Milnor's link invariants attached to certain Galois groups over Q

By Masanori MORISHITA

Department of Mathematics, Kanazawa University, Kakumamachi, Kanazawa, Ishikawa 920-1192

(Communicated by Shokichi IYANAGA, M. J. A., Feb. 14, 2000)

Abstract: This is a résumé of the author's recent work on certain analogies between primes and links. The purpose of this article is to introduce a new invariant, called Milnor invariant, in algebraic number theory, based on an analogy between the structure of a certain Galois group over the rational number field and that of the group of a link in three dimensional Euclidean space. It then turns out that the Legendre, Rédei symbols are interpreted as our link invariants. We expect that this is a tip of an arithmetical theory after the model of link theory which may give a new insight in algebraic number theory. The details will be published elsewhere.

Key words: Galois groups; link groups; Milnor invariants; Rédei symbol.

1. The Galois group with restricted ramification and the group of a link. In this section, we recall some basic results, due to Hasse, Iwasawa and Koch, on the structure of a certain Galois group with restricted ramification ([5]), and Milnor's results on the group of a link ([6], [7]).

Let l denote a fixed prime number throughout this article. Let p be a prime number which is congruent to 1 modulo l, $p \equiv 1 \bmod l$. Let $\mathbf{Q}_p(l)$ denote the maximal l-extension over the p-adic number field $\mathbf{Q}_p$. Then, the field $\mathbf{Q}_p(l)$ is generated by the primitive l^n-th root ζ_{l^n} of 1 and $\sqrt[l^n]{p}$ for all $n \geq 1$, and the Galois group $G_p(l)$ of $\mathbf{Q}_p(l)/\mathbf{Q}_p$ is generated topologically by two elements σ and τ which are defined by

$$(1.1)\qquad \begin{aligned} \sigma(\zeta_{l^n}) &= \zeta_{l^n}^p, \quad \sigma(\sqrt[l^n]{p}) = \sqrt[l^n]{p} \\ \tau(\zeta_{l^n}) &= \zeta_{l^n}, \quad \tau(\sqrt[l^n]{p}) = \zeta_{l^n}\sqrt[l^n]{p} \end{aligned}$$

where ζ_{l^n} are chosen so that $\zeta_{l^n}^{l^m} = \zeta_{l^{n-m}}$ for $n \geq m$. The inertia subgroup of $G_p(l)$ is generated by τ and σ is an extension of the Forbenius automorphism of the maximal unramified subextension of $\mathbf{Q}_p(l)/\mathbf{Q}_p$. The relation of between σ and τ is given by

$$\tau^{p-1}[\tau, \sigma] = 1$$

where $[\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1}$.

Let $p_1, \ldots, p_n$ be distinct n prime numbers so that $p_i \equiv 1 \bmod l$ for $1 \leq i \leq n$. Set $S = \{p_1, \ldots, p_n\}$ and let $G_S(l)$ be the maximal pro-l quotient of the étale fundamental group of the complement of S in Spec $\mathbf{Z}$: $G_S(l) = \pi_1(\mathrm{Spec}\,\mathbf{Z} \backslash S)(l)$. This is the Galois group of the maximal pro-l extension $\mathbf{Q}_S(l)$ over the rational number field $\mathbf{Q}$ which is unramified outside $S \cup \{\infty\}$, where ∞ is the infinite place of $\mathbf{Q}$, and it has the following group presentation. Choose a prime divisor $\wp_i$ in $\mathbf{Q}_S(l)$ over p_i for $1 \leq i \leq n$. The embedding $\mathbf{Q}_S(l) \hookrightarrow \mathbf{Q}_{p_i}(l)$ induces the surjective homomorphism $G_{p_i} \to G_i$ for each i, where G_i is the decomposition group of $\wp_i$. We choose a generator τ_i of the inertia group of $\wp_i$ and an extension σ_i of the Frobenius automorphism of the subfield corresponding to I_i so that σ_i and τ_i are the images of σ and τ given in 1.1 for $p = p_i$, respectively. We may see that σ_i is an extension of the Artin symbol $(\eta_i, \mathbf{Q}_S(l)^{ab}/\mathbf{Q})$ where $\mathbf{Q}_S(l)^{ab}$ is the maximal abelian subextension of $\mathbf{Q}_S(l)/\mathbf{Q}$ and η_i is the idele whose p_i-component is p_i and other components are all 1, and that τ_i is an extension of $(\lambda_i, \mathbf{Q}_S(l)^{ab}/\mathbf{Q})$ where λ_i is the idele whose p_i-component is a primitive root g_i mod p_i and other components are all 1. Define an integer $l_{i,j}$ by $p_i^{-1} \equiv g_j^{l_{i,j}} \bmod p_j$ for $1 \leq i \neq j \leq n$. Then, the Galois group $G_S(l)$ is generated topologically by $\tau_1, \ldots, \tau_n$ and the relations are given by

$$\tau_i^{p_i - 1}[\tau_i, \sigma_i] = 1, \quad 1 \leq i \leq n.$$

We also note that modulo the commutator $G_S(l)^{(2)} = [G_S(l), G_S(l)]$, we have the following con-

---

Dedicated to Prof. Takashi Ono on his seventy-first birthday.

1991 Mathematics Subject Classification. Primary 11R32; Secondary 57M25.

Partly supported by the Grants-in-Aid for Scientific Research (C), (No. 11640017), Ministry of Education, Science, Sports and Culture, Japan.

gruence relation:

$$\sigma_i \equiv \prod_{j\neq i} \tau_j^{l_{i,j}} \mod G_S(l)^{(2)}. \tag{1.2}$$

To state this result in terms of the group permutation, let $\mathcal{F}_n$ be the free pro-l group generated by the free words $x_1, \dots, x_n$ representing $\tau_1, \dots, \tau_n$ respectively and y_i is the (pro-l) word in $x_1, \dots, x_n$ representing σ_i $(1 \le i \le n)$. Then, the group $G_S(l)$ has the presentation

(1.3)

$$\begin{aligned} G_S(l) &= \langle x_1, \dots, x_n \mid x_i^{p_i-1}[x_i, y_i] = 1,\ 1 \le i \le n\rangle \\ &= \langle x_1, \dots, x_n \mid x_i^{p_i-1} \textstyle\prod_{j\neq i}[x_i, x_j]^{l_{i,j}} \rho = 1, \\ &\qquad \text{with } \rho \in \mathcal{F}_n^{(3)},\ 1 \le i \le n\rangle \end{aligned}$$

where $\mathcal{F}_n^{(3)}$ is the 3rd term of the lower central series of $\mathcal{F}_n$.

In turn, let L be a link in three dimensional Euclidean space $\mathbf{R}^3$ consisting of n-component knots $K_1, \dots, K_n$ and let G_L be the group of a link L: $G_L = \pi_1(\mathbf{R}^3 \backslash L)$. Milnor showed that the quotient $G_L/G_L^{(q)}$, where $G_L^{(q)}$ is the q-th term of the lower central series of G_L, $q \ge 1$, has the following presentation. Let F_n be the free group generated by the free words $\alpha_1, \dots, \alpha_n$ where α_i represents the i-th meridian a_i around K_i. Then, for each $n \ge 1$, there is a word $\beta_i^{(q)}$ in $\alpha_1, \dots, \alpha_n$ representing the i-th longitude b_i around K_i in $G_L/G_L^{(q)}$, and one has

$$\begin{aligned} G_L/G_L^{(q)} = \langle \alpha_1, \dots, \alpha_n \mid [\alpha_i, \beta_i^{(q)}] = 1, \\ 1 \le i \le n,\ F_r^{(q)} = 1\rangle \end{aligned} \tag{1.4}$$

and also sees that we have the following congruence relation:

$$b_i \equiv \prod_{j\neq i} a_j^{\mathrm{lk}(K_i, K_j)} \mod G_L^{(2)}. \tag{1.5}$$

where $\mathrm{lk}(K_i, K_j)$ is the linking number of K_i and K_j. We note that we can choose $\beta_i^{(q)}$ to be independent of q and reduce $G_L^{(q)}$ to the identity when the link L is obtained by the closure of a pure braid of n-strings and in this case the presentation of G_L is closer to that of $G_S(l)$.

Summing up, from the view point of Galois and link groups 1.2 $\sim$ 1.5, the elements τ_i and σ_i play similar roles to the meridian and longitude respectively and "primes look like a link !".

2. The Milnor invariant attached to a Galois group. In this section, we introduce an analog of the Milnor $\overline{\mu}$-invariant for a link ([7], [12]) in algebraic number theory, based on the analogy between Galois and link groups discussed in the previous section. We keep the same notations in the section 1.

Let $\mathbf{F}_l[[X_1, \dots, X_n]]_{nc}$ be the free power series ring in n noncommutting variables $X_1, \dots, X_n$ over the finite field $\mathbf{F}_l$ with l elements. The Magnus embedding of the free pro-l group $\mathcal{F}_n$ is the injective group homomorphism $\mathcal{F}_n \to \mathbf{F}_l[[X_1, \dots, X_n]]_{nc}^{\times}$ sending x_i to $1 + X_i$ and x_i^{-1} to $1 - X_i + X_i^2 - \cdots$ for $1 \le i \le n$. By this embedding, we identify an element f of $\mathcal{F}_n$ with its Magnus expansion, denoted by $1 + \sum \epsilon_I(f) X_I$, where I is a multi-index $I = (i_1 \cdots i_r)$ of length r $(r \ge 1)$, $1 \le i_1, \dots, i_r \le n$. Alternative description of $\epsilon_I(f)$ is given by using the Magnus embedding $\mathcal{F}_n \hookrightarrow \mathbf{Z}_l[[X_1, \dots, X_n]]_{nc}$ over l-adic integer ring $\mathbf{Z}_l$ and the Fox free differential calculus founded by Ihara [4] for free almost pro-l groups:

$$\epsilon_I(f) = \epsilon\left(\frac{\partial^r f}{\partial x_{i_1} \cdots \partial x_{i_r}}\right) \mod l$$

where ϵ is the augmentation homomorphism $\mathbf{Z}_l[[X_1, \dots, X_n]]_{nc} \to \mathbf{Z}_l$.

We then define the *Milnor μ_l-invariant*, denoted by $\mu_l(I)$, for a multi-index $I = (i_1 \cdots i_r)$ $(r \ge 1)$ by

$$\mu_l(J) := \epsilon_{I'}(y_{i_r}) \in \mathbf{F}_l$$

where $I' = (i_1 \cdots i_{r-1})$. By convention, we set $\mu_l(I) = 0$ for an index I of length 1. As Milnor concerned, we should care whether $\mu_l(I)$ is an invariant of the Galois group $G_S(l)$. First, as for $\mu_l(ij)$ for a multi-index of length 2, we have the following interpretation as "linking number".

Theorem 2.1. *Let i, j be indeces between* 1 *and n. When $i = j$, we have $\mu_l(ii) = 0$. When $i \neq j$, we have*

$$\zeta_l^{\mu_l(ij)} = \zeta_l^{l_{j,i}} = \left(\frac{p_j}{p_i}\right)_l$$

where ζ_l is a primitive l-th root of 1 given in (1.1) *and $(p_j/p_i)_l = (p_j, p_i/\mathbf{Q}_{p_i})$ is the l-th power* (*norm*) *residue symbol in $\mathbf{Q}_{p_i}$. In particular, $\zeta_l^{\mu_l(ij)}$ depends only on p_i, p_j and l. If p_i, $p_j \equiv 1 \mod 4$, we have the symmetry $\mu_l(ij) = \mu_l(ji)$.*

We call $\mu_l(ij)$ *the linking number of* p_i *and* p_j $\mod l$, denoted by $\mathrm{lk}_l(p_i, p_j)$, in view of 1.2, 1.5 and 2.1.

Remark 2.2. Waldspurger [13] introduced the linking number of two prime numbers for the case $l \neq 2$, in the cohomological manner using Artin-Verdier duality, and expressed it by the norm residue symbol. The result is essentially same as ours.

The Milnor invariant for a link involves a certain indeterminacy so that it becomes an isotopy invariant. In our case, $\mu_l(I)$ is well-defined as an invariant of the Galois group $G_S(l)$ in the following manner.

Let l^{m_i} be the maximal power of l dividing $p_i - 1$ for $1 \le i \le n$, and set $m = \min\{m_i | 1 \le i \le n\}$

Theorem 2.3. *Let r be an integer with $2 \le r \le l^m - 1$ and suppose that $\mu_l(J) = 0$ for any multi-index J of length $\le r-1$. Then, for a multi-index I of length r, $\mu_l(I)$ is independent of the choice of $\wp_i$ and an invariant of $G_S(l)$, namely, $\mu_l(I)$ is not changed under the following operations*:

1) *x_i or y_i is replaced by a conjugate,*
2) *y_i is multiplied by a product of conjugates of words $x_i^{p_i-1}[x_i, y_i]$.*

Remark 2.4.

1) Under the same assumption of the above theorem, let $i_1 \cdots i_s$ and $j_1 \cdots j_t$ be multi-indices with $s+t = r-1$. Then, by a theorem of Chen-Fox-Lyndon ([1]), we have the shuffle relation
$$\sum \mu_l(h_1 \cdots h_{s+t} k) = 0,$$
$h_1 \cdots h_{s+t}$ ranges over all proper shuffles of $i_1 \cdots i_s$ and $j_1 \cdots j_t$ (cf [7]).
2) In our choice of σ_i and τ_i, 1.1 means a normalization. In general, an extension of the Frobenius automorphism for $\wp_i$ has the ambiguity by the multiplication of τ_i^c, $c \in \mathbf{Z}_l$. However, when j is distinct from $j_1, \ldots, j_s$, then $\mu_l(j_1 \cdots j_s i)$ does not change if σ_i is replaced by $\sigma_i \tau_i^c$.

Let $\mathbf{F}_l[[G]]$ be the completed group ring of a pro-l group G over $\mathbf{F}_l$ and I_G its augmentation ideal. Let G_q be the Zassenhaus filtration of G defined by
$$G_q = \{g \in G \mid g - 1 \in I_G^q\}$$
for an integer $q \ge 1$. By the definition of our Milnor invariant, we have the following

Theorem 2.5. *Let r be an integer with $1 \le r \le l^m$. Suppose $\mu_l(I) = 0$ for any multi-index I of length $\le r$. Then, for any $q \le r$, the canonical homomorphism $\mathcal{F}_n \to G_S(l)$ induces the isomorphism*
$$\mathcal{F}_n/(\mathcal{F}_n)_q \xrightarrow{\sim} G_S(l)/G_S(l)_q.$$

3. Relation with the Rédei symbol.

Rédei [10] introduced a triple symbol $[a_1, a_2, a_3]$ which describes a prime decomposition law in a certain dihedral extension of degree 8. In this section, we interpret the Rédei symbol as our 3-rd order Milnor invariant when a_1, a_2, a_3 are prime numbers and $\mu_2(ij) = 0$ for $1 \le i,\ j \le 3$.

Let p_1, p_2, p_3 be distinct prime numbers $\equiv 1 \bmod 4$. We assume
$$\left(\frac{p_i}{p_j}\right)_2 = 1,\ 1 \le i, j \le 3 \tag{3.1}$$
or equivalently
$$\mu_2(ij) = 0,\ 1 \le i,\ j \le 3.$$
Set $k_i = \mathbf{Q}(\sqrt{p_i})$, $i = 1,\ 2$ and $k_{12} = k_1 k_2$. We assume that there is an algebraic integer $\theta_2 \in k_1$ such that $N_{k_1/\mathbf{Q}}(\theta_2) = \theta_2 \overline{\theta_2} = p_2$ and that $\theta_1 := (\sqrt{\theta_2} + \sqrt{\overline{\theta_2}})^2$ also satisfies $N_{k_2/\mathbf{Q}}(\theta_1) = \theta_1 \overline{\theta_1} = p_1$. Set $K = k_{12}(\sqrt{\theta_1}) = k_{12}(\sqrt{\theta_2})$. Then, we see that $K/\mathbf{Q}$ is a dihedral extension of degree 8. Such examples are supplied when $(p_1, p_2, p_3) = (5, 41, 61)$, $(5, 29, 181)$ for instance. By our assumption, p_3 is completely decomposed in the extension $k_{12}/\mathbf{Q}$. Take a prime divisor $\wp$ in k_{12} over p_3. The Rédei symbol is then defined by
$$[p_1, p_2, p_3] = \begin{cases} 1, & \left(\frac{K/k_{12}}{\wp}\right) = \mathrm{id} \\ -1, & \text{otherwise} \end{cases} \tag{3.2}$$

Now, for $S = \{p_1, p_2, p_3, \infty\}$, we have $K \subset \mathbf{Q}_S(2)$ and the canonical projection $\mathcal{F}_3 \to G_S(2) \to \mathrm{Gal}(K/\mathbf{Q})$. The images $\overline{x_i}$ of $x_i \in \mathcal{F}_3$ generate $\mathrm{Gal}(K/\mathbf{Q})$ and for suitable choices of $\wp_i$ in the section 1, we may assume that the relations are given by
$$\overline{x_1}^2 = \overline{x_2}^2 = 1, \quad (\overline{x_2 x_1})^4 = 1, \quad \overline{x_3} = 1.$$
We note that these relations do not affect the computation of $\mu_2(123)$, the coefficient of $X_1 X_2$ in the Magnus expansion of y_3, and so it is an invariant for $\mathrm{Gal}(K/\mathbf{Q})$. Then we have the following

Theorem 3.3. $(-1)^{\mu_2(123)} = [p_1, p_2, p_3]$.

Example 3.4. $(p_1, p_2, p_3) = (5, 41, 61)$, $(5, 29, 181)$. Then we have
$$\mathrm{lk}_l(p_i, p_j) = 0 \quad \text{for} \quad 1 \le i \le 3, \qquad \mu_2(123) = 1.$$
Namely, any two of p_1, p_2, p_3 are unlinked, but we cannot pull the three of them apart. We wish to call these prime numbers *Borromean primes mod* 2 after the model of Borromean ring (cf [9] 6.4).

Remark 3.5. As Murasugi [8] interpreted the Milnor invariant as a covering linkage invariant for a certain finite nilpotent covering space, 3.2 and 3.3 suggest that our Milnor invariant may also be interpreted as the Artin symbols in a certain nilpotent extension.

Remark 3.6. We may introduce an analog of the Alexander module as a certain ideal in $\mathbf{F}_l[G_S(l)/G_S(l)^{(2)}] = \mathbf{F}_l[\mathbf{Z}/(l^{m_1}) \times \cdots \times \mathbf{Z}/(l^{m_n})]$ after the model of link theory ([2], [3]). It is certainly interesting to investigate the realtions with the Milnor invariant.

Remark 3.7. The analogy between Galois and link groups discussed in this article suggests that the Galois group of a finite algebraic number field with a certain ramification condition may have an analogous nature that a certain three-manifold group does. We note that Reznikov [11] explored an *arithmetic topology* after the model of class field and Golod-Shafarevich theory, where his results concern the geometry of three manifolds, but philosophy seems to be close to ours.

Acknowledgement. I wish to thank T. Ono for his inspiring remark on the analogy between Gauss sum and Gauss integral expressing the linking number and for encouraging me to write up my ideas in this article. The analogy between Milnor invariant and Rédei symbol was kindly suggested to me by M. Kontsevich. Many thanks go to J. Hillman and K. Murasugi for answering my questions on link theory patiently and encouraging me to pursue this work. I am also thankful to J. Morava for drawing my attention to Reznikov's work, and to Y. Furuta and A. Nomura for communications on Rédei symbol and l-extensions. Finally, I am grateful to K. Lai and University of Sydney, and to V. Platonov and University of Waterloo for their support and hospitality during the summer and autumn of 1999, while this work was developed.

References

[1] Chen, K., Fox, R. H. and Lyndon, R. C.: Free differential calculus, IV. The quotient groups of the lower central series, Ann. of Math., **68**, 81–95 (1958).

[2] Hillman, J.: Alexander Ideals of Links. Lec. Note in Math., **895**, Springer, Berlin-Heidelberg-New York (1981).

[3] Hillman, J.: Algebraic invariants of links, enlarged edition of [H1] (preprint).

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

[5] Koch, H.: Galoissche Theorie der p-Erweiterungen. Springer, Berlin-Heidelberg-New York (1970).

[6] Milnor, J.: Link groups. Ann. of Math., **59**, 177–195 (1954).

[7] Milnor, J.: Isotopy of Links, in Algebraic Geometry and Topology, A symposium in Honour of S. Lefshetz. (eds. Fox, R. H., Spencer D. S. and Tucker, W.). Princeton Univ. Press, Princeton, pp. 280–306 (1957).

[8] Murasugi, K.: Nilpotent coverings of links and Milnor's invariant. Low-dimensional topology, London Math. Soc. Lecture Note Ser., **95**, Cambridge Univ. Press, Cambridge-New York, 106–142 (1985).

[9] Murasugi, K., and Kurpita, B. I.: A Study of Braids. Math. Appl., **484**, Kluwer Acad. Publ., Dordrecht-Boston-London (1999).

[10] Rédei, L.: Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper. I. J. Reine Angew. Math., **180**, 1–43 (1938).

[11] Reznikov, A.: Three-manifolds class field theory (Homology of coverings for a nonvirtually b_1-positive manifold). Sel. Math. New Ser., **3**, 361–399 (1997).

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

[13] Waldspurger, J.-L.: Entrelacements sur Spec($\mathbf{Z}$). Bull. Sci. Math., **100**, 113–139 (1976).