On the Class Field Theory and Norm Index Computations

Ahmad Sabihi

Department of Mathematics
Sharif University of Technology, Tehran, Iran
sabihi2000@yahoo.com

Abstract. In this paper, the author reviews and proves some theorems in Algebraic Number Theory. These theorems are the base of the one of the most important theories in Algebra and Number Theory where is called Class Field Theory.

Mathematics Subject Classification: 11R29, 11R04, 11S31

Keywords: Class Field Theory, Algebraic Number Theory, Algebraic Numbers, Norm Index Computations, Artin Symbol, Reciprocity Law

1. Introduction

Relations between ideal class groups and abelian extensions of number field were known during the end of the nineteenth century. Hilbert [1] was the first who defined what is now called the Hilbert class field, namely the maximal unramified abelian extension, then he conjectured its principal properties, but he proved them in special cases. The general proofs were given by Furtwängler. Weber defined the generalized ideal classes and proved the uniqueness of the class field corresponding to them, conjecturing the existence, and pointing out that infinitely many primes in a generalized ideal class would follow from the existence of the class field.

Finally, in 1920 Takagi extended the Weber and Hilbert-Furtwängler's theorems to the most general case, specially proving the existence theorem for abelian extensions corresponding to the generalized ideal class groups. Therefore, from about 1880 to 1927, we see the class field theory developing from three themes: 1- The decomposition of primes 2- Abelian extensions 3- Ideal class groups. In 1936, Chevally introduced the ideles in order to formulate the class field theory for infinite extensions. Shortly afterward, Weil [2] introduced adeles and gave his adelic proof of the Riemann-Roch's theorem.
There is another approach to the class field theory, first started in the early thirties by Hasse, namely through the theory of simple algebras, centering around the fundamental theorem that a simple algebra over \( k \) splits over \( k \) if and only if it splits locally everywhere (Albert-Hasse-Brauer-Noether). Hasse also shows how to associate invariants with a division algebra and how the reciprocity law has a formulation in terms of the sum of the invariants being equal to 0.

In the following of subject, the author introduces to the algebraic integers and class field in the Chapter three and encourages the reader for studying and tracking subjects in [3-15]. T. Kubota and S. Oka [16] showed that the Artin's reciprocity law for a general abelian extension of finite degree over an algebraic number field of a finite degree as \( K/F \) can be derived from a cyclotomic extension and Kummer's extension by elementary algebraic arguments so that \( n = (K:F) \) is odd. They also showed that for the even case, one can obtain it by some more advanced efforts that are a consequence of Hasse's norm theorem for quadratic extension of an algebraic field.

2. Norm Index Computations

2.1 The Herbrand Quotient

Beginning by considerations of general abelian groups which will be used both in the local and global case, one can recall the index relation [17].

\[
(A : B) = (A^f : B^f)(A_f : B_f)
\]  

(2-1)

If \( A \supset B \) are abelian groups, then \( f \) will be a homomorphism of \( A \)

Let \( f \) and \( g \) be homomorphisms of \( A \) into itself such that

\[
fog = gof = 0
\]  

(2-2)

then the Herbrand Quotient should be defined:

\[
Q(A) = Q_{f,g}(A) = \frac{(A_f : A^g)}{(A_g : A^f)}
\]  

(2-3)

if the indices in the numerator and denominator are finite.

Theorem 1

If \( B \) is a subgroup of \( A \) which is mapped into itself by \( f \) and \( g \) so that \( f \) and \( g \) may also be viewed as endomorphisms of the factor group \( A/B \) then

\[
Q(A) = Q(B)Q(A/B)
\]  

(2-4)

in the sense that if two of the quotients are defined, so is third and the relation holds. Furthermore, if \( A \) is finite, then [17]

\[
Q(A) = 1
\]  

(2-5)

Proof:

One may view the quotient \( Q \) as an Euler-Poincare's characteristic of a complex of length 2 and apply a general result of an elementary nature to deduce the multiplicativity property. One shall reproduce a sketch of the proof below in
special case. Firstly a proof should be given for the simpler case when $B$ is of finite index in $A$. Therefore

\[(A : B) = \left(\frac{A_f : B^g}{B_f : B^g}\right) = \left(\frac{A_f : A^g}{B_f : B^g}\right)
\]

Whence

\[(A : B) = \left(\frac{A_f : A^g}{B_f : B^g}\right) = \left(\frac{A : B}{A^g : B^g}\right) = \left(\frac{A_f : A^g}{B_f : B^g}\right)
\]

The left hand side is symmetric in $f$ and $g$ so that

\[(A : B) = \left(\frac{A_f : A^g}{B_f : B^g}\right) = \left(\frac{A : B}{A^g : B^g}\right) = \left(\frac{A_f : A^g}{B_f : B^g}\right)
\]

This proves that $Q(A) = Q(B)$. The reader can verify for himself that all the steps were legitimate (i.e. under the assumption that $Q(A)$ or $Q(B)$ is finite, then it has never been divided by zero or infinity.)

Now for the general case, one can write a sequence

\[0 \to B \to A \to C \to 0
\]

where $C = A/B$. Define

\[H_0(A) = A_f / A^g \quad \text{and} \quad H_1(A) = A^g / A^f
\]

and similarly for $B$ and $C$. Then a diagram could be constructed as below:

\[
\begin{array}{ccc}
H_0(A) & \xrightarrow{\delta} & H_0(C) \\
\delta & & \\
H_1(B) & \xleftarrow{\delta} & H_1(A)
\end{array}
\]

which is exact i.e. such that the image of each arrow is the kernel of the next arrow. Going from $B$ to $A$ and $A$ to $C$ the arrows are simply the natural homomorphisms induced by the inclusion $B \to A$ and the canonical map $A \to A/B = C$. The maps $\delta$ are defined as follows: Let $c \in C_f$ represent an element of $H_0(C)$. Then $fc = 0$ and there exists $a \in A$ such that $c = ja$ if $j : A \to C$ is the canonical homomorphism. Then

\[jfa = fja = 0
\]

so $fa \in B$ and in fact $fa \in B^g$. It is immediate to verify that the association $c \mapsto \text{class of } fa \mod B^g$ is a well defined homomorphism whose kernel contains $C^g$ and hence defines a homomorphism

\[\delta : H_0(C) \to H_1(B)
\]

The map from $H_0(C)$ to $H_0(B)$ is defined similarly. It is a routine matter to prove that with these definitions, the hexagon is exact.

If the quotient $Q$ is defined for two out of three of $A$, $B$, $C$ we see from the hexagon and the exactness that it must be defined for the third. Under the
condition, the author orders his six groups in the diagram clockwise, starting say with \( H_6(A) \) and denotes them by \( M_i \) \((i = 1, \ldots, 6 \mod 6)\) let \( k_i \) be the order of the kernel of the arrow leaving \( M_i \) and let \( m_i \) be the order of the image of the arrow arriving at \( M_i \) then
\[
\text{ord } M_i = m_i k_{i+1}
\]
Furthermore \( m_j = k_i \) by exactness. Hence
\[
m_1 m_2 m_3 k_2 k_4 k_6 = m_2 m_4 m_6 k_1 k_3 k_5
\]
Dividing suitably yields the relation \( Q(A) = Q(B)Q(C) \) thus providing the multiplicativity of \( Q \)

The next step is the proof for the second statement i.e. \( Q(A) = 1 \) if \( A \) is finite.

Consider the following lattice of subgroups:

```
A_f \ 
\ 
Ag \ 
\ 
Ag \ 
\ 
Af \ 
\ 
0
```

Under the map \( g \) there is an isomorphism \( A/A_g \approx A^g \) and similarly with \( f \)
replacing \( g \) thus opposite slanting sides of the hexagon are equal.

It follows that the vertical sides are also equal, thus it is proved what the author
wants. (Equality here means that the corresponding factor groups have the same
order. As an abuse of language, it is very much less obnoxious than the
corresponding abuse in plane geometry…)

The preceding theorem will be referred to as the Q-Machine. It will be used in
the following context. Let \( G \) be a cyclic group operating on an abelian group \( A \)
let \( \sigma \) be a generator of \( G \) let
\[
f = 1 - \sigma \quad \text{and} \quad g = 1 + \sigma + \ldots + \sigma^{n-1}
\]
where \( n \) is the order of \( G \) let \( A^G \) be the subgroup \( A_{1-\sigma} \) i.e. the subgroup of \( A \)
consisting of those elements fixed by \( G \). Note that
\[
1 + \sigma + \ldots + \sigma^{n-1} = Tr_G
\]
is a "trace" map which in multiplicative notation would be denoted by a norm
map. Thus the quotient in this case is
\[
Q(G, A) = Q(A) = \frac{(A^G : Tr_G A)}{(AT_r : (1 - \sigma) A)}
\]
The numerator is the trace index (norm index in multiplicative notation).If
\( G \) operates with trivial action on \( Z \) (or any infinite cyclic group) then one sees
\[
Q(G, Z) = (G : 1)
\]
i.e. the Herbrand quotient is equal to the order of \( G \). This follows because
\( Z^G = Z, \; Tr(Z) = nZ \) (where \( n \) is the order of \( G \)) and \( Z_{Tr} = 0 \)
Let $G$ be an arbitrary finite group operating on an abelian group $A$. One can associate with $(G, A)$ two abelian groups

$$H^0(G, A) = A^G / Tr_{G} A \quad \text{and} \quad H^{-1}(G, A) = A_{tr} / I_{G} A$$

(2-20)

where $I_{G}$ is the ideal of the group ring $\mathbb{Z}[G]$ generated by all elements $(1 - \sigma)$ for $\sigma \in G$. It is an ideal, because for $\tau \in G$ could be written:

$$\tau - \tau \sigma = \tau - 1 + 1 - \tau \sigma$$

(2-21)

Thus $I_{G} A$ by definition consists of the $G$-submodule generated by the elements $a - \sigma a$ with $a \in A$ and $\sigma \in G$ if $G$ is cyclic, and $\sigma$ is a generator of $G$ then

$$I_{G} A = (1 - \sigma)A$$

(2-22)

Because $1 - \sigma' = (1 - \sigma)(1 + \ldots + \sigma^{i-1})$

In homological terminology, one can see that the numerator and denominator of the Herbrand quotient are simply orders of cohomology groups, namely the orders of $H^0$ and $H^{-1}$ respectively.

### 2.2 Semi-local Representations

The author shall prove some theorems which are useful in computing these orders in a situation which arises all the time. Consider a finite group $G$ operating on the abelian group $A$ assume that $A$ is the direct sum of subgroups [17]

$$A = \prod_{i=1}^{s} A_i$$

(2-23)

and that $G$ permutes these subgroups $A_i$ transitively. When that occurs, one can say that the operation of $G$ is semi-local. Let $G_i$ be the decomposition group of $A_i$ (i.e. the subgroup of elements $\sigma \in G$ such that $\sigma A_i = A_i$) then call $(G_i, A_i)$ its local component. Each element $a \in G$ can be written uniquely

$$a = \sum_{i=1}^{s} a_i$$

(2-24)

with $a_i \in A_i$ furthermore let

$$G = \bigcup_{i=1}^{s} \sigma_i G_i$$

(2-25)

be a left coset decomposition of $G$. One can choose the indices $i$ in such a way that $\sigma_i A_i = A_i$ in that case, each element $a_i \in A_i$ can be written as $\sigma_i a'_i$ for a uniquely determined element $a'_i \in A_i$

**Theorem 2**

The projection $\pi : A \rightarrow A_i$ induces an isomorphism [17]

$$H^0(G, A) \approx H^0(G_i, A_i)$$

(2-26)

**Proof:**

...
One first observes that $A^G$ consists of all elements of form
\[ \sum_{i=1}^{s} \sigma_i a_i \quad \text{with} \quad a_i \in A_i^{G_i} \] (2-27)
Namely, it is clear that such an element is fixed under $G$ on the other hand, if
\[ a = \sum_{i=1}^{s} \sigma_i a_i' \] (2-28)
is fixed under $G$ then for a fixed index $j$ may apply $\sigma_j^{-1}$ and see that $a'_j = \sigma_j^{-1} \sigma_j a_j'$ is the $A_i$-component of $\sigma_j^{-1} a = a$. Hence $a'_j = a'_i$ for all $j$ thus proving the author's assertion. In particular, an element of $A^G$ is uniquely determined by its first component and thus the projection gives an isomorphism
\[ A^G \xrightarrow{\sim} A_i^{G_i} \] (2-29)
On the other hand, for a fixed $j$ and $a_j \in A_j$ could be written:
\[ Tr_G(\sigma_j a_j) = \sum_{\sigma \in G} \sigma a_j = \sum_{i=1}^{s} \sigma_i Tr_{G_i}(a_i) \] (2-30)
This shows that $Tr_G(A)$ consists precisely of those elements of the form
\[ \sum_{i=1}^{s} \sigma_i Tr_{G_i}(a_i) \quad a_i \in A_i \] (2-31)
Thus it is clear that $A^G / Tr_G(A) \cong A_i^{G_i} / Tr_{G_i}(A_i)$ and the theorem is proved.

**Theorem 3**

There is an isomorphism, that to be described in the proof [17]
\[ H^{-1}(G, A) \cong H^{-1}(G_1, A_1) \] (2-32)

**Proof:**

Let
\[ a = \sum_{i=1}^{s} \sigma_i a_i' \quad a_i' \in A_i \] (2-33)
Then
\[ Tr_G(a) = \sum_{j=1}^{s} \sigma_j Tr_{G_i}(a_i' + ... + a_i') \] (2-34)
Hence $Tr_G(a) = 0$ if only if $Tr_{G_i}(a_i' + ... + a_i') = 0$ the map $a \mapsto a_i' + ... + a_i'$ is therefore a homomorphism
\[ \lambda : \text{Ker } Tr_{G_i} \rightarrow \text{Ker } Tr_{G_i} \] (2-35)
which is obviously surjective (take $a = a_i$ in the $\text{Ker } Tr_{G_i}$) the author shows that $\lambda$ maps $I_G A$ into $I_{G_1} A_1$ if $\sigma \in G$ then there is a permutation $\pi$ of the indices $i$ such that
\[ \sigma \sigma_i = \sigma \sigma_{\pi(i)} \tau_{\pi(i)} \] (2-36)
with some $\tau_{\pi(i)} \in G_1$. Hence
Field theory and norm index computations

\( \lambda(\sigma a - a) = \sum_{i=1}^{s} (\tau_{x(i)}a'_i - a'_i) \) \hspace{1cm} (2-37)

thus proving our assertion. To conclude the proof, it will suffice to show that if \( \lambda(a) = 0 \) then \( a \in I_G A \). But if \( a'_i + \ldots + a'_i = 0 \) one can write

\[ a = \sum_{i=1}^{s} (\sigma_i a'_i - a'_i) \] \hspace{1cm} (2-38)

And so \( a \in I_G A \). This proves the theorem.

Remark: the two theorems are frequently used in case \( G_1 = \{1\} \) and in that case, one sees that \( H^0(G, A) = H^{-1}(G, A) = 0 \) this occurs in the case of the "regular" representation of \( G \) of which the following is an important case. Let \( K / k \) be a Galois extension with group \( G \). It is known from elementary algebra that there is a normal basis for \( K / k \), i.e. a basis consisting of elements \( \{\omega_\sigma\}_{\sigma \in G} \) such that for any \( \tau \in G \) then \( \tau \omega_\sigma = \omega_{\tau \sigma} \). In that case, \( G \) permutes the 1-dimensional \( k \)-spaces \( k, \omega_\sigma \) transitively, and each decomposition group is trivial. Thus get

\[ H^0(G, K) = H^{-1}(G, K) = 0 \] \hspace{1cm} (2-39)

If \( K / k \) is cyclic, then could always be written:

\[ H^{-1}(G, K^*) = 1 \] \hspace{1cm} (2-40)

This is nothing but Hilbert's Theorem 90.

2.3 The Local Norm Index

Let \( k \) be a \( \mathfrak{p} \)-adic field. Let \( K / k \) be cyclic extension of degree \( N \) with group \( G \) and let \( \sigma \) be a generator. Let \( U_k \) be the group of units in \( k \) and \( U_K \) the group of units in \( K \). Let \( e \) be the ramification index and \( f \) the residue class degree as usual. The Galois group \( G \) operates on \( U_k \) and \( K^* \) so that

\[ H^0(G, K^*) = k^* / N_k^k K^* \] \hspace{1cm} (2-41)

or less precisely in the index \( (k^* : N_k^k K^*) \)

Theorem 4

Hypotheses being as above could be written [17]:

\[ Q(G, K^*) = (k^* : N_k^k K^*) = [K : k], \]
\[ (U_k : N_k^k U_K) = e, \quad Q(G, U_K) = 1 \] \hspace{1cm} (2-42)

Proof:

The author uses Q-machine. By Hilbert's Theorem 90 one knows that \( H^{-1}(G, K^*) = 1 \). Hence

\[ Q(K^*) = (k^* : N_k^k K^*) \] \hspace{1cm} (2-43)

is the norm index. Consider \( K^* / U_K \approx Z \) (with trivial action, because \( |\sigma \alpha| = |\alpha| \) for all \( \alpha \in K^* \)) where

\[ [K : k] = Q(Z) = Q(K^*) / Q(U_K) \] \hspace{1cm} (2-44)
Provided that one can show that \( Q(U_K) \) is defined. In fact, one shall prove that it is equal to 1.

Let \( \{ \omega_r \} \) be a normal basis of \( K \) over \( k \) after multiplying the elements of this basis by a high power of a prime element \( \pi \) in \( k \) and could be assumed that they have small absolute value. Let

\[
M = \sum_{r \in \mathcal{O}} \mathfrak{p} \omega_r
\]

(2-45)

Where \( \mathfrak{p} \) is the ring of integers in \( k \). Then \( G \) acts on \( M \) semilocally, with trivial decomposition group, Furthermore \( \exp M = V \) is \( G \)-isomorphic to \( M \) (the inverse is given by the log) and \( V \) is an open subgroup of the units, whence of finite index in \( U_K \). Therefore one could write:

\[
Q(V) = (U_K) = 1
\]

(2-46)

As desired.

Finally, one notes that

\[
Q(U_K) = \frac{(U_K : N_K^K U_K)}{(H : U_K^{1-\sigma})}
\]

(2-47)

where \( H \) is the kernel of the norm in \( U_K \). Using Hilbert's Theorem 90 again, together with the fact that \( |\sigma\alpha| = |\alpha| \) for all \( \alpha \in K^* \) and one sees that \( H = K^{* \sigma} \).

Hence the denominator of \( Q(U_K) \) is given by

\[
\frac{(H : U_K^{1-\sigma})}{(K^{* \sigma} : k^* U_K)} = \frac{(K^{* \sigma} : k^* U_K^{1-\sigma})}{(k^* : k^*)} = e
\]

(2-48)

This shows that \( (U_K : N_K^K U_K) = e \) and concludes the proof of the theorem.

Observe that one should recover the result that if \( K / k \) is unramified, then every unit in \( k \) is a norm of a unit in \( K \) because \( e = 1 \).

Remark if \( k \) is the real or complex field, then the result of theorem 4 holds also and the verification is trivial. One must interpret the "units" then to mean the whole multiplication group of the field, and \( e = [K : k] \) is equal to 2 or 1.

In the local class field theory, one shall see that the factor group \( k^* / N_K^K K^* \) is isomorphic to \( G \) and not only in the cyclic case but also in the abelian case.

Finally, the inequality (2-49) is satisfied

\[
(k^* : N_K^K K^*) \leq [K : k]
\]

(2-49)

Follows easily for an arbitrary abelian extension \( K / k \) to see this, consider a tower

\[
K \owns E \owns k
\]

(2-50)

Assume that the inequality is proved for each step of tower, namely \( K / E \) and \( E / k \) then

\[
k^* \owns N_E^E E^* \owns N_K^K K^*
\]

(2-51)

because \( N_K^K = N_k^E \circ N_E^K \). Therefore
Field theory and norm index computations

\[(k^* : N_k^K K^*) = (k^* : N_k^E E^*)(N_k^E E^* : N_k^K K^*) \] (2-52)

but

\[(N_k^E E^* : N_k^E N_k^K K^*) \] divides \((E^* : N_k^K K^*)\)

since the degree of an extension is multiplicative in towers, one sees that if the norm index inequality holds in each step of tower, then it holds for \(K/k\) this reduces the inequality to cyclic steps, in which case one apply Theorem 4.

Similarly, for any abelian extension \(K/k\) could be written:

\[(U_k : N_k^K U_K) \leq e \] (2-53)

**Theorem 5: Theorem on Units**

One must turn to the global case, and throughout this section assume \(k\) be a number field. Then \(U_k\) denotes the group of units in \(k\).

Under a log mapping, one can embed the units (modulo roots of unity) into a Euclidean space \(\mathbb{R}^s\). If \(K/k\) is a Galois extension with group \(G\), then one can define an operation of \(G\) on \(\mathbb{R}^s\) which makes this a \(G\)-embedding in a natural way, and allows us to visualize the operation of \(G\) on the units somewhat more clearly. This is done as follows.

Let \(S\) be a finite set of absolute values on \(k\) containing all Archimedean ones, and let \(S_K\) be the set of absolute values \(w\) on \(K\) such that \(wv\) for some \(v \in S\).

For each \(w \in S_K\) select a symbol \(X_w\) and let \(E^s\) be the \(s\)-dimensional real space having \(\{X_w\}\) as basis, for \(w \in S_K\) thus \(s\) is the number of elements of \(S_K\) if \(\sigma \in G\) one can define

\[\sigma X_w = X_{\sigma w}\] (2-54)

and extend \(\sigma\) to all of \(E^s\) by linearity. Then \(G\) operates on \(E^s\).

By a lattice in \(E^s\) one means, as usual, a free abelian subgroup of rank \(s\) such that a \(\mathbb{Z}\)-basis for this subgroup is also an \(\mathbb{R}\)-basis for \(E^s\).

**Theorem 6**

Let \(M\) be a lattice in \(E^s\) which is invariant under \(G\) (i.e. \(\sigma M \subset M\) for all \(\sigma \in G\)) then there exists a sublattice \(M'\) of finite index in \(M\) which is invariant under \(G\) and has a \(\mathbb{Z}\)-basis \(\{Y_w\}\) \((w \in S_K)\) such that \([17]\)

\[\sigma Y_w = Y_{\sigma w}\] (2-55)

**Proof:**

Taking the supermum on \(E^s\) with respect to the coordinates relative to the basis \(\{X_w\}\) since \(M\) is a lattice, there is a number \(b\) such that for any \(X \in E^s\) there is some \(Z \in M\) such that

\[|X - Z| < b\] (2-56)
For each $v \in S$ let $\overline{v}$ be a fixed element of $S_\kappa$ such that $\overline{v}|^v$ take $t$ real and large positive, and find some $Z_\tau \in M$ such that
\[ |tX_\tau - Z_\tau| < b \] (2-57)

For $w|^v$ let
\[ Y_w = \sum_{\sigma|^w} \sigma Z_\overline{\tau} \] (2-58)

The sum is taken over all $\sigma \in P$ such that $\sigma \overline{v} = w$ and the family $\{Y_w\}$ is a basic for a sublattice $M'$ satisfying our requirements.

First the action of $G$ is the desired one, because for $\tau \in G$
\[ \tau Y_w = \sum_{\sigma|^w} \tau \sigma Z_\overline{\tau} = \sum_{\rho|^w} \rho Z_\tau = Y_{\tau w} \] (2-59)

The second sum is taken over those elements $\rho \in G$ such $\rho \overline{v} = \tau w$ making the transformation $\rho = \tau \sigma$ this proves our first assertion.

The author now shows that the vectors $\{Y_w\}$ are linearly independent over $R$. Suppose that
\[ \sum_w c_w Y_w = 0 \] (2-60)

with real $c_w$. If not all $c_w = 0$ one may assume that $|c_w| \leq 1$ for all $w$ and also $c_w = 1$ for some $w$ let
\[ Z_\overline{\tau} = tX_\overline{\tau} + B_\overline{\tau} \] (2-61)

with a vector $B_\overline{\tau}$ such that $|B_\overline{\tau}| < b$. Then
\[ Y_w = \sum_{\sigma|^w} \sigma Z_\overline{\tau} = t \sum_{\sigma|^w} X_{\sigma \overline{\tau}} + B'_w \] (2-62)

where $|B'_w| \leq Nb$ and $N =$ order of $G$. Hence
\[ Y_w = tm_w X_w + B'_w \] (2-63)

If $m_w$ is the number of $\sigma \in G$ such $\sigma \overline{v} = w$ thus one obtains
\[ 0 = \sum_w c_w Y_w = t \sum_w c_w m_w Y_w + B' \] (2-64)

where $|B'| \leq sNb$. Looking at that $w$ such that $c_w = 1$ it is seen that if $t$ was selected sufficiently large then there is a contradiction, thus the theorem is proved.

One observes that $M'$ is $G$-isomorphic to the lattice having $\{X_w\}$ as a basis. Therefore one is able to decompose $M'$ into a direct sum
\[ M' = \bigoplus_{v \in S} \bigoplus_{w|^v} ZY_w \] (2-65)

and each subgroup
\[ M'_v = \bigoplus ZY_w \] (2-66)
is semilocal (i.e. $G$ permutes the factors $ZY_w$ transitively) with decomposition group $G_w$ for each $w$ acting trivially on the local component $ZY_w$ which is $G_w$-isomorphic to $Z$-itself.

One can now apply the semilocal theory, and the $Q$-machine.

**Lemma 1**

*Let $G$ be cyclic of order $N$ then*

$$Q(G, M) = Q(G, M') = \prod_{v \in \mathbb{S}} N_v$$

*where $N_v$ is the order of the composition group $G_w$ for any $w | v$*

**Proof:**

It could be written:

$$Q(G, M') = \prod_{v \in \mathbb{S}} Q(G, M'_v) = \prod_{v \in \mathbb{S}} Q(G_v, ZY_v)$$

and $Q(G_w, Z) = N_w$ so this Lemma follows because $(M : M')$ is finite.

**Lemma 2**

*Let $K / k$ be cyclic of order $N$ and let $K_S$ be the $S$-units in $K$ then*

$$Q(G, K_S) = \frac{1}{N} \prod_{v \in \mathbb{S}} N_v$$

**Proof:**

The map

$$L : K_S \rightarrow E^s$$

Given by

$$L(\xi) = \sum_{w \in S_K} \log ||\xi|| X_w \quad (w \in S_K)$$

is a $G$-homomorphism of $K_S$ into $E^s$ whose image is a lattice in a hyperplane of $E^s$, and whose kernel is finite. Let $X_0$ be the vector

$$X_0 = \sum_{w \in S_K} X_w$$

then $X_0$ and $L(K_S)$ generate a lattice $M$ in $E^s$ to which one can apply Theorem 5. The $Q$-machine gives:

$$Q(M') = Q(M) = Q(L(K_S))Q(Z)$$

but $Q(Z) = N$ this proves the Lemma.

**2.4 Formalism of the Artin Symbol**
Let $K/k$ be an abelian extension, and let $\mathfrak{p}$ be a prime of $k$ which is unramified in $K$ one should know that there exists a unique element $\sigma$ of the Galois group $G$ lying in the decomposition group $G_{\mathfrak{p}}$ (for any $\beta|\mathfrak{p}$ they all coincide in the abelian case) having the effect [17]

$$\sigma\alpha \equiv \alpha^{\mathfrak{p}} \pmod{\beta} \quad \alpha \in \mathcal{O}_K$$

(2-74)

This element $\sigma$ depends only on $\mathfrak{p}$ and is denoted by $(\mathfrak{p}, K/k)$ and will be called the Artin Symbol of $\mathfrak{p}$ in $G$.

Consider the map

$$\mathfrak{p} \mapsto (\mathfrak{p}, K/k)$$

(2-75)
to the subgroup $I(\partial)$ of fractional ideals prime to the discriminant $\partial$ of $K/k$, by multiplicativity. In the other word, if $a$ is prime to $\partial$ and

$$a = \prod \mathfrak{p}^{\nu_{\mathfrak{p}}}$$

(2-76)

then define

$$(a, K/k) = \prod (\mathfrak{p}, K/k)^{\nu_{\mathfrak{p}}}$$

(2-77)
call again $(a, K/k)$ the Artin Symbol of $a$, and the map

$$a \mapsto (a, K/k)$$

(2-78)
is a homomorphism

$$\omega : I(\partial) \to G(K/k)$$

(2-79)
which will also be called the reciprocity law map, or the Artin map.

### 3. Class Fields

Let $K/k$ be an abelian extension. For any admissible cycle $c$ there is an isomorphism

$$J/k * N^K_j K \approx I(c) / P^{N(c)}_c$$

(3-1)

where $N(c) = N(c, K/k)$ denotes the subgroup of $I(c)$ consisting of all norms $N^K_j K$ where $N$ is the fractional ideal of $K$ prime to $c$ (i.e. by definition, relatively prime to every prime ideal $\beta$ of $K$ lying above some prime ideal $\mathfrak{p} | c$).

The subgroup

$$P^{N(c)}_c \subset I(c)$$

(3-2)
is of great importance in class field theory. It is useful only if $c$ is admissible for $K/k$. This isomorphism allows us therefore to define the Artin map for ideals, and can get a map

$$\omega : J_k \to G(K/k)$$

(3-3)

Also denoted by

$$a \mapsto (a, K/k)$$

(3-4)
which one may once more describe explicitly as follows. Select $\alpha \in k^*$ such that

$$\alpha a \equiv 1 \pmod{c}$$

(3-5)

If $a$ is the associated ideal of $\alpha a$ then

$$(a, K/k) = (a, K/k)$$

(3-6)
This is well-defined. Observe that from the definition, one gets
For all $\alpha \in k^*$ thus the Artin map on ideles may be viewed as defined on the idele classes, and yields an isomorphism

$$C_k / N_k^K C_k \approx G(K / k) \tag{3-8}$$

If $a$ is an idele, and $a_v$ its $v$-component for $v \in M_k$ then one will identify $a_v$ with the idele whose $v$-component is $a_v$ and having component 1 at all $v' \in M_k$, $v' \neq v$ thus one is able to write the correspondence

$$a_v \leftrightarrow (\ldots, 1, 1, a_v, 1, 1, \ldots) \tag{3-9}$$

for $a_v \in k^*_v$. If $a$ is an idele, then $a_v$ is a unit for almost all $v$ let $S$ be a finite set of absolute values on $k$ containing the archimedean ones and all $v$ which are ramified in $K$. Let $S$ also contains those $v$ at which $a_v$ is not a unit. If $v \notin S$ then $a_v$ is a local norm, and hence the idele

$$a^S = \prod_{v \in S} a_v \tag{3-10}$$

is in $N_k^K J_K$. Hence $(a, K / k) = 1$ and

$$(a, K / k) = \prod_{v \in S} (a_v, K / k) \tag{3-11}$$

Since $(a_v, K / k) = 1$ for all but a finite number of $v$ one may summarize the preceding discussion in a theorem as follows:

**Theorem 7**

Let $K / k$ be abelian. The Artin map $a \mapsto (a, K / k)$ induces an isomorphism

$$C_k / N_k^K C_k = J_k / k * N_k^K J_K \approx G(K / k) \tag{3-12}$$

and for any idele $a$, the relation (3-13) will be concluded $[17]$

$$(a, K / k) = \prod_{v \in M_k} (a_v, K / k) \tag{3-13}$$

Next one has the formal properties of the symbol $(a, K / k)$ similar to the symbol for ideals.

**Theorem 8**

The map $K \to N_k^K C_k$ (resp. $K \to k * N_k^K J_K$) establishes a bijection between finite abelian extensions of $k$ and open subgroups of $C_k$ (resp. of $J_k$, containing $k *$). If $K$ belongs to $H$ and $K'$ belongs to $H'$, then $K \subset K'$ if and only if $H \supset H'$. Furthermore, $KK'$ belongs to $H \cap H'$, and $K \cap K'$ belongs to $HH'$ $[17]$.

**Proof:**

Suppose that $H$ belongs to $K$ and $H'$ belongs to $K'$. The kernel of the Artin map

$$C_k \to G(KK'/k) \tag{3-14}$$
is $H \cap H'$, because of the consistency property below:

Let $K' \supset K \supset k$ be a bigger abelian extension. Then could be written:

$$\text{res}_k (a, K'/k) = (a, K/k) \quad (3-15)$$

Therefore $H \cap H'$ belongs to $KK'$. If $K \subset K'$, it follows from the transitivity of the norm that $H \supset H'$. Conversely, if $H \supset H'$, then $H \cap H' = H'$, and

$$(C_k : H') = [K' : k] = [KK' : k] \quad (3-16)$$

since $k \subset K' \subset KK'$, we conclude that $KK' = K'$, whence $K \subset K'$.

This proves the theorem, except for the fact that every open subgroup of $C_k$ belongs to an abelian extension. For this section of the proof, refer to [17].

**Lemma 3**

Let $K/Q$ be an abelian extension of the rationals. Then $K$ is cyclotomic, i.e. there is a root of unity $\zeta$ such that $K \subset Q(\zeta)$.

**Proof:**

Let $mv_{\infty}$ be an admissible cycle for $K/Q$, and let $H$ be the class group of $K$. Then

$$H_m = QW_{mv_{\infty}} \subset H \quad (3-17)$$

whence $K \subset Q(\zeta_m)$ by Theorem 8. This Lemma is a conclusion of Kronecker's Theorem.

**Theorem 9**

Let $K/k$ be the class field of $H$, and let $E/k$ be finite. Then $KE/E$ is the class field of $N_{E/k}(H)[17]$.

**Proof:**

The Kernel of the Artin map

$$C_E \rightarrow G(KE/E) \quad (3-18)$$

is precisely equal to $N_{E/k}(H)$ because for $b \in C_E$ could be written:

$$\text{res}_k (b, KE/E) = (N_{E} \epsilon b, K/k) \quad (3-19)$$

and an automorphism of $KE/E$ is determined by its effect on $K$. This proves the theorem.
References


Received: November, 2008