数理解析研究所講究録 1376 巻 2004 年 92-102

IDEAL CLASS GROUPS AND KNOT THEORY

森下昌紀 (金沢大・理)
Masanori Morishita(Kanazawa Univ.)

Introduction

I would like to discuss a classical problem on ideal class groups from the viewpoint of the analogy between algebraic number theory and knot theory [Mo5].

The problem with which I am concerned here goes back to the work of C.F. Gauss [G] two hundred years ago. Namely, his theory of genera on binary quadratic forms is stated in terms of a number field as follows: Let $k = \mathbf{Q}(\sqrt{d})$ be a quadratic field with discrimiant d where $d = p_1 \cdots p_n$, $p_i \equiv 1 \bmod 4$ (for simplicity). Then the narrow ideal class group H_k of k has 2-rank $n-1$ so that the 2-primary part $H_k(2)$ of H_k has the form

$$H_k(2) = \bigoplus_{i=1}^{n-1} \mathbf{Z}/2^{a_i}\mathbf{Z} \quad (a_i \geq 1).$$

Since Gauss' time, it has been a problem to determine the whole structure of $H_k(2)$, namely to describe the 2^q-rank

$$e_q := \#\{i \mid a_i \geq q\} \quad (q \geq 1).$$

Among many works on this problem, L. Rédei [R1] showed the following remarkable formula

$$e_2 = n - 1 - \mathrm{rank}_{\mathbf{F}_2}(L_2), \quad L_2 = \begin{pmatrix} \left(\frac{d/p_1}{p_1}\right) & \left(\frac{p_2}{p_1}\right) & \cdots & \left(\frac{p_n}{p_1}\right) \\ \left(\frac{p_1}{p_2}\right) & \left(\frac{d/p_2}{p_2}\right) & \cdots & \left(\frac{p_n}{p_2}\right) \\ \vdots & \vdots & \ddots & \vdots \\ \left(\frac{p_1}{p_n}\right) & \left(\frac{p_2}{p_n}\right) & \cdots & \left(\frac{d/p_n}{p_n}\right) \end{pmatrix}$$

and further he gave similar formulas for e_3 in some cases using the triple symbol introduced by himself [R2]. Though many authors have studied this problem, in particular the case of $n = 2$, by using the power residue symbols and arithmetical consideration such as Pell's equations (see for example [B], [Ha], [Y] etc), it still remains a problem to obtain general formulas extending Rédei's mentioned above for higher e_q's.

As one easily see, the problem has an immediate generalization for a cyclic extension k over $\mathbf{Q}$ of arbitrary prime degree l and is formulated as a problem on the Galois module structure of the l-primary part $H_k(l)$ of the ideal class group H_k of k. Namely, by the genus theory of Iyanaga-Tamagawa [IT], $H_k(l)$ has the form $H_k(l) = \bigoplus_{i=1}^{n-1} \mathbf{Z}_l[\zeta]/\mathfrak{m}^{a_i}$ $(a_i \geq 1)$

where ζ is a primitive l-th root of unity and $\mathfrak{m}$ is the maximal ideal of $\mathbf{Z}_l[\zeta]$ generated by $\zeta - 1$. Hence the determination of the $\mathbf{Z}_l[\zeta]$-module structure of $H_k(l)$ is again equivalent to that of the $\mathfrak{m}^q$-rank $e_q := \#\{i \mid a_i \geq q\}$ $(q \geq 1)$.

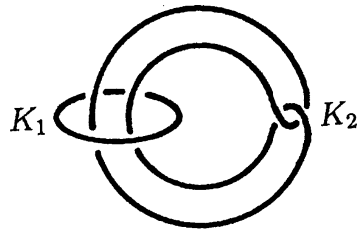
The result of mine is to give a solution to this problem (for general l) in light of the analogy between primes and knots (Theorem 5.4 below). The idea is to

regard Rédei's matrix L_2 as the mod 2 linking matrix for prime numbers $p_1, \cdots p_n$ and describe the e_q's by introducing the higher linking matrices defined in terms of the arithmetic Milnor invariants.

In fact, we introduce the *Alexander module* for prime numbers and give its presentation matrix by a sort of *universal higher linking matrix*, called the *Traldi matrix*, defined in terms of the Milnor invariants. Our higher linking matrices are then obtained by truncating and specializing the Traldi matrix.

As the analogy (cf. Section 1) suggests, we can ask a similar problem for the l-homology of a l-fold cyclic branched cover of a link. Actually, I first worked on this link-theoretic counterpart jointly with J. Hillman and D. Matei [HMM] and then translated each step of our arguments into the arithmetic. Then it turned out that the analogy between primes and knots is so close that the whole argument in topology side could be translated. So, knot theory is suggestive and useful for the study of such arithmetical problems to get the geometric intuition about what's going on. Conversely, I should say that our method to solve the link-theoretic counterpart is rather arithmetical in flavour of Iwasawa theory. We use the pro-l completion of a link group, l-adic Milnor invariants and the completed Alexander modules over the Iwasawa algebra. It seems to me that our results may indicate further possibilities of our arithmetic approach to link theory.

Finally, let me give an example illustrative of a picture in my mind: Let $L = K_1 \cup K_2$ be the following link of 2-components (Whitehead link) and let M be the double cover of S^3 branched over L.

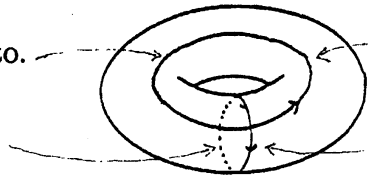


We then have the linking number $\mathrm{lk}(K_1, K_2) \equiv 0 \bmod 4$ and the Milnor number $\mu(1122) \equiv 1 \bmod 2$ from which it follows $H_1(M, \mathbf{Z})(2) = \mathbf{Z}/8\mathbf{Z}$. Here the condition $\mathrm{lk}(K_1, K_2) \equiv 0 \bmod 4$ corresponds to that on the 4-th power residue symbol $\left(\frac{p_1}{p_2}\right)_4 = \left(\frac{p_2}{p_1}\right)_4 = 1$ for $p_1, p_2 \equiv 1 \bmod 4$ in the arithmetic side. The latter is the condition (cf. [Y]) for the class number h_k of $k = \mathbf{Q}(\sqrt{p_1 p_2})$ is divisible by 8. Yamamoto gave a condition for h_k to be divisible by 16 using a solution of a certain Pell's equation. Our condition is given in terms of the higher linking number which is more conceptual.

1. Analogies between number fields and 3-manifolds

We start to recall basic analogies in *arithmetic topology* bridging algebraic number theory and 3-dimensional topology. This analogy was first noticed by B. Mazur in the 1960's and developed by A. Reznikov [Rez], M. Kapranov [K] and the author [Mo3,4] in recent years. Here is a part of the dictionary:

number ring $\mathrm{Spec}(\mathcal{O}_k) \cup \{\infty\}$ $\mathrm{Spec}(\mathbf{Z}) \cup \{\infty\}$	$\longleftrightarrow$	3-manifold M S^3
prime : $\mathrm{Spec}(\mathbf{F}_\mathfrak{p}) \subset \mathrm{Spec}(\mathcal{O}_k)$ primes $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ infinite prime	$\longleftrightarrow$	knot $K : S^1 \subset M$ link $K_1 \cup \cdots \cup K_n$ end
$\mathfrak{p}$-adic integers $\mathrm{Spec}(\mathcal{O}_\mathfrak{p})$	$\longleftrightarrow$	tube n.b.d $V(K)$
$\mathfrak{p}$-adic field $\mathrm{Spec}(k_\mathfrak{p})$	$\longleftrightarrow$	torus $\partial V(K)$
$\pi_1(\mathrm{Spec}(\mathcal{O}_\mathfrak{p})) = \langle\sigma\rangle$	$\longleftrightarrow$	$\pi_1(V(K)) = \langle\beta\rangle$
$\pi_1^{tame}(\mathrm{Spec}(k_\mathfrak{p})) = \langle\tau, \sigma \mid \tau^{p-1}[\tau, \sigma] = 1\rangle$	$\longleftrightarrow$	$\pi_1(\partial V(K)) = \langle\alpha, \beta \mid [\alpha, \beta] = 1\rangle$



$k^\times \to \bigoplus_{\mathfrak{p}:\text{primes}} \mathbf{Z}$ $a \mapsto a\mathcal{O}_k$	$\longleftrightarrow$	$C_2(M, \mathbf{Z}) \xrightarrow{\partial} C_1(M, \mathbf{Z})$ $\Sigma \mapsto \partial\Sigma$
class group H_k	$\longleftrightarrow$	$H_1(M, \mathbf{Z})$
$\mathcal{O}_k^\times$	$\longleftrightarrow$	$H_2(M, \mathbf{Z})$
$\pi_1(\mathrm{Spec}(\mathcal{O}_k) \setminus \{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\})$ max. Galois group with given ramification	$\longleftrightarrow$	$\pi_1(M \setminus K_1 \cup \cdots \cup K_n)$ link group
power residue symbol	$\longleftrightarrow$	linking number

For more analogies, we refer to [Mo3,4].

2. Milnor invariants

Throughout this note, we fix a prime number l. Let S be a set of n distinct prime numbers $p_1, \cdots, p_n$ such that $p_i \equiv 1 \bmod l$, $1 \leq i \leq n$. We write $p_i - 1 = m_i q_i$, $m_i = l^{f_i}$, $(l, q_i) = 1$, $1 \leq i \leq n$, and set $m_S = \min\{m_i \mid 1 \leq i \leq n\}$ and fix a power m of l with $1 \leq m \leq m_S$. Let G_S be the Galois group of the maximal pro-l extension $\mathbf{Q}_S$ of the rational number field $\mathbf{Q}$ unramified outside $S \cup \{\infty\}$, and let τ_i and σ_i be a *monodromy* and a *Frobenius automorphism* over p_i respectively (cf. [Mo1,2]). H. Koch [Ko] derived the following information on the presentation of the pro-l group G_S. Let F be the free pro-l group on n generators $x_1, \cdots, x_n$ and let $\pi : F \to G_S$ be the continuous homomorphism defined by $\pi(x_i) = \tau_i$ for $1 \leq i \leq n$. Then π is surjective and the kernel of π is the closed subgroup of F generated normally by $x_1^{p_1-1}[x_1, y_1], \cdots, x_n^{p_n-1}[x_n, y_n]$ where $y_i \in F$ represents σ_i in G_S and $[x_i, y_i] = x_i y_i x_i^{-1} y_i^{-1}$:

$$G_S = \langle x_1, \cdots, x_n \mid x_1^{p_1-1}[x_1, y_1] = \cdots = x_n^{p_n-1}[x_n, y_n] = 1 \rangle. \tag{2.1}$$

On the other hand, for a link L consisting of n knots $K_1, \cdots, K_n$ in the 3-sphere S^3, the pro-l completion $\widehat{G_L}$ of the topological fundamental group $G_L = \pi_1(S^3 \setminus L)$ of the complement of L in S^3 is shown to have the following presentation [HMM]:

$$\widehat{G_L} = \langle x_1, \cdots, x_n \mid [x_1, y_1] = \cdots = [x_n, y_n] = 1 \rangle \tag{2.2}$$

where x_i and y_i represent a *meridian* α_i and a *longitude* β_i around K_i respectively. Our basic idea is to *regard* (2.1) *as an arithmetic analogy of* (2.2). Note that the pair (τ_i, σ_i) of a monodromy and a Frobenius automorphism over p_i corresponds to the pair (α_i, β_i) of a meridian and a longitude around K_i. In view of this analogy, we introduce an arithmetic analogue for prime numbers S of the Milnor link invariants (higher linking numbers) [Mi],[Tu].

Let $\partial_i = \frac{\partial}{\partial x_i} : \mathbf{Z}_l[[F]] \to \mathbf{Z}_l[[F]]$ be the Fox derivative on the free pro-l group F for $1 \leq i \leq n$ ([F],[Ih]), and let $\epsilon : \mathbf{Z}_l[[F]] \to \mathbf{Z}_l$ be the augmentation map. We then define, for a multi-index $I = (i_1 \cdots i_r)$,

$$\mu(I) = \epsilon(\partial_{i_1} \cdots \partial_{i_{r-1}}(y_{i_r})), \quad \text{and} \quad \mu_m(I) = \mu(I) \bmod m.$$

By convention, we set $\mu(I) = 0$ for $|I| = 1$. We call $\mu(I)$ (resp. $\mu_m(I)$) the (resp. *mod* m) *Milnor number*. For a multi-index I, $1 \leq |I| < m_S$, we define the indeterminacy $\Delta(I)$ to be the ideal of $\mathbf{Z}/m\mathbf{Z}$ generated by the binomial coefficients $\binom{m_S}{t}$ and $\mu_m(J)$ where $1 \leq t < |I|$ and J ranges over all cyclic permutations of proper subsequences of I. We set

$$\overline{\mu}_m(I) = \mu_m(I) \bmod \Delta(I)$$

and we call them the Milnor $\overline{\mu}_m$ invariant for prime numbers S.

The following theorem asserts that the power residue symbol and the Rédei triple symbol [R2] are regarded as arithmetic analogues of the linking number and the triple linking number respectively:

Theorem 2.3. ([Mo1]) (1) *For $i \neq j$, we have $\left(\frac{p_j}{p_i}\right)_m = \zeta_m^{\mu_m(ij)}$ where $\left(\frac{p_j}{p_i}\right)_m$ denotes the m-th power residue symbol in $\mathbf{Q}_{p_i}$ and ζ_m is a primitive root of unity in $\mathbf{Q}_{p_i}$.*
(2) *Assume that $p_i \equiv 1$ mod 4 and the Legendre symbols $\left(\frac{p_j}{p_i}\right) = 1$ for $1 \leq i \neq j \leq 3$, and let $[p_1, p_2, p_2]$ denote the Redei triple symbol. Then we have*

$$[p_1, p_2, p_3] = (-1)^{\mu_2(123)}.$$

More generally, the Milnor invariants are interpreted as arithmetic symbols describing the prime decomposition law in Heisenberg extensions. Let $N_r(R)$ be the upper Heisenberg group of degree r over a commutative ring R, namely the group of upper triangular $r \times r$ unipotent matrices over R. For a multi-index $I = (i_1 \cdots i_r)$, $2 \leq r < m_S$ such that $\Delta(I) \neq \mathbf{Z}/m\mathbf{Z}$, we define a representation

$$\rho_I : F \longrightarrow N_r((\mathbf{Z}/m\mathbf{Z})/\Delta(I))$$

by

$$\rho_I(f) = \begin{bmatrix} 1 & \epsilon(\partial_{i_1}(f))_m & \epsilon(\partial_{i_1}\partial_{i_2}(f))_m & \cdots & \epsilon(\partial_{i_1}\cdots\partial_{i_{r-1}}(f))_m \\ & 1 & \epsilon(\partial_{i_2}(f))_m & \cdots & \epsilon(\partial_{i_2}\cdots\partial_{i_{r-1}}(f))_m \\ & & \ddots & \ddots & \vdots \\ & \mathbf{0} & & \ddots & \epsilon(\partial_{i_{r-1}}(f))_m \\ & & & & 1 \end{bmatrix} \mod \Delta(I).$$

Theorem 2.4. ([Mo2]). *Notations being as above,*
(1) *the representation ρ_I factors through G_S, and it gives a surjective representation of G_S onto $N_r((\mathbf{Z}/m\mathbf{Z})/\Delta(I))$ if $i_1, \cdots, i_{r-1}$ are distinct each other.*
(2) *Suppose $i_1, \cdots, i_{r-1}$ are distinct each other. If k_r denotes the extension of $\mathbf{Q}$ corresponding to $\mathrm{Ker}(\rho_I)$, $k_r/\mathbf{Q}$ is a Galois extension ramified over $p_{i1}, \cdots, p_{i_{r-1}}$ with Galois group $N_r((\mathbf{Z}/m\mathbf{Z})/\Delta(I))$ and we have*

$$\rho_I(\sigma_{i_r}) = \begin{bmatrix} 1 & 0 & \cdots & 0 & \mu_m(I) \\ & 1 & 0 & \cdots & 0 \\ & & \ddots & \ddots & \vdots \\ & \mathbf{0} & & 1 & 0 \\ & & & & 1 \end{bmatrix} \mod \Delta(I).$$

Hence, p_{i_r} is completely decomposed in $k_r/\mathbf{Q}$ if and only if $\overline{\mu}_m(I) = 0$.

3. The Alexander module of the Galois group G_S.

Let H_S be the abelianization of G_S and let $\psi : \mathbf{Z}_l[[G_S]] \to \mathbf{Z}_l[[H_S]]$ be the $\mathbf{Z}_l$-algebra homomorphism of the completed group rings induced by the natural map $G_S \to H_S$. Since $H_S \simeq \mathbf{Z}/m_1\mathbf{Z} \times \cdots \times \mathbf{Z}/m_n\mathbf{Z}$, $\mathbf{Z}_l[[H_S]]$ is isomorphic to $\mathbf{Z}_l[t_1, \cdots, t_n]/(t_1^{m_1} - 1, \cdots t_n^{m_n} - 1)$ which is identified with $\Lambda_S = \mathbf{Z}_l[[X_1, \cdots, X_n]]/((1+X_1)^{m_1} - 1, \cdots, (1+X_n)^{m_n} - 1)$ by sending t_i to $1 + X_i$. We write the same π to stand for the $\mathbf{Z}_l$-algebra homomorphism $\pi : \mathbf{Z}_l[[F]] \to \mathbf{Z}_l[[G_S]]$ of the completed group rings induced by π. By virtue of the presentation (2.1) of G_S, we define the *Alexander matrix* $P_S = (P_S(i,j))$ of G_S by

$$P_S(i,j) = \psi \circ \pi \left(\partial_j (x_i^{p_i - 1}[x_i, y_i]) \right)$$

and then the *Alexander module* A_S of G_S is given as the Λ_S-module presented by P_S:

$$A_S = \mathrm{Coker}({\Lambda_S}^n \xrightarrow{P_S} {\Lambda_S}^n).$$

Let H be the cyclic group $\langle t \mid t^m = 1 \rangle$ of order m and let $\lambda : H_S \to H$ be the homomorphism defined by $\lambda(t_i) = t$ for $1 \leq i \leq n$. The group ring $\mathbf{Z}_l[H]$ is identified with $\mathbf{Z}_l[t]/(t^m - 1) \simeq \mathbf{Z}_l[[X]]/((1+X)^m - 1)$ by which we denote Λ. We use the same λ for the $\mathbf{Z}_l$-algebra homomorphism $\Lambda_S \to \Lambda$ induced by λ. The *reduced Alexander matrix* $\overline{P}_S$ is then defined by $\lambda(P_S)$ and the *reduced Alexander module* $\overline{A}_S$ of G_S by the Λ-module presented by $\overline{P}_S$:

$$\overline{A}_S = \mathrm{Coker}(\Lambda^n \xrightarrow{\overline{P}_S} \Lambda^n) = A_S \otimes_{\Lambda_S} \Lambda.$$

We introduce the arithmetic analog of the Traldi matrix [Tr] as follows.

Definition 3.1. The *Traldi matrix* $T_S = (T_S(i,j))$ of G_S over Λ_S is defined by

$$T_S(i,j) = \begin{cases} X_i^{-1}((1+X_i)^{p_i - 1} - 1) - \displaystyle\sum_{r \geq 1} \sum_{\substack{1 \leq i_1, \cdots, i_r \leq n \\ i_r \neq i}} \mu(i_1 \cdots i_r i) X_{i_1} \cdots X_{i_r} & i = j \\ \mu(ji) X_i + \displaystyle\sum_{r \geq 1} \sum_{1 \leq i_1 \cdots i_r \leq n} \mu(i_1 \cdots i_r j i) X_i X_{i_1} \cdots X_{i_r} & i \neq j. \end{cases}$$

where $T_S(i,j)$ is regarded as an element of Λ_S and we also define the *reduced Traldi matrix* $\overline{T}_S$ of G_S over Λ by

$$\overline{T}_S = \lambda(T_S) = T_S(X, \cdots, X).$$

By computing the Alexander matrix in terms of the Milnor number using the Fox free differential calculus, we obtain

Theorem 3.2. *The Traldi matrix T_S (resp. reduced Traldi matrix $\overline{T}_S$) gives a presentation matrix of the Alexander module A_S (resp. reduced Alexander module $\overline{A}_S$) over Λ_S (resp. Λ).*

Finally, we introduce the *truncated Traldi matrices* as follows.

Definition 3.3. For $q \geq 2$, the *q-th truncated Traldi matrix* $T_S{}^{(q)} = (T_S{}^{(q)}(i,j))$ is defined by

$$T_S{}^{(q)}(i,j) = \begin{cases} X_i^{-1}((1+X_i)^{p_i-1}-1) - \sum_{r=1}^{q-1} \sum_{\substack{1 \leq i_1,\cdots,i_r \leq n \\ i_r \neq i}} \mu(i_1 \cdots i_r i) X_{i_1} \cdots X_{i_r} & i = j \\ \mu(ji)X_i + \sum_{r=1}^{q-2} \sum_{1 \leq i_1,\cdots,i_r \leq n} \mu(i_1 \cdots i_r ji) X_i X_{i_1} \cdots X_{i_r} & i \neq j \end{cases}$$

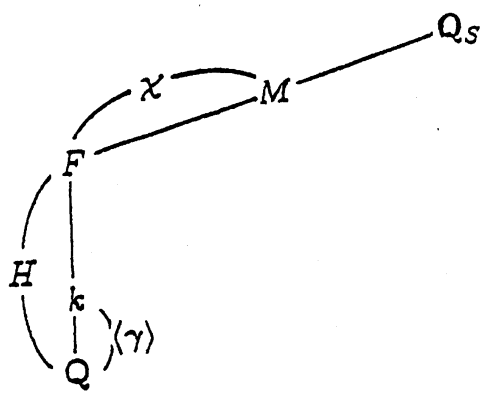
and we also define the *q-th truncated reduced Traldi matrix* $\overline{T}_S{}^{(k)}$ by

$$\overline{T}_S{}^{(q)} := \lambda(T_S{}^{(q)}) = T_S{}^{(q)}(X, \cdots, X).$$

Remark. We note $\overline{T}_S{}^{(2)} = X \cdot L^{(2)}$ where $L^{(2)} = (L^{(2)}(i,j))$ is given by $L^{(2)}(i,i) = -\sum_{j \neq i} \mu(ji), L^{(2)}(i,j) = \mu(ji)$ for $i \neq j$. By (1) of Theorem 2.3, Rédei's matrix L_2 [R1] mentioned in the introduction is essentially same as the *linking matrix* $L^{(2)}$. Thus our Traldi matrix T_S is regarded as a *universal higher linking matrix.*

4. Relation between the Alexander module and the l-class group

Let K be the subextension of $\mathbf{Q}_S/\mathbf{Q}$ corresponding to the kernel of $\lambda \circ \psi : G_S \to H$ so that K is a cyclic extension of degree m over $\mathbf{Q}$ with Galois group $\mathrm{Gal}(K/\mathbf{Q}) = H = \langle t \rangle$. Let k be the (unique) subfield of K of degree l over $\mathbf{Q}$ so that k is a cyclic extension of $\mathbf{Q}$ with Galois group $\mathrm{Gal}(k/\mathbf{Q}) = H/H^l = \langle \gamma \rangle$, $\gamma = t \bmod H^l$. Let M be the maximal abelian subextension of $\mathbf{Q}_S/K$ and let $\mathcal{X}$ denote the Galois group of M over K on which H acts via inner automorphism so that $\mathcal{X}$ is regarded as a Λ-module. Note that the narrow l-class group $H_k(l)$ of k is isomorphic to the Galois group over k of the narrow Hilbert l-class field of k by the Artin reciprocity map.



Firstly, we recall the Crowell exact sequence which gives the relation between the reduced Alexander module $\overline{A}_S$ and the Galois group $\mathcal{X}$.

Theorem 4.1 ([Mo1,Theorem 2.2.9]) *There is a split exact sequence of Λ-modules*

$$0 \longrightarrow \mathcal{X} \xrightarrow{\iota} \overline{A}_S \xrightarrow{\kappa} I_\Lambda \longrightarrow 0$$

where I_Λ is the augmentation ideal of Λ and ι and κ are given as follows: $\iota(g \bmod [\mathcal{Y},\mathcal{Y}]) = (\lambda \circ \psi \circ \pi(\partial_i(f))$ for $\pi(f) = g$ and $\kappa((\alpha_i) \bmod \mathrm{Im}(\overline{P}_S)) = (t-1)\sum_{i=1}^{n} \alpha_i$.

Next, we give the connection between $\mathcal{X}$ and the l-class group $H_k(l)$. Set $\nu_l(t) = 1+t+\cdots+t^{l-1}$. Since the norm $\nu_l(\gamma)$ acts trivially on $H_k(l)$, $H_k(l)$ is regarded as a module over the complete discrete valuation ring $\mathcal{O} := \mathbf{Z}_l[H]/(\nu_l(t)) = \Lambda/(\nu_l(1+X)) = \mathbf{Z}_l[\zeta]$ where $\zeta = t \bmod (\nu_l(t))$. The following theorem is proven by the standard arguments in Iwasawa theory [W].

Theorem 4.2. *Notation being as above, we have an isomorphism of $\mathcal{O}$-modules*

$$\mathcal{X}/\nu_l(t)\mathcal{X} \simeq H_k(l).$$

By Theorems 4.1 and 4.2, we obtain the following relation between the reduced Alexander module $\overline{A}_S$ and the l-class group $H_k(l)$, which is analogous to the relation between the reduced Alexander module of a link and the homology of a cyclic branched cover (cf. [Hi, 5.4,5.7]).

Theorem 4.3. *We have an isomorphism of $\mathcal{O}$-modules*

$$\overline{A}_S \otimes_\Lambda \mathcal{O} \simeq H_k(l) \oplus \mathcal{O}.$$

5. Galois module structure of the l-class group

We first recall the genus theory for the number field k [IT]. Let $\mathfrak{m}$ be the maximal ideal of $\mathcal{O}$ generated by $\varpi = \zeta - 1$ with residue field $\mathcal{O}/\mathfrak{m} = \mathbf{F}_l$ of l elements.

Lemma 5.1. *The dimension of $H_k(l) \otimes_{\mathcal{O}} \mathbf{F}_l$ over $\mathbf{F}_l$ is $n-1$.*

By Lemma 5.1, we have the isomorphism

$$H_k(l) \simeq \bigoplus_{i=1}^{n-1} \mathcal{O}/\mathfrak{m}^{a_i} \quad (a_i \geq 1)$$

of $\mathcal{O}$-modules. Hence the determination of the $\mathcal{O}$-module structure of $H_k(l)$ is equivalent to that of the $\mathfrak{m}^q$-rank

$$e_q = \#\{i \mid a_i \geq q\} = \dim_{\mathbf{F}_l} H_k(l) \otimes_{\mathcal{O}} \mathfrak{m}^{q-1}/\mathfrak{m}^q \quad (q \geq 1).$$

We describe the $\mathfrak{m}^q$-rank e_q in terms of the *higher linking matrices* obtained from the truncated reduced Traldi matrices (3.3) evaluated at $X = \varpi$.

Definition 5.2. The *higher linking matrix* $L_S = (L_S(i,j))$ over $\mathcal{O}$ is defined by

$$L_S(i,j) = \overline{T}_S(i,j)(\varpi) = \begin{cases} -\sum_{r\geq 1} \sum_{\substack{1\leq i_1,\cdots,i_r\leq n \\ i_r\neq i}} \mu(i_1\cdots i_r i)\varpi^r & i=j \\ \mu(ji)\varpi + \sum_{r\geq 1} \sum_{1\leq i_1,\cdots,i_r\leq n} \mu(i_1\cdots i_r ji)\varpi^{r+1} & i\neq j. \end{cases}$$

For $q \geq 2$, the *q-th truncated higher linking matrix* $L_S^{(q)}$ is defined by

$$L_S^{(q)}(i,j) = \overline{T}_S^{(q)}(i,j)(\varpi) = \begin{cases} -\sum_{r=1}^{q-1} \sum_{\substack{1\leq i_1,\cdots,i_r\leq n \\ i_r\neq i}} \mu(i_1\cdots i_r i)\varpi^r & i=j \\ \mu(ji)\varpi + \sum_{r=1}^{q-2} \sum_{1\leq i_1,\cdots,i_r\leq n} \mu(i_1\cdots i_r ji)\varpi^{r+1} & i\neq j. \end{cases}$$

By Theorems 3.2 and 4.3, we have

Theorem 5.3. *The higher linking matrix L_S gives a presentation matrix for the $\mathcal{O}$-module $H_k(l) \oplus \mathcal{O}$. For $q \geq 2$, the q-th truncated higher linking matrix $L_S^{(q)}$ gives a presentation matrix for the $\mathcal{O}/\mathfrak{m}^q$-module $(H_k(l) \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m}^q) \oplus \mathcal{O}/\mathfrak{m}^q$.*

Restating Theorem 5.3 in terms of e_q, we obatin our main formula.

Theorem 5.4. *For $q \geq 2$, we have*

$$e_q = n - 1 - \operatorname{rank}_{\mathbf{F}_l}\left(L_S^{(q)} \otimes \mathfrak{m}^{q-1}/\mathfrak{m}^q\right)$$

where for a $n \times n$ matrix A over $\mathcal{O}$, we denote by $A \otimes \mathfrak{m}^{q-1}/\mathfrak{m}^q$ the $\mathbf{F}_l$-linear map on $(\mathfrak{m}^{q-1}/\mathfrak{m}^q)^n$ induced by A.

For the initial term of $k = 2$, we recover Rédei's formula for arbitrary l.

Corollary 5.5. *We have*

$$e_2 = n - 1 - \operatorname{rank}_{\mathbf{F}_l}(L \bmod l)$$

where $L = (L_{ij})$ is the linking matrix defined by $L_{ii} = -\sum_{j\neq i} \mu(ji), L_{ij} = \mu(ji)$ for $i \neq j$.

Let us see the case of $n = 2$. By Lemma 5.1, $H_k(l)$ has m-rank 1

$$H_k(l) = \mathcal{O}/\mathfrak{m}^a \quad (a \geq 1)$$

and $e_q = 0$ or 1. By Theorem 4.5 we have

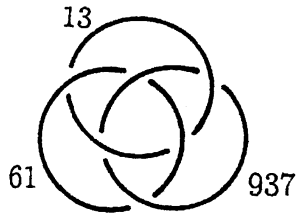
$$e_q = 1 \Longleftrightarrow L_S^{(q)} \equiv O_2 \bmod \varpi^q.$$

where O_2 is 2 by 2 zero matrix. Since $L_S^{(q)}(1,2) = -L_S^{(q)}(1,1)$, $L_S^{(q)}(2,2) = -L_S^{(q)}(2,1)$, we have the following

Corollary 5.6. *Suppose $n = 2$. For each $q \geq 1$, assuming $e_q = 1$, we have*

$$e_{q+1} = 1 \Longleftrightarrow \begin{cases} \sum_{r=1}^{q} \sum_{i_1,\cdots,i_{r-1}=1,2} \mu(i_1 \cdots i_{r-1}21)\varpi^r \equiv 0 \bmod \varpi^{q+1}, \\ \sum_{r=1}^{q} \sum_{i_1,\cdots,i_{r-1}=1,2} \mu(i_1 \cdots i_{r-1}12)\varpi^r \equiv 0 \bmod \varpi^{q+1}. \end{cases}$$

Example. D. Vogel [V] computed many Milnor invariants making the computer program. He finds that the triple $S = \{13, 61, 937\}$ is really an arithmetical analog mod 2 of the Borromean ring in the sense that $\mu_2(ij) = 0$ for all $1 \leq i, j \leq 3$ and $\mu_2(ijk) = 1$ for any parmutation ijk of 123 and $\mu_2(ijk) = 0$ for other ijk.



Further, we have all $\mu_4(ij) = 0$ (I owe this computation to Prof. K. Yamamura). We then find that $L_S^{(2)} \equiv O_3 \bmod 4$ and

$$L_S^{(3)} \equiv \begin{pmatrix} 0 & 4 & 4 \\ 4 & 0 & 4 \\ 4 & 4 & 0 \end{pmatrix} \bmod 8, \text{ i.e, } \operatorname{rank}_{\mathbf{F}_2}(L_S^{(3)} \otimes (4)/(8)) = 2$$

and so $e_2 = 2$ and $e_3 = 0$ by Theorem 4.4. Hence $H_k(2) = \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ for $k = \mathbf{Q}(\sqrt{13 \cdot 61 \cdot 937})$.

On the other hand, for the triple $\{5, 101, 8081\}$, all Milnor number $\mu_2(I)$ vanishes if $|I| \leq 3$ ([V]). Further all $\mu_4(ij) = 0$ (Yamamura) and so $L_S^{(3)} \equiv O_3 \bmod 8$. Hence $e_3 = 2$ and $H_k \otimes \mathbf{Z}/8\mathbf{Z} = \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ for $k = \mathbf{Q}(\sqrt{5 \cdot 101 \cdot 8081})$.

After the conference, Prof. K. Yamamura kindly informed me of the existence of [BS] where there is given an algorithm to calculate by computer the 2-part of a quadratic field with discriminant up to 500 figures. My approach is conceptual and geometric, and I think that the most essential aspect of my work lies in bridging two fields in mathematics.

REFERENCES

[B] H. Bauer, *Zur Berechnung der 2-Klassenzahl der quadratischen Zahlköper mit genau zwei verschiedenen Diskriminantenprimteilern*, J. Reine Angew. Math. **248** (1971), 42–46.

[BS] W. Bosma et P. Stevenhagen, *On the computation of quadratic 2-class groups*, J. Théor. Nombres Bordeaux (2) **8** (1996), 283–313; Erratum: **9** (1997), 249.

[F] R.H. Fox, *Free differential calculus. I: Derivation in the free group ring*, Ann. of Math **57** (1953), 547-560.

[G] C.F. Gauss, *Disquisitiones arithmeticae*, Yale Univ, 1966.

[Ha] H. Hasse, *An algorithm for determining the structure of the 2-Sylow-subgroups of the divisor class group of a quadratic number field*, Symposia Mathematica, Vol. XV (Convegno di Strutture in Corpi Algebrici, INDAM, Rome, 1973), Academic Press, London, 1975, pp. 341-352.

[Hi] J.A. Hillman; *Algebraic invariants of links*, Series on Knots and Everything, **32**, World Scientific Publishing Co, 2002.

[HMM] J. Hillman, D. Matei and M. Morishita, *Pro-p link groups and p-homology groups*, preprint, (2003).

[Ih] Y. Ihara, *On Galois representations arising from towers of coverings of* $\mathbf{P}^1\backslash\{0,1,\infty\}$, Invent. Math. **86** (1986), 427-459.

[IT] S. Iyanaga, T. Tamagawa, *Sur la theorie du corps de classes sur le corps des nombres rationnels*, J. Math. Soc. Japan **3** (1951), 220–227.

[K] M. Kapranov, *Analogies between number fields and 3-manifolds*, unpublished note (1996).

[Mi] J. Milnor, *Isotopy of links*, in Algebraic Geometry and Topology, A symposium in honour of S. Lefschetz (edited by R.H. Fox, D.S. Spencer and W. Tucker), Princeton Univ. Press, Princeton (1957), 280-306.

[Mo1] M. Morishita, *On certain analogies between knots and primes*, J. Reine Angew. Math. **550** (2002), 141-167.

[Mo2] ———, *Milnor invariants and Massey products for prime numbers*, Compositio Math. **140** (2004), 69-83.

[Mo3] ———, 数論と 3 次元トポロジー, 数理科学「トポロジーの新世紀」**6** 月号 (2003), 34-40.

[Mo4] ———, *Analogies between knots and primes, 3-manifolds and number fields*, Proceedings of JAMI conference "Primes and Knots" (2003) Baltimore, Contemp. Math., AMS.

[Mo5] ———, *Milnor invariants and l-class groups*, submitted (2004).

[R1] L. Rédei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math. **171** (1934), 55-60.

[R2] ———, *Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper, I*, J. Reine Angew. Math. **180** (1938), 1-43.

[Rez] A. Reznikov, *Embedded incompressible surfaces and homology of ramified coverings of three-manifolds*, Sel. math. New ser **6** (2000), 1-39.

[Tr] L. Traldi, *Milnor's invariants and the completions of link modules*, Trans. Amer. Math. Soc. **284** (1984), 401-424.

[Tu] V. Turaev, *Milnor's invariants and Massey products*, English transl. J. Soviet Math. **12** (1979), 128-137.

[V] D. Vogel, *Massey products in the Galois cohomology of number fileds*, Dissertation, Univ. Heidelberg (2004).

[Y] Y. Yamamoto, *Divisibility by* 16 *of class number of quadratic fields whose* 2*-class groups are cyclic*, Osaka J. Math. **21** (1984), 1–22.

[W.] L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, **83**, Springer-Verlag, New York, 1982.