수학강의록 제1권

TOPICS IN ALGEBRA, ALGEBRAIC GEOMETRY AND NUMBER THEORY I

김명환(편저)

서울대학교
수학연구소
대역해석학 연구센터

PREFACE

These lecture notes are designed to present basic tools in the research area related to algebra, algebraic geometry, and number theory. The lectures were given at Seoul National University in 1990.

It is a great honor that this book is selected to be the first volume of the lecture notes series of the Research Institute of Mathematics at Seoul National University. We hope this book can help the readers to overcome the gap between the graduate courses and the actual research in the above mentioned subjects.

We are indebted to many people – Professors Y. Ko, J.M. Chung, Y.H. Cho, I.-S. Lee, to name a few – for their invaluable helps ; especially to Professor O.K. Yoon, the director of RIM at SNU. Our thanks also go to Mrs. Park for her excellent TeXing of our manuscripts.

authors

CONTENTS

INTRODUCTION TO GROUP COHOMOLOGY

JAE MOON KIM

Contents

Introduction

The purpose of this lecture is to give a short introduction to the cohomology theory of groups, which plays a critial role in abstract class field theory, as formulated by Artin and Tate. With this in mind, some examples are taken from number fields. You may ignore them if you have never studied number fields before since they are not required for later use in this context.

I would like to put some emphasis on the first section of this lecture note. The first half of the first section consists of boring definitions. But you have to get through them. Once you get used to those definitions, you are half way through. I also recommend you to read the construction of cohomology theory carefully appearing in the second half of the same section. It not only gives you confidence in computing cohomology groups but also has many similarities to other cohomology theories. The remaining sections are treated shortly. It does not mean, however, that they are less important than the first one. The philosoply is that once you have a good understanding of the first section, the rest will be natural and interesting. So I left many of the details as exercises. Since they will be used later, I encourage you to try all of them.

My sincere thanks are due to professors R. Gold and K. Rubin at Ohio State University. This lecture note is based on two lectures I took from them.

§1. Cohomology of finite groups

Let G be a finite group. By a G-module we mean an abelian group A on which G acts (equivalently, A is a $\mathbf{Z}[G]$-module). For given G-modules A and B, a group homomorphism $u : A \to B$ is called a G-homomorphism if it preserves the G-actions; that is,

$$u(\sigma a) = \sigma u(a)\ \forall \sigma \in G,\ a \in A.$$

Denote by $\mathrm{Hom}_G(A, B)$ the set of all G-homomorphisms $A \to B$ and by $\mathrm{Hom}_{\mathbf{Z}}(A, B)$ the set of all group homomorphisms. We can make the abelian group $\mathrm{Hom}_{\mathbf{Z}}(A, B)$ into a G-module by defining

$$\sigma.f = \sigma \circ f \circ \sigma^{-1},\ \text{i.e.,}\ (\sigma.f)(a) = \sigma f(\sigma^{-1}a)\ \forall a \in A,\ \sigma \in G.$$

Note that

$$\mathrm{Hom}_G(A, B) = \mathrm{Hom}_{\mathbf{Z}}(A, B)^G$$

where M^G means the set of elements of M which are invariant under G.

DEFINITION 1.1. A G-module A is called G-regular if there is $\rho \in \mathrm{Hom}_{\mathbf{Z}}(A, A)$ such that

$$\sum_{\sigma \in G} \sigma \circ \rho(\sigma^{-1}a) = a \ \forall a \in A.$$

REMARK. For any x in a G-module M, the norm of x, written by Nx, is defined by

$$Nx = \sum_{\sigma} \sigma x.$$

Under this definition, the condition in Definition 1.1 simply states that $N\rho = 1_A$.

EXERCISE 1.1. Show that $\mathbf{Z}[G]$ is G-regular.

(Hint : Define $\rho : \sum n_\sigma \sigma \mapsto n_1 \cdot 1$).

For any two G-modules A, B, the abelian group $A \otimes_{\mathbf{Z}} B$ is a G-module under $\sigma(a \otimes b) = \sigma a \otimes \sigma b$.

EXERCISE 1.2. If A is G-regular, then for any G-module B, $A \otimes_{\mathbf{Z}} B$ is G-regular, Hence, in particular, $\mathbf{Z}[G] \otimes B$ is G-regular for any B.

Now we introduce some terminologies taken from homological algebra. But all the definitions are given only for G-modules. A functor, for example, means a functor (in usual sense) from the category of G-modules to the category of abelian groups.

DEFINITION 1.2. A connected sequence of functors $\{F^i\}_{a \leq i \leq b}$ is a collection of functors so that for every short exact sequence (will be abbreviated by s.e.s. from now on)

$$E : 0 \to A \xrightarrow{u} B \xrightarrow{v} C \to 0$$

of G-modules, there is a homomorphism (called the connecting homomorphism)

$$\partial_E^i : F^i(C) \to F^{i+1}(A) \quad \text{for} \quad a \leq i < b.$$

Definition 1.3. A connected sequence of functors $\{F^i\}_{a\leq i\leq b}$ is called cohomological (resp. exact cohomological) if

(i) For each s.e.s. $E : 0 \to A \overset{u}{\to} B \overset{v}{\to} C \to 0$, the sequence

$$F^a(A) \to \cdots \to F^{i-1}(C) \xrightarrow{\partial_E^{i-1}} F^i(A) \xrightarrow{F^i(u)} F^i(B) \xrightarrow{F^i(v)} F^i(C)$$
$$\xrightarrow{\partial_E^i} F^{i+1}(A) \to \cdots \to F^b(C)$$

is a complex (resp. exact).

(ii) If

$$\begin{tikzcd}
E : 0 \arrow[r] & A \arrow[r, "u"] \arrow[d, "\alpha"] & B \arrow[r, "v"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
E' : 0 \arrow[r] & A' \arrow[r, "u'"] & B' \arrow[r, "v'"] & C' \arrow[r] & 0
\end{tikzcd}$$

has exact rows and commutative squares, then

$$\begin{tikzcd}
F^i(C) \arrow[r, "\partial_E^i"] \arrow[d, "F^i(\gamma)"'] & F^{i+1}(A) \arrow[d, "F^{i+1}(\alpha)"] \\
F^i(C') \arrow[r, "\partial_{E'}^i"] & F^{i+1}(A')
\end{tikzcd}$$

commutes for $a \leq i < b$.

Remark. Condition (ii) in the definition 1.3 plus the definition of a functor guarantees the conmutativity of

$$\begin{tikzcd}
{} \arrow[r] & F^{i-1}(C) \arrow[r] \arrow[d] & F^i(A) \arrow[r] \arrow[d] & F^i(B) \arrow[r] \arrow[d] & F^i(C) \arrow[r] \arrow[d] & F^{i+1}(A) \arrow[r] \arrow[d] & {} \\
{} \arrow[r] & F^{i-1}(C') \arrow[r] & F^i(A') \arrow[r] & F^i(B') \arrow[r] & F^i(C') \arrow[r] & F^{i+1}(A') \arrow[r] & {}
\end{tikzcd}$$

Definition 1.4. Let $\{F^i\}$ and $\{H^i\}$ be two connected sequences of functors. Let $\varphi^i : F^i \to H^i$ be a morphism. The collection $\varphi = \{\varphi^i\}$

is said to be a morphism of connected sequence $\{F^i\} \xrightarrow{\varphi} \{H^i\}$ if for any s.e.s $0 \to A \xrightarrow{u} B \xrightarrow{v} C \to 0$,

$$\begin{tikzcd}
F^i(C) \arrow[r, "\partial^i"] \arrow[d, "\varphi^i(C)"'] & F^{i+1}(A) \arrow[d, "\varphi^{i+1}(A)"] \\
H^i(C) \arrow[r, "\partial^i"] & H^{i+1}(A)
\end{tikzcd}$$

is commutative.

Remark. Definition 1.4 and the definition of a morphism of functors imply the commutativity of

$$\begin{tikzcd}
{} \arrow[r] & F^{i-1}(C) \arrow[r] \arrow[d] & F^i(A) \arrow[r] \arrow[d] & F^i(B) \arrow[r] \arrow[d] & F^i(C) \arrow[r] \arrow[d] & F^{i+1}(A) \arrow[r] \arrow[d] & {} \\
{} \arrow[r] & H^{i-1}(C) \arrow[r] & H^i(A) \arrow[r] & H^i(B) \arrow[r] & H^i(C) \arrow[r] & H^{i+1}(A) \arrow[r] & {}
\end{tikzcd}$$

Definition 1.5. A functor F is called effaceable if for every G-module A, there is a G-monomorphism $A \xrightarrow{u} B$ so that $F(u) = 0$ and coeffaceable if for every G-module A, there is a G-epimorphism $B \xrightarrow{u} A$ so that $F(u) = 0$.

Definition 1.6. If $\{F^i\}_{i=1,2}$ and $\{H^i\}_{i=1,2}$ are connected sequences of functors and if $\varphi^1 : F^1 \to H^1$ is a morphism of functors, then any morphism $\varphi^2 : F^2 \to H^2$ so that

$$\varphi = \{\varphi^1, \varphi^2\} : \{F^i\}_{i=1,2} \to \{H^i\}_{i=1,2}$$

is a morphism of connected sequence is called an extension (upward) of φ^1 to $F^2 \to H^2$. Conversely if φ^2 is given then any $\varphi^1 : F^1 \to H^1$ so that $\{\varphi^1, \varphi^2\}$ is a morphism of connected sequence is called an extension (downward) of φ^2.

Now we give a lemma (without proof) on the extension of morphisms of functors that is of fundamental importance.

Main lemma.

(a) Suppose $\{F^i\}_{i=1,2}$ is an exact cohomological sequence with F^2 effaceable. Suppose $\{H^i\}_{i=1,2}$ is cohomological. Then any morphism $\varphi^1 : F^1 \to H^1$ has a unique extension $\varphi^2 : F^2 \to H^2$.

(b) Suppose $\{F^i\}_{i=1,2}$ is cohomological and $\{H^i\}_{i=1,2}$ is exact cohomological with H^1 coeffaceable. Then any morphism $\varphi^2 : F^2 \to H^2$ has a unique extension $\varphi^1 : F^1 \to H^1$.

Exercise 1.3. For any G-module A, let $F_G(A) = A^G/NA$, where

$$A^G = \{a \in A \,|\, \sigma a = a \;\forall \sigma \in G\} \text{ and } NA = \{Na \,|\, a \in A\}.$$

Show that F_G is well defined and that F_G is a functor.

Definition 1.7. A cohomology theory for G-modules is an exact cohomological sequence $\{F^n\}_{-\infty<n<\infty}$ of functors satisfying (i) $F^0 \approx F_G$ and (ii) $F^n(A) = 0$ for any G-regular module A and for all $n \in \mathbf{Z}$.
By (i), we mean there is a morphism $\varphi : F^0 \to F_G$ so that for each A, $\varphi(A) : F^0(A) \to F_G(A)$ is an isomorphism.

Theorem 1.1. *There exists a unique cohomology theory for G-modules up to isomorphism (The terminology "isomorphism" will become clear in the proof of the uniqueness).*

Proof of uniqueness. We need a lemma: if $F(A) = 0$ for every G-regular module A, then F is both effaceable and coeffaceable.

Proof of lemma. Define a G-homomorphism $\mu : \mathbf{Z} \to \mathbf{Z}[G]$ by

$$\mu(1) = N = \sum_{\sigma\in G} \sigma.$$

Then μ is a monomorphism, since μ followed by h is the identity on $\mathbf{Z}$, where $h : \mathbf{Z}[G] \to \mathbf{Z}$ is defined by $h(\sum n_\sigma \sigma) = n_1$. For any A, we have

$$\mathbf{Z} \otimes A \simeq A \xrightarrow{\mu\otimes 1_A} \mathbf{Z}[G] \otimes A.$$

Then $\mu \otimes 1_A$ is a G-monomorphism, since $(\mu \otimes 1_A) \circ (h \otimes 1_A) = 1$. By Exercise 1.2, $F(\mathbf{Z}[G] \otimes A) = 0$, so F is effaceable. For coeffaceable, we can prove in the same way by defining $\varepsilon : \mathbf{Z}[G] \to \mathbf{Z}$ by $\varepsilon(\sum n_\sigma \sigma) = \sum n_\sigma$ and $l : \mathbf{Z} \to \mathbf{Z}[G]$ by $l(1) = 1_G$.

Suppose $\{F^n\}_{n\in\mathbf{Z}}$ and $\{H^n\}_{n\in\mathbf{Z}}$ are two cohomology theories. The above lemma shows that each F^n and H^n is effaceable and coeffaceable. By axiom (i),

$$F^0 \approx F_G,\ H^0 \approx F_G.$$

Then there is an isomorphism $\varphi^0 : F^0 \to H^0$. Let ψ^0 be its inverse. Then, by the main lemma, φ^0 extends uniquely to $\varphi^q : F^q \to H^q$ for all $q \in \mathbf{Z}$ and ψ^0 extends uniquely to $\psi^q : H^q \to F^q$ for all $q \in \mathbf{Z}$. Then $\varphi^q \circ \psi^q$ extends $\varphi^0 \circ \psi^0 = 1_{H^0}$ and $\psi^q \circ \varphi^q$ extends $\psi^0 \circ \varphi^0 = 1_{F^0}$. But clearly the extension of the identity map is the identity map. So by the uniqueness of extension,

$$\psi^q \circ \psi^q = 1_{F^q} \text{ and } \varphi^q \circ \psi^q = 1_{H^q}.$$

So φ^q is an isomorphism for all q. This proves the uniqueness.

Proof of existence.

Let $G^n = G \times \cdots \times G$ be the n fold cartesian product of G. Let

$$X_n = \oplus_{(\sigma_1,\cdots,\sigma_n)\in G^n} \mathbf{Z}[G][\sigma_1, \cdots, \sigma_n]$$

be the free $\mathbf{Z}[G]$-module on symbols $[\sigma_1, \cdots, \sigma_n]$ and

$$X_0 = \mathbf{Z}[G][\cdot]$$

be free $\mathbf{Z}[G]$-module of rank 1 on symbol $[\cdot]$. We define G-homomorphism $d_n : X_n \to X_{n-1}$ for $n \geq 2$ by

$$\begin{aligned} d_n[\sigma_1, \sigma_2, \cdots, \sigma_n] &= \sigma_1[\sigma_2, \cdots, \sigma_n] \\ &+ \sum_{i=1}^{n-1} (-1)^i [\sigma_1, \cdots, \sigma_i\sigma_{i+1}, \cdots, \sigma_n] + (-1)^n [\sigma_1, \cdots, \sigma_{n-1}] \end{aligned}$$

and $d_1 : X_1 \to X_0$ by $d_1[\sigma] = \sigma[\cdot] - [\cdot]$.

Also define $\varepsilon : X_0 \to \mathbf{Z}$ by $\varepsilon[\cdot] = 1$.

Note that $\mathbf{Z}$ is a $\mathbf{Z}[G]$-module with the trivial action. So

$$\varepsilon(\sum_\sigma n_\sigma \sigma[\cdot]) = \sum_\sigma n_\sigma \sigma \varepsilon[\cdot] = \sum_\sigma n_\sigma \sigma \cdot 1 = \sum_\sigma n_\sigma.$$

Then

EXERCISE 1.4.

$$\cdots \to X_n \xrightarrow{d_n} X_{n-1} \to \cdots \to X_1 \xrightarrow{d_1} X_0 \xrightarrow{\varepsilon} \mathbf{Z} \to 0$$

is exact (Hint : Define a $\mathbf{Z}$-homomorphism $s_{n-1} : X_{n-1} \to X_n$ by

$$\sigma_0[\sigma_1, \cdots, \sigma_{n-1}] \overset{s_{n-1}}{\mapsto} [\sigma_0, \sigma_1, \cdots, \sigma_{n-1}],$$

and $\mu : \mathbf{Z} \to X_0$ by

$$\mu(1) = [\cdot].$$

Then $d_{n+1} \circ s_n + s_{n-1} \circ d_n = 1_{X_n}$, $d_1 \circ s_0 + \mu \circ d_0 = 1_{X_0}$.)

Define X_{-n} by $X_{-n} = \mathrm{Hom}_{\mathbf{Z}}(X_{n-1}, \mathbf{Z})$ for $n \geq 1$. Then

EXERCISE 1.5.

$$\cdots \to X_n \to X_{n-1} \to \cdots \to X_0 \xrightarrow{d_0} X_{-1} \xrightarrow{d_{-1}} X_{-2} \to \cdots \to X_{-n} \xrightarrow{d_{-n}} \cdots$$

is exact, where $d_0[\cdot] = \varepsilon$ and $d_n(f) = f \circ d_n$ for any $f \in X_{-n}$. (Hint : define s_{-n} as before.)

For a given G-module A, let $A_n = \mathrm{Hom}_G(X_n, A)$. Then we easily get a complex

$$\cdots \to A_{n-1} \xrightarrow{\partial^A_{n-1}} A_n \xrightarrow{\partial^A_n} A_{n+1} \to \cdots .$$

Define

$$F^n(A) = \mathrm{Ker}\, \partial^A_n / \mathrm{Im}\, \partial^A_{n-1}, \; n \in \mathbf{Z}.$$

We claim that this is the one we are looking for. For this, we have to check

(i) $\{F^n\}$ is a connected sequence of functors which is exact cohomological.

(ii) $F^n(A) = 0$ for any G-regular module A and $\forall a \in \mathbf{Z}$.

(iii) $F^0(A) \simeq A^G/NA$.

Proof of (i). Let $u : A \to B$ be a G-homomorphism. Then the map $A_n \to B_n$ defined by $f \mapsto u \circ f$ induces a homomorphism $F^n(u) : F^n(A) \to F^n(B)$. We leave the details to the reader to show that F^n is indeed a functor. Suppose $0 \to A \to B \to C \to 0$ is a G-module s.e.s. Then

Exercise 1.6. $0 \to A_n \to B_n \to C_n \to 0$ is exact for all n. Thus we get an exact sequence of complexes

$$\begin{tikzcd}
 & {} \arrow[d] & {} \arrow[d] & {} \arrow[d] & \\
0 \arrow[r] & A_{n-1} \arrow[r] \arrow[d] & B_{n-1} \arrow[r] \arrow[d] & C_{n-1} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A_n \arrow[r] \arrow[d] & B_n \arrow[r] \arrow[d] & C_n \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A_{n+1} \arrow[r] \arrow[d] & B_{n+1} \arrow[r] \arrow[d] & C_{n+1} \arrow[r] \arrow[d] & 0 \\
 & {} & {} & {} &
\end{tikzcd}$$

which induces the exact sequence

$$\cdots \to F^n(A) \to F^n(B) \to F^n(C) \to F^{n+1}(A) \to \cdots .$$

Proof of (ii). First, we show that $F^n(\mathbf{Z}[G] \otimes_{\mathbf{Z}} A) = 0$ for all $n \in \mathbf{Z}$ and for any G-module A. For this, we need

Exercise 1.7.

$$\mathrm{Hom}_G(B, \mathbf{Z}[G] \otimes A) \simeq \mathrm{Hom}_{\mathbf{Z}}(B, A)$$

for any G-modules A and B. (Hint : Define $\varphi : \mathrm{Hom}_G(B, \mathbf{Z}[G] \otimes A) \to \mathrm{Hom}_{\mathbf{Z}}(B, A)$ and $\psi : \mathrm{Hom}_{\mathbf{Z}}(B, A) \to \mathrm{Hom}_G(B, \mathbf{Z}[G] \otimes A)$ as follows. As was mentioned earlier, we have a map $h : \mathbf{Z}[G] \otimes A \to A$. Define

$$\varphi(f) = h \circ f \text{ and } \psi(g)(b) = \sum_{\sigma \in G} \sigma \otimes \sigma g(\sigma^{-1} b).)$$

Hence we have

$$\begin{tikzcd}
\cdots \arrow[r] & \mathrm{Hom}_G(X_{n-1}, \mathbf{Z}[G] \otimes A) \arrow[r] \arrow[d] & \mathrm{Hom}_G(X_n, \mathbf{Z}[G] \otimes A) \arrow[r] \arrow[d] & {} \\
\cdots \arrow[r] & \mathrm{Hom}_{\mathbf{Z}}(X_{n-1}, A) \arrow[r, "\Delta_{n-1}"] & \mathrm{Hom}_{\mathbf{Z}}(X_n, A) \arrow[r, "\Delta_n"] & {}
\end{tikzcd}$$

$$\begin{tikzcd}
\mathrm{Hom}_G(X_{n+1}, \mathbf{Z}[G] \otimes A) \arrow[r] \arrow[d] & \cdots \\
\mathrm{Hom}_{\mathbf{Z}}(X_{n+1}, A) \arrow[r] & \cdots
\end{tikzcd}$$

Therefore $F^n(\mathbf{Z}[G] \otimes A) \simeq \mathrm{Ker}\,\Delta_n / \mathrm{Im}\,\Delta_{n-1}$. But

EXERCISE 1.8.

$$\cdots \to \mathrm{Hom}_{\mathbf{Z}}(X_{n-1}, A) \to \mathrm{Hom}_{\mathbf{Z}}(X_n, A) \to \mathrm{Hom}_{\mathbf{Z}}(X_{n+1}, A) \to \cdots$$

is exact for all n. (Hint : Consider s_n) This shows

$$F^n(\mathbf{Z}[G] \otimes A) = 0.$$

Now suppose A is any G-regular module. Let $\rho : A \to A$ so that $N\rho = 1_A$. Define $l : \mathbf{Z}[G] \otimes A \to A$ by

$$l(\sigma \otimes a) = \sigma\rho(\sigma^{-1}a)$$

and $\lambda : A \to \mathbf{Z}[G] \otimes A$ by

$$\lambda(a) = N \otimes a = \sum_{\sigma} \sigma \otimes a.$$

Then l and λ are G-homomorphisms satisfying $l \circ \lambda = 1_A$. Thus $F^n(l) \circ F^n(\lambda) = 1_{F^n(A)}$. So $F^n(\lambda)$ is an injection. But we know that $F^n(\mathbf{Z}[G] \otimes A) = 0$. This proves (ii).

Proof of (iii). While we are proving this, we will also calculate F^{-1} and F^1 explicitely. We analyze $X_{-1}, X_{-2}, d_0, d_{-1}, \partial_{-2}, \partial_{-1}, \partial_0$ and ∂_1 one by one.

(a) X_{-1} : By definition, $X_{-1} = \mathrm{Hom}_{\mathbf{Z}}(X_0, \mathbf{Z})$, where $X_0 = \mathbf{Z}[G][\cdot]$ has a free $\mathbf{Z}$-basis composed of elements $\sigma[\cdot]$. Define a $\mathbf{Z}$-homomorphism $\tau(\cdot) : \mathbf{Z}[G][\cdot] \to \mathbf{Z}$ by

$$\tau(\cdot)(\sigma[\cdot]) = \begin{cases} 1 & \text{if } \sigma = \tau \\ 0 & \text{if } \sigma \neq \tau. \end{cases}$$

Then $\tau(\cdot)$ form a free $\mathbf{Z}$-basis for X_{-1}. So

$$X_{-1} = \oplus_{\tau\in G}\mathbf{Z}\tau(\cdot) = \mathbf{Z}[G](\cdot)$$

is a free $\mathbf{Z}[G]$-module on symbol $(\cdot)$.

(b) X_{-2} : Similarly, define a $\mathbf{Z}$-homomorphism $\tau(\sigma) : X_1 \to \mathbf{Z}$ by

$$\tau(\sigma)(\rho[\mu]) = \begin{cases} 1 & \text{if } \rho = \tau \text{ and } \sigma = \mu \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$X_{-2} = \oplus_{\tau,\sigma\in G}\mathbf{Z}\tau(\sigma) = \oplus_{\sigma\in G}\mathbf{Z}[G](\sigma)$$

is a free $\mathbf{Z}[G]$-module on symbols $(\sigma)_{\sigma\in G}$.

(c) d_0 : $d_0[\cdot] = \varepsilon$, where $\varepsilon = \sum_{\sigma\in G}\sigma(\cdot) = N(\cdot)$ (check this). Hence $d_0[\cdot] = N(\cdot)$.

(d) d_{-1} : d_{-1} is a G-homomorphism $X_{-1} \to X_{-2}$.

$$d_{-1}(\cdot)[\sigma] = (\cdot)d_1[\sigma] = (\cdot)(\sigma[\cdot] - [\cdot]) = \begin{cases} 0 & \text{if } \sigma = 1 \\ 1 & \text{if } \sigma \neq 1. \end{cases}$$

Check that $\sum_\tau(\tau - 1)(\tau^{-1}) \in X_{-2}$ has the same value on each $[\sigma]$. Hence $d_{-1}(\cdot) = \sum_\tau(\tau - 1)(\tau^{-1})$.

Next we analyze $\partial_{-2}, \partial_{-1}, \partial_0$ and ∂_1. Note that

$$\begin{aligned} \mathrm{Hom}_G(X_n, A) &= \{\text{maps} : G^n \to A\} \text{ for } n \geq 1 \\ \mathrm{Hom}_G(X_0, A) &= \{\text{maps} : [\cdot] \to A\} = A \\ \mathrm{Hom}_G(X_{-1}, A) &= \{\text{maps} : (\cdot) \to A\} = A, \text{ and} \\ \mathrm{Hom}_G(X_{-n}, A) &= \{\text{maps} : G^{n-1} \to A\}. \end{aligned}$$

(e) ∂_{-2} : $\mathrm{Hom}_G(X_{-2}, A) = \{\text{maps} : G \to A\} \to \mathrm{Hom}_G(X_{-1}, A) = A$. Take $f \in \mathrm{Hom}_G(X_{-2}, A)$. So f is identified with a map $G \to A$. $\partial_{-2}(f)$ is determined by its value at $(\cdot)$.

$$\begin{aligned} \partial_{-2}(f)(\cdot) &= f \circ d_{-1}(\cdot) \\ &= f(\sum_\sigma(\sigma - 1)(\sigma^{-1})) \\ &= \sum_\sigma(\sigma - 1)f(\sigma^{-1}). \end{aligned}$$

(f) $\partial_{-1} : \mathrm{Hom}_G(X_{-1}, A) = A \to \mathrm{Hom}_G(X_0, A) = A$. Take $a \in A$, which comes from $f_a \in \mathrm{Hom}_G(X_{-1}, A)$ with $f_a(\cdot) = a$. Then

$$\partial_{-1}(a) = \partial_{-1} f_a : X_0 \to A.$$
$$\partial_{-1} f_a[\cdot] = f_a d_0[\cdot] = f_a(N(\cdot)) = N f_a(\cdot) = Na.$$

Hence $\partial_{-1}(a) = Na$.

(g) $\partial_0 : \mathrm{Hom}_G(X_0, A) = A \to \mathrm{Hom}_G(X_1, A) = \{\text{maps} : G \to A\}$. Take $a \in A$ coming from $f_a \in \mathrm{Hom}_G(X_0, A)$ such that $f_a[\cdot] = a$.

$$\partial_0 a = \partial_0 f_a : X_1 \to A.$$
$$\partial_0 f_a[\sigma] = f_a d_1[\sigma] = f_a(\sigma[\cdot] - [\cdot]) = \sigma a - a = (\sigma - 1)a.$$

Hence $\partial_0 a$ is the map from G to A such that $(\partial_0 a)(\sigma) = (\sigma - 1)a$.

(h) $\partial_1 : \mathrm{Hom}_G(X_1, A) = \{\text{maps} : G \to A\} \to \mathrm{Hom}_G(X_2, A) = \{\text{maps} : G \times G \to A\}$. Take $f : G \to A$.

$$\begin{aligned}(\partial_1 f)(\sigma, \tau) &= f d_2[\sigma, \tau] \\ &= f(\sigma[\tau] - [\sigma\tau] + [\sigma]) \\ &= \sigma f(\tau) - f(\sigma\tau) + f(\sigma).\end{aligned}$$

Therefore,

$$\begin{aligned}
\mathrm{Im}\,\partial_{-2} &= \{\sum_\sigma (\sigma - 1) f(\sigma^{-1}) \,|\, f \in \{\text{maps} : G \to A\}\} \\
&= \{\sum_\sigma (\sigma - 1) a_\sigma \,|\, a_\sigma \in A\} = IA \text{ (notation)} \\
\mathrm{Ker}\,\partial_{-1} &= \{a \in A \,|\, Na = 0\} = {}_N A \text{ (notation)} \\
\mathrm{Im}\,\partial_{-1} &= \{Na \,|\, a \in A\} = NA \text{ (notation)} \\
\mathrm{Ker}\,\partial_0 &= \{a \in A \,|\, (\partial_0 a)(\sigma) = (\sigma - 1)a = 0 \ \forall \sigma\} \\
&= \{a \in A \,|\, \sigma a = a \ \forall \sigma\} = A^G \\
\mathrm{Im}\,\partial_0 &= \{\text{maps}\, G \xrightarrow{f} A \,|\, f(\sigma) = (\sigma - 1)a \text{ for some } a \in A\} \\
\mathrm{Ker}\,\partial_1 &= \{\text{maps}\, G \xrightarrow{f} A \,|\, f(\sigma\tau) = \sigma f(\tau) + f(\sigma) \ \forall \sigma, \tau \in G\}.
\end{aligned}$$

Elements of Ker ∂_1 are called crossed homomorphism and those of Im ∂_0 are called trivial crossed homomorphisms. Summarizing all the discussion :

$$\begin{aligned} F^{-1}(A) &= {}_N A/IA, \\ F^0(A) &= A^G/NA, \\ F^1(A) &= \frac{\{\text{crossed homo}\}}{\{\text{trivial crossed homo}\}}. \end{aligned}$$

This finishes the proof of theorem and more.

From now on, we shall write $H^n(G,A)$ for $F^n(A)$ and u_n for $F^n(u)$ for each $u : A \to B$. The object from here on is to find as much information about the groups $H^n(G,A)$.

EXAMPLES.

(1) Suppose a group G with g elements acts on A trivially, then

$$\begin{aligned} H^{-1}(G,A) &= {}_g A = \{a \in A \mid ga = 0\} \\ H^0(G,A) &= A/gA, \ gA = \{ga \mid a \in A\} \\ H^1(G,A) &= \mathrm{Hom}_{\mathbf{Z}}(G,A). \end{aligned}$$

(2) Let F be a Galois extension of a field K. Let $G = Gal(F/K)$. Then

$$H^1(G,F^\times) = 0.$$

Proof. Let $\varphi : G \to F^\times$ be a crossed homomorphism. We want $a \in F^\times$ such that $\varphi(\sigma) = (\sigma - 1)a = \dfrac{a^\sigma}{a}\ \forall \sigma$. By the linear independence of characters, $\sum_\sigma \varphi(\sigma)\sigma$ is not 0. Hence there exists an element $x \in F^\times$ such that $b = \sum \varphi(\sigma)x^\sigma \neq 0$. Then

$$\begin{aligned} b^\tau &= (\sum_\sigma \varphi(\sigma)x^\sigma)^\tau \\ &= \sum_\sigma \tau\varphi(\sigma)x^{\tau\sigma} \\ &= \sum_\sigma \frac{\varphi(\tau\sigma)}{\varphi(\tau)}x^{\tau\sigma} \\ &= \frac{1}{\varphi(\tau)}b. \end{aligned}$$

So $\varphi(\tau) = \dfrac{b}{b^\tau}$. Take $a = \dfrac{1}{b}$.

(3) Under the same situation as in (2),

$$H^n(G, F) = 0 \text{ for all } n \in \mathbf{Z}.$$

Proof. By the normal basis theorem, there exists an element $\mathcal{O} \in F$ such that $\{\mathcal{O}^\sigma \mid \sigma \in G\}$ is a basis for F over K. So

$$F \simeq \oplus_\sigma K\mathcal{O}^\sigma \simeq K[G],$$

which is G-regular (why ?). Hence $H^n(G, F) = 0$.

Exercise 1.9. Let $^{\#}(G) = g$. Then

$$gH^i(G, A) = 0 \ \forall A,\ \forall i.$$

(Hint: Main lemma. Also note that a multiplication by an integer is a morphism).

Exercise 1.10. Let $u : A \to B$ be a G-homomorphism. Then

(i) $u_{-1} : H^{-1}(G, A) \to H^{-1}(G, B)$ is defined by

$$u_{-1}(a + IA) = u(a) + IB.$$

(ii) $u_0 : H^0(G, A) \to H^0(G, B)$ is defined by

$$u_0(a + NA) = u(a) + NB.$$

(iii) $u_1 : H^1(G, A) \to H^1(G, B)$ is defined by

$$u_1(\bar{f}) = \overline{u \circ f},$$

where $\bar{f}$ and $\overline{u \circ f}$ are the reductions of f and $u \circ f$ by trivial crossed homomorphisms.

EXERCISE 1.11. Let $0 \to A \xrightarrow{u} B \xrightarrow{v} C \to 0$ be a G-module s.e.s. Then

(i) $\partial^{-1} : H^{-1}(C) \to H^0(A)$ is defined as follows : Take $c \in {}_NC$. Choose $b \in B$ such that $v(b) = c$. Take the preimage a of Nb under u. Then $\partial^{-1}(c + IC) = a + NA$.

(ii) $\partial^0 : H^0(C) \to H^1(A)$ is defined as follows : $\forall c \in C^G$, choose $b \in B$ such that $v(b) = c$. Define $f_c : G \to A$ by $f_c(\sigma) = a_\sigma$, where $u(a_\sigma) = (\sigma - 1)b$.

EXERCISE 1.12. For each G-module A, define a functor $\tilde{H}$ by $\tilde{H}(A) = A^G$. Then $\tilde{H}$ is an left exact functor i.e., for any s.e.s. $0 \to A \to B \to C \to 0$,

$$0 \to A^G \to B^G \to C^G$$

is exact. Moreover there exists a unique exact cohomological connected sequence of functors $\{\tilde{H}^n\}_{n \geq 0}$ such that

$$\tilde{H}^n(A) = H^n(G, A) \text{ for } n \geq 1$$
$$\tilde{H}^0(A) = \tilde{H}(A) = A^G.$$

(Hint: just follow the proof of theorem keeping $n \geq 0$.)

§2. Cyclic case and the Herbrand quotient

Let G be any finite group (cyclic or not) and fix $\sigma \in G$. We define a morphism $\varphi^1_\sigma : H^1(G, *) \to H^{-1}(G, *)$ as follows : For a given G-module A, define

$$\varphi^1_\sigma(A) : H^1(G, A) \to H^{-1}(G, A)$$

by $\varphi^1_\sigma(f) = f(\sigma)$. This is well defined. Indeed, $Nf(\sigma) = \sum_\tau \tau f(\sigma) = \sum_\tau (f(\tau\sigma - f(\tau)) = 0$ and if f is a trivial crossed homomorphism, say $f(\sigma) = (\sigma - 1)a$ for some a, then $\varphi^1_\sigma(f) = f(\sigma) = (\sigma - 1)a \in IA$. By the main lemma, this morphism φ^1_σ extends (up and down) uniquely to

$$\varphi^i_\sigma : H^i(G, *) \to H^{i-2}(G, *).$$

This does not give much information about $H^i(G, A)$ in general. But when G is cyclic and σ is a generator of σ, these morphisms $\{\varphi^i_\sigma\}$ turn out to be quite useful.

Let $G = \langle\sigma\rangle$ be a finite cyclic group, and let $g = {}^{\#}G$. Define

$$\psi_\sigma^{-1}(A) : H^{-1}(G, A) \to H^1(G, A)$$

by $\psi_\sigma^{-1}(A)(a) = f_a$, where $f_a : G \to A$ is defined by $f_a(\sigma^i) = (\sigma^{i-1} + \cdots + \sigma + 1)a$. One can check that $\psi_\sigma^{-1} : H^{-1}(G, *) \to H^1(G, *)$ is a well defined morphism. By the main lemma, ψ_σ^{-1} extends to

$$\psi_\sigma^i : H^i(G, *) \to H^{i+2}(G, *).$$

It is easy to see $\psi_\sigma^{-1} \circ \varphi_\sigma^1 = id$, $\varphi_\sigma^1 \circ \psi_\sigma^{-1} = id$. Hence by the uniqueness of the main lemma $\varphi_\sigma^i(A)$ is an isomorphism $\forall i$ and for any G-module A. Therefore

THEOREM 2.1. *Let $G = \langle\sigma\rangle$ be a finite cyclic group. Then*

$$H^i(G, A) = \begin{cases} A^G/NA & \text{if } i = \text{even} \\ \\ {}_N A/IA & \text{if } i = \text{odd} \end{cases}$$

Note that when $G = \langle\sigma\rangle$ is cyclic, $IA = (\sigma - 1)A$.

EXERCISE 2.1. Suppose $H^i(G, A)$ is periodic with period 2 for every A, i.e., $H^i(G, A) = \begin{cases} H^0(G, A) & \text{if } i = \text{even} \\ \\ H^1(G, A) & \text{if } i = \text{odd} \end{cases}$. Then G is a cyclic group. (Hint: Consider

$$0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0$$

with trivial G-actions. Also use $H^1(G, \mathbf{Q}/\mathbf{Z}) = \mathrm{Hom}_{\mathbf{Z}}(G, \mathbf{Q}/\mathbf{Z}) = G/[G, G]$).

EXAMPLES.

(1) Hilbert Theorem 90 : Let F be a cyclic extension of K. Then $H^{-1}(G, F) = 0$ and $H^{-1}(G, F^X) = 0$. First part was treated in §1 and the second part comes from $H^{-1}(G, F^X) = H^1(G, F^X) = 0$.

(2) Given a number field L, we denote the ideal group, principal ideal group and ideal class group of L by I_L, P_L and C_L respectively. Also let E_L be the unit group of $\mathcal{O}$, the ring of integers of L. Let F,

K be two number fields such that F is a Galois extension of K with the Galois group G.

From the s.e.s. $0 \to E_F \to F^X \to P_F \to 0$, we have (see Ex 1.12) a long exact sequence

$$\begin{tikzcd}
0 \arrow[r] & E_F^G \arrow[r] \arrow[d, equal] & F^{X^G} \arrow[r] \arrow[d, equal] & P_F^G \arrow[r] & H^1(E_F) \arrow[r] & H^1(F^X) \arrow[r] \arrow[d, equal] & {} \\
& E_K & K^X & & & 0 & \\
& & H^1(P_F) \arrow[r] & H^2(E_F) \arrow[r] & H^2(F^X) \arrow[r] & \cdots &
\end{tikzcd}$$

So we get

$$\begin{cases} 0 \to E_K \to K^X \to P_F^G \to H^1(E_F) \to 0 \\ 0 \to H^1(P_F) \to H^2(E_F) \to H^2(F^X) \to \cdots \end{cases}$$

Therefore, $H^1(E_F) = P_F^G/P_K$, and $H^1(P_F) = \mathrm{Ker}(H^2(E_F) \to H^2(F^\times))$. From $0 \to P_F \to I_F \to C_F \to 0$, we have

$$0 \to P_F^G \to I_F^G \to C_F^G \to H^1(P_F) \to H^1(I_F) \to \cdots .$$

It is a fact that $H^1(G, I_F) = 0$. But it is an easy exercise that

Exercise 2.2. If G is cyclic, then $H^1(G, I_F) = 0$.

Anyway, we have

$$0 \to P_F^G/P_K \to I_F^G/P_K \to C_F^G \to H^1(P_F) \to 0.$$

The first term P_P^G/P_K was already studied : $P_F^G/P_K = H^1(E_F)$. For the second term, look at

$$0 \to I_K/P_K \to I_F^G/P_K \to I_F^G/I_K \to 0.$$

$I_K/P_K = C_K$, and $I_F^G/I_K = \oplus_p \mathbf{Z}/e_p\mathbf{Z}$, where p runs through all the prime (nonzero) ideals of $\mathcal{O}_F$ and e_p is the corresponding ramification index. Hence if the class number of K is 1, then the above sequence becomes

$$0 \to H^1(E_F) \to \oplus_p \mathbf{Z}/e_p\mathbf{Z} \to C_F^G \to \mathrm{Ker}(H^2(E_F) \to H^2(F^X)) \to 0.$$

Even if C_K is not trivial, we have the following Genus formula :

$$\#(C_F^G) = \#(C_K)\frac{(\Pi_p e_p)\#[\mathrm{Ker}(H^2(E_F) \to H^2(F^X))]}{\#(H^1(E_F))}$$

In particular, if G is cyclic,

$$\#(C_F^G) = \#(C_K)\frac{(\Pi_p e_p)\#[\mathrm{Ker}(H^0(E_F) \to H^0(K^X))]}{[{}_N E_F : E_F^{\sigma-1}]}.$$

We give a very special example when $F = \mathbf{Q}(\sqrt{-d})$ is an imaginary quadratic field and $K = \mathbf{Q}$. The followings are easy to check.

$$\begin{cases} H^1(E_F) = E_F/E_F^2 = \mathbf{Z}/2\mathbf{Z} \\ I_F^G/I_K = (\mathbf{Z}/2\mathbf{Z})^r, \text{ where } r = \#\text{ramified primes} \\ C_F^G = (C_F)_2 = 2 - \text{torsion of } C_F \\ \mathrm{Ker}(H^0(E_F) \to H^0(F^X)) = 0. \end{cases}$$

Hence

$$0 \to \mathbf{Z}/2\mathbf{Z} \to (\mathbf{Z}/2\mathbf{Z})^r \to (C_F)_2 \to 0$$

is exact, therefore $(C_F)_2 \simeq (\mathbf{Z}/2\mathbf{Z})^{r-1}$.

EXERCISE 2.3. (1) Work out when F is real quadratic. (2) As a consequence, when $F = \mathbf{Q}(\sqrt{p})$ with $p \equiv 1$ (4), $N\varepsilon = -1$ if ε is the fundamental unit.

DEFINITION 2.1. Let G be a finite cyclic group. For any G-module A, define the Herbrand quotient $h(A)$ of A by

$$h(A) = \frac{\#H^0(G,A)}{\#H^1(G,A)} \text{ if it exists.}$$

EXERCISE 2.4. (1) If A is finite, then $h(A) = 1$. (2) For a s.e.s. $0 \to A \to B \to C \to 0$, if two of $h(A)$, $h(B)$ and $h(C)$ are defined, then so is the third, and $h(B) = h(A)h(C)$.

Examples. (3) Let F, K be number fields, where F is a cyclic extension of K with the Galois group G. Then $h(\mathcal{O}_F) = 1$, where $\mathcal{O}_F$ is the ring of integers of F.

Proof. By the normal basis theorem, there exists $\alpha \in \mathcal{O}_F$ such that $\mathcal{O}'_F$, the $\mathcal{O}_K$-module generated by $\{\alpha^\sigma \mid \sigma \in G\}$, is of finite index in $\mathcal{O}_F$. Hence from the s.e.s.

$$\mathcal{O} \to \mathcal{O}'_F \to \mathcal{O}_F \to \mathcal{O}_F/\mathcal{O}'_F \to 0,$$

we have $h(\mathcal{O}_F) = h(\mathcal{O}'_F)h(\mathcal{O}_F/\mathcal{O}'_F) = h(\mathcal{O}'_F)$ by Ex 2.4. But $\mathcal{O}'_F = \mathcal{O}_K[G]$ is G-regular. Hence $H^i(\mathcal{O}'_F) = 0$ $^\forall i$.

(4) Let F, K and G as in Example (3). Then $h(E_F) = \frac{1}{[F:K]}$, where E_F is the unit group of F. This is true in general. But we prove only when $K = \mathbf{Q}$ and F is totally real, or $K =$ imaginary quadratic.

Proof. There exists a unit $\varepsilon \in E_F$ such that the subgroup E' generated by $\{\varepsilon^\sigma \mid \sigma \in G\}$ is of finite index in E_F with $N\varepsilon = 1$. So from

$$0 \to E' \to E \to \text{finite} \to 0,$$

$h(E_F) = h(E') = h(\mathbf{Z}[G]/\mathbf{Z}N) = \frac{h(\mathbf{Z}[G])}{h(\mathbf{Z}N)} = \frac{h(\mathbf{Z}[G])}{h(\mathbf{Z})} = \frac{1}{\#(G)}$.

(5) In the example (2), if we assume that the class number of K is 1, then we have an exact sequence:

$$0 \to H^1(E_F) \to \oplus_p \mathbf{Z}/p\mathbf{Z} \to C_F^G \to H^1(G, P_F) \to 0.$$

Suppose that $(\#G, \#E_K) = 1$. Then $H^0(G, E_F) = 0$ (why ?), which implies $H^1(G, P_F) = 0$ and $\#H^1(G, E_F) = \#G$. Therefore, $\#(C_F^G) = \#(\oplus_p \mathbf{Z}/e_p\mathbf{Z})/\#(G) = \frac{\Pi_p e_p}{[F:K]}$.

§3. Some basic maps

Let H be a subgroup of G. Since any G-module can be thought of as an H-module, we may consider $H^i(H, *)$ as functors of G-modules. The following lemma will be used throughout this section, especially when we use the main lemma stated in §1.

LEMMA 3.1. *If A is a G-regular module, then A is H-regular.*

Proof. Let $G = \cup_{s\in S} Hs$ be a coset decomposition. Let $\rho : A \to A$ be such that $N_G\rho = 1_A$. Define $\rho' = \sum_{s\in S} s\cdot\rho$. Then $N_H\rho'(a) = \sum_{\gamma\in H} \gamma\rho'\gamma^{-1}(a) = \sum_{\gamma\in H}\sum_{s\in S}\gamma s\rho(s^{-1}\gamma^{-1}a) = \sum_{\gamma\in H}\sum_{s\in S}(\gamma s)\rho((\gamma s)^{-1}a) = \sum_{\sigma\in G}\sigma\rho\sigma^{-1}(a) = a.$

EXERCISE 3.1. Check that $\{H^n(H,*)\}$ is an exact cohomological sequence of G-functors which is both effaceable and coeffaceable as G-functors.

Let $\sigma \in G$. Define a morphism

$$\sigma_0(A) : H^0(H,A) \to H^0(\sigma H\sigma^{-1}, A)$$

by $[a] \mapsto [\sigma a]$, check this is well defined and is a morphism. Since $H^n(H,*)$ is both effaceable and coeffaceable, we can extend this morphism to all levels

$$\sigma_n(A) : H^n(H,A) \to H^n(\sigma H\sigma^{-1}, A).$$

Obviously σ_n's are isomorphism (σ^{-1} yields the inverse).

EXERCISE 3.2. If $\sigma \in H$, then $\sigma_n : H^n(H,A) \to H^n(H,A)$ is the identity map for all $n \in \mathbf{Z}$.

REMARK. If H is normal in G, $H^n(H,A)$ becomes a G-module, hence a G/H-module by the above map σ_n.

We now define two morphisms ; *restriction* and *corestriction.* Let H be a subgroup of G. Define

$$\mathrm{res}_0^{G,H} : H^0(G,A) \to H^0(H,A)$$

by $[a] \mapsto [a]$. Check this is well defined and is a morphism. By the main lemma, $\mathrm{res}_0^{G,H}$ can be extended to arbitrary level;

$$\mathrm{res}_n^{G,H} : H^n(G,A) \to H^n(H,A).$$

EXERCISE 3.3. (i) $\mathrm{res}_1^{G,H} : H^1(G,A) \to H^1(H,A)$ is defined by $[f] \mapsto [f|_H]$.

(ii) $\mathrm{res}_{-1}^{G,H} : H^{-1}(G,A) \to H^{-1}(H,A)$ is defined by $[a] \mapsto [\sum_{s\in S} sa]$, where $G = \cup_{s\in S} Hs$ is a coset decomposition.

Define

$$\mathrm{cores}_0^{H,G} : H^0(H,A) \to H^0(G,A)$$

by $[a] \mapsto [\sum_{s\in S} sa]$, where $G = \cup_{s\in S} sH$ is a coset decomposition. Again this a well defined morphism which can be extended to arbitrary levels

$$\mathrm{cores}_n^{H,G} : H^n(H,A) \to H^n(G,A).$$

PROPOSITION 3.1. *res_n and cores_n are transitive and commute with σ_n. Namely, the following four diagrams are commutative. Let $H < K < G$.*

(i)

$$\begin{tikzcd}
H^n(G,A) \arrow[rr, "\mathrm{res}^{G,K}"] \arrow[dr, "\mathrm{res}^{G,H}"'] & & H^n(K,A) \arrow[dl, "\mathrm{res}^{K,H}"] \\
& H^n(H,A) &
\end{tikzcd}$$

(ii)

$$\begin{tikzcd}
H^n(G,A) & & H^n(K,A) \arrow[ll, "\mathrm{cores}^{K,G}"'] \\
& H^n(H,A) \arrow[ul, "\mathrm{cores}^{H,G}"] \arrow[ur, "\mathrm{cores}^{H,K}"'] &
\end{tikzcd}$$

(iii)

$$\begin{tikzcd}
H^n(K,A) \arrow[r, "\mathrm{res}"] \arrow[d, "\sigma_n"'] & H^n(H,A) \arrow[d, "\sigma_n"] \\
H^n(\sigma K\sigma^{-1},A) \arrow[r, "\mathrm{res}"] & H^n(\sigma H\sigma^{-1},A)
\end{tikzcd}$$

(iv)

$$\begin{tikzcd}
H^n(K,A) \arrow[d, "\sigma_n"'] & H^n(H,A) \arrow[l, "\mathrm{cores}"] \arrow[d, "\sigma_n"] \\
H^n(\sigma K^{\sigma^{-1}},A) & H^n(\sigma H\sigma^{-1},A) \arrow[l, "\mathrm{cores}"]
\end{tikzcd}$$

Proof. Check these diagrams at level $n = 0$ and use the main lemma. Details are left as exercises.

Suppose H is normal in G. Then from (iii), (iv) in Poposition 3.1 (with $K = G$), we have the following commutative diagrams.

$$\begin{tikzcd}
H^n(G,A) \arrow[r, "\text{res}"] \arrow[d, "\sigma_n = id"'] & H^n(H,A) \arrow[d, "\sigma_n"] \\
H^n(G,A) \arrow[r, "\text{res}"] & H^n(H,A)
\end{tikzcd}$$

and

$$\begin{tikzcd}
H^n(G,A) \arrow[d, "\sigma_n = id"'] & H^n(H,A) \arrow[l, "\text{cores}"'] \arrow[d, "\sigma_n"] \\
H^n(G,A) & H^n(H,A) \arrow[l, "\text{cores}"']
\end{tikzcd} .$$

Thus $^\forall x \in H^n(G,A)$, $\sigma_n(\text{res}\, x) = \text{res}(id\, x) = \text{res}\, x$. Hence $\text{res}\, x$ in fixed under G. Similarly, $\sigma_n x - x \in \text{Ker(cores)}$ for any $x \in H^n(H,A)$. Therefore we obtain

COROLLARY. Suppose H is normal in G. Then

(i) $\text{Im}(\text{res}_n^{G,H}) \subset H^n(H,A)^G = H^n(H,A)^{G/H}$
(ii) $I_G H^n(H,A) \subset \text{Ker}(\text{cores}_n^{H,G})$.

Therefore res and cores induce

(i)′ $\text{res}_n^{G,H} : H^n(G,A) \to H^n(H,A)^{G/H}$
(ii)′ $\text{cores}_n^{H,G} : H^n(H,A)/I_G H^n(H,A) \to H^n(G,A)$.

Now we compose res and cores in both ways.

(a) cores $\circ$ res

Let $m = (G : H)$. Then

$$\text{cores}_0^{H,G} \circ \text{res}_0^{G,H}([a]) = m[a]$$

for any $[a] \in H^0(G,A)$. Thus

$$\text{cores}_0^{H,G} \circ \text{res}_0^{G,H} = m = \text{multiplication by } m.$$

Therefore

$$\mathrm{cores}_n^{H,G} \circ \mathrm{res}_n^{G,H} = m$$

for all $n \in \mathbf{Z}$ by the main lemma. Namely, the following is commutative;

$$\begin{tikzcd}
H^n(G,A) \arrow[r, "\mathrm{res}"] \arrow[dr, "\times m"'] & H^n(H,A) \arrow[d, "\mathrm{cores}"] \\
 & H^n(G,A)
\end{tikzcd}$$

EXERCISE 3.4. Let $^{\#}(G) = g$. Then $gH^n(G,A) = 0$ for all $n \in \mathbf{Z}$ and for any G-module A. (Hint : Take $H = (0)$).

(b) res o cores

$\mathrm{res}_0^{G,H} \circ \mathrm{cores}_0^{H,G}([a]) = \mathrm{res}_0^{G,H}([\sum sa]) = [\sum sa]$. Define

$$\lambda_0 : H^0(H,A) \to H^0(H,A)$$

by $[a] \mapsto [\sum sa]$. Then λ_0 is a morphism which can be extended to arbitrary level

$$\lambda_n : H^n(H,A) \to H^n(H,A).$$

Since $\lambda_0 = \mathrm{res}_0^{G,H} \circ \mathrm{cores}_0^{H,G}$, the following is commutative for all $n \in \mathbf{Z}$;

$$\begin{tikzcd}
H^n(H,A) \arrow[r, "\mathrm{cores}"] \arrow[dr, "\lambda_n"'] & H^n(G,A) \arrow[d, "\mathrm{res}"] \\
 & H^n(H,A)
\end{tikzcd}$$

EXERCISES 3.5. If H is normal in G, then $\lambda_n = \sum_{s \in S} s_n$.

For any abelian group R and for any prime p, let R_p be the p-component of R i.e. $R_p = \{x \in R \,|\, p^m x = 0 \text{ for some } m\}$. So if R is finite, then R_p is the Sylow p-subgroup. Note that for any two Sylow p-subgroup G_p and G_p' of G,

$$H^n(G_p, A) \simeq H^n(G_p', A)$$

since they are conjugate. Fix a Sylow p-subgroup G_p of G. Let $n_p = (G : G_p)$. From $n_p = \text{cores} \circ \text{res}$, we have the following commutative diagram.

$$\begin{tikzcd}
H^n(G,A)_p \arrow[rr, "\text{res}"] \arrow[dr, "n_p"'] & & H^n(G_p,A) \arrow[dl, "\text{cores}"] \\
& H^n(G,A)_p &
\end{tikzcd}$$

EXERCISE 3.6. Check the above diagram.

But $n_p : H^n(G,A)_p \to H^n(G,A)_p$ is an isomorphism. Hence

$$\text{res} : H^n(G,A)_p \to H^n(G_p,A)$$

is 1-1 and

$$\text{cores} : H^n(G_p,A) \to H^n(G,A)_p$$

is onto. Therefore we proved

PROPOSITION 3.2.
(i) $H^n(G,A) = \oplus_p H^n(G,A)_p = \oplus_p cores(H^n(G_p,A))$
(ii) So if $H^n(G_p,A) = 0$ *for all* p*, then* $H^n(G,A) = 0$.

Suppose G_p *is normal in* G*. Then*

$$res : H^n(G,A)_p \to H^n(G_p,A)^G$$

is an isomorphism. To see this, look at the following commutative diagram

$$\begin{tikzcd}
H^n(G_p,A)^G \arrow[rr, "\text{cores}"] \arrow[dr, "\lambda_n"'] & & H^n(G,A)_p \arrow[dl, "res"] \\
& H^n(G_p,A)^G &
\end{tikzcd}$$

But $\lambda_n = \sum_{s \in S} s_n = n_p$ *on* $H^n(G_p,A)^G$*, which is an isomorphism. Thus res is onto. Therefore*

PROPOSITION 3.3. *If* G_p *is normal in* G*, then*

$$H^n(G,A)_p \simeq H^n(G_p,A)^G.$$

Hence, if G_p *is normal for all* p*, then*

$$H^n(G,A) \simeq \oplus_p H^n(G,A)_p \simeq \oplus_p H^n(G_p,A)^G$$

EXERCISE 3.7. Let H be a subgroup of G. Let $^{\#}(H) = h$ and $(G : H) = m$. Suppose $(h, m) = 1$. Then

(i) res : $H^n(G, A)_h \to H^n(H, A)$ is 1-1 and cores : $H^n(H, A) \to H^n(G, A)_h$ is onto, where $H^n(G, A)_h = \{x \in H^n(G, A) \mid hx = 0\}$.

(ii) If H is normal in G, then res : $H^n(G, A)_h \to H^n(H, A)^G$ is an isomorphism.

We introduce the inflation map. Let H be a normal subgroup of G. For any G/H-module B, B has a natural G-module structure by $\sigma b = \bar{\sigma} b$ for any $\sigma \in G$. Define a morphism

$$\varphi_1 : H^1(G/H, B) \to H^1(G, B)$$

by $[f] \mapsto [f \circ \pi]$, where π is the canonical projection $\pi : G \to G/H$. Check this is well defined and is a morphism of G/H-functors. By the main lemma, φ_1 has unique extensions

$$\varphi_n : H^n(G/H, B) \to H^n(G, B)$$

for all $n \geq 1$. (Caution : we cannot extend φ_1 downward. Why ?).

Let A be a G-module. Then A^H is a G/H-module, hence a G-module. So

$$\varphi_n : H^n(G/H, A^H) \to H^n(G, A^H)$$

is defined for $n \geq 1$. From the inclusion map $i : A^H \to A$, we also have

$$i_n : H^n(G, A^H) \to H^n(G, A).$$

The composition $i_n \circ \varphi_n : H^n(G/H, A^H) \to H^n(G, A)$ is called the inflation map for $n \geq 1$.

EXERCISE 3.8.

(i) Let $u : A \to B$ be a G-homomorphism. Then the following diagram is commutative (i.e. the inflation map commutes with the induced maps).

$$\begin{tikzcd}
H^n(G/H, A^H) \arrow[r, "\text{inflation}"] \arrow[d, "u_n"'] & H^n(G, A) \arrow[d, "u_n"] \\
H^n(G/H, B^H) \arrow[r, "\text{inflation}"] & H^n(G, B)
\end{tikzcd}$$

(ii) For a s.e.s. $0 \to A \to B \to C \to 0$, suppose $H^1(H,C) = 0$ so that

$$0 \to A^H \to B^H \to C^H \to 0$$

is exact. Then the inflation map commutes with the connecting homomorphisms. Namely the following is commutative.

$$\begin{tikzcd}
H^n(G/H, C^H) \arrow[r, "\text{inflation}"] \arrow[d, "\partial"'] & H^n(G,C) \arrow[d, "\partial"] \\
H^{n+1}(G/H, A^H) \arrow[r, "\text{inflation}"] & H^{n+1}(G,A)
\end{tikzcd}$$

THEOREM 3.1 (FUNDAMENTAL EXACT SEQUENCE). *For any G-module A,*

(1) $0 \to H^1(G/H, A^H) \xrightarrow{\text{inflation}} H^1(G,A) \xrightarrow{\text{res}} H^1(H,A)$ *is exact.*

(2) $0 \to H^n(G/H, A^H) \xrightarrow{\text{inflation}} H^n(G,A) \xrightarrow{\text{res}} H^n(H,A)$ *is exact if* $H^q(H,A) = 0$ *for* $1 \leq q < n$.

Proof of (1). It is easy to show that

EXERCISE 3.9. (i) inflation is injective (ii) res∘inflation $= 0$. Hence it is enough to show that Ker(res) $\subset$ Im(inflation). Take $[f] \in H^1(G,A)$ such that res$([f]) = 0$ in $H^1(H,A)$. This means $f : G \to A$ is a crossed homomorphism such that $f|_H$ is a trivial crossed map, in other words $f(h) = (h-1)a$, for some $a \in A$ and for all $h \in H$. Let $g : G \to A$ be the trivial crossed map such that $g(\sigma) = (\sigma - 1)a$ with the same a as before. Define $l : G \to A$ by $l(\sigma) = f(\sigma) - g(\sigma)$. Then as elements of $H^1(G,A)$, $[f] = [l]$. Since $l|_H = 0$, $l(h\sigma) = hl(\sigma) + l(h) = hl(\sigma)$ and $l(h\sigma) = l(\sigma h') = \sigma l(h') + l(\sigma) = l(\sigma)$. Thus $l(\sigma) \in A^H$ for all $\sigma \in G$ and $l(H\sigma) = l(\sigma)$. Hence l fuctors through G/H with images in A^H. Define

$$\tilde{f} : G/H \to A^H$$

by $\tilde{f}(\bar{\sigma}) = l(\sigma)$. Then inflation $([\tilde{f}]) = [f]$.

Proof of (2). We use the induction on n. We have a s.e.s.

$$0 \to A \xrightarrow{u} \mathbf{Z}[G] \otimes A \to B \to 0,$$

where $u(a) = N\otimes a$ and $B = \mathbf{Z}[G]\otimes A/u(A)$. Since $H^i(H, \mathbf{Z}[G]\otimes A) = 0$ $\forall i$,

$$H^q(H,B) \simeq H^{q+1}(H,A) = 0$$

for $1 \leq q < n-1$. Hence, by the induction hypothesis,

$$0 \to H^{n-1}(G/H, B^H) \xrightarrow{\text{inflation}} H^{n-1}(G,B) \xrightarrow{\text{res}} H^{n-1}(H,B)$$

is exact.

Since $H^1(H,A) = 0$,

$$0 \to A^H \xrightarrow{u} (\mathbf{Z}[G] \otimes A)^H \to B^H \to 0$$

is a s.e.s. One can easily show that

EXERCISE 3.10. If A is G-regular, then A^H is G/H-regular. Therefore, $H^i(G/H, B^H) \simeq H^{i+1}(G/H, A^H)$ for all i. Hence from the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & H^{n-1}(G/H,B^H) \arrow[r, "\text{inflation}"] \arrow[d] & H^{n-1}(G,B) \arrow[r, "\text{res}"] \arrow[d] & H^{n-1}(H,B) \arrow[d] \\
& H^n(G/H,A^H) \arrow[r, "\text{inflation}"] & H^n(G,A) \arrow[r, "\text{res}"] & H^n(H,A),
\end{tikzcd}$$

we get the desired exact sequence.

REMARK. (i) There is a map, called transgression,

$$tr : H^1(H,A)^G \to H^2(G/H, A^H)$$

which makes the following exact;

$$0 \to H^1(G/H,A^H) \xrightarrow{\text{inf}} H^1(G,A) \xrightarrow{\text{res}} H^1(H,A)^G \xrightarrow{\text{tr}}$$
$$H^2(G/H,A^H) \xrightarrow{\text{inf}} H^2(G,A).$$

Similarly, one can define tr on higher levels.

(ii) Suppose H is a normal sylow subgroup of G, or more generally, suppose $((G:H), \#(H)) = 1$. Then it is an immediate consequence of the above theorem and the proposition 3.3 that

$$0 \to H^n(G/H,A^H) \xrightarrow{\text{inf}} H^n(G,A) \xrightarrow{\text{res}} H^n(H,A)^G \to 0$$

is exact $\forall n \geq 1$.

EXERCISE 3.11. Define tr in the above Remark so that the sequence described there becomes exact.

§4. Tate-Nakayama Theorems

In this section, we prove two of three Tate-Nakayama theorems that are useful in the abstract study of class field theory (class formations). The remaining one will be proved in §5.

DEFINITION 4.1. A G-module A is said to be cohomologically trivial if $H^n(H, A) = 0$ for all $n \in \mathbf{Z}$ and for any subgroup H of G.

EXAMPLES. (i) Any G-regular module is cohomologically trivial.

(i) Let $^{\#}(G) = g$. Suppose A is uniquely divisible by g, i.e., $A \xrightarrow{\times g} A$ is an isomorphism. Then A is cohomologically trivial.

EXERCISE 4.1. Justify (ii). (Hint: the inverse map of the multiplication by g is of norm 1, hence A is G-regular). In particular, $\mathbf{Q}$ is cohomologically trivial.

THEOREM 4.1 (FIRST TATE-NAKAYAMA THEOREM). *Let A be a G-module so that, for some integer r, $H^r(H, A) = H^{r+1}(H, A) = 0$ for all subgroups H of G. Then A is cohomologically trivial.*

Proof. Since $H^n(G, A) = \oplus_p \text{cores}(H^n(G_p, A))$ by proposition 3.2, we may assume that G is a p-group for some prime p.

Step 1. If $H^2(H, A) = H^3(H, A) = 0$ for all subgroup H, then $H^1(H, A) = H^4(H, A) = 0$ for all H.

Proof of Step 1. Let $^{\#}(G) = p^k$. We use the induction on k. If $k = 1$, then G is cyclic, so we are done. Assume this for $k - 1$. For any proper subgroup H, $H^1(H, A) = H^4(H, A) = 0$ by the induction hypothesis. So it remains to prove $H^1(G, A) = H^4(G, A) = 0$. Take a normal subgroup K of G of index p. Then

$$0 \to H^n(G/K, A^K) \xrightarrow{\text{inf}} H^n(G, A) \xrightarrow{\text{res}} H^n(K, A) = 0$$

is exact for $1 \leq n \leq 4$. Therefore

$$H^n(G/K, A^K) \simeq H^n(G, A)$$

for $1 \leq n \leq 4$. But $H^2(G,A) = H^3(G,A) = 0$. So $H^2(G/K, A^K) = H^3(G/K, A^K) = 0$. $H^1(G/K, A^K) = H^4(G/K, A^K) = 0$ since G/K is cyclic. Hence $H^1(G,A) = H^4(G,A) = 0$.

Step 2. If $H^r(H,A) = H^{r+1}(H,A) = 0$ for all H, then $H^{r-1}(H,A) = H^{r+2}(H,A) = 0$ for all H. Note that the theorem follows from this by using step 2 successively.

Proof of step 2. We can construct a s.e.s.

$$E_1 : 0 \to B_1 \to R_1 \to A \to 0,$$

where R_1 is G-regular and $B_1 = \operatorname{Ker}(R_1 \to A)$. This was done earlier. Then we have

$$H^n(H,A) \simeq H^{n+1}(H,B_1)$$

for any subgroup H of G. Do the same for B_1, namely take

$$E_2 : 0 \to B_2 \to R_2 \to B \to 0$$

with R_2 G-regular. Then

$$H^{n+1}(H,B_1) \simeq H^{n+2}(H,B_2)$$

for all H. Clearly continuing this process gives that for any integer $q \geq 0$ there is a G-module B_q so that

$$H^n(H,A) \simeq H^{n+q}(H,B_q).$$

EXERCISE 4.2. For any $q \geq 0$, there is a G-module B_{-q} so that $H^n(H,A) \simeq H^{n-q}(H,B_{-q})$ for all subgroup H of G.

Hence for any $q \in \mathbf{Z}$, there is a G-module $B(= B_q)$ so that

$$H^n(H,A) \simeq H^{n+q}(H,B)$$

for all n and all subgroup H of G. Our assumption is $H^r(H,A) = H^{r+1}(H,A) = 0$ for all subgroups H of G. Choose a G-module B so that

$$H^n(H,A) \simeq H^{n+q}(H,B)$$

with $r + q = 2$. So $H^2(H,B) = H^3(H,B) = 0$. Thus $H^1(H,B) = H^{r-1}(H,A) = 0$ and $H^4(H,B) = H^{r+2}(H,A) = 0$ by step 1.

Remark. This theorem can be strengthened : if $H^r(G_p, A) = H^{r+1}(G_p, A) = 0$ for all Sylow subgroups of G, then A is cohomologically trivial. (See Serre : Local fields).

Theorem 4.2 (Second Tate-Nakayama theorem). *Let $u : A \to B$ be a G-homomorphism and $u_n(H) : H^n(H, A) \to H^n(H, B)$ be its induced homomorphism on the cohomology of any subgroup H of G. If, for some integer r, we have*

(i) *$u_r(H)$ is an epimorphism for all H*
(ii) *$u_{r+1}(H)$ is an isomorphism for all H, and*
(iii) *$u_{r+2}(H)$ is a monomorphism for all H,*

then $u_n(H)$ is an isomorphism for all subgroup H of G and all $n \in \mathbf{Z}$.

Proof. Consider

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\alpha"] \arrow[dr, "u"'] & B \oplus (A \otimes \mathbf{Z}[G]) \arrow[r, "\beta"] \arrow[d, "\pi"] & \mathrm{Coker}(\alpha) \arrow[r] & 0 \\
 & & B & &
\end{tikzcd}$$

where $\alpha(a) = (u(a), a \otimes N)$ and π, β are projections. For convenience, we let $C = B \oplus (A \otimes \mathbf{Z}[G])$ and $A' = \mathrm{Coker}(\alpha)$. Note that

$$H^n(H, B) \simeq H^n(H, C)$$

for all $n \in \mathbf{Z}$ and all H. We denote $H^n(H, *)$ by $H^n(*)$ to simplify notations. We have the following exact and conmutative sequence;

$$\begin{tikzcd}
{} \arrow[r] & H^r(A) \arrow[r, "\alpha_r"] \arrow[dr, "u_r"'] & H^r(C) \arrow[r, "\beta_r"] \arrow[d, "\pi_r"] & H^r(A') \arrow[r, "\partial_r"] & H^{r+1}(A) \arrow[r, "\alpha_{r+1}"] \arrow[dr, "u_{r+1}"'] & H^{r+1}(C) \arrow[d, "\pi_{r+1}"] \\
 & & H^r(B) & & & H^{r+1}(B)
\end{tikzcd}$$

$$\begin{tikzcd}
{} \arrow[r, "\beta_{r+1}"] & H^{r+1}(A') \arrow[r, "\partial_{r+1}"] & H^{r+2}(A) \arrow[r, "\alpha_{r+2}"] \arrow[dr, "u_{r+2}"'] & H^{r+2}(C) \arrow[r] \arrow[d, "\pi_{r+2}"] & \cdots \\
 & & & H^{r+2}(B) &
\end{tikzcd}$$

Since u_r is onto, α_r is onto, whence $\beta_r = 0$. Since u_{r+1} is an isomorphism, so is α_{r+1}, whence $\partial_r = \beta_{r+1} = 0$. And since u_{r+2} is 1-1, so is α_{r+2}, whence $\partial_{r+1} = 0$. Therefore $H^r(A') = H^{r+1}(A') = 0$. Since this is true for all subgroup H of G, by the 1^{st} Tate-Nakayama theorem, A' is cohomologically trivial. Hence

$$\alpha_n : H^n(H,A) \to H^{n+1}(H,C)$$

is an isomorphism for all H and all $n \in \mathbf{Z}$. This implies the 2^{nd} Tate-Nakayama theorem for $u_n = \pi_n \circ \alpha_n$.

Remark.

(i) Let $u : A \to B$ be a G-homomorphism so that $u_n(H) : H^n(H,A) \to H^n(H,B)$ is an isomorphism for $n = r$ and $n = r+1$ for some integer r and for all subgroups H of G. Then $u_n(H)$ is an isomorphism for all n and all H. (See Evans ; An extension of Tate's theorem of cohomological triviality, Proceedings of Amer. Math. Soc).

(ii) There are modules (Evans, same paper) A and B such that $H^n(H,A) \simeq H^n(H,B)$ for $n = r$ and $n = r+1$ and all subgroups H of G, but yet $H^n(H,A) \not\simeq H^n(H,B)$ for all n. It is, of course, that the isomorphisms for $n = r$ and $n = r+1$ are only group isomorphisms and are not induced by any G-homomorphism $A \xrightarrow{u} B$.

(iii) One can find in Serre's book (Local fields) that there is a statement of the second theorem involving only Sylow subgroups.

Exercise 4.3. Give an example of a group G and a module A such that $H^r(G,A) = H^{r+1}(G,A) = 0$ for some r but $H^n(G,A) \neq 0$ for all n. (Hint : Consider $0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0$).

§5. Cup product

We only give an axiomatic characterization of the cup product without the proof of existence or uniqueness, then use those axioms to prove the third Tate-Nakayama theorem. It turns out in pratice that it is the axims not the existence proof (even if can be done explicitly) that is useful.

The group G is fixed in what follows and for the sake of notation we write $H^n(A)$ in place of $H^n(G,A)$. All the tensor products are over $\mathbf{Z}$ and $\otimes = \otimes_{\mathbf{Z}}$.

Definition 5.1. The cup product is a collection of homomorphisms

$$\varphi^{p,q}(A,B) : H^p(A) \otimes H^q(B) \to H^{p+q}(A \otimes B)$$

defined for all integers p and q and pairs A, B of G-modules that satisfy the following four axioms (we userally write $\varphi^{p,q}$ instead of $\varphi^{p,q}(A,B)$).

(i) if $A \overset{u}{\longrightarrow} C$ and $B \overset{v}{\longrightarrow} D$ are G-homomorphisms, then the following diagrams commute:

$$\begin{tikzcd}
H^p(A) \otimes H^q(B) \arrow[r, "\varphi^{p,q}"] \arrow[d, "u_p \otimes 1"'] & H^{p+q}(A \otimes B) \arrow[d, "(u \otimes 1)_{p+q}"] \\
H^p(C) \otimes H^q(B) \arrow[r, "\varphi^{p,q}"] & H^{p+q}(C \otimes B)
\end{tikzcd}$$

and

$$\begin{tikzcd}
H^p(A) \otimes H^q(B) \arrow[r, "\varphi^{p,q}"] \arrow[d, "1 \otimes v_q"'] & H^{p+q}(A \otimes B) \arrow[d, "(1 \otimes v)_{p+q}"] \\
H^p(A) \otimes H^q(D) \arrow[r, "\varphi^{p,q}"] & H^{p+q}(A \otimes D)
\end{tikzcd}$$

(ii) $\varphi^{0,0}$ is induced by the natural map $A^G \otimes B^G \to (A \otimes B)^G$ given by $a \otimes b \mapsto a \otimes b$.

(iii) if $E : 0 \to A \overset{u}{\longrightarrow} B \overset{v}{\longrightarrow} C \to 0$ is exact and if, for some D, $E \otimes D : 0 \to A \otimes D \xrightarrow{u \otimes 1} B \otimes D \xrightarrow{v \otimes 1} C \otimes D \to 0$ is exact, the following diagram commutes:

$$\begin{tikzcd}
H^p(C) \otimes H^q(D) \arrow[r, "\varphi^{p,q}"] \arrow[d, "\partial^p_E \otimes 1"'] & H^{p+q}(C \otimes D) \arrow[d, "\partial^{p+q}_{E \otimes D}"] \\
H^{p+1}(A) \otimes H^q(D) \arrow[r, "\varphi^{p+1,q}"] & H^{p+q+1}(A \otimes D)
\end{tikzcd}$$

(iv) if $E : 0 \to A \overset{u}{\longrightarrow} B \overset{v}{\longrightarrow} C \to 0$ is exact and if, for some D, $D \otimes E : 0 \to D \otimes A \xrightarrow{1 \otimes u} D \otimes B \xrightarrow{1 \otimes v} D \otimes C \to 0$ is exact, then the following diagram commutes:

$$\begin{tikzcd}
H^p(D) \otimes H^q(C) \arrow[r, "\varphi^{p,q}"] \arrow[d, "1\otimes\partial^q_E"] \arrow[dr, phantom, "(-1)^p"] & H^{p+q}(C \otimes C) \arrow[d, "\partial^{p+q}_{D\otimes E}"] \\
H^p(D) \otimes H^{q+1}(A) \arrow[r, "\varphi^{p,q+1}"] & H^{p+q+1}(D \otimes A)
\end{tikzcd},$$

that is

$$\partial^{p+q}_{D\otimes E} \circ \varphi^{p,q} = (-1)^p \varphi^{p,q+1} \circ (1 \otimes \partial^q_E).$$

These axioms describe the cup product uniquely. Other notations for the cup product are

$$\varphi^{p,q}(x \otimes y) = x \vee y \text{ or } x.y$$

for $x \in H^p(A)$ and $y \in H^q(B)$. Under the notation $\vee$, axions (iii) and (iv) read, for example,

$$\partial(x \vee y) = \partial x \vee y,$$
$$\partial(x \vee y) = (-1)^p x \vee \partial y.$$

Choose a G-module A and an integer p and keep them fixed. Then for any G-module B and any integer q we have

$$\varphi^{p,q} : H^p(A) \otimes H^q(B) \to H^{p+q}(A \otimes B).$$

Choose $x \in H^p(A)$ and define a homomorphism

$$\varphi^q_x : H^q(B) \to H^{p+q}(A \otimes B)$$

by $\varphi^q_x(y) = \varphi^{p+q}(x \otimes y)$. In particular take $p = 0$. Then $H^0(A) = A^G/NA$, so for every element $a \in A^G$ ($\bar{a} = a + NA \in H^0(A)$) we have

$$\varphi^q_{\bar{a}} : H^q(B) \to H^q(A \otimes B).$$

We will describe this map explicitely. Meanwhile, we need

Exercise 5.1. For any G-module A, there are exact sequences $0 \to A \to R \to B \to 0$ and $0 \to B' \to R' \to A \to 0$ where R and R' are G-regular and the sequences are $\mathbf{Z}$-split.

Proposition 5.1. *$\varphi^q_{\bar{a}}$ is the induced map $(\psi_a)_q$, where $\psi_a : B \to A \otimes B$ is defined by $\psi_a(b) = a \otimes b$.*

Proof. For $q = 0$, it is nothing but the axiom (ii). Suppose it is true for all B and for $0 \le n < q$. Choose $E : 0 \to B \to R \to C \to 0$, $\mathbf{Z}$-split with $R = G$-regular. Then $A \otimes E : 0 \to A \otimes B \to A \otimes R \to A \otimes C \to 0$ is exact, so by axiom (iv), we have a commutative diagram;

$$\begin{tikzcd}
H^0(A) \otimes H^{q-1}(C) \arrow[r] \arrow[d] \arrow[dr, phantom, "(-1)^0"] & H^{0,q-1}(A \otimes C) \arrow[d] \\
H^0(A) \otimes H^q(B) \arrow[r] & H^{0,q}(A \otimes B).
\end{tikzcd}$$

Also the diagram

$$\begin{tikzcd}
0 \arrow[r] & B \arrow[r] \arrow[d, "\psi_a"] & R \arrow[r] \arrow[d, "\psi_a"] & C \arrow[r] \arrow[d, "\psi_a"] & 0 \\
0 \arrow[r] & A \otimes B \arrow[r] & A \otimes R \arrow[r] & A \otimes C \arrow[r] & 0
\end{tikzcd}$$

commutes so we have the following commutative diagram;

$$\begin{tikzcd}
H^{q-1}(C) \arrow[r, "\partial^{q-1}_E"] \arrow[d, "(\psi_a)_{q-1}"] & H^q(B) \arrow[d, "(\psi_a)_q ."] \\
H^{q-1}(A \otimes C) \arrow[r, "\partial^{q-1}_{A \otimes E}"] & H^q(A \otimes B)
\end{tikzcd}$$

Choose $x \in H^q(B)$. Then there is $y \in H^{q-1}(C)$ so that $\partial y = x$. Then $\varphi^q_{\bar{a}}(x) = \varphi^{0,q}(\bar{a} \otimes x) = \varphi^{0,q} \circ (1 \otimes \partial)(\bar{a} \otimes y) = \partial \circ \varphi^{0,q-1}(\bar{a} \otimes y) = \partial \varphi^{q-1}_{\bar{a}}(y) = \partial(\psi_a)_{q-1}(y) = (\psi_a)_q \partial(y) = (\psi_a)_q(x)$. So $\varphi^q_{\bar{a}} = (\psi_a)_q$ for any B.

For negative dimensions, the procedure is exactly the same except taking $E : 0 \to C \to R \to B \to 0$.

PROPOSITION 5.2. *For any $x \in H^p(A)$ and $y \in H^q(B)$, $x \vee y = (-1)^{pq} y \vee x$ under the natural identification $A \otimes B$ with $B \otimes A$.*

Proof.

Step 1. $p = q = 0$: Axiom (ii)

Step 2. $q = 0$, $p > 0$: Suppose it is true for $0 \leq l < p$. Take a $\mathbf{Z}$-split exact sequence

$$E : 0 \to A \to R \to A' \to 0.$$

Then

$$H^{q-1}(A') \overset{\partial}{\simeq} H^q(A).$$

Hence for a given $x \in H^q(A)$, there is $x' \in H^{q-1}(A')$ such that $\partial x' = x$. Thus $x \vee y = (\partial x') \vee y = \partial(x' \vee y) = \partial((-1)^{(p-1) \cdot 0} y \vee x') = \partial(y \vee x') = (-1)^0 y \vee \partial x' = y \vee x$.

Step 3. $q = 0$, $p < 0$: Same procedure with $E : 0 \to A' \to R \to A \to 0$.

Step 4. $q < 0$, $p =$ arbitrary : Suppose it is true for all p when $q < l \leq 0$. Consider a $\mathbf{Z}$-split sequence

$$E : 0 \to B' \to R \to B \to 0.$$

Then for $x \in H^p(A)$, $y \in H^q(B)$,

$$\partial(x \vee y) = (-1)^p x \vee \partial y = (-1)^p (-1)^{p(q+1)} \partial y \vee x = (-1)^{pq} \partial(y \vee x).$$

Since ∂ is an isomorphism, $x \vee y = (-1)^{pq} y \vee x$.

Step 5. $q > 0$, $p =$ arbitrary : Same procedure.

Now we are ready to introduce the third Tate-Nakayama theorem. We have, for any G-module A and for a given $\alpha \in H^p(G, A)$,

$$\varphi_\alpha^q : H^q(G, \mathbf{Z}) \to H^{p+q}(G, A)$$

given by $x \mapsto \alpha \vee x$. Then for any subgroup H of G define

$$f_\alpha^n(H) : H^n(H, \mathbf{Z}) \to H^{n+p}(H, A)$$

by $x \mapsto (\operatorname{res} \alpha) \vee x$, that is $f_\alpha^n(H) = \varphi_{\operatorname{res}(\alpha)}^n$.

THEOREM 5.1 (THIRD TATE-NAKAYAMA THEOREM). *Let A be a G-module so that for some integer q and for all subgroups H of G we have $(\alpha \in H^p(G,A))$.*

(i) *$f^q_\alpha(H)$ is an epimorphism*
(ii) *$f^{q+1}_\alpha(H)$ is an isomorphism*
(iii) *$f^{q+2}_\alpha(H)$ is a monomorphism.*

Then $f^n_\alpha(H)$ is an isomorphism for all n and all H.

Proof. We use the induction on p. It is an easy exercise to check the case $p = 0$. (Use proposition 5.1 and the 2^{nd} Tate-Nakayama theorem).

Suppose $\alpha \in H^p(G,A)$ and that the theorem is true for all l so that $0 \le l < p$. Take

$$E : 0 \to A \to R \to A' \to 0$$

which is $\mathbf{Z}$-split exact sequence with R = G-regular. We claim that the following is commutative (α' is taken so that $\partial\alpha' = \alpha$).

$$\begin{tikzcd}
H^n(H,\mathbf{Z}) \arrow[rr, "f^n_{\alpha'}(H)"] \arrow[dr, "f^n_\alpha(H)"'] & & H^{n+p-1}(H,A') \arrow[dl, "\partial"] \\
& H^{n+p}(H,A) &
\end{tikzcd}$$

This is true because $f^n_\alpha(H)(x) = \operatorname{res}\alpha \vee x = \operatorname{res}(\partial\alpha') \vee x = \partial(\operatorname{res}\alpha') \vee x = \partial(\operatorname{res}\alpha' \vee x) = \partial f^n_{\alpha'}(H)(x)$.

But ∂ is an isomorphism and so $f^n_{\alpha'}(H)$ satisfies the hypothesis (i), (ii), (iii) of the theorem. By the induction hypothesis, $f^n_{\alpha'}(H)$ is an isomorphism for all n and all H, but then so is $f^n_\alpha(H)$.

To show this for $p < 0$, choose an exact sequence $E : 0 \to A' \to R \to A \to 0$ and proceed as usual.

Now we get a very important corollary which is used strongly in the axiomatic treatment of class field theory (see Artin-Tate : class field theory).

THEOREM 5.2. *Suppose for some G-module A we have*

(i) *$H^1(H,A) = 0$ for all subgroups H of G*
(ii) *$H^2(H,A)$ = cyclic group of order $^{\#}(H)$ generated by $\operatorname{res}(\alpha)$, where $\langle\alpha\rangle = H^2(G,A)$.*

Then $f^n_\alpha(H) : H^n(H, \mathbf{Z}) \to H^{n+2}(H, A)$ is an isomorphism for all n and all H.

Proof. Look at $f^n_\alpha(H)$ for $-1 \le n \le 1$. For $n = -1$,

$$f^{-1}_\alpha(H) : H^{-1}(H, \mathbf{Z}) \to H^1(H, A) = 0$$

is onto, and for $n = 1$,

$$f^1_\alpha(H) : H^1(H, \mathbf{Z}) = 0 \to H^3(H, A)$$

is one to one. For $n = 0$, we have the following. We know $H^0(H, \mathbf{Z}) = \mathbf{Z}/h\mathbf{Z}$, where $h = {}^\#(H)$. Also $H^2(H, A) = \langle \operatorname{res} \alpha \rangle$ is cyclic of order h. So we must show

$$f^0_\alpha(H) : \mathbf{Z}/h\mathbf{Z} \to \langle \operatorname{res} \alpha \rangle$$

is an isomorphism. For $\bar{a} \in \mathbf{Z}/h\mathbf{Z}$, $f^0_\alpha(H)(\bar{a}) = \operatorname{res} \alpha \vee \bar{a} = \bar{a} \vee \operatorname{res} \alpha = \varphi^2_{\bar{a}}(\operatorname{res} \alpha) = (\psi_a)_2(\operatorname{res} \alpha)$, where $\psi_a : A \to A$ is the multiplication by a i.e., $x \mapsto ax$. Thus $f^0_\alpha(H)(\bar{a}) = a \operatorname{res} \alpha$. Hence $f^0_\alpha(H)$ is an isomorphism. Apply the 3rd Tate-Nakayama theorem to finish the proof.

REMARK. If the hypothesis of theorem 5.2 holds, the case $n = -2$ is of most interest for class field theory:

$$f^{-2}_\alpha(H) : H^{-2}(H, \mathbf{Z}) = H/H' \xrightarrow{\sim} H^0(H, A) = A^H/N_H A.$$

Then the module A determines the group H.

EXERCISE 5.2. For $x \in H^p(G, A)$, $y \in H^q(G, B)$, $\operatorname{res}(x \vee y) = \operatorname{res} x \vee \operatorname{res} y$

EXERCISE 5.3. For $x \in H^p(G, A)$, $y \in H^q(H, B)$, $\operatorname{cores}(\operatorname{res} x \vee y) = x \vee \operatorname{cores} y$.

§6. Semi local theory

Suppose $A = \Pi_\alpha A_\alpha$ is a direct product of G-modules. Then A is a G-module under $\sigma(a_\sigma) = (\sigma a_\alpha)$. Let $\pi_\alpha : A \to A_\alpha$ be the projection onto the α^{th} coordinate. Then clearly π_α is a G-homomorphism, hence induces

$$(\pi_\alpha)_n : H^n(G, A) \to H^n(G, A_\alpha).$$

Then we have a homomorphism

$$\pi_n : H^n(G, A) \to \Pi_\alpha H^n(G, A_\alpha).$$

EXERCISE 6.1. Show that π_n is an isomorphism for all n.

DEFINITION 6.1. A set S is said to be a G-set if G acts on S transitively.

Let S be a G-set. For each $\mathcal{P} \in S$, let $G_{\mathcal{P}} = \{\sigma \in G \,|\, \sigma\mathcal{P} = \mathcal{P}\}$, which is a subgroup of G.

EXERCISE 6.2. Suppose $\mathcal{P}' = \tau\mathcal{P}$ for $\tau \in G$. Then $G_{\mathcal{P}'} = \tau G_{\mathcal{P}} \tau^{-1}$.

Let $\{A_{\mathcal{P}} \,|\, \mathcal{P} \in S\}$ be a collection of abelian groups indexed by S such that for each $\sigma \in G$, we have a homomorphism $\sigma : A_{\mathcal{P}} \to A_{\sigma\mathcal{P}}$ so that $1 : A_{\mathcal{P}} \to A_{\mathcal{P}}$ is the identity map and the following diagram commutes;

$$\begin{tikzcd}
A_{\mathcal{P}} \arrow[rr, "\sigma"] \arrow[dr, "\tau\sigma"'] & & A_{\sigma\mathcal{P}} \arrow[dl, "\tau"] \\
& A_{\tau\sigma\mathcal{P}} &
\end{tikzcd}$$

Then $\sigma : A_{\mathcal{P}} \to A_{\sigma\mathcal{P}}$ is an isomorphism.

Let $A = \Pi_{\mathcal{P} \in S} A_{\mathcal{P}}$. Then A can be made a G-module as follows : if $a = (a_{\mathcal{P}}) \in A$, then define σa to have $\mathcal{P}$-component $(\sigma a)_{\mathcal{P}} = \sigma a_{\sigma^{-1}\mathcal{P}}$. Then (i) $1a = a$ (ii) $\sigma(\tau a) = (\sigma\tau)a$ (iii) $\sigma(a + a') = \sigma a + \sigma a'$.

EXERCISE 6.3. Prove (ii). Also for any $\mathcal{P}$, we have $A_{\mathcal{P}}$ is a $G_{\mathcal{P}}$-module.

PROPOSITION 6.1. *$H^n(G_{\mathcal{P}}, A_{\mathcal{P}}) \simeq H^n(G_{\mathcal{P}'}, A_{\mathcal{P}'})$ for any two $\mathcal{P}$, $\mathcal{P}' \in S$.*

Proof. Left as an exericise.

For any $\mathcal{P} \in S$, we have the projection map $\pi_{\mathcal{P}} : A \to A_{\mathcal{P}}$ which is a $G_{\mathcal{P}}$-homomorphism, and so induces $(\pi_{\mathcal{P}})_n : H^n(G_{\mathcal{P}}, A) \to H^n(G_{\mathcal{P}}, A_{\mathcal{P}})$. Also we have restriction res : $H^n(G, A) \to H^n(G_{\mathcal{P}}, A)$. Define $h_n = (\pi_{\mathcal{P}})_n \circ \mathrm{res} : H^n(G, A) \to H^n(G_{\mathcal{P}}, A_{\mathcal{P}})$.

THEOREM 6.1. *$h_n : H^n(G, A) \overset{\sim}{\longrightarrow} H^n(G_{\mathcal{P}}, A_{\mathcal{P}})$ is an isomorphism for all n and any $\mathcal{P} \in S$.*

Proof. Left as an exercise.

References

1. E. Artin and J.T. Tate, *Class field theory*, Harvard Univ. Press, Cambridge, Massachusettes, 1961.
2. K. Brown, *Cohomology of Groups*, G.T.M. **87**, Springer-Verlag 1982.
3. S. Eilenberg and S. Maclane, *Cohomology theory in abstract groups*, Ann. of Math. **48** (1947), 51–78.
4. L. Evens, *An extension of Tate's theorem on cohomology triviality*, Proc. Amer. Math. Soc. 00 (1965), 289–291.
5. J.P. Serre, *Local fields*, G.T.M. 67, Springer-Verlag 1979.
6. E. Weiss, *Cohomology of groups*, Academic Press, 1969.

Department of Mathematics
Inha University
Inchon 402-751, Korea

INTRODUCTION TO QUADRATIC FORMS

Myung-Hwan Kim

Contents

I. Quadratic Forms over Fields

1. Abstract Theory of Quadratic Forms

Let F be a field with ch$F \neq 2$. Let V be a quadratic space, i.e., V is a finite dimensional vector space over F equipped with a symmetric bilinear form $B : V \times V \to F$. Let $Q : V \to F$ be the quadratic map associated to B, i.e.,

$$Q(x) = B(x,x), \ {}^{\forall}x \in V.$$

Fix a basis $x_1, \cdots, x_n$ for V over F. Then for $x = a_1x_1 + \cdots + a_nx_n \in V$, we have

$$Q(x) = \sum_{i=1}^{n} Q(x_i)a_i^2 + \sum_{i \neq j} B(x_i,x_j)a_ia_j = (a_1, \cdots, a_n)M_Q \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

where $M_Q = (B(x_i,x_j))$ is the symmetric $n \times n$ matrix associated to Q.

DEFINITION1.1. The discriminant dV of V is defined to be $\det M_Q$, which is well-defined modulo $(F^{\times})^2$. A quadratic space V is said to be regular if $dV \neq 0$.

One can easily check that a quadratic space V is regular if and only if rad$V = 0$, where rad$V = \{x \in V | B(x,V) = 0\}$

DEFINITION1.2. Let V, V' be quadratic spaces with quadratic maps Q, Q', respectively. A linear transformation $\sigma : V \to V'$ is called a representation if $Q'(\sigma x) = Q(x)$, ${}^{\forall}x \in V$. A bijective representation is called an isometry. We set

$$O(V,V') = \{\sigma : V \to V' \text{ isometry}\}$$
$$O(V) = O(V,V).$$

$O(V)$ is called the orthogonal group of V.

We say that V is represented by (or, isometric to) V' if there exists a representation (or, isometry) from V into (or, onto) V' and write $V \to V'$ (or, $V \simeq V'$).

For $\alpha \in F$, let $\langle\alpha\rangle$ denote a one dimensional quadratic space Fx with $Q(x) = \alpha$. Note that if $V \neq 0$, then V has an orthogonal basis $x_1, \ldots, x_n$ such that

$$V = Fx_1 \perp Fx_2 \perp \cdots \perp Fx_n \simeq \langle\alpha_1\rangle \perp \langle a_2\rangle \perp \cdots \perp \langle\alpha_n\rangle$$

where $\alpha_i = Q(x_i)$, $B(x_i, x_j) = 0$, $^\forall i \neq j$. For a subspace U of V, we define the orthogonal complement U^* of U by

$$U^* = \{x \in V \mid B(x, U) = 0\}.$$

It is easy to see that if U is a regular subspace of V, then U splits V, i.e., $V = U \perp U^*$.

DEFINITION1.3. A non-zero $x \in V$ is called an isotropic vector if $Q(x) = 0$ and an anisotropic vector otherwise. V is called an isotropic space if it contains an isotropic vector and an anisotropic space otherwise. V is said to be totally isotropic if every non-zero vector of V is isotropic. V is said to be universal if $Q(V) = F$.

A quadratic space H of dimension 2 is called a hyperbolic plane if there exists a basis x_1, x_2 for H for which $M_H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. It is easy to see that a binary quadratic space H is hyperbolic if and only if $dH = -1$ if and only if H is isotropic and regular. Note that a hyperbolic plane is universal. One can easily prove the following structure theorem of regular quadratic spaces.

THEOREM1.4. *Let U be a maximal totally isotropic subspace of a regular space V. If $\dim U = r$, then*

$$V \simeq H_1 \perp H_2 \perp \cdots \perp H_r \perp V_0$$

where H_i are hyperbolic planes for all $i = 1, \ldots, r$ and V_0 is anisotropic or null.

V is called a hyperbolic space if $V_0 = 0$. Note that if V is isotropic, then V is universal. We state the following theorem due to Witt [W]:

THEOREM1.5(WITT). (1) *Let U, W be isometric regular subspaces of V. Then U^*, W^* are isometric.*

(2) *Let V, V' be isometric regular spaces. Let U be any subspace of V and $\sigma : U \to V'$ be an injective representation. Then there exist a prolongation of σ to an isometry $\bar{\sigma} : V \to V'$.*

The dimension r of a maximal totally isotropic subspace U of a regular space V is an invariant of V, called the index of V and denoted by $\operatorname{ind} V$. Indeed, if W is another maximal totally isotropic subspace of V such that $\dim U \leq \dim W$, then there exists an injective representation $\sigma : U \to W$, which can be prolonged to an isometry $\bar{\sigma} : V \to V$. Since $U = \bar{\sigma}^{-1}(W)$, $\dim U = \dim W$ as asserted.

Let V be a regular quadratic space from now on unless specified otherwise. $\sigma \in O(V)$ is called a rotation if $\det \sigma = 1$ and a reflection if $\det \sigma = -1$. Note that $\det \sigma = \pm 1$, ${}^{\forall}\sigma \in O(V)$. Let

$$O^+(V) = \{\sigma \in O(V) \mid \det \sigma = 1\}.$$

$O^+(V)$ is a subgroup of $O(V)$ such that $(O(V) : O^+(V)) = 2$. It is a well-known fact that every isometry $\sigma \in O(V)$ is a product of at most $n(= \dim V)$ symmetries, where a symmetry $\tau_x \in O(V)$ is a reflection defined by

$$\tau_x(y) = y - \frac{2B(x,y)}{Q(x,x)}x, \quad {}^{\forall}y \in V,$$

for any given anisotropic vector x of V.

2. The Algebras of Quadratic Forms

Let A be an algebra over F. We say that A is central if the center of A is $F1_A$ and that A is simple if A contains no non-trivial proper two-sided ideals. So every division algebra is simple. We state Weddeburn's Theorem :

THEOREM2.1(WEDDERBURN). *Let A be a central simple algebra over F. Then there exist a unique positive integer n and a unique central division algebra $D = D_A$ (up to algebra isomorphism) such that*

$$A \simeq M_n(F) \otimes D \simeq M_n(D).$$

Proof. See [L] for a detailed proof.

DEFINITION2.2. Let A, B be central simple algebras over F. We say that A, B are similar, write $A \sim B$, if $D_A \simeq D_B$.

Note that if $A \sim B$ and $\dim A = \dim B$, then $A \simeq B$.

REMARK2.3. $Br(F) = \{\text{central simple algebras over} \, F\}/\sim$ is a group, called the Brauer group, under $\otimes_F$. It is known that $Br(\mathbf{R}) \simeq \{\pm 1\}$, $Br(\mathbf{F}_q) \simeq 0$, and $Br(k_\wp) \simeq \mathbf{Q}/\mathbf{Z}$, where $k_\wp$ is the $\wp$-adic completion of a number field k at a prime spot $\wp$.

DEFINITION2.4. Let V be a regular quadratic space over F. An algebra A is said to be compatible with V if A contains V as a subspace and $x^2 = Q(x)1_A$, $^\forall x \in V$. An algebra C, which is compatible with V, is called a Clifford algebra of V if for any algebra A compatible with V, there exists a unique algebra isomorphism $\varphi : C \to A$ such that $\varphi x = x$, $^\forall x \in V$.

Such C always exists uniquely up to isomorphism. In fact, C is generated by V with $\dim C = 2^n$. A basis of C is

$$\{x_1^{e_1} \cdots x_n^{e_n} \mid e_i = 0 \text{ or } 1\},$$

which we call the derived basis from $x_1, \cdots, x_n$, where $V = Fx_1 \perp \cdots \perp Fx_n$.

DEFINITION2.5. Let $\sigma = \tau_{u_1} \cdots \tau_{u_r} \in O(V)$. We define

$$\theta(\sigma) = Q(u_1) \cdots Q(u_r)$$

and call it the spinor norm of σ.

The spinor norm θ is well-defined modulo $(F^\times)^2$. Note that $\theta(\sigma) \neq 0$ and $\theta(\sigma\tau) = \theta(\sigma)\theta(\tau)$. One knows that $\theta(\sigma) = \det(\frac{1+\sigma}{2})$ for $\sigma \in O^+(V)$ if the determinant is not zero. We set

$$O'(V) = \{\sigma \in O^+(V) \mid \theta(\sigma) = 1\}.$$

DEFINITION2.6. Let $V = F1_V + Fx_1 + Fx_2 + Fx_3$ be an algebra satisfying $x_1^2 = \alpha 1_V$, $x_2^2 = \beta 1_V$, $x_1x_2 = x_3 = -x_2x_1$ for $\alpha, \beta \in F^{\times}$. V is called a quaternion algrbra, denoted by $(\alpha, \beta) = (\frac{\alpha, \beta}{F})$. For $x = a_0 1_V + a_1x_1 + a_2x_2 + a_3x_3 \in (\alpha, \beta)$, we define

$$\begin{aligned}\bar{x} &= a_0 1_V - a_1x_1 - a_2x_2 - a_3x_3 \\ Nx = x\bar{x} &= (a_0^2 - a_1^2\alpha - a_2^2\beta + a_3^2\alpha\beta)1_V \\ Tx = x + \bar{x} &= 2a_0 1_V.\end{aligned}$$

We denote the set of pure quatarnions by $(\alpha, \beta)^0 = Fx_1 + Fx_2 + Fx_3$.

It is easy to show that (α, β) is central simple and $(1, -1) \simeq M_2(F)$. If $V \simeq \langle\alpha\rangle\perp\langle\beta\rangle$ is a regular quadratic space over F, then (α, β) is isomorphic to the Clifford algebra C of V.

We now give a quadratic structure to (α, β) as follows :

$$B(x, y)1_V = \frac{1}{2}T(x\bar{y}) \text{ and } \mathbf{Q}(x)1_V = Nx.$$

Then $d(\alpha, \beta) = 1$ and

$$\begin{aligned}(\alpha, \beta) &= F1_V \perp (\alpha, \beta)^0 \\ &= F1_V \perp Fx_1 \perp Fx_2 \perp Fx_3 \\ &\simeq \langle 1\rangle\perp\langle -\alpha\rangle\perp\langle -\beta\rangle\perp\langle \alpha\beta\rangle.\end{aligned}$$

The followings are easy to verify :

THEOREM2.7. (1) *Let C, D be quaternion algebras. Then C, D are isomorphic if and only if C, D are isometric if and only if C^0, D^0 are isometric.*

(2) *Let $\alpha, \beta \in F^{\times}$. Then $(\alpha, \beta) \simeq (1, -1)$ if and only if (α, β) is not a division algebra if and only if (α, β) is isotropic if and only if $(\alpha, \beta)^0$ is isotropic if and only if $\langle\alpha\rangle\perp\langle\beta\rangle$ represents 1.*

(3) *Let $\alpha, \beta, \gamma, \lambda, \mu \in F^{\times}$. Then the followings hold :*

$$(1, \alpha) \simeq (1, -1) \simeq (\alpha, -\alpha) \simeq (\alpha, 1 - \alpha)$$

$$(\beta, \alpha) \simeq (\alpha, \beta) \simeq (\alpha\lambda^2, \beta\mu^2)$$

$$(\alpha, \alpha\beta) \simeq (\alpha, -\beta)$$

$$(\alpha, \beta) \otimes (\alpha, \gamma) \simeq (\alpha, \beta\gamma) \otimes (1, -1) \sim (\alpha, \beta\gamma)$$

$$(\alpha, \beta) \otimes (\alpha, \beta) \sim (1, -1).$$

DEFINITION2.7. Let $V \simeq \langle\alpha_1\rangle\perp\cdots\perp\langle\alpha_n\rangle$ be a regular quadratic space. We define the Hasse algebra SV of V by

$$SV = \bigotimes_{i=1}^{n}(\alpha_i, d_i)$$

where $d_i = \alpha_1\cdots\alpha_i$.

SV is unique up to isomorphism. It is easy to see that $SV \sim \otimes_{1\leq i\leq j\leq n}(\alpha_i,\alpha_j)$ and that $SV \sim SU\otimes(dU, dW)\otimes SW$ if $V = U\perp W$.

THEOREM2.8. *Let V, V' be regular quadratic spaces of* $\dim n$, $1\leq n\leq 3$. *Then*

$$V \simeq V' \text{ if and only if } dV = dV' \text{ and } SV \sim SV'.$$

Proof. It is enough to prove the sufficiency. For $n = 1$, there is nothing to prove. Let $n = 3$. By scaling, we may assume $dV = dV' = 1$ and then

$$V \simeq \langle-\alpha\rangle\perp\langle-\beta\rangle\perp\langle\alpha\beta\rangle \simeq (\alpha,\beta)^0$$
$$V' \simeq \langle-\gamma\rangle\perp\langle-\delta\rangle\perp\langle\gamma\delta\rangle \simeq (\gamma,\delta)^0$$

for some $\alpha,\beta,\gamma,\delta\in F^\times$. From $SV\sim SV'$ follows $(\alpha,\beta)\sim(\gamma,\delta)$ and hence $(\alpha,\beta)\simeq(\gamma,\delta)$ as algebras. So by Theorem 2.7-(1),

$$V \simeq (\alpha,\beta)^0 \simeq (\gamma,\delta)^0 \simeq V'.$$

Now for $n = 2$, the theorem follows by applying Witt's Theorem to $W = V\perp\langle1\rangle \simeq V'\perp\langle1\rangle = W'$.

THEOREM2.9. *Let F be a field with the property that every regular quadratic space of dimension ≥ 5 over it is isotropic. Then two regular quadratic spaces V, V' over F is isometric if and only if*

$$\dim V = \dim V',\ dV = dV', \text{ and } SV \sim SV'.$$

Proof. It is enough to prove the sufficiency. Let $\dim V = \dim V' = n$. For $n = 1, 2, 3$, the theorem follows from Theorem 2.8. So assume $n\geq 4$. We use induction on n. Consider $V\perp\langle-1\rangle$, which is isotropic by hypothesis. Obviously, $1\in Q(V)$ and hence $\langle1\rangle$ splits V, i.e., $V = \langle1\rangle\perp U$ for some $(n-1)$-ary subspace U of V. Similary, $V' = \langle1\rangle\perp U'$ for some $(n-1)$-ary subspace U' of V'. $U\simeq U'$ follows immediately from induction hypothesis, which proves $V\simeq V'$.

3. Hasse-Minkowski Theorem

DEFINITION3.1. Any n-ary regular quadratic space V over $\mathbf{R}$ can be written in the form $V \simeq \underbrace{\langle 1\rangle \perp \cdots \perp \langle 1\rangle}_{p} \perp \underbrace{\langle -1\rangle \perp \cdots \perp \langle -1\rangle}_{q}$, where $p+q=n$. V is said to be positive (negative) definite if $q=0$ ($p=0$). V is said to be definite (indefinite) if $pq=0$ ($pq \neq 0$). We set $\operatorname{ind}^+ V = p$, $\operatorname{ind}^- V = q$, and $\operatorname{ind} V = \min(p,q)$.

For regular spaces V, V' over $\mathbf{R}$, we have $V \rightarrow V'$ if and only if $\operatorname{ind}^+ V \leq \operatorname{ind}^+ V'$ and $\operatorname{ind}^- V \leq \operatorname{ind}^- V'$. $V \simeq V'$ if and only if $\operatorname{ind}^+ V = \operatorname{ind}^+ V'$ and $\operatorname{ind}^- V = \operatorname{ind}^- V'$. Note that there are exactly two non-isomorphic quaternion algebras over $\mathbf{R}$, namely,

$$\left(\frac{-1,-1}{\mathbf{R}}\right) \text{ and } \left(\frac{1,-1}{\mathbf{R}}\right).$$

REMARK3.2. Any n-ary regular quadratic space over $\mathbf{C}$ is of the form $V \simeq \langle 1\rangle \perp \cdots \perp \langle 1\rangle$. So for any regular spaces V, V' over $\mathbf{C}$, we have $V \rightarrow V'$ if and only if $\dim V \leq \dim V'$ and $V \simeq V'$ if and only if $\dim V = \dim V'$. Furthermore, we have only one quaternion algebra up to isomorphism over $\mathbf{C}$, namely,

$$\left(\frac{1,-1}{\mathbf{C}}\right).$$

Let F be a local field with a prime spot $\wp$. We let $\mathcal{O} = \mathcal{O}(\wp)$, $\wp = m(\wp)$, and $U = U(\wp)$, be the ring of integers of F at $\wp$, the maximal ideal of $\mathcal{O}$, and the unit group of $\mathcal{O}$, respectively. One can easily prove the following :

(Local Square Theorem) For any $\alpha \in \mathcal{O}$, $1+4\pi\alpha$ is a square, where π is a prime element of F.

Any $\xi \in F$ can be expressed in the form $\xi = \eta^2 + \alpha$ for at least one pair $\eta, \alpha \in F$. We define the quadratic defect $\delta(\xi)$ of ξ by

$$\delta(\xi) = \bigcap_{\alpha \in F; \xi = \eta^2 + \alpha} \alpha\mathcal{O}.$$

It is well-known that for a unit $\varepsilon \in F$,

$$\delta(\varepsilon) = \begin{cases} 0 \text{ or } \mathcal{O} & \text{if } \wp \text{ is non-dyadic} \\ 0, 4\mathcal{O}, 4\wp^{-1}, \cdots, \wp^2, \wp & \text{if } \wp \text{ is dyadic.} \end{cases}$$

Also known that there exists $\Delta \in U$ with $\delta(\Delta) = 4\mathcal{O}$. Of course, $4\mathcal{O} = \mathcal{O}$ if $\wp$ is non-dyadic. Note that $\delta(\xi) = 0$ if and only if ξ is a square.

DEFINITION3.3. Let $F = \mathbf{R}, \mathbf{C}$, or a local field and let $\wp =$ real, complex, or prime spots, accordingly. For $\alpha, \beta \in F^\times$, we define the Hilbert symbol

$$(\frac{\alpha, \beta}{\wp}) = \begin{cases} 1 & \text{if } \alpha\xi^2 + \beta\eta^2 = 1 \text{ for some } \xi, \eta \in F \\ -1 & \text{otherwise.} \end{cases}$$

For a regular space $V \simeq \langle\alpha_1\rangle \perp \cdots \perp \langle\alpha_n\rangle$, we define the Hasse symbol

$$S_\wp V = \prod_{i=1}^{n} (\frac{\alpha_i, d_i}{\wp})$$

where $d_i = \alpha_1 \cdots \alpha_i$.

REMARK3.4(HILBERT RECIPROCITY LAW). For any $\alpha, \beta \in F^\times$,

$$\prod_\wp (\frac{\alpha, \beta}{\wp}) = 1$$

and for any regular quadratic space V,

$$\prod_\wp S_\wp V = 1.$$

Note that a quaternion algebra $(\frac{\alpha, \beta}{F})$ is a division algebra if and only if $(\frac{\alpha, \beta}{\wp}) = -1$.

We come back to the case when F is a local field with a prime spot $\wp$. We fix π,Δ as above. We have the following very useful property : If V is a binary space over F with dV a prime element, then for any $\gamma \in F^{\times}, V$ represents either γ or $\Delta\gamma$ but not both.

From this, it is easy to see that $(\frac{\pi, \Delta}{\wp}) = -1$, $(\frac{\varepsilon, \Delta}{\wp}) = 1$, $^{\forall}\varepsilon \in U$, and that every quaternion division algebra is isomorphic to $(\frac{\pi, \Delta}{F})$. So there are exactly two non-isomorphic quaternion algebras over F, namely,

$$(\frac{\pi, \Delta}{F}) \text{ and } (\frac{1, -1}{F}).$$

Combining these facts, one obtains the following : If V is an anisotropic quaternary space over F, then $dV = 1$ and

$$V \simeq \langle 1\rangle \perp \langle -\Delta\rangle \perp \langle \pi\rangle \perp \langle -\pi\Delta\rangle$$

Therefore, V is universal if $\dim V = 4$ and hence V is isotropic if V is regular over F with $\dim V \geq 5$.

THEOREM3.5. *Let V, V' be regular spaces over a local field F with a prime spot $\wp$. Then*

(1) *$V \to V'$ if and only if*

$$\begin{cases} V' \simeq V \text{ when } \dim V' = \dim V, \\ V' \simeq V \perp \langle dV \cdot dV'\rangle \text{ when } \dim V' = \dim V + 1, \\ V' \simeq V \perp H \text{ when } \dim V' = \dim V + 2 \text{ and } dV' = -dV. \end{cases}$$

Here H is a hyperbolic plane.

(2) *$V \simeq V'$ if and only if*

$$\dim V = \dim V',\ dV = dV', \text{ and } S_{\wp}V = S_{\wp}V'.$$

Proof. (1) It is enough to prove the sufficiency. Let $r = \dim V' - \dim V$. When $r = 0, 1$, it is trivial.

Let $r \geq 3$ and let

$$V \simeq \langle\alpha_1\rangle\perp\ldots\perp\langle\alpha_n\rangle$$
$$V' \simeq \langle\beta_1\rangle\perp\ldots\perp\langle\beta_m\rangle.$$

Since $\langle\beta_1\rangle\perp\langle\beta_{n+1}\rangle\perp\langle\beta_{n+2}\rangle\perp\langle\beta_{n+3}\rangle$ represents α_1,

$$V' \simeq \langle\alpha_1\rangle\perp\langle\beta_2\rangle\perp\ldots\perp\langle\beta_n\rangle\perp\langle\gamma_{n+1}\rangle\perp\ldots\perp\langle\gamma_m\rangle.$$

Repeating this process, one concludes that

$$V' \simeq \langle\alpha_1\rangle\perp\ldots\perp\langle\alpha_n\rangle\perp\langle\delta_{n+1}\rangle\perp\ldots\perp\langle\delta_m\rangle,$$

which implies $V \to V'$.

Now let $r = 2$. If $dV' = -dV$, then the theorem follows from the given condition. So we assume $dV' \neq -dV$. Since $\dim(V'\perp H) - \dim V = 4$, we have $V \to V'\perp H$ and hence $V\perp W \simeq V'\perp H$ for some quaternary space W. $dW \neq 1$ implies that W is isotropic. So $W \simeq W_1\perp H_1$, where H_1 is a hyperbolic plane. According to Witt's Theorem, $V\perp W_1 \simeq V'$ and hence $V \to V'$.

(2) Clear from the above and Theorem 2.9.

Let F be a global field and $\alpha \in F$. We list the following two standard results from algebraic number theory :

(Global Square Theorem) α is a square if and only if α is a square at almost all spots on F.

(Local-Global Norm Theorem) Let E be a quadratic extension of F. Then α is a global norm if and only if α is a local norm at every spot on F.

Let V be a quadratic space over a global field F and let $\wp$ be a prime spot on F. By $V_\wp$ we denote the quadratic space $F_\wp V$ over $F_\wp$, the $\wp$-adic completion of F at $\wp$.

THEOREM3.6. *A regular quadratic space over a global field F is isotropic if and only if it is isotropic at every spot on F.*

Proof. It is enough to show the sufficiency. Let V be a regular n-ary quadratic space over a global field F. We may assume $n \geq 2$. Fix an orthogonal basis $x_1, \ldots, x_n$ for which $V \simeq \langle\alpha_1\rangle\perp\cdots\perp\langle\alpha_n\rangle$, $\alpha_i \in F^\times$.

Let $n = 2$. $dV_\wp = \alpha_1\alpha_2 = -1$. So $-\alpha_1\alpha_2$ is a square at each $\wp$. Hence $-\alpha_1\alpha_2$ is a square in F by GST. So $dV = -1$, that is, V is a hyperbolic plane, which is isotropic.

Let $n = 3$. By scaling, we may assume $V \simeq \langle -\alpha\rangle \perp P$, $P \simeq \langle 1\rangle \perp \langle -\beta\rangle$ with β non-square. (If β is a square, then P is a hyperbolic plane.) Since $V_\wp$ is isotropic, $P_\wp$ represents α at each $\wp$. So $\alpha = \xi_\wp^2 - \beta\eta_\wp^2$ for some $\xi_\wp, \eta_\wp \in F_\wp$, i.e., α is a local norm from $E = F(\sqrt{\beta})$ to F at each $\wp$. So α is a global norm, i.e., $\alpha = \xi^2 - \beta\eta^2$ for some $\xi, \eta \in F$. This proves that V is isotropic.

Let $n = 4$. Assume $dV = 1$. Then any regular ternary subspace U of V is isotropic because $U_\wp$ is isotropic at each $\wp$. (This is because $V_\wp$ is isotropic and $dV_\wp = 1$.) So V is isotropic. Now assume $dV \neq 1$. Let $V = Fx_1 \perp Fx_2 \perp Fx_3 \perp Fx_4$, $Q(x_i) = \alpha_i$, $i = 1, 2, 3, 4$. Let $\beta = \alpha_1\alpha_2\alpha_3\alpha_4$, $E = F(\sqrt{\beta})$. $(EV)_{\mathcal{P}}$ is isotropic for any spot $\mathcal{P}$ on E because $V_\wp$ is isotropic for any $\wp$ on F. But $d(EV) = 1$ because β is a square in E and this implies EV is isotropic. It follows immediately that V is isotropic.

Let $n \geq 5$. We use induction on n. Let $U = Fx_1 \perp Fx_2$, $W = Fx_3 \perp \cdots \perp Fx_n$ such that $V = U \perp W$. Let

$$T = \{\wp \text{ on } F \mid W_\wp \text{is anisotropic } \}.$$

Clearly, T is a finite set. There exists $\mu_\wp \in F_\wp^\times$ for any $\wp \in T$ such that $\mu_\wp \in Q(U_\wp)$, $-\mu_\wp \in Q(W_\wp)$. By Chinese Remainder Theorem or Weak Approximation Theorem, one can find $\mu \in F^\times$ such that μ is close to $\mu_\wp$, ${}^\forall\wp \in T$. Since $(F_\wp^\times)^2$ is open in $F_\wp^\times$, $\mu \in \mu_\wp(F_\wp^\times)^2$, ${}^\forall\wp \in T$. Write $V \simeq \langle\mu'\rangle \perp \langle\mu\rangle \perp W$. Then $\langle\mu\rangle \perp W$ is isotropic since $-\mu \in -\mu_\wp(F_\wp^\times)^2 \subseteq Q(W_\wp)$, ${}^\forall\wp \in T$, and $W_\wp$ is isotropic at every $\wp \notin T$. This completes the proof.

REMARK3.7. An n-ary regular quadratic space over a function field is isotropic if $n \geq 5$.

THEOREM3.8(HASSE-MINKOWSKI). *Let V, V' be regular spaces over a global field F. Then,*

(1) *$V \to V'$ if and only if $V_\wp \to V'_\wp$ for all $\wp$ on F.*

(2) *$V \simeq V'$ if and only if $V_\wp \simeq V'_\wp$ for all $\wp$ on F.*

Proof. (1) It is enough to prove the sufficiency. Let $\alpha \in F^\times$ be represented by $V'_\wp$ for any $\wp$. Then $\langle -\alpha\rangle \perp V'_\wp$ is isotropic at any $\wp$ and hence $\langle -\alpha\rangle \perp V'$ is. This proves the theorem when $\dim V = 1$. We use induction on $\dim V$. Let $\dim V \geq 2$. For any nonzero $\alpha \in Q(V)$, we may write $V \simeq \langle -\alpha\rangle \perp W$ and $V' \simeq \langle -\alpha\rangle \perp W'$. Since $V_\wp \to V'_\wp$ for all $\wp$, $W_\wp \to W'_\wp$ for all $\wp$. So $W \to W'$ by induction hypothesis and hence $V \to V'$.

(2) Clear from (1).

II. Quadratic Forms over Rings

4. Classification of Lattices over Local Fields

Let F be a global field or a local field, ch$F \neq 2$, $\mathcal{O}$ the ring of integers of F, U the group of units of F, and I the group of nonzero fractional ideals of F.

DEFINITION4.1. Let V be a vector space over F with $\dim V = n$. An $\mathcal{O}$-module L in V is called a lattice in V if $L \subseteq \mathcal{O}x_1 + \cdots + \mathcal{O}x_n$ for some basis $x_1, \cdots, x_n$ for V. A lattice L is on V if $FL = V$. We define rank$L = \dim FL$. A lattice L is said to be free if $L = \mathcal{O}x_1 + \cdots + \mathcal{O}x_r$ for some basis $x_1, \cdots, x_r$ for FL. We call $x_1, \cdots, x_r$ a basis for L in this case and define $\dim L = r = \dim FL = $ rank$L$.

The followings are basic properties on lattices.

THEOREM4.2. (1) *There exists a basis $x_1, \cdots, x_r$ for FL such that*

$$L = \mathcal{A}_1 x_1 + \cdots + \mathcal{A}_r x_r$$

where $\mathcal{A}_i = \{\alpha \in F \,|\, \alpha x_i \in L\} \in I$, called the coefficient of x_i with respect to L. Furthermore, one can find a basis $z_1, z_2, \cdots, z_r$ for FL such that

$$L = \mathcal{A}z_1 + \mathcal{O}z_2 + \cdots + \mathcal{O}z_r,$$

where $\mathcal{A}$ is the coefficient of z_1 with respect to L. Note that every L is free if $\mathcal{O}$ is a p.i.d.

(2) *For lattices L, K on V, there exists a basis $x_1, \cdots, x_n$ for V such that*

$$L = \mathcal{A}_1 x_1 + \cdots + \mathcal{A}_n x_n$$
$$K = \mathcal{A}_1\mathcal{B}_1 x_1 + \cdots + \mathcal{A}_n\mathcal{B}_n x_n$$

where $\mathcal{A}_i, \mathcal{B}_i \in I$ and $\mathcal{B}_n \subseteq \mathcal{B}_{n-1} \subseteq \cdots \subseteq \mathcal{B}_1$. The fractional ideals $\mathcal{B}_1, \cdots, \mathcal{B}_n$ are uniquely determined by L and K, called the invariant factors of K in L.

Let F be a global field and $\wp$ a prime spot. Let $\mathcal{O}_\wp$ and $U_\wp$ denote the ring of integers of $F_\wp$ and and the group of units of $\mathcal{O}_\wp$, respectively.

Let L be a lattice in a vector space V over F. By the localization of L at $\wp$, we mean an $\mathcal{O}_\wp$-module generated by L, denoted by $L_\wp$. Clearly $L_\wp$ is a lattice in $V_\wp$. So for $L = \mathcal{A}_1 x_1 + \cdots + \mathcal{A}_n x_n$, the localization of L at $\wp$ is given by

$$L_\wp = \mathcal{A}_{1,\wp} x_1 + \cdots + \mathcal{A}_{n,\wp} x_n$$

where $\mathcal{A}_\wp$ denotes the closure of $\mathcal{A}$ in $F_\wp$ for $\mathcal{A} \in I$.

DEFINITION4.3. Let K, L be lattices on V where V is a regular n-ary quadratic space over F, a global or a local field. We define $K \simeq L$ if $K = \sigma L$ for some $\sigma \in O(V)$. This is an equivalence relation and we call the equivalence class of L the class of L, denoted by $clsL$. Similary, we define cls^+L, the proper class of L, to be the set of all lattices K on V satisfying $K = \sigma L$ for some $\sigma \in O^+(V)$. We define

$$O(L) = \{\sigma \in O(V) \,|\, \sigma L = L\}$$
$$O^+(L) = O(L) \cap O^+(V).$$

$O(L)$ and $O^+(L)$ are called the orthogonal group and the proper orthogonal group, respectively, of L.

Note that

$$clsL = cls^+L \text{ if and only if } (O(L) : O^+(L)) = 2.$$

So $clsL = cls^+L$ if $O(L) \cap O^-(V) \neq \phi$. We say that L is regular if FL is regular.

We now define several invariants of a lattice L in V over F, which are necessary in what follows, where F is a global or a local field. The scale sL of L is an $\mathcal{O}$-module generated by $B(L, L)$. The norm nL of L is an $\mathcal{O}$-module generated by $Q(L)$. Note that

$$2sL \subset nL \subset sL.$$

If we assume L is a non-zero regular lattice, then sL, nL are fractional ideals of F. The volume of vL of L is defined by

$$vL = \mathcal{A}_1^2 \cdots \mathcal{A}_r^2 \det(x_1, \cdots, x_r)$$

where $L = \mathcal{A}_1x_1 + \cdots + \mathcal{A}_rx_r$ for some basis $x_1, \cdots, x_r$ for FL and $\det(x_1, \cdots, x_r) = \det(B(x_i, x_j))$. It is easy to see that vL is well-defined and that

$$vL \subseteq (sL)^r.$$

A lattice L in V is called an $\mathcal{A}$-modular lattice ($\mathcal{A} \in I$) if

$$sL = \mathcal{A} \text{ and } vL = (sL)^r$$

where $r = \mathrm{rank}L$. L is said to be unimodular if L is $\mathcal{O}$-modular. The dual lattice $L^\sharp$ of L is defined by

$$L^\sharp = \{x \in FL \,|\, B(x, L) \subset \mathcal{O}\}.$$

If $L = \mathcal{A}_1x_1 + \cdots + \mathcal{A}_rx_r$, then

$$L^\sharp = \mathcal{A}_1^{-1}y_1 + \cdots + \mathcal{A}_r^{-1}y_r$$

where $y_1, \cdots, y_r$ is the dual basis of $x_1, \cdots, x_r$ for FL. Note that L is $\mathcal{A}$-modular if and only if $\mathcal{A}L^\sharp = L$. So L is unimodular if and only if $L^\sharp = L$.

Let L be a lattice with $sL = \mathcal{A}$ and J an $\mathcal{A}$-modular sublattice of L. Since FJ is regular, FJ splits FL, i.e., $FL = FJ \perp U$ for some subspace U of FL. Pick any $x \in L$ and write $x = y + z$, with $y \in FJ, z \in U$. Then

$$B(y, J) = B(x, J) \subseteq sL = \mathcal{A}$$

implies $y \in J$ since J is $\mathcal{A}$-modular. Now $z = x - y \in L \cap U$. Therefore, we may conclude that

$$L = J \perp K$$

for some sublattice $K (= L \cap U)$ of L, i.e., J splits L in this case.

We now assume that F is a local field with a prime spot $\wp$, and let V be a regular quadratic space over F. Let L be a regular lattice in V. Obviously, L is free in this case. It is a well-known fact that L can be split into 1-and 2-dimensional modular lattices as follows : If there exists $x \in L$ such that $Q(x)\mathcal{O} = sL$, then take $J = \mathcal{O}x$; if not, choose $x, y \in L$ such that $B(x, y)\mathcal{O} = sL$ and take $J = \mathcal{O}x + \mathcal{O}y$. Then J is an sL-modular sublattice of L and J splits L, i.e., $L = J \perp K$. Note that $sK \subseteq sL$. Repeat this procedure for $K, \cdots$. Regrouping those components suitably, we have

$$L = L_1 \perp L_2 \perp \cdots \perp L_t$$

with a proper chain of fractional ideals

$$sL_1 \supset sL_2 \supset \cdots \supset sL_t$$

where L_i are sL_i-modular. We call such a splitting a Jordan splitting of L. Assume $L = L_1 \perp \cdots \perp L_t = K_1 \perp \cdots \perp K_r$ be two Jordan splittings of L. Then they are of the same type in the sense that

$$t = r,\ sL_i = sK_i,\ \dim L_i = \dim K_i,$$
$$nL_i = sL_i \text{ if and only if } nK_i = sK_i,\ {}^{\forall}i = 1, 2, \ldots, t.$$

Note that the last condition is redundunt if $\wp$ is non-dyadic.

We give the following theorem on classification of lattices over non-dyadic local fields. See [O] for a detailed proof.

THEOREM4.4. *Let L, K be regular lattices of the same Jordan type on a regular quadratic space V over a non-dyadic local field F with Jordan splittings*

$$L = L_1 \perp \cdots \perp L_t$$
$$K = K_1 \perp \cdots \perp K_t.$$

Then

$$clsL = clsK \text{ if and only if } FL_i \simeq FK_i,\ {}^{\forall}i = 1, \cdots, t.$$

We need more definitions to deal with lattices over dyadic local fields. Let F be a dyadic local field and let L be a lattice in a regular space V over F. The norm group gL of L is defined by

$$gL = Q(L) + 2sL.$$

Clearly,

$$2sL \subseteq gL \subseteq nL.$$

A norm generator ν of L is defined to be a scalar of largest value in gL. ν is determined uniquely up to multiplication by a unit square modulo $\omega = \omega(L^{sL})$, a fractinal ideal introduced in the below. One can easily check that ν is a norm generator of L if and only if $\nu \in gL \subseteq \nu\mathcal{O}$, i.e.,

$$\nu \in gL \text{ with } \nu\mathcal{O} = nL.$$

The weight ωL of L is defined by

$$\omega L = \wp \cdot mL + 2sL$$

where mL is the largest fractinal ideal of F contained in gL. Of course, gL is not necessarily a fractional ideal of F. For a nonzero fractional ideal $\mathcal{A}$ of F, $L^{\mathcal{A}}$ is a sublattice of L defined by

$$L^{\mathcal{A}} = \{x \in L \,|\, B(x, L) \subseteq \mathcal{A}\}.$$

One can easily check that

$$L^{\mathcal{A}} = \mathcal{A}L^{\sharp} \cap L.$$

Let $L = L_1 \perp L_2 \perp \cdots \perp L_t$ be a Jordan splitting of L. Then

$$t,\ \dim L_i,\ sL_i,\ \omega_i = \omega(L^{sL_i}),\ \nu_i$$

are called the fundamental invariants of the Jordan splitting, where ν_i is a norm generator of L^{sL_i} for each i. Any two Jordan splittings of the same lattice have the same fundamental invariants. So we may regard the invariants are of the lattice.

Note that

$$\omega_1 \supseteq \cdots \supseteq \omega_t$$
$$g_1 \supseteq \cdots \supseteq g_t$$

where $g_i = g(L^{sL_i})$. Also note that

$$g_i = g(L^{sL_i}) = \nu_i\mathcal{O}^2 + \omega_i.$$

We define $\mathcal{F}_i$ by

$$(sL_i)^2\mathcal{F}_i = \begin{cases} \sum \delta(\alpha\beta) & \text{if } \mathrm{ord}_\wp \nu_i + \mathrm{ord}_\wp \nu_{i+1} \text{ is odd} \\ \sum \delta(\alpha\beta) + 2\wp^{\frac{1}{2}(\mathrm{ord}_\wp \nu_i + \mathrm{ord}_\wp \nu_{i+1} + 2\mathrm{ord}_\wp sL_i)} & \text{otherwise} \end{cases}$$

where the summation is over $\alpha \in g_i, \beta \in g_{i+1}$. The following formula is useful in determining $\mathcal{F}_i$:

$$(sL_i)^2\mathcal{F}_i = \begin{cases} \nu_i\nu_{i+1}\mathcal{O} & \text{if } \mathrm{ord}_\wp \nu_i + \mathrm{ord}_\wp \nu_{i+1} \text{ is odd} \\ \delta(\nu_i\nu_{i+1}) + \nu_i\omega_{i+1} + \nu_{i+1}\omega_i & \\ +2\wp^{\frac{1}{2}(\mathrm{ord}_\wp \nu_i + \mathrm{ord}_\wp \nu_{i+1} + 2\mathrm{ord}_\wp sL_i)} & \text{otherwise.} \end{cases}$$

The following remarkable theorem due to O'Meara provides a tool for classifying lattices over dyadic local fields. See [O] for a detailed proof.

THEOREM4.5. *Let L, K be regular lattices over a dyadic local field F having the same fundamental invariants. Let*

$$L_{(i)} = L_1 \perp \cdots \perp L_i$$
$$K_{(i)} = K_1 \perp \cdots \perp K_i$$

for each $i = 1, 2, \ldots, t$, where

$$L = L_1 \perp \cdots \perp L_t$$
$$K = K_1 \perp \cdots \perp K_t$$

are given Jordan splittings. Then $clsL = clsK$ if and only if for $1 \leq i \leq t-1$

(1) $dL_{(i)} \equiv dK_{(i)} \cdot \varepsilon^2$ (mod $\mathcal{F}_i$) *for some* $\varepsilon \in U$, *and*
(2) $FL_{(i)} \to FK_{(i)} \perp \langle \nu_{i+1} \rangle$ *if* $\mathcal{F}_i \subset 4\nu_{i+1}\omega_{i+1}^{-1}$,
$FL_{(i)} \to FK_{(i)} \perp \langle \nu_i \rangle$ *if* $\mathcal{F}_i \subset 4\nu_i\omega_i^{-1}$.

We now introduce an effective way of computing the above invariants.

Let L be a lattice on V over a local field F with a prime spot $\wp$. Since L is free, $L = \mathcal{O}x_1 + \cdots + \mathcal{O}x_n$. Then sL is the largest among $B(x_i, x_j)\mathcal{O}$ and nL is the largest among $Q(x_i)\mathcal{O}$ and $2(sL)$. A norm generator ν of L can be obtained as follows : If $nL = 2(sL)$, take any $\nu \in F$ satisfying $\nu\mathcal{O} = 2(sL)$; otherwise, take $\nu = Q(x_i)$ for which $Q(x_i)\mathcal{O}$ is the largest. As for the weight ωL, one can use the following formula :

$$\omega L = \sum_j \nu\delta(Q(x_j)/\nu) + 2(sL).$$

One can get a Jordan splitting of L as follows :

(case 1) $\wp$: non-dyadic

We may assume $Q(x_1)\mathcal{O} = sL$ by adjusting given basis if necessary. Take $y_i = \tau_{x_1}(x_i) \in L$, $i = 2, \cdots, n$. Then

$$L = \mathcal{O}x_1 \perp (\mathcal{O}y_2 + \cdots + \mathcal{O}y_n).$$

Repeating this procedure for $\mathcal{O}y_2 + \cdots + \mathcal{O}y_n$, we can obtain an orthogonal basis for L. Regrouping these basis vectors suitably, we get a Jordan splitting.

(case 2) $\wp$: dyadic

If there exists x_1 with $Q(x_1)\mathcal{O} = sL$, do the same as above. Otherwise, $Q(x_i)\mathcal{O}$ is properly contained in sL for all i. Then there exist x_1, x_2 such that $B(x_1, x_2)\mathcal{O} = sL$. Taking $y_i = x_i + \xi_i x_1 + \eta_i x_2$ for some $\xi_i, \eta_i \in \mathcal{O}$, $i = 3, \cdots, n$, we have

$$L = (\mathcal{O}x_1 + \mathcal{O}x_2) \perp (\mathcal{O}y_3 + \cdots + \mathcal{O}y_n).$$

Repeating and regrouping as above, we get a Jordan splitting.

5. Genus and Spinor Genus

Let V be an n-ary regular quadratic space over F, a global field or a local field. Let $\wp$ be a spot on F. We fix a basis $x_1, \cdots, x_n$ for V.

For $x = a_1x_1 + \cdots + a_nx_n \in V$, $a_i \in F$, we define

$$\|x\|_\wp = \max_{1 \le i \le n} |a_i|_\wp.$$

Similary for $\sigma \in L_F(V)$, $\sigma x_j = \sum_{i=1}^n a_{ij}x_i$, $a_{ij} \in F$, we define

$$\|\sigma\|_\wp = \max_{1\leq i,j\leq n} |a_{ij}|_\wp = \max_{1\leq j\leq n} \|\sigma x_j\|_\wp$$

where $L_F(V)$ is the space of F-linear maps from V to V.

Then V, $L_F(V)$ become normed vector spaces, hence topological vector spaces. Note also that all the following maps are continuous :

$$x \mapsto \|x\|_\wp,\ x \mapsto Q(x),\ (x,y) \mapsto B(x,y)$$
$$x \mapsto \tau_x \text{ (for anisotropic } x),\ (\sigma,\tau) \mapsto \sigma\tau,\ \sigma \mapsto \det\sigma$$
$$\sigma \mapsto \sigma^{-1} \text{ (for invertible } \sigma),\ \sigma \mapsto \|\sigma\|_\wp.$$

REMARK5.1. Let F be a local field with a prime spot $\wp$.

(1) Let $\sigma \in O(V)$. Since $\det\sigma = \pm 1$, we have $\|\sigma\| \geq 1$. On the other hand, $\sigma L \subseteq L$ implies $\|\sigma\| \leq 1$. Therefore, $\|\sigma\| = 1, \sigma L = L$. And hence

$$O(L) = \{\sigma \in O(V) \mid \|\sigma\| = 1\}.$$

(2) Let

$$L = \mathcal{O}x_1 + \cdots + \mathcal{O}x_n$$
$$L' = \mathcal{O}x_1' + \cdots + \mathcal{O}x_n'$$

and let $\sigma \in O(V)$ be close to 1. Then $\|\sigma-1\|' < 1$ implies $\|\sigma\|' = 1$ and $\sigma L' = L'$, where $\| \ \|'$ is the norm with respect to the basis $x_1', \ldots, x_n'$.

(3) Let $\sigma L = L'$ for $\sigma \in O(V)$ and let $\tau \in O(V)$ be close to σ. Then $\|\tau^{-1}\sigma - 1\| \leq \|\tau^{-1}\| \cdot \|\sigma - \tau\| < 1$ implies $\tau^{-1}\sigma L = L$, or $\sigma L = \tau L = L'$.

Let F be a global field and let $\wp \in \Omega_F$, where Ω_F is the set of all non-trivial spots on F. For $\sigma \in L_F(V)$, we define $\sigma_\wp : V_\wp \to V_\wp$ in a canonical manner, and call it the localization of σ at $\wp$. It is easy to see that

$$O(V)_\wp \subset O(V_\wp),\ O^+(V)_\wp \subset O^+(V_\wp),\ O'(V)_\wp \subset O'(V_\wp),\ {}^\forall\wp \in \Omega_F$$

and that

$$O(L)_\wp \subset O(L_\wp),\ O^+(L)_\wp \subset O^+(L_\wp),\ {}^\forall\wp < \infty.$$

DEFINITION 5.2. We set

$$J_F = \{i = (i_\wp)_{\wp\in\Omega_F} \mid |i_\wp|_\wp = 1 \text{ for almost all } \wp \in \Omega_F\}$$

and call it the idele group of F, which is a subgroup of $\prod_{\wp\in\Omega_F} F_\wp^\times$. The diagonal image of $F^\times$ in J_F is called the subgroup of principle ideles, denoted by P_F.

DEFINITION 5.3. We set

$$\begin{aligned} J_V =& \{\Sigma = (\Sigma_\wp)_{\wp\in\Omega_F} \mid \Sigma_\wp \in O^+(V_\wp),\ {}^\forall\wp \in \Omega_F \\ &\text{such that } \|\Sigma_\wp\|_\wp = 1 \text{ for almost all } \wp \in \Omega_F\} \end{aligned}$$

and call it the group of split rotations of V.

Notice that J_V is independent of the choice of a basis (on which $\| \ \|_\wp$ is dependent). We set

$$J'_V = \{\Sigma = (\Sigma_\wp)_{\wp\in\Omega_F} \in J_V \mid \Sigma_\wp \in O'(V_\wp)\ {}^\forall\wp \in \Omega_F\}.$$

It is easy to see that J'_V contains the commutator subgroup of J_V. Consider a map $O^+(V) \to J_V$ defined by $\sigma \mapsto (\sigma_\wp)_{\wp\in\Omega_F}$. Since $\|\sigma_\wp\|_\wp = 1$ for almost all $\wp \in \Omega_F$, this map is well-defined. We denote the image by P_V and call it the subgroup of principal split rotations.

Let

$$J_L = \{\Sigma = (\Sigma_\wp)_{\wp\in\Omega_F} \in J_V \mid \Sigma_\wp \in O^+(L_\wp),\ {}^\forall\wp < \infty\}$$

and let P_L be the diagonal image of $O^+(L)$ in J_V under the map above. Then one can easily see that

$$P_L = P_V \cap J_L.$$

Let

$$D = \theta(O^+(V)) \subset F^\times$$

and let P_D be the diagonal image of D in J_F, where θ is the spinor norm map in Definition 2.5.

We set

$$J_F^L = \{i = (i_\wp)_{\wp\in\Omega_F} \in J_F \mid i_\wp \in \theta(O^+(L_\wp)),\ {}^\forall\wp < \infty\}.$$

REMARK5.4. Let $\Sigma = (\Sigma_\wp)_{\wp \in \Omega_F} \in J_V$. Let L be a lattice on V. Then $\Sigma_\wp L_\wp$ is a lattice on $V_\wp$ for each $\wp < \infty$. It is known that there exists a unique lattice K on V such that $K_\wp = \Sigma_\wp L_\wp$, ${}^\forall\wp < \infty$. We denote this K by ΣL. From this we may rewrite J_L by

$$J_L = \{\Sigma \in J_V \,|\, \Sigma L = L\}.$$

DEFINITION5.5. Let K, L be lattices on V. We write $K \in genL$ (the genus of L) if there exists $\Sigma_\wp \in O(V_\wp)$ such that $\Sigma_\wp L_\wp = K_\wp$, ${}^\forall\wp < \infty$, and write $K \in gen^+L$ (the proper genus of L) if $\Sigma_\wp$ can be taken from $O^+(V_\wp)$, ${}^\forall\wp < \infty$.

From the definition follows immediately that

$$genK = genL \text{ if and only if } clsK_\wp = clsL_\wp,\ {}^\forall\wp < \infty$$
$$gen^+K = gen^+L \text{ if and only if } cls^+K_\wp = cls^+L_\wp,\ {}^\forall\wp < \infty.$$

It is well known that the class and the proper class of a lattice are identical over a local field and therefore, we may conclude that

$$genL = gen^+L.$$

Hence, $K \in genL$ if $K = \Sigma L$ for some $\Sigma \in J_V$, i.e.,

$$genL = \{\Sigma L \,|\, \Sigma \in J_V\}.$$

DEFINITION5.6. We write $K \in spnL$ (the spinor genus) if there exists $\sigma \in O(V)$, $\Sigma_\wp \in O'(V_\wp)$ such that $\sigma_\wp \Sigma_\wp L_\wp = K_\wp$, ${}^\forall\wp < \infty$, and write $K \in spn^+L$ (the proper spinor genus) if σ can be taken from $O^+(V)$.

As above, we have

$$spnL = \{\sigma\Sigma L \,|\, \sigma \in O(V),\ \Sigma \in J'_V\}$$
$$spn^+L = \{\sigma\Sigma L \,|\, \sigma \in O^+(V),\ \Sigma \in J'_V\}.$$

Note that

$$clsL \subseteq spnL \subseteq genL$$
$$cls^+L \subseteq spn^+L \subseteq gen^+L (= gen\,L).$$

DEFINITION5.7. We call the number of classes in the genus of L the class number of L and denote it by h_L. We define g_L to be the number of spinor genera in the genus of L and call it the spinor number of L. Similary define h_L^+, g_L^+ to be the numbers of proper classes, proper spinor genera, respectively, in the proper genus of L which is identical with the genus of L.

Clearly $h_L \geq g_L$ and $h_L^+ \geq g_L^+$. In any given class, there are one or two proper classes. Hence we have $h_L \leq h_L^+ \leq 2h_L$. Similary $g_L \leq g_L^+ \leq 2g_L$. One can check easily that

$$\Sigma(spn\, L) = spn(\Sigma L) \text{ and } \Sigma(spn^+ L) = spn^+(\Sigma L), \ {}^\forall\Sigma \in J_V.$$

Form this, we may conclude $g_L^+ = 2g_L$ or $g_L^+ = g_L$.

6. Class Number and Spinor Number

In this section, we introduce some important theorems on the class numbers and the spinor numbers of lattices. We start with the following classical theorem.

THEOREM6.1. *h_L is finite.*

Proof. In fact, lattices in the same genus have the same volume, scale, norm, and one can prove that the number of classes with given rank, scale, and volume is finite. We skip the detailed proof here.

THEOREM6.2. *g_L^+ divides $(J_F : P_D J_F^L)$ and*

$$g_L^+ = (J_V : J_V' P_V J_L).$$

In particular, if $n \geq 3$, then

$$g_L^+ = (J_V : J_V' P_V J_L) = (J_F : P_D J_F^L).$$

Proof. Note that $J_V' P_V J_L$ is a normal subgroup of J_V. From definitions follows that

$$spn^+(\Sigma_1 L) = spn^+(\Sigma_2 L) \text{ if and only if } \Sigma_2 \in \Sigma_1 J_V' P_V J_L.$$

Therefore, $g_L^+ = (J_V : J'_V P_V J_L)$. We consider a map

$$\Phi : J_V \to J_F / P_D J_F^L$$

defined as follows : Let $\Sigma \in J_V$. Then $\Sigma_\wp L_\wp = L_\wp$ so that $\theta(\Sigma_\wp) \subseteq U_\wp(F_\wp^\times)^2$ for almost all $\wp$. Now choose an idele $i = (i_\wp) \in J_F$ with $i_\wp \in \theta(\Sigma_\wp)$, $^\forall\wp \in \Omega_F$, and set $\Phi(\Sigma) = iP_D J_F^L$. If j is another idele associated to Σ in this manner, then $j \in iJ_F^2$. Since $J_F^2 \subseteq J_F^L \subseteq P_D J_F^L$, Φ is a well-defined group homomorphism. Since $J'_V P_V J_L$ is the kernel of Φ, the first assertion follows.

If $n \geq 3$, then one can show that Φ is surjective, from which follows the second assertion.

.

It is known that $g_L^+ = 2^r$ for some integer $r \geq 0$ and that for any integer $r \geq 0$ one can find a lattice L with $g_L^+ = 2^r$.

Let Ω_∞ denote the set of all infinite prime spots on F and let

$$J_F^\infty = \prod_{\wp<\infty} U_\wp \times \prod_{\wp\in\Omega_\infty} F_\wp^\times .$$

THEOREM6.3. *Assume that* $J_F = P_D J_F^\infty$. *Then*

$$spn^+ L = gen L \;\; if \;\; \theta(O^+(L_\wp)) \supseteq U_\wp(F_\wp^\times)^2, \; ^\forall\wp < \infty.$$

Proof. For all $\wp < \infty$, $J_F^\infty \subseteq J_F^L$ because $\theta(O^+(L_\wp)) \supseteq U_\wp(F_\wp^\times)^2$, $^\forall\wp < \infty$. So $(J_F : P_D J_F^L) \leq (J_F : P_D J_F^\infty) = 1$ and hence $g_L^+ = 1$, i.e., $spn^+ L = gen L (= gen^+ L)$.

THEOREM6.4. *Let* V *be a regular quadratic space over a global field* F *with* $\dim V \geq 3$ *and let* L *be a lattice on* V. *Assume* $V_\wp$ *is isotropic for some* $\wp \in \Omega_\infty$ *(*V *is indefinite). Then*

$$spn^+ L = cls^+ L \text{ and } spn L = cls L.$$

In addition, if $J_F = P_D J_F^\infty$ *and* L *is modular, then*

$$cls^+ L = gen L.$$

Proof. We prove $spnL = clsL$. The proper case can be done similary. Let $K \in spnL$. Then $K_\wp = \sigma\Sigma_\wp L_\wp$ for some $\sigma \in O(V)$ and $\Sigma_\wp \in O'(V_\wp)$, ${}^\forall\wp < \infty$. Since $\sigma^{-1}K \in clsK$, we may assume $\sigma = 1$ so that $K_\wp = \Sigma_\wp L_\wp$, ${}^\forall\wp < \infty$. Fix a basis $x_1, \dots, x_n$ and let M be the lattice $M = \mathcal{O}x_1 + \cdots + \mathcal{O}x_n$. Since $K_\wp = L_\wp = M_\wp$ for almost all $\wp$, the set T of finte prime spots at which $K_\wp = L_\wp = M_\wp$ does not hold is finite. Then one can find (by applying so called the Strong Approximation Theorem for Rotations) $\rho \in O'(V)$ such that $\|\rho\|_\wp = 1$ for all finite $\wp \notin T$ and $\|\rho - \Sigma_\wp\|_\wp$ is arbitrary small at any $\wp \in T$. This implies $(\rho L)_\wp = K_\wp$ for all $\wp < \infty$. Hence $\rho L = K$, or $K \in clsL$. This proves the first assertion.

The second assertion is clear from the first and Theorem 6.3.

THEOREM6.5. *Let V be a regular guadratic space over $\mathbf{Q}$ with $\dim V \geq 3$ such that V_∞ is isotropic (V is indefinite). Let L, K be modular lattices on V such that L, K have the same norm and scale. Then*

$$cls^+L = cls^+K.$$

Proof. From Theorems 4.4 and 4.5 follows that $genL = genK$. On the other hand, one can easily check that $J_{\mathbf{Q}} = P_D J_{\mathbf{Q}}^\infty$. So From the second part of the above theorem follows that

$$cls^+L = genL = genK = cls^+K.$$

DEFINITION6.6. Let K, L be lattices in a regular quadratic space over a global field F. We say that K is represented by $genL$ if $K_\wp \rightarrow L_\wp$, ${}^\forall\wp < \infty$, and write $K \rightarrow genL$. One can define $K \rightarrow gen^+L$ similary, but we know that $K \rightarrow gen^+L$ is just same as $K \rightarrow genL$. We say that K is represented by $spnL$ (or by spn^+L) if $\sigma\Sigma K \subseteq L$ for some $\sigma \in O(V)$ (or $\sigma \in O^+(V)$) and $\Sigma \in J'_V$, and write $K \rightarrow spnL$ (or $K \rightarrow spn^+L$). Finally, We say that K is represented by $clsL$ (or by cls^+L), write $K \rightarrow clsL$ (or $K \rightarrow cls^+L$), if $\sigma K \subseteq L$ for some $\sigma \in O(V)$ (or $\sigma \in O^+(V)$).

We list the following remarkable theorem on a local-global relation of representations of lattices.

THEOREM6.7(HSIA-KITAOKA-KNESER). *Let* $\dim FL \geq \dim FK + 3$. *Then*

$$K \rightarrow genL \text{ if and only if } K \rightarrow spn^{+}L.$$

In particular, if V *is indefinite, then*

$$K \rightarrow genL \text{ if and only if } K \rightarrow cls^{+}L.$$

Proof. See [HKK] for a detailed proof of the first assertion. The second assertion follows immediately from the first asserion and Theorem 6.4.

References

[A] E. Artin, Algebraic Numbers and Algebraic Functions, Princeton University Press, 1951.

[Ca] J.W.S. Cassels, Rational Quadratic Forms, Academic Press, 1978.

[Ch] C. Chevalley, The Algebraic Theory of Spinors, Columbia University Press, 1954.

[D] L.E. Dickson, Studies in the Theory of Numbers, University of Chicago Press, 1930.

[Ea] A. Earnest, Binary Quadratic Forms over Rings of Algebraic Integers : a survey of recent results, Number Theory (J.-M. De Koninck & C. Levesque éd.) (1989), 133-159.

[Ei] M. Eichler, Quadratische Formen und orthogonale Gruppen, Springer-Verlag, 1952.

[H] J.S. Hsia, Arithmetic Theory of Integral Quadratic Forms (a survey), Proceedings of the Queen's Number Theory Conference, Queen's Papers in Pure and Applied Math. 54 (1980), 173-204.

[HKK] J.S. Hsia, Y. Kitaoka, M. Kneser, Representations of Positive Definite Quadratic Forms, Crelle's J. 301 (1978), 132-141.

[J] B.W. Jones, The Arithmetic Theory of Quadratic Forms, Wiley, 1950.

[K] M. Kneser, Quadratische Formen, Göttingen, 1974.

[L] T.Y. Lam, The Algebraic Theory of Quadratic Forms, Benjamin, 1973.

[O] O.T. O'Meara, Intro. to Quadratic Forms, Springer-Verlag, 1973.

[P] A. Pfister, Some Remarks on Historical Development of the Algebraic Theory of Quadratic Forms, CMS Conference Proceeding v. 4 (1984), 1-16.

[S] W. Scharlau, Quadratic and Hermitian Forms, Springer-Verlag, 1985.

[Wa] G.L. Watson, Integral Quadratic Forms, Cambridge University Press, 1960.

[We] A. Weil, Adeles and Algebraic Groups, Birkhaäuser, 1982.

[Wi] E. Witt, Theorie der quad. Formen in beliebigen Körpern, Crelle's J. 176 (1937), 31-44.

Department of Mathematics
Seoul National University
Seoul 151-742, Korea

EXPLICIT FORMS OF THE NORM RESIDUE SYMBOL

DAE SAN KIM

Department of Mathematics
Seoul Women's University
Seoul 139-240, Korea

DEFINITION. (k,ν) is a local field if it is complete w.r.t. the normalized discrete valuation ν and its residue class field is finite. (k any field, $\nu : k \to \mathbf{Z} \cup \{\infty\}$ is a normalized discrete valuation if

i) $\nu(k^x) = \mathbf{Z}$, $\nu(0) = \infty$
ii) ${}^{\forall}x, y \in k, \nu(x+y) \geq \min(\nu(x), \nu(y))$
iii) $\nu(x) + \nu(y) = \nu(xy))$

KNOWN. Local fields fall into two types :

(a) In characteristic 0, they are finite extensions of $\mathbf{Q}_p$.
(b) In char $p > 0$, they are the Laurent series fields in one variable with coefficients in a finite field i.e., $(\mathbf{F}_q((T)), \nu_T)$

NOTATION. $\mathcal{O} = \{x \in k \,|\, \nu(x) \geq 0\}$ the valuation ring, $p = \{x \in k \,|\, \nu(x) > 0\}$ the maximal ideal, $t = \mathcal{O}/p$ the residue class field $\cong \mathbf{F}_q$. Fix $\pi \in k$ s.t. $\nu(\pi) = 1$, called a prime element of k. Then $p^n = \mathcal{O}\pi^n = \{x \in k \,|\, \nu(x) \geq n\}$'s are the ideals of k ($n = 0, \pm 1, \pm 2, \cdots$), $U = \{x \in k \,|\, \nu(x) = 0\}$ the unit group.

FACTS. a) (k,ν) local field. Then k is a non-discrete, totally disconnected, locally compact field.

$$\mathcal{O} = p^0 \supset p \supset p^2 \supset \cdots \supset p^n \supset \cdots$$

open compact subgroups of k and form a neighborhood base of 0.

b) k^X a non-discrete, totally disconnected, locally compact group (with the induced topology).

$$U = U^0 \supset U^1 = 1 + p \supset U^2 = 1 + p^2 \supset \cdots \supset U^n = 1 + p^n \supset \cdots$$

open compact subgroups and form a neighborhood base of 1.

(k,ν) p-field with residue field $t = \mathcal{O}/p = \mathbf{F}_q$

$$\text{structure of } k^X : k^X = \pi^{\mathbf{Z}} \times U$$

KNOWN. $k^X \supseteq V =$ the set of all $(q-1)$-st roots of $1 =$ the set of all roots of 1, prime to p, and the canonical map $\mathcal{O} \to \mathcal{O}/p$ induces

$$V \xrightarrow{\sim} (\mathcal{O}/p)^X.$$

$V \cup \{0\}$ is a complete set of representatives for $\mathcal{O}/p$.

$$k^{\times} = \pi^{\mathbf{Z}} \times V \times U_1.$$

One can put $\mathbf{Z}_p$-module structure on any abelian pro-p-group $G = \varprojlim G_i$, G_i finite abelian p-groups. In particular, $U_1 = \varprojlim U_1/U_n$ is a $\mathbf{Z}_p$-module.

a) $\operatorname{char} k = 0 : U_1 \cong W \oplus \mathbf{Z}_p^d$, $d = [k : \mathbf{Q}_p]$, $W =$ the set of all p-power roots of 1 in k, which is a finite cyclic group of U_1.

b) $\operatorname{char} k = p : U_1 \cong$ the direct product of countably infinite copies of $\mathbf{Z}_p$.

$(k', \nu')/(k, \nu)$ finite extension of local fields. Then $\nu' \,|\, k = e\nu$ for some positive integer e, called the ramification index and denoted by $e = e(k'/k)$. Also, $f = f(k'/k) = [t' : t]$ i.e., if $t = \mathbf{F}_q$ then $t' = \mathbf{F}_{q^f}$. Can show :

$$\xi_i \pi'^j (i = 1, \cdots, f, \; j = 0, \cdots, e-1)$$

forms a basis for the free $\mathcal{O}$-module $\mathcal{O}'$ where ξ_i are elements of $\mathcal{O}'$ whose residues are a basis for t' over t. This implies $[k' : k] = ef$.

Definition. k'/k unramified if $e = 1$, $f = n$, and k'/k totally ramified if $e = n$, $f = 1$.

Facts. $\nu(\pi) = \nu'(\pi') = 1$.

$$k'/k \text{ unramified } \Leftrightarrow \pi \text{ is a prime element of } k',$$

$$k'/k \text{ totally ramified } \Leftrightarrow N_{k'/k}(\pi') \text{ is a prime element of } k.$$

$k \subseteq k' \subseteq k''$ finite extension of local fields. $e(k''/k) = e(k'/k)e(k''/k')$, $f(k''/k) = f(k'/k)f(k''/k') \Rightarrow k''/k$ unramified (totally ramified) $\Leftrightarrow$ both k''/k' and k'/k are unramified (totally ramified).

Proposition. *(k, ν) local field with $t = \mathbf{F}_q$. $^\forall$ integer $n \geq 1$, $\exists$ an unramified extension k'/k of degree n (unique up to an isomorphism over k). k' is a splitting field of $X^{q^n} - X$ over k and cyclic extension of degree n. In fact,*

$$Gal(k'/k) \xrightarrow{\sim} Gal(t'/t).$$

DEFINITION.

$$Gal(k'/k) \to Gal(t'/t)(\varphi \mapsto (\omega \mapsto \omega^q))$$

is called the Frobenius automorphism of the unramified extension k'/k, and characterized by

$$\varphi(y) \equiv y^q \bmod p', \ ^{\forall}y \in \mathcal{O}'.$$

k'/k finite extension of local fields with $[k' : k] = ef$

Let k_0 be the splitting field of $X^{q^f} - X$ over k, in k'. Then it is the maximal unramified extension in k', called the inertia field of k'/k.

GENERAL PICTURE.
(k, ν) : local field with $t = \mathbf{F}_q$
Ω : a fixed algebraic closure of k
μ : the unique extension of ν to Ω
$(\bar{\Omega}, \bar{\mu})$: the completion of (Ω, μ)
F : algebraic extension of k in Ω
$\mu_F : \mu \,|\, F$
$\bar{F}$: the closure of F in $\bar{\Omega}$
$\mu_{\bar{F}} : \bar{\mu} \,|\, \bar{F}$

DEFINITION. F algebraic extension of k in Ω i.e., $k \subseteq F \subseteq \Omega$. F/k unramified if

$$e(k'/k) = 1 \text{ for all } k \subseteq k' \subseteq F \text{ with } [k' : k] < \infty.$$

F/k totally ramified if

$$f(k'/k) = 1 \text{ for all } k \subseteq k' \subseteq F \text{ with } [k' : k] < \infty.$$

KNOWN. $^{\forall}$ integer n, $\exists$ a unique unramified extension k_{ur}^n of degree n in Ω i.e.,

$$k_{ur}^n = k(V_n), \ V_n = \text{ the group of } (q^n - 1) - \text{th roots of 1 in } \Omega.$$

Note : $k_{ur}^n \subseteq k_{ur}^m \Leftrightarrow n \,|\, m$. Put

$$K = \cup_{n \geq 1} k_{ur}^n = k_{ur},$$

the unique maximal unramified extension of k in Ω. For $n\,|\,m$,

$$\begin{tikzcd}
\mathbf{Z}/m\mathbf{Z} \arrow[r, "\sim"] \arrow[d] & Gal(k_{ur}^m/k) \arrow[r, "\sim"] \arrow[d] & Gal(t^m/t) \arrow[d] \\
\mathbf{Z}/n\mathbf{Z} \arrow[r, "\sim"] & Gal(k_{ur}^n/k) \arrow[r, "\sim"] & Gal(t^n/t)
\end{tikzcd}$$

is commutative, where the first isomorphism of the bottom row is given by (a mod n) $\mapsto \varphi_n^a$.

$$\hat{\mathbf{Z}} = \varprojlim \mathbf{Z}/n\mathbf{Z} = \Pi_p \mathbf{Z}_p \cong Gal(k_{ur}/k)$$
$$\cong Gal(t_K/t)$$

Again, the unique $\varphi_k \in$ Gal(k_{ur}/k) satisfying

$$\varphi_k(\alpha) \equiv \alpha^q\, mod\, p_k \ (\alpha \in \mathcal{O}_K)$$

is called the Frobenius automorphism of k (or k_{ur}/k). Note that φ_k is a topological generator of Gal(k_{ur}/k). Also, note that

$$F/k \text{ is totally ramified } \Leftrightarrow F \cap k_{ur} = k.$$

General Reference of the sequel:

Lubin and Tate, "Formal complex multiplication in local fields", Ann. Math., 81(1965).

Serre, "Local class field theory" in Algebraic # theory (edited by Cassels and Frölich), Academic Press (1976).

Basic facts about Formal Power Series :

R commutative ring with 1. ${}^\forall f, g \in R[[X_1, \cdots, X_n]]$, write

$$f \equiv g \ (\text{mod deg } d)$$

if $f - g$ contains only terms with total degree $\geq d$. Let $f \in R[[X_1, \cdots, X_n]]$, $g_1, \cdots g_n \in R[[Y_1, \cdots, Y_m]]$ with $g_j \equiv 0$ (mod deg 1). Then $f \circ (g_1, \cdots, g_n)$ is well defined.

Assume further that R is a topological ring. Put the topology on $R[[X_1, \cdots, X_n]]$ so that

$$\sum a_{i_1 \cdots i_n} X_1^{i_1} \cdots X_n^{i_n} \mapsto \{a_{i_1 \cdots i_n}\}_{i_1, \cdots, i_n \geq 0}$$

is a homeomorphism. $f \in \mathcal{O}_{\bar{\Omega}}[[X_1, \cdots, X_n]]$, $g_1, \cdots, g_n \in \mathcal{O}_{\bar{\Omega}}[[Y_1, \cdots, Y_m]]$ with constant terms in $p_{\bar{\Omega}}$. Then $f \circ (g_1, \cdots, g_n)$ converges in the above topology. In particular, for $\alpha_1, \cdots, \alpha_n \in p_{\bar{\Omega}}$, $f(\alpha_1, \cdots, \alpha_n)$ is well defined in $\mathcal{O}_{\bar{\Omega}}$.

MAIN LEMMA. $\mu_{\bar{K}}(\pi_1) = \mu_{\bar{K}}(\pi_2) = 1$, $f_1, f_2 \in \mathcal{O}_{\bar{K}}[[X]]$ are *s.t.*

$$f_1(X) \equiv \pi_1 X,\ f_2(X) \equiv \pi_2 X\ (deg 2),$$

$$f_1(X) \equiv f_2(X) \equiv X^q (mod p_{\bar{K}}),$$

$$L(X_1, \cdots, X_m) = \alpha_1 X_1 + \cdots + \alpha_m X_m,\ \alpha_j \in \mathcal{O}_{\bar{K}}$$

is s.t.

$$\pi_1 L(X_1, \cdots, X_m) = \pi_2 L^{\varphi}(X_1, \cdots, X_m).$$

Then $\exists$ *! power series* $F = F(X_1, \cdots, X_m) \in \mathcal{O}_{\bar{K}}[[X_1, \cdots, X_m]]$ s.t.

$$F \equiv L\ (deg 2),\ f_1 \circ F = F^{\varphi} \circ f_2.$$

Proof. $^{\forall}n \geq 1$, Construct F_n of total degree $\leq n$ in $\mathcal{O}_{\bar{K}}[X_1, \cdots, X_m]$ s.t.

$$f_1 \circ F_n \equiv F_n^{\varphi} \circ f_2\ (deg\ (n+1)) \text{ and}$$

$$F_{n+1} \equiv F_n\ (deg\ (n+1)).$$

For $n = 1$, let $F_1 = L$. Then $\lim_{n\to\infty} F_n = F$ is the desired one.

R any commutative ring with 1.

DEFINITION. $F(X,Y) \in R[[X,Y]]$ is a formal group law over R (1-dimensional commutative) if

i) $F(X,Y) = X + Y (\text{deg } 2)$
ii) $F(F(X,Y),Z) = F(X, F(Y,Z))$
iii) $F(X,Y) = F(Y,X)$
iv) $F(X,0) = X$ and $F(0,Y) = Y$
v) $\exists !\ i_F(X) \in M = XR[[X]]$ such that $F(X, i_F(X)) = 0$

(iv) and v) are consequences of i), ii) and iii))

(Good Reference : Hazewinkel, "Formal Groups and Applications", Academic press (1978))

EXAMPLE. $G_a(X,Y) = X + Y$, $G_m(X,Y) = X + Y + XY$

DEFINITION. F, G formal group laws over R. $f(X) \in M$ is a morphism from F to G (and denoted by $f : F \to G$) if $f \circ F = G \circ f$. Further, if f is invertible in M, i.e.,

$$f \circ f^{-1} = f^{-1} \circ f = X$$

then $f^{-1} : G \to F$ and we say $f : F \xrightarrow{\sim} G$ an isomorphism i.e.,

$$F^f = f \circ F \circ f^{-1} = G.$$

FACTS. $\mathrm{Hom}_R(F, G)$ is a subgroup of the abelian group M_G where $M_G = M$ with the addition

$$f \dot{+}_G g = G \circ (f, g) = G(f(X), g(X)).$$

Moreover, $\mathrm{End}_R(F)$ is a ring with the addition $f \dot{+}_F g$ and the multiplication $f \circ g$.

CONVENTION. For simplicity, both the unique extension of φ_k to $\bar{K} = \bar{k}_{ur}$ and φ_k will be denoted by φ. Put $R = \mathcal{O}_{\bar{K}}$. For each prime element π of $\bar{K}$,

$$\mathcal{F}_\pi = \{f \in R[[X]] \mid f(X) \equiv \pi X(\deg 2), f(X) \equiv X^q(p_{\bar{K}})\}.$$

Put $\mathcal{F} = \bigcup\limits_{\substack{\pi \\ \mu_{\bar{K}}(\pi)=1}} \mathcal{F}_\pi.$

PROPOSITION. (a) $^\forall f \in \mathcal{F}_\pi$, $\exists!$ *formal group law* $F_f(X, Y)$ *over* R *such that*

$$f \circ F_f = F_f^\varphi \circ f$$

(b) *Let* $f \in \mathcal{F}_\pi$. $^\forall a \in \mathcal{O} = \mathcal{O}_k$, $\exists!$ $[a]_f(X) \in R[[X]]$ *such that*

$$[a]_f \equiv aX(\deg 2), \;\; f \circ [a]_f = [a]_f^\varphi \circ f.$$

(c) $a \mapsto [a]_f$ *defines an injective ring homomorphism of*

$$\mathcal{O} \to \mathrm{End}_R(F_f).$$

(d) *Let $f \in \mathcal{F}_\pi$, $f' \in \mathcal{F}_{\pi'}$. Then $\exists\theta$ invertible in $M = XR[[X]]$ such that*

$$f' \circ \theta = \theta^\varphi \circ f,\ F_f^\theta = F_{f'},\ [a]_f^\theta = [a]_{f'}\ (^\forall a \in \mathcal{O}_k).$$

Proof. (a) Apply the main lemma with $\pi_1 = \pi_2 = \pi$, $f_1 = f_2 = f$, $L(X,Y) = X + Y$.

(b) Apply the main lemma with $\pi_1 = \pi_2 = \pi$, $f_1 = f_2 = f$, $L(X) = aX$.

(d) Need the facts :

$$0 \to \mathcal{O}_k \to \mathcal{O}_{\bar{K}} \xrightarrow{\varphi-1} \mathcal{O}_{\bar{K}} \to 0,$$

$$1 \to U(k) \to U(\bar{K}) \xrightarrow{\varphi-1} U(\bar{K}) \to 1$$

are exact.

Suppose $\pi' = \pi\xi$, $\xi \in U(\bar{K})$. Find $\eta \in U(\bar{K})$ such that $\eta^{\varphi-1} = \xi$. Then

$$\pi' L(X) = \pi L^\varphi(X) \text{ for } L(X) = \eta X.$$

Apply the main lemma with $f_1 = f', f_2 = f$, $\pi_1 = \pi'$, $\pi_2 = \pi$, $L(X) = \eta X$. $\exists!\ \theta(X) \in R[[X]]$ such that

$$\theta(X) \equiv \eta X(\deg 2) \text{ and } f' \circ \theta = \theta^\varphi \circ f.$$

Let $m = p_{\bar{\Omega}}$ be the maximal ideal of $\bar{\Omega}$. Let $f \in \mathcal{F}$. Then m_f is the set m with the addition $\alpha \dot{+}_f \beta = F_f(\alpha,\beta)$, scalar multiplication $a \cdot_f \alpha = [a]_f(\alpha)(\alpha,\beta \in m, a \in \mathcal{O} = \mathcal{O}_k)$ i.e., m_f is an $\mathcal{O}$-module. For integer $n \geq -1$, put

$$\begin{aligned} W_f^n &= \{\alpha \in m_f \,|\, p^{n+1} \cdot_f \alpha = 0\} \\ &= \{\alpha \in m_f \,|\, \pi^{n+1} \cdot_f \alpha = 0\}. \end{aligned}$$

We have a chain of $\mathcal{O}$-submodules of m_f :

$$(0) = W_f^{-1} \subseteq W_f^0 \subset W_f^1 \subseteq \cdots \subseteq W_f^n \subseteq \cdots \subseteq W_f = \bigcup_{n=\geq -1} W_f^n.$$

NOTE. f' another one in $\mathcal{F}$. Then $\exists\ \theta \in XR[[X]]$ invertible such that

$$F_f^\theta = F_{f'},\ [a]_f^\theta = [a]_{f'}.$$

Thus

$$m_f \to m_{f'}(\alpha \mapsto \theta(\alpha))$$

is an isomorphism of $\mathcal{O}$-modules. Also, it induces $\mathcal{O}$-isomorphisms

$$W_f^n \xrightarrow{\sim} W_{f'}^n,\ W_f \xrightarrow{\sim} W_{f'}.$$

PROPOSITION. *a) For $f \in \mathcal{F}$ and $i \geq 0$, let*

$$f_i = f^{\varphi^i},\ g_i = f_i \circ f_{i-1} \circ \cdots \circ f_0,\ g_{-1}(X) = X.$$

Then $W_f^n = \{\alpha \in m \mid g_n(\alpha) = 0\}$, $n \geq -1$.

b) Fix $m \geq 1$, $k \subseteq k' = k_{ur}^m \subseteq \Omega$, π a prime element of k'. Then actually

$$F_f(X,Y) \in \mathcal{O}'[[X,Y]],\ [a]_f(X) \in \mathcal{O}'[[X]] \text{ for } a \in \mathcal{O}.$$

$$\begin{aligned} g_n &= f_n \circ g_{n-1} = f^{\varphi^n} \circ g_{n-1} = \pi^{\varphi^n} g_{n-1} + g_{n-1}^q \\ &= (\pi^{\varphi^n} + g_{n-1}^{q-1})g_{n-1} = h_n g_{n-1} = h_n(X)h_{n-1}(X)\cdots h_0(X)X, \end{aligned}$$

where $f(X) = \pi X + X^q \in \mathcal{O}'[X]$ belongs to $\mathcal{F}$.

b$_1$) *h_n monic separable polynomial of* deg$(q-1)q^n$*, irreducible in $\bar{K}[X]$.*

b$_2$) *g_n monic separable polynomial of* deg q^{n+1} *in $\mathcal{O}'[X]$, $W_f^n = \{\alpha \in \Omega \mid g_n(\alpha) = 0\}$. So $|W_f^n| = q^{n+1}$ and $k'(W_f^n)/k'$ finite Galois extension.*

b$_3$) *Let $\alpha_0 \in \Omega$ be such that $h_n(\alpha_0) = 0$. Then $\alpha_0 \in W_f^n$, $\alpha_0 \notin W_f^{n-1}$, $(q-1)q^n = [k'(\alpha_0) : k'] = [k'(W_f^n) : k']$, $\pi^{\varphi^n} = N(-\alpha_0) = N_{k'(\alpha_0)/k'}(-\alpha_0)$.*

c) Let $f \in \mathcal{F}$.

c$_1$) $[W_f^n : 0] = q^{n+1}$, $n \geq -1$.

c$_2$) *Fix* $\alpha_0 \in W_f^n$, $\alpha_0 \notin W_f^{n-1}$, $n \geq 0$. *Then* $W_f^n = \mathcal{O} \cdot_f \alpha_0$ *and* $a \mapsto a \cdot_f \alpha_0$ *induces the isomorphism*

$$\mathcal{O}/p^{n+1} \xrightarrow{\sim} W_f^n.$$

c$_3$) $p^i \cdot_f W_f^n = W_f^{n-i}$ *for* $0 \leq i \leq n$.

d) $\mathcal{O} \to End(W_f^n)$ $(a \mapsto (\beta \mapsto a \cdot_f \beta))$ *induces*

$$\mathcal{O}/p^{n+1} \xrightarrow{\sim} End(W_f^n)$$

and

$$U/U_{n+1} \xrightarrow{\sim} Aut(W_f^n).$$

Proof. c),d) follow from a),b).

a) For $n = -1$, clear. If f' and $\mathcal{O}$ are as before, then

$$f' \circ \theta = \theta^{\varphi} \circ f \Rightarrow f_i' \circ \theta^{\varphi^i} = \theta^{\varphi^{i+1}} \circ f_i$$

i.e., $f_i' = \theta^{\varphi^{i+1}} \circ f_i \circ \theta^{-\varphi^i}$ and hence

$$g_n' = f_n' \circ f_{n-1}' \circ \cdots \circ f_0' = \theta^{\varphi^{n+1}} \circ g_n \circ \theta^{-1}.$$

Reduce to the case of $f(X) = \pi X + X^q$, π a prime element of k $(f \in \mathcal{F})$. Since $f \equiv \pi X(\deg 2)$ and $f \circ f = f^{\varphi} \circ f$,

$$f = [\pi]_f,\ f_i = f,\ g_n = f \circ f \circ \cdots \circ f = [\pi^{n+1}]_f.$$

Thus $W_f^n = \{\alpha \in m_f \mid \pi^{n+1} \cdot_f \alpha = 0\} = \{\alpha \in m \mid g_n(\alpha) = 0\}$.

b) See that

$$g_n(X) = a_n X + \cdots + X^{q^{n+1}} \equiv X^{q^{n+1}} (p'),\ a_n = \pi^{1+\varphi+\cdots+\varphi^n},$$
$$h_n(X) = \pi^{\varphi^n} + (a_{n-1}X + \cdots + X^{q^n})^{q-1} \equiv X^{(q-1)q^n}\ (p').$$

Note that h_n is a Eisenstein polynomial and hence irreducible in $\bar{K}[X]$. $dh_n/dX = (q-1)a_{n-1}^{q-1}X^{q-2} + \cdots \neq 0$. So $h_n(X)$ is separable.

EXAMPLE. $k = \mathbf{Q}_p$, $\pi = p$. Then $f(X) = (1+X)^p - 1 = pX + \binom{p}{2}X^2 + \cdots + X^p \in \mathcal{F}_p$. $F(X,Y) = (1+X)(1+Y) - 1$ is a formal group law over $R = \mathcal{O}_{\bar{K}}$ such that $f \circ F = F^{\varphi} \circ f$ i.e., $F = F_f$. For $a \in \mathbf{Z}_p$, define

$$(1+X)^a = \sum_{n=0}^{\infty} \binom{a}{n} X^n, \quad \binom{a}{n} = \frac{a(a-1)\cdots(a-n+1)}{n!} \in \mathbf{Z}_p.$$

By definition, for $a \in \mathbf{Z}_p$ $[a]_f(X) \in R[[X]]$ is the unique one satisfying $[a]_f \equiv aX(\deg 2)$, $f \circ [a]_f = [a]_f^{\varphi} \circ f$.

CHECK. $[a]_f = (1+X)^a - 1 = \sum_{n=1}^{\infty} \binom{a}{n} X^n$, $a \in \mathbf{Z}_p$.

Now,

$$\begin{aligned} W_f^n &= \{\alpha \in p_{\bar{\Omega}} \mid [p^{n+1}]_f(\alpha) = 0\} \\ &= \{\alpha \in p_{\bar{\Omega}} \mid (1+\alpha)^{p^{n+1}} = 1\} \\ &= \{\zeta - 1 \mid \zeta \in \Omega,\ \zeta^{p^{n+1}} = 1\} \end{aligned}$$

and $\mathbf{Q}_p(W_f^n)$ is the cyclotomic field of p^{n+1}-th roots of 1, which is a totally ramified abelian extension, with

$$\mathrm{Gal}(\mathbf{Q}_p(W_f^n)/\mathbf{Q}_p) \xrightarrow{\sim} \mathrm{Aut}(W_f^m) \xrightarrow{\sim} \mathbf{Z}_p^X/(1+p^{n+1}\mathbf{Z}_p).$$

REMARK. $k' = k_{ur}^n \subseteq \Omega$, $\mathcal{O}' =$ the valuation ring of k'. π_1, π_2 prime elements of k', $f_1, f_2 \in \mathcal{O}'[[X]]$, and $L \in \mathcal{O}'[X_1, \cdots, X_m]$. Then one can show that actually $F(X_1, \cdots, X_m) \in \mathcal{O}'[[X_1, \cdots, X_m]]$ in the main lemma.

SOME EXTENSIONS. $f \in \mathcal{F}$, $W_f^n \subseteq m_f = m \subseteq \bar{\Omega}$. See that $\bar{K}(W_f^n)$ is a finite Galois extension over $\bar{K}$ and it does not depend on the choice of $f \in \mathcal{F}$. Put $\bar{L}^n = \bar{K}(W_f^n)$, for every $f \in \mathcal{F}$, $n \geq -1$. So we have a sequence in $\bar{\Omega}$:

$$\bar{K} = \bar{L}^{-1} \subseteq \bar{L}^0 \subseteq \cdots \subseteq \bar{L}^n \subseteq \cdots \subseteq \bar{L} \subseteq \bar{\Omega},$$
$$\bar{L} = \text{ the union of all } \bar{L}^n,\ n \geq -1 = \bar{K}(W_f), \text{ for any } f \in \mathcal{F}.$$

PROPOSITION. *For $n \geq 0$, $\exists$ a natural homomorphism*

$$\delta^n : U = U(k) \to Gal(\bar{L}^n/\bar{K})$$

such that for $u \in U$, every $f \in \mathcal{F}$, $\alpha \in W_f^n$,

$$\delta^n(u)(\alpha) = u \cdot_f \alpha = [u]_f(\alpha),$$

and induces an isomorphism

$$U/U_{n+1} \xrightarrow{\sim} Gal(\bar{L}^n/\bar{K}).$$

(In particular, $\bar{L}^n/\bar{K}$ is an abelian extension of degree $[\bar{L}^n : \bar{K}] = (q-1)q^n$)

Also, $\bar{L}/\bar{K}$ is an abelian extension and $\exists$ a topological isomorphism

$\delta : U \to Gal(\bar{L}/\bar{K})$ by passing to inverse limits.

RELATIVE LUBIN-TATE GROUPS. For integer $m \geq 1$, $\mathcal{O}^m =$ the valuation ring of k_{ur}^m, π a prime element of k_{ur}^m, $\mathcal{F}_\pi \subseteq R[[X]]$, $R = \mathcal{O}_{\bar{K}}$, as before. Put

$$\begin{aligned}
\mathcal{F}_\pi^m &= \mathcal{F}_\pi \cap \mathcal{O}^m[[X]], \\
\mathcal{F}^m &= \text{ the union of } \mathcal{F}_\pi^m \text{ for all prime elements } \pi \text{ of } k_{ur}^m, \\
\mathcal{F}^\infty &= \text{ the union of } \mathcal{F}^m \text{ for all integers } m \geq 1.
\end{aligned}$$

See that $k_{ur}^m(W_f^n)$ depends only on m, n, π, and is independent of $f \in \mathcal{F}_\pi^m$.

Also, $K(W_f^n)$ depends only n, and is independent of $f \in \mathcal{F}^\infty$.

Put

$$\begin{aligned}
k_\pi^{m,n} &= k_{ur}^m(W_f^n), \text{ for any } f \in \mathcal{F}_\pi^m, \\
L^n &= K(W_f^n), \text{ for any } f \in \mathcal{F}^\infty.
\end{aligned}$$

PROPOSITION. *a)* $\bar{L}^n$ *is the closure of* L^n *in* $\bar{\Omega}$,

$$\bar{L}^n = \bar{K}L^n,\ K = \bar{K} \cap L^n,\ Gal(\bar{L}^n/\bar{K}) \xrightarrow{\sim} Gal(L^n/K).$$

b) $L^n = Kk_\pi^{m,n},\ k_{ur}^m = K \cap k_\pi^{m,n}$, *and*

$$\begin{aligned} Gal(L^n/k_{ur}^m) &= Gal(L^n/k_\pi^{m,n}) \times Gal(L^n/K) \\ &\xrightarrow{\sim} Gal(K/k_{ur}^m) \times Gal(k_\pi^{m,n}/k_{ur}^m). \end{aligned}$$

c) $L^n/k, L^n/K, k_\pi^{m,n}/k, k_\pi^{m,n}/k_{ur}^m$ *abelian extensions and*

$$[L^n : K] = [k_\pi^{m,n} : k_{ur}^m] = (q-1)q^n, [k_\pi^{m,n} : k] = m(q-1)q^n.$$

PROPOSITION. *For* $n \geq 0$, $\exists$ *a homomorphism*

$$\delta^n : U = U(k) \to Gal(L^n/K)$$

such that $^\forall f \in \mathcal{F}^\infty$, $u \in U$, $\alpha \in W_f^n$, $\delta^n(u)\alpha = u \cdot_f \alpha$, *and induces an isomorphism*

$$U/U_{n+1} \xrightarrow{\sim} Gal(L^n/K).$$

Moreover, similarly we have

$$\delta_\pi^n : U = U(k) \to Gal(k_\pi^{m,n}/k_{ur}^m)$$

for π *a prime element of* k_{ur}^m *inducing the isomorphism*

$$U/U_{n+1} \xrightarrow{\sim} Gal(k_\pi^{m,n}/k_{ur}^m)$$

and this isomorphism induces

$$U_{i+1}/U_{n+1} \xrightarrow{\sim} \delta_\pi^n(U_{i+1}) = Gal(k_\pi^{m,n}/k_\pi^{m,i}),\ \text{for } 0 \leq i \leq n.$$

PROPOSITION. *π a prime element of k^m_{ur}.*

a) *$k^{m,n}_\pi / k^m_{ur}$ totally ramified finite abelian extension and $\pi \in N(k^{m,n}_\pi / k^m_{ur})$.*

b) *$f \in \mathcal{F}^m_\pi$, $\alpha \in W^n_f$, $\alpha \notin W^{n-1}_f$. Then α is a prime element of $k^{m,n}_\pi$, and $k^{m,n}_\pi = k^m_{ur}(\alpha)$, $\mathcal{O}^{m,n} = \mathcal{O}^m[\alpha]$.*

c) *The complete set of conjugates of α over $k^m_{ur} = W^n_f \backslash W^{n-1}_f$.*

d) *For $0 \leq i \leq n$, the complete set of conjugates of α over $k^{m,i}_\pi = \alpha \dot{+}_f W^{n-i-1}_f$.*

Again, π is a prime element of k^m_{ur}.

$$k^m_{ur} = k^{m,-1}_\pi \subseteq k^{m,0}_\pi \subseteq \cdots \subseteq k^{m,n}_{ur} \subseteq \cdots \subseteq k^{m,\infty}_\pi \subseteq \Omega,$$
$$k_{ur} = K = L^{-1} \subseteq L^0 \subseteq \cdots \subseteq L^n \subseteq \cdots \subseteq L \subseteq \Omega.$$

See

$$k^{m,\infty}_\pi = k^m_{ur}(W_f), \text{ for any } f \in \mathcal{F}^m_\pi,$$
$$L = k_{ur}(W_f), \text{ for any } f \in \mathcal{F}^\infty.$$

PROPOSITION. *L/k abelian extension and $L = k_{ur} k^{m,\infty}_\pi$, $k^m_{ur} = k_{ur} \cap k^{m,\infty}_\pi$. $k^{m,\infty}_\pi$ is a maximal totally ramified extension of k^m_{ur} in L, and*

$$\begin{aligned} Gal(L/k^m_{ur}) &= Gal(L/k^{m,\infty}_\pi) \times Gal(L/k_{ur}) \\ &\xrightarrow{\sim} Gal(k_{ur}/k^m_{ur}) \times Gal(k^{m,\infty}_\pi / k^m_{ur}). \end{aligned}$$

Also, $\exists$ topological isomorphisms

$$\delta : U \xrightarrow{\sim} Gal(L/k_{ur}),$$
$$\delta_\pi : U \xrightarrow{\sim} Gal(k^{m,\infty}_\pi / k^m_{ur}).$$

For simplicity, we put $k^{1,n}_\pi \equiv k^n_\pi$, $n \geq -1$.

Also, for $m = 1$ and $\pi \in k = k^1_{ur}$, put $k_\pi \equiv k^{1,\infty}_\pi$. By the above proposition, $L = k_{ur} k_\pi$, $k = k_{ur} \cap k_\pi$, k_π totally ramified, maximal extension of k in L, and

$$\begin{aligned} Gal(L/k) &= Gal(L/k_\pi) \times Gal(L/k_{ur}) \\ &\xrightarrow{\sim} Gal(k_{ur}/k) \times Gal(k_\pi/k), \end{aligned}$$

$$\delta_\pi : U \xrightarrow{\sim} Gal(k_\pi/k).$$

One can show that $L = k_{ab}$ and hence

$$\mathrm{Gal}(L/k) \cong \hat{\mathbf{Z}} \times U(k).$$

PROPOSITION. *For any prime element π of k,*

$$N(k_\pi^n/k) = \langle\pi\rangle \times U_{n+1},\ n \geq -1.$$

COROLLARY. *Let π be as in the above. Then $N(k_\pi/k) = \langle\pi\rangle$, More generally, if F is totally ramified extension of k in Ω containing k_π then $N(F/k) = \langle\pi\rangle$.*

REMARK. For these, we need Coleman's Norm Operators.

Coleman's Norm Operator :
$\pi \in k = k_{ur}^1$, $k_\pi^n = k_\pi^{1,n}$, $S = \mathcal{O}[[X]]$, $S^X = \{g(X) \in S \,|\, g(0) \in U\}$, $\mathcal{F}_\pi^1 = \mathcal{F}_\pi \cap S \ni f$. Note : $[\pi]_f = f$.

LEMMA. *$h(X)$ a monic polynomial in $\mathcal{O}[X]$ such that*

$$h(X) = \Pi_{i=1}^m (X - \alpha_i),\ \alpha_i \text{ distinct in } P_\Omega.$$

If $f(X)$ is a power series in $\mathcal{O}[[X]]$ such that $f(\alpha_i) = 0$, $^\forall i = 1, \cdots, m$ then $f(X) = h(X)g(X)$ for some $g \in \mathcal{O}[[X]]$.

LEMMA. *$g \in S$ such that $g(W_f^0) = 0$. Then $g(X) = [\pi]_f h(X)$ for some $h(X) \in S$.*

Proof. Reduce to $f(X) = \pi X + X^q = [\pi]_f$ and apply the above lemma and the fact that $W_f^0 =$ the set of all roots, in Ω, of a separable polynomial f.

From now on, we fix $f \in \mathcal{F}_\pi' = \mathcal{F}_\pi \cap S$ and omit the subscript f in everything. $\mathcal{O}_n =$ the valuation ring of $k_\pi^n = k(W^n)$, p_n its maximal ideal, $t_n = \mathcal{O}_n/p_n$. For $\alpha \in W^n$, note that $F_f(X, \alpha) = X \dot{+} \alpha$ is a well-defined series in $\mathcal{O}_n[[X]]$, since $\alpha \in p_n \subseteq m \cap k_\pi^n$.
For $g \in S$, $g(X \dot{+} \alpha)$ is also well-defined, since $X \dot{+} \alpha \equiv \alpha$ (deg 1).

LEMMA. *$g \in S$ satisfies $g(X \dot{+} \gamma) = g(X)$, $^{\forall}\gamma \in W^0$. Then $\exists\, h \in S$ such that $g = h \circ [\pi]$.*

Actually, such an h is unique in view of :

LEMMA. *Let $g = h \circ [\pi]$ for $g, h \in S$.*

$$^{\forall}n \geq 0,\ g \equiv 0 \ mod\ p^n \Leftrightarrow h \equiv 0 \ mod\ p^n.$$

Thus $g = 0 \Leftrightarrow h = 0$.

Let $h \in S$. Put

$$h_1(X) = \Pi_{\gamma \in W^0} h(X \dot{+} \gamma) \in \mathcal{O}_0[[X]].$$

Since all $\gamma \in W^0$, $\gamma \neq 0$ are conjugate over k,

$$h_1^\sigma = h_1,\ \sigma \in \mathrm{Gal}(k_\pi^0/k)$$
$$\text{and hence } h_1(X) \in S.$$

From the associativity of the formal group law,

$$h_1(X \dot{+} \gamma) = h_1(X),\ ^{\forall}\gamma \in W^0.$$

Thus by the above lemmas $\exists!\, N(h) = N_f(h)$ such that

$$N(h) \circ [\pi] = \Pi_\gamma h(X \dot{+} \gamma).$$

The map $N = N_f : S \to S$ is called the Coleman's norm operator.

Properties of N :

a) $N(h_1 h_2) = N(h_1)N(h_2)$, $^{\forall}h_1, h_2 \in S$.

b) $N(h) \equiv h \mod p$.

c) $h \in X^i S^X$ for $i \geq 0 \Rightarrow N(h) \in X^i S^X$.

d) $h \equiv 1 \mod p^i$, $i \geq 1 \Rightarrow N(h) \equiv 1 \mod p^{i+1}$.

In general, we define

$$N^0(h) = h,\ N^n(h) = N(N^{n-1}(h)),\ \text{for } n \geq 1.$$

Then

a) $N^n(h) \circ [\pi^n] = \Pi_{\alpha \in W^{n-1}} h(X \dot{+} \alpha)$

b) If $h \in X^i S^X (i \geq 0)$,

$$N^{n+1}(h)/N^n(h) \in S^X \text{ and}$$
$$N^{n+1}(h) \equiv N^n(h) \mod p^{n+1}, \; n \geq 0.$$

Now, choose $\alpha \in W^n$, $\alpha \notin W^{n-1}$, $n \geq 0$. Put

$$\alpha_i = \pi^{n-i} \cdot \alpha = [\pi^{n-i}](\alpha), \; 0 \leq i \leq n.$$

Then $\alpha_i \in W^i, \alpha_i \notin W^{i-1}$. Saw that α_i is a prime element of k_π^i, $\mathcal{O}_i = \mathcal{O}[\alpha_i]$, $p_i = \mathcal{O}_i\alpha_i$.

LEMMA. *$\beta_i \in \pi^{n-i} p_0 \mathcal{O}_i$, $0 \leq i \leq n$. $\exists\, h \in S = \mathcal{O}[[X]]$ such that $h(\alpha_i) = \beta_i$, ${}^\forall i = 1, \cdots, n$.*

Proof. Put

$$g_i(X) = [\pi^{n+1}][\pi^i]/[\pi^{i+1}], \; i = 0, \cdots, n.$$

See that

$$g_i(\alpha_j) = \begin{cases} \pi^{n-i}\alpha_0, & \text{if } j = i \\ 0, & \text{otherwise.} \end{cases}$$

Since $\beta_i = \pi^{n-i} p_0 \mathcal{O}_i = \pi^{n-i}\alpha_0 \mathcal{O}[\alpha_i]$, we can write $\beta_i = \pi^{n-i}\alpha_0 h_i(\alpha_i)$, $h_i \in \mathcal{O}[X]$. Then $h = \sum_{i=0}^n g_i h_i$ is the desired one.

Main proposition of Coleman in [1].

PROPOSITION. *$\xi \in U(k_\pi^n)$, and let*

$$\xi_i = N_{n,i}(\xi) = N_{k_\pi^n/k_\pi^i}(\xi), \; 0 \leq i \leq n.$$

$\exists$ a power series $h(X) \in \mathcal{O}[[X]]$ such that $\xi_i = h(\alpha_i)$, $0 \leq i \leq n$.

Proof. Since $\xi \in U(k_\pi^n) \subseteq \mathcal{O}_n = \mathcal{O}[\alpha]$, we may write $\xi = h_1(\alpha)$, $h_1 \in \mathcal{O}[X]$. Clearly, $h_1 \in S^X$.

Know ;

$$N^{n-i}(h_1) \circ [\pi^{n-i}] = \Pi_\gamma h_1(X \dot{+} \gamma), \; \gamma \in W^{n-i-1}.$$

Put $X = \alpha$:

$$N^{n-i}(h_1)(\alpha_i) = \Pi_\gamma h_1(\alpha \dot{+} \gamma) = N_{n,i}(h_1(\alpha)) = N_{n,i}(\xi) = \xi_i.$$

If $h_2 = N^n(h_1) \in S^X$, then

$$N^{n-i}(h_1) \equiv N^{n-i+1}(h_1) \equiv \cdots \equiv N^n(h_1) = h_2(p^{n-i+1}).$$

Put $X = \alpha_i : \xi_i \equiv h_2(\alpha_i) \mod (p^{n-i+1})$.

$$\text{Thus } \beta_i = \xi_i - h_2(\alpha_i) \in \pi^{n-i+1}\mathcal{O}_i \subseteq \pi^{n-i}p_0\mathcal{O}_i.$$

By the above lemma, $\beta_i = h_3(\alpha_i)$.
Then $h = h_2 + h_3$ is the desired one.

Fundamental theorems in local class field theory :

NOTE. It is instructive to compare all of the following results with the cohomological treatment in "Algebraic numbers and functions" by E. Artin.

We will grant that $L = L_k = k_{ab}$ in Ω. In view of the isomorphism

$$\mathrm{Gal}(k_{ab}/k_\pi) \xrightarrow{\sim} \mathrm{Gal}(k_{ur}/k),$$

$\exists!\ \psi_\pi \in \mathrm{Gal}(k_{ab}/k_\pi)$ such that

$$\psi_\pi \,|\, k_{ur} = \varphi_k, \quad \psi_\pi \,|\, k_\pi = 1.$$

Moreover, k_π is the fixed field of ψ_π in k_{ab}. Fix a prime element π_0 of k and write $\psi = \psi_{\pi_0}$. Since $\mathrm{Gal}(k_{ab}/k)$ is abelian, we can define a homomorphism

$$\rho : k^X \to \mathrm{Gal}(k_{ab}/k)$$

given by

$$\pi_0^m u(m \in \mathbf{Z}, u \in U) \mapsto \psi^m \delta(u^{-1})$$

where $\delta : U \xrightarrow{\sim} \mathrm{Gal}(k_{ab}/k_{ur})$ is the previously introduced isomorphism. ρ is called either Artin or Norm residue map. Clearly,

$$\rho(x) \,|\, k_{ur} = \psi^m \,|\, k_{ur} = \varphi_k^m, \ m = \nu(x).$$

FACTS. (a) The above $\rho = \rho_k : k^X \to \mathrm{Gal}(k_{ab}/k)$ is the unique homomorphism satisfying

$$\rho_k(\pi) = \psi_\pi \text{ for all prime elements } \pi \text{ of } k.$$

Proof. Since k^X is generated by prime elements of k, the uniqueness is clear. For the asserted, apply the following lemma for $\pi' = \pi$, $m = 1$; if π' is a prime element of $k' = k_{ur}^m$, $m \geq 1$ and $x = N_{k'/k}(\pi')$, then $\rho(x)$ is the unique element σ of $\mathrm{Gal}(k_{ab}/k)$ such that

$$\sigma \mid k_{ur} = \varphi_k^m, \ \sigma \mid k_\pi^{m,\infty} = 1.$$

(b) ρ_k induces a topological isomorphism

$$U \xrightarrow{\sim} \mathrm{Gal}(k_{ab}/k_{ur}) \text{ given by } u \mapsto \delta(u^{-1}).$$

For any prime element π of k, it also induces

$$U \xrightarrow{\sim} \mathrm{Gal}(k_\pi/k), \text{ given by } \ u \mapsto \delta_\pi(u^{-1})$$

and δ_π is the previously introduced one.

(c) For $x = \pi^m u (m \in \mathbf{Z}, u \in U)$, π any prime element of k,

$$\rho_k(x) = \rho_k(\pi)^m \rho_k(u) = \psi_\pi^m \delta(u^{-1}) \text{ and}$$
$$\rho_k(x) \mid k_{ur} = \psi_\pi^m \mid k_{ur} = \varphi_k^m.$$

Thus these two properties hold true for any prime element π of k.

(d) ρ_k is injective and continuous in the ν-topology of k^X and Krull topology of $\mathrm{Gal}(k_{ab}/k)$.

Proof. Suppose $\rho_k(\pi^m u) = 1$. Then $\varphi_k^m = \rho_k(\pi^m u) \mid k_{ur} = 1$. Since φ_k is of infinite order, $m = 0$ and hence $\delta(u^{-1}) = \rho_k(u) = 1$. Since δ is an isomorphism, $u = 1$. Continuity follows from the topological isomorphism $U \xrightarrow{\sim} \mathrm{Gal}(k_{ab}/k_{ur})$ and the openess of U.

(e) The image of ρ_k is a dense subgroup of $\mathrm{Gal}(k_{ab}/k)$.

$$\mathrm{Im}\,\rho_k = \{\sigma \in \mathrm{Gal}(k_{ab}/k) | \ \sigma \mid k_{ur} = \varphi_k^m \text{ for some integer } m\}.$$

In particular, if $\sigma \mid k_{ur} = \varphi_k$, then $\exists!$ prime element π of k such that $\sigma = \rho_k(\pi)$.

Functorial properties of Norm Residue Maps :

(a) For a finite extension k'/k of local fields,

$$\begin{tikzcd} k'^X \arrow[r] \arrow[d, "N_{k'/k}"'] & \mathrm{Gal}(k'_{ab}/k') \arrow[d, "\mathrm{res}"] \\ k^X \arrow[r] & \mathrm{Gal}(k_{ab}/k) \end{tikzcd}$$ is commutative.

Proof. By using the inertia field of the extension k'/k, we may assume that k'/k is either unramified or totally ramified. Consider each case.

(b) Suppose $\sigma : (k, \nu) \xrightarrow{\sim} (k', \nu')$ i.e., $\sigma = k \xrightarrow{\sim} k'$ and $\nu = \nu' \circ \sigma$. Extend σ to an isomorphism of fields $\sigma : k_{ab} \xrightarrow{\sim} k'_{ab}$, and define an isomorphism

$$\sigma^* : \mathrm{Gal}(k_{ab}/k) \xrightarrow{\sim} \mathrm{Gal}(k'_{ab}/k') \text{ given by } \tau \mapsto \sigma\tau\sigma^{-1}.$$

Then

$$\begin{tikzcd} k^X \arrow[r, "\rho_k"] \arrow[d, "\sigma"'] & \mathrm{Gal}(k_{ab}/k) \arrow[d, "\sigma^*"] \\ k'^X \arrow[r, "\rho_{k'}"] & \mathrm{Gal}(k'_{ab}/k') \end{tikzcd}$$ is commutative.

(c) Let

$$\begin{aligned} \Omega_s &= \text{the maximal galois extension of } (k, \nu) \text{ in } \Omega \\ &= \text{the separable closure of } k \text{ in } \Omega. \end{aligned}$$

For a finite separable extension k'/k, put

$$\begin{aligned} G &= \mathrm{Gal}(\Omega_s/k), \\ H &= \mathrm{Gal}(\Omega_s/k'), \\ G' &= \mathrm{Gal}(\Omega_s/k_{ab}), \\ H' &= \mathrm{Gal}(\Omega_s/k'_{ab}). \end{aligned}$$

Then $[G:H]=[k':k]=n$, and G' and H' are topological commutator subgroups of G and H, respectively.

Let $\{\tau_1,\cdots,\tau_n\}$ be a set of representatives for the set of all right cosets of H in G i.e., $G=\cup_{i=1}^{n}H\tau_i$ (disjoint).

For each $\sigma\in G$ and i $(1\le i\le n)$,

$$\exists!\ h_i(\sigma)\in H \text{ and } i'\ (1\le i'\le n) \text{ such that } \tau_i\sigma=h_i(\sigma)\tau_{i'}.$$

Then we have the well-defined homomorphism

$$t_{G/H}:G\to H/H'\ (\sigma\mapsto \Pi_{i=1}^{n}h_i(\sigma)H'\in H/H'),$$

called the transfer (Vorlagerung in German) map. Since H/H' is abelian, $t_{G/H}$ induces

$$G/G'\to H/H'$$

which is again denoted by the same symbol.

From now on, for each finite separable extension k'/k, $t_{k'/k}$ will denote either of the following homomorphisms ;

$$\mathrm{Gal}(\Omega_s/k)\to\mathrm{Gal}(k'_{ab}/k'),\mathrm{Gal}(k_{ab}/k)\to\mathrm{Gal}(k'_{ab}/k').$$

Properties of transfer map :

(a) For $k\subseteq k'\subseteq k''$, $t_{k''/k}=t_{k''/k'}\circ t_{k'/k}$.

(b) For $\sigma\in G=\mathrm{Gal}(\Omega_s/k)$,

$$n=[k':k]=[G;H],\ t_{k'/k}(\sigma)G'=\sigma^nG'$$

i.e., $t_{k'/k}(\sigma)\,|\,k_{ab}=\sigma^n\,|\,k_{ab}$ (pf : restrict $\tau_i\sigma=h_i(\sigma)\tau_i'$ to k_{ab} and note $\mathrm{Gal}(k_{ab}/k)$ is abelian)

(c) If k'/k is Galois and $\sigma\in H=\mathrm{Gal}(\Omega_s/k')$, then $t_{k'/k}(\sigma)=\Pi_\tau(\tau\sigma\tau^{-1})H'$, where τ ranges over a set of representatives for G/H (pf : $H\lhd G\Rightarrow\tau_i\sigma=(\tau_i\sigma\tau_i^{-1})\tau_i$, $\tau_i\sigma\tau_i^{-1}\in H$)

(d) If k'/k is cyclic and $\langle\sigma H\rangle=G/H=\mathrm{Gal}(k'/k)$, then $t_{k'/k}(\sigma)=\sigma^nH'$ i.e., $t_{k'(\sigma)}\,|\,k'_{ab}=\sigma^n\,|\,k'_{ab}$ (pf : $G=\cup_{i=1}^{n}H\sigma^i$ (disjoint). Thus $^\forall i$,

$$\sigma^i\sigma=\begin{cases} e\sigma^{i+1}, & \text{if } i<n \quad\text{and}\quad \sigma^n\in H\\ \sigma^n\sigma, & \text{if } i=n\end{cases}\ )$$

Denote by (k'/k) the diagram:

$$\begin{tikzcd} k^X \arrow[r, "\rho_k"] \arrow[d] & \mathrm{Gal}(k_{ab}/k) \arrow[d, "t_{k'/k}"] \\ k'^X \arrow[r, "\rho_{k'}"] & \mathrm{Gal}(k'_{ab}/k') \end{tikzcd}$$

LEMMA. *If (k'/k) is commutative, then*

$$t_{k'/k} : Gal(k_{ab}/k) \to Gal(k'_{ab}/k')$$

is injective.

Proof. Suppose $t_{k'/k}(\sigma) = 1$ and extend σ to an automorphism of Ω_s, again denoted by σ. By (b) above,

$$\sigma^n \mid k_{ab} = t_{k'/k}(\sigma) \mid k_{ab} = 1.$$

Since $\mathrm{Gal}(k_{ur}/k) \simeq \hat{\mathbf{Z}}$ is torsion free, $\sigma \in \mathrm{Gal}(k_{ab}/k_{ur})$. Thus $\sigma = \rho_k(u)$ for some $u \in U$. By commutativity of (k'/k),

$$\rho_{k'}(u) = t_{k'/k}(\rho_k(u)) = t_{k'/k}(\sigma) = 1.$$

Since $\rho_{k'}$ induces $U' \xrightarrow{\sim} \mathrm{Gal}(k'_{ab}/k'_{ur})$, $u = 1$ and $\sigma = 1$.

COROLLARY. *For $k \subseteq k' \subseteq k''$,*
(i) If (k''/k') and (k'/k) are commutative, so is (k''/k).
(ii) If (k''/k') and (k''/k) are commutative, so is (k'/k).

Proof. (i) is trivial. For (ii), use the above lemma.

THEOREM. *For any finite extension k'/k of local fields and $x \in k^X$,*

$$\rho_k(x) \mid (k' \cap k_{ab}) = 1 \Leftrightarrow x \in N(k'/k)$$

Proof. ($\Leftarrow$) If $x = N_{k'/k}(x')$, $x' \in k'^X$, then by functoriality (a)

$$\rho_k(x) \mid (k' \cap k_{ab}) = \rho_{k'}(x') \mid (k' \cap k_{ab}) = 1.$$

($\Rightarrow$) Since $\mathrm{Gal}(k_{ab}k'/k') \xrightarrow{\sim} \mathrm{Gal}(k_{ab}/k' \cap k_{ab})$, $\rho_k(x)$ can be extended to an automorphism in $\mathrm{Gal}(k_{ab}k'/k')$ and then to an automorphism σ of $\mathrm{Gal}(k'_{ab}/k')$. Put

$$k_{ur}^m = (k' \cap k_{ab}) \cap k_{ur} = k' \cap k_{ur}.$$

Then $\rho_k(x) \,|\, k_{ur}^m = 1$ i.e., a power of φ_k^m over k_{ur}^m. Since $\mathrm{Gal}(k'_{ur}/k') \xrightarrow{\sim} \mathrm{Gal}(k_{ur}/k_{ur}^m)(\varphi_{k'} \mapsto \varphi_k^m)$, $\sigma \,|\, k'_{ur}$ is a power of $\varphi_{k'}$. By Facts (e), $\sigma = \rho_{k'}(x')$ for some $x' \in k'^X$.

Thus by functoriality (a) again,

$$\rho_k(x) = \sigma \,|\, k_{ab} = \rho_k(N_{k'/k}(x')).$$

Since ρ_k is injective, $x = N_{k'/k}(x')$.

THEOREM. *For any finite separable extension k'/k, the diagram (k'/k) is commutative.*

Proof. 1st reduction : Since $\exists$ a finite Galois extension k''/k such that $k \subseteq k' \subseteq k''$, one can reduce to Galois case by the above cor (ii).

2nd reduction : Using ramification groups, one can show that $\mathrm{Gal}(k'/k)$ is always solvable for a finite Galois extension of local fields. Thus we may assume k'/k is abelian by cor (i).

REMARK. We grant the following facts : (k'/k) is commutative if k'/k is unramified, and $\rho_{k'}(x) = t_{k'/k}(\rho_k(x))$ if k'/k is finite Galois and $x \in N(k'/k)$.

Let $n = [k' : k]$, $E = k_{ur}^n$, $E' = Ek'$, and let π be a prime element of k. Then

$$\langle \rho_k(\pi) | E \rangle = \mathrm{Gal}(E/k) \text{ and}$$
$$\rho_E(\pi) = t_{E/k} \circ \rho_k(\pi)$$

by the 1st remark. By properties of transfer (d),

$$\begin{aligned} \rho_E(\pi) \,|\, k' &= t_{E/k} \circ \rho_k(\pi) \,|\, k' \\ &= \rho_k(\pi)^n \,|\, k' \\ &= 1 \end{aligned}$$

Thus $\rho_E(\pi)\,|\,E' = 1 \Rightarrow \pi \in N(E'/E)$ by the above theorem. By the 2nd remark,

$$\begin{aligned}\rho_{E'}(\pi) = t_{E'/E}(\rho_E(\pi)) &= t_{E'/E} \circ t_{E/k} \circ \rho_k(\pi)\\ &= t_{E'/k}(\rho_k(\pi)).\end{aligned}$$

For any finite abelian extension k'/k, $\rho_{k'/k}$ is the composite

$$k^X \xrightarrow{\rho_k} \mathrm{Gal}(k_{ab}/k) \xrightarrow{\text{res}} \mathrm{Gal}(k'/k) = \mathrm{Gal}(k_{ab}/k)/\mathrm{Gal}(k_{ab}/k').$$

THEOREM. *For a finite abelian extension k'/k, $\rho_{k'/k}$ induces the isomorphism*

$$k^X/N(k'/k) \xrightarrow{\sim} \mathit{Gal}(k'/k).$$

Also, $N(k'/k) = \rho_k^{-1}(\mathit{Gal}(k_{ab}/k'))$ and

$$\mathit{Gal}(k_{ab}/k') = \text{ the closure of } \rho_k(N(k'/k)) \text{ in } \mathit{Gal}(k_{ab}/k).$$

Proof. Recall that for any finite extension k'/k

$$\rho_k(x)\,|\,k' \cap k_{ab} = 1 \Leftrightarrow x \in N(k'/k).$$

Hence $\mathrm{Ker}\,\rho_{k'/k} = N(k'/k)$. Since $\rho_k(k^X)$ is dense in $\mathrm{Gal}(k_{ab}/k)$ and $\mathrm{Gal}(k_{ab}/k')$ is open in $\mathrm{Gal}(k_{ab}/k)$, $\rho_{k'/k}$ is surjective. The second statement is clear. Since $\mathrm{Gal}(k_{ab}/k')$ is closed and $\rho_k(N(k'/k)) \subset \mathrm{Gal}(k_{ab}/k')$,

$$\rho_k(N(k'/k))^- \subset \mathrm{Gal}(k_{ab}/k').$$

Since $k^X/N(k'/k) \xrightarrow{\sim} \mathrm{Gal}(k_{ab}/k)/\mathrm{Gal}(k_{ab}/k')$ is given by

$$aN(k'/k) \mapsto \rho_k(a)\mathrm{Gal}(k_{ab}/k')$$

i.e., $\rho_k(aN(k'/k)) \subset \rho_k(a)\mathrm{Gal}(k_{ab}/k')$ and

$\rho_k(k^X)$ is dense in $\mathrm{Gal}(k_{ab}/k)$, we must have

$$\rho_k(aN(k'/k))^- = \rho_k(a)\mathrm{Gal}(k_{ab}/k').$$

COROLLARY. *For any finite abelian extension k'/k, we have the fundamental equality in local class field theory i.e.,*

$$[k^X : N(k'/k)] = [k' : k].$$

COROLLARY.

(i) *For any finite extension k'/k,*

$$N(k'/k) = N(k' \cap k_{ab}/k),$$

$$[k^X : N(k'/k)] \leq [k' : k],$$

and equality holds iff k'/k abelian.

(ii) *If k'/k is finite and k''/k finite abelian, then*

$$N(k'/k) \subseteq N(k''/k) \Leftrightarrow k \subseteq k'' \subseteq k'.$$

(iii) *If k'/k is finite abelian and $k \subseteq k'' \subseteq k'$, then the isomorphism $k^X/N(k'/k) \xrightarrow{\sim} Gal(k'/k)$ induces*

$$N(k''/k)/N(k'/k) \xrightarrow{\sim} Gal(k'/k'').$$

Proof. (i) Use the fact that for any finite extension k'/k

$$\rho_k(x) \,|\, k' \cap k_{ab} = 1 \Leftrightarrow x \in N(k'/k)$$

and the above corollary.

(ii) Use the 2^{nd} statement in the above theorem.

(iii) Follows from the commutativity of

$$\begin{tikzcd}
k^X/N(k'/k) \arrow[r, "\sim"] \arrow[d] & \mathrm{Gal}(k'/k) \arrow[d] \\
k^X/N(k''/k) \arrow[r, "\sim"] & \mathrm{Gal}(k''/k)\,.
\end{tikzcd}$$

REMARK. For a prime element π of k, $m \geq 1$, $n \geq 0$,

$$N(k_\pi^{m,n}) = \langle \pi^m \rangle \times U_{n+1}$$

THEOREM. *(the existence and uniqueness theorem in local class field theory)*

For any closed subgroup H of k^X with finite index, there exists a unique k'/k finite abelian extension such that $H = N(k'/k)$.

Proof. Let $m = [k^X : H]$, and let π a prime element of k. Then $\pi^m \in H$ and $H \cap U(k)$ is a closed subgroup of $U(k)$ with

$$\begin{aligned}
&[U(k) : H \cap U(k)] = [U(k)H : H] \leq [k^X : H] = m \\
&\Rightarrow H \cap U(k) \text{ is open } U(k) \\
&\Rightarrow \exists n \geq 0 \text{ such that } U_{n+1} \subset H \cap U(k) \subseteq H.
\end{aligned}$$

Thus

$$N(k_\pi^{m,n}) = \langle \pi^m \rangle \times U_{n+1} \subseteq H \subseteq k^X.$$

Since $k^X/N(k_\pi^{m,n}/k) \xrightarrow{\sim} \mathrm{Gal}(k_\pi^{m,n}/k)$, $\exists$ a field k', $k \subseteq k' \subseteq k_\pi^{m,n}$ such that

$$H/N(k_\pi^{m,n}/k) \xrightarrow{\sim} \mathrm{Gal}(k_\pi^{m,n}/k'),$$

which is induced by $\rho_{k_\pi^{m,n}/k}$.

By the above cor (iii),

$$N(k'/k)/N(k_\pi^{m,n}/k) \xrightarrow{\sim} \mathrm{Gal}(k_\pi^{m,n}/k'),$$

also induced by $\rho_{k_\pi^{m,n}/k}$. Thus $H = N(k'/k)$ and k'/k is abelian. Uniqueness follows from the above cor (ii).

COROLLARY. *There exists an order reversing 1-1 correspondence between {finite abelian extensions k'/k in Ω} and {closed subgroups of finite index in k^X}. Moreover,*

$$\begin{aligned}
&k' \subset k'' \Leftrightarrow N(k'/k) \supset N(k''/k), \\
&N(k'k''/k) = N(k'/k) \cap N(k''/k), \\
&N(k' \cap k''/k) = N(k'/k)N(k''/k).
\end{aligned}$$

Proof. $k' \mapsto N(k'/k)$ is the correspondence.
By the above cor (ii),

$$k' \subset k'' \Leftrightarrow N(k'/k) \supset N(k''/k).$$

Clearly,

$$N(k'k''/k) \subset N(k'/k) \cap N(k''/k).$$

Conversely, if $x \in N(k'/k) \cap N(k''/k)$, then $\rho_k(x)$ fixes k' and k'' and hence does $k'k''$ i.e.,

$$\rho_k(x) \in \mathrm{Gal}(k_{ab}/k'k'') \Rightarrow x \in N(k'k''/k).$$

Clearly,

$$N(k' \cap k''/k) \supset N(k'/k)N(k''/k).$$

But

$$[N(k' \cap k''/k) : N(k'/k)] = [k' : k' \cap k''],$$

$$\begin{aligned}[N(k'/k)N(k''/k) : N(k'/k)] &= [N(k''/k) : N(k'/k) \cap N(k''/k)] \\ &= [N(k''/k) : N(k'k''/k)] \\ &= [k'k'' : k''] \\ &= [k' : k' \cap k''].\end{aligned}$$

Explicit Forms of the Norm Residue Symbol :

Definition. Let (k, ν) be a local field with a prime element π of k. By a π-sequence of k we mean a pair $(f, w = (w_n)_{n \geq 0})$

$$\text{where } f \in \mathcal{F}_\pi^1,\ (w_n)_{n \geq 0} \subset W_f = \cup_n W_f^n$$

such that

$$w_0 \in W_f^\circ,\ w_0 \neq 0,\ w_n = f(w_{n+1}) = \pi \cdot_f w_{n+1},\ n \geq 0.$$

REMARK. (a) Since $\pi \cdot_f W_f^{n+1} = W_f^n$, for a given $f \in \mathcal{F}_\pi^1$, a π-sequence always exists.

(b) Actually, $w_n \in W_f^n$, $w_n \notin W_f^{n-1}$, $W_f^n = \mathcal{O} \cdot_f w_n$.

DEFINITION. If $(f', w' = (w'_n)_{n \geq 0})$ is another π-sequence, then an invertible $h(x) \in M = X\mathcal{O}[[X]]$ is an isomorphism of (f, w) to (f', w') if

$$h \circ f \circ h^{-1} = f', \ h(w_n) = w'_n, \ n \geq 0.$$

We write $h : (f, w) \xrightarrow{\sim} (f', w')$. Moreover, h induces the following isomorphisms over $\mathcal{O}$:

$$F_f \xrightarrow{\sim} F_{f'}, \ W_f^n \xrightarrow{\sim} W_{f'}^n, \ W_f \xrightarrow{\sim} W_{f'}.$$

LEMMA. *Let $(f, w = (w_n)_{n \geq 0})$ be a π-sequence. If $g(X) \in \mathcal{O}[[X]]$ is such that $g(w_i) = 0$ for $1 \leq i \leq n$, then*

$$[\pi^{n+1}]_f \,|\, Xg(X) \textit{ in } \mathcal{O}[[X]].$$

In addition, if $g(w_i) = 0$ for all $i \geq 0$, then $g(x) = 0$.

Proof. Since $W_f^i - W_f^{i-1}$ are the conjugates of w_i over k and g has coefficients in $\mathcal{O}$,

$$g(w_i) = 0 \Rightarrow g(\beta) = 0, \ ^\forall\beta \in W_f^i - W_f^{i-1}.$$

Thus $Xg(X)$ is such that $\alpha g(\alpha) = 0$ for all $\alpha \in W_f^n \Rightarrow [\pi^{n+1}]_f \,|\, Xg(X)$. Since $f = [\pi]_f \in (\pi, X)$ is the unique maximal ideal of $\mathcal{O}[[X]]$,

$$[\pi^{n+1}]_f = [\pi]_f \circ \cdots \circ [\pi]_f \in (\pi, X)^{n+1}.$$

Thus if $g(w_i) = 0$, $i \geq 0$, then

$$Xg(X) \in (\pi, X)^{n+1}, \ n \geq 0 \Rightarrow Xg(X) = 0 \Rightarrow g(X) = 0.$$

LEMMA. *For $(f, w = (w_n)_{n\geq 0})$, $(f', w' = (w'_n)_{n\geq 0})$ π-sequences of k, $\exists !$ isomorphism $h : (f, w) \overset{\sim}{\longrightarrow} (f', w')$. Moreover, if $w = w'$, then $h(X) = X$ so that $f = f'$.*

Proof. $\exists \theta(X) \in \mathcal{O}[[X]]$ such that

$$\theta(X) \equiv X \ (\deg 2), \text{ and } \theta \circ f = f' \circ \theta.$$

If $w'' = (\theta(w_n))_{n\geq 0}$, then $\theta : (f, w) \overset{\sim}{\longrightarrow} (f', w'')$ and hence we may assume $f = f'$ for the existence. Since $w'_n \in W^n_f - W^{n-1}_f$ and $W^n_f = \mathcal{O} \cdot_f w_n$,

$$\exists u_n \in U(k) \text{ such that } u_n \cdot_f w_n = w'_n$$

and u_n is unique up to modulo $U_{n+1} = 1 + p^{n+1}$. For $m \geq n \geq 0$, $u_m \cdot_f w_n = w'_n$ and

$$u_n \cdot_f w_n = w'_n \Rightarrow u_m \equiv u_n (mod\ U_{n+1}, \text{ multiplicative}).$$

Thus $\exists u \in U$ such that

$$u \equiv u_n \ (mod\ U_{n+1}),\ n \geq 0 \text{ and } u \underset{f}{\cdot} w_n = w'_n.$$

If $h = [u]_f$, then $h \circ f \circ h^{-1} = [u\pi u^{-1}]_f = f$ and $h(w_n) = w'_n$. It is enough to show : $w = w' \Rightarrow h(X) = X$ for uniqueness. Since $g(X) = h(X) - X$ satisfies $g(w_i) = 0$, $g(X) = 0$ by the above lemma.

DEFINITION. A π-sequence $(f, w = (w_n)_{n\geq 0})$ is normed if

$$N_{m,n}(w_m) = N_{k^m_\pi / k^n_\pi}(w_m) = w_n, \text{ for all } 0 \leq n \leq m.$$

REMARK. The normedness of (f, w) depends only on f. Actually,

$$(f, w) \text{ is normed } \Leftrightarrow [\pi]_f(X) = \Pi_{\gamma \in W^0_f}(X \dot{+}_f \gamma)$$

i.e., $N_f(X) = X$.

Proof. ($\Longleftarrow$) Since $w_{n+1} \dot{+}_f W^0_f$ is the complete set of conjugates of w_{n+1} over k^n_π,

$$N_{n+1,n}(w_{n+1}) = \Pi_{\gamma \in W^0_f}(w_{n+1} \dot{+}_f \gamma) = [\pi]_f(w_{n+1}) = w_n.$$

($\Longrightarrow$) If $g(X) = [\pi]_f(X) - \Pi_{\gamma\in W_f^0}(X \dot{+}_f \gamma)$, then for $n \geq 0$

$$g(w_{n+1}) = w_n - N_{n+1,n}(w_{n+1}) = 0 \text{ and } g(w_0) = 0,$$

since $\pi \cdot_f w_0 \in W_f^{-1} = 0$, $0 \in w_0 \dot{+}_f W_f^0 = W_f^0$.

Let $B = \lim\limits_{\substack{\leftarrow \\ n}} (k_\pi^n)^X$ with respect to

$$N_{m,n} : (k_\pi^m)^X \to (k_\pi^n)^X,\ 0 \leq n \leq m,$$
$$\text{and let } N_n = N_{k_\pi^n/k},\ n \geq 0.$$

Since $N_n(\beta_n) = N_m(\beta_m)$, for all $m, n \geq 0$,

$$\text{define } \nu(\beta) = \nu(N_n(\beta_n)),\ \text{for any } n \geq 0.$$

In particular, $\nu(w) = 1$ for a normed π-sequence (f, w), since k_π^n/k is totally ramified. Clearly,

$$\nu(\beta\beta') = \nu(\beta) + \nu(\beta') \text{ for } \beta, \beta' \in B$$

and B is generated by the $\beta's$ with $\nu(\beta) = 1$.

THEOREM. *(i) For a π-sequence (f, w) and $\beta \in B$ with $\nu(\beta) = 0$,*

$$\exists!\ t(X) \in \mathcal{O}[[X]]^X \textit{ such that } t(w_n) = \beta_n,\ n \geq 0.$$

(ii) If (f, w) is normed and $\beta \in B$ is such that $\nu(\beta) = l$ then

$$\exists!\ t(X) \in X^l\mathcal{O}[[X]]^X \textit{ such that } t(w_n) = \beta_n,\ n \geq 0.$$

Proof. β_n is a unit of k_π^n, since $0 = \nu(\beta) = \nu(N_n(\beta_n))$. Thus

$$\exists t_n(X) \in \mathcal{O}[[X]] \text{ such that } t_n(w_i) = \beta_i,\ 0 \leq i \leq n.$$

Since $(t_{n+1} - t_n)(w_i) = \beta_i - \beta_i = 0$, $0 \leq i \leq n$,

$$Xt_{n+1} \equiv Xt_n\ (mod\ [\pi^{n+1}]_f).$$

Since $[\pi^{n+1}]_f \in (\pi, X)^{n+1}$, the limit $\lim_{n\to\infty} Xt_n$ exists in $\mathcal{O}[[X]]$, which can be written as Xt, $t \in \mathcal{O}[[X]]$. Then

$$Xt \equiv Xt_n\ (mod\ [\pi^{n+1}]_f) \text{ and}$$
$$w_n t(w_n) = w_n t_n(w_n) = w_n\beta_n \text{ i.e., } t(w_n) = \beta_n.$$

Clearly, $t \in \mathcal{O}[[X]]^X$ and is unique by the 1st of the above lemmas. (ii) follows from (i).

REMARK. For a fixed π-sequence (f, w),

$$\exists!\ t_\beta(X) \in X^l\mathcal{O}[[X]]^X \text{ such that } t_\beta(w_n) = \beta_n,\ n \geq 0,$$

for each $\beta \in B$ with $\nu(\beta) = l$. Uniqueness $\Rightarrow t_{\beta\beta'} = t_\beta t_{\beta'},\ \beta, \beta' \in B$. Claim :

$$\begin{aligned}&\{(f_\beta, \beta) \mid \beta \in B, \nu(\beta) = 1\}\\ &=\text{the set of all normed } \pi - \text{sequences for } k,\end{aligned}$$

where for $\beta \in B$, $\nu(\beta) = 1$ $f_\beta = t_\beta \circ f \circ t_\beta^{-1} \in \mathcal{F}_\pi^1$.

Proof. Since $t_\beta \in X\mathcal{O}[[X]]^X$, t_β is invertible in M. $t_\beta(w_n) = \beta_n, n \geq 0$

$$\Rightarrow (f_\beta, \beta) \text{ is a normed } \pi - \text{sequence and } t_\beta : (f, w) \overset{\sim}{\longrightarrow} (f_\beta, \beta).$$

By 2nd lemma of the above, f_β is the unique series in $\mathcal{O}[[X]]$ such that (f_β, β) is a π-sequence. So f_β depends only on β and is independent of (f, w). Conversely, if (f', w') is any normed π-sequence, then $\nu(w') = 1$, $w' \in B$ and hence $(f_{w'}, w')$ is a normed π-sequence, and

$$(f', w') \overset{\sim}{\longrightarrow} (f_{w'}, w') \Rightarrow f' = f_{w'}$$

by the 2nd lemma.

Let π be a prime element of (k, ν), $f \in \mathcal{F}_\pi^1$, p_n the maximal ideal of k_π^n $(n \geq 0)$.

LEMMA. *Let $n \geq 0$. For $\alpha \in p_n$,*

$$\exists \xi \in m_f = p_{\bar{\Omega}} \text{ such that } \pi^{n+1} \cdot_f \xi = \alpha.$$

Then $k_\pi^n(\xi)/k_\pi^n$ is abelian, $[k_\pi^n(\xi) : k_\pi^n] \mid q^{n+1}$, $k_\pi^n(\xi)$ depends only on α (independent of the choice of such a ξ).

Proof. Reduce to $f(X) = \pi X + X^q$. $[\pi^{n+1}]_f = f \circ \cdots \circ f$ is a polynomial of degree q^{n+1} in $\mathcal{O}[X]$. Thus it has a solution $\xi \in m_f$. Clearly,

$$\xi \dot{+}_f W_f^n \text{ is the set of all roots of } [\pi^{n+1}]_f - \alpha = 0 \text{ in } \Omega,$$

$k_\pi^n(\xi)/k_\pi^n$ is finite Galois independent of ξ. For $\sigma \in \mathrm{Gal}(k_\pi^n(\xi)/k_\pi^n)$,

$$\pi^{n+1} \cdot_f \xi = \alpha \Rightarrow \pi^{n+1} \cdot_f \sigma(\xi) = \alpha \text{ i.e., } \sigma(\xi)\dot{-}_f\xi \in W_f^n$$

and for σ, $\tau \in \mathrm{Gal}(k_\pi^n(\xi)/k_\pi^n)$,

$$\begin{aligned}&\sigma\tau(\xi)\dot{-}_f\xi\\ &=(\sigma(\xi)\dot{-}_f\xi)\dot{+}_f\sigma(\tau(\xi)\dot{-}_f\xi)\\ &=(\sigma(\xi)\dot{-}_f\xi)\dot{+}_f(\tau(\xi)\dot{-}_f\xi) \text{ i.e.,}\end{aligned}$$

$$\mathrm{Gal}(k_\pi^n(\xi)/k_\pi^n) \to W_f^n(\sigma \mapsto \sigma(\xi)\dot{-}_f\xi)$$

is an injective homomorphism, and hence $\mathrm{Gal}(k_\pi^n(\xi)/k_\pi^n)$ is abelian.

For $\alpha \in p_n$, $\beta \in (k_\pi^n)^X$, define the pairing

$$(\ ,\ )_{n,f} : p_n \times (k_\pi^n)^X \to W_f^n \text{ by}$$

$$(\alpha,\beta)_{n,f} = \rho_n(\beta)(\xi)\dot{-}_f\xi,$$

where ρ_n is the Artin map of k_π^n, $\pi^{n+1} \cdot_f \xi = \alpha$. This is well-defined, since if $\pi^{n+1} \cdot_f \xi' = \alpha$, then

$$\xi' \in \xi\dot{+}_f W_f^n \Rightarrow \rho_n(\beta)(\xi')\dot{-}_f\xi' = \rho_n(\beta)(\xi)\dot{-}_f\xi.$$

Properties of of $(\ ,\ )_{n,f}$:

(i)

$$\begin{aligned}(\alpha_1\dot{+}\alpha_2,\beta)_n &= (\alpha_1,\beta)_n\dot{+}(\alpha_2,\beta)_n,\\ (\alpha,\beta_1\beta_2)_n &= (\alpha,\beta_1)_n\dot{+}(\alpha,\beta_2)_n,\\ (a\cdot\alpha,\beta)_n &= a\cdot(\alpha,\beta)_n,\ a \in \mathcal{O}.\end{aligned}$$

(ii) $(\alpha,\beta)_n = 0 \Leftrightarrow \beta \in N(k_\pi^n(\xi)/k_\pi^n)$, $\pi^{n+1}\cdot\xi = \alpha$.

(iii) If $N_f(X) = X$ and α a prime element of k_π^n, then $(\alpha,\alpha)_{n,f} = 0$.

(iv) For $0 \le n \le m$,

$$(\pi^{m-n} \cdot_f \alpha, \beta')_m = (\alpha, N_{m,n}(\beta'))_n$$

for $\alpha \in p_n$, $\beta' \in (k_\pi^m)^X$.

(v) Let $f, f' \in \mathcal{F}_\pi^1$, $h : F_f \xrightarrow{\sim} F_{f'}$ over $\mathcal{O}$. Then

$$h((\alpha,\beta)_{n,f}) = (h(\alpha),\beta)_{n,f'} \text{ for } \alpha \in p_n,\ \beta \in (k_\pi^n)^X.$$

Let $A_f = \varinjlim p_n$, with respect to

$$p_n \to p_m \ (\alpha \mapsto \pi^{m-n} \cdot_f \alpha) \text{ for } 0 \leq n \leq m.$$

Then A_f is an $\mathcal{O}$-module.

Define

$$(\ ,\ )_f : A_f \times B \to W_f \text{ by}$$

$$(\alpha, \beta)_f =: (\alpha_n, \beta_n)_{n,f}, \text{ if } \alpha \text{ is represented by } \alpha_n \in p_n.$$

This well-defined in view of (iv), and satisfies bimultiplicativity,

$$(a \cdot_f \alpha, \beta)_f = a \cdot_f (\alpha, \beta)_f, \ a \in \mathcal{O},$$

$$h((\alpha, \beta)_f) = (h(\alpha), \beta)_{f'} \text{ for } h : F_f \xrightarrow{\sim} F_{f'} \text{ over } \mathcal{O}.$$

From now on, assume (k, ν) is a p-field with characteristic 0 (due to the existence of logarithm). ∃! isomorphism over k

$$\lambda_0 : F_f \xrightarrow{\sim} G_a \text{ (i.e., } \lambda_0(X \dot{+}_{F_f} Y) = \lambda_0(X) + \lambda_0(Y))$$

such that $\lambda_0(X) \equiv X$ (deg 2).

Clearly, $\lambda : F_f \xrightarrow{\sim} G_a$ is the unique isomorphism over k such that

$$\lambda(X) \equiv uX \ (\deg 2), \text{ for } \lambda = u\lambda_0, \ u \in U(k),$$

called logarithms of F_f.

In fact,

$$\lambda(X) = \sum_{n=1}^{\infty} \frac{c_n}{n} X^n, \ c_1 = u, \ c_n \in \mathcal{O}, \ n \geq 1.$$

If $f' \in \mathcal{F}_\pi^1$ and $h : F_{f'} \xrightarrow{\sim} F_f$ isomorphism over $\mathcal{O}$, then

$$h(X) \equiv u'X \ (\deg 2), \ u' \in U(k),$$

and hence

$$\lambda\circ h : F_{f'} \xrightarrow{\sim} G_a,\ \lambda\circ h(X) \equiv uu'X\ (\deg 2)$$

i.e., $\lambda\circ h$ is also a logarithm.

Properties of a logarithm λ of F_f:

(i) $\lambda(\alpha)$ converges in $\bar{\Omega}$ for any $\alpha\in m_f$. In particular,

$$\alpha\in p_m \Rightarrow \lambda(\alpha)\in k_\pi^m.$$

(ii) $\lambda(\alpha\dot{+}_f\beta) = \lambda(\alpha)+\lambda(\beta), \lambda(a\cdot_f\alpha) = a\lambda(\alpha)$, for $\alpha,\beta\in m_f,\ a\in \mathcal{O}$.

Fix a normed π-sequence $(f, w = (w_n)_{n\geq 0})$, λ a logarithm of F_f, $t_\beta(X)$ the unique power series such that $t_\beta(w_m) = \beta_m$, $m\geq 0$.

Define

$$\delta(\beta)_n = \frac{1}{\lambda'(w_n)}\frac{t'_\beta(w_n)}{t_\beta(w_n)},\ n\geq 0, \text{ for } \beta\in B.$$

Note : $\delta(\beta)_n\in k_\pi^n$.

Properties of δ:

(i) $\delta(\beta\beta')_n = \delta(\beta)_n+\delta(\beta')_n,\ \beta,\beta'\in B$

(ii) $\delta(\beta)_n\in p_n^{-1}$

(iii) For $m\geq n\geq 0$,

$$T_{m,n}(\delta(\beta)_m) = \pi^{m-n}\delta(\beta)_n\ (T_{m,n} : k_\pi^m\to k_\pi^n \text{ the trace})$$

Define

$$x_n(\alpha_n,\beta) = \frac{1}{\pi^{n+1}}T_n(\lambda(\alpha_n)\delta(\beta)_n)\in k,$$

where $T_n : k_\pi^n\to k$ the trace. $x_n(\alpha_n,\beta)$ is independent of the choice of λ.

Properties of x_n:

For $\alpha_n,\alpha'_n\in p_n,\ \beta,\beta'\in B$,

(i)

$$x_n(\alpha_n\dot{+}\alpha'_n,\beta) = x_n(\alpha_n,\beta)+x_n(\alpha'_n,\beta),$$
$$x_n(\alpha_n,\beta\beta') = x_n(\alpha_n,\beta)+x_n(\alpha_n,\beta'),$$
$$x_n(a\cdot_f\alpha_n,\beta) = ax_n(\alpha_n,\beta),\ a\in\mathcal{O}.$$

(ii) $x_m(\pi^{m-n}\cdot_f\alpha_n,\beta) = \pi^{m-n}x_n(\alpha_n,\beta),\ 0\leq n\leq m.$

Define $[\ ,\ ]_w : A_f \times B \to W_f$ by

$$(*)\qquad \begin{aligned}[\alpha,\beta]_w &= x_m(\alpha_m,\beta)\cdot_f w_m\\ &= \left[\frac{1}{\pi^{m+1}}T_m(\lambda(\alpha_m)\delta(\beta)_m)\right]_f \cdot w_m\\ &= \left[\frac{1}{\pi^{m+1}}T_m(\lambda(\alpha_m)\frac{1}{\lambda'(w_m)}\frac{t'_\beta(w_m)}{t_\beta(w_m)}\right]_f \cdot w_m\end{aligned}$$

for sufficiently large m, since in view of (ii), α_m represents α and $x_m(\alpha_m,\beta) \in \mathcal{O}$ for sufficiently large m, $(*)$ is independent of m for all sufficiently large m.

Then $[\ ,\ ]_w$ is a pairing and

$$[a\cdot_f \alpha,\beta]_w = a\cdot_f [\alpha,\beta]_w,\ a\in\mathcal{O}.$$

Moreover, if (f',w') is another normed π-sequence and $h : (f,w) \xrightarrow{\sim} (f',w')$, then h induces the isomorphism $F_f \xrightarrow{\sim} F_{f'}$ over $\mathcal{O}$, $\mathcal{O}$-isomorphisms

$$W_f \xrightarrow{\sim} W_{f'},\ A_f \xrightarrow{\sim} A_{f'},\ \text{and } h([\alpha,\beta]_w) = [h(\alpha),\beta]_{w'}.$$

THEOREM (MAIN THEOREM). *For any normed π-sequence of k, $\alpha \in A_f$, $\beta \in B$,*

$$(\alpha,\beta)_f = [\alpha,\beta]_w.$$

Moreover, if α is represented by $\alpha_n \in p_n$, then

$$x_n = \frac{1}{\pi^{n+1}}T_n(\lambda(\alpha_n)\delta(\beta)_n) \in \mathcal{O}$$

and

$$(\alpha,\beta)_f = [\frac{1}{\pi^{n+1}}T_n(\lambda(\alpha_n)\delta(\beta)_n)]\cdot_f w_n.$$

Proof. We may assume $\nu(\beta) = 1$ by using the multiplicativity of 2^{nd} component, since B is generated by all β's with $\nu(\beta) = 1$. Since t_β :

$(f,w) \xrightarrow{\sim} (f_\beta, \beta)$, $h((\alpha,\beta)_f) = (h(\alpha),\beta)_{f'}$, $h([\alpha,\beta]_w) = [h(\alpha),\beta]_{w'}$, it's sufficient to show :

$$(\alpha, w)_f = [\alpha, w]_w \text{ for } (f,w) \text{ a normed } \pi - \text{sequence of } k,$$

which will be proved in the lemma below. For the 2nd statement ; if α is represented by $\alpha_n \in p_n$, then $x_m \in \mathcal{O}$ and

$$(\alpha,\beta)_f = [\alpha,\beta]_w = x_m \cdot_f w_m \text{ for } m \text{ large.}$$

But

$$x_m \cdot_f w_n = (\alpha_n, \beta_n)_{n,f} \in W_f^n \Rightarrow \pi^{n+1} \cdot_f x_m \cdot_f w_m = 0$$
$$\Rightarrow \pi^{n+1} \cdot_f x_m \in p^{m+1} \Rightarrow \pi^{n+1} \cdot_f (\pi^{m-n} x_n) \in p^{m+1} \Rightarrow x_n \in \mathcal{O}.$$

LEMMA. *For (f,w) a normed π-sequence of k, $(\alpha,w)_f = [\alpha,w]_w$ for every $\alpha \in A_f$.*

Proof. Until the end of proof, "$\equiv$ mod π^{an+c}" means

$\exists$ an integer c, independent of n, such that the congruence holds.

Step 1. For a prime element α' of k_π^n, $(\alpha', \alpha')_n = 0$, which is stated before.

Step 2. Since $\alpha_m = \pi^{m-n} \cdot \alpha_n$ for $m \geq n$, $\alpha_n \to 0$ rapidly and hence $\alpha_n \dot{+} w_n$ is a prime element of k_π^n for n large. By step 1 and bimultiplicativity,

$$\begin{aligned} 0 &= (\alpha_n \dot{+} w_n, \alpha_n \dot{+} w_n) \\ &= (\alpha_n \dot{+} w_n, w_n(1+\gamma_n)) \\ &= (\alpha_n, w_n) \dot{+} (\alpha_n, 1+\gamma_n) \dot{+} (w_n, 1+\gamma_n), \\ &\quad \text{if we write } \alpha_n \dot{+} w_n = w_n(1+\gamma_n) \end{aligned}$$

Step 3. For large n, $(\alpha_n, 1+\gamma_n)_n = 0$. Recall that $m \geq n$,

$$(\alpha_m, 1+\gamma_m)_m = (\alpha_n, N_{m,n}(1+\gamma_m))_n.$$

As $m \to \infty$, $\alpha_m \to 0 \Rightarrow \gamma_m \to 0 \Rightarrow N_{m,n}(1+\gamma_m) \to 1$. Since the Artin map is continuous, $(\alpha_m, 1+\gamma_m)_m \to 0$. But for n large, α is represented by α_n and $(\alpha_n, N_{m,n}(1+\gamma_m))_n \in W_f^n$ by definition. Since W_f^n is discrete,

$$(\alpha_m, 1+\gamma_m)_m = 0 \text{ for large } m.$$

Step 4.

$$\begin{aligned}(\alpha_n, w_n)_n &= \dot{-}(w_n, 1+\gamma_n)_n \text{ by step 2 and 3}\\ &= \cdot - [\rho_n(1+\gamma_n)(w_{2n+1}) \dot{-} w_{2n+1}]\end{aligned}$$

(since $\pi^{n+1} \cdot w_{2n+1} = w_n$ and by definition)

$$= w_{2n+1} \dot{-} \rho_k(N_n(1+\gamma_n))(w_{2n+1})$$

(by norm compatibility of Artin map, where $\rho_k : k^X \to \mathrm{Gal}(k_{ab}/k)$)

$$= [1 - N_n(1+\gamma_n)^{-1}] \cdot w_{2n+1}$$

(since ρ_k induces $U(k) \xrightarrow{\sim} \mathrm{Gal}(k_{ab}/k_{ur})$, given by $u \mapsto \delta(u^{-1})$)

Step 5. For $\alpha \in A_f$, $\exists c' = c'(\alpha)$ integer such that for any $n \geq c'$,

$$\alpha \text{ is represented by } \alpha_n \in p_n, \text{ satisfying } \mu(\alpha_n) \geq n - c'.$$

$(*)$ For $\gamma \in m_f$,

$$\mu(\pi \cdot \gamma) \geq \min(\mu(\gamma^q), \mu(\pi\gamma)) = \min(q\mu(\gamma), \mu(\gamma)+1).$$

Since $[\pi]_f \equiv X^q \ (mod p)$, $[\pi]_f = \pi X + \cdots \in X\mathcal{O}[[X]]$.
If $\mu(\gamma) < \frac{1}{q-1}$, then $\mu(\pi \cdot \gamma) \geq q\mu(\gamma)$. Thus

$$(**) \ \exists\, j \geq 0 \text{ such that } \mu(\pi^j \cdot \gamma) \geq \frac{1}{q-1}, \text{ for large } j.$$

By $(*)$ and $(**)$,

$$\mu(\pi^{i+j} \cdot \gamma) \geq \mu(\pi^j \cdot \gamma) + i \geq i, \ i \geq 0.$$

If α is represented by $\alpha_{j'}$, put

$$\gamma = \alpha_{j'},\ c = j + j',\ n = i + j + j'.$$

Step 6. Grant that

$$\mathcal{D}(k_\pi^n/k) = p^{n+1}p_0^{-1}\mathcal{O}_n,$$

p_0 the maximal ideal of $k_\pi^0 \Rightarrow \pi^{-n}\mathcal{O}_n \subset \mathcal{D}(k_\pi^n/k)^{-1}$.

$$\alpha_n \dot{+} w_n = w_n(1+\gamma_n),\ \gamma_n = \frac{\alpha_n}{w_n} + \sum_{i,j\geq 1} c_{ij}\alpha_n^i w_n^{j-1},\ c_{ij} \in \mathcal{O}.$$

Since $\mu(\alpha_n/w_n) < \mu(c_{ij}\alpha_n^i w_n^{j-1})$,

$$\mu(\gamma_n) = \mu(\alpha_n) - \mu(w_n) \geq n - c' - 1,$$

with the c' in step 5.

Put

$$c = 3c' + 3 + e,\ e = \nu(p) \geq 1, \text{ integer.}$$

Assume that n is large enough. Since $\gamma_n \in \pi^{n-c'-1}\mathcal{O}_n$, $T_n(\mathcal{D}(k_\pi^n/k)^{-1}) \subseteq \mathcal{O}$,

$$\begin{aligned} T_n(\gamma_n) &\equiv 0 \ (mod\, \pi^{2n-c'-1}) \\ &\equiv 0 \ (mod\, \pi^{2n-c}) \\ &\equiv 0 \ (mod\, \pi^{n+1}) \end{aligned}$$

Also,

$$\begin{aligned} T_n(\gamma_n^2) &\equiv 0 \ (mod\, \pi^{3n-2c'-2}) \\ &\equiv 0 \ (mod\, \pi^{3n-c}) \end{aligned}$$

Now,

$$\begin{aligned} 1 - N_n(1+\gamma_n)^{-1} &\equiv 1 - \Pi_\sigma(1-\gamma_n+\gamma_n^2)^\sigma \ (\pi^{3n-3c'-3}) \\ &\equiv 1 - \Pi_\sigma(1-\gamma_n+\gamma_n^2)^\sigma \ (\pi^{3n-c}) \\ &\equiv \sum \gamma_n^\sigma - \frac{1}{2}\sum(\gamma_n^2)^\sigma - \frac{1}{2}\sum\sum \gamma_n^{\sigma_1}\gamma_n^{\sigma_2} \ (\pi^{3n-c}) \\ &\equiv T_n(\gamma_n) - \frac{1}{2}T_n(\gamma_n^2) - \frac{1}{2}(T_n(\gamma_n))^2 \ (\pi^{3n-c}) \\ &\equiv T_n(\gamma_n) \ (\pi^{3n-c}) \end{aligned}$$

Step 7. For $\mu(\gamma) \geq e$,

$$\mu(\gamma^j/j) \geq 2\mu(\gamma) - e, \ j \geq 2.$$

If $j = p^a j'$, $a \geq 0$, $(j', p) = 1$, then

$$\mu(\gamma^j/j) = j\mu(\gamma) - \mu(j) = j\mu(\gamma) - ae.$$

If $a = 0$, then it's true. For $a \geq 1$,

$$\begin{aligned} \mu(\gamma^j/j) - 2\mu(\gamma) + e &= (j-2)\mu(\gamma) - (a-1)e \\ &\geq (j-a-1)\mu(\gamma), \text{ and} \end{aligned}$$

$$j - 1 - a \geq p^a - 1 - a \geq 0 \text{ for } a \geq 1.$$

$$\begin{aligned} \alpha_n \dot{+} w_n &= w_n(1+\gamma_n) \Rightarrow \\ &\lambda(\alpha_n) + \lambda(w_n) \\ &= \lambda(w_n(1+\gamma_n)) \\ &= \sum_{i=1}^{\infty} c_i w_n^i \frac{(1+\gamma_n)^i}{i} \\ &= \sum_{i=1}^{\infty} c_i w_n^i (\frac{1}{i} + \gamma_n + \sum_{j=2}^{i} \binom{i-1}{j-1} \frac{\gamma_n^j}{j}) \end{aligned}$$

By the above,

$$\begin{aligned} \mu(\gamma_n^j/j) &\geq 2\mu(\gamma_n) - e \\ &\geq 2(n - c' - 1) - e \end{aligned}$$

and hence

$$\begin{aligned} \lambda(\alpha_n) + \lambda(w_n) &\equiv w_n\gamma_n\lambda'(w_n) + \lambda(w_n) \ (\pi^{2(n-c'-1)-e}) \\ \lambda(\alpha_n) &\equiv w_n\gamma_n\lambda'(w_n) \ (\pi^{2(n-c'-1)-e}) \\ \gamma_n &\equiv \lambda(\alpha_n)/w_n\lambda'(w_n) \ (\pi^{2(n-c'-1)-e-1}) \\ T_n(\gamma_n) &\equiv T_n(\lambda(\alpha_n)\delta(w)_n) \ (\pi^{3n-2c'-e-3}) \\ &\equiv T_n(\lambda(\alpha_n)\delta(w)_n) \ (\pi^{3n-c}), \end{aligned}$$

since $\delta(w)_n = \frac{1}{\lambda'(w_n)w_n} \in p_n^{-1}$.

$$\frac{1}{\pi^{n+1}}T_n(\gamma_n) \in \mathcal{O} \Rightarrow \frac{1}{\pi^{n+1}}T_n(\lambda(\alpha_n)\delta(w)_n) \in \mathcal{O} \text{ and}$$

$\frac{1}{\pi^{n+1}}T_n(\lambda(\alpha_n)\delta(w)_n) \equiv 0\,(\pi^{n+1})$, since n large enough $\Rightarrow 3n-c \geq 2n+2$.

Step 8. By step 4,

$$\begin{aligned}(\alpha_n, w_n)_n &= [1 - N_n(1+\gamma_n)^{-1}] \cdot w_{2n+1} \\ &= T_n(\gamma_n) \cdot w_{2n+1} \\ &= \frac{1}{\pi^{n+1}}T_n(\gamma_n) \cdot \pi^{n+1} \cdot w_{2n+1} \\ &= \frac{1}{\pi^{n+1}}T_n(\gamma_n) \cdot w_n \\ &= \frac{1}{\pi^{n+1}}T_n(\lambda(\alpha_n)\delta(w)_n) \cdot w_n \\ &= [\alpha, w]_w.\end{aligned}$$

References

1. R.Coleman, *Division Values in Local Fields*, Inv. Math. 53 (1979), 91–116.
2. ______, *The Arithmetic of Lubin-Tate Division Towers*, Duke Math. J. 48 (1981), 449–466.
3. ______, *The Dilogarithm and the Norm Residue Symbol*, Bull. Soc. Math. France 109 (1981), 373–402.
4. E.de Shalit, *Relative Lubin-Tate groups*, Proc. of the AMS 95 (1985), 1–4.
5. ______, *The explicit Reciprocity law in Local class field theory*, Duke Math. J. 53 (1986), 163–176.
6. K. Iwasawa, *Explicit formulas for the norm residue symbol*, J. Math. Soc. Japan 20 (1968), 151–164.
7. V.A. Kolyvagin, *Formal groups and the norm residue Symbol*, Izvestija, English trans. in 15 (1980), 289–348.
8. S.V. Vostokov, *Explicit form of the law of reciprocity*, Izvestija, English trans. in vol. 13 (1979), 557–588.
9. ______, *An Explicit Pairing Formula in Formal Modules*, Doklady, English trans. in vol. 19 (1978), 830–833.
10. S. Sen, *On explicit reciprocity laws*, J. Crelle, I: 313 (1980), 1–26, II : 323 (1981), 68–87.
11. A. Wiles, *Higher explcit reciprocity laws*, Ann. of Math. 107 (1978), 235–254.

PRINCIPAL HOMOGENEOUS SPACES

Sung Sik Woo

Contents

§1. Weil-Châtelet (WC) groups

Let G be a commutative algebraic group over a field k. Suppose X is a variety over k on which G operates. Further we assume the G-action is trivial with respect to the "étale site" of spec k, i.e., there is a finite separable extension K of k such that

$$X_K \times G_K \to X_K$$

is isomorphic to the G_K-action on itself. Here G_K denotes the base extension of G to the field K. A variety X over k with an action of a commutative algebraic group G such that it is trivial with respect to the étale site of spec k is called a *principal homogeneous space* (P.H.S) *for G over k.*

Note that the $\bar{k}$-rational points $G(\bar{k})$ of G acts on $X(\bar{k})$ simply and transitively, i.e., for any x, y in $X(\bar{k})$ there is a unique $g \in G(\bar{k})$ such that $Xg = y$. Hence we get a *subtraction* map

$$X(\bar{k}) \times X(\bar{k}) \to G(\bar{k}).$$

We will denote the image of (x, y) by $x^{-1}y$.

Let X_1 and X_2 be two P.H.S's for G over k. We want to define their "sum" ; let $X_1 \overset{G}{\times} X_2$ be the quotient of $X_1 \times X_2$ under the G-action

$$(X_1, X_2)g = (x_1 g^{-1}, x_2 g).$$

We endow a G-action on $X_1 \overset{G}{\times} X_2$ via

$$(x_1, x_2)g = (x_1 g, x_2)(= (x_1, x_2 g)).$$

Then $X_1 \overset{G}{\times} X_2$ becomes a P.H.S [W].

Two P.H.S's X_1 and X_2 are said to be *equivalent* if there is an isomorphism of X_1 onto X_2 defined over k which is compatible with the group action. A P.H.S is *trivial* if it is equivalent to the G-action on itself.

PROPOSITION 1. *The set of all equivalence clases of P.H.S's for G over k form a commutative group.*

Proof. If X is a P.H.S for G. Then we define a P.H.S X^- by modifying the G-action of X;

$$X^- \times G \to X^-$$
$$(g, x) \mapsto xg^{-1}.$$

Then X^- becomes the inverse to X with respect to the sum operation. See [W] for detail.

The group of all equivalence classes of P.H.S's for G over k is called the *Weil-Châtelet* group for G over k, and we denote this group by $WC(G/k)$.

PROPOSITION 2. *A P.H.S X for G over k is trivial if and only if $X(k) \neq \phi$.*

Proof. Suppose X is trivial. Then there is an isomorphism $\varphi : G \to X$ defined over k. The identity $e \in G$ is a k-point by the defenition of an algebraic group. Since φ is defined over k, $\varphi(e)$ is a k-point of X. Conversely suppose p_0 be a k-point of X, then the map

$$\varphi : G \to X$$

defined by $\varphi(g) = p_0 g$ is an isomorphism over k.

Note that any element of $WC(G/k)$ is of finite order. In fact if X is a P.H.S and let $\sum_{i=1}^{n} x_i$ be a positive cycle of dimension 0 which is rational over k. Let X_n be a P.H.S which represents the class nX. Then there is "canonical" map

$$X \times \cdots \times X \to X_n$$

sending $(x_1, \cdots, x_n)$ to a k-rational point of X_n. Hence by the above proposition X_n must be trivial.

THEOREM 1. *Let A be an abelian variety over k and $X \in WC(A/k)$. Then there is an isomorphism*

$$Pic^0(X) \xrightarrow{\cong} A$$

which respects the action of the Galois group $G(\bar{k}/k)$. In particular,

$$Pic^0_k(A) \cong A(k).$$

Proof. (Sketch). The sum map

$$\mathrm{Div}^0(X(\bar{k})) \to A(\bar{k})$$

which sends $\sum_{i=1}^k n_i([P_i] - [P_0])$ to $\sum n_i(P_i - P_0)$ is surjective. The kernel of this map is precisely the principal divisors. And this map respect the $G(\bar{k}/k)$-action.

§2. WC groups and Galois, étale cohomology

In this section we will relate the WC group with various cohomology groups [S,LT].

PROPOSITION 3. *Let X be a P.H.S for G-over k and K/k be a Galois extension such that X_K is trivial. Let $\mathcal{G} = Gal(K/k)$. Then*

$$X \cong G_K/\mathcal{G}.$$

Proof. Consider the fiber product diagram

$$\begin{tikzcd} X_K \arrow[r] \arrow[d] & X \arrow[d] \\ \mathrm{Spec}\, K \arrow[r] & \mathrm{Spec}(k) \end{tikzcd}$$

Since $\mathrm{Spec}\, K \to \mathrm{Spec}\, k$ is Galois with group $\mathcal{G}$, $X_K \to X$ is also Galois with group $\mathcal{G}$. But since $X_K \cong G_K$, we have $X \cong G_K/\mathcal{G}$.

Let K/k be a Golois extension with group $\mathcal{G}$. Let $x \in X(K)$, $\sigma \in \mathcal{G}$. Then using the subtraction map of section 1, we can write

$$x^{-1}x^{\sigma} = g_{\sigma}$$

for some $g_{\sigma} \in G(K)$. The assignment $\sigma \mapsto g_{\sigma}$ defines a 1-cocycle. In fact, $x^{\sigma\tau} = xg_{\sigma\tau}$. On the other hand, we have

$$x^{\sigma\tau} = (x^{\sigma})^{\tau} = (xg_{\sigma})^{\tau} = x^{\tau}g_{\sigma}^{\tau} = xg_{\tau}g_{\sigma}^{\tau}.$$

Hence we have

$$g_{\sigma\tau} = g_{\tau}g_{\sigma}^{\tau}.$$

Therefore we get a map from the set of P.H.S's with a K-rational points to the Galois cohomology group $H^1(K/k, G)$.

PROPOSITION 4. *There is an isomorphism between $H^1(K/k, G(K))$ and the set of P.H.S's for G over k which have K-rational points. In particular,*

$$WC(G/k) \xrightarrow{\simeq} H^1(\bar{k}/k, G).$$

Proof. Let $\mathcal{G}$ be the Galois group Gal(K/k). If $\{g_{\sigma}\}$ is a cocycle, then we define the $\mathcal{G}$-action on G_K by $g\sigma = gg_{\sigma}$. Then the P.H.S we look for is $X = G_K/\mathcal{G}$ (cf. Proposition 3).

Note that we have reprove the fact that $WC(G/k)$ is a torsion group since the Galois cohomology group is torsion [KJ].

Now we relate WC groups with étale cohomology groups [M].

THEOREM 1. *Let $X = Spec(k)$, and let $\mathcal{G} = Gal(\bar{k}/k)$. Then*

$$H^1(X_{\text{ét}}, G) = H^1(\mathcal{G}, G).$$

Proof. There is a categorical equivalence,

$$\{\text{Sheaves on } X_{\text{ét}}\} \leftrightarrow \{\text{Discrete } \mathcal{G} - \text{modules}\};$$

for a sheaf S on $X_{\text{ét}}$ a discrete $\mathcal{G}$-module $\varinjlim S(K)$, where K runs over all finite seperable extension of k, and for a given $\mathcal{G}$-module M, we associate the sheaf S_M on $X_{\text{ét}}$ defined by

$$S_M(K) = M^{\text{Gal}(\bar{k}/K)}.$$

The cohomology group $H^1(X_{\text{ét}}, -)$ and $H^1(\mathcal{G}, -)$ are the right derived functors of $U \mapsto \Gamma(U, S)$ and $M \mapsto M^G$ respectively.

§3. WC groups over a finite field

Throughout this section k will be a finite field of $q = p^n$ elements. We will show that a P.H.S over a finite field is trivial [S2].

Let G be a (commutative) algebraic group over k. Let $\varphi : G \to G$ be the Frobenius map which is given by

$$\varphi(x_0, \cdots, x_n) = (x_0^q, \cdots, x_n^q)$$

in its homogeneous coordinates. Note that this map is not k-linear. In order to make this map to be k-linear we introduce k-scheme structure on G which will be denoted by G_q: As a topological space, G_q is the same as G and if $U \subseteq G_q$ affine open with coordinate ring A, then the k-action on A is givne by

$$(\alpha, f) \mapsto \alpha^q f.$$

Now the map described above becomes k-linear and we denote it by F. We have a commutative diagram,

$$\begin{tikzcd} G \arrow[r, "F"] \arrow[d, "\pi"'] & G_q \arrow[d, "\pi"] \\ \operatorname{Spec} k \arrow[r, "id"] & \operatorname{Spec} k. \end{tikzcd}$$

LEMMA 1. *Let G be a connected algebraic group over k. Then the map of G to G_q sending g to $F(g)g^{-1}$ is surjective.*

Proof. For any $h \in G$, we define.

$$u_h : G \to G,$$

by $u_h(g) = g^{-1}hF(g)$. Note that the differential of F vanishes. Hence $d(u_h) = d(g^{-1})hF(g)$. Therefore $d(u_h)$ is surjective for all h ; u_h is generically surjective. Let aU_h be an open set contained in $u_h(G)$, and let $z \in G$. Since G is connected, we can choose an element t in $U_z \cap U_e$. Writing $t = g^{-1}zFg$, we have $t = h^{-1}F(h)$. Then $z = u^{-1}Fu$ with $u = hg^{-1}$.

PROPOSITION 5. *Every P.H.S X for G over a finite field k is trivial.*

Proof. Let $x \in X$. There is $g \in G(\bar{k})$ such that $x = F(x)g$. By Lemma 1, there is $h \in G$ such that $g = F(h)h^{-1}$. Hence $xh = F(x)F(h)$. On the other hand since $X \times G \to X$ is defined over k, we have $F(x)F(h) = F(xh)$. Hence $xh = F(xh)$. Therefore $xh \in X(k)$.

Next we will prove a stronger result which implies Proposition 5.

THEOREM 2. *Let k be a finite field of q elements and K be a finite extension of k. Let $\mathcal{G} = Gal(K/k)$. Then*

$$H^m(\mathcal{G}, G(K)) = (0) \ \forall\ m \geq 1.$$

Proof. Since $\mathcal{G}$ is cyclic $H^m(\mathcal{G}, G(K))$ depends only on the points of m [KJ]. For $m = 1$, we have to show that every 1-cocycle is of the form $x - x^q$. Let's write g^q the image of g under the Frobenius map. Let $g \in G(K)$ be a cocycle so that

$$(*) \qquad \sum_{\sigma \in \mathcal{G}} g^{\sigma} = g + g^q + \cdots + g^{q^{n-1}} = 0$$

where $n = [K : k]$. Then by Lemma 1, $g = x^q - x$ for some $x \in G(\bar{k})$. Using $(*)$ we see that $x = x^{q^n}$. Hence $x \in G(K)$. That is $H^1(\mathcal{G}, G(K)) = 0$.

Now since $G(K)$ is a finite group and $\mathcal{G}$ is a cyclic group we have that the Herbrand quotient $h(G(K)) = 1$ [KJ]. Therefore $H^2(\mathcal{G}, G(K)) = 0$.

§4. Brauer groups

Let K/k be a Galois extension with group $\mathcal{G}$, and let A be a $\mathcal{G}$-module. Then we have the inflation map

$$H^*(\mathcal{G}/\mathcal{H}, A^{\mathcal{H}}) \xrightarrow{\text{inf}} H^*(\mathcal{G}/\mathcal{H}', A^{\mathcal{H}'})$$

whenever $\mathcal{H} < \mathcal{H}' \Delta \mathcal{G}$ [KJ]. We define the *Brauer group*, $Br(k)$ of a field k to be $\varinjlim H^2(K/k, K^*)$ where the limit is taken over all finite Galois extension of k. Theorem 2 says that the Brauer group of a finite field is trivial.

Let us recall the Wedderban-Artin theorem [S1].

THEOREM 3. *Let A be a finite dimensional k-algebra. Then the following conditions are equivalent.*

(i) *A has no nontrivial two sided ideal and its center is k, i.e., A is a central simple k-algebra.*

(ii) *$A \otimes_k \bar{k} \cong M(n, \bar{k})$ for some n.*

(iii) *$A \cong M(n, D)$ where D is a division algebra with center k.*

Two central simple algebras are said to be *equivalent* if their associated division algebras are k-isomorphic. Let A_k be the set of all equivalence classes of central simple k-algebras. Then A_k becomes an abelian group which is the "classical Brauer group". Of course, the classical Brauer group coincide with the cohomological definition of Brauer group. The standard results on Brauer group are [S1];

(i) If k is algebraically closed then $Br(k) = 0$.

(ii) $Br(\mathbf{R}) = \mathbf{Z}/2\mathbf{Z}$ which is generated by the real quatenion algebra.

(iii) The Brauer group of a p-adic local field is canonically isomorphic to $\mathbf{Q}/\mathbf{Z}$.

§5. Over local fields

When A is an abelian variety over a p-adic local field k, Tate proved [T] that $WC(A/k)$ is isomorphic to the continuous character group of its dual abelian variety $\hat{A}$. Throughout this section *k is a p-adic local field* even though sometimes it is unnecessary.

First we introduce a pairing on zero cycles on abelian varieties [L]. Let A, B be abelian varieties over a field k. Let $Z(A)$ be the group of zero cycles of degree zero, and let $S : Z(A) \to A$ be the sum map. Form an exact sequence,

$$0 \to Y(A) \to Z(A) \xrightarrow{S} A \to 0.$$

Let $D \in \mathrm{Div}(A \times B)$, $\mathcal{A} \in Y(A)$ and $\mathcal{B} \in Z(B)$. We define $D(\mathcal{A})$ to be

$$D(\mathcal{A}) = Pr_B(D.\mathcal{A} \times B)$$

which is a divisor of B. Now if $\mathcal{A} \in Y(A)$ then $D(\mathcal{A})$ is a principal divisor on B, say $D(\mathcal{A}) = (g)$, where g is a rational function on B. We define

$$D(\mathcal{A}, \mathcal{B}) = g(\mathcal{B}) = \prod_b g(b)^{\mathrm{ord}_b(\mathcal{B})}$$

where the product is taken over all support of $\mathcal{B}$. Then we have [L].

THEOREM 4 (LANG'S RECIPROCITY). *For $\mathcal{A} \in Y(A)$, $\mathcal{B} \in Y(B)$, we have*

$$D(\mathcal{A},\mathcal{B}) = {}^tD(\mathcal{B},\mathcal{A}).$$

From this one deduces the Weil's reciprocity law.

COROLLARY (WEIL'S RECIPROCITY). *If f and g are two rational functions on a smooth curve with disjoint support, then*

$$f((g)) = g((f)).$$

Throughout this section we will use the notation A_k to denote the k-rational points of A for typographical reason.

Let α be a class in $WC(A/k)$, $b \in B_k$ and $D \in \mathrm{Div}(A \times B)$. Represent α as a cocycle (a_σ) in $H^1(\mathcal{G}_{K/k}, A_K)$. Now lift a_σ to α_σ in $Z_K(A)$. Then

$$(\delta\alpha)_{\sigma\tau} = \sigma\alpha_\tau - \alpha_{\sigma\tau} + \alpha_\sigma$$

is an element of $Y_K(A)$. Choose a lift $\bar{b}$ in $Z_k(B)$ of $b \in B_k$. We define

$$c_{\sigma,\tau} = D((\delta\alpha)_{\sigma,\tau}, \bar{b}).$$

Then $(c_{\sigma,\tau})$ is a 2-cocycle of $\mathcal{G}_{K/k}$ with values in K^*. Using Lang's recipocity one shows that this is well defined. Summing up, corresponding to $D \in \mathrm{Div}(A \times B)$, we defined a pairing,

$$D : WC(A/k) \times B_k \to H^2(\mathcal{G}, \bar{k}^*)$$

where $\mathcal{G} = \mathrm{Gal}(\bar{k}/k)$.

We have a canonical isomorphism (§4),

$$Br(k) = H^2(\mathcal{G}, \bar{k}^*) \xrightarrow{\simeq} \mathbf{Q}/\mathbf{Z}.$$

In particular, we will take $B = \hat{A} = Pic^0(A)$, and D a Poincaré divisor. Using the isomorphism $H^2(\mathcal{G}, \bar{k}^*) \cong Br(k)$ we have a pairing

$$\langle\ ,\ \rangle : WC(A/k) \times \hat{A}_k \to Q/\mathbf{Z} \xrightarrow{\exp(2\pi i)} \mathbf{C}^*,$$

or

$$h_k : WC(A/k) \to \hat{A}_k^* = \mathrm{Hom}_{\mathrm{cont}}(\hat{A}_k, \mathbf{C}^*).$$

THEOREM 5 (TATE). *If k is a p-adic local field then the map*

$$h_k : WC(A/k) \to \hat{A}_k^*$$

is a isomorphism.

For the rest of this section we sketch Tate's proof of the theorem. We first need

THEOREM 6 (LUTZ-MATTUCK). *Let A be an abelian variety over k of dimension r. Then A_k contains a subgroup A'_k of finite index such that $A'_k \cong \mathcal{O}_k^r$. Further if K/k is a finite Galois extension with group $\mathcal{G}$, then we can choose an isomorphism $A'_K \cong \mathcal{O}_K^r$ as a $\mathcal{G}$-isomorphism.*

Now by [KJ], we have

$$h(A_K) = h(A'_K) = h(\mathcal{O}_K)^r = 1.$$

Hence $[H^1(\mathcal{G}, A_K) : 0] = [H^0(\mathcal{G}, A_K) : 0]$.

For an abelian group X, write $q(X) = [X : mX]/[X_m; 0]$ where X_m is the kernel of $X \xrightarrow{m} X$. Then q is additive with respect to exact sequences and $q = 1$ for a finite abelian group. We have

$$q(A_k) = q(A'_k) = q(\mathcal{O}_k)^r = \frac{1}{|m|_k^r}$$

where $|m|_k = [\mathcal{O}_k : m\mathcal{O}_k]^{-1}$. Since $[(\mathbf{Z}/m\mathbf{Z})^{2r} : 0] = [A_m : 0] = m^{2r}$ if $A_m \subseteq A_k$, we conclude that ;

$$[A_k : mA_k] = (\frac{m^2}{|m|_k})^r \quad \text{if } A_m \subseteq A_k. \tag{1}$$

Consider an exact sequence

$$0 \to A_m \to A \xrightarrow{m} A \to 0$$

on the étale site of spec(k), to get a cohomology exact sequence,

$$\begin{aligned} 0 \to A_m \cap A_k \to A_k \xrightarrow{m} A_k \xrightarrow{\delta} \\ \to WC(A_m/k) \to WC(A/k) \xrightarrow{m} WC(A/k) \to \cdots \end{aligned}$$

Therefore we get a short exact sequence

$$0 \to A_k/mA_k \to WC(A_m/k) \to WC_m(A/k) \to 0$$

Now suppose $A_m \subseteq A_k$, $B_m \subseteq B_k$. Then $\mathcal{G} = \mathrm{Gal}(\bar{k}/k)$ acts trivially on A_m. Hence

$$\begin{aligned} WC(A_m/k) &\cong H^1(\mathcal{G}, A_m) \\ &= \mathrm{Hom}_{\mathrm{Cont}}(\mathcal{G}, A_m) \\ &= \mathrm{Hom}(k^*/k^{*^m}, A_m) \\ &= \mathrm{Hom}(k^*/k^{*^m}, (\mathbf{Z}/mZ)^{2r}). \end{aligned}$$

Hence

$$[WC(A_m/k) : 0] = [k^*; k^{*^m}]^{2r} = (\frac{m^2}{|m|_k})^{2r}$$

since $\mu_m \subseteq k^*$ (This follows from nondegeneracy of Weil's pairing.) Therefore we conclude that

$$(2) \qquad [WC_m(A/k) : 0] = (\frac{m^2}{|m|_k})^r \text{ if } A_m \subset A_k \text{ and } B_m \subset B_k.$$

Now we use,

LEMMA. *Let m be a prime, $A_m \subseteq A_k$, $B_m \subseteq B_k$ and $b \in B_k$. If for any $\alpha \in WC_m(A/k)$ we have $\langle \alpha, b\rangle = 1$, then $b \in mB_k$.*

See [T] for a proof.

For any X we will write X_m (resp. $X(m)$) for the m-torsion (resp. m-primary) part of X.

PROPOSITION 6. *If $A_m \subseteq A_k$ and $B_m \subset B_k$, then $(h_k)_m$ is bijective and $h_k(m)$ is injective.*

Proof. By (1) and (2), the domain and the range of

$$(h_k)_m : WC_m(A/k) \to (B_k^*)_m = (B_k/mB_k)^*$$

have the same number of elements, namely $(m^2/|m|_k)^r$. The above lemma implies that $(h_k)_m$ is injective ; $h_k(m)$ is injective. Hence $(h_k)_m$ is bijective.

Let K/k be a Galois extension with group $\mathcal{G}_K$. We have the commutative diagram

$$\begin{tikzcd}
H^1(\mathcal{G}_K, A_K) \arrow[r, "\inf"] \arrow[d, "h_{K/k}"'] & WC(A/k) \arrow[d, "h_k"'] \\
H^0(\mathcal{G}_K, B_K)^* \arrow[r] & B_k^*
\end{tikzcd}$$

The inf map is injective the map [KJ]. Now interchanging the role of A and B we get

$$\hat{h}_{K/k} : H^1(\mathcal{G}_K, B_K) \to H^0(G, A_K)^*.$$

LEMMA 2. *Let $A_m \subseteq A_k$, $B_m \subseteq B_k$ and K/k be cyclic. Then $h_{K/k}(m)$ and $\hat{h}_{K/k}(m)$ are isomorphisms.*

Proof. Since the map inf and $\hat{h}_{K/k}(m)$ are injective, we have $h_{K/k}(m)$ is injective. Similarly $\hat{h}_{K/k}(m)$ is also injective. The index computation shows that the domain of $h_{K/k}(m)$ and the range of $\hat{h}_{K/k}(m)$ have the same number of elements. Therefore $h_{K/k}(m)$ and $\hat{h}_{K/k}(m)$ are isomorphisms.

LEMMA 3. *Suppose $k \subset K \subset L$ with K/k cyclic and L/k arbitrary Galois. If $h_{K/k}(m)$, $\hat{h}_{K/k}(m)$, and $h_{L/K}(m)$ are bijective, then $h_{L/k}(m)$ is bijective.*

Proof. We apply the five lemma to the m-primary part of the following diagram [KJ].

$$\begin{tikzcd}
0 \arrow[r] & H^1(K/k, A) \arrow[r, "\inf"] \arrow[d, "h_{K/k}"'] & H^1(L/k, A) \arrow[r, "\mathrm{res}"] \arrow[d, "h_{L/k}"'] & H^1(L/K, A)^G \arrow[d, "h_{L/K}"'] \\
0 \arrow[r] & H^0(K/k, B)^* \arrow[r] & H^0(L/k, B) \arrow[r] & (H^0(L/K, B)^*)^G
\end{tikzcd}$$

$$\begin{tikzcd}
{} \arrow[r, "tg"] & H^2(K/k, A) \arrow[r, "\sigma", "\approx"'] \arrow[d, "\hat{h}^*_{K/k}"'] & H^0(K/k, A) \arrow[d, "\hat{h}^*_{K/k}"'] \\
{} \arrow[r, "tg^*"] & H^{-1}(K/k, B) \arrow[r, "\approx", "\sigma-1"'] & H^1(K/k, B)^*
\end{tikzcd}$$

PROPOSITION 7. *If L/k is a Galois extension and if $A_m \subseteq A_k$, $B_m \subseteq B_k$, then $h_{L/k}(m)$ is an isomorphism.*

Proof. Local Golois groups are solvable.

Now we get rid of our assumptions that $A_m \subseteq A_k$, $B_m \subseteq B_k$ using $K = k(A_m, B_m)$.

PROPOSITION 8. *The map $h_k(m)$ is surjective.*

Proof. See [T].

LEMMA 4. *Suppose K/k is cyclic. If $h_K(m)$ and $\hat{h}_K(m)$ are injective, then $h_k(m)$ and $\hat{h}_k(m)$ are injective.*

Proof. Let $\mathcal{G} = \mathrm{Gal}(K/k)$. Consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & H^1(\mathcal{G}, A_K) \arrow[r, "\mathrm{inf}"] \arrow[d, "h_{K/k}"'] & WC(A/k) \arrow[r, "\mathrm{res}"] \arrow[d, "h_k"'] & WC(A/K) \arrow[d, "h_K"'] \\
0 \arrow[r] & H^0(\mathcal{G}, B_K)^* \arrow[r] & B_k^* \arrow[r] & B_K^*
\end{tikzcd}$$

Since $h_k(m)$ is surjective and $h_K(m)$ is injective we see that $h_{K/k}(m)$ is surjective. Similarly, we also have that $\hat{h}_{K/k}(m)$ is surjective. Now the index argument shows that $h_{K/k}(m)$ and $\hat{h}_{K/k}$ are injective. Daigram chasing shows that injectivity of $h_k(m)$ follows from that of $h_K(m)$. Similarly for $\hat{h}_k(m)$.

Now apply the above lemma to $K = k(A_m, B_m)$ to prove our assertion of the theorem that $WC(A/k) \cong (\hat{A}_k)^*$.

§6. Shafarevich groups and duality

Throughout this section K will be a mumber field. Let M_K be the set of all places of K (including the places at infinity). The *Shafarevich group* Ш(A/K) is defined by

$$Ш(A/K) = \mathrm{Ker}(WC(A/K) \to \prod_{v \in M_K} WC(A/K_v))$$

where K_v is the local field at v. The Shafarevich group measures the failure of the Hasse principle.

A conjecture asserts that the group $\text{Ш}(A/K)$ is finite. Rescently, people found many examples of elliptic curves whose Ш group is finite.

In 1962, Tate [T1] (Cassels for elliptic curves) defined an alternating pairing

$$\text{Ш}(A/K) \times \text{Ш}(\hat{A}/K) \to \mathbf{Q}/\mathbf{Z}$$

and showed that its kernel is the divisible elements. We will sketch the construction of the pairing following [M1].

We will return to our convention to denote X_F for the base extension of X to F for F/K.

Let $a \in \text{Ш}(A/K)$. Represent a by a P.H.S X over K. We form an exact sequence

$$0 \to \bar{K}^* \to \bar{K}(X)^* \to Q \to 0,$$

where Q is defined to be the cokernel of $\bar{K}^* \to \bar{K}^*(X)$. Taking cohomology we have a commutative diagram,

$$\begin{tikzcd}
 & Br(K) \arrow[r] \arrow[d] & H^2(\mathcal{G}_K, \bar{K}(X)^*) \arrow[r] \arrow[d] & H^2(\mathcal{G}_K, Q) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \oplus_r Br(K_v) \arrow[r] & \oplus_v H^2(\mathcal{G}_v, \bar{K}_v(X)^*) \arrow[r] & \oplus_v H^2(\mathcal{G}_v, Q) &
\end{tikzcd}$$

The zero at the top right comes from the fact that $H^r(\mathcal{G}_K, \bar{K}^*) = 0$ if r is odd bigger than 2. The zero at the lower left follows by composing the injections,

$$Br(K_v) \to Br(X_{K_v}) \to Br(K_v(X));$$

injectivity of the first map follows from local triviality of X and injectivity of the second is a general theorem.

Now consider the other part of the exact sequence

$$0 \to Q \to \mathrm{Div}^0(X_{\bar{K}}) \to \mathrm{Pic}^0(X_{\bar{K}}) \to 0.$$

This yields the diagram,

$$\begin{tikzcd}
{} \arrow[r] & H^1(\mathcal{G}_K, \mathrm{Div}^0(X_{\bar{K}})) \arrow[r] & H^1(\mathcal{G}_K, \mathrm{Pic}^0(X_{\bar{K}})) \arrow[r] \arrow[d, equal] & H^2(\mathcal{G}_K, Q) \arrow[r] \arrow[dd] & {} \\
 & & \text{Ш}(A/K) = H^1(\mathcal{G}_K, \hat{A}_{\bar{K}}) \arrow[d] & & \\
 & {} \arrow[r] & \oplus H^1(\mathcal{G}_v, \hat{A}) \arrow[r] & \oplus H^2(\mathcal{G}_v, Q) \arrow[r] & 0
\end{tikzcd}$$

Let $a' \in \text{Ш}(\hat{A}/K)$. Send it to b' in $H^2(\mathcal{G}_K, Q)$. Then in the first diagram, we can lift it to $b'' \in H^2(\mathcal{G}_K, \bar{K}(X)^*)$ and send it to $b''' \in \oplus H^2(\mathcal{G}_v, \bar{K}_v(X)^*)$. By local triviality of X, it comes from $\oplus_v c_v \in \oplus_v B_r(K_v)$. We can view c_v as an element of $\mathbf{Q}/\mathbf{Z}$ (§4). Finally we define

$$\langle a, a' \rangle = \sum_v c_v \in \mathbf{Q}/\mathbf{Z}.$$

THEOREM 7 (TATE). *The pairing*

$$\langle\ ,\ \rangle : \text{Ш}(A/K) \times \text{Ш}(\hat{A}/K) \to \mathbf{Q}/\mathbf{Z}$$

is alternating and its kernel consists of all divisible elements of Ш *group, i.e., if $\langle a, a' \rangle = 0$ for all a' then there is an arbitrary large integer N and $b \in \text{Ш}(A/K)$ such that $a = Nb$.*

References

[KJ] Jae Moon Kim, *Note on cohomology*, in this volume.

[L] S.Lang, *Abelian varieties*, Springer-Verlag, 1983.

[LT] S.Lang and J.Tate, *Principal homogeneous spaces over abelian varieties*, A.J.M. 80, 1958.

[M] J.S.Milne, *Étale cohomology*, Princeton University Press, 1980.

[M1] ———, *Arithmetic duality theorems*, Academic Press, 1986.

[S] J.P.Serre, *Espaces fibrés algébriques*, Séminaire C.Chevalley 2e année, 1958.

[S1] ———, *Local fields*, Springer-Verlag 1979.

[S2] ———, *Algebraic groups and class fields*, Springer-Verlag, 1988.

[T] J.Tate, *WC groups over p-adic fields*, Séminaire Bourbaki, 1957.

[T1] ———, *Duality theorems in Galois cohomology over number fields*, Proc. Intern, Cong. Math. Stockholm, 1962.

[W] A.Weil, *On algebraic groups and homogeneous spaces*, A.J.M. Vol. 77, 1955.

Department of Mathematics
Ewha Womans University
Seoul 120-750, Korea

ELLIPTIC CURVES

SUNG SIK WOO

Contents

I. Generalities

A. Cubic equations and elliptic curves

Let k be a field of char $k \neq 2, 3$. Usually k will be a number field, the field of complex numbers or a finite field. Using linear coordinate changes we can reduce a cubic polynomial to the form,

$$(1) \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \ a_i \in \bar{k},$$

which we call a *Weierstrass form.* We will say that the cubic given by the equation (1) is defined over k if $a_i \in k$. We can reduce this equation, by substuting y into $(1/2)(y - a_1x - a_3)$ and completing the square, to

$$(1') \qquad y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

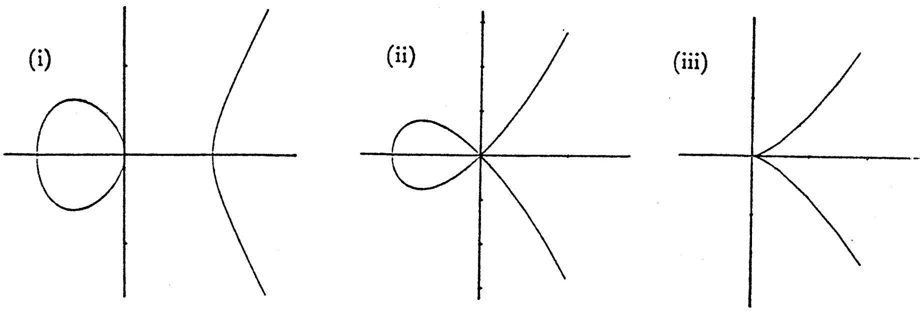
Further, we can replace (x, y) by $(\frac{x-3b_2}{36}, \frac{y}{216})$ to get

$$(2) \qquad y^2 = x^3 + 27c_4x - 54c_6.$$

If k is algebraically closed, we may rewrite (1) in the following forms,

$$(3) \qquad \begin{aligned} &\text{(i) } y^2 = x(x-1)(x-\lambda), \ \lambda \neq 0, 1 \ (\textit{Legendre form.}) \\ &\text{(ii) } y^2 = x^2(x+1) \\ &\text{(iii) } y^2 = x^3. \end{aligned}$$

When $k = \mathbf{R}$, we can sketch the graphs;



(Warning : One should not depend too heavely on these pictures.)

We want to "compactify" the zero set of these cubic equations. For this, we view these cubic equations defined on

$$\mathbf{P}_k^2 = \{(X:Y:Z) \in k^3 - (0,0,0) | (X:Y:Z) = (\alpha X:\alpha Y:\alpha Z), \alpha \in k^*\},$$

which is "compact". (Indeed, $\mathbf{P}_{\mathbf{C}}^2$ is compact.) Now we homogenize the cubic equation ; for example, (2) becomes,

$$\text{(2')} \qquad Y^2Z = X^3 - 27c_4XZ^2 - c_6Z^3,$$

and (3)(i) becomes,

$$\text{(3')} \qquad Y^2Z = X(X-Z)(X-\lambda Z),\ \lambda \neq 0,1.\ \mathit{ets..}$$

If f is a homogeneous cubic, then $f(\alpha P) = \alpha^3 f(P)$ for $P = (P_0, P_1, P_2)$ and $\alpha \neq 0$. Hence the zero set of a homogeneous cubic is well defined and being a closed subset of a compact set it is again compact. We notice that $\mathbf{P}_k^2$ is gotten by adding the line at ∞,

$$L_\infty = \{(X:Y:Z) \in \mathbf{P}^2 \,|\, Z = 0\}$$

to the affine plane $\mathbf{A}^2$. In fact, $\mathbf{P}_k^2 - L_\infty = \{(X:Y:1) \in \mathbf{P}^2\} = \mathbf{A}^2$. The cubic equations are chosen so that they intersect L_∞ at just one point $(0:1:0)(=\infty)$, with multiplicity 3.

The zero set of the eq. (2') in $\mathbf{P}^2$ is called an *elliptic curve* over k provided $\Delta = (c_4^3 - c_6^2)/1728 \neq 0$ (we do not need to assume char $k \neq 2,3$). The condition on Δ is equivalent to that the cubic curve $F = 0$ is nonsingular i.e., $F_X(P) \neq 0$ or $F_Y(P) \neq 0$ for all P on the curve. If $k = \mathbf{C}$, one can use implict function theorem to prove that a nonsingular curve is a one dimensional complex (orientible) manifold. Also this is equivalent to that F can be reduced into (3') with $\lambda \neq 0, 1$.

B. j-invariant

We say that two elliptic curves E, E' are *isomorphic* over k if one can transform the equation of E to that of E' by linear change of coordinates over k. There is an easy criterion for two elliptic curves to be isomorphic; we define

$$j(E) = c_4^3/\Delta \text{ in (2') and}$$

$$j(E) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2} \text{ in (3')},$$

which we call that *j-invariant* of an elliptic curve E. Elliptic curves are classified by their j-invariants [S,H].

THEOREM. *Two elliptic curves are isomorphic (over $\bar{k}$) if and only if they have the same j-invariant. Futher, if $j \in \bar{k}$, then there exists an elliptic curve E defined over $k(j)$ such that $j = j(E)$.*

The above theorem says when k is algebraically closed, the moduli space of elliptic curves is $k(= \mathbf{A}_k^1)$.

EXAMPLES. (1) $y^2 + y = x^3$, $\Delta = -27$, $j = 0$.
(2) $y^2 = x^3 + x$, $\Delta = -64$, $j = 1728 = 2^6 3^3$.
Hence, in char $k \neq 2, 3$, these are elliptic curves and they are not isomorphic.
(3) (The Fermat curve.) $X^3 + Y^3 = Z^3$, $\Delta = -1/27$, $j = 0$. (Replace X by $x + z$ and set $x = -1/3$ to get $z^2 - (1/3)z = y^3 - 1/27$ which is the form (1).)

Hence, the elliptic curves (1) and (3) are isomorphic if char $k \neq 2, 3$.

C. Group structure on elliptic curves

We can give a group structure on an elliptic curve. For this we use, the Bezout's theorem [F] when k is algebraically closed.

THEOREM. *If k is algebraically closed, two curves (i.e., zero set of a homogeneous polynomial in $\mathbf{P}^2$) of degree m, n resp. intersect exactly at mn points counting multiplicities, if they do not "overlap".*

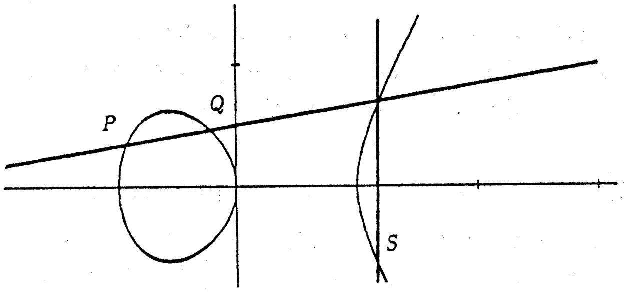
A *rational function* is a quotient of two homogeneous polynomials of the same degree. Hence, it is a well defined function on $\mathbf{P}^2$ provided its denominator is not zero.

COROLLARY. *The number of zeros of a rational function is the same as number of poles on a curve.*

To define a group structure on an elliptic curve E we choose a base point $O = (0 : 1 : 0)$, the point at ∞ which will play the role of identity. For P, Q on E, let us denote the line in $\mathbf{P}^2$ passing through P and Q by L_{PQ}. Then, by Bezout, L_{PQ} intersect with E at the third point, say R. And L_{OR} intersect at the third point S. Now we define,

$$[P] + [Q] = [S].$$

One checks [F,S] that this operation is associative and commutative.



The group law on a cubic curve

We can view L_{PQ}, L_{OR} as a "function" on $\mathbf{P}^2$. Consider $f = L_{PQ}/L_{OR}$ (this is indeed a function). Then,

$$(f)_0 = (\text{the zero set of } f \text{ on } E) = P + Q + R,$$
$$(f)_\infty = (\text{the pole set of } f \text{ on } E) = R + O + S.$$

Hence we get,

$$\text{div}(f) = (\text{divisor of } f) = (f)_0 - (f)_\infty \doteq P + Q - S - O = 0.$$

Thus, $[P] + [Q] = [S]$ implies that $P + Q - S - O$ is a divisor of the rational function $f = L_{PQ}/L_{OR}$.

Even if k is not algebraically closed, one can show that the set of k-points,

$$E(k) = \{(X : Y : Z) \in E \,|\, X, Y, Z \in k\}$$

is also a group.

II. Complex elliptic curve

Throughout this chapter k will be the field of complex numbers $\mathbf{C}$. Let C be a nonsingular curve given by a homogeneous polynomial of degree n in $\mathbf{P}^2$. Then, as in the case of an elleptic curve it is a two dimensional real orientible manifold. Its genus g can be easily computed by the formula,

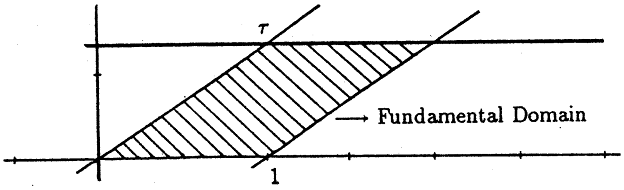
$$g = \frac{(n-1)(n-2)}{2}.$$

Hence if $n = 3$, we get $g = 1$. Topologically, we know that genus 1 (orientable) two dimensional manifold is a torus.

THEOREM (RIEMANN'S EXISTENCE THEOREM). *Every complex one dimensional manifold (=Riemann surface) is an algebraic curve. I.e., it is given by zeros of polynomial equations.*

A. Elliptic functions, Weierstrass p-function

A complex torus is given by $\mathbf{C}/\Lambda$, where $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$, $\omega_i \in \mathbf{C}$. One can normalize the generators $[\omega_1, \omega_2]$ for the lattice so that it becomes $[1, \tau]$ with $\mathrm{Im}(\tau) > 0$.



An ***elliptic function*** is a complex meromorphic function (i.e., it has Laurent series expansion at every point) such that $f(z+\omega) = f(z)$ for all lattice point ω in $\mathbf{Z} + \tau\mathbf{Z}$.

We notice that the set of all elliptic functions form a field. Also, notice that if an elliptic function has no pole then it is a constant. In fact, if it has no pole it is bounded on a fundamental domain, and the periodicity implies that it is bounded on $\mathbf{C}$. Liouville theorem says it must be a constant. Furthermore, residue theorem says that an elliptic function has at least a pole of order 2.

An example of an elliptic function is the Weierstrass p-function [A];

$$\mathbf{p}(z) = \frac{1}{z^2} + \sum{}'(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2})$$

where $\sum'$ denote the summation over all $\omega \in \Lambda - \{0\}$. Its derivative is

$$\mathbf{p}'(z) = \sum_{\omega \in \Lambda} \frac{-2}{(z-\omega)^3},$$

and the Laurent series expansion of $\mathbf{p}'(z)$ at 0 is given by

$$\mathbf{p}'(z) = (-2)/z^3 + 6s_4 z + 20 s_6 z^3 + \cdots$$

which is also elliptic. (Of course, one needs to check the convergence.)

Let $g_2 = 60s_4$ and $g_3 = 140s_6$. Then $g_2 = 60\sum'(1/\omega^4)$, and $g_3 = 140\sum'(1/\omega^6)$. We have [A,L], THEOREM. *The field of meromorphic functions is* $\mathbf{C}(\mathbf{p}(z), \mathbf{p}'(z))$ *with the relation,*

$$(\mathbf{p}'(z))^2 = 4(\mathbf{p}(z))^3 - g_2\mathbf{p}(z) - g_3.$$

This is the cubic equation for an elliptic curve we would like to have. Using this we will explain why Riemann's existence theorem should be true in case of an elliptic curve; consider the map

$$\mathbf{C}/\Lambda \to \mathbf{P}^2$$
$$z \to (\mathbf{p}(z) : \mathbf{p}'(z) : 1).$$

This map is well defined for all z except on the pole set of $\mathbf{p}$ and $\mathbf{p}'$. One can prove that this map induces a bijection of $\mathbf{C}/\Lambda$ onto the zero set of $y^2 = 4x^3 - g_2x - g_3$ in $\mathbf{P}^2_{\mathbf{C}}$, and the natural group structure on $\mathbf{C}/\Lambda$ is the same as the previous one on an elliptic curve. In this case, the j-invariant becomes

$$j(\tau) = 1728\,\frac{g_2^3}{\Delta}, \text{ where } \Delta = g_2^3 - 27g_3^2.$$

B. Abel's theorem

We saw that a meromorphic function has the same number of zeros as its poles. Hence, we can write its divisor as

$$\operatorname{div}(f) = \sum_{i=1}^{n}((P_i) - (Q_i)),\ P_i, Q_i \in \mathbf{C}.$$

What is the necessary and sufficient condition for a divisor $\sum((P_i) - (Q_i))$ to be a divisor of a meromorphic (=rational) function ?

THEOREM (ABEL). *A divisor* $\sum_{i=1}^{n}((P_i)-(Q_i))$ $(n \geq 1)$ *is a divisor of a meromorphic function if and only if* $\sum P_i = \sum Q_i$ *modulo the lattice* Λ.

For a proof of this theorem we refer [F].

III. Arithmetic aspects

A. Rational points

Let K be a number field (a finite extention of $\mathbf{Q}$, so you may think $K = \mathbf{Q}$) and let A be the ring of integers (in case $K = \mathbf{Q}$, $A = \mathbf{Z}$). Suppose E is an elliptic curve whose defining equation has coefficients in K. Then, our question is "how many solutions with coordinates in K are there?" The solutions in K-coordinates are called the *K-points* of E and is denoted by $E(K)$. We first have [S],

THEOREM (MODELL-WEIL). *If E is an elliptic curve defined over a number field K, then the group of K-points on E is an abelian group of finite rank.*

EXAMPLES. (1) Since Fermat's theorem is known to be true for $n = 3$, we know $X^3 + Y^3 = Z^3$ has three $\mathbf{Q}$-points; $(1 : -1 : 0)$, $(1 : 0 : 1)$ and $(0 : 1 : 1)$. Hence, the group of $\mathbf{Q}$-points is $\mathbf{Z}/3\mathbf{Z}$.

(2) If E is given by $y^2 + y = x^3 - x$, then $E(\mathbf{Q}) = \mathbf{Z}$, [H, p.336].

In general, computing such group is very difficult. Examples of elliptic curves so far we found, have rank at most 12. A conjecture asserts that there exist elliptic curves E such that the rank of $E(\mathbf{Q})$ is arbitrarily large.

In contrast to the results of elliptic curves, in 1983, Faltings (Inv. Math. 1983) proved the Modell's conjecture:

THEOREM. *If C is a nonsingular curve defined over a number field K, and if the genus is bigger than 1 (e.g., a plane curve whose degree is bigger than 3), then C has only finitely many K-points.*

B. Integral points

When an affine elliptic curve (=nonsingular cubic in x, y) is defined over a ring of integers A, how about the solutions with coordinats in A?

THEOREM (SIEGEL). *If a nonsingular cubic in two variables is defined over A, then it has only finitely many solutions with coordinates in A.*

C. Elliptic curve over a finite field

Suppose an elliptic curve E is defined over A, the ring of integers. Let $\mathbf{p}$ be a prime ideal of A, then $A/\mathbf{p}$ is a finite field k with $q = p^n$ elements. We can reduce the cubic equation mod. $\mathbf{p}$ to get E' over k. (This corresponds to looking at a fiber of a certain map.) The reduced elliptic curve E' may or may not be nonsingular. However, if E' is nonsingular, we have [S].

THEOREM (E. ARTIN, HASSE). *The number of k-points on E' is given by the formula,*

$$\#(E'(k)) = 1 - Tr(\pi) + q,$$

where π is the Frobenius endomorphism. It differs from $1 + q$ by at most $2\sqrt{q}$.

References

[A] Ahlfos, *Complex analysis*, Ch.7, McGraw-Hill, 1979.
[F] Fulton, *Algebraic curves*, Ch.5, Sec.6, Benjamin, 1969.
[H] Harsthone, *Algebraic geometry*, Ch.4, Sec.4, Springer-Verlag, 1977.
[L] Lang, *Elliptic functions*, Addison-Wesley, 1973.
[S] Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 1986.
[T] Tate, *The arithmetic of elliptic curves*, Inv. Math. 23, 1974.

Department of Mathematics
Ewha Womans University
Seoul 120-750, Korea