Available online at www.sciencedirect.com
ScienceDirect
Journal of Number Theory 128 (2008) 1587–1601
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

Actions of Galois groups on invariants of number fields

A. Kontogeorgis

University of the Ægean, Department of Mathematics, Karlovassi, Samos, Greece

Received 5 January 2007; revised 13 March 2007

Available online 16 June 2007

Communicated by Pilar Bayer

Abstract

In this paper we investigate the connection between relations among various invariants of number fields L^H corresponding to subgroups H acting on L and of linear relations among norm idempotents.

1. Introduction

Let C be an algebraic curve defined over an algebraically closed field of arbitrary characteristic and let $G \subset \mathrm{Aut}(C)$ be a subgroup of the full automorphism group. For a subgroup H of G, let C^H be the quotient curve and let g_H and γ_H be the genus and the p-rank of the Jacobian of C^H. In the group algebra $k[G]$ the norm idempotents ε_H are defined by

$$\varepsilon_H = \frac{1}{|H|} \sum_{h \in H} h.$$

E. Kani and M. Rosen [3,4] studied the action of automorphisms on the Jacobian variety of the curve, and they proved that every linear relation among the norm idempotents coming from subgroups H of G implies the same relations for g_H, γ_H. This is a generalization of results proved by R. Accola [1].

E-mail address: kontogar@aegean.gr.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2007.04.012

They also have proved that such a linear relation implies the same relations for the zeta functions of the corresponding fields L^H, where L is the function field of an algebraic curve or a number field [4, Proposition 1.2], i.e.,

$$\sum r_H \varepsilon_H = 0 \quad \Rightarrow \quad \prod \zeta_H(s)^{r_H} = 1. \tag{1}$$

There is an analogy between the theory of numbers fields and the theory of non-singular curves. In this analogy one completes the spectra of the rings of integers of number fields by adding the infinite primes. For more information concerning the similarities of number fields and the theory of curves we refer to [6, I.13] or to the more elementary [5]. One can define for number fields the analogues of the notions of genus [6, III.3], Jacobian variety [6, III.2] and Tate module.

It is known that a lot of information concerning a number field, can be obtained from the corresponding zeta function. Let L/L^G be a Galois extension of number fields. Let L^H be the number field corresponding to the subgroup H, of the Galois group G. Using the characterization of the residues of the zeta functions for number fields at $s = 1$, Kani and Rosen arrived at a formula, involving the class number h_{L^H}, the regulator $\operatorname{Reg}(L^H)$, and the number w_H of roots of unity of finite order in L^H:

$$\prod \left(h_{L^H} \operatorname{Reg}\left(L^H\right)\right)^{r_H} = \prod w_H^{r_H},$$

where H runs over the subgroups of G. The last equality was also proved by R. Brauer [2] in 1950.

In this paper we express the dependence of several group invariants of the subfields L^H, corresponding to the Galois subgroups H, in terms of the linear relations among norm idempotents defined by the subgroup H.

In order to do so we give a generalization of the notion of Tate modules for the "Jacobian" of a Number Field, and we consider the action of the Galois group on it. In our study arise problems that are similar to those stemming from wild ramification of the action of a group on a curve defined over a field of positive characteristic.

Consider a number field L. Fix a subfield K such that the extension L/K is Galois with Galois group G. For every subgroup H of G we define, as usual, the fixed field L^H. The following functions from the set of subgroups G to $\mathbb{Z}$ are defined:

(1) Let $r_H, 2s_H$ be the number of real and imaginary embeddings of L^H to $\bar{\mathbb{Q}}$. We set $\lambda_H = r_H + s_H - 1$.
(2) Consider the class group $\operatorname{Cl}(L^H)$. It is a finite Abelian group, hence it can be written as

$$\operatorname{Cl}\left(L^H\right) = \bigoplus_{p \mid \mid \operatorname{Cl}(L^H)\mid} \operatorname{Cl}\left(L^H\right)_p,$$

where $\operatorname{Cl}(L^H)_p$ is the p-part of the Abelian group $\operatorname{Cl}(L^H)$. The group $\operatorname{Cl}(L^H)_p$ in turn can be expressed as a finite direct sum of Abelian groups $\operatorname{Cl}(L^H)_{p,n}$ that are sums of $\lambda_{H,p,n}$ summands of cyclic groups $\mu(p^n)$ of order p^n, i.e.,

$$\operatorname{Cl}\left(L^H\right)_p = \bigoplus_{n=1}^{\infty} \operatorname{Cl}\left(L^H\right)_{p,n} = \bigoplus_{n=1}^{\infty} \bigoplus_{\mu=1}^{\lambda_{H,p,n}} \mu\left(p^n\right).$$

Notice that in the above formulas $\lambda_{H,p,n} = 0$ for all but finite triples (H, p, n), and that $\mathrm{Cl}(L^H)_{p,n}$ are free $\mathbb{Z}/p^n\mathbb{Z}$-modules of rank $\lambda_{H,p,n}$.

(3) Consider the group $\mu(L^H)$ of units of finite order in the field L^H. It is a cyclic group and can be written as

$$\mu\big(L^H\big) = \bigoplus_{p||\mu(L^H)|} \mu\big(p^{v(H,p)}\big) = \bigoplus_{p||\mu(L^H)|} \bigoplus_{p,n} \mu\big(p^n\big)^{k_{H,p,n}},$$

where $v(H, p)$ denotes the valuation at p of $|\mu(L^H)|$. The number $k_{H,p,n}$ can be seen as the rank of the $\mathbb{Z}$-submodule of $\mu(L^H)$ isomorphic to a direct product of $\mu(p^n)$ summands. Notice that since $\mu(L^H)$ is a cyclic group, for a fixed prime p there is only one pair (p, n) so that $k_{H,p,n} \neq 0$ and for this particular $(p, n) = (p, v(H, p))$ we have $k_{H,p,n} = 1$.

We will show that the above functions λ_H, $\lambda_{H,p,n}$, $k_{H,p,n}$ behave like the p-ranks of the Jacobians of algebraic curves. Namely, we prove that every linear relation among norm idempotents of the subgroup implies the same relations for the above functions:

Theorem 1.1. *Let L/K be a Galois extension with Galois group G. Every relation $\sum r_H \varepsilon_H = 0$ among norm idempotents implies the relation $\sum r_H \lambda_H = 0$. If moreover in the sum $\sum r_H \varepsilon_H = 0$, $r_H = 0$ for all subgroups H of G with $(p, |H|) \neq 1$ then $\sum r_H \lambda_{H,p,n} = 0$ and $\sum r_H k_{H,p,n} = 0$.*

Let L be a number field of discriminant $\sqrt{D_L}$, group of units of finite order $\mu(L)$, and let $r, 2s$ be the numbers of real and imaginary embeddings of L, respectively. Let w_L denote the order of $\mu(L)$. The Arakelov genus is defined by

$$g_L = \log \frac{w_L \sqrt{|D_L|}}{2^r (2\pi)^s}.$$

It is interesting to ask whether a relation among norm idempotents implies the same relation among Arakelov genera. The answer is yes provided we have "tame ramification" in the group of units that are contained in L, i.e.,

Proposition 1.2. *Let L/K be a Galois extension with Galois group G. Consider the set S of subgroups $H < G$, such that $(|H|, w_L) = 1$. Every linear relation $\sum_{H \in S} r_H \varepsilon_H = 0$ among norm idempotents corresponding to subgroups $H \in S$, implies the same relation among the Arakelov genera g_{L^H}, of the fixed fields L^H. In particular, if the order of the Galois group is prime to w_L, then $\sum r_H \varepsilon_H = 0$ implies $\sum r_H g_{L^H} = 0$.*

In [7] G. van der Geer and R. Schoof introduced the notion of effectivity of an Arakelov divisor, a notion that is close to the definition of the effectivity of a divisor on an algebraic curve. This notion gives rise to a new notion of $H^0(D)$, for Arakelov divisors D and leads naturally to a new invariant η_L for the number field L. Let $M(L)$ be the Minkowski space of the field L (for all definitions we refer to Section 5) and let A be a divisor supported on the set of infinite primes of L. For every such A Eq. (11) gives rise to a metric $\|\cdot\|_{L,A}$ on $M(L)$. The invariant η_L is then defined as

$$\eta_L := \left(\sum_{x \in \mathcal{O}_L} e^{-\pi \|x\|_{L,0}^2} \right),$$

where $\|\cdot\|_{L,0}$ is the metric on the Minkowski space of the number field L defined by

$$\|x\|_{L,0}^2 = \sum \bigl|\sigma(x)\bigr|^2.$$

Given a relation $\sum n_H \epsilon_H = 0$, we will prove a formula for the η-invariants corresponding to subfields L^H of L. In order to do so we have to change the model at the infinite primes by considering a different metric $\|\cdot\|_{L,A}$ on the Minkowski vector space. We introduce the invariants

$$\eta_A(L) := \Biggl(\sum_{x\in\mathcal{O}_L} e^{-\pi\|x\|_{L,A}^2} \Biggr),$$

for every divisor A supported at infinite primes. We will prove the following

Proposition 1.3. *Let $\sum n_H \epsilon_H = 0$ be a linear relation among norm idempotents. If $\mathbb{P}(L^H, \mathbb{R})$ (respectively $\mathbb{P}(L^H, \mathbb{C})$) denotes the real (respectively complex) infinite primes and*

$$B(H) = -\frac{\log(|H|)}{2} \sum_{\sigma\in\mathbb{P}(L^H,\mathbb{R})} \sigma - \log\frac{|H|}{2} \sum_{\sigma\in\mathbb{P}(L^H,\mathbb{C})} \sigma$$

is a divisor supported on infinite primes of the field L^H, then the following formula holds

$$0 = \sum_H \lambda_H \eta_{B(H)}\bigl(L^H\bigr).$$

2. Notation

Let K be a number field with ring of algebraic integers $\mathcal{O}_K$. We are following the notation of the book of J. Neukirch [6]. An Arakelov divisor of K, is a formal sum

$$D = \sum_p v_p p,$$

where p runs over the finite and infinite primes of K, and $v_p \in \mathbb{Z}$ if p is a finite prime and $v_p \in \mathbb{R}$ if p is an infinite prime. We will denote by

$$\operatorname{Div}(\bar{\mathcal{O}}_K) \cong \operatorname{Div}(\mathcal{O}_K) \times \bigoplus_{p|\infty} \mathbb{R}p$$

the set of Arakelov divisors on K. There is a canonical homomorphism

$$\operatorname{div} : K^* \to \operatorname{Div}(\bar{\mathcal{O}}_K)$$

sending $f \in K^*$ to $\sum_p u_p(f)p$, where $v_p(f)$ is the normalized p-adic valuation of f if p is a finite prime, and $v_p(f) = -\log|\tau(f)|$, where $\tau \in \operatorname{Hom}_{\mathbb{Q}}(K, \bar{\mathcal{O}}_K)$ is the monomorphism corresponding to the infinite prime p. The Arakelov class group $\mathrm{CH}^1(\bar{\mathcal{O}}_K)$ is defined as

$$\mathrm{CH}^1(\bar{\mathcal{O}}_K) = \frac{\operatorname{Div}(\bar{\mathcal{O}}_K)}{\operatorname{div}(K^*)}$$

and it is equipped with the quotient topology. Since $\prod_p |f|_p = 1$ we can define on $\mathrm{CH}^1(\bar{\mathcal{O}}_K)$ a continuous function

$$\deg : \mathrm{CH}^1(\bar{\mathcal{O}}_K) \to \mathbb{R}$$

sending $D = \sum \nu_p p$ to $\sum_p \nu_p \log(N(P))$, where $N(P)$ denotes the norm of P. The kernel of the degree map is a compact group denoted by $\mathrm{CH}^1(\bar{\mathcal{O}}_K)^0 =: J_K$. It can be proved [6, Satz 1.11] that J_K is given by the short exact sequence

$$1 \to H/\Gamma \to J_K \xrightarrow{\phi} \mathrm{Cl}(K) \to 1,$$

where H/Γ is homeomorphic to a torus of dimension $r+s-1$ and $\mathrm{Cl}(K)$ is the ordinary class group of the number field K.

Following the theory of Jacobian varieties on a curve we set

$$J_{K,p^n} := \left\{\text{Elements in } J_K \text{ annihilated by } p^n\right\},$$

where p is a prime number of $\mathbb{Z}$. For the p-part of J_K we have the following short exact sequence:

$$1 \to \left(\mathbb{Z}/p^n\mathbb{Z}\right)^{r+s-1} \to J_{K,p^n} \to \mathrm{Cl}(K)_{p^n} \to 1,$$

where $\mathrm{Cl}(K)_{p^n} \cong \bigoplus_{i=1}^{\lambda_{K,n}} \mathbb{Z}/p^n\mathbb{Z}$ is the subgroup annihilated by p^n. Using the classification theorem of finite Abelian groups we can write

$$J_{K,p^n} \cong \bigoplus_{i=1}^{r+s-1+\lambda_{K,n}} \mathbb{Z}/p^n\mathbb{Z}.$$

The groups J_{K,p^n} form an inverse system and we can define the inverse limit forming the Tate module of J_K at p. Namely, we set

$$T_p(J_K) = \lim_{\leftarrow} J_{K,p^n}. \tag{2}$$

The Tate module is a free $\mathbb{Z}_p$-submodule of rank $s+r-1$. Since the order of the ordinary class group $\mathrm{Cl}(K)$ is finite $\lambda_{K,n} = 0$, for large n, and this implies that the information of the p-part of the class group is lost after taking the inverse limit. We will study the p-part $\mathrm{Cl}(K)_p$ of the class group separately.

The action of G on the primes of L induces a representation

$$\rho : G \to \mathrm{End}(J_L),$$

and since endomorphisms of J_L preserve the orders of the elements in the class group we can define representations

$$\rho_p : G \to \mathrm{End}(J_{L,p}).$$

Every ρ_p gives rise to a representation

$$\hat{\rho}_p : \mathbb{Q}_p[G] \to \mathrm{End}^0\big(T_p(J_L)\big) := \mathrm{End}\big(T_p(J_L)\big) \otimes_{\mathbb{Z}} \mathbb{Q}_p \tag{3}$$

and to a representation

$$\tilde{\rho}_p : \mathbb{Z}_{(p)}[G] \to \mathrm{End}\big(\mathrm{Cl}(L)_p\big) \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}, \tag{4}$$

where $\mathbb{Z}_{(p)}$ denotes the localization of the integer ring with respect to the prime ideal p. Observe that for the $\mathbb{Q}_p$ vector space $T_p(J_L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ we have $\mathrm{End}^0(T_p(J_L)) \cong \mathrm{End}(T_p(J_L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$. Since there is p-torsion on the $\mathbb{Z}$-module $\mathrm{Cl}(L)_p$ we cannot tensor by a field, without trivializing. The closest structure to vector space we can obtain without trivializing, is by tensoring with the localization $\mathbb{Z}_{(p)}$. Therefore the representation (4) can be seen as a representation on the $\mathbb{Z}_{(p)}$-module $\mathrm{Cl}(L)_p \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$.

The p-part of the class group can be factored, by the classification theorem of Abelian groups, as follows:

$$\mathrm{Cl}(L)_p = \bigoplus_{\nu=1}^{\infty} \bigoplus_{\mu=1}^{\lambda_{\{1\},p,\nu}} \mu\big(p^{\nu}\big),$$

and

$$\mathrm{Cl}(L)_p \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)} = \bigoplus_{\nu=1}^{\infty} \bigoplus_{\mu=1}^{\lambda_{\{1\},p,\nu}} \mathbb{Z}_{(p)}/p^{\nu}\mathbb{Z}_{(p)}.$$

Since endomorphisms that came from $\mathbb{Z}_{(p)}[G]$ preserve the order of the group, the representation $\tilde{\rho}_p$ can be factored as a sum of matrix representations

$$\tilde{\rho}_{p,\nu} : \mathbb{Z}_{(p)}[G] \to M_{\lambda_{\{1\},p,\nu}}\big(\mathbb{Z}_{(p)}/p^{\nu}\mathbb{Z}_{(p)}\big), \tag{5}$$

where $M_r(R)$, denotes the $r \times r$ matrices with coefficients from the ring R. We define the trace of $\tilde{\rho}_p$ to be the sequence $\mathrm{tr}(\tilde{\rho}_p) := (\mathrm{tr}(\tilde{\rho}_{p,\nu}))_{\nu}$. Obviously, $\mathrm{tr}(\tilde{\rho}_{p,\nu}) = 0$ for all but finite ν.

3. Field extensions

Let K, L be two number fields and let $\tau : K \hookrightarrow L$ be a field inclusion. For an Arakelov divisor $D = \sum_P \nu_P P$ of L we define

$$\tau_*(D) := \sum_p \left(\sum_{P|p} \nu_P f_{P/p} \right) p \in \mathrm{Div}(\bar{\mathcal{O}}_K),$$

where $f_{P/p}$ denotes the inertia degree of P over τK and $P \mid p$ means that $\tau p = P|_{\tau K}$. Conversely for an Arakelov divisor $D = \sum_p \nu_p p$ of K we define

$$\tau^*(D) = \sum_p \sum_{P|p} \nu_p e_{P/p} P \in \mathrm{Div}(\bar{\mathcal{O}}_L),$$

where $e_{P/p}$ denotes the ramification index of P over τK. The maps τ_*, τ^* induce maps

$$\tau_* : \mathrm{CH}^1(\bar{\mathcal{O}}_L) \to \mathrm{CH}^1(\bar{\mathcal{O}}_K)$$

and

$$\tau^* : \mathrm{CH}^1(\bar{\mathcal{O}}_K) \to \mathrm{CH}^1(\bar{\mathcal{O}}_L)$$

such that $\tau_* \circ \tau^* = [L : K]$ and $\deg(\tau_* D) = \deg(D)$, $\deg(\tau^* D) = [L : K]\deg(D)$ [6, p. 204]. We can therefore construct the following homomorphisms:

$$\tau_* : J_L \to J_K \quad \text{and} \quad \tau^* : J_K \to J_L. \tag{6}$$

Definition 3.1. Let $\mathbb{Z}_{(p)}$ denote the localization of the ring of integers with respect to a prime ideal. We will denote by R either a field of characteristic zero or $\mathbb{Z}_{(p)}$.

Lemma 3.2. *Let V, W be two finitely generated R-modules. Suppose that there are two R-module homomorphisms $f_{V,W} : V \to W$, $f_{W,V} : W \to V$, such that*

$$f_{V,W} \circ f_{W,V} = n \,\mathrm{Id}_W$$

and with $(n, p) = 1$ if $R = \mathbb{Z}_{(p)}$. Then there is a map: $\phi : \mathrm{End}(W) \to \mathrm{End}(V)$, such that $\mathrm{tr}(a) = \mathrm{tr}(\phi(a))$. In particular, if $a = \mathrm{Id}_W$, then $\phi(\mathrm{Id}_W) \in \mathrm{End}(V)$, has trace equal to $\mathrm{rank}(W)$.

Proof. For every $a \in \mathrm{End}(W)$ we define $\phi(a) \in \mathrm{End}(V)$ by

$$\phi(a) := \frac{1}{n} f_{W,V} \circ a \circ f_{V,W}. \tag{7}$$

Since n is an invertible element in R the map $f_{V,W}$ is onto. We consider the following short exact sequence of R-modules:

$$0 \longrightarrow \ker f_{V,W} \longrightarrow V \underset{\frac{1}{n} f_{W,V}}{\overset{f_{V,W}}{\rightleftarrows}} W \longrightarrow 0.$$

By construction, $\phi(a)$ is zero on $\ker f_{V,W}$, and $\mathrm{tr}(a) = \mathrm{tr}(\phi(a))$. In particular, for $a = \mathrm{Id}_W$ we have that $\mathrm{tr}(\mathrm{Id}_W) = \mathrm{rank}(W)$, hence $\mathrm{tr}(\phi(\mathrm{Id}_W)) = \mathrm{rank}(W)$. □

Remark. Let V be an $R[G]$ module associated to a representation $\rho : R[G] \to \mathrm{End}(V)$. For every element $\alpha \in R[G]$ we will denote by $\mathrm{tr}(\alpha)$ the element $\mathrm{tr}(\rho(\alpha))$.

Lemma 3.3. *For a given group G, let S be the following set of subgroups of G:*

$$S := \begin{cases} \text{all subgroups of } G & \text{if } R \text{ is a field,} \\ H < G,\ p \nmid |H| & \text{if } R \text{ is } \mathbb{Z}_{(p)}. \end{cases}$$

Let V be an $R[G]$-module that is a free R-module. Assume that for every $H \in S$ we can find an R-module $V(H)$ and two R-module homomorphisms $f^H : V(H) \to V$ and $f_H : V \to V(H)$, such that

$$f_H \circ f^H = |H| \cdot \mathrm{Id}_{V(H)}$$

and

$$f^H \circ f_H = \sum_{h \in H} h.$$

Let $\phi : \mathrm{End}(V(H)) \to \mathrm{End}(V)$ denote the map defined in (7). *We have $\phi(\mathrm{Id}_{V(H)}) = \epsilon_H$, $\mathrm{tr}(\epsilon_H) = \mathrm{rank}_R V(H)$, and, if $\sum_{H \in S} n_H \varepsilon_H = 0$ then $\sum_{H \in S} n_H \,\mathrm{rank}_R V(H) = 0$.*

Proof. We apply Lemma 3.2 for $W = V(H)$, $f_{W,V} = f^H$ and $f_{V,W} = f_H$. We compute $\phi(\mathrm{Id}_{V(H)}) = \frac{1}{|H|} f^H \circ \mathrm{Id}_{V(H)} \circ f_H = \varepsilon_H$, so $\mathrm{tr}(\varepsilon_H) = \mathrm{rank}_R(V(H))$ again by Lemma 3.2.

Observe that $\mathrm{tr}(\sum_{H \in S} n_H \varepsilon_H) = \sum_{H \in S} n_H \,\mathrm{rank}_R V(H)$ and the desired result follows by applying tr to $\sum_{H \in S} n_H \varepsilon_H = 0$. □

Remark. In the above lemma it was necessary to restrict ourselves to subgroups of order not divisible by p. The problems that appear for groups divisible by p, are of similar nature with the problems that appear in wild ramified extensions of rings. Indeed, in the case of wild ramification of an extension of rings S/R with Galois group G, the ring S is not $R[G]$-projective.

Proposition 3.4. *Let L/L^H be a Galois extension with Galois group H, and let $\tau : K := L^H \hookrightarrow L$ be the natural inclusion. Let $T_p(J_K)$ and $T_p(J_L)$ be the Tate modules defined in* (2), *and $\hat{\rho}_p$ be the representation defined in* (3). *There is a map $\phi : \mathrm{End}(T_p(J_K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \to \mathrm{End}(T_p(J_L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$ such that*:

- $\hat{\rho}_p(\varepsilon_H) = \phi(\mathrm{Id}_{T_p(J_K)})$;
- *for any $\alpha \in \mathrm{End}(T_p(J_K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$ we have*

$$\mathrm{tr}\big(\phi(\alpha)|_{J_L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p}\big) = \mathrm{tr}(\alpha|_{J_K \otimes_{\mathbb{Z}_p} \mathbb{Q}_p});$$

- $\mathrm{tr}\,\hat{\rho}_p(\varepsilon_H) = \lambda_H$.

Moreover, every linear relation $\sum r_H \epsilon_H = 0$ in norm idempotents implies that $\sum r_H \lambda_H = 0$.

Proof. The homomorphisms defined in (6) can be extended linearly to maps $f_H := \tau_* \otimes \mathrm{Id}$, $f^H := \tau^* \otimes \mathrm{Id}$ from $J_K \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ to $J_L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. The first assertion is a direct application of Lemma 3.3 if we set $V(H) = T_p(J_K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, $V = T_p(J_L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. The second assertion is an application of 3.2. The rest assertions follow by Lemma 3.3. □

Proposition 3.5. *Let L/L^H be a Galois extension with Galois group H, and let $\tau : K := L^H \hookrightarrow L$ be the natural inclusion. Let p be a prime number, $p \nmid |H|$. Let $\tilde{\rho}_{p,n}$ be the representation defined in* (4). *There is a map $\phi_2 : \mathrm{End}(\mathrm{Cl}(K)_{p,n} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}) \to \mathrm{End}(\mathrm{Cl}(L)_{p,n} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)})$ such that*:

- $\tilde{\rho}_{p,n}(\varepsilon_H) = \phi_2(\mathrm{Id}_{\mathrm{Cl}(K)_{p,n}})$;
- *for every* $\alpha \in \mathrm{End}(\mathrm{Cl}(K)_{p,n} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)})$ *we have*

$$\mathrm{tr}\big(\phi_2(\alpha)|_{\mathrm{Cl}(L)_{p,n}\otimes_{\mathbb{Z}}\mathbb{Z}_{(p)}}\big) = \mathrm{tr}(\alpha|_{\mathrm{Cl}(K)_{p,n}\otimes_{\mathbb{Z}}\mathbb{Z}_{(p)}});$$

- $\mathrm{tr}\,\tilde{\rho}_{p,n}(\varepsilon_H) = \lambda_{H,p,v}$.

Moreover, every linear relation $\sum_{(p,|H|)=1} r_H \epsilon_H = 0$ *implies that* $\sum r_H \lambda_{H,p,v} = 0$.

Proof. Observe that since $(p,|H|) = 1$ the norm idempotent is a well-defined endomorphism. As before, the homomorphisms defined in (6) can be extended $\mathbb{Z}_{(p)}$-linearly to maps $f^H := \tau^* \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$, $f_H := \tau_* \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ from $\mathrm{Cl}(K)_{p,n} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ to $\mathrm{Cl}(L)_{p,n} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$, where

$$\mathrm{Cl}(K)_{p,n} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)} = \bigoplus_{v=1}^{\infty} \bigoplus_{\mu=1}^{\lambda_{H,p,v}} \frac{\mathbb{Z}_{(p)}}{p^v \mathbb{Z}_{(p)}}.$$

The desired result is a direct consequence of Lemma 3.3 if we set $V(H) = \mathrm{Cl}(K)_{p,n} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$, $V = \mathrm{Cl}(L)_{p,n} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$. □

We will now study the action of the Galois group on the groups $\mu(L)$, $\mu(L^H)$ of units contained in the fields L, L^H, respectively.

Proposition 3.6. *Let* L/L^G *be a Galois extension with Galois group* G. *Let* w_L *be the order of the group* $\mu(L)$ *of units of finite order. Let* $v(H,p)$ *be the valuation at* p *of the order* w_{L^H} *of the group of units* $\mu(L^H)$ *of* L^H *that have finite order. Every linear relation of the form* $\sum_{(|H|,p)=1} n_H \varepsilon_H = 0$, *implies the same relation* $\sum n_H v(H,p) = 0$.

Proof. Consider the norm

$$N_{L/L^H} : \mu(L) \to \mu\big(L^H\big),$$

and the inclusion function $i_{L^H,L} : \mu(L^H) \to \mu(L)$. We have

$$N_{L/L^H} \circ i_{L^H,L} = |H| \cdot \mathrm{Id}_{\mu(L^H)}$$

and

$$i_{L^H,L} \circ N_{L/L^H} = \sum_{h\in H} h.$$

The group $\mu(L)$ is a cyclic group of order m, and $\mu(L^H)$ is a subgroup of the cyclic group $\mu(L)$. The group $\mu(L)$ can be considered as a direct sum

$$\mu(L) = \bigoplus_{i=1}^{r} \mu\big(p_i^{v(\{1\},p_i)}\big) = \bigoplus_{p} \bigoplus_{n=1}^{\infty} \mu\big(p^n\big)^{k_{\{1\},p,n}},$$

where p_i are the different prime divisors of m. Let $\mu(L^H)_p = \bigoplus_{n=1}^{\infty} \mu(p^n)^{k_{H,p,n}}$ denote the p-part of $\mu(L^H)$. Each direct summand $\mu(L)_p$, gives rise to a $\mathbb{Z}_{(p)}$-module $\mu(L)_p \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$. We can decompose in a similar way $\mu(L^H)_p \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ as a direct sum of $\mathbb{Z}_{(p)}$-modules:

$$\mu\big(L^H\big)_p \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)} = \bigoplus_{n=1}^{\infty} \frac{\mathbb{Z}_{(p)}}{p^n \mathbb{Z}_{(p)}}^{k_{H,p,n}}.$$

The N_{L/L^H} and i_{L,L^H} group homomorphism give rise to $\mathbb{Z}_{(p)}$-module homomorphisms from $\mu(L)_p \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ to $\mu(L^H)_p \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$. The desired result follows by Lemma 3.3 by taking $f_H = N_{L/L^H} \otimes \mathrm{Id}$ and $f^H = i_{L^H,L} \otimes \mathrm{Id}$. □

4. Analytic methods

In this section we give an analytic proof of Proposition 1.2. Consider the zeta function of an algebraic number field L,

$$\zeta_L(s) := \sum_{A \in I_L} \frac{1}{N(A)^s}, \quad \mathrm{Re}(s) > 1,$$

where A runs over the integral ideals I_L of the ring of integers of L. It is known that $\zeta_L(s)$ admits a meromorphic extension in $\mathbb{C} \setminus \{1\}$ with only one pole at $s = 1$. Moreover the residue at $s = 1$ can be computed [6, Satz VII 5.11]

$$\mathrm{Res}_{s=1} \zeta_L(s) = \lim_{s \to 1^+} (s-1)\zeta_L(s) = \frac{2^r (2\pi)^s \,\mathrm{Reg}(L)}{|\mu(L)|\sqrt{|D_L|}} h_L.$$

The Arakelov genus g_L of the number field L is defined by

$$g_L = \log \frac{|\mu(L)|\sqrt{|D_L|}}{2^r (2\pi)^s},$$

therefore

$$\mathrm{Res}_{s=1} \zeta_L(s) = e^{-g_L} \,\mathrm{Reg}(L) h_L.$$

Let $\sum r_H \varepsilon_H = 0$ be a norm idempotent relation. The product formula (1) implies that

$$\lim_{s \to 1^+} \sum r_H \log\big((s-1)\zeta_{L^H}(s)\big) = \sum r_H \lim_{s \to 1^+} \log(s-1).$$

The left-hand side is finite (the regulator of every number field is not zero), therefore $\sum r_H = 0$ and moreover

$$\sum r_H \big(-g_{L^H} + \log\big(\mathrm{Reg}\big(L^H\big) h_{L^H}\big)\big) = 0 \quad \Rightarrow \quad \sum r_H g_{L^H} = \sum n_h \log\big(\mathrm{Reg}\big(L^H\big) h_{L^H}\big). \tag{8}$$

Remark. The relation $\sum r_H = 0$ can also be proved by applying the character of the trivial representation on the sum $\sum r_H \varepsilon_H$.

On the other hand, using the functional equation of the $\zeta_{L^H}(s)$ we can prove that

$$\lim_{s\to 0} \frac{\zeta_{L^H}(s)}{s^{r_H+s_H-1}} = -\frac{h_{L^H}\operatorname{Reg}(L^H)}{|\mu(L^H)|},$$

therefore since $\lambda_H = r_H + s_H - 1$ and $\sum r_H \lambda_H = 0$ we have

$$\sum r_H \log\bigl(h_{L^H}\operatorname{Reg}\bigl(L^H\bigr)\bigr) = \sum r_H \log\bigl|\mu\bigl(L^H\bigr)\bigr|. \tag{9}$$

Combining (8), (9), we arrive at

$$\sum r_H g_{L^H} = \sum r_H \log\bigl(\mu\bigl(L^H\bigr)\bigr). \tag{10}$$

For every H, such that $(|H|, |\mu(L)|) = 1$, we write $|\mu(L^H)| = \prod_{i=1}^{r} p_i^{n_i k_{H,p_i,n}}$. The right-hand side of (10) is written

$$\sum_H r_H \log\bigl(\bigl|\mu\bigl(L^H\bigr)\bigr|\bigr) = \sum_H r_H \log\left(\prod_{i=1}^{r} p_i^{n_i k_{H,p_i,n}}\right) = \sum_{i=1}^{r} \log\bigl(p_i^{n_i}\bigr) \sum_H r_H k_{H,p_i,n} = 0$$

by Proposition 3.6 and the proof of Proposition 1.2 is now complete.

5. The η invariant

In order to apply the proof given in previous sections we would like to realize the function

$$\sum_{x\in\mathcal{O}_L} e^{-\pi\|x\|_L^2}$$

as the trace of a suitable linear operator.

If L is a number field we will denote by r the number of real embeddings and by s the number of complex nonequivalent embeddings. The Minkowski space is defined by

$$M(L) = \mathbb{R}^r \times \mathbb{C}^s,$$

and it can be seen as a real vector space of dimension $r+2s$. We will define the set of real infinite primes of L by $\mathbb{P}(L,\mathbb{R})$ and by $\mathbb{P}(L,\mathbb{C})$ the set of complex infinite primes. The field L can be embedded on the Minkowski space by the map

$$i_L : L \to M(L),$$

$$x \mapsto \bigl(\sigma_1(x), \ldots, \sigma_r(x), \sigma_{r+1}(x), \ldots, \sigma_{r+s}(x)\bigr).$$

For more information about the Minkowski space we refer to [6, I.5]. Every divisor

$$A = \sum_{\sigma \in \mathbb{P}(L,\mathbb{R})} a_\sigma \sigma + \sum_{\sigma \in \mathbb{P}(L,\mathbb{C})} a_\sigma \sigma,$$

supported on the set of infinite primes gives rise to the metric

$$\|x\|_{L,A}^2 = \sum_{\sigma \in \mathbb{P}(L,\mathbb{R})} |x_\sigma|^2 e^{-2a_\sigma} + \sum_{\sigma \in \mathbb{P}(L,\mathbb{C})} |x_\sigma|^2 2e^{-a_\sigma}, \tag{11}$$

where $x = (x_\sigma)$ is an element of the Minkowski space $M(L)$.

Let L/K be a Galois extension of number fields with Galois group $\mathrm{Gal}(L/K) = H$. An infinite complex prime σ of K is extended to $|H|$ infinite primes of L, i.e.,

$$\sigma = \sum_{i=1}^{|H|} \sigma_i. \tag{12}$$

On the other hand, an infinite real prime τ of K gives rise to $a(\tau)$ real infinite primes $\{\sigma_1, \ldots, \sigma_{a(\tau)}\}$ of L and to $b(\tau)$ pairs $\{\sigma_{a(\tau)+1}, \ldots, \sigma_{a(\tau)+b(\tau)}, \overline{\sigma_{a(\tau)+1}}, \ldots, \overline{\sigma_{a(\tau)+b(\tau)}}\}$ of complex infinite primes of L, where $a(\tau) + 2b(\tau) = |H|$. So the real infinite prime σ is decomposed in L as follows:

$$\sigma = \sum_{i=1}^{a(\tau)} \sigma_i + \sum_{j=1}^{b(\tau)} \sigma_{a(\tau)+j}^2. \tag{13}$$

Lemma 5.1. *Let L/K be a Galois extension of number fields, with Galois group H. Consider the set $\mathbb{P}(L,\infty)$ (respectively $\mathbb{P}(K,\infty)$) of infinite primes of L (respectively K) and let r_L, s_L (respectively r_K, s_K) denote the number of real and complex embeddings of K (respectively L). Let D be a divisor supported at the infinite primes of L, such that D is H-invariant, i.e.,*

$$D = \sum_{\sigma \in \mathbb{P}(L,\infty)} a_\sigma \sigma = \sum_{\tau \in \mathbb{P}(K,\infty)} a_\tau \sum_{\sigma | \tau} \sigma.$$

Let us denote by D^H the divisor

$$D^H = \sum_{\tau \in \mathbb{P}(K,\infty)} a_\tau \tau.$$

If $\|\cdot\|_{L,D}$ is the metric on the Minkowski space $\mathbb{R}^{r_L} \times \mathbb{C}^{s_L}$ introduced by D and $\|\cdot\|_{K,D^H}$ is the metric on the Minkowski space $\mathbb{R}^{r_K} \times \mathbb{C}^{s_K}$ introduced by D^H, then for every $x \in K \subset L$ considered as an element on the spaces $\mathbb{R}^{r_L} \times \mathbb{C}^{s_L}$ and $\mathbb{R}^{r_K} \times \mathbb{C}^{s_K}$ we have

$$\left\| i_L(x) \right\|_{L,D}^2 = |H| \cdot \left\| i_K(x) \right\|_{K,D^H}^2. \tag{14}$$

Proof. Let $x \in K \subset L$. We compute

$$\left\|i_K(x)\right\|_{K,D^H}^2 = \sum_{\tau\in\mathbb{P}(K,\mathbb{R})} \left|\tau(x)\right|^2 e^{-2a_\tau} + \sum_{\tau\in\mathbb{P}(K,\mathbb{C})} \left|\tau(x)\right|^2 2e^{-a_\tau}.$$

Observe that all infinite primes of L extending τ give on $x \in K$ the same value. Therefore, if $\tau \in \mathbb{P}(K,\mathbb{R})$ then the contribution to the norm of the infinite primes $a_\tau \sum_{\sigma|\tau} \sigma$ above τ is according to (13):

$$\left|\tau(x)\right|^2 \left(a(\tau)e^{-2a_\tau} + b(\tau)2e^{-2a_\tau}\right) = \left|\tau(x)\right|^2 |H| e^{-2a_\tau}.$$

On the other hand, if τ is a complex prime, then the contribution to the norm of the infinite primes above τ is according to (12)

$$\left|\tau(x)\right|^2 |H| 2e^{-a_\tau}.$$

The desired result follows by adding all the contributions of primes of L above each infinite prime τ of K. □

To every number field L we attach the Hilbert space V_L consisting of functions $f : \mathcal{O}_L \to \mathbb{R}$, such that $\sum_{y\in\mathcal{O}_L} |f(y)|^2 < \infty$.

Let H be a group acting on the number field L. The space V_L is acted on by H as follows:

$$f^h(x) = f(hx), \quad \text{for } h \in H.$$

Let V_{L^H} be the Hilbert space of functions $f : \mathcal{O}_{L^H} \to \mathbb{R}$ such that $\sum_{y\in\mathcal{O}_{L^H}} |f(y)|^2 < \infty$.

The norm idempotent ϵ_H induces a map $\epsilon_H^* : V_{L^H} \to V_L$, sending the function $f : \mathcal{O}_{L^H} \to \mathbb{R}$ to the function $f \circ \epsilon_H : \mathcal{O}_L \to \mathbb{R}$. Moreover we will consider the restriction map rest : $V_{\mathcal{O}_L} \to V_{\mathcal{O}_{L^H}}$ sending a function $f : \mathcal{O}_L \to \mathbb{R}$, to the restriction on $\mathcal{O}_{L^H}$.

Since the vector spaces we treat are of infinite dimension we cannot use the trace of the identity map. Instead, we consider the diagonal linear operator

$$T_D : V_{\mathcal{O}_L} \to V_{\mathcal{O}_L},$$

sending a function $f(x)$ to the function $T_D f(x) = e^{-\pi\|x\|_{L,D}^2} f(x)$. Let $\delta_x(\cdot)$ denote the basis functions

$$\delta_x(y) = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{if } x \neq y. \end{cases}$$

We observe that the trace of the linear operator $T_D \circ \epsilon$ is given by

$$\operatorname{tr}\left(T_D \circ \epsilon_H^*\right) = \sum_{x\in\mathcal{O}_L} \left\langle T \circ \epsilon_H^*(\delta_x), \delta_x \right\rangle = \sum_{x\in\mathcal{O}_{L^H}} e^{-\pi\|x\|_{L,D}^2}. \tag{15}$$

Indeed, if $x \in \mathcal{O}_L$ is an element of $\mathcal{O}_{L^H}$ then $\epsilon_H(x) = x$, and if $x \in \mathcal{O}_L \backslash \mathcal{O}_{L^H}$ then $\epsilon_H(x) \neq x$ since $\epsilon_H(x) \in \mathcal{O}_{L^H}$. We compute

$$\left\langle \epsilon_H^*(\delta_x), \delta_x \right\rangle = \begin{cases} 1 & \text{if } x \in \mathcal{O}_{L^H}, \\ 0 & \text{if } x \in \mathcal{O}_L \backslash \mathcal{O}_{L^H} \end{cases}$$

and the formula (15) follows. Suppose now that D is an H-invariant divisor. Then Eq. (14) together with (15) gives that

$$\operatorname{tr}\left(T_D \circ \epsilon_H^*\right) = \sum_{x \in \mathcal{O}_{L^H}} e^{-\pi \|x\|^2_{K, D^H |H|}}. \tag{16}$$

Proposition 5.2. *Given a number field K and a divisor A supported on infinite primes, define the numbers*

$$\eta_A(K) := \sum_{x \in \mathcal{O}_K} e^{-\pi \|x\|^2_{K,A}}.$$

If $\sum_H \lambda_H \epsilon_H = 0$ is a linear relation among norm idempotents, and D is a divisor supported on infinite primes of L and moreover it is H-invariant for all groups H that appear on the sum, then the following relation holds

$$0 = \sum_H \lambda_H \eta_{D+B(H)}\left(L^H\right),$$

where

$$B(H) = -\frac{\log(|H|)}{2} \sum_{\sigma \in \mathbb{P}(L^H, \mathbb{R})} \sigma - \log \frac{|H|}{2} \sum_{\sigma \in \mathbb{P}(L^H, \mathbb{C})} \sigma.$$

In particular if $D = 0$ then

$$0 = \sum_H \lambda_H \eta_{B(H)}\left(L^H\right).$$

Proof. The desired result follows by linearity of the trace map composed by T_D, the relation $\sum_H \lambda_H \epsilon_H = 0$ and Eq. (16). □

Observe that Proposition 1.3 is a special case of Proposition 5.2 for $D = 0$.

Acknowledgments

The author wishes to thank Professor G. van der Geer and the anonymous referee for their remarks and comments.

References

[1] Robert D.M. Accola, Two theorems on Riemann surfaces with noncyclic automorphism groups, Proc. Amer. Math. Soc. 25 (1970) 598–602.
[2] Richard Brauer, Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers, Math. Nachr. 4 (1951) 158–174.
[3] E. Kani, M. Rosen, Idempotent relations and factors of Jacobians, Math. Ann. 284 (2) (1989) 307–327.
[4] Ernst Kani, Michael Rosen, Idempotent relations among arithmetic invariants attached to number fields and algebraic varieties, J. Number Theory 46 (2) (1994) 230–254.
[5] Dino Lorenzini, An Invitation to Arithmetic Geometry, Grad. Stud. Math., vol. 9, Amer. Math. Soc., Providence, RI, 1996, xvi+397 pp.
[6] Jürgen Neukirch, Algebraische Zahlentheorie, Springer-Verlag, Berlin, 1992, xiii, 595 S. (in German).
[7] Gerard van der Geer, René Schoof, Effectivity of Arakelov divisors and the theta divisor of a number field, Selecta Math. (N.S.) 6 (4) (2000) 377–398.