $\beta^m \in F$ with β in an algebraic closure of F. Hence $\{a, b\}$ generates $K_2F/(K_2F)^m$ and Property (b) fixes the homomorphism φ. The case when F is Archimedean is in the following section. □

3.7 Archimedean local fields

Let F be an Archimedean local field. By Theorem 3.16 the field F is isomorphic either to $\mathbb{C}$ or to $\mathbb{R}$. We will prove that the norm-residue symbol is the unique pairing

$$(\cdot,\cdot) : F^* \times F^* \to \mu_m$$

having the properties of Theorem 3.80.

Since every element of $\mathbb{C}$ is an m-th power, the norm-residue symbol is the trivial map if we have $F \cong \mathbb{C}$. Now suppose $F \cong \mathbb{R}$. Since there are only two roots of unity in $\mathbb{R}$, namely the elements 1 and -1, we have only two possible values for m: either $m = 1$ or $m = 2$. For $m = 1$ the first power norm-residue symbol is again the trivial map, because its image is the trivial group. For $m = 2$ we have a pairing

$$(\cdot,\cdot) : \mathbb{R}^*/\mathbb{R}_{>0} \times \mathbb{R}^*/\mathbb{R}_{>0} \longrightarrow \langle -1 \rangle.$$

Since by Property (c) in Theorem 3.80 this map is surjective and $\mathbb{R}^* \otimes \mathbb{R}^*$

modulo squares has order 2, for all $a, b \in \mathbb{R}^*$ we get

$$(a,b) = \begin{cases} -1 & \text{if } a < 0 \text{ and } b < 0, \\ 1 & \text{otherwise.} \end{cases}$$

Theorem 3.81. *The triple $(\mathbb{R}^*/\mathbb{R}_{>0}, \langle -1 \rangle, (\cdot,\cdot))$ is a skew abelian group of order 2 and its skew element is $-1 \cdot \mathbb{R}_{>0}$.*

Proof. The result follows from the explicit description of the norm-residue symbol for Archimedean local fields in Section 3.7. □

3.8 Non-Archimedean local fields

Theorem 3.82. *Let m be a positive integer, let F be a non-Archimedean local field containing a primitive m-th root of unity, let μ_m be the group of m-th roots of unity in F, and let $(\cdot,\cdot)_{F,m} : F^*/F^{*m} \times F^*/F^{*m} \to \mu_m$ be the pairing induced by the m-th power norm-residue symbol. Then the triple $(F^*/F^{*m}, \mu_m, (\cdot,\cdot)_{F,m})$ is a skew abelian group with the following properties.*

(a) *Its skew element is $-1 \cdot F^{*m}$.*

(b) *It is a symplectic abelian group if and only if one has $-1 \in F^{*m}$.*

(c) *If the characteristic of F is positive, then one has a group isomorphism*

$$F^*/F^{*m} \cong (\mathbb{Z}/m\mathbb{Z})^2.$$

(d) *If the characteristic of F is 0, then one has a group isomorphism*

$$F^*/F^{*m} \cong (\mathbb{Z}/m_p\mathbb{Z})^2 \oplus (\mathbb{Z}/p^{\mathrm{v}_p(m)}\mathbb{Z})^{d+2},$$

where p is the characteristic of the residue field of F, $m_p = m/p^{\mathrm{v}_p(m)}$, and $d = [F : \mathbb{Q}_p]$.

(e) *Its 2-rank is 0 if one has $m \not\equiv 0 \bmod 2$.*

(f) *Its 2-rank is 2 if one has $m \equiv 0 \bmod 2$ and the characteristic of the residue field of F is odd.*

(g) *Its 2-rank is $[F : \mathbb{Q}_2] + 2$ if one has $m \equiv 0 \bmod 2$, the characteristic of F is 0, and the characteristic of the residue field of F is 2.*

Proof. Since the norm-residue symbol is an antisymmetric pairing, by Theorem 3.70 the triple $(F^*/F^{*m}, \mu_m, (\cdot,\cdot)_{F,m})$ is a skew abelian group.

(a) This follows from Corollary 3.75.

(b) This follows from (a) and Theorem 2.15.

(c) This follows from Theorem 3.37 and Theorem 3.39.

(d) This follows from 3.37 and Theorem 3.38.

The statements about the 2-rank follow from the isomorphisms in (c) and (d). □

Definition 3.83 (Conductor)**.** Let F/E be an abelian extension of non-Archimedean local fields, let $n \in \mathbb{Z}_{\geq 0}$ be the smallest integer such that $U_E^{(n)} \subseteq \mathrm{N}_{F/E}\, F^*$, where $U_E^{(n)}$ is the n-th higher unit group of E, and let $\mathfrak{P}_E$ be the maximal ideal of the ring of integers of E. The *conductor* $\mathfrak{f}$ of F/E is the ideal

$$\mathfrak{f} = \mathfrak{P}_E^n.$$

Theorem 3.84. *Let F/E be an unramified extension of non-Archimedean local fields and for each $n \in \mathbb{Z}_{\geq 0}$ let $U_E^{(n)}$ and $U_F^{(n)}$ be the n-th higher unit groups of the rings of integers of E and of F, respectively. Then for each $n \in \mathbb{Z}_{\geq 0}$ one has*

$$\mathrm{N}_{F/E}\, U_F^{(n)} = U_E^{(n)}.$$

Proof. See Corollary 1.4 of Chapter III in [50] by Neukirch. □

Theorem 3.85. *An abelian extension F/E of non-Archimedean local fields is unramified if and only if its conductor $\mathfrak{f}$ is equal to $1 = \mathfrak{P}_E^0$, where $\mathfrak{P}_E$ is the maximal ideal of the ring of integers of E.*

Proof. See Proposition 3.4 of Chapter III in [50] by Neukirch. □

Theorem 3.86. *Let m be a positive integer, let F be a non-Archimedean local field containing a primitive m-th root of unity, let U_F be the group of units of the ring of integers of F, and let $b \in F^*$. Then the following are equivalent.*

(i) *The extension $F(\beta)/F$ is unramified, where $\beta^m = b$ with β in an algebraic extension of F.*

(ii) *For all $a \in U_F$ one has $(a, b) = 1$.*

Proof. (i) $\Longrightarrow$ (ii) If $F(\beta)/F$ is unramified, then by (b) in Theorem 3.80 for all $a \in U_F$ we have

$$(a, b) = \mathrm{Fr}^{\mathrm{v}_F(a)}(\beta)/\beta = \mathrm{Fr}^0(\beta)/\beta = 1.$$

(i) $\Longrightarrow$ (ii) Now suppose $(a, b) = 1$ for all $a \in U_F$. From Lemma 3.72 we obtain that a is contained in $\mathrm{N}_{F(\beta)/F}\, F(\beta)^*$. Hence, we have

$$U_F \subseteq \mathrm{N}_{F(\beta)/F}\, F(\beta)^*,$$

that is, the conductor of the extension $F(\beta)/F$ is 1. By Theorem 3.85 the extension $F(\beta)/F$ is unramified. □

Lemma 3.87. *Let m be a positive integer, let F be a non-Archimedean local field, and let $a \in F^*$. If the extension $F(\alpha)/F$ is unramified, where $\alpha^m = a$ with α in an algebraic extension of F, then one has*

$$\mathrm{v}_F(a) \equiv 0 \bmod m,$$

where $\mathrm{v}_F : F \to \mathbb{Z} \cup \{+\infty\}$ is the normalized valuation on F.

Proof. Suppose that the extension $F(\alpha)/F$ is unramified. By Theorem 3.53 the normalized valuation $\mathrm{v}_{F(\alpha)}$ on $F(\alpha)$ restricted to F equals the normalized valuation v_F on F. From the equality $\alpha^m = a$, we get

$$\mathrm{v}_F(a) = \mathrm{v}_{F(\alpha)}(a) = \mathrm{v}_{F(\alpha)}(\alpha^m) = m\,\mathrm{v}_{F(\alpha)}(\alpha) \equiv 0 \bmod m.$$

This concludes the proof. □

Remark 3.88. Let m be a positive integer, let F be a non-Archimedean local field, and let U_F be the group of units of the ring of integers of F. Since we have $U_F^m = F^{*m} \cap U_F$, the second isomorphism theorem for groups gives the isomorphism $U_F F^{*m}/F^{*m} \cong U_F/U_F^m$. Hence, we may consider U_F/U_F^m as a subgroup of F^*/F^{*m}.

Theorem 3.89. *Let m be a positive integer, let F be a non-Archimedean local field containing a primitive m-th root of unity, and let μ_m be the group of m-th roots of unity in F. Let U_F be the group of units of the ring of integers of F and let $(U_F/U_F^m)^\perp$ be the annihilator in F^*/F^{*m} of U_F/U_F^m with respect to pairing*

$$(\cdot,\cdot) : F^*/F^{*m} \times F^*/F^{*m} \longrightarrow \mu_m$$

induced by the norm-residue symbol. Then the group $(U_F/U_F^m)^\perp$ is cyclic of order m and is a subgroup of U_F/U_F^m of index $|m|^{-1}$, where $|\cdot| : F \to \mathbb{R}_{\geq 0}$ is the normalized absolute value on F.

Proof. Theorem 3.86 states that any m-th root of an element $a \in F^*$ that is mapped into $(U_F/U_F^m)^\perp$ by the projection $F^* \to F^*/F^{*m}$ generates an unramified extension of F. By Lemma 3.87 we have $\mathrm{v}_F(a) \equiv 0 \mod m$, that is, the element a is mapped into U_F/U_F^m. Therefore, we obtain the inclusion $(U_F/U_F^m)^\perp \subseteq U_F/U_F^m$.

Theorem 3.37 implies that U_F/U_F^m is an index m subgroup of F^*/F^{*m} and the quotient group $(F^*/F^{*m})/(U_F/U_F^m)$ is cyclic of order m. Since the induced pairing is a perfect, the group $(U_F/U_F^m)^\perp$ is cyclic of order m. By Theorem 3.71 the group $(U_F/U_F^m)^\perp$ is an index $|m|^{-1}$ subgroup of U_F/U_F^m. □

Corollary 3.90. *Let $U_F^\perp$ be the annihilator in U_F of U_F with respect to the norm-residue symbol. Then one has the equality $(U_F/U_F^m)^\perp = U_F^\perp/U_F^m$ and the norm-residue symbol induces a perfect pairing*

$$(\cdot,\cdot) : U_F/U_F^\perp \times U_F/U_F^\perp \to \mu_m.$$

Proof. Since we have $U_F^m = F^{*m} \cap U_F^\perp$, we may also consider $U_F^\perp/U_F^m$ as a subgroup of F^*/F^{*m}. From the inclusion $(U_F/U_F^m)^\perp \subseteq U_F/U_F^m$ of Theorem 3.89 we obtain the equality $(U_F/U_F^m)^\perp = U_F^\perp/U_F^m$. Taking the quotient $(U_F/U_F^m)/(U_F/U_F^m)^\perp$ we get the induced perfect pairing. □

The present situation is summarized in the following diagram.

$$\begin{array}{c} F^*/F^{*m} \\ \Big| m \\ U_F/U_F^m \\ \Big| |m|^{-1} \\ (U_F/U_F^m)^\perp = U_F^\perp/U_F^m \\ \Big| m \\ 1 \end{array}$$

Corollary 3.91. *Let $U_F^\perp$ be the annihilator in U_F of U_F with respect to the norm-residue symbol. Then one has the following.*

(a) *There is a group isomorphism $U_F^\perp/U_F^m \cong \mathbb{Z}/m\mathbb{Z}$.*

(b) *If the characteristic of F is positive, then the group $U_F/U_F^\perp$ is trivial.*

(c) *If the characteristic of F is 0, then one has a group isomorphism*

$$U_F/U_F^\perp \cong (\mathbb{Z}/p^{\mathrm{v}_p(m)}\mathbb{Z})^d,$$

where p is the characteristic of the residue field of F and $d = [F : \mathbb{Q}_p]$.

Proof. (a) By Theorem 3.37 we get $F^*/(U_F F^{*m}) \cong \mathbb{Z}/m\mathbb{Z}$. Since the finite group $(U_F/U_F^m)^\perp$ is the dual of $F^*/(U_F F^{*m})$ with respect to a perfect pairing, by Theorem 2.17 we have $(U_F/U_F^m)^\perp \cong F^*/(U_F F^{*m})$. From the equality $(U_F/U_F^m)^\perp = U_F^\perp/U_F^m$ of Corollary 3.90 we obtain an isomorphism

$$U_F^\perp/U_F^m \cong \mathbb{Z}/m\mathbb{Z}.$$

(b) If the characteristic of F is positive, then we have $|m| = 1$, where $|\cdot| : F \to \mathbb{R}_{\geq 0}$ is the normalized absolute value on F. The result follows from Theorem 3.89 and Corollary 3.90.

(c) Suppose that the characteristic of F is 0. Theorem 3.38 gives an isomorphism

$$U_F/U_F^m \cong \mathbb{Z}/m\mathbb{Z} \oplus (\mathbb{Z}/p^{\mathrm{v}_p(m)}\mathbb{Z})^d.$$

Since $U_F^\perp/U_F^m$ is a cyclic subgroup of U_F/U_F^m of maximal order, the exact sequence

$$1 \to U_F^\perp/U_F^m \to U_F/U_F^m \to U_F/U_F^\perp \to 1$$

splits. An isomorphism

$$U_F/U_F^\perp \cong (\mathbb{Z}/p^{\mathrm{v}_p(m)}\mathbb{Z})^d$$

follows from the splitting of the exact sequence. □

Corollary 3.92. *Let m be a positive integer, let F be a non-Archimedean local field containing a primitive m-th root of unity, let μ_m be the group of m-th roots of unity in F, let p be the characteristic of the residue field of F, let U_F be the group of units of the ring of integers of F, and let $U_F^{\perp}$ be the annihilator in U_F of U_F with respect to the norm-residue symbol $(\cdot,\cdot)_{F,m} : F^* \times F^* \to \mu_m$. Then the triple $(U_F/U_F^{\perp}, \mu_m, (\cdot,\cdot)_{F,m})$ is a skew abelian group with the following properties.*

(a) *Its skew element is $-1 \cdot U_F^{\perp}$.*

(b) *It is a symplectic abelian group if and only if the extension $F(\sqrt[m]{-1})/F$ is unramified.*

(c) *It is the trivial group if and only if the characteristic of F is positive or one has $m \not\equiv 0 \bmod p$.*

(d) *Its 2-rank equals 0 if $p \neq 2$.*

(e) *Its 2-rank equals $[F : \mathbb{Q}_p]$ if $p = 2$, the characteristic of F is 0, and $m \equiv 0 \bmod 2$.*

Proof. Since the norm-residue symbol is an antisymmetric pairing, Corollary 3.90 implies that the triple $(U_F/U_F^{\perp}, \mu_m, (\cdot,\cdot)_{F,m})$ is a skew abelian group. Corollary 3.75 gives (a). Now Theorem 2.15 and Theorem 3.86 imply (b). By Theorem 3.89 and Corollary 3.90 the cardinality of $U_F/U_F^{\perp}$ equals $|m|^{-1}$, where $|\cdot| : F \to \mathbb{R}_{\geq 0}$ is the normalized absolute value on F. Hence (c) and (d) follow. Corollary 3.91 gives (e). □

Corollary 3.93. *Let m be a positive integer, let F be a non-Archimedean local field of characteristic zero containing a primitive m-th root of unity, let p the characteristic of the residue field of F, let U_F be the group of units of the ring of integers of F, and let $n = p^{\mathrm{v}_p(m)}$. Let $U_{F,m}^{\perp}$ and $U_{F,n}^{\perp}$ be the annihilators in U_F of U_F with respect to the m-th power norm-residue symbol and to the n-th power norm-residue symbol, respectively. Then one has the equality $U_{F,m}^{\perp} = U_{F,n}^{\perp}$ and the pair (φ, ψ) of group isomorphisms*

$$\begin{aligned} \varphi : U_F/U_{F,m}^{\perp} &\to U_F/U_{F,n}^{\perp}, & \psi : \mu_m^{m/n} &\to \mu_n, \\ a \cdot U_{F,m}^{\perp} &\mapsto a \cdot U_{F,n}^{\perp}, & \zeta &\mapsto \zeta^{m/n}, \end{aligned}$$

is a similarity of skew abelian groups from $(U_F/U_{F,m}^{\perp}, \mu_m, (\cdot,\cdot)_{F,m})$ to $(U_F/U_{F,n}^{\perp}, \mu_n, (\cdot,\cdot)_{F,n})$, where μ_m and μ_n are the groups of m-th roots of unity in F and of n-th roots of unity in F, respectively.

Proof. By Theorem 3.76 we have the inclusion $U_{F,m}^{\perp} \subseteq U_{F,n}^{\perp}$. Hence, there is a natural projection $\varphi : U_F/U_{F,m}^{\perp} \to U_F/U_{F,n}^{\perp}$. Since it is a surjective group homomorphism and by Corollary 3.91 is a map between two group of the same cardinality, it is a group isomorphism. This proves the equality $U_{F,m}^{\perp} = U_{F,n}^{\perp}$.

Let χ be the group homomorphism $\chi : \mu_m \to \mu_n$, $\zeta \mapsto \zeta^{m/n}$. By Theorem 3.76 the diagram

$$\begin{array}{ccc} U_F/U_{F,m}^{\perp} \times U_F/U_{F,m}^{\perp} & \xrightarrow{(\cdot,\cdot)_{F,m}} & \mu_m \\ \varphi \downarrow \quad \varphi \downarrow & & \chi \downarrow \\ U_F/U_{F,n}^{\perp} \times U_F/U_{F,n}^{\perp} & \xrightarrow{(\cdot,\cdot)_{F,n}} & \mu_n \end{array}$$

commutes. Since by Corollary 3.91 the group $U_F/U_{F,m}^{\perp}$ is a p-group, the image of $(\cdot,\cdot)_{F,m}$ is contained in μ_n. It equals $\mu_m^{m/n}$, because by Corollary 3.90 the pairing $(\cdot,\cdot)_{F,m} : U_F/U_{F,m}^{\perp} \times U_F/U_{F,m}^{\perp} \to \mu_m$ is perfect and by Corollary 3.91 the group $U_F/U_{F,m}^{\perp}$ contains an element of order n. Hence $\psi = \chi|_{\mu_m^{m/n}}$ is a group isomorphism between the images of $(\cdot,\cdot)_{F,m}$ and $(\cdot,\cdot)_{F,n}$. We conclude that the pair (φ, ψ) is a similarity of skew abelian groups. □

Theorem 3.94. *Let F be a non-Archimedean local field with residue field $\mathbb{F}$ and let $f(X)$ be a monic polynomial over the ring of integers of F whose residue class in $\mathbb{F}[X]$ is a monic separable polynomial over $\mathbb{F}$. Let α be a root of $f(X)$ in an algebraic closure of F. Then the extension $F(\alpha)/F$ is unramified.*

Proof. See (ii) of Proposition 1 in Section 7 of Chapter I in [9] by Cassels and Fröhlich or Proposition 3.2 of Chapter II in [15] by Fesenko and Vostokov. □

Theorem 3.95. *Let p be a prime number, let ζ_p be a primitive p-th root of unity, and let F be a finite extension of $\mathbb{Q}_p(\zeta_p)$. Let $\mathfrak{P}$ be the maximal ideal of the ring of integers $\mathcal{O}_F$ of F and let $\lambda = 1 - \zeta_p$. Let $a \in F^*$ and let α be an element in an algebraic closure of F with $\alpha^p = a$. Then one has the following.*

(a) *The extension $F(\alpha)/F$ is unramified if and only if $a \in (1+\lambda^p\mathcal{O}_F) \cdot F^{*p}$.*

(b) *The extension $F(\alpha)/F$ is unramified of degree p if and only if there exists $c \in \mathcal{O}_F$ such that $\mathrm{Tr}_{(\mathcal{O}_F/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z})}\, \overline{c} \neq 0$ and $a \in (1 + c\lambda^p) \cdot F^{*p}$, where $\overline{c}$ is the reduction modulo $\mathfrak{P}$ of c and $\mathrm{Tr}_{(\mathcal{O}_F/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z})}$ is the trace map from $\mathcal{O}_F/\mathfrak{P}$ to $\mathbb{Z}/p\mathbb{Z}$.*

To prove Theorem 3.95 we will use Lemma 3.96. For a different proof of the lemma see [66] and Exercise 9.4 in [74].

Lemma 3.96. *One has*

$$\frac{\lambda^{p-1}}{p} \equiv -1 \bmod \lambda\mathcal{O}_F.$$

Proof. The case $p = 2$ is trivial. Setting X equal to λ in the equality

$$\sum_{i=0}^{p-1}(1-X)^i = \frac{(1-X)^p - 1}{-X} = (-X)^{p-1} + pXf + p,$$

where f a polynomial in X with integer coefficients, we get

$$0 = \sum_{i=0}^{p-1} \zeta_p^i \equiv (-\lambda)^{p-1} + p \bmod p\lambda\mathcal{O}_F.$$

Since we have $(-\lambda)^{p-1} = \lambda^{p-1}$ if p is odd, dividing by p gives us the desired result. □

Proof (of Theorem 3.95*).* Let $b \in \mathcal{O}_F$ with $b \equiv 1 \bmod \lambda^p\mathcal{O}_F$. We can write $b = 1 + \lambda^p c$ with $c \in \mathcal{O}_F$. Let $x = (\beta - 1)/\lambda$, where β is in an algebraic closure of F and $\beta^p = b$. From the identity

$$(1 + \lambda x)^p = b$$

we obtain

$$x^p + \left(\sum_{i=1}^{p-1} \binom{p}{i} \frac{(\lambda x)^i}{\lambda^p} \right) + \frac{1-b}{\lambda^p} = 0.$$

Let $f(X)$ be the polynomial

$$f(X) = X^p + \left(\sum_{i=2}^{p-1} \binom{p}{i} \frac{(\lambda X)^i}{\lambda^p} \right) + \frac{\lambda p X}{\lambda^p} - c$$

in $F[X]$. All coefficients of the terms of degree d with $2 \le d \le p-1$ are in $\mathfrak{P}$. By Lemma 3.96 we know $\frac{\lambda^{p-1}}{p} \equiv -1 \bmod \lambda\mathcal{O}_F$. Hence x is a root of a polynomial $f(X) \in \mathcal{O}_F[X]$ such that $f(X) \equiv X^p - X - \overline{c} \bmod \mathfrak{P}$, where $\overline{c}$ is the reduction modulo $\mathfrak{P}$ of c. Since we have $f'(X) \equiv -1 \bmod \mathfrak{P}$, by Theorem 3.94 the extension $F(x)/F = F(\beta)/F$ is unramified. This proves that if we have $a \in (1 + \lambda^p\mathcal{O}_F) \cdot F^{*p}$ then the extension $F(\alpha)/F$ is unramified.

The Artin–Schreier polynomial $X^p - X - \overline{c} \in (\mathcal{O}_F/\mathfrak{P})[X]$ splits into linear factors, which is equivalent by Hensel's lemma to the extension $F(\beta)/F$ being trivial, if and only if we have $\mathrm{Tr}_{(\mathcal{O}_F/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z})}\, \overline{c} = 0$. Otherwise, it is irreducible and the extension $F(\beta)/F$ has degree p. This proves the if part of (b).

Now assume $\mathrm{Tr}_{(\mathcal{O}_F/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z})}\, \overline{c} \neq 0$. The uniqueness of unramified extensions of given degree and Kummer theory imply that the extension $F(\alpha)/F$ is unramified if and only if we have $a \in \langle b \rangle \cdot F^{*p}$. Since for every $n \in \mathbb{Z}$ we have $b^n \equiv 1 \bmod \lambda^p\mathcal{O}_F$, we get (a). Moreover, the extension $F(\alpha)/F$ is unramified of degree p if and only if we have $a \in b^n \cdot F^{*p}$ with $n \in \mathbb{Z} \setminus p\mathbb{Z}$. Since for every $n \in \mathbb{Z} \setminus p\mathbb{Z}$ we have $b^n \equiv 1 + \lambda^p nc \bmod \lambda^{p+1}\mathcal{O}_F$ and $\mathrm{Tr}_{(\mathcal{O}_F/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z})}\, \overline{nc} \neq 0$, we get (b). □

Lemma 3.97. *Let p be a prime number, let ζ_p be a primitive p-th root of unity, let F be a finite extension of $\mathbb{Q}_p(\zeta_p)$, let e be the normalized valuation $\mathrm{v}_F(p)$,*

let $e_0 = e/(p-1)$, and for each $n \in \mathbb{Z}_{>0}$ let $U^{(n)}$ be the n-th higher unit group of the ring of integers of F. Then for each integer $i > e_0$ the p-th power group homomorphism $F^* \to F^*$, $a \mapsto a^p$, induces an isomorphism $U^{(i)} \xrightarrow{\sim} U^{(i+e)}$.

Proof. See Lemma A.4 of Appendix in [48] by Milnor. □

Lemma 3.98. *Let p be a prime, let n be a positive integer, and let $m = p^n$. Let ζ_p and ζ_m be a primitive p-th root of unity and a primitive m-th root of unity, respectively. Let F be a finite extension of $\mathbb{Q}_p(\zeta_m)$, let $\mathcal{O}_F$ be the ring of integers of F, and let $\lambda = 1 - \zeta_p$. Let $a \in F$ with $a \equiv 1 \bmod p^n\lambda\mathcal{O}_F$ and let α be an element in an algebraic closure of F with $\alpha^{p^n} = a$. Then the extension $F(\alpha)/F$ is unramified of degree dividing p.*

Proof. By Lemma 3.97 the p^{n-1}-th power group homomorphism $F^* \to F^*$, $x \mapsto x^{p^{n-1}}$, induces an isomorphism $U^{(e_0+e)} \xrightarrow{\sim} U^{(e_0+ne)}$, where $e = \mathrm{v}_F(p)$ and $e_0 = e/(p-1) = \mathrm{v}_F(\lambda)$. We choose $\beta \in \alpha \cdot \langle\zeta_m\rangle$ with $\beta^p \in F^*$ and $\beta^p \equiv 1 \bmod p\lambda\mathcal{O}_K$. It exists, because we have $\mathrm{v}_F(a-1) \geq e_0 + ne$. The equality $F(\alpha) = F(\beta)$ shows that it is sufficient to prove that the extension $F(\beta)/F$ is unramified of degree dividing p. Theorem 3.95 implies that the extension $F(\beta)/F$ is unramified. It is of degree dividing p, because we have $\beta^p \in F^*$ and $\zeta_p \in F$. □

Lemma 3.99 (Bouw [7])**.** *Let p be a prime, let n be a positive integer, and let $m = p^n$. Let ζ_p and ζ_m be a primitive p-th root of unity and a primitive m-th root of unity, respectively, and let $\lambda = 1 - \zeta_p$. Let F be a finite extension of $\mathbb{Q}_p(\zeta_m)$, let $\mathrm{v}_F : F \to \mathbb{Z} \cup \{+\infty\}$ be the normalized valuation on F, and let E/F be an unramified extension of non-Archimedean local fields of degree m. Then there exists $\alpha \in E^*$ such that $\alpha^m \in F^*$, $E = F(\alpha)$, and $\mathrm{v}_F(\alpha^m - 1) = \mathrm{v}_F(p\lambda)$.*

Proof. Let $K/\mathbb{Q}_p$ be the maximal unramified extension of $\mathbb{Q}_p$ that is contained in F and let $L = K(\zeta_m)$. Let M/L be the maximal unramified extension of L that is contained in E. Since the extension E/F is unramified of degree m and F/E is totally ramified, the extension M/L is unramified of degree m. By Kummer theory there is $\alpha \in M$ such that $\alpha^m \in L^*$ and $M = L(\alpha)$. Moreover, we have $E = F(\alpha)$. By Lemma 3.87 we can assume $\mathrm{v}_M(\alpha) = 0$. Since every root of unity of order coprime to p is an m-th power, we can assume $\mathrm{v}_M(\alpha - 1) \geq 1$. By Theorem 3.53 the normalized valuation v_M on M restricted to L equals the normalized valuation v_L on L. Since we have $\alpha^m - 1 = \prod_{i=0}^{m-1}(\alpha\zeta_m^i - 1)$ and $\mathrm{v}(\zeta_m - 1) \geq 1$, we get

$$\mathrm{v}_L(\alpha^m - 1) = \mathrm{v}_M(\alpha^m - 1) = \sum_{i=0}^{m-1} \mathrm{v}_M(\alpha\zeta_m^i - 1) \geq m.$$

Since we have $\alpha^m \notin L^{*p}$, Theorem 3.95 gives $\mathrm{v}_L(\alpha^m - 1) \leq \mathrm{v}_L(\lambda^p)$. We obtain

$$\mathrm{v}_L(\alpha^m - 1) \leq \mathrm{v}_L(\lambda^p) = m\,\mathrm{v}_L(1 - \zeta_m) = m,$$

because the extension $L/\mathbb{Q}_p(\zeta_m)$ is unramified and $1-\zeta_m$ is a prime element of $\mathbb{Q}_p(\zeta_m)$. Hence, we get $\mathrm{v}_L(\alpha^m-1) = m = \mathrm{v}_L(\lambda^p)$. Lemma 3.96 implies $\mathrm{v}_L(\lambda^{p-1}) = \mathrm{v}_L(p)$ and therefore we have $\mathrm{v}_L(\alpha^m-1) = \mathrm{v}_L(p\lambda)$. The equality $\mathrm{v}_F(\alpha^m-1) = \mathrm{v}_F(p\lambda)$ follows. □

3.9 Functorial properties

Theorem 3.100. *Let d and m be positive integers such that d divides m. Let F and E be local fields containing a primitive m-th root of unity and a primitive d-th root of unity, respectively. Let $\mu_m(F)$ and $\mu_d(E)$ be the groups of m-th and d-th roots of unity in F and in E, respectively, and let $\sigma : E \to F$ be a continuous homomorphism. Let $\sigma_* = \sigma|_{E^*} : E^* \to F^*$ and $\sigma^* = F^* \to E^*$ be the maps*

$$\sigma_* = \sigma|_{E^*} : E^* \to F^* \quad \text{and} \quad \sigma^* = \sigma^{-1} \circ \mathrm{N}_{F^*/\sigma E^*} : F^* \to E^*.$$

Then the maps $\sigma^* : F^* \to E^*$ and $(a \mapsto a^{m/d}) \circ \sigma_* : E^* \to F^*$ shown in the diagram

$$\begin{array}{ccc} F^* \times F^* & \xrightarrow{(\cdot,\cdot)_{F,m}} & \mu_m(F) \\ {\scriptstyle \sigma^*}\downarrow & \uparrow{\scriptstyle (a\mapsto a^{m/d})\circ\sigma_*} & \uparrow{\scriptstyle \sigma|_{\mu_d(E)}} \\ E^* \times E^* & \xrightarrow{(\cdot,\cdot)_{E,d}} & \mu_d(E) \end{array}$$

are adjoint with respect to the norm-residue symbol, that is, for all $a \in E^*$ and $b \in F^*$ one has

$$\sigma\left(\sigma^*(b), a\right)_{E,d} = \left(b, \sigma_*(a)^{m/d}\right)_{F,m}.$$

Proof. See Lemma 1 in Section 3.1 of Chapter IV in [28] by Iyanaga. □

Corollary 3.101. *Let m be a positive integer, let F be a local field containing a primitive m-th root of unity, and let $\sigma : F \to F$ be a continuous automorphism of F. Then, for all a, $b \in F^*$ one has*

$$(\sigma a, \sigma b) = \sigma\left(a, b\right).$$

Proof. Apply Theorem 3.100 with $E = F$ and $d = m$. □

3.10 The field of two-adic rationals and its unramified extensions

We present in a more explicit way the quadratic norm-residue symbol in the field $\mathbb{Q}_2$ of 2-adic rationals. For unramified extensions of $\mathbb{Q}_2$ we state and prove

Lemma 3.106.

Lemma 3.102. *Let $\mathbb{Q}_2$ be the field of 2-adic rationals, let $\mathbb{Z}_2$ be its ring of integers, let U be group of units of $\mathbb{Z}_2$, and for each $n \in \mathbb{Z}_{\geq 0}$ let $U^{(n)}$ be its n-th higher unit group. Then there is the equality*

$$\mathbb{Z}_2^{*2} = U^{(3)}.$$

Proof. By Theorem 3.37 we have the equalities

$$\mathbb{Z}_2^* = U = U^{(1)}.$$

Hence, if a is an element in $\mathbb{Z}_2^*$, we can write $a = 1 + 2x$ with $x \in \mathbb{Z}_2$. By squaring we obtain

$$a^2 = 1 + 4x(1 + x) \equiv 1 \bmod 8.$$

Since by definition we have $1 + 8\mathbb{Z}_2 = U^{(3)}$, we get $a^2 \in U^{(3)}$ and therefore the inclusion $\mathbb{Z}_2^{*2} \subseteq U^{(3)}$. Theorem 3.71 gives $[\mathbb{Z}_2^* : \mathbb{Z}_2^{*2}] = 4$. Since $U^{(3)}$ has also index 4 in $\mathbb{Z}_2^*$, we obtain the equality $\mathbb{Z}_2^{*2} = U^{(3)}$. □

Theorem 3.103. *Let $\mathbb{Q}_2$ be the field of 2-adic rationals and for every $a \in \mathbb{Q}_2^*$ let $\overline{a}$ be the residue class $a \bmod \mathbb{Q}_2^{*2}$ of a in $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$. Then the natural map*

$$\langle \overline{2} \rangle \times \langle \overline{-1} \rangle \times \langle \overline{5} \rangle \xrightarrow{\sim} \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$$

is a group isomorphism and each of the groups $\langle \overline{2} \rangle$, $\langle \overline{-1} \rangle$, and $\langle \overline{5} \rangle$ has order 2.

Proof. The split sequence of Theorem 3.37 gives the isomorphism

$$\mathbb{Q}_2^* \cong \langle 2 \rangle \times \mathbb{Z}_2^*.$$

By squaring and applying Lemma 3.102 we obtain the isomorphism

$$\mathbb{Q}_2^{*2} \cong \langle 4 \rangle \times U^{(3)}.$$

Taking the quotients we get the desired isomorphism. Since by definition we have $1 + 8\mathbb{Z}_2 = U^{(3)}$, each element in $\{\overline{2}, \overline{-1}, \overline{5}\}$ has nontrivial image in $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ and therefore each of the groups $\langle \overline{2} \rangle$, $\langle \overline{-1} \rangle$, and $\langle \overline{5} \rangle$ has order 2. □

Theorem 3.104. *Let $\mathbb{Q}_2$ be the field of 2-adic rationals and for every $a \in \mathbb{Q}_2^*$ let $\overline{a}$ be the residue class $a \bmod \mathbb{Q}_2^{*2}$ of a in $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$. Then the table*

$(\cdot,\cdot)$	$\overline{2}$	$\overline{-1}$	$\overline{5}$
$\overline{2}$	1	1	-1
$\overline{-1}$	1	-1	1
$\overline{5}$	-1	1	1

gives an explicit description of the perfect pairing

$$(\cdot,\cdot) : \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \times \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \to \{\pm 1\}$$

induced by the quadratic norm-residue symbol

$$(\cdot,\cdot)_{\mathbb{Q}_2,2} : \mathbb{Q}_2^* \times \mathbb{Q}_2^* \to \{\pm 1\}.$$

Proof. Using bilinearity of Theorem 3.69 and the relations of Theorem 3.74 we obtain the equalities

$$\begin{gathered}
1 = (1-2,2) = (-1,2), \\
1 = (1-5,5) = (4,5)(-1,5) = (2^2,5)(-1,5) = (2,5)^2(-1,5) = (-1,5), \\
1 = (-2,2) = (-1,2)(2,2) = (2,2), \\
1 = (-5,5) = (-1,5)(5,5) = (5,5), \\
1 = (-1,2)(2,-1) = (2,-1), \\
1 = (-1,5)(5,-1) = (5,-1).
\end{gathered}$$

Since by Theorem 3.70 the pairing induced by the norm-residue symbol is perfect, we get

$$(2,5) = (5,2) = (-1,-1) = -1. \qquad \square$$

Corollary 3.105. *Let $\mathbb{Q}_2$ be the field of 2-adic rationals and let U be the unit group of the ring of integers of $\mathbb{Q}_2$. Then the annihilator $U^\perp$ in U of U with respect to the norm-residue symbol $(\cdot,\cdot)_{\mathbb{Q}_2,2} : \mathbb{Q}_2 \times \mathbb{Q}_2 \to \{\pm 1\}$ is the second higher unit group $U^{(2)}$ of the ring of integers of $\mathbb{Q}_2$ and the perfect pairing*

$$(\cdot,\cdot) : U/U^\perp \times U/U^\perp \to \mu_2$$

induced by the norm-residue symbol is given by

$$\text{for } a,b \in \mathbb{Z}_2^* \quad (a,b) = \begin{cases} -1 \text{ if } a \equiv b \equiv 3 \bmod 4, \\ 1 \text{ otherwise.} \end{cases}$$

Proof. This follows from Theorem 3.104. $\square$

The diagram of Section 3.8 becomes the following one on the left. On the right

we show what each piece is canonically equal to.

$$\begin{array}{c} \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \\ \Big| \\ {\scriptstyle 2} \\ \Big| \\ U/U^2 \\ \Big| \\ {\scriptstyle |2|^{-1}=2} \\ \Big| \\ (U/U^2)^{\perp} \\ \Big| \\ {\scriptstyle 2} \\ \Big| \\ 1 \end{array} \qquad \begin{array}{c} \langle \overline{2} \rangle \times (\mathbb{Z}/8\mathbb{Z})^* \\ \Big| \\ {\scriptstyle \mathbb{Z}/2\mathbb{Z}} \\ \Big| \\ (\mathbb{Z}/8\mathbb{Z})^* \\ \Big| \\ {\scriptstyle (\mathbb{Z}/4\mathbb{Z})^*} \\ \Big| \\ \langle \overline{5} \rangle \\ \Big| \\ {\scriptstyle \mathbb{Z}/2\mathbb{Z}} \\ \Big| \\ 1 \end{array}$$

Lemma 3.106. *Let F be a finite unramified extension of the field $\mathbb{Q}_2$ of 2-adic rationals, let $\mathcal{O}_F$ be the ring of integers of F, let $\mathfrak{P}$ be the maximal ideal of $\mathcal{O}_F$, and let $(\cdot,\cdot)_F : F^* \times F^* \to \{\pm 1\}$ be the quadratic norm-residue symbol of F. Then for all $a, b \in \mathcal{O}_F$ one has*

$$(1+2a, 1+2b)_F = (-1)^{\mathrm{Tr}_{\mathfrak{P}}((a+\mathfrak{P})(b+\mathfrak{P}))}$$

with $\mathrm{Tr}_{\mathfrak{P}}$ denoting the trace map from $\mathcal{O}_F/\mathfrak{P}$ to $\mathbb{Z}/2\mathbb{Z}$.

Proof. Let U_F be the group of units of the ring of integers of F. Let $d \in 1+4\mathcal{O}_F$ and let δ be an element in an algebraic closure of F with $\delta^2 = d$. Since by Theorem 3.95 the extension $F(\delta)/F$ is unramified, Theorem 3.86 implies that for all $c \in U_F$ we have $(c, d) = 1$. Hence, we may assume $a, b \in U_F$ and therefore we have

$$\frac{1+2b}{1-4ab} \in F^* \setminus \{1\}.$$

By Theorem 3.74 for each $c \in F^* \setminus \{1\}$ one has $(1-c, c)_F = 1$. The equality

$$\left(\frac{-2b(1+2a)}{1-4ab}, \frac{1+2b}{1-4ab} \right)_F = 1$$

follows. Since the norm-residue symbol is an antisymmetric bilinear map and we have just proved that for all $c \in U_F$ we have $(c, 1-4ab) = 1$, we obtain the equality

$$(1+2a, 1+2b)_F = (1-4ab, 2)_F .$$

Let $(\cdot,\cdot)_{\mathbb{Q}_2} : \mathbb{Q}_2^* \times \mathbb{Q}_2^* \to \{\pm 1\}$ be the quadratic norm-residue symbol of $\mathbb{Q}_2$ and denote the norm map from F to $\mathbb{Q}_2$ by $\mathrm{N}_{F/\mathbb{Q}_2}$. Theorem 3.100 implies the equality

$$(1-4ab, 2)_F = \left(\mathrm{N}_{F/\mathbb{Q}_2}(1-4ab), 2\right)_{\mathbb{Q}_2} .$$

Since we have the congruence

$$\mathrm{N}_{F/\mathbb{Q}_2}(1-4ab) \equiv 1 - 4\,\mathrm{Tr}_{\mathfrak{P}}((a+\mathfrak{P})(b+\mathfrak{P})) \bmod 8,$$

the statement of Lemma 3.106 follows from Theorem 3.104. □