§3. Global CFT in terms of idèles

In this section K denotes a number field.

<u>Def.</u>: ring of adeles over K

$$\mathbb{A}_K = \{ \alpha = (\alpha_\mathfrak{p}) \in \prod_{\mathfrak{p} \in S_K} K_\mathfrak{p} \mid \alpha_\mathfrak{p} \in \mathcal{O}_{K,\mathfrak{p}} \text{ for almost all } \mathfrak{p} \in S_K^{<\infty} \}$$

$$= \bigcup_S \mathbb{A}_{K,S} \text{ with } \mathbb{A}_{K,S} = \prod_{\mathfrak{p} \in S} K_\mathfrak{p} \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_{K,\mathfrak{p}}$$

where S runs through the finite subsets of S_K containing S_K^∞.

There is a natural topology on $\mathbb{A}_K$ with a basis given by subsets of the form $\prod_{\mathfrak{p} \in S} W_\mathfrak{p} \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_{K,\mathfrak{p}}$ with $S \subseteq S_K$ finite, $S \supseteq S_K^\infty$, $W_\mathfrak{p} \subseteq K_\mathfrak{p}$ open nbhd. of 0 $\forall \mathfrak{p} \in S$

(This is <u>not</u> the product topology on $\prod_{\mathfrak{p} \in S_K} K_\mathfrak{p}$ restricted to $\mathbb{A}_K$. For instance, the subset $U = \prod_{\mathfrak{p} \in S_K^\infty} K_\mathfrak{p} \times \prod_{\mathfrak{p} \in S_K^{<\infty}} \mathcal{O}_{K,\mathfrak{p}}$ by definition open in $\mathbb{A}_K$, but not open w.r.t. the topology given by product topology. Otherwise there would be a finite subset $T \subseteq S_K$ and open nbh. $V_\mathfrak{p} \subseteq K_\mathfrak{p}$ of 0 $\forall \mathfrak{p} \in T$ s.t.

$$U \supseteq \Big(\prod_{\mathfrak{p} \in T} V_\mathfrak{p} \times \prod_{\mathfrak{p} \notin T} K_\mathfrak{p} \Big) \cap \mathbb{A}_K. \qquad (3)$$

Now choose some $\mathfrak{p}_0 \in S_K^{<\infty} \setminus T$ and define $\alpha = (\alpha_\mathfrak{p}) \in \mathbb{A}_K$ by $\alpha_\mathfrak{p} = \begin{cases} 0 & \mathfrak{p} \neq \mathfrak{p}_0 \\ \beta & \mathfrak{p} = \mathfrak{p}_0 \end{cases}$, where β is an arbitrary element in $K_\mathfrak{p} \setminus \mathcal{O}_{K,\mathfrak{p}}$. Then α lies in the right hand side of (3), but not in U.

<u>But</u>: If one restricts the topology on $\mathbb{A}_K$ to the

subrings of the form $\mathbb{A}_{K,S}$, one obtains the product topology on these subrings.

<u>Def.</u>: The <u>idèle group</u> I_K over K is the unit group of $\mathbb{A}_K$. As for $\mathbb{A}_K$, we have

$$I_K = \bigcup_S I_{K,S} \quad , \quad I_{K,S} = \prod_{\mathfrak{p}\in S} K_{\mathfrak{p}}^{\times} \times \prod_{\mathfrak{p}\notin S} \mathcal{O}_{K,\mathfrak{p}}^{\times}$$

$$(S \subseteq S_K \text{ finite}, \quad S \supseteq S_K^{\infty})$$

and a topology with a basis given by

$$\prod_{\mathfrak{p}\in S} W_{\mathfrak{p}} \times \prod_{\mathfrak{p}\notin S} \mathcal{O}_{K,\mathfrak{p}}^{\times} \qquad (4)$$

with open neighborhoods $W_{\mathfrak{p}}$ of 1 for all $\mathfrak{p} \in S$.
(This topology is strictly finer than the topology of $\mathbb{A}_K$ restricted to I_K. It is the coarsest top. on I_K such that the map $I_K \to \mathbb{A}_K \times \mathbb{A}_K$, $\alpha \mapsto (\alpha, \alpha^{-1})$ is continuous.)

<u>Remark</u>: Since $\mathcal{O}_{K,\mathfrak{p}}^{\times}$ is compact $\forall\, \mathfrak{p} \in S_K^{<\infty}$, by Tychonoff's theorem subsets of the form (4) are locally compact. Hence I_K is a <u>locally compact</u> topological group.

If we consider the different embeddings of some $\alpha \in K^{\times}$ into the completions $K_{\mathfrak{p}}^{\times}$, it turns out that $\alpha \in \mathcal{O}_{K,\mathfrak{p}}^{\times}$ for almost all $\mathfrak{p} \in S_K^{<\infty}$. Hence there is a canonical diagonal embedding $i: K^{\times} \hookrightarrow I_K$ which sends $\alpha \in K^{\times}$ to $(\alpha_{\mathfrak{p}})_{\mathfrak{p}\in S_K}$ with $\alpha_{\mathfrak{p}} = \alpha$ $\forall\, \mathfrak{p} \in S_K$. The factor group $C_K = I_K / K^*$ is called the <u>idèle class group</u> of K. Using the product formula $\prod_{\mathfrak{p} \in S_K} |\alpha|_\mathfrak{p} = 1 \quad \forall \alpha \in K^*$, one can show quite easily that the image of K^* in I_K is discrete and thus closed. So if one equips C_K with the quotient topology, one obtains a locally compact Hausdorff topological group.

<u>Def.</u>: Let $L|K$ be a finite extension of number fields. For every $\mathfrak{p} \in S_K$ we define $L_\mathfrak{p}^* = \prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}^*$. Every $\alpha_\mathfrak{p} \in L_\mathfrak{p}^*$ defines an Automorphism $\alpha_\mathfrak{p} : L_\mathfrak{p}^* \to L_\mathfrak{p}^*$, $x \mapsto \alpha_\mathfrak{p} x$ on $L_\mathfrak{p}$ as a $K_\mathfrak{p}^*$- vector space and we put

$$N_{L_\mathfrak{p}|K_\mathfrak{p}}(\alpha_\mathfrak{p}) = \det(\alpha_\mathfrak{p})$$

We thus get a homomorphism $N_{L_\mathfrak{p}|K_\mathfrak{p}} : L_\mathfrak{p}^* \to K_\mathfrak{p}^*$, and combining these maps for all $\mathfrak{p} \in S_K$ we obtain a homomorphism $N_{L|K} : I_L \to I_K$. The elements in $i(L^*)$ are mapped to $i(K^*)$, so that there is an induced map $N_{L|K} : C_L \to C_K$.

<u>Theorem</u> (global reciprocity law)

For every finite Galois extension $L|K$ of number fields there is a canonical surjective homomorphism

$(\cdot, L|K) : C_K \to Gal(L|K)^{ab}$ with kernel $N_{L|K} C_L$.

There is no obvious analogue of condition (a), but (b) to (d) also hold in the global case (with K^* replaced by C_K everywhere).

<u>Theorem</u> (global existence theorem)

Let K be a number field. There is a bijective correspondence $L \mapsto \mathcal{N}_L = N_{L|K} C_L$ between

(i) finite abelian extensions $L|K$

(ii) closed subgroups of C_K of finite index

For two such extensions $L_1|K$, $L_2|K$, the same conditions hold as in the local case.

The following theorem describes the relation between the local and the global reciprocity law.

<u>Theorem:</u> Let $L|K$ denote a finite abelian extension of number fields. Let $\mathfrak{p}$ be a prime of K and $\mathfrak{P}$ a prime of L such that $\mathfrak{P}|\mathfrak{p}$ (i.e. $\mathfrak{P} | \mathfrak{p}\mathcal{O}_L$ if $\mathfrak{p}$ is finite and $\tau|_L = \sigma$ if $\mathfrak{p} = \sigma$, $\mathfrak{P} = \{\tau, \bar\tau\}$ infinite primes). Then there is a commutative diagram

$$\begin{array}{ccc} K_{\mathfrak{p}}^{\times} & \xrightarrow{(\cdot,\, L_{\mathfrak{P}}|K_{\mathfrak{p}})} & \mathrm{Gal}(L_{\mathfrak{P}}|K_{\mathfrak{p}}) \\ {\scriptstyle \langle\,\rangle}\downarrow & & \downarrow \\ C_K & \xrightarrow{(\cdot,\, L|K)} & \mathrm{Gal}(L|K) \end{array}$$

Here the left arrow sends $\beta \in K_{\mathfrak{p}}^{\times}$ to the class of the idèle $\alpha = (\alpha_{\mathfrak{q}})_{\mathfrak{q}}$ given by $\alpha_{\mathfrak{q}} = \begin{cases} \beta & \mathfrak{q} = \mathfrak{p} \\ 1 & \text{else} \end{cases}$

For the arrow on the right, remember that there is a canonical isomorphism $\mathrm{Gal}(L_{\mathfrak{P}}|K_{\mathfrak{p}}) \cong D_{\mathfrak{P}}$ ($D_{\mathfrak{P}}$ = decomposition group of $\mathfrak{P}$), and the arrow is given by the inclusion $D_{\mathfrak{P}} \hookrightarrow \mathrm{Gal}(L|K)$.

Corollary. If $L|K$ is finite abelian and $\alpha = (\alpha_\mathfrak{p})_\mathfrak{p} \in I_K$, V

then $(\alpha, L|K) = \prod_\mathfrak{p} (\alpha_\mathfrak{p}, L_\mathfrak{P}|K_\mathfrak{p})$, where $\mathfrak{P}$ is an arbitrary divisor of $\mathfrak{p}$ for every $\mathfrak{p} \in S_K$. In particular, for an idèle $a \in K^*$ we have $\prod_\mathfrak{p} (a, L_\mathfrak{P}|K_\mathfrak{p}) = id_L$. $(*)$

sketch: It suffices to check the equation for idèles of the form $\langle \alpha_\mathfrak{p} \rangle$ $(\alpha_\mathfrak{p} \in K_\mathfrak{p}^*)$, where it follows directly from the commutative diagram. For $a \in K^*$ notice that $(\;\cdot\;, L|K)$ depends only on idèle classes.

Remark: One can use $(*)$ in order to derive a product formula for the various Hilbert symbols introduced in §2:

$$\prod_\mathfrak{p} \left(\frac{a,b}{\mathfrak{p}}\right) = 1 \quad \text{for } a, b \in K^* \qquad (**)$$

where K^* denotes a number field which contains μ_n.

generalized Legendre symbol $\left(\frac{a}{\mathfrak{p}}\right) := \left(\frac{\pi, a}{\mathfrak{p}}\right)$

($\mathfrak{p}$ prime with $\mathfrak{p} \nmid n$, π local unif. for $K_\mathfrak{p}$, $a \in U_\mathfrak{p}$)

This symbol satisfies $\left(\frac{a}{\mathfrak{p}}\right) = 1 \iff a \equiv \alpha^n \mod \mathfrak{p}$ for some $\alpha \in U_\mathfrak{p}$.

generalized Jacobi symbol $\left(\frac{a}{\mathfrak{b}}\right) = \prod_\mathfrak{p} \left(\frac{a}{\mathfrak{p}}\right)^{n_\mathfrak{p}}$ if $\mathfrak{b} = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}$

If $\mathfrak{b} = (b)$ is principal, define $\left(\frac{a}{b}\right) := \left(\frac{a}{\mathfrak{b}}\right)$. Now using $(**)$, one derives the formula $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{\mathfrak{p} | n\infty} \left(\frac{a,b}{\mathfrak{p}}\right)$, the <u>reciprocity law for n-th power residues</u>.

Next we will discuss the relation between ideal- and idèle-theoretic class field theory. Notice that there is a surjective homomorphism

$$I_K \to J_K, \quad \alpha = (\alpha_p)_p \mapsto \prod_{p \in S_K^{<\infty}} p^{v_p(\alpha_p)}$$

whose kernel is I_{K,S_∞}. It induces a surjective hom.

$$C_K \to Cl_K \quad \text{with kernel} \quad I_{K,S_K^\infty} K^*/K^*$$

Now we are going to derive a similar description for the ray class group. For every modulus m we define $I_K^m = \prod_p U_p^{(n_p)}$ where $n_p = m(p)$ $\forall p \in S_K$. For p finite, we already defined $U_p^{(n_p)}$ in §2. For real p, we put $U_p^{(n_p)} = \begin{cases} \mathbb{R}^* & \text{if } n_p = 0 \\ \mathbb{R}_+^* & \text{if } n_p = 1 \end{cases}$ and $U_p^{(0)} = \mathbb{C}^*$ for complex p. Furthermore, we let $C_K^m = I_K^m K^*/K^*$ and call it the <u>congruence subgroup</u> modulo m.

<u>Theorem:</u> The closed subgroups of finite index in C_K are precisely those which contain a congruence subgroup C_K^m for some modulus m.

sketch: (i) Let $U \leq C_K$ be closed of finite index.
I_K^m open in $I_K \Rightarrow C_K^m$ open in C_K
Furthermore, $(C_K : C_K^m)$ is finite: Notice that $I_K^m \subseteq I_{K,S_K^\infty}$; furthermore $(C_K : I_{K,S_K^\infty} K^*/K^*) = \# Cl_K = h_K < \infty$ and $(C_K : C_K^m) = h(I_{K,S_K^\infty} K^* : I_K^m K^*) \leq h(I_{K,S_K^\infty} : I_K^m)$

$$= h \prod_{\mathfrak{p} \in S_K^{<\infty}} (U_\mathfrak{p} : U_\mathfrak{p}^{(n_\mathfrak{p})}) \prod_{\mathfrak{p} \in S_K^{\infty}} (K_\mathfrak{p}^* : U_\mathfrak{p}^{(n_\mathfrak{p})}) < \infty .$$

$\Rightarrow C_K^{\mathfrak{m}}$ is closed as the complement of the union of finitely many open cosets

$\Rightarrow \mathcal{U}$ is closed of finite index, since it is the union of finitely many $C_K^{\mathfrak{m}}$ - cosets.

(ii) Let $\mathcal{N} \subseteq C_K$ be closed of finite index.

$\Rightarrow \mathcal{N}$ is open as the complement of finitely many cosets

$\Rightarrow$ preimage $\mathcal{J}$ of $\mathcal{N}$ in I_K is open

By definition of the topology on I_K, $\mathcal{J}$ contains a subset of the form $W = \prod_{\mathfrak{p} \in S} W_\mathfrak{p} \times \prod_{\mathfrak{p} \notin S} U_\mathfrak{p}$

($S \subseteq S_K$ finite, $W_\mathfrak{p} \subseteq K_\mathfrak{p}^*$ open neighborhood of 1).

For finite $\mathfrak{p}$, choose $n_\mathfrak{p} \geq 0$ s.t. $U^{(n_\mathfrak{p})} \subseteq W_\mathfrak{p}$, and for $\mathfrak{p}$ real, define $n_\mathfrak{p} = 1$. Now one can show that $I_K^{\mathfrak{m}} \subseteq W$ and $C_K^{\mathfrak{m}} \subseteq \mathcal{N}$.

<u>Theorem</u>: The map $I_K \to J_K$ defined above induces an isomorphism $C_K / C_K^{\mathfrak{m}} \cong Cl_K^{\mathfrak{m}}$ for every modulus $\mathfrak{m}$.

One can show that for every finite abelian extension $L|K$ contained in the ray class field $K^{\mathfrak{m}}$ there is a commutative diagram

$$\begin{tikzcd} C_K \arrow[r, "{(\ ,L|K)}"] \arrow[d, "\cong"'] & \mathrm{Gal}(L|K) \\ \mathfrak{Cl}_{\mathfrak{m}} \arrow[ur, "\left(\frac{L|K}{\cdot}\right)"'] & \end{tikzcd}$$

(For the proof, one uses the compatibility between local and global reciprocity law.)

In particular, this shows that $C_K^{\mathfrak{m}}$ coincides with the norm subgroup $N_{K^{\mathfrak{m}}|K} C_{K^{\mathfrak{m}}}$ of the ray class field.

($\Rightarrow$ $\mathfrak{Cl}_K \cong N_{H_K|K} C_{H_K}$, the isomorphism use in the proof of the principal ideal theorem)

(1) § 1. The theorems of classical global CFT

number field = finite (algebraic) extension of $\mathbb{Q}$

Reminder: The ring of integers $\mathcal{O}_K$ of a number field K is a Dedekind domain, which means that every ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ has a unique factorization of prime ideals.

In particular, if $L \supseteq K$ are number fields, $n = [L:K]$, then for every prime $\mathfrak{p}$ in K there are primes $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ in L and $e_1, \dots, e_r \in \mathbb{N}$ such that $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$.

ramification index $e(\mathfrak{P}_i | \mathfrak{p}) = e_i$

inertia degree $f(\mathfrak{P}_i | \mathfrak{p}) = [\lambda_i : \kappa]$ where $\lambda_i = \mathcal{O}_L / \mathfrak{P}_i$ and $\kappa = \mathcal{O}_K / \mathfrak{p}$ denote the residue class fields of $\mathfrak{P}_i$ and $\mathfrak{p}$, respectively

fundamental equation $n = \sum_{i=1}^{r} e_i f_i$

$\mathfrak{p}$ ramified $\Leftrightarrow$ $e_i > 1$ for some i

$\mathfrak{p}$ split $\Leftrightarrow$ $r = n$ $(\Rightarrow e_i = f_i = 1$ for $1 \le i \le r)$

$Spl(L|K) = \{ \mathfrak{p} \mid \mathfrak{p}$ split prime in $K \}$

There are two basic problems in ANT:

(1) Describe the finite extensions of K in terms of arithmetic properties of K.

(2) Describe the factorization of the primes of K in these extensions.

Example In quadratic extensions $L = \mathbb{Q}(\sqrt{d})$ of $\mathbb{Q}$ ($d \in \mathbb{Z}$, $d \neq 0, 1$ square-free) only three cases can occur:

(I) inert case $p\mathcal{O}_L$ is prime in L

(S) split case $p\mathcal{O}_L = \mathfrak{P}_1 \mathfrak{P}_2$, $\mathfrak{P}_1, \mathfrak{P}_2$ different primes in L

(R) ramified case $p\mathcal{O}_L = \mathfrak{P}^2$, $\mathfrak{P}$ prime in L

For the odd primes, the factorization type is determined

(2) by the Legendre symbol.

p is inert in L $\iff$ $\left(\frac{d}{p}\right) = -1$

p is split in L $\iff$ $\left(\frac{d}{p}\right) = 1$

p is ramified in L $\iff$ $\left(\frac{d}{p}\right) = 0$

By the quadratic reciprocity law, this means that the factorization type can be described by congruence conditions

$d=-1$, p prime > 2 $\quad p \equiv 3\ (4) \Rightarrow$ p inert
$\quad p \equiv 1\ (4) \Rightarrow$ p split

$d=-3$, p prime > 3 $\quad p \equiv 2\ (3) \Rightarrow$ p inert
$\quad p \equiv 1\ (3) \Rightarrow$ p split

$d=2$, p prime > 2 $\quad p \equiv 3,5\ (8) \Rightarrow$ p inert
$\quad p \equiv 1,7\ (8) \Rightarrow$ p split

Do such congruence conditions hold for more general number fields? (And beside, is there a generalization of quadratic reciprocity for n-th powers?)

Relation between problem (2) and (1)

Facts from ANT for a Galois extension $L|K$ of number fields:

(i) $\mathfrak{p}$ prime in K, $\mathfrak{P}, \mathfrak{P}'$ primes in L dividing $\mathfrak{p}\mathcal{O}_L \Rightarrow \exists\, \sigma \in \mathrm{Gal}(L|K)$ such that $\sigma\mathfrak{P} = \mathfrak{P}'$

(ii) factorization $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^e \cdots \mathfrak{P}_r^e$, $\mathfrak{P}_i$ different primes in L with the same inertia degree f ($\Rightarrow [L:K] = ref$)

(iii) If $\mathfrak{p}$ is an unramified in L ($e=1$) and $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$, then the decomposition group $D_\mathfrak{P} = \{\sigma \in \mathrm{Gal}(L|K) \mid \sigma\mathfrak{P} = \mathfrak{P}\}$ is mapped isomorphically onto $\mathrm{Gal}(\lambda|\kappa)$, where $\lambda = \mathcal{O}_L/\mathfrak{P}$ and $\kappa = \mathcal{O}_K/\mathfrak{p}$. Let $q = \#\kappa$. The unique $\sigma \in D_\mathfrak{P}$ with $\sigma(\alpha) \equiv \alpha^q \bmod \mathfrak{P}$ $\forall \alpha \in \mathcal{O}_L$ is called the Frobenius element of $\mathfrak{P}$ and denoted by $\left(\frac{L|K}{\mathfrak{P}}\right)$.

(3) (iv) If in (iii) $\mathfrak{P}'$ is another prime dividing $\mathfrak{p}\mathcal{O}_L$, $\mathfrak{P}' = \sigma\mathfrak{P}$, then $D_{\mathfrak{P}'} = \sigma D_{\mathfrak{P}} \sigma^{-1}$ and $\left(\frac{L|K}{\mathfrak{P}'}\right) = \left(\frac{L|K}{\mathfrak{P}}\right)$ $\Rightarrow$ All Frobenius elements corresponding to divisors of $\mathfrak{p}$ form a conjugacy class in $Gal(L|K)$, which we denote by $\left(\frac{L|K}{\mathfrak{p}}\right)$. If $L|K$ is abelian, then this class consists of one element, for which we use the same notation.

(v) For all unramified primes $\mathfrak{p}$ ($e=1$) we have

$$\mathfrak{p} \in Spl(L|K) \iff \left(\frac{L|K}{\mathfrak{p}}\right) = \{id_L\}$$

More generally, if each $\tau \in \left(\frac{L|K}{\mathfrak{p}}\right)$ is of order f, then $\mathfrak{p}\mathcal{O}_L$ decomposes into $r = \frac{[L:K]}{f}$ different prime ideals.

(Reason: By (iv) each $\tau \in \left(\frac{L|K}{\mathfrak{p}}\right)$ is of the form $\left(\frac{L|K}{\mathfrak{P}}\right)$ for some $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$, so by (iii) we have $f = ord(\tau) = \# D_{\mathfrak{P}} = \# Gal(\lambda|\kappa) = [\lambda:\kappa] = f(\mathfrak{P}|\mathfrak{p})$. Since $e(\mathfrak{P}|\mathfrak{p}) = 1$, we obtain $r = \frac{[L:K]}{f}$.)

<u>Theorem</u>: Let $L|K$ be a finite Galois extension of number fields.

(i) The <u>density</u> of $Spl(L|K)$ in the set $S_K^{<\infty}$ of primes in K equals $\frac{1}{[L:K]}$.

(ii) If $L'|K$ is another finite Galois extension, then $L \subseteq L' \iff Spl(L|K) \supseteq Spl(L'|K)$.

(iii) The Galois extension $L|K$ is uniquely determined by the subset $Spl(L|K) \subseteq S_K^{<\infty}$.

(proof: (i) is a special case of the Čebotarev density theorem

(ii) „$\Rightarrow$" If $\mathfrak{p}$ is split in L', it must be split in L.

„$\Leftarrow$" Show that $Spl(LL'|K) = Spl(L|K) \cap Spl(L'|K)$.

Let $\mathfrak{P}$ be a prime divisor of $\mathfrak{p}\mathcal{O}_{LL'}$, $\mathfrak{P}_L = \mathfrak{P} \cap \mathcal{O}_L$, $\mathfrak{P}_{L'} = \mathfrak{P} \cap \mathcal{O}_{L'}$.

$\mathfrak{p} \in Spl(LL'|K) \iff \left(\frac{LL'|K}{\mathfrak{p}}\right) = \{id_{LL'}\} \iff \left(\frac{LL'|K}{\mathfrak{P}}\right) = id_{LL'}$

$\iff \left(\frac{LL'|K}{\mathfrak{P}}\right)\Big|_L = id_L \wedge \left(\frac{LL'|K}{\mathfrak{P}}\right)\Big|_{L'} = id_{L'} \iff$

(4) $\left(\frac{L|K}{\mathfrak{P}_L}\right) = id_L \wedge \left(\frac{L'|K}{\mathfrak{P}_{L'}}\right) = id_{L'} \iff \left(\frac{L|K}{\mathfrak{p}}\right) = \{id_L\} \wedge$

$\left(\frac{L'|K}{\mathfrak{p}}\right) = \{id_{L'}\} \iff \mathfrak{p} \in Spl(L|K) \cap Spl(L'|K)$.

Now $Spl(L|K) \supseteq Spl(L'|K) \Rightarrow Spl(L'|K) = Spl(L|K) \cap Spl(L'|K) \overset{s.a.}{\Rightarrow} Spl(L'|K) = Spl(LL'|K) \overset{(i)}{\Rightarrow} [L':K] = [LL':K]$
$\Rightarrow L' = LL' \Rightarrow L \subseteq L'$

(iii) follows immediately from (ii) ; in fact, for $L = L'$ it is sufficient that $Spl(L|K)$ and $Spl(L'|K)$ differ by only finitely many elements)

Back to problem (2). Given some finite Galois extension $L|K$, we would like to describe the factorization of $\mathfrak{p}\mathcal{O}_L$ for primes $\mathfrak{p}$ in K. However, the concept of „congruence condition" doesn't make sense for general K, since not every prime $\mathfrak{p}$ is a principal ideal. The deviation of $\mathcal{O}_K$ from being a principal ideal domain is measured by $Cl_K = J_K / P_K$, the <u>ideal class group</u> of K. By global CFT, Cl_K classifies the <u>unramified</u> extensions of K.

<u>Def.:</u> Let K be a number field.

finite prime = prime ideal of $\mathcal{O}_K$
infinite prime = embedding $K \hookrightarrow \mathbb{R}$ or complex-conjugate pair of embeddings $K \hookrightarrow \mathbb{C}$ (real resp. complex prime)

$S_K = S_K^{<\infty} \cup S_K^{\infty}$ set of finite and infinite primes

The elements of S_K are in 1-to-1-correspondence with the equivalence classes of <u>valuations</u> on K.

Now let $L|K$ be a finite extension. An infinite prime σ is <u>ramified</u> in L if σ is real and there is a complex prime $\{\tau, \bar{\tau}\}$ such that $\tau|_K = \sigma$, <u>unramified</u> otherwise.

(5) The extension $L|K$ is unramified if all $\mathfrak{p} \in S_K$ are unramified in L.

Def.: Let K be a number field and $\hat{U}$ a subgroup of J_K. A finite abelian extension $L|K$ is called the class field of $\hat{U}$ iff

$$\mathrm{Spl}(L|K) = \{ \mathfrak{p} \mid \mathfrak{p} \in S_K^{<\infty} \text{ and } \mathfrak{p} \in \hat{U} \}$$

Similarly, L is called the class field of a subgroup $U \leq Cl_K$ iff it is the class field of $\hat{U} = \pi^{-1}(U)$, where $\pi : J_K \to Cl_K$ is the canonical surjection.

Def: Let $L|K$ be a finite abelian extension. Then the Artin map of $L|K$ is the uniquely determined homomorphism

$$\left(\frac{L|K}{\cdot}\right) : J_K \to \mathrm{Gal}(L|K)$$

which sends every prime $\mathfrak{p}$ in K to the Frobenius element $\left(\frac{L|K}{\mathfrak{p}}\right)$.

Theorem (global reciprocity law, unramified version)

(i) For every unramified finite abelian extension $L|K$ there is a subgrp $U \leq Cl_K$ such that the Artin map induces an isomorphism $Cl_K/U \cong \mathrm{Gal}(L|K)$. ($\Rightarrow$ Every finite abelian ext is the class field of some subgroup of Cl_K.)

(ii) For every subgroup U there is an unramified abelian extension $L|K$ such that the Artin map induces an isom. $Cl_K/U \cong \mathrm{Gal}(L|K)$. ($\Rightarrow$ For every subgroup there is a class field.)

(Show that $Cl_K/U \cong \mathrm{Gal}(L|K)$ implies that L is the class field of U. For every finite prime $\mathfrak{p}$ of K we have to show the equivalence $\mathfrak{p} \in \mathrm{Spl}(L|K) \Leftrightarrow \mathfrak{p} \in \hat{U} = \pi^{-1}(U)$. By assumption, $\hat{U}$ is the kernel of the Artin map, and we have seen before that $\left(\frac{L|K}{\mathfrak{p}}\right) = id_L$ iff $\mathfrak{p}$ is split in L.)

Corollary The class field corresponding to the subgroup $U = \{[(1)]\}$ is called the Hilbert class field H_K of K. Here the

(6) Artin map induces an isomorphism $Cl_K \cong Gal(H_K|K)$. It is the largest unramified finite abelian extension of K, i.e. any other such extension is contained in it.

(proof: Let $L|K$ be an arbitrary unramified finite abelian ext. Then $\ker\left(\frac{L|K}{\cdot}\right) \supseteq \ker\left(\frac{H_K|K}{\cdot}\right) = P_K \Rightarrow Spl(L|K) \supseteq Spl(H_K|K) \Rightarrow L \subseteq H_K$)

Example: The Hilbert class field of $K = \mathbb{Q}(\sqrt{-5})$ is $\mathcal{O}_H = \mathbb{Q}(\sqrt{-1}, \sqrt{5})$.

(sketch: We have $\mathcal{O}_H = \mathbb{Z}[\sqrt{-1}, \frac{1}{2}(1+\sqrt{5})]$. The only prime numbers that ramify in H are 2 and 5 (since $d_H =$), with ramification index 2 each. Since 2 and 5 are also ramified in $\mathbb{Q}(\sqrt{-5})$ with ramification index 2, it follows that $K|H$ is unramified. Since $[H:K] = \# Cl_K = 2$, H is the Hilbert class field of K.)

Corollary: A prime $\mathfrak{p}$ in K is split in H_K iff it is a principal ideal in K.

(proof: $\mathfrak{p} \in Spl(H_K|K) \Leftrightarrow \left(\frac{H_K|K}{\mathfrak{p}}\right) = id_{H_K} \overset{\text{isom.}}{\Leftrightarrow} [\mathfrak{p}] = [(1)]$
$\Leftrightarrow \mathfrak{p}$ is a principal ideal)

Theorem (Principal ideal theorem)
Let K be a number field and $H = H_K$ its Hilbert class field. Then every ideal in $\mathcal{O}_K$ becomes principal in H, more precisely, for every ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ there is an $\alpha \in \mathcal{O}_H$ s.t. $\mathfrak{a}\mathcal{O}_K = (\alpha)$.

(proof: Let G be a group and H a subgroup of finite index. Then there is a canonical homomorphism $Ver: G^{ab} \to H^{ab}$ which is defined as follows: Take a set R of representatives of the right cosets and a map $\varphi: G \to R$ which sends every $g \in G$ to the unique $g' \in R$ with $Hg = Hg'$. Then define

$$Ver(g) := \prod_{h \in R} hg\, \varphi(hg)^{-1} H'$$

Since $H(hg) = H\varphi(hg) \Leftrightarrow hg\,\varphi(hg) \in H$ it follows that $Ver(g)$

is contained in $H/M = H^{ab}$. One can show that $\mathrm{Ver}: G \to H^{ab}$ is a homomorphism which does not depend on the choice of R. Since H^{ab} is abelian, we have an induced map $\mathrm{Ver}: G^{ab} \to H^{ab}$.

<u>Prop.</u>: If G is finite (more generally finitely generated), then the map $\mathrm{Ver}: G^{ab} \to (G')^{ab}$ is trivial.

For the theorem, let H_1 be the Hilbert class field of K and H_2 the Hilbert class field of H_1. We have to show that the map $Cl_K \to Cl_{H_1}$, $[\mathfrak{a}] \mapsto [\mathfrak{a}\mathcal{O}_{H_1}]$ is trivial. The idel-theoretic description of global CFT yields a commutative diagram

$$
\begin{array}{ccccc}
Cl_{H_1} & \xrightarrow{\cong} & C_{H_1}/N_{H_2|H_1}C_{H_2} & \xrightarrow{\cong} & \mathrm{Gal}(H_2|H_1) \\
\uparrow & & \uparrow & & \uparrow \mathrm{Ver} \\
Cl_K & \xrightarrow{\cong} & C_K/N_{H_1|K}C_{H_1} & \xrightarrow{\cong} & \mathrm{Gal}(H_1|K)
\end{array}
$$

As we know, $H_1|K$ is the largest unramified finite abelian extension of K. Since $H_1|K$ and $H_2|H_1$ are both unramified, the same holds for $H_2|K$. Hence by maximality $H_1|K$ must be the largest abelian subextension of $H_2|K$. This implies that $\mathrm{Gal}(H_2|H_1)$ is the commutator subgroup of $\mathrm{Gal}(H_2|K)$, and $\mathrm{Gal}(H_1|K) = \mathrm{Gal}(H_2|K)^{ab}$. Since $H_2|H_1$ is abelian, $\mathrm{Gal}(H_2|H_1) = \mathrm{Gal}(H_2|H_1)^{ab}$, so the arrow on the right is a homomorphism $G^{ab} \to H^{ab}$ with $G = \mathrm{Gal}(H_2|K)$ and $H = \mathrm{Gal}(H_2|H_1) = G'$. By the proposition, this map is trivial, so by the commutativity the map $Cl_K \to Cl_{H_1}$ is trivial as well.)

(On the bottom line of the diagram, the canonical form of the reciprocity isomorphism is $C_K/N_{H_2|K}C_{H_2} \xrightarrow{\cong} \mathrm{Gal}(H_2|K)^{ab}$. But since $H_1|K$ is the largest abelian subextension of $H_2|K$, the norm groups $N_{H_1|K}C_{H_1}$ and $N_{H_2|K}C_{H_2}$ coincide.)

Considering only unramified abelian extensions is very restrictive. For example, it is known that $\mathbb{Q}$ has no unramified extensions

(8) Let $m \in \mathbb{N}$, $m \geq 3$ and m odd or $4 \mid m$. We consider $K_m = \mathbb{Q}(\zeta_m)$ with $\zeta_m = e^{2\pi i/m}$, the m-th cyclotomic extension of $\mathbb{Q}$. As we know there is a canonical isomorphism $(\mathbb{Z}/_{m}\mathbb{Z})^* \cong \mathrm{Gal}(K_m|\mathbb{Q})$.

Is it possible to map some kind of „ideal class group" isomorphically onto $\mathrm{Gal}(K_m|\mathbb{Q})$? It would be canonical to send the prime ideal (p) to $p \bmod m$. This is a class in $(\mathbb{Z}/_{m}\mathbb{Z})^*$ only if $p \nmid m$, so we exclude these primes (by coincidence, these are precisely the primes that ramify in K_m). Now we extend this map to all fractional ideals $(\frac{r}{s})$ with $r, s \in \mathbb{Z}$ coprime to m. $\Rightarrow$ obtain a surjective map onto $(\mathbb{Z}/_{m}\mathbb{Z})^*$. $(\frac{r}{s})$ is mapped to $1 \bmod m$ iff $r \equiv s \bmod p^{v_p(m)}$ for all $p \mid m$ and $\mathrm{sgn}(r) = \mathrm{sgn}(s)$

Def.: A modulus of a number field is a map
$\mathfrak{m} : S_K \to \mathbb{Z}$ s.t. $\mathfrak{m}(\mathfrak{p}) = 0$ for almost all $\mathfrak{p} \in S_K$ and $\mathfrak{m}(\mathfrak{p}) \in \{0, 1\}$ if $\mathfrak{p}$ is real, $\mathfrak{m}(\mathfrak{p}) = 0$ if $\mathfrak{p}$ is complex, $\mathfrak{m}(\mathfrak{p}) \geq 0$ for all finite primes.

For every modulus $\mathfrak{m}$, we let $S(\mathfrak{m}) \subseteq S_K$ denote the set of primes $\mathfrak{p}$ with $\mathfrak{m}(\mathfrak{p}) > 0$. Furthermore

$$J_{\mathfrak{m}} = \{ \mathfrak{a} \mid \mathfrak{a} \text{ ideal} \neq (0) \text{ with factorization } \prod_{i=1} \mathfrak{p}_i^{r_i} \ (r_i \in \mathbb{Z}), \ r_i = 0 \text{ if } \mathfrak{p}_i \in S(\mathfrak{m}) \}$$

$$P_{\mathfrak{m}} = \{ (\alpha) \mid \alpha \in K^*, \ \alpha \equiv 1 \bmod \mathfrak{m} \}$$

If $\alpha = \frac{b}{c}$ with $b, c \in \mathcal{O}_K$, then $\alpha \equiv 1 \bmod \mathfrak{m}$ means that
(i) $b \equiv c \bmod \mathfrak{p}^v$ for all finite primes $\mathfrak{p}$ with $v = \mathfrak{m}(\mathfrak{p}) > 0$
(ii) $\sigma(\alpha) > 0$ for all real primes σ with $\mathfrak{m}(\sigma) = 1$.

The group $Cl_{\mathfrak{m}} = J_{\mathfrak{m}} / P_{\mathfrak{m}}$ is called the ray class group of $\mathfrak{m}$.

Example: For the modulus $\mathfrak{m} = m\infty$ ($m \in \mathbb{N}$ as above, ∞ the unique infinite prime of $K = \mathbb{Q}$, Cl_m is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$.

Remark: As before, we can define class fields attached to subgroups of J_m or Cl_m. Let $L|K$ denote a finite abelian extension and $S \subseteq S_K^{<\infty}$ a finite set of primes which contains the primes that ramify in L. Then L is called the class field of $U \leq J_m$ if $Spl(L|K) \setminus S = \hat{U} \setminus S$.

The class field of $U \leq Cl_m$ is by definition the class field of $U = \pi^{-1}(\hat{U})$, where $\pi : J_m \to Cl_m$ denotes the canonical projection.

Remark: As in the unramified case, we can define the Artin map $\left(\frac{L|K}{\cdot}\right) : J_m \to Gal(L|K)$, if $L|K$ is a finite abelian extension whose ramifying primes are all divisors of m. If we put $\hat{U} = \ker\left(\frac{L|K}{\cdot}\right)$, then L is the class field of $\hat{U}$ since

$$\mathfrak{p} \in Spl(L|K) \iff \left(\frac{L|K}{\mathfrak{p}}\right) = id_L \iff \mathfrak{p} \in \ker\left(\frac{L|K}{\cdot}\right) = \hat{U}$$

Theorem (global reciprocity)

(i) Let $L|K$ be a finite abelian extension and $S \subseteq S_K$ the set of primes that ramify in L. Then there is a modulus m with $S = S(m)$ and a subgroup $U \leq Cl_m$ such that the Artin symbol induces an isomorphism $Cl_m / U \cong Gal(L|K)$. ($\Rightarrow$ L is the class field of U)

(ii) Let m be a modulus in K and $U \leq Cl_m$ a subgroup. Then there is a finite abelian extension $L|K$ which is unramified at all primes $\mathfrak{p} \nmid m$ such that the Artin map induces an isomorphism $Cl_m / U \cong Gal(L|K)$.

Def.: The field which corresponds to the trivial subgroup

(10) of Cl_m is called the ray class field K^m of K.

By definition, we have $Cl_m \cong Gal(K^m|K)$. Every finite abelian extension $L|K$ is contained in a ray class field. To see this, let m be a module and $U \leq Cl_m$ a subgroup with $Cl_m / U \cong Gal(L|K)$. Then $\hat{U} = \pi^{-1}(U)$ is the kernel of $\left(\frac{L|K}{\cdot}\right) : J_m \to Gal(L|K)$, and $P_m \supseteq \hat{U}$ is the kernel of $\left(\frac{K^m|K}{\cdot}\right) : J_m \to Gal(K^m|K)$. We obtain

$Spl(L|K) \supseteq Spl(K^m|K)$ and $L \subseteq K^m$.

Prop.: For every $m \in \mathbb{N}$ as above, $K_m = \mathbb{Q}(\zeta_m)$ is the ray class field of $\mathfrak{m} = m\infty$.

(proof: For every prime $p \nmid m$, the Frobenius $\left(\frac{K_m|\mathbb{Q}}{p}\right)$ sends ζ_m to ζ_m^p. This shows that the kernel of the Artin map $\left(\frac{K_m|\mathbb{Q}}{\cdot}\right) : J_m \to Gal(K_m|\mathbb{Q})$ is P_m. Now the assertion follows from the unicity of the class field.)

Corollary: (prime decomposition)

Let $L|K$ be finite abelian and $U \leq Cl_m$ the corresponding group. For any prime $\mathfrak{p}$ in K with $\mathfrak{p} \nmid m$, if f is the order of $[\mathfrak{p}]$ in Cl_m / U, then $\mathfrak{p}\mathcal{O}_L$ factorizes in $r = \frac{[L:K]}{f}$ different primes.

(proof: Let $\mathfrak{P}$ be a divisor of $\mathfrak{p}\mathcal{O}_L$ and $\lambda = \mathcal{O}_L / \mathfrak{P}$, $\kappa = \mathcal{O}_K / \mathfrak{p}$ the corresponding residue class fields. Then $f(\mathfrak{P}|\mathfrak{p}) = \# Gal(\lambda|\kappa)$ $= \# D_{\mathfrak{P}} = \mathrm{ord}\left(\left(\frac{L|K}{\mathfrak{P}}\right)\right) = \mathrm{ord}\left(\left(\frac{L|K}{\mathfrak{p}}\right)\right) = \mathrm{ord}([\mathfrak{p}]) = f$. If $\mathfrak{p}\mathcal{O}_L$ decomposes into s different primes, then

$$s = \frac{[L:K]}{e(\mathfrak{P}|\mathfrak{p})\, f(\mathfrak{P}|\mathfrak{p})} = \frac{[L:K]}{f} = r \quad)$$

(11) <u>Remark</u>: If $\mathfrak{m}, \mathfrak{n}$ are moduli of K s.t. $\mathfrak{m} | \mathfrak{n}$, then $K^{\mathfrak{m}} \subseteq K^{\mathfrak{n}}$.

(proof: The inclusion $J_{\mathfrak{n}} \hookrightarrow J_{\mathfrak{m}}$ induces a surjective map $Cl_{\mathfrak{n}} \twoheadrightarrow Cl_{\mathfrak{m}}$. Here the surjectivity is a consequence of the fact that every ideal class in $Cl_{\mathfrak{m}}$ contains infinitely many prime ideals, a statement that generalizes Dirichlet's prime number theorem. Since $\left(\frac{K^{\mathfrak{n}}|K}{\cdot}\right)\Big|_{K^{\mathfrak{m}}} = \left(\frac{K^{\mathfrak{m}}|K}{\cdot}\right)$, there is a commutative diagram

$$\begin{array}{ccc} Cl_{\mathfrak{n}} & \xrightarrow{\sim} & Gal(K^{\mathfrak{n}}|K) \\ & \searrow & \downarrow \\ & & Gal(K^{\mathfrak{m}}|K) \end{array}$$

where the arrow on the right is restriction and the two others are given by the Artin symbol. Since $P_{\mathfrak{m}}$ is the kernel of $J_{\mathfrak{m}} \to Gal(K^{\mathfrak{m}}|K)$, the arrow $Cl_{\mathfrak{n}} \to Gal(K^{\mathfrak{m}}|K)$ factorizes over $Cl_{\mathfrak{m}}$, and we obtain a commutative diagram

$$\begin{array}{ccc} Cl_{\mathfrak{n}} & \xrightarrow{\sim} & Gal(K^{\mathfrak{n}}|K) \\ \downarrow & & \downarrow \\ Cl_{\mathfrak{m}} & \xrightarrow{\sim} & Gal(K^{\mathfrak{m}}|K) \end{array}$$

Now if $\mathfrak{p} \nmid \mathfrak{n}$ is a prime in the kernel of $J_{\mathfrak{n}} \to Gal(K^{\mathfrak{n}}|K)$, it is also contained in the kernel of $J_{\mathfrak{m}} \to Gal(K^{\mathfrak{m}}|K)$, so that $Spl(K^{\mathfrak{n}}|K) \subseteq Spl(K^{\mathfrak{m}}|K) \Rightarrow K^{\mathfrak{n}} \supseteq K^{\mathfrak{m}}$.)

<u>Corollary</u>: If $L|\mathbb{Q}$ is finite abelian, then the factorization of $p\mathcal{O}_L$ (p prime) is determined by congruence conditions.

(proof: We may assume that L is contained in $K^{\mathfrak{m}}$ with $\mathfrak{m} = m\infty$, $m \in \mathbb{N}$, $m \geq 3$ and m odd or $4|m$. There is a subgroup U of $Cl_{\mathfrak{m}}$ and a commutative diagram

$$\begin{tikzcd} Cl_m / U \arrow[dr, "\sim"'] & (\mathbb{Z}/m\mathbb{Z})^\times \arrow[l, two heads] \arrow[d] \\ & \mathrm{Gal}(L|\mathbb{Q}) \end{tikzcd}$$

which is induced by the diagram

$$\begin{tikzcd} Cl_m \arrow[dr, "\sim"'] & (\mathbb{Z}/m\mathbb{Z})^\times \arrow[l, "\sim"'] \arrow[d] \\ & \mathrm{Gal}(\mathbb{Q}(\zeta_m)|\mathbb{Q}) \end{tikzcd}$$

which is commutative since the $\left(\frac{\mathbb{Q}(\zeta_m)|\mathbb{Q}}{p}\right)(\zeta_m) = \zeta_m^p$ for every $p \nmid m$.

Now if $p, q \nmid m$ are primes such that $p \equiv p'$ mod m, then $\left(\frac{L|\mathbb{Q}}{p}\right) = \left(\frac{L|\mathbb{Q}}{q}\right)$. Since $\left(\frac{L|\mathbb{Q}}{p}\right)$ and $\left(\frac{L|\mathbb{Q}}{q}\right)$ have the same order, by the above theorem $p\mathcal{O}_L$ and $q\mathcal{O}_L$ factorizes into the same number of primes.)

§2. Local class field theory

Def.: A *local field* is a field which is locally compact with respect to a non-trivial valuation.

One can show that every local field is isomorphic to a field in the following list

(i) if the valuation is archimedian, $\mathbb{R}$ or $\mathbb{C}$

(ii) if the valuation is non-arch. and $\mathrm{char}(K) = 0$, a finite extension of $\mathbb{Q}_p$ (p-adic rationals) for some prime number p (called p-adic number fields)

(iii) if the valuation is non-archimedian and $\mathrm{char}(K) = p > 0$, the field $\mathbb{F}_q((t))$ of Laurent series over $\mathbb{F}_q$, $q = p^n$ for some $n \in \mathbb{N}$

If $(K, |\,|)$ is a valued field, one can construct the completion $K_{|\,|}$ of K w.r.t this valuation. For instance, if K is a number field and $\mathfrak{p}$ a prime in K, we define $q = (\mathcal{O}_K : \mathfrak{p})$ and $|\alpha|_\mathfrak{p} = q^{-n}$ for $\alpha \in \mathcal{O}_K$, where $n \in \mathbb{N}_0$ is maximal with $\mathfrak{p}^n \mid (\alpha)$.
The completion $K_\mathfrak{p} = K_{|.|_\mathfrak{p}}$ is the field of $\mathfrak{p}$-adic numbers.
If $R \subseteq \mathcal{O}_K$ is a set of representatives for $\mathcal{O}_K/\mathfrak{p}$ with $0 \in R$ and $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, then every $\alpha \in K_\mathfrak{p}^*$ can be written as a power series $\alpha = \sum_{n=r}^{\infty} a_n \pi^n$ with $r \in \mathbb{Z}$, $a_n \in R$ $\forall n \geq r$ and $a_r \neq 0$ in a unique way.
Similarly, one obtains $\mathbb{F}_q((t)) = \{ \sum_{n=r}^{\infty} a_n t^n \mid r \in \mathbb{Z}, a_n \in \mathbb{F}_q \; \forall n \geq r, a_r \neq 0 \}$ as the completion of the rational function field $\mathbb{F}_q(t)$ w.r.t. the valuation defined by the prime ideal (t) in the polynomial ring $\mathbb{F}_q[t]$.

Def.: Let $(K, |\cdot|)$ be a non-archimedian local field.
It is convenient to define $v: K^\times \to \mathbb{R}$ by $v(\alpha) = -\log|\alpha|$.

valuation ring of K	$\mathcal{O}_K = \{\alpha \in K^\times \mid v(\alpha) \geq 0\} \cup \{0\}$
maximal ideal	$\mathfrak{m}_K = \{\alpha \in K^\times \mid v(\alpha) > 0\} \cup \{0\}$
residue class field	$\kappa = \mathcal{O}_K / \mathfrak{m}_K$
unit group of $\mathcal{O}_K$	$U_K = \{\alpha \in K^\times \mid v(\alpha) = 0\}$

Let $\pi \in K^\times$ such that $v(\pi) = \min\{v(\alpha) \mid \alpha \in \mathfrak{m}_K \setminus \{0\}\}$. Then π generates $\mathfrak{m}_K$, i.e. $\mathfrak{m}_K = (\pi)$. Such an element is called a local uniformizer of K. Every $\alpha \in K^\times$ can be written as $\alpha = u\pi^n$ with $u \in U_K$ and $n \in \mathbb{Z}$ in a unique way. This means that there are topological isomorphisms

$$K^\times \cong U_K \times \langle \pi \rangle \cong U_K \times \mathbb{Z}$$

Without changing the topology on K, we may assume that $v(\pi) = 1$. The subgroups given for each $n \in \mathbb{N}$ by

$$U_K^{(n)} = \{\alpha \in K^\times \mid v(\alpha - 1) \geq n\}$$ „n-te Einseinheiten"

form a basis of open neighborhoods of $1 \in U_K$.

Now let $L|K$ denote a finite extension of non-archimedian fields, with residue class fields $\kappa = \mathcal{O}_K / \mathfrak{m}_K$ and $\lambda = \mathcal{O}_L / \mathfrak{m}_L$.

inertia degree	$f = [\lambda : \kappa]$
ramification index	$e \in \mathbb{N}$ s.t. $\mathfrak{m}_L^e = \mathfrak{m}_K \mathcal{O}_L$

If $L|K$ is separable (which we assume from now on), then $[L:K] = ef$. If $e = 1$, then $L|K$ is called unramified. Such an extension is always a Galois extension, and there is a natural isomorphism $\mathrm{Gal}(L|K) \cong \mathrm{Gal}(\lambda|\kappa)$. If $\#\kappa = q$, then $\mathrm{Gal}(\lambda|\kappa)$ is generated by the automorphism $\bar{\alpha} \mapsto \bar{\alpha}^q$, and its preimage $\varphi_{L|K} \in Gal(L|K)$ is called the Frobenius automorphism of $L|K$.

Theorem: (local reciprocity law)
For every finite Galois extension $L|K$ of local fields there is a canonical surjective homomorphism

$$(\cdot, L|K) : K^* \longrightarrow Gal(L|K)^{ab} \quad \text{with kernel}$$

$N_{L|K} L^*$ subject to the following conditions

(a) If $L|K$ is unramified, then $(\pi, L|K) = \varphi_{L|K}$ for every local uniformizer π of K.

(b) If $L|K$, $L'|K'$ are finite Galois extensions such that $L \subseteq L'$, $K \subseteq K'$ and $[K':K] < \infty$, then there is a commutative diagram

$$\begin{array}{ccc} (K')^* & \longrightarrow & Gal(L'|K')^{ab} \\ N_{K'|K} \downarrow & & \downarrow \sigma' \mapsto \sigma'|_L \\ K^* & \longrightarrow & Gal(L|K)^{ab} \end{array}$$

In particular, for $K = K'$ we obtain diagrams of the form

$$\begin{tikzcd} K^* \arrow[r] \arrow[dr] & Gal(L'|K)^{ab} \arrow[d] \\ & Gal(L|K)^{ab} \end{tikzcd}$$

which give rise to a canonical homomorphism
$K^* \to Gal(K_s|K)^{ab}$ (K_s = seperable closure of K) with dense image.

(c) Let k be a local field and $G = Gal(k_s|k)$ its absolute Galois group. Then for every finite Galois extension $L|K$ with $k \subseteq K \subseteq L \subseteq k_s$ and every $\sigma \in G$ there is a commutative diagram

$$\begin{array}{ccc} K^\times & \longrightarrow & \mathrm{Gal}(L|K)^{ab} \\ \sigma \downarrow & & \downarrow \sigma^*: \tau \mapsto \sigma\tau\sigma^{-1} \\ \sigma(K)^\times & \longrightarrow & \mathrm{Gal}(\sigma(L)|\sigma(K))^{ab} \end{array}$$

(d) $L|K$, $L'|K'$ finite Galois extensions with $K \subseteq K' \subseteq L$

$$\begin{array}{ccc} (K')^\times & \longrightarrow & \mathrm{Gal}(L|K')^{ab} \\ \uparrow & & \uparrow \mathrm{Ver} \\ K^\times & \longrightarrow & \mathrm{Gal}(L|K)^{ab} \end{array}$$

<u>Theorem:</u> (existence theorem of local CFT)

Let K be a local field. There is a bijective correspondence $L \mapsto \mathcal{N}_L = N_{L|K} L^\times$ between

(i) finite abelian extensions $L|K$

(ii) open subgroups of $K^\times$ of finite index

Furthermore, if $L_1|K$, $L_2|K$ are two such extensions, then

$$L_1 \subseteq L_2 \iff \mathcal{N}_{L_1} \supseteq \mathcal{N}_{L_2}$$
$$\mathcal{N}_{L_1 L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$$
$$\mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1} \mathcal{N}_{L_2}$$

<u>Remark:</u> If $\mathrm{char}(K) = 0$, then every subgroup of $K^\times$ of finite index is open. Every such subgroup contains $(K^\times)^m$ for some $m \in \mathbb{N}$, and every $\alpha \in U_K$ close enough to 1 is an m-th power (follows from Newton's lemma applied to the polynomial $x^m - \alpha$ under the condition $|1-\alpha| < |m|^2$; for $\mathrm{char}(K) = p > 0$ it may happen that $|m|^2 = 0$). In positive characteristic, there are subgroups of finite index that are not open.

Example: For every $m \in \mathbb{N}$ we let ζ_m denote a primitive m-th root of unity.

(i) For every $n \in \mathbb{N}$, the norm group of $\mathbb{Q}_p(\zeta_{p^n})$ is (the image of) $\langle p \rangle \times U_{\mathbb{Q}_p}^{(n)}$

assume $p \neq 2$, define $K = \mathbb{Q}_p$, $L = \mathbb{Q}_p(\zeta_{p^n})$, $\pi = 1 - \zeta_{p^n}$
known from algebraic number theory: $L|K$ is purely ramified of degree $p^{n-1}(p-1)$ (no inertia), π is local unif. with $N_{L|K}(\pi) = p$; furthermore:

$$\exp : ((p^\nu), +) \xrightarrow{\sim} (U_K^{(\nu)}, \cdot)$$

is an isomorphism for all $\nu \in \mathbb{N}$

Now $\alpha \mapsto p^{n-1}(p-1)\alpha$ is an isomorphism between (p) and (p^n), so by the exponential $\alpha \mapsto \alpha^{p^{n-1}(p-1)}$ maps $U_K^{(1)}$ isomorphically onto $U_K^{(n)}$ $\Rightarrow$ $U_K^{(n)} \subseteq N_{L|K} L^\times$
$N_{L|K}(\pi) = p \Rightarrow \langle p \rangle \times U_K^{(n)} \subseteq N_{L|K} L^\times$ Both groups have index $p^{n-1}(p-1)$ in $K^\times$ $\Rightarrow$ equality

(ii) For every unramified extension $L|\mathbb{Q}_p$ of degree f (e.g. $L = \mathbb{Q}_p(\zeta_{p^f-1})$), the norm group of L is $\langle p^f \rangle \times U_{\mathbb{Q}_p}$.

By property (a) of the reciprocity isomorphism, $U_{\mathbb{Q}_p}$ is mapped to zero, and p is mapped to $\varphi_{L|\mathbb{Q}_p}$, which is an element of order f. Hence $\langle p^f \rangle \times U_{\mathbb{Q}_p}$ is contained in the kernel, which is a subgroup of order f. Since $f = [L : \mathbb{Q}_p] = (\mathbb{Q}_p^\times : N_{L|\mathbb{Q}_p} L^\times)$, we have equality again.

Corollary: (local Kronecker-Weber theorem)

Every abelian extension $L|\mathbb{Q}_p$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta_m)|\mathbb{Q}_p$.

The subgroup $\mathcal{N}_L = N_{L|\mathbb{Q}_p} L^\times$ of $\mathbb{Q}_p^\times$ is open and of finite index. The subgroups $\langle p^f\rangle \times U_{\mathbb{Q}_p}^{(n)}$ form a fundamental system of neighborhoods of unity, so $\mathcal{N}_L \supseteq \langle p^f\rangle \times U_{\mathbb{Q}_p}^{(n)}$ for $f, n \in \mathbb{N}$ large enough. Now $\langle p\rangle \times U_{\mathbb{Q}_p}^{(n)}$ is the norm group of $L_1 = \mathbb{Q}_p(\zeta_{p^n})$, and $\langle p^f\rangle \times U_{\mathbb{Q}_p}$ is the norm group of $L_2 = \mathbb{Q}_p(\zeta_{p^f-1})$, so

$$\langle p^f\rangle \times U_{\mathbb{Q}_p}^{(n)} = \langle p\rangle \times U_{\mathbb{Q}_p}^{(n)} \cap \langle p^f\rangle \times U_{\mathbb{Q}_p}$$

is the norm group of $L_1L_2 = \mathbb{Q}_p(\zeta_m)$, $m = p^n(p^f-1)$. From $\mathcal{N}_L \supseteq \mathcal{N}_{L_1L_2}$ we obtain $L \subseteq L_1L_2 = \mathbb{Q}_p(\zeta_m)$ $\square$

Now let K be a local field and $n \in \mathbb{N}$ with $\mathrm{char}(K) \nmid n$ if $\mathrm{char}(K)$ is positiv. We assume that K contains the cyclic group μ_n of order n of the n-th roots of unity.

Another important application of local CFT is the construction of the Hilbert symbol

$$\left(\frac{\ ,\ }{\mathfrak{p}}\right) : K^\times/(K^\times)^n \times K^\times/(K^\times)^n \longrightarrow \mu_n$$

which is a non-degenerate bilinear form with the property $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right) = 1 \Leftrightarrow \alpha$ is norm of $K(\sqrt[n]{\beta})|K$ $\forall\, \alpha, \beta \in K^\times$.

(Here $\mathfrak{p}$ denotes the maximal ideal of K.) We just describe the construction of this symbol via local CFT.

Let $L = K(\sqrt[n]{K^{\times}})$; by Kummer theory, one can show that this is the largest abelian extension of exponent n.
In the first step, we define a map

$$K^{\times}/(K^{\times})^n \to \mathrm{Hom}(\mathrm{Gal}(L|K), \mu_n) \qquad (1)$$

For every $a \in K^{\times}$, choose some $\alpha \in L$ with $\alpha^n = a$ and define $\chi_a \in \mathrm{Hom}(\mathrm{Gal}(L|K), \mu_n)$ by $\chi_a(\sigma) = \frac{\sigma(\alpha)}{\alpha}$. It is clear that χ_a is homomorphism. Furthermore, if $\beta \in L$ is another element with $\beta^n = a$, then there is some $\zeta \in \mu_n$ with $\beta = \zeta\alpha$, and $\frac{\sigma(\beta)}{\beta} = \frac{\sigma(\zeta\alpha)}{\zeta\alpha} = \frac{\zeta\,\sigma(\alpha)}{\zeta\,\alpha} = \frac{\sigma(\alpha)}{\alpha}$, so χ_a is indendependent from the choice of α.

One checks easily that $K^{\times} \to \mathrm{Hom}(\mathrm{Gal}(L|F), \mu_n)$ is a homomorphism. If $a \in (K^{\times})^n$, then <u>any</u> $\alpha \in L$ with $\alpha^n = a$ lies in K, so $\chi_a(\sigma) = \frac{\sigma(\alpha)}{\alpha} = \frac{\alpha}{\alpha} = 1 \;\; \forall \sigma \in \mathrm{Gal}(L|K)$.
This shows that $(K^{\times})^n$ is contained in the kernel, which yields (1). Using the long exact cohomology seq. associated to the sequence $1 \to \mu_n \to K_s^{\times} \xrightarrow{\alpha \mapsto \alpha^n} K_s^{\times} \to 1$ one can show that (1) is actually an isomorphism.

By explicit knowledge of the structure of $K^{\times}$, one can show that $K^{\times}/(K^{\times})^n$ is a <u>finite</u> group. Hence by (1), the group $\mathrm{Hom}(\mathrm{Gal}(L|K), \mu_n)$ and $\mathrm{Gal}(L|K)$ as the Pontryagin dual are both finite. Now since $K^{\times}/N_{L|K}L^{\times} \cong \mathrm{Gal}(L|K)$ has exponent n, we have $(K^{\times})^n \subseteq N_{L|K}L^{\times}$. Furthermore, since $\# K^{\times}/(K^{\times})^n \underset{\text{duality}}{=} \# \mathrm{Gal}(L|K) = \# K^{\times}/N_{L|K}L^{\times}$, both groups are equal.

Finally, there is a natural map (7)

$$\mathrm{Gal}(L|K) \times \mathrm{Hom}(\mathrm{Gal}(L|K), \mu_n) \to \mu_n \qquad (2)$$

given by $(\sigma, \chi) \mapsto \chi(\sigma)$. By local reciprocity, we have a canonical isomorphism $\mathrm{Gal}(L|K) \cong K^*/N_{L|K}L^* = K^*/(K^*)^n$, and $\mathrm{Hom}(\mathrm{Gal}(L|K), \mu_n) \cong K^*/(K^*)^n$ as stated above. Applying these two isomorphisms to (2), we obtain the desired bilinear map.