Osaka University Knowledge Archive

Title	Integral representations of unramified Galois groups and matrix divisors over number fields
Author(s)	Morishita, Masanori
Citation	Osaka Journal of Mathematics. 1995, 32(3), p. 565-575
Version Type	VoR
URL	https://doi.org/10.18910/10928
rights	
Note	

Osaka University Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

Osaka University

Morishita, M.
Osaka J. Math.
32 (1995), 565-576

INTEGRAL REPRESENTATIONS OF UNRAMIFIED GALOIS GROUPS AND MATRIX DIVISORS OVER NUMBER FIELDS

MASANORI MORISHITA

(Received October 13, 1993)

Introduction

The purpose of the present note is to pursue some analogies for number fields after the model of A. Weil's work [13].

Weil ([13]) studied the space of representations of the fundamental group of a curve and showed it has a structure of an algebraic variety, as a generalization of the Jacobian variety, by employing his generalized Riemann-Roch theorem for matrix divisors. He used the Poincaré zeta (theta) Fuchs functions in order to attach matrix divisor classes to representations of the fundamental group. This process may be regarded as a sort of non-abelian Kummer theory. Actually, we may observe that the "Poincaré sum" in Hilbert's theorem 90 plays an analogous role to the Poincaré zeta (theta) Fuchs function.

Following the principle on the analogy between number fields and function fields ([14]), we would like to discuss some analogies, for number fields, of the function field case described as above. In Section 1, we introduce matrix divisors for number fields. A version of the Riemann-Roch theorem for them is then known as the Poisson summation formula ([11], 4.2). So, this section has totally expository nature. In Section 2, we will attach matrix divisor classes to integral, unitary representations of unramified Galois groups by means of Hilbert's theorem 90 for the general linear group and see some general properties. In Section 3, we discuss an example.

NOTATION. $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$ and $\boldsymbol{C}$ denote the ring of rational integers, the fields of rational, real and complex numbers respectively. For a number field K of finite degree over $\boldsymbol{Q}$, we use the following notation.
$\mathcal{O}_K$: =the ring of integers in K.
X_K : =Spec($\mathcal{O}_K$) together with the structure sheaf $\mathcal{O}_{X_K}$
X_K° : =the set of closed points of X_K=the set of finite places of K.
X_K^∞ : =the set of complex conjugation classes of the embeddings of K into $\boldsymbol{C}$=the set of infinite places of K.

$\bar{X}_K$: $=X_K \cup X_K^\infty$.
K_v : =the completion of K at $v \in X_K^\circ \cup X_K^\infty$.
$\mathcal{O}_v$: =the ring of integers in K_v for $v \in X_K^\circ$.
$\kappa(v)$: =the residue field of $\mathcal{O}_v$
$\boldsymbol{A}_K$: =the adele ring of K.
$\boldsymbol{A}_K^\infty$: $=\prod_{v \in X_K^\circ} \mathcal{O}_v \times \prod_{v \in X_K^\infty} K_v$.
$R^\times$: =the group of invertible elements in a ring R.
h_K : =the class number of K.
$\tilde{K}$: =the maximal unramified extension of K.

1. Matrix divisors for number fields

Thoughout this section, a number field K of finite degree over $\boldsymbol{Q}$ will be fixed and so the subscript K will be omitted often.

1.1. Let GL_n denote the general linear group of rank n over K and $GL_n(\boldsymbol{A})$ denote its adele group. We take the standard maximal compact subgroup $U_n(K_v)$ of $GL_n(\mathcal{O}_v)$: $U_n(K_v)=GL_n(\mathcal{O}_v)$ if $v \in X^\circ$, $O(n)$ (orthogonal group) if $K_v \simeq \boldsymbol{R}$, $U(n)$ (unitary group) if $K_v \simeq \boldsymbol{C}$, and set $U_n(\boldsymbol{A})$: $=\prod_v U_n(K_v)$.

We call a coset $D=div(a)=aU_n(\boldsymbol{A}) \in GL_n(\boldsymbol{A})/U_n(\boldsymbol{A})$, $a \in GL_n(\boldsymbol{A})$, a divisor of rank n over $\bar{X}$. For $\alpha \in GL_n(K)$, call $\alpha U_n(\boldsymbol{A})$ a principal divisor, where $GL_n(K)$ is embedded into $GL_n(\boldsymbol{A})$ diagonally. Two divisors D and D' of rank n are equivalent if there is $\alpha \in GL(K)$ so that $\alpha D=D'$. The set of divisor classes of rank n on $\bar{X}$ is the double coset space $GL_n(K)\backslash GL_n(\boldsymbol{A})/U_n(\boldsymbol{A})$ which is denoted by $Cl_n(\bar{X})$ for simplicity. We set $Cl(\bar{X})$: $=\bigcup_{n \geq 1} Cl_n(\bar{X})$.

The set $Cl(\bar{X})$ has natural operations. For two divisors $D_1=div(a_1)$ of rank n_1 and $D_2=div(a_2)$ of rank n_2, the sum $D_1 \oplus D_2$ and $D_1 \otimes D_2$ are well defined to be the divisors $div(a_1 \oplus a_2)$ of rank n_1+n_2 and $div(a_1 \otimes a_2)$ of rank $n_1 n_2$ respectively, and both operations are associative. Those of divisor classes are commutative and distributive. The dual $D^\vee$ of $D=div(a)$ is $div({}^t a^{-1})$ and the i-th exterior power $\wedge^i D$ is $div(\wedge^i a)$. The degree of $D=div(a)$, $a \in GL_n(\boldsymbol{A})$, is well defined to be $deg_K(D):=\|\wedge^n a\|_K=\|\det(a)\|_K$, where $\| \ \|_K$ stands for the idele volume. Owing to the product formula, the degree of a principal divisor is 1 and so the degree is a continuous function on $Cl_n(\bar{X})$ with values in positive real numbers. For degrees of the sum and product, we have $deg(D_1 \oplus D_2)= deg(D_1)deg(D_2)$, $deg(D_1 \otimes D_2)=deg(D_1)^{n_2} deg(D_2)^{n_1}$. We set $Cl(\bar{X})_1$: $=\bigcup_{n \geq 1} Cl_n(\bar{X})_1$, $Cl_n(\bar{X})_1$=the degree 1 part of $Cl_n(\bar{X})$.

1.2. We note that the set $Cl_n(\bar{X})$ is much bigger than the usual class set of GL_n over K, $Cl_n(X)$: $=GL_n(K)\backslash GL_n(\boldsymbol{A})/GL_n(\boldsymbol{A}^\infty)$. Actually, the strong

approximation property of the special linear group ([2]) implies that the determinant induces a bijection $Cl_n(X) \simeq Cl_1(X)$=the ideal class group of K. On the other hand, to see the structure of $Cl_n(\bar{X})$, let $\{g_i\}(1 \leq i \leq h_K)$ be a set of complete representatives of $Cl_1(X)$. We then have a decomposition

$$GL_n(\boldsymbol{A}) = \bigcup_{i=1}^{h} GL_n(K) g_i GL_n(\boldsymbol{A}^\infty),\ g_i = \mathrm{diag}(g_i, 1, \cdots, 1).$$

Put $\Gamma_i = GL_n(K) \cap g_i GL_n(\boldsymbol{A}^\infty) g_i^{-1}$. By sending the class of $((a_v)_{v \in X^\infty}, (g_{iv})_{v \in X^\infty})$ in $GL_n(K) \backslash GL_n(K) g_i GL_n(\boldsymbol{A}^\infty)/U_n(\boldsymbol{A})$ to $\Gamma_i(a_v) \prod_{v \in X^\infty} U_n(K_v)$, we obtain

$$Cl_n(\bar{X}) \simeq \bigcup_{i=1}^{h} \Gamma_i \backslash \mathcal{H}_n,$$

where $\mathcal{H}_n = \prod_{v \in X^\infty} GL_n(K_v)/U_n(K_v)$.

Let $Cl_n(\bar{X})_1$ denote the degree 1 part of $Cl_n(\bar{X})$. In particular, $Cl_1(\bar{X})$, which should be the analogous object, in our context, of the Jacobian variety of a curve, is rh-dimensional real torus ($r = \#X^\infty - 1$) by the Dirichlet unit theorem.

1.3. It is not difficult to interpret a matrix divisor as a transition matrix of a hermitian vector bundle on $\bar{X}$. A hermitian vector bundle on $\bar{X}$ is a pair$(\mathcal{E}, <\ ,\ > = \{<\ ,\ >_v\}_{v \in X^\infty})$, where $\mathcal{E}$ is a locally free $\mathcal{O}_X$-module of rank n and $<\ ,\ >_v$ is a positive definite hermitian form on the n-dimensional K_v-vector space $\mathcal{E} \otimes_{\mathcal{O}_X} K_v$ for each $v \in X^\infty$, which is preserved under the complex conjegation. Two hermitian bundles $(\mathcal{E}_1, <\ ,\ >_1)$ and $(\mathcal{E}_2, <\ ,\ >_2)$ are isometric if there is an isomorphism $\mathcal{E}_1 \xrightarrow{\sim} \mathcal{E}_2$ preserving the hermitian forms for the induced K_v-linear map $\mathcal{E}_1 \otimes K_v \xrightarrow{\sim} \mathcal{E}_2 \otimes K_v$ for each $v \in X^\infty$. Denote by $Pic_n(\bar{X})$ the set of isometry classes of hermitian vector bundles of rank n on $\bar{X}$ and put $Pic(\bar{X}) := \bigcup_{n \geq 1} Pic_n(\bar{X})$. $Pic(\bar{X})$ also has operations such as sum, product, dual and exterior power. The correspondence between $Cl_n(\bar{X})$ and $Pic_n(\bar{X})$ is given as follows;

$Cl_n(\bar{X}) \to Pic_n(\bar{X})$: Take a divisor $D = div(a)$, $a \in GL_n(\boldsymbol{A})$. For an open subset U of X, set $\Gamma(U, \mathcal{E}) := K^n \cap (\prod_{v \in U^\circ} a_v \mathcal{O}_v^n)$. Then, $\mathcal{E}$ is a locally free $\mathcal{O}_X$-module of rank n. The hermitian form $<\ ,\ >_v$ on $\mathcal{E} \otimes K_v = K_v^n$, $v \in X^\infty$ is defined by $<x, y>_v := <a_v^{-1}x, a_v^{-1}y>_{0,v}$ where $<\ ,\ >_{0,v}$ is the trivial form defined by $<x, y>_{0,v} := \sum_{i=1}^n x_i \bar{y}_i$ for $x = (x_i)$, $y = (y_i) \in K_v^n$.

$Pic_n(\bar{X}) \to Cl_n(\bar{X})$: Take a hermitian vector bundle $(\mathcal{E}, <\ ,\ >)$ of rank n over $\bar{X}$. Let $V := \mathcal{E} \otimes_{\mathcal{O}_X} K$ be the generic fibre together with a basis $u_1, \ldots, u_n$. Note that $\mathcal{E}_v := \mathcal{E} \otimes \mathcal{O}_v$ is a free $\mathcal{O}_v$-module of rank n for each $v \in X^\circ$ which is a $\mathcal{O}_v$-lattice in $V \otimes K_v$. Choosing $\mathcal{O}_v$-basis $e_v^1, \cdots, e_v^n$ of $\mathcal{E}_v$ for $v \in X^\circ$, and K_v-orthonormal basis $e_v^1, \cdots, e_v^n$ of $V \otimes K_v$ with respect to $<\ ,\ >_v$ for $v \in X^\infty$, define the transition matrices $a = (a_v) \in GL_n(\boldsymbol{A})$ by $(e_v^1, \cdots, e_v^n) = a_v(u_1, \cdots, u_n)$. We then associate the class of a in $Cl_n(\bar{X})$ to $(\mathcal{E}, <\ ,\ >)$.

It is easy to see that the induced bijection $Cl(\bar{X}) \simeq Pic(\bar{X})$ preserves the sums, products, exterior powers and duals.

1.4. We give a version of Riemann-Roch theorem by writing explicitly down the Poisson summation formula (cf [11], 4.2) in the following way. Let $(\mathcal{O}(D), <\ ,\ >_D)$ be the hermitian bundle corresponding to a divisor $D=div(a)$, $a\in GL_n(\boldsymbol{A})$, on $\bar{X}$ as in 1.2. Define the functions $f_{D,v}$ on $K_v^n(v\in X^\circ\cup X^\infty)$ by

$$f_{D,v}: =\text{the characteristic function of } a_v\mathcal{O}_v^n,\ v\in X^\circ,$$
$$f_{D,v}(x): =\begin{cases}\exp[-\pi<x,\ x>_{D,v}] & K_v\simeq \boldsymbol{R},\\ \exp[-2\pi<x,\ x>_{D,v}] & K_v\simeq \boldsymbol{C}.\end{cases}$$

Set $f_D=\prod_v f_{D,v}$ on $\boldsymbol{A}^n$ and $f_D^\infty=\prod_{v\in X^\infty} f_{D,v}$ on $\prod_{v\in X^\infty}K_v^n$ and define

$$l(D): =\sum_{x\in K^n} f_D(x)=\sum_{x\in\Gamma(X,\ \mathcal{O}(D))} f_D^\infty(x).$$

We easily see that $l(D)$ depends only on the class of $D\in Cl(\bar{X})$. Let δ_v be the local different of $K_v/\boldsymbol{Q}_v$ for $v\in X^\circ$ and $\delta_v=1$ for $v\in X^\infty$. The canonical divisor W on $\bar{X}$ is defined to be $div(\delta)^{-1}$, $\delta=(\delta_v)\in Cl_1(\bar{X})$. Now, by computing the both sides of the Poisson summation formula

$$\sum_{x\in K^n} f_D(x)=\sum_{x\in K^n} f_D^\vee(x)$$

where $f_D^\vee$=the Fourier transform of f_D with respect to the self dual measure on $\boldsymbol{A}^n$ ([15], Ch. VII, §2), we obtain

$$l(D)=l(D^\vee\otimes W)deg(D)^n|d_K|^{-n/2},$$

where $|d_K|=deg(W)$ is the absolute value of the discriminant of K.

REMARK. We can formulate Grothendieck-like Riemann-Roch theorem introducing the Grothendieck ring made out of all isometry classes of hermitian vector bundles on $\bar{X}$. For this, we refer to J. Neukirch's account ([4], Kap. III).

2. Poincaré sums of integral representations of unramified Galois groups

2.1. Let $\tilde{K}$ be the maximal unramified extension of K and G its Galois group equipped with the Krull topology. Put $U_n(\mathcal{O}_K): =GL_n(K)\cap U_n(\boldsymbol{A}_K)$

Suppose we are given a continuous homomorphism

$$\rho:\ G\longrightarrow U_n(\mathcal{O}_K).$$

Denote by K_ρ the subfield of $\tilde{K}/K$ correponding to $\mathrm{Ker}(\rho)$.

Choose a finite Galois subextension of L of $\tilde{K}/K$ containing K_ρ. Then, ρ determines 1-cocycle $\mathrm{Gal}(L/K)\to GL_n(L)$. By Hilbert-Speiser ([8], Prop. 3, p159), we can find $Z\in GL_n(L)$ so that

$$\rho(s)=Z^{-1}s(Z)\ \text{for all}\ s\in\mathrm{Gal}(L/K), \tag{1}$$

where $s(Z)=(s(Z_{i,j}))$ if $Z=(Z_{i,j})$.

We note that Z^{-1} is given as a "Poincaré sum"

$$Z^{-1}=\sum_{s\in \mathrm{Gal}(L/K)} \rho(s)s(T) \text{ for some } T\in M_n(L). \tag{2}$$

There Poincaré sums play analogous role to the Poincaré zeta (theta) Fuchs functions in [13].

Let $R_n(\bar{X}_K)$ denote the set of all continuous homomorphisms of G into $U_n(\mathcal{O}_K)$. First of all, $R_n(\bar{X}_K)$ contains regular representions of finite quotients of G and Galois theory tells us

Lemma 2.1.1. *$\tilde{K}$ is generated over K by all Z's satisfying* (1) *for all $\rho\in R_n(\bar{X}_K)$.*

Proof. For a finite Galois subextension L of $\tilde{K}/K$, consider the regular representation reg : $\mathrm{Gal}(L/K)\to U_n(\boldsymbol{Z})\subset U_n(\mathcal{O}_K)$. By (1), we have $Z\in GL_n(L)$ so that $\mathrm{reg}(s)=Z^{-1}s(Z)$ for all $s\in\mathrm{Gal}(L/K)$. Therefore, $s(Z)=Z$ if and only if $s\in \mathrm{Ker}(\mathrm{reg})=\{1\}$. This implies $L=K(Z)$. (Q.E.D.)

For the choice of T in (2), we have

Lemma 2.1.2. *We can take any normal basis element θ of L/K as T. Moreover, its trace $\sum_{s\in\mathrm{Gal}(L/K)} tr(\rho(s))s(\theta)$ generates K_ρ over K.*

Proof. [7], Theorems (2.4) and (3.2). (Q.E.D.)

Next, we attach a divisor class of rank n over $\bar{X}_K$ to each $\rho\in R_n(\bar{X}_K)$. The following Galois descent argument was communicated by T. Ono.

A finite Galois subextension L/K of $\tilde{K}/K$ being as above, consider the exact sequence of $\mathrm{Gal}(L/K)$-pointed sets

$$1\to U_n(\boldsymbol{A}_L)\to G_n(\boldsymbol{A}_L)\to GL_n(\boldsymbol{A}_L)/U_n(\boldsymbol{A}_L)\to 1 \tag{3}$$

We first see

Lemma 2.1.3. $H^1(L/K,\ U_n(\boldsymbol{A}_L))=\{1\}$.

Proof. It is enough to show $H^1(L_w/K_v,\ GL_n(\mathcal{O}_w))=1$ where $\mathcal{O}_w$ is the ring of integers in L_w, $w|v$, $v\in X_K^\circ$. The argument in ([8], Prop.3, p159) shows that this follows from its reduction $H^1(\kappa(w)/\kappa(v),\ GL_n(\kappa(w)))=1$ by lifting, since L_w/K_v is unramified. (Q.E.D.)

Hence, (3) induces the bijection ([9], 5.4, Prop. 36)

$$GL_n(\boldsymbol{A}_K)/U_n(\boldsymbol{A}_K) \simeq (GL_n(\boldsymbol{A}_L)/U_n(\boldsymbol{A}_L))^{\mathrm{Gal}(L/K)}, \tag{4}$$

where the right hand side means the $\mathrm{Gal}(L/K)$-invariant part.

Embedding the global Z in (1) diagonally in $GL_n(\boldsymbol{A}_L)$, $ZU_n(\boldsymbol{A}_L)$ is $\mathrm{Gal}(L/K)$-invariant by (1) and so we obtain the corresponding divisor $div(z)=zU_n(\boldsymbol{A}_K)$ over $\bar{X}_K$ under (4): $zU_n(\boldsymbol{A}_L)=ZU_n(\boldsymbol{A}_L)$.

We then define a map

$$\bar{\Phi}_n : R_n(\bar{X}_K) \longrightarrow Cl_n(\bar{X}_K)$$

by setting $\bar{\Phi}_n(\rho) :=$ the class of $div(z)$, z being as above. We will also write $c(\rho)$ for $\bar{\Phi}_n(\rho)$ below.

First of all, we need to check

Lemma 2.1.4. *$\bar{\Phi}_n$ is well defined, namely, it is independent of the choice of L and Z in the above.*

Proof. Suppose (L', Z') is another choice which gives $div(z')$. We may assume $L \subset L'$. Since $Z'^{-1}s(Z')=\rho(s)=Z^{-1}s(Z)$ for all $s \in \mathrm{Gal}(L'/K)$, $Z'Z^{-1} \in GL_n(K)$ and so $div(z)$ and $div(z')$ belong to the same class. (Q.E.D.)

Like the function field case, we easily see

Proposition 2.1.5. $\mathrm{Image}(\bar{\Phi}_n) \subset Cl_n(\bar{X}_K)_1$.

Proof. Suppose $\bar{\Phi}_n(\rho)=$ the class of $div(z)$ as above. Then, $1=deg_L(div(Z)) = deg_K(div(z))^{[L:K]}$. (Q.E.D.)

For the preimage of $\bar{\Phi}_n$, we have

Proposition 2.1.6. *For $\rho_1, \rho_2 \in R_n(\bar{X}_K)$, $\bar{\Phi}_n(\rho_1)=\bar{\Phi}_n(\rho_2)$ if and only if there is $B \in U_n(\mathcal{O}_F)$ so that $\rho_2(s)=B^{-1}\rho_1(s)s(B)$ for all $s \in \mathrm{Gal}(F/K)$, where F is any finite Galois subextension of $\tilde{K}/K$ containing the fields corresponding to* $\ker(\rho_i)(i=1, 2)$ *and* $U_n(\mathcal{O}_F) := GL_n(F) \cap U_n(\boldsymbol{A}_F)$.

Proof. Suppose $\rho_i(s)=Z_i^{-1}s(Z_i)$ and $z_iU_n(\boldsymbol{A}_F)=Z_iU_n(\boldsymbol{A}_F)$ with $Z_i \in GL_n(F)$, $z_i \in GL_n(\boldsymbol{A}_K)$, $i=1, 2$.
$\Rightarrow$: Since $div(z_1)$ and $div(z_2)$ are in the same class in $Cl_n(\bar{X}_K)$, $Z_2=\alpha Z_1 u$ with $\alpha \in GL_n(K)$, $u \in U_n(\boldsymbol{A}_F)$. Put $B=Z_1^{-1}\alpha^{-1}Z_2=u$. Then, $B \in U_n(\mathcal{O}_F)$ and $\rho_2(s)=$

$B^{-1}\rho_1(s)s(B)$.
$\Leftarrow$: Since $Z_2^{-1}s(Z_2)=B^{-1}Z_1^{-1}s(Z_1)s(B)$, $Z_1BZ_2^{-1}\in GL_n(K)$ and so $div(z_1)$ and $div(z_2)$ are in the same class. (Q.E.D.)

Denote by $M_n(\bar{X}_K)$ the quotient space of $R_n(\bar{X}_K)$ by the equivalence relation in 2.1.6. Set $M(\bar{X}_K)=\bigcup_{n\geq 1} M_n(\bar{X}_K)$. Getting all $\bar{\Phi}_n$ together, we have

$$\bar{\Phi}: M(\bar{X}_K)\longrightarrow Cl(\bar{X}_K)_1.$$

$M(\bar{X}_K)$ also has the operations such as sum, product, exterior power and dual.

We can prove in a straightforward manner the following

Theorem 2.1.7. *The injective map $\bar{\Phi}$ constructed in the above preserves sums, products, exterior poweres and duals.*

REMARK 2.1.8. Let $R_n(X_K)$ denote the set of continuous homomorphisms of G into $GL_n(\mathcal{O}_K)$. By the similar argument using Hilbert-Speiser theorem, we obtain a map

$$\Phi_n: R_n(X_K)\longrightarrow Cl_n(X_K)$$

for each n. However, as we have noted in 1.2. we have a commutative diagram

$$\begin{array}{ccc} R_n(X_K) & \xrightarrow{\Phi_n} & Cl_n(X_K) \\ \det\downarrow & & \wr\downarrow\det \\ R_1(X_K) & \xrightarrow{\Phi_1} & Cl_1(X_K) \end{array} \quad =\text{the ideal class group of } K$$

So, Φ_n does not reflect the non-abelian nature. Actually, we shall find an example in Section 3 which shows that $\bar{\Phi}_2(\rho_1)\neq\bar{\Phi}_2(\rho_2)$ and $\Phi_2(\rho_1)=\Phi_2(\rho_2)$ for some ρ_1, $\rho_2\in R_2(\bar{X}_K)$.

2.1.9. Unlike the function field case, the divisor classes which become principal in a finite unramified extension may not be obtained from representaions in $R_n(\bar{X}_K)$ via $\bar{\Phi}_n$, since $U_n(\mathcal{O}_K)\neq U_n(\mathcal{O}_L)$ can happen for some unramified extension L/K.

2.1.10. Suppose K/k is a Galois extension for some k. Then, the Galois group $\mathrm{Gal}(K/k)$ acts on both $R_n(\bar{X}_K)$ and $Cl_n(\bar{X}_K)$ in natural manners. By the construction of $\bar{\Phi}_n$, we can easily see that $\bar{\Phi}_n$ is $\mathrm{Gal}(K/k)$-equivariant.

2.2. Let $\rho\in R_1(\bar{X}_K)$. Since $U_1(\mathcal{O}_K)$ is the group of roots of 1 in K, by 2.1.7, $c(\rho)^m$ is trivial, where m is the number of roots of 1 in K. Conversely, suppose $c\in Cl_n(\bar{X}_K)$ satisfies $c^m=1$ and K containas m-th roots of 1. If D is a divisor

belonging to c, $D^m=\alpha U_1(\boldsymbol{A}_K)$ for some $\alpha\in K^\times$. The cyclic extension $K(\sqrt[m]{\alpha})/K$ is unramified outside m. Suppose it is unramified (everywhere). Define ρ by $\rho(s)=s(\sqrt[m]{\alpha})/\sqrt[m]{\alpha}$ for $s\in\mathrm{Gal}(K(\sqrt[m]{\alpha})/K)$. Then, ρ is in $R_1(\bar{X}_K)$ and satisfies $c(\rho)(=\Phi_1(\rho))=c$. We want to proceed the above observation in the non-abelian situation as Weil started ([13], pp85-86. See also [5]).

Let $\rho\in R_n(\bar{X}_K)$, namely, we have a faithful representation ρ: $\mathrm{Gal}(K_\rho/K)\to U_n(\mathcal{O}_K)$. Since the character values $\chi(s)=tr(\rho(s))$, $s\in\mathrm{Gal}(K_\rho/K)$, take algebraic integers, there exist polynomials f and g whose coefficients are non-negative integers so that $f(\chi(s))=g(\chi(s))$ for all $s\in\mathrm{Gal}(K_\rho/K)$. Hence, the representation theory tells that two representations $f(\rho)$ and $g(\rho)$ are K-equivalent. Here, note that $f(\rho)$ and $g(\rho)$ are in $R_N(\bar{X}_K)$, $N=f(n)=g(n)$. Suppose further that $f(\rho)$ and $g(\rho)$ are equivalent in the sense of 2.1.6. Then, we have $f(c(\rho))=g(c(\rho))$.

Conversely, suppose a divisor $div(z)$ of rank n becomes principal in a finite unramified extension L over K and its class c satisfies $f(c)=g(c)$ with polynomials f and g whose coefficients are non-negative integers. Then, we can find $\alpha\in GL_N(K)$, $u\in U_N(\boldsymbol{A}_K)$ and $Z\in GL_n(L)$, $N=f(n)=g(n)$, such that $\alpha f(z)=g(z)u$, $f(z)U_N(\boldsymbol{A}_L)=f(Z)U_N(\boldsymbol{A}_L)$. Hence, we have $\alpha f(Z)=g(Z)B$ with $B\in U_n(\mathcal{O}_L)$. Define ρ by $\rho(s)=Z^{-1}s(Z)$, $s\in\mathrm{Gal}(L/K)$. We then easily see that $f(\rho(s))=B^{-1}g(\rho(s))s(B)$. According to Weil [12], the set $\{Z\in GL_n(\bar{K})|f(Z)=A^{-1}g(Z)A\}$ is finite for $A\in GL_N(K)$ and it is in $GL_n(K)$ if K is large enough ([10]). In our case, we must assume further that $\rho(s)$ defined above is in $U_n(\mathcal{O}_K)$. Then, we have $\rho\in R_n(\bar{X}_K)$ and $c(\rho)=c$.

3. An example

In this section, we give an example of a number field K whose maximal non-abelian unramified extension $\tilde{K}$ is given explicitly and see the images in $Cl_2(\bar{X}_K)$ of some representations in $R_2(\bar{X}_K)$ under Φ in Section 2. The author learned from K. Yamamura (letters to the author, Jan. and Feb. 1992) our method to make the maximal unramified externsion, which is finite over the ground field, using Odlyzko's results ([3], [6]) on the lower bounds of root discriminants (cf. [16]). By using the idea in Appendix of [16], we can give a simple remark on the maximal unramified Galois group $\mathrm{Gal}(\tilde{K}/K)$. Let $n_K=[K:\boldsymbol{Q}]$ and let $r_1(K)$(resp. $r_2(K)$) denote the number of real (resp. imaginary) places of K. Set $rd_K=|d_K|^{1/n_K}=$the root discriminant of K. Let $B(n, r_1, r_2)$ be the lower bound for the disriminant of a number field L of degree $\geq n$ so that $r_i(L)/n_L=r_i/n(i=1, 2)$. We then have

Proposition 3.1. *Assume* $rd_K<B(60n_K, 60r_1(K), 60r_2(K))$. *Then, the Galois group* $\mathrm{Gal}(\tilde{K}/K)$ *is prosolvable, namely,* $\tilde{K}$ *is the union of Hilbert class*

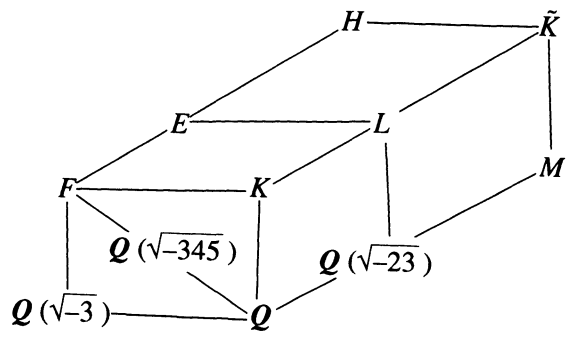
fields tower of K.

Proof. Suppose $\mathrm{Gal}(\tilde{K}/K)$ is not prosolvable. Then, there exists a finite unramified Galois extension L over K so that $\mathrm{Gal}(L/K)$ is not solvable. Hence, $[L:K]\geq 60$ and $rd_K=rd_L\geq B(n_L,\ r_1(L),\ r_2(L))\geq B(60n_K,\ 60r_1(K),\ 60r_2(K))$, which contradicts our assumption. (Q.E.D.)

Now, let $K=\boldsymbol{Q}(\sqrt{-155})$. The Hilbert class field of K is $L=\boldsymbol{Q}(\sqrt{5},\ \sqrt{-23})$. The class number of $\boldsymbol{Q}(\sqrt{-23})$ is 3 and its Hilbert class field M is the splitting field of X^3-X-1 over $\boldsymbol{Q}$. Since $h_L=(1/2)h_{\boldsymbol{Q}(\sqrt{5})}h_{\boldsymbol{Q}(\sqrt{-23})}h_K=3$, the composite field $N=KM$ is the Hilbert class field of L. We claim that $\tilde{K}=N$:

Proof. (K. Yamamura) According to the table in [3], an imaginary number field with degree ≥ 36 has the root discriminant $\geq 12.53\ldots$. Since N has the degree 12 and its root discriminant is that of $K=\sqrt{155}=10.72\ldots$, we have $[\tilde{N}:N]\leq 2$. Assume $[\tilde{N}:N]=2$. Since $\tilde{N}/L$ is non-abelian Galois extension of degree 6, its Galois group is the symmetric group on 3 letters. It, however, contains the normal subextension N/L of degree 3. This is contradiction. (Q.E.D.)

Let $F=K(\sqrt{-3})=\boldsymbol{Q}(\sqrt{-155},\ \sqrt{-3})$. Let's see the Hilbert class field tower of F again. The composite field $E:=FL=\boldsymbol{Q}(\sqrt{5},\ \sqrt{-23},\ \sqrt{-3})$ is the Hilbert class field of F, since $h_F=(1/2)h_{\boldsymbol{Q}(\sqrt{-3})}h_{\boldsymbol{Q}(\sqrt{345})}h_K=2$. Hirabayashi-Yoshino's computation [1] tells us the class number of $E=3$. Hence, $H:=F\tilde{K}$ is the Hilbert class field of E.



We claim that $H=\tilde{F}$ under the Generalized Riemann Hypothesis.

Proof. The root discriminant of $F=$that of $\boldsymbol{Q}(\sqrt{345})=18.59\cdots$. By the table in [3], under G.R.H, an imaginary number field with degree ≥ 96 has the root discriminant $\geq 19.05\ldots$. So, we have $[\tilde{H}:H]\leq 3$. By the same reason as in the

case of N/K, $[\widetilde{H} : H] \neq 2$. Also, $[\widetilde{H} : H]$ can not be 3 because if it were so, the non-abelian Galois group $\mathrm{Gal}(\widetilde{H}/E)$ of order 3^2 would be abelian. (Q.E.D)

Hence, the Galois group $\mathrm{Gal}(H/F) \simeq \mathrm{Gal}(\widetilde{K}/K)$ is the symmetric group on 3 letters. Let σ, $\tau \in G$ so that $\sigma^3 = \tau^2 = 1$, $\tau\sigma\tau = \sigma^{-1}$.

First, consider 3 representations $\rho_i (0 \leq i \leq 2)$ of $\mathrm{Gal}(\widetilde{K}/K)$ into $U_2(\mathcal{O}_K)$:

$$\rho_0(\sigma) = \rho_0(\tau) = 1_2\,;\ \rho_1(\sigma) = 1_2,\ \rho_1(\tau) = -1_2\,;$$
$$\rho_2(\sigma) = 1_2,\ \rho_2(\tau) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

We want to see the images $c(\rho_i) \in Cl_2(\overline{X}_K)$ whose structure is given as follow. The ideal class group $Cl_1(X_K)$ is generated by the prime $\wp$ over 5 and we can take $\pi = (5 + \sqrt{-155})/2$ for a prime element of K_v. Let $g = (1, \cdots, 1, \pi, 1, \cdots) \in \boldsymbol{A}_K^\times$ and $\Gamma = GL_2(K) \cap gGL_2(\boldsymbol{A}_K^\infty)g^{-1}$. By the correpondence given in 1.2, we have

$$Cl_2(\overline{X}_K) \simeq S^1 \cup S^2,$$
$$S^1 = GL_2(\mathcal{O}_K) \backslash GL_2(\boldsymbol{C})/U(n),\ S^2 = \Gamma \backslash GL_2(\boldsymbol{C})/U(n),$$
$$Cl_n(X_K) \simeq Cl_1(X_K) = \{[1], [\wp]\}.$$

Note that under the natural map $Cl_n(\overline{X}_K) \to Cl_n(X_K)$, S^1 and S^2 go to $[1]$ and $[\wp]$ respectively.

Let $\rho_i(s) = Z_i^{-1} s(Z_i)$, $\mathrm{Gal}(\widetilde{K}/K)$, $z_i U_2(\boldsymbol{A}_{K_i}) = Z_i U_2(\boldsymbol{A}_{K_i})$ with $Z_i \in GL_2(K_i)$, $z_i \in GL_2(\boldsymbol{A}_K)$, $K \subset K_i \subset \widetilde{K}$, $0 \leq i \leq 2$. Actually, we can take

$$Z_0 = z_0 = 1_2,\ K_0 = K,$$
$$Z_1 = \sqrt{5}1_2,\ z_1 = (\sqrt{5}1_2, 1_2, \cdots, 1_2, \pi 1_2, 1_2, \cdots),\ K_1 = L$$
$$Z_2 = \begin{pmatrix} \sqrt{5} & 0 \\ 0 & 1 \end{pmatrix},\ z_2\left(\begin{pmatrix} \sqrt{5} & 0 \\ 0 & 1 \end{pmatrix}, 1_2, \cdots, 1_2, \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}, 1_2, \cdots\right),\ K_2 = L.$$

By the above correspondence, we have

$$c(\rho_0) = [1_2] \in S^1,\ c(\rho_1) = [(\sqrt{5}/\pi)1_2] \in S^1,$$
$$c(\rho_2) = \left[\begin{pmatrix} \sqrt{5} & 0 \\ 0 & 1 \end{pmatrix}\right] \in S^2$$

Here, we see $c(\rho_0) \neq c(\rho_1)$, although $\Phi_2(\rho_0) = \Phi_2(\rho_1) = [1] \in Cl_1(X_K)$.

Next, consider the faithful representation ρ of $\mathrm{Gal}(H/F)$ into $U_2(\mathcal{O}_F)$ defined by

$$\rho(\sigma) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix},\ \rho(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

where ω is a primitive cubic root of 1.

Letting $\theta_i (1 \leq i \leq 3)$ be the roots of $X^3 - X - 1$, $Z = \begin{pmatrix} \theta_3(\theta_1 - \theta_2) & \theta_1(\theta_2 - \theta_3) \\ 2(\theta_1 - \theta_2) & 2(\theta_2 - \theta_3) \end{pmatrix}$. $\begin{pmatrix} 1 & 1 \\ -\omega & -\omega^2 \end{pmatrix}$ satisfies $\rho(s) = Z^{-1} s(Z)$ for all $s \in \mathrm{Gal}(H/F)$ (This Z was found by T. Ono). But I do not know $z \in GL_2(\boldsymbol{A}_F)$ with $zU_2(\boldsymbol{A}_H) = ZU_2(\boldsymbol{A}_H)$.

Put $f(x) = x^2 + 2x$ and $g(x) = x^3$. By Takahishi [10], ρ satisfies

$$f(\rho) = C^{-1} g(\rho) C, C = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in U_8(\mathcal{O}_F)$$

Hence, we have $f(c(\rho)) = g(c(\rho))$ in $Cl_8(\overline{X}_F)$ as we have seen in 2.2.

ACKNOWLEDGEMENT. I wish to thank Professor Takashi Ono for discussion on Section 2 and ceaseless encouragement. My thanks also go to Professor Ken Yamamura to whom I owe Section 3 a great deal, and Professor Mikihito Hirabayashi for his computation of a certain class number in Section 3.

References

[1] M. Hirabayashi and K. Yoshino: *Unit Indices of Imaginary Abelian Number Fields,* J. of Number Theory. **34**(1990), 346-361.
[2] M. Kneser: *Strong Approximation,* Proc. Symp. Pure Mth., Providence, A.M.S., RI., **9** (1965), 187-196.
[3] J. Martinet: *Petits discriminants des corps de nombers,* in Journées Arithmétiques 1980, 151-193, ed. J.V.Armitage, London Math. Soc. Lecture Note Ser. **56**, cambridge Univ. Press. 1982.
[4] J. Neukirch: Algebraische Zahlentheorie, Springer, 1992.
[5] M. Nori: *On the representations of the fundamental group,* Compositio Math., **33** 1976, 29-41.
[6] A. Odlyzko: *Discriminants bounds,* (unpublished table), Nov. 29th, 1976.
[7] T. Ono: *A note on Poincaré sums of Galois representations,* Proc. Japan Acad., **67A**(1991), 145-147.
[8] J.-P. Serre: Corps Locaux, Hermann, Paris, 1962.
[9] ———: Cohomologie Galoisienne, Lect. Note in Math. **5,** Springer, 1964.
[10] S. Takahashi: *Generation of Galois extensions by matrix roots,* J.Math.Soc. Japan, **20** (1968), 365-370.
[11] J. Tate: *Fourier Analysis in Number Fields and Hecke's Zeta Functions,* in Algebraic Number Theory ed. J.W.S. Cassels and Fröhlich, 305-347, Acad. Press, London-New York, 1967.
[12] A. Weil: *Une propriété caractéristique des groupes finis de substitutions,* C.R.Acad. Sci. Paris, **199** (1934), 180-182.
[13] ———: *Géneralisation des fonctions abéliennes,* J.de Math. P. et App. **17** (1938), 47-87.
[14] ———: *Sur l'analogie entre les corps les de nombres algébrique et les corps de fonction*

algebrique, Revue Scient., **77** (1939), 104-106.
[15] ———: Basic Number Theory, Grundl. Math. Wiss., v. **144,** Springer, 1974.
[16] K. Yamamura: *The determination of the imaginary abelian number fields with class number one,* Math. Comp., v. **62,** no. **206** (1994), 899-921.

Department of Mathematics
Faculty of Science
Kanazawa University
Kakuma, Kanazawa, 920-11
Japan