I find the proofs of the Norm index, reciprocity and existence theorem are best explained in Lang’s book which we follow very closely. However, he uses idelic language which we translate back into the language of congruence groups.

1.6. **Proof of the Norm index Theorem.** Throughout this section $L/K$ is a cyclic extension with Galois group $G = \langle \sigma \rangle$. We recall that the Tate cohomology of a cyclic group $G$ is periodic with period 2, more precisely there is a class $c \in H^2(G, \mathbb{Z}) = \hat{H}^2(G, \mathbb{Z})$ so that cup-product with $c$ gives an isomorphism

$$
\cup c : \hat{H}^i(G, M) \cong \hat{H}^{i+2}(G, M)
$$

for any $G$-module $M$ and $i \in \mathbb{Z}$. The Herbrand quotient

$$
q(M) := \frac{|\hat{H}^0(G, M)|}{|\hat{H}^1(G, M)|}
$$

is defined if both groups are finite and can be viewed as some sort of Euler characteristic of the cohomology of $M$. It behaves like an Euler characteristic in that for any (finite length) exact sequence

$$
\cdots \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow \cdots
$$

one has

$$
\cdots q(M_1) - q(M_2) \cdot q(M_3) - \cdots = 1.
$$

Note also that $q(M) = 1$ for finite $M$ since one has exact sequences

$$
0 \rightarrow M^G \rightarrow M \xrightarrow{1-\sigma} M \rightarrow M^G \rightarrow 0
$$

and

$$
0 \rightarrow \hat{H}^{-1}(G, M) \rightarrow M^G \xrightarrow{N_G} M \rightarrow \hat{H}^0(G, M) \rightarrow 0
$$

and

$$
\hat{H}^{-1}(G, M) \cong \hat{H}^1(G, M)
$$

by (10).

Let $m$ be a modulus only divisible by the primes ramified in $L/K$ (with exponents to be determined later in the proof of Lemma 1.6) and let $S$ be the set of primes dividing $m$ together with the infinite primes. Using Lemmas 1.5, 1.6, 1.7 below the proof of the Norm index theorem is as follows. Consider the map of short exact sequences

$$
0 \rightarrow N_{L/K}(J_m^L) \rightarrow N_{L/K}(J^L) \rightarrow \mathbb{Z}^\times \rightarrow 0
$$

where the vertical maps send elements to their ideals and

$$
K^\times, m := \{ \alpha \in K^\times | \alpha \equiv 1 \mod m \}.
$$

By definition of $P^m$ the map $\phi$ is surjective, so we get

$$
coker(\psi) \cong coker(\eta).
$$

Using Lemma 1.6 we have

$$
|J^m/Q_L| = \prod_{\mathfrak{p} \in S} |G_{\mathfrak{p}}| \cdot \frac{|coker(\eta)|}{|ker(\eta)|} = \prod_{\mathfrak{p} \in S} |G_{\mathfrak{p}}| \cdot \frac{|coker(\psi)| \cdot |ker(\phi)|}{|ker(\psi)|}.
$$
and if we can show
\[ \frac{|\ker(\psi)|}{|\coker(\psi)|} = q(O_{L,S}^\times)^{-1} \]

Lemma 1.7 gives
\[ |J^m/Q_L| = |G| \cdot |\ker(\phi)| \geq |G| = [L : K]. \]

But we already know the opposite inequality by Theorem 1.3 and this gives the norm index theorem, Theorem 1.5.

To show (13) we would like to argue as follows. Take the exact sequence of $G$-modules
\[ 0 \to O_{L,S}^\times \to L^\times \to J^m_L \to Cl(O_{L,S}) \to 0 \]
and conclude
\[ 1 = q(O_{L,S}^\times) \cdot q(L^\times)^{-1} \cdot q(J^m_L) \cdot q(Cl(O_{L,S}))^{-1} \]
\[ = q(O_{L,S}^\times) \cdot |\hat{H}^0(G, L^\times)|^{-1} \cdot |\hat{H}^0(G, J^m_L)| \]
\[ = q(O_{L,S}^\times) \cdot |\ker(\psi)|^{-1} \cdot |\coker(\psi)| \]
using Lemma 1.5 and the finiteness of $Cl(O_{L,S})$. Unfortunately, this neat argument does not work since $\hat{H}^0(G, L^\times) = \mathbb{N}_{L/K}(L^\times)$ and $\hat{H}^0(G, J^m_L) = \mathbb{N}_{L/K}(J^m_L)$ are not finite and the Herbrand quotient is not defined. But it is straightforward to work around this difficulty which results in a more clumsy argument as follows. The sequence (15) induces a commutative diagram

\[
\begin{array}{ccccccc}
\hat{H}^{-1}(Cl(O_{L,S})) & \to & \hat{H}^0(O_{L,S}^\times) & \to & \hat{H}^0(L^\times) & \to & \hat{H}^0((L^\times)) & \to & \hat{H}^1(O_{L,S}^\times) \\
\alpha & & & & & & & & \\
\hat{H}^{-1}((L^\times)) & \to & \hat{H}^0(O_{L,S}^\times) & \to & \hat{H}^0(L^\times) & \to & \hat{H}^0((L^\times)) & \to & \hat{H}^1(O_{L,S}^\times) \\
\hat{H}^0(O_{L,S}^\times) & \to & \hat{H}^0((L^\times)) & \to & \hat{H}^0(J^m_L) & \to & \hat{H}^0(Cl(O_{L,S})) & \to & \hat{H}^1(L^\times) \\
\hat{H}^{-1}(Cl(O_{L,S})) & \to & \hat{H}^0(O_{L,S}^\times) & \to & \hat{H}^0((L^\times)) & \to & \hat{H}^0(J^m_L) & \to & \hat{H}^0(Cl(O_{L,S})) & \to & \hat{H}^1(L^\times) \\
\end{array}
\]

where the second and fourth row are exact and the indicated injections and surjections hold because of Lemma 1.5. An easy diagram chase gives an exact sequence
\[ 0 \to \hat{H}^{-1}((L^\times)) \to \hat{H}^0(O_{L,S}^\times) \to \ker(\psi) \to \ker(\alpha) \to 0 \]
and a completely dual argument gives an exact sequence
\[ 0 \to \ker(\alpha) \to \ker(\psi) \to \hat{H}^0(Cl(O_{L,S})) \to \hat{H}^1((L^\times)) \to 0. \]
Hence
\[
\frac{|\text{coker}(\psi)|}{|\text{ker}(\psi)|} = \frac{|\text{coker}(\alpha)| \cdot |\hat{H}^0(\text{Cl}(O_{L,S}))| \cdot |\hat{H}^{-1}(L^\times)|}{|\hat{H}^1(\mathcal{O}_{L,S}^\times)| \cdot |\hat{H}^0(\mathcal{O}_{L,S}^\times)| \cdot |\text{ker}(\alpha)|} = \frac{|\hat{H}^1(\mathcal{O}_{L,S}^\times)| \cdot |\hat{H}^0(\text{Cl}(O_{L,S}))| \cdot |\hat{H}^{-1}(L^\times)|}{|\hat{H}^1(\mathcal{O}_{L,S}^\times)| \cdot |\hat{H}^0(\mathcal{O}_{L,S}^\times)| \cdot |\hat{H}^{-1}(\text{Cl}(O_{L,S}))|} = q(\mathcal{O}_{L,S}^\times)^{-1} \cdot q(\text{Cl}(O_{L,S})) = q(\mathcal{O}_{L,S}^\times)^{-1}.
\]

using (11) and the finiteness of $\text{Cl}(O_{L,S})$.

**Lemma 1.5.** For any Galois extension $L/K$ with group $G$ one has
\[
H^1(G, L^\times) = H^1(G, J^m_L) = 0.
\]

**Proof.** The first part is of course just Hilbert’s theorem 90 for which we refer to Lang’s book on algebra, for example. Concerning the second, one has an isomorphism of $G$-modules
\[
J^m_L \cong \bigoplus_{p \mid m} \bigoplus_{f \mid p} \mathbb{Z} \cong \bigoplus_{p \mid m} \text{Ind}^G_{G_p} \mathbb{Z}
\]
and Shapiro’s Lemma gives
\[
H^1(G, J^m_L) \cong \bigoplus_{p \mid m} H^1(G_p, \mathbb{Z}) \cong \bigoplus_{p \mid m} \text{Hom}(G_p, \mathbb{Z}) = 0.
\]

\[
\square
\]

**Remark 1.6.1.** Note that we have surreptitiously commuted cohomology with an infinite direct sum. What follows immediately from the definition is that cohomology commutes with arbitrary direct products of coefficients (exercise)
\[
H^i(G, \prod_i M_i) \cong \prod_i H^i(G, M_i).
\]

If $P$ is a finitely generated projective module over a ring $R$ one also has
\[
\text{Hom}_R(P, \bigoplus_i M_i) \cong \bigoplus_i \text{Hom}_R(P, M_i)
\]
since there is a natural map (from right to left) which is an isomorphism for $P = R$ and hence for any retract of $R^n$. If $G$ is a group of type $FP_\infty$, i.e. so that $\mathbb{Z}$ has a resolution by finitely generated, projective $R = \mathbb{Z}G$-modules, then cohomology commutes with direct sums (in fact arbitrary direct limits). Now a finite group is certainly of type $FP_\infty$ since the standard resolution consists of finitely generated $\mathbb{Z}G$-modules.

**Lemma 1.6.** For $p \in S$ denote by $G_p \subseteq G$ the decomposition group. For $m$ sufficiently large one has
\[
[K^\times : N_{L/K} L^\times : K^{\times,m}] = \prod_{p \in S} |G_p|
\]
where $K^{\times,m}$ was defined in (12).
Proof. The proof is short if one uses local class field theory. For each \( p \in S \) and \( \mathfrak{p} \mid p \) the norm subgroup \( N_{L_{\mathfrak{p}}/K_{\mathfrak{p}}} L_{\mathfrak{p}}^\times \subseteq K_{\mathfrak{p}}^\times \) is open and hence contains a subgroup

\[
U(n_p) = \begin{cases} 
1 + p^n \mathcal{O}_{K_p} & \text{p finite} \\
K_p^2 & \text{p real and } n_p = 1
\end{cases}
\]

for suitable \( n_p > 0 \). These are the exponents in our modulus. The natural map

\[
K^\times /N_{L/K} L^\times \cdot K^\times,m \rightarrow \prod_{p \in S} K_p^\times /N_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(L_{\mathfrak{p}}^\times)
\]

is bijective because of weak approximation, Theorem 1.1. More precisely, given \( \alpha_p \in K_p^\times \), we can find \( \alpha \in K^\times \) so that \( \alpha/\alpha_p \equiv 1 \mod p^n \) and hence \( \alpha \) maps to the class of \( (\alpha_p)_{p \in S} \). If \( \alpha \) goes to zero, i.e. \( \alpha = N_{L_{\mathfrak{p}}/K_{\mathfrak{p}}} (\beta_{\mathfrak{p}}) \) then again by weak approximation we can find \( \beta \in L^\times \) so that \( \beta/\beta_{\mathfrak{p}} \equiv 1 \mod \mathfrak{p}^n \) and hence \( N_{L/K}(\beta)/N_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(\beta_{\mathfrak{p}}) \equiv 1 \mod \mathfrak{p}^n \). This means \( \alpha /N_{L/K}(\beta) \in K^\times,m \), i.e. the class of \( \alpha \) vanishes in the left hand side.

Local class field theory gives

\[
|K_p^\times /N_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(L_{\mathfrak{p}}^\times)| = |L_{\mathfrak{p}} : K_p| = |G_p|
\]

and this finishes the proof of Lemma 1.6. However, since we won’t be using local class field theory anywhere else in the entire proof, we would like to indicate how Lemma 1.6 also has a self-contained proof. The first thing to notice is

\[
q(L_{\mathfrak{p}}^\times) = |H^0(G_p, \mathcal{O}_{L_{\mathfrak{p}}})| = K_p^\times /N_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(L_{\mathfrak{p}}^\times)
\]

because of Hilbert 90 but we also need to check that \( N_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(L_{\mathfrak{p}}^\times) \) is a subgroup of finite index. This follows since it contains \( N_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(K_{\mathfrak{p}}^\times) = (K_{\mathfrak{p}}^\times)^{G_{\mathfrak{p}}} \) and \( (K_{\mathfrak{p}}^\times)^n \) has finite index by explicit computation (see also the section on the proof of the existence theorem). Since the \( G_{\mathfrak{p}} \)-action preserves valuations we get

\[
q(L_{\mathfrak{p}}^\times) = q(\mathbb{Z}) \cdot q(\mathcal{O}_{L_{\mathfrak{p}}}) = |G_p| \cdot q(\mathcal{O}_{L_{\mathfrak{p}}})
\]

where \( \mathbb{Z} \) has trivial \( G_{\mathfrak{p}} \)-action. Now \( \mathcal{O}_{L_{\mathfrak{p}}}^\times \) has a finite index submodule \( 1 + \mathfrak{p}^n \) which is mapped isomorphically by the logarithm series (with inverse the exponential series) to the finite index submodule \( \mathfrak{p}^n \subseteq \mathcal{O}_{L_{\mathfrak{p}}} \) and \( \mathcal{O}_{L_{\mathfrak{p}}} \) contains a finite index sublattice \( \mathcal{O}_{K_{\mathfrak{p}}}[G_{\mathfrak{p}}] \cdot \beta \) by the normal basis theorem for the Galois extension \( L_{\mathfrak{p}}/K_{\mathfrak{p}} \) (wlog we can assume a normal basis \( \beta \) lies in \( \mathcal{O}_{L_{\mathfrak{p}}} \)). Putting all this information together we get

\[
q(\mathcal{O}_{L_{\mathfrak{p}}}) = q(1 + \mathfrak{p}^n) = q(\mathfrak{p}^n) = q(\mathcal{O}_{L_{\mathfrak{p}}}) = q(\mathcal{O}_{K_{\mathfrak{p}}}[G_{\mathfrak{p}}]) = 1
\]

since \( \mathcal{O}_{K_{\mathfrak{p}}}[G_{\mathfrak{p}}] \) is cohomologically trivial. These computations already show (17) but there is a subtle point left to prove, namely the existence of a conductor, a subgroup \( U(n_p) \) contained in \( N_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(L_{\mathfrak{p}}^\times) \). It turns out that any finite index subgroup of \( E^\times \), where \( E \) is a local field of characteristic zero, is open and hence contains a group \( U(n) \) for \( n \) large enough. It is enough to show this for the groups \( (E^\times)^n \) which one can do by an explicit analysis similar to the one we just gave for \( L_{\mathfrak{p}}^\times \). However the statement is wrong if \( E \) is a local field of characteristic \( p \). Then \( E^\times/(E^\times)^p \) is a countable product of copies of \( \mathbb{Z}/p \) and it turns out that not every finite index subgroup is open. So here one would also have to show that the norm subgroup of a finite extension is open.
Finally, to make the proof independent of local class field theory, we also have to show directly that
\[ N_{L_p/K_p}(\mathcal{O}_{L_p}^\times) = \mathcal{O}_{K_p}^\times \]
if \( L_p/K_p \) is unramified (so that an unramified prime will not appear in the modulus \( m \)). For this we use that for the extension of finite residue fields \( l/k \) we have
\[ \hat{H}^1(G_p,l^\times) = H^1(G_p,l^\times) = 0 \]
by Hilbert 90 and hence
\[ \hat{H}^0(G_p,l^\times) = q(l^\times) = 1 \]
since \( l^\times \) is finite. So the norm map \( N_{l/k} : l^\times \to k^\times \) is surjective. Similarly, the normal basis theorem for the Galois extension \( l/k \) shows that the additive group \( l \) is \( G_p \)-cohomologically trivial, in particular \( \hat{H}^0(G_p, l) = 0 \), i.e. the trace map is surjective. One can now filter \( \mathcal{O}_{L_p}^\times \) by its standard \( G_p \)-invariant open subgroups \( 1+\mathfrak{p}^n \) with subquotients \( l^\times, l, l, ... \) and show that the Norm map is surjective for all quotients \( \mathcal{O}_{L_p}^\times/(1+\mathfrak{p}^n) \), i.e. \( N_{L_p/K_p}(\mathcal{O}_{L_p}^\times) = 0 \). Since \( N_{L_p/K_p}(\mathcal{O}_{L_p}^\times) \) is a finite index subgroup it contains some subgroup \( 1+\mathfrak{p}^n \) and we are done. \( \square \)

We summarize the facts about local fields that we have obtained in the proof of Lemma 1.6.

**Corollary 1.6.** For a cyclic extension \( L_p/K_p \) of local fields with group \( G_p \) we have
\[ q(L_p^\times) = |G_p|, \quad q(\mathcal{O}_{L_p}^\times) = 1. \]
If \( L_p/K_p \) is unramified we even have
\[ \hat{H}^0(G_p, \mathcal{O}_{L_p}^\times) = \hat{H}^1(G_p, \mathcal{O}_{L_p}^\times) = 0. \]

**Lemma 1.7.** One has
\[ q(\mathcal{O}_{L,S}^\times) = \prod_{p \in S} |G_p|/|G|. \]

**Proof.** This is a beautiful application of the \( S \)-unit theorem and the Herbrand index. Recall the \( S \)-unit regulator map
\[ \rho : \mathcal{O}_{L,S}^\times \to \bigoplus_{p \in S} \mathbb{R} \]
which is \( G \)-equivariant. One way to phrase the unit theorem is to say that it induces an exact sequence of \( G \)-modules
\[ 0 \to \mathcal{O}_{L,S}^\times \otimes_{\mathbb{Z}} \mathbb{R} \xrightarrow{\rho_p} \bigoplus_{p \in S_L} \mathbb{R} \xrightarrow{\sum} \mathbb{R} \to 0. \]

Defining a \( \mathbb{Z}[G] \)-module \( X_S \) by the exact sequence
\[ 0 \to X_S \to \bigoplus_{p \in S_L} \mathbb{Z} \xrightarrow{\sum} \mathbb{Z} \to 0 \]
the unit theorem shows that there is an isomorphism of \( \mathbb{R}[G] \)-modules
\[ \mathcal{O}_{L,S}^\times \otimes_{\mathbb{Z}} \mathbb{R} \cong X_S \otimes_{\mathbb{Z}} \mathbb{R}. \]
Using elementary representation theory (of finite groups over fields of characteristic zero) there is then an isomorphism of \( \mathbb{Q}[G] \)-modules
\[
\mathcal{O}_{L,S}^G \otimes \mathbb{Q} \cong X_S \otimes \mathbb{Q}.
\]
So we have two \( \mathbb{Z}[G] \)-lattices \( \mathcal{O}_{L,S}^G/\mu(L) \) and \( X_S \) in the same \( \mathbb{Q} \)-vector space which allows us to compare their Herbrand indices:
\[
\overline{q}(\mathcal{O}_{L,S}^G) = \overline{q}(\mathcal{O}_{L,S}^G/\mu(L)) = \overline{q}(\mathcal{O}_{L,S}^G/\mu(L) \cap X_S) = \overline{q}(X_S).
\]
But \( \overline{q}(X_S) \) is straightforward to compute
\[
\overline{q}(X_S) = \frac{\prod_{p \in S} |G_p|}{|G|}.
\]
\( \square \)

Since the following two statements have one-line proofs given what we did in this section, we mention them here but they will probably not be used elsewhere.

**Corollary 1.7.** In the situation of Theorem 1.5, if an element \( \alpha \in K^{\times,m} \) generates an ideal that is a norm, then \( \alpha \) is the norm of an element.

**Proof.** Inequality (14) is an equality which implies that \( \ker(\phi) = 0 \) where
\[
\phi : \frac{N_{L/K}(L^\times) \cdot K^{\times,m}}{N_{L/K}(L^\times)} \rightarrow \frac{N_{L/K}(J_{L}^m) \cdot \mathfrak{P}^m}{N_{L/K}(J_{L}^m)}.
\]
\( \square \)

**Corollary 1.8.** (Hasse Norm Theorem) If \( L/K \) is cyclic and \( \alpha \in K^\times \) is locally a norm at every place \( p \) of \( K \) then \( \alpha \) is globally a norm, i.e. \( \alpha = N_{L/K}(\beta) \) for some \( \beta \in L \).

**Proof.** Recall the isomorphism (16)
\[
K^\times/N_{L/K}(L^\times) \cdot K^{\times,m} \cong \prod_{p \in S} K_p^\times/N_{L_p/K_p}(L_p^\times).
\]
By assumption \( \alpha \) vanishes in the right hand side, hence \( \alpha = N_{L/K}(\beta_1) \cdot \alpha_1 \) and since \( (\alpha) \in J_{L}^m \) was the norm of an ideal in \( J_{L}^m \), so is \( \alpha_1 \). By the previous corollary \( \alpha_1 = N_{L/K}(\beta_2) \), hence \( \alpha = N_{L/K}(\beta_1 \beta_2) \).
\( \square \)

### 1.7. Proof of the Reciprocity theorem

Both as a warm-up and as an ingredient in the general proof we look at cyclotomic extensions.

**Lemma 1.8.** Let \( K \) be any number field and \( L/K \) a subextension of \( K(\zeta_m)/K \). Then for \( m = (m) \mathfrak{m}_\infty \) where \( \mathfrak{m}_\infty \) is the product of all real places of \( K \) and for any \( \alpha \in K \) with \( \alpha \equiv 1 \mod m \) we have
\[
((\alpha), L/K) = 1.
\]
In particular \( L/K \) is a class field.
Proof. In a diagram of fields

$$L = KE$$

$$K$$

$$E$$

$$k$$

we have (exercise)

$$\tag{18} (\alpha, L/K)|_E = (N_{K/k}\alpha, E/k).$$

Applying this to $k = \mathbb{Q}$ and $E = \mathbb{Q}(\zeta_m)$ and using that $N_{K/\mathbb{Q}}(\alpha) = \prod \sigma(\alpha) \equiv 1 \mod m\infty$ we deduce for $\gamma := ((\alpha), K(\zeta_m)/K) \in \text{Gal}(K(\zeta_m)/K)$

$$\gamma|_{\mathbb{Q}(\zeta_m)} = ((N_{K/\mathbb{Q}}(\alpha)), \mathbb{Q}(\zeta_m)/\mathbb{Q}) = 1.$$

In particular $\gamma(\zeta_m) = 1$ and hence $\gamma = 1$. $\square$

The next step is to treat the case of a cyclic extension $L/K$. We cannot show directly what we want, that $\ker(\rho)$ contains some group $P_m$, but we will be able to show the opposite inclusion $\ker(\rho) \subseteq P_m \cdot N_{L/K}(J_m^P)$. Together with the Norm index theorem this implies equality.

**Proposition 1.5.** Let $L/K$ be cyclic. Then for the modulus $m$ from Theorem 1.5 we have $\ker(\rho) \subseteq P_m \cdot N_{L/K}(J_m^P)$.

**Proof.** Let $\rho : J^m \to \text{Gal}(L/K)$ be the Artin map for the modulus from Theorem 1.5 which we know is divisible only by the ramified primes in $L/K$. Let $\alpha \in \ker(\rho)$ and

$$\alpha = \prod_{i=1}^r p_i^{\nu_i}$$

the prime factorization of $\alpha$. There is a miraculous "Artin's Lemma", to be proved below, which turns every cyclic extension $L/K$ into a cyclotomic extension. More precisely it produces a diagram of fields

$$\tag{19} E_i(\zeta_m)$$

$$\downarrow$$

$$LE_i$$

$$\downarrow$$

$$L$$

$$E_i$$

$$\downarrow$$

$$K$$

where $E = E_1 \cdots E_r/K$ is linearly disjoint from $L/K$ so that all groups

$$\tag{20} \text{Gal}(LE/E) \cong \text{Gal}(LE_i/E_i) \cong \text{Gal}(L/K) = \langle \sigma \rangle$$
are cyclic but, crucially \( LE_i/E_i \) is cyclotomic for a set of pairwise relatively prime integers \( m_i, i = 1, \ldots, r \). Moreover, \( p_i \) splits completely in \( E_i/K \) and is prime to all \( m_j \). We can write

\[
(p_{i, n}^{\alpha_i}, L/K) = \sigma^{d_i}
\]

and have \( 1 = (a, L/K) = \sigma \sum d_i \), hence

\[
\sum d_i = dn
\]

where \( n = [L : K] = |< \sigma >| \). Since the Artin map is always surjective there is a fractional ideal \( \mathfrak{B} \) in \( E \) (which we can take to be prime to \( m \) and the \( m_i \)) such that

\[
(\mathfrak{B}, LE/E) = \sigma.
\]

By (18) we get for \( b = N_{E/K} \mathfrak{B} \)

\[
(b, L/K) = \sigma.
\]

Now we can write

\[
p_{i, n}^{\alpha_i} b^{-d_i} = N_{E_i/K} A_i
\]

since \( b \) is a Norm (even from \( E_i \), not only \( E \)) and since \( p_i \) is a norm since it is totally split in \( E_i/K \). Since \( (p_{i, n}^{\alpha_i} b^{-d_i}, L/K) = 1 \) we get \( (A_i, LE_i/E_i) = 1 \). But \( LE_i/E_i \) is cyclotomic and so we can write

\[
A_i = (\alpha_i) N_{L_i/E_i} \mathfrak{B}_i
\]

for some \( \alpha_i \equiv 1 \ mod m(m_i)m_{i, \infty} \) (note that we can take any multiple of the modulus \( (m_i)m_{i, \infty} \) from Lemma 1.8). Applying \( N_{E_i/K} \) we get

\[
p_{i, n}^{\alpha_i} b^{-d_i} = N_{E_i/K} (\alpha_i) N_{L_i/E_i} \mathfrak{B}_i = N_{E_i/K} (\alpha_i) N_{L_i/K} (N_{L_i/E_i} \mathfrak{B}_i)
\]

where \( N_{E_i/K} (\alpha_i) \equiv 1 \ mod m \). Taking the product over \( i = 1, \ldots, r \) yields

\[
ab^{-dn} \in P^m \cdot N_{L/K}(J_{L}^m).
\]

But \( n = [L : K] \) and therefore \( b^{-dn} = N_{L/K} (b^{-d}) \) is also a norm. Hence

\[
a \in P^m \cdot N_{L/K}(J_{L}^m).
\]

Lemma 1.9. Let \( a, r \in \mathbb{Z}^{>1} \) and \( q \) be a prime number. Then there exists a prime \( p \) such that \( a \) has order \( q^r \) modulo \( p \).

Proof. If \( p \mid \phi_n(a) \) where \( \phi_n \) is the \( n \)-th cyclotomic polynomial then either \( p \mid n \) or \( a \) has exact order \( n \) mod \( p \) (follows from separability of \( x^n - 1 = \phi_n(x)(x^{d-1}) \cdot \) if \( d \mid n \) and \( d < n \)). For a prime power \( n = q^r \) we can write (binomial expansion, \( q \) divides all \( \binom{q}{i} \) for \( 1 \leq i \leq q - 1 \))

\[
\phi_{q^r}(a) = \frac{a^{q^r} - 1}{a^{q^{r-1}} - 1} = (a^{q^{r-1}} - 1) + q(a^{q^{r-1}} - 1)^{q-2} + \cdots + q.
\]

and so if \( q \mid \phi_{q^r}(a) \) then \( q \mid a^{q^{r-1}} - 1 \). If \( q - 1 > 1 \) we find \( q^2 \mid \phi_{q^r}(a) \) and if \( q = 2 \) we have \( \phi_2(a) = a^{2^{r-1}} + 1 \equiv 1, 2 \ mod 4 \) (as \( r > 1 \)) and so again \( q^2 \mid \phi_{q^r}(a) \). Since \( \phi_{q^r}(a) > q \) there is then another prime \( p \neq q \) dividing \( \phi_{q^r}(a) \).

In any abelian group we say two elements \( a, b \) are independent if the cyclic groups they generate have trivial intersection.
Lemma 1.10. Let

\[ n = q_1^{r_1} \cdots q_s^{r_s} \]

be a positive integer and \( a > 1 \) another one. Then there exist primes \( p_i, p_i' \), larger than any given bound, and a positive integer \( b > 1 \) so that for

\[ m = p_1 \cdots p_sp_1' \cdots p_s' \]

\( a \) and \( b \) have order in \((\mathbb{Z}/m\mathbb{Z})^\times\) divisible by \( n \) and are independent in \((\mathbb{Z}/m\mathbb{Z})^\times\).

Proof. By letting \( r \to \infty \) in Lemma 1.9 we can find arbitrarily large distinct primes \( p_1, \ldots, p_s \) so that \( a \) has order \( q_i^{r_i} \mod p_i \) with \( r_i > r_i' \). Then we find still larger distinct primes \( p_1', \ldots, p_s' \), \( p_i' \neq p_j \), so that \( a \) has order \( q_i^{r_i'} \mod p_i' \) with \( r_i' > r_i \). Then \( a \) certainly has order divisible by \( n \) modulo \( m \). Let \( b \) be a positive integer such that

\[ b \equiv a \mod p_1 \cdots p_s, \quad b \equiv 1 \mod p_1' \cdots p_s'. \]

Then \( b \) has order divisible by \( n \) modulo \( m \). Finally suppose

\[ a^\alpha b^\beta \equiv 1 \mod m. \]

Then \( a^\alpha \equiv 1 \mod p_1' \cdots p_s' \) and hence \( q_i^{r_i'} \cdots q_s^{r_s'} \) divides \( a \). This implies \( a^\alpha \equiv 1 \mod p_1 \cdots p_s \) and hence \( a^\alpha \equiv 1 \mod m \). Therefore \( b^\beta \equiv 1 \mod m \) and hence \( a \) and \( b \) are independent modulo \( m \). \( \square \)

Here is a translation of this Lemma in terms of cyclotomic fields.

Lemma 1.11. Let \( L/K \) be an extension of degree \( n \), \( p \) a prime of \( K \) and \( S \) a finite set of prime numbers. Then there exists an integer \( n \), relatively prime to the primes in \( S \) and to \( p \) so that

(i) \( L \cap \mathbb{Q}(\zeta_m) = \mathbb{Q} \) and hence \( L \cap K(\zeta_m) = K \).
(ii) The Artin symbol \( \rho := (p, K(\zeta_m)/K) \) has order divisible by \( n \).
(iii) There exists \( \tau \in \text{Gal}(K(\zeta_m)/K) \) of order divisible by \( n \) and independent of \( \rho \).

Proof. Apply Lemma 1.10 with \( a = Np \). Take \( m \) only divisible by primes unramified in \( L/\mathbb{Q} \) so that \( L \cap \mathbb{Q}(\zeta_m) = \mathbb{Q} \). Then the cyclotomic polynomial \( \Phi_m(X) \) is irreducible over any subfield of \( L \) hence over \( K' := L \cap K(\zeta_m) \) and over \( K \), i.e. \([K(\zeta_m) : K] = [K'(\zeta_m) : K'] = [K(\zeta_m) : K'] \) and \( K' = K \). So (i) is satisfied and one has isomorphisms

\[ \text{Gal}(L(\zeta_m)/L) \cong \text{Gal}(K(\zeta_m)/K) \cong \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times. \]

By (18) we have \( \rho(\zeta_m) = \zeta_m^a \) so that (ii) holds. Choosing \( b \) as in Lemma 1.10 and setting \( \tau(\zeta_m) = \zeta_m^b \) we get (iii). \( \square \)
Lemma 1.11 results in the following diagram of fields where $E$ is the field we are going to construct in the next Lemma.

\[
\begin{array}{c}
\text{L} \\
\downarrow \\
\text{E} \\
\downarrow \\
\text{K} \\
\downarrow \\
\text{Q(ζm)} \\
\end{array}
\]

\[
\begin{array}{c}
\text{L(ζm)} = E(ζm) \\
\end{array}
\]

\[
\begin{array}{c}
\text{L} \\
\downarrow \\
\text{E} \\
\downarrow \\
\text{K} \\
\downarrow \\
\text{Q} \\
\end{array}
\]

\[
\begin{array}{c}
\text{K(ζm)} \\
\end{array}
\]

**Lemma 1.12.** (Artin’s Lemma) Let $L/K$ be a cyclic extension, $\mathfrak{p}$ a prime of $K$ unramified in $L/K$ and $S$ a finite set of prime numbers. Then there exists an integer $m$, relatively prime to the primes in $S$ and to $\mathfrak{p}$, and a finite extension $E/K$ so that

1. $L \cap K(ζ_m) = K$.
2. $L \cap E = K$.
3. $L(ζ_m) = E(ζ_m)$.
4. $\mathfrak{p}$ splits completely in $E/K$.

**Proof.** Choosing $m$ as in Lemma 1.11 we have

$$G := \text{Gal}(L(ζ_m)/K) \cong \text{Gal}(L/K) \times \text{Gal}(K(ζ_m)/K)$$

and condition (0) is satisfied. Let $σ$ be a generator of $\text{Gal}(L/K)$ and $τ$ be as in Lemma 1.11, let $H$ be the subgroup generated by

$$\{ (σ, τ), ((p, L/K), (p, K(ζ_m)/K)) \}$$

and let $E$ be the fixed field of $H$. Condition (1) is satisfied since $H$ and

$$\text{Gal}(L(ζ_m)/L) \cong 1 \times \text{Gal}(K(ζ_m)/K)$$

generate $G$. Condition (2) is satisfied since the intersection of $H$ and

$$\text{Gal}(L(ζ_m)/K(ζ_m)) \cong \text{Gal}(L/K) \times 1$$

is trivial (uses independence and divisibility by $n$ of $τ$ and $ρ$). Finally, condition (3) is satisfied since the decomposition group

$$< ((p, L/K), (p, K(ζ_m)/K)) >$$

of $\mathfrak{p}$ in $L(ζ_m)/K$ is contained in $H$. □

We can now finally produce our diagram (19). We apply Artin’s Lemma to $p_1, \ldots, p_r$, in succession, making sure that $m_1, \ldots, m_r$ are pairwise relatively prime. Then the compositum $E = E_1 \cdots E_r$ satisfies $L \cap E = K$ as well as (20). This is an easy exercise in Galois theory.

Now on to the proof of the reciprocity theorem, Theorem 1.6. Given an abelian extension $L/K$, let $L_i/K$ be the (finite) family of cyclic subextensions. If $ρ_i$ denotes
the Artin map for $L_i/K$ we know by Prop. 1.5 that $P^m \subset \ker(\rho_i)$ where $m_i$ is only divisible by primes ramified in $L_i/K$. Then for $m := \prod_i m_i$ we have

$$P^m \subset \bigcap_i \ker(\rho_i) = \ker(\rho)$$

and $m$ is only divisible by primes ramified in $L/K$.

At this point, i.e. having proven the norm index and the reciprocity theorem, we also have a (rather complicated) proof of the Kronecker-Weber theorem.

**Corollary 1.9. (Kronecker-Weber)** If $L/\mathbb{Q}$ is abelian, then $L \subseteq \mathbb{Q}(\zeta_m)$ for some $m$.

**Proof.** By Theorem 1.6 we know that $L/\mathbb{Q}$ is a class field for some modulus $(m)\infty$. By direct computation $\mathbb{Q}(\zeta_m)$ is the ray class field for $(m)\infty$. The conclusion now follows from Prop. 1.4. □

1.8. **Proof of the existence theorem.**

1.8.1. **Kummer theory.** The main tool to construct extensions is Kummer theory. Recall that for any field $K$ and integer $n$ prime to the characteristic of $K$ the vanishing of $H^1(K, \mathbb{K}^x)$ (Hilbert’s theorem 90) gives an isomorphism

$$K^x/\mathbb{K}^x)^n \cong H^1(K, \mu_n)$$

and if $K$ contains a primitive $n$-th root of unity we get

$$K^x/\mathbb{K}^x)^n \cong H^1(K, \mu_n) \cong \text{Hom}_{\text{cont}}(G_K, \mu_n).$$

By duality for locally compact abelian groups there is then a bijection between subgroups

$$B/\mathbb{K}^x)^n \subseteq K^x/\mathbb{K}^x)^n$$

and continuous surjections

$$G_K \rightarrow G_K/U \cong \text{Gal}(B/K)$$

to quotients of exponent $n$. By Galois theory these are in turn in bijection with abelian extensions $K(\sqrt[n]{B})/K$ of exponent $n$. Our notation indicates how these extensions are constructed out of a subgroup $B$. This correspondence already looks a little like class field theory but it’s a duality between a multiplicative group and a Galois group whereas the reciprocity map is an isomorphism between such groups.

If $K$ is a number field we know already by Theorem 1.6 that all these extensions are class fields. So a natural question is to compute their norm subgroup $Q_K(\sqrt[n]{S})$ for a suitable modulus $m$ from the group $B$. We shall only do this for

$$B = \mathcal{O}_{K,S}^x \cdot (\mathbb{K}^x)^n$$

where $S$ is a large enough set of places containing all infinite places and

$$\mathcal{O}_{K,S} = \{ \alpha \in K | \mathfrak{p} \notin S \Rightarrow |\alpha|_\mathfrak{p} \leq 1 \}$$

is the ring of $S$-integers. More precisely we have

**Proposition 1.6.** Assume $K$ contains a primitive $n$-th root of unity. Let $S$ be a finite set of places of $K$ such that

- $\mathfrak{p} \nmid \infty \Rightarrow \mathfrak{p} \in S$
- $\mathfrak{p} | n \Rightarrow \mathfrak{p} \in S$
Denote by \( m_S = \prod_{p \in S} p^{m_p} \) a modulus so that for all \( p \in S \) we have \( m_p > 0 \) and
\[ \alpha \equiv 1 \mod p^{m_p} \Rightarrow \alpha \in (K_p^\infty)^n. \]

Then
\[ L_{S,n} := K \left( \sqrt[\infty]{O_{K,S}} \right) \]
is the class field for the congruence group
\[ P^m_S \subseteq (K_{S,n}^\infty) \subseteq J^m_S \]
where
\[ K_{S,n}^\infty := K^\infty \cap \prod_{p \in S} (K_p^\infty)^n. \]

Moreover
\[ [L_{S,n} : K] = n^{|S|}. \]

**Proof.** We first compute the degree
\[ [L_{S,n} : K] = |O_{K,S}^\infty (K^\infty)^n / (K^\infty)^n| = |O_{K,S}^\infty / O_{K,S} \cap (K^\infty)^n| \]
of \( L_{S,n} \) over \( K \). If an \( S \)-unit has an \( n \)-th root in \( K \) then its \( n \)-th root is again an \( S \)-unit, i.e.
\[ O_{K,S} \cap (K^\infty)^n = (O_{K,S}^\infty)^n \]
and hence
\[ [L_{S,n} : K] = [O_{K,S}^\infty : (O_{K,S}^\infty)^n]. \]

By Dirichlet’s theorem for \( S \)-units we have \( O_{K,S}^\infty \cong \mu(K) \times \mathbb{Z}^{s-1} \) where \( s = |S| \) and hence
\[ [L_{S,n} : K] = [O_{K,S}^\infty : (O_{K,S}^\infty)^n] = |\mu(K) / (K^\infty)^n| \cdot n^{s-1} = n^s. \]

So for example, if \( K = \mathbb{Q} \) we can only take \( n = 2 \) and then for \( S = \{p_1, \ldots, p_{s-1}, \infty\} \) we get
\[ L_{S,2} = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{s-1}}, \sqrt{-1}) \]
which has degree \( 2^s \).

In general \( L_{S,n} \) is unramified outside \( S \), since if \( p \notin S \) then \( \alpha \in O_{K,S}^\infty \subseteq O_{K,p}^\infty \) and \( \sqrt[\infty]{p} \) satisfies the monic equation with integer coefficients \( f(X) = X^n - \alpha \) and \( f'(\alpha) = na^{n-1} \in O_{K,p}^\infty \). By Theorem 1.6 there is a modulus \( m_S \) only divisible by primes in \( S \), and which we can increase to satisfy (21), so that \( L_{S,n} / K \) is a class field and
\[ J^{m_S} / P^{m_S} : N_{L_{S,n}/K} (J^{m_S}_{L_{S,n}}) \cong \text{Gal}(L_{S,n}/K) \]
is a group of exponent \( n \) and order \( n^s \). To see the inclusion
\[ (K_{S,n}^\infty) \subseteq P^{m_S} : N_{L_{S,n}/K} (J^{m_S}_{L_{S,n}}) = \text{ker}(\rho_{L_{S,n}}) \]
write \( \alpha = \beta_p^m \) for each \( p \in S \) and use Theorem 1.1 (weak approximation) to find \( \beta \in K^\infty \) so that \( \beta_p / \beta \equiv 1 \mod m_S \) and hence \( (\alpha / \beta^m) \in P^{m_S} \). As \( \text{Gal}(L_{S,n}/K) \) has exponent \( n \) we have \( (\beta^m) \in \text{ker}(\rho_{L_{S,n}}) \) and conclude \( \alpha \in \text{ker}(\rho_{L_{S,n}}) \).

To see that (24) is in fact an equality it suffices to compute that
\[ [J^{m_S} : (K_{S,n}^\infty)] = n^s. \]
We have \((K_{S,n}^\times) = K_{S,n}^\times/\mathcal{O}_{K,S,n}^\times\) where
\[
\mathcal{O}_{K,S,n}^\times := \mathcal{O}_{K,S}^\times \cap K_{S,n}^\times = \mathcal{O}_{K,S}^\times \cap \prod_{p \in S} (K_p^\times)^n
\]
and we recall that \(\mathcal{O}_{K,S}^\times\) is also the kernel of the natural map \(K^\times \to J_{m^S}\). Consider the commutative diagram with exact rows
\[
\begin{array}{cccccc}
0 & \longrightarrow & K_{S,n}^\times/\mathcal{O}_{K,S,n}^\times & \longrightarrow & 1 \times J_{m^S} & \longrightarrow & H & \longrightarrow & 0 \\
& & \psi_1 & & \phi_1 & & & & \\
0 & \longrightarrow & K^\times/\mathcal{O}_{K,S,n}^\times & \longrightarrow & \prod_{p \in S} K_p^\times/(K_p^\times)^n \times J_{m^S} & \longrightarrow & H & \longrightarrow & 0 \\
& & \psi_2 & & \phi_2 & & & & \\
0 & \longrightarrow & \mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S,n}^\times & \longrightarrow & \prod_{p \in S} K_p^\times/(K_p^\times)^n \times 1 & \longrightarrow & H & \longrightarrow & 0
\end{array}
\]
where \(\phi_i\) are the natural inclusions, \(\psi_i\) are their respective pullbacks and we obtain isomorphisms on \(H\) since \(\text{coker}(\phi_i) \cong \text{coker}(\psi_i)\). To see this last claim, note that \(K^\times\) surjects onto both \(\prod_{p \in S} K_p^\times/(K_p^\times)^n\) (by weak approximation) and \(J_{m^S}\) (by our assumption that the primes in \(S\) generate \(\text{Cl}(K)\)) and that the map \(\text{coker}(\phi_i) \to \text{coker}(\psi_i)\) has trivial kernel since \(\psi_i\) was a pullback of \(\phi_i\).

The bottom row now consists of finite groups and we get
\[
|J_{m^S} : (K_{S,n}^\times)| = |H| = \prod_{p \in S} |K_p^\times/(K_p^\times)^n|/|\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S,n}^\times| = \prod_{p \in S} n^{2s} |n_p|^{1/n^s} = n^s
\]
using Lemma 1.13, Lemma 1.14 and the product formula \(\prod_p |n_p| = 1\).

**Lemma 1.13.** One has \(\mathcal{O}_{K,S,n}^\times = (\mathcal{O}_{K,S}^\times)^n\) and therefore by (23)
\[
|\mathcal{O}_{K,S}^\times/\mathcal{O}_{K,S,n}^\times| = |\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^n| = n^s.
\]

**Proof.** The inclusion \(\mathcal{O}_{K,S,n}^\times \supseteq (\mathcal{O}_{K,S}^\times)^n\) is clear. Now take \(\alpha \in \mathcal{O}_{K,S,n}^\times\) and consider the extension \(L = K(\sqrt[n]{\alpha})\). Then all \(p \in S\) are split completely in \(L/K\). For any \(q \notin S\) we find \(\pi \in K^\times\) with \((\pi) = q\) in \(J_{m^S}\). For \(p \in S\) let \(\mathfrak{p}\) be a place of \(L\) dividing \(p\). By weak approximation we can find \(\beta \in L\) so that, for all \(p \in S\), \(\beta/\pi \equiv 1 \mod \mathfrak{p}^{n_p}\) and \(\beta \equiv 1 \mod q^{n_p}\) for all \(\mathfrak{p} \neq q\). Then \(N_{L/K}(\beta)/\pi \equiv 1 \mod p^{n_p}\), i.e. \((\pi) \in \mathcal{O}_{p,ms}^\times, N_{L/K}(J_{L,m^S})\). We conclude \(J_{m^S} = \mathcal{O}_{p,ms}^\times, N_{L/K}(J_{L,m^S})\), i.e. \(L = K\) by the reciprocity theorem. This means \(\alpha \in \mathcal{O}_{K,S}^\times \cap (K^\times)^n = (\mathcal{O}_{K,S}^\times)^n\). \(\square\)

**Lemma 1.14.** If \(E\) is a local field of characteristic zero with normalized absolute value \(|\cdot|\) one has
\[
|E^\times / (E^\times)^n| = \frac{n \cdot |\mu_n(E)|}{|n|}.
\]
Proof. For $E = \mathbb{C}$ both sides are 0 since $\|x\| = x^2$ for positive real $x$. For $E = \mathbb{R}$ both sides are of order 1, resp. 2, according to whether $n$ is odd, resp. even.

Now assume $E$ is non-archimedean. Setting $q(A) = \frac{\|\ker(n)\|}{\|\ker(n)\|}$ for an abelian group $A$ for which both quantities are finite, $q$ is multiplicative in exact sequences and $q(A) = 1$ if $A$ is finite. The exact sequence

$$0 \to \mathcal{O}_E^\times \to E^\times \to \mathbb{Z} \to 0$$

gives

$$|E^\times/(E^\times)^n|/|\mu_n(E)| = q(E^\times) = n \cdot q(\mathcal{O}_E^\times)$$

and the sequence

$$0 \to 1 + m_E^c \to \mathcal{O}_K^\times \to Q \to 0$$

gives

$$q(\mathcal{O}_E^\times) = q(1 + m_E^c).$$

Now if $e$ is large enough the logarithm series gives an isomorphism

$$\log : 1 + m_E^c \cong m_E$$

and $q(m_E^c) = q(\mathcal{O}_E) = 1/||n||$ by the definition of normalized absolute value (if $\mathcal{O}_K$ has Haar measure 1 and $\alpha \in E^\times$ then $||\alpha||$ is the Haar measure of $\alpha \mathcal{O}_K$, i.e. $[\mathcal{O}_K : \alpha \mathcal{O}_K]^{-1}$ if $\alpha \in \mathcal{O}_E^\times$).

\[\square\]

**Corollary 1.10.** If $\zeta_n \in K$ and $Q \subseteq J^m$ is a congruence group such that $J^m/Q$ has exponent $n$, then there exists a class field for $Q$.

Proof. First note that if $m'$ is a multiple of $m$ and we set $H = J^m/Q$ we have a commutative diagram analogous to (9)

$$\begin{array}{ccc}
0 & \longrightarrow & Q \cap J^{m'} \\
\downarrow & & \downarrow \iota \\
0 & \longrightarrow & Q
\end{array} \quad \begin{array}{ccc}
J^{m'} & \longrightarrow & H \\
\pi' & & \pi \\
J^m & \longrightarrow & H
\end{array} \quad 0$$

where now we must use the fact that $Q$ is a congruence subgroup to get surjectivity of $\pi'$. Indeed, given

$${\alpha} \in \bigoplus_{p \mid m'} \mathbb{Z},$$

by Theorem 1.1 we can find $\alpha \equiv 1 \mod m$ also satisfying $v_p(\alpha) = v_p(\zeta_n)$ for $p \nmid m$ and then $\alpha/(\alpha) \in J^{m'}$.

Given $m$ and $Q$ we first increase $m$ to $m' = m_S$ so that the set $S$ of primes dividing $m_S$ satisfies the conditions in Prop.1.6. Now we proceed as in the proof of (24). Given $\alpha \in K^n_{S,n}$ and $p \in S$ there is $\beta_p \in \mathcal{O}_p$ with $\beta_p^n = \alpha$. By Theorem 1.1 there is $\beta \in K^\times$ with $\beta/\beta_p \equiv 1 \mod p^{m_p}$ and hence $\beta^n/\beta_p^n \equiv 1 \mod p^{m_p}$. Then $\alpha/\beta^n \equiv 1 \mod m_S$, i.e. $(\alpha/\beta^n) \in J^{m_S} \subseteq Q$. Since $J^{m_S}/Q$ has exponent $n$ we have $(\beta)^n \in Q$, hence $(\alpha) \in Q$, hence $(K^n_{S,n}) \subseteq Q$. By Prop. 1.6 $(K^n_{S,n})$ has a class field and so by Lemma 1.4 $Q$ has a class field. \[\square\]
1.8.2. Reduction to $\mathbb{J}^m/Q$ of exponent $n$ and $\zeta_m \in K$. If $m$ is a modulus in $K$ we lift it to any extension $L$ in the obvious way (send $p$ to its factorization) and denote it again by $m$. We have for all $\alpha \in L$

\[ \alpha \equiv 1 \mod m \Rightarrow \forall \sigma : L \rightarrow K \quad \sigma(\alpha) \equiv 1 \mod m \Rightarrow N_{L/K}(\alpha) \equiv 1 \mod m, \]

i.e. $N_{L/K}$ maps $P_L^m$ to $P^m$ (we have used this before in the proof of the reciprocity theorem). If $L/K$ is Galois such a lifted modulus satisfies $\sigma(m) = m$ for all $\sigma \in G$.

**Lemma 1.15.** Let $L/K$ be Galois with group $G$.

a) If $E/L$ is a class field with norm subgroup $P_L^m \subseteq Q_E \subseteq J_L^m$, then for any $\sigma \in G$ the field $E^\sigma := E \otimes_{L,\sigma} / L$ is a class field for $Q_E^\sigma \subseteq J_L^m$.

b) If $\sigma(m) = m$ and $Q_E^\sigma = Q_E$ for all $\sigma \in G$ then $E/K$ is Galois and the reciprocity isomorphism

\[ \rho_m : J_L^m/Q_E \cong \text{Gal}(E/L) \]

is $G$-equivariant where $G$ acts on $\text{Gal}(E/L)$ by conjugation.

c) If in the situation of b) $Q_E = N_{L/K}^{-1}(Q)$ for some congruence subgroup $P^n \subseteq Q \subseteq J^m$ of $K$ then $G$ acts trivially on $\text{Gal}(E/L)$.

d) If in the situation of c) $L/K$ is cyclic and a class field for a congruence subgroup $Q \subseteq J_L$ then $E/K$ is a class field for $Q$.

e) If in the situation of c) $L/K$ is cyclic and $Q$ is any congruence subgroup such that $Q_E = N_{L/K}^{-1}(Q)$ has a class field (over $L$), then $Q$ has a class field (over $K$).

**Proof.** Part a) we leave as an exercise. For part b) note that under the assumptions we have $E^\sigma = E$ for all $\sigma \in G$, i.e. $E/K$ is Galois. Note that $\phi = \text{Frob}_p$ is the unique automorphism in $\text{Gal}(E/L)$ so that

\[ \forall x \in \mathcal{O}_E \quad x^{P} \equiv \phi(x) \mod \mathfrak{p} \]

for a prime $\mathfrak{p}$ above $p$ (the choice doesn’t matter since $\text{Gal}(E/L)$ is abelian). This implies for any lift $\tilde{\sigma} \equiv \text{Gal}(E/K)$ of $\sigma$

\[ \forall x \in \mathcal{O}_E \quad x^{P} \equiv \tilde{\sigma}(\phi)^{-1}(x) \mod \tilde{\sigma}(\mathfrak{p}) \]

and $\tilde{\sigma}(\mathfrak{p})$ is a prime above $\sigma(p)$. So we get the characterizing property of $\text{Frob}_{\sigma(p)}$ and this implies that $\rho_m$ is $G$-equivariant. If $Q_E = N_{L/K}^{-1}(Q)$ is a pullback then $Q_E$ contains $N_{L/K}^{-1}(P^m)$ which contains $P_L^m$ by the above remark. Hence $Q_E$ is a congruence subgroup. Moreover, the $G$-action on $J_L^m/Q$ is trivial, since $N_{L/K}(\sigma(a)) = N_{L/K}(\sigma(a))$ for all $\sigma \in G$, i.e. $\sigma(a)/a \in N_{L/K}^{-1}(Q)$. This proves c).

If moreover $L/K$ is cyclic, then $\text{Gal}(E/K)$ must be abelian since the lift $\tilde{\sigma}$ of any generator $\sigma$ commutes with all $\tau \in \text{Gal}(E/L)$ and $\tilde{\sigma}$ and $\text{Gal}(E/L)$ generate $\text{Gal}(E/K)$. By definition of $Q_E := N_{L/K}(J_L^m) \cdot P^m$ the composite homomorphism

\[ \pi : J_L^m \xrightarrow{N_{L/K}} Q_L \rightarrow Q_L/P^m \]

is surjective, hence for any subgroup $P^m \subseteq Q \subseteq Q_L \subseteq J^m$ and $Q_E := \pi^{-1}(Q/P^m)$

\[ J_L^m/Q_E = J_L^m/\pi^{-1}(Q/P^m) \cong (Q_L/P^m)/(Q/P^m) \cong Q_L/Q. \]

(25)

If $E/L$ is a class field for $Q_E$ then

\[ N_{E/K}(J_E^m) = N_{L/K}(N_{E/L}(J_L^m)) \subseteq N_{L/K}(Q_E) \subseteq Q \]
and using (25)
\[ [J^m : Q] = [J^m : Q_L] \cdot [Q_L : Q] = [J^m : Q_L] \cdot [J^m_L : Q_E] = [L : K] \cdot [E : L] = [E : K]. \]
Hence \( E/K \) is a class field for \( Q \) and this gives d). For e) first use the reciprocity theorem to deduce that \( L/K \) is a class field, then take a common modulus \( m \) for \( Q \) and \( Q_L \) and note that
\[ Q_E = N_{L/K}^{-1}(Q) = N_{L/K}^{-1}(Q \cap Q_L) \]
has a class field \( E/L \). By d) \( E/K \) is the class field for \( Q \cap Q_L \subseteq J^m \) and by Lemma 1.4 there is a class field for \( Q \subseteq J^m \) since \( Q \cap Q_L \subseteq Q \).

We can now conclude the proof of Theorem 1.7. Given any congruence subgroup \( P^m \subseteq Q \subseteq J^m \), let \( n \) be its exponent. There is a tower of cyclic extensions
\[ K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_r = K(\zeta_n) \]
giving us a sequence of congruence subgroups
\[ Q_0 = Q, \quad Q_i = N_{K_i/K_{i-1}}^{-1}(Q_{i-1}) = N_{K_i/K_{i-1}}^{-1}(Q_{i-1} \cap Q_{K_i}). \]
By an easy upward induction and (25) all groups \( J^m_{K_i} / Q_i \) have exponent \( n \). By Corollary 1.10 \( Q_r \) has a class field and by Lemma 1.15 e) and an easy downward induction all \( Q_i \) have class fields. In particular \( Q = Q_0 \) has a class field.