Compositio Math. 140 (2004) 69–83
DOI: 10.1112/S0010437X03000137

Milnor invariants and Massey products for prime numbers

Masanori Morishita

Dedicated to Professor Yoshiomi Furuta

Abstract

Following the analogy between primes and knots, we introduce the refined Milnor invariants for prime numbers and establish their connection with certain Massey products in Galois cohomology. This generalizes the well-known relation between the power residue symbol and cup product and gives a cohomological interpretation of L. Rédei's triple symbol.

Introduction

In our previous paper [Mor02a], we discussed foundational analogies between knots and primes, based on an analogy between the structure of a link group and that of a certain maximal pro-l Galois group, l being a prime number, over the rational number field $\mathbb{Q}$ with given ramification. In particular, we introduced arithmetic analogues of Milnor's link invariants for prime numbers and showed that the classical symbols by Legendre and Rédei could be interpreted as our Milnor invariants [Mor02a, § 3]. The purpose of the present paper is to continue this line of study and investigate the connection between our Milnor invariants and certain Massey products in Galois cohomology following link theory.

The Massey products were first introduced by Massey [Mas58] as higher order cohomology operations generalizing the cup product to describe the higher linking properties, and their fundamental properties were investigated by Kraines [Kra66] and May [May69] in general contexts. Their connection with the Milnor invariants for links was conjectured by Stallings [Sta65] and proven by Turaev [Tur79] and Porter [Por80]. Following the analogy between knots and primes (cf. [Kap96, Maz65, Mor00, Mor01a, Mor01b, Mor01c, Mor02a, Mor02b, Mor03, Rez00, Sik01, Wal76]), we investigate in this paper their analogies for prime numbers and establish an arithmetic analog of Turaev–Porter's theorem. This generalizes the well-known relation between the power residue symbol and the cup product (cf. [Koc70, Ser68]), and also gives a cohomological interpretation of the triple symbol of Rédei [Réd38, Fur80].

The contents are organized as follows. In § 1, we refine our Milnor μ_l-invariants for primes in [Mor02a] by introducing a certain indeterminacy following the construction of Milnor's $\overline{\mu}$-invariants of a link [Mil57] and give some basic properties for the refined invariants. In § 2, we introduce the Massey products in the context of the cohomology of profinite groups and recall basic properties needed for our arithmetic applications, and then we establish the relation between the Milnor invariants for primes and the Massey products in the Galois cohomology. Here, we apply Turaev's

Received 27 September 2002, accepted in final form 4 March 2003.
2000 Mathematics Subject Classification 11R, 57M.
Keywords: Primes and knots, Milnor invariants, Massey products.
The author was partially supported by the Grants-in-Aid for Scientific Research (C), Ministry of Education, Culture, Sports, Science and Technology, Japan.

argument for links [Tur79] to our arithmetic for primes introducing the notion of the normalized Massey system in Galois cohomology, based on the analogy between a link group and our Galois group.

Convention. For a profinite group G, the lower central series of G is defined by $G^{(1)} = G$, $G^{(q+1)} = [G^{(q)}, G]$ for $q \geqslant 1$ where $[A, B]$ stands for the closed subgroup generated by $[a, b] = a^{-1}b^{-1}ab$, $a \in A$, $b \in B$. For a profinite commutative ring R, we denote by $R[[G]]$ the completed group ring and by $I_{R[[G]]}$ the augmentation ideal, the kernel of the augmentation map $\epsilon_{R[[G]]} : R[[G]] \longrightarrow R$. For a profinite group G, the Zassenhaus filtration of G over the ring $\mathbb{Z}/m\mathbb{Z}$, $m > 1$, is defined by $G_{1,m} = G, G_{q,m} = G \cap (1 + I^q_{\mathbb{Z}/m\mathbb{Z}[[G]]})$ for $q \geqslant 1$.

1. The refined Milnor invariants for prime numbers

In this section, we refine the Milnor μ_l-invariants for prime numbers in [Mor02a] by introducing a certain indeterminacy along the line of the construction of the Milnor $\overline{\mu}$-invariants of a link [Mil57], and give their basic properties. Throughout this paper, we denote by l a given prime number.

1.1 The pro-l Galois group with restricted ramification

Let S be a given finite set of n distinct prime numbers $p_1, \ldots, p_n$ such that $p_i \equiv 1 \bmod l$, $1 \leqslant i \leqslant n$. We write $p_i - 1 = l^{e_i}q_i$, $(l, q_i) = 1$, $1 \leqslant i \leqslant n$, and set $e_S = \min\{e_i \mid 1 \leqslant i \leqslant n\}$. In the following, we fix a power $m = l^e$ of l with $1 \leqslant e \leqslant e_S$. Let $G_S(l)$ be the maximal pro-l quotient of the étale fundamental group of the complement of S in $\mathrm{Spec}(\mathbb{Z})$ which is the Galois group of the maximal pro-l extension $\mathbb{Q}_S(l)$ of $\mathbb{Q}$ unramified outside $S \cup \{\infty\}$, where ∞ is the infinite prime of $\mathbb{Q}$. The structure of the pro-l group $G_S(l)$ is given as follows [Mor02a, § 1.2]; [Koc70]. Choose a prime $\mathfrak{p}_i$ of $\mathbb{Q}_S(l)$ lying over p_i for $1 \leqslant i \leqslant n$. Let τ_i be a generator of the inertia group I_i of $\mathfrak{p}_i$, called a *monodromy* over p_i, and let σ_i be an extension of the Frobenius automorphism of the subfield corresponding to I_i, called a *Frobenius automorphism* over p_i. We may see that σ_i is an extension of the Artin symbol $(\eta_i, \mathbb{Q}_S(l)^{ab}/\mathbb{Q})$ and τ_i is an extension of $(\lambda_i, \mathbb{Q}_S(l)^{ab}/\mathbb{Q})$ where $\mathbb{Q}_S(l)^{ab}$ is the maximal abelian subextension of $\mathbb{Q}_S(l)/\mathbb{Q}$, η_i (respectively λ_i) is the idele whose p_i-component is p_i (respectively a primitive root g_i mod p_i), and other components are all 1. Then one has the following information on the presentation of the pro-l group $G_S(l)$. Let F be the free pro-l group on the words $x_1, \ldots, x_n$ representing $\tau_1, \ldots, \tau_n$, respectively, and $y_i \in F$ the pro-l word in $x_1, \ldots, x_n$ representing σ_i $(1 \leqslant i \leqslant n)$. The Galois group $G_S(l)$ has the following minimal presentation [Koc70, § 11]

$$1 \longrightarrow N \longrightarrow F \xrightarrow{\pi} G_S(l) \longrightarrow 1 \tag{1.1.1}$$

where N is the closed subgroup of F generated normally by $x_i^{p_i-1}[x_i^{-1}, y_i^{-1}]$, $1 \leqslant i \leqslant n$. Here we see the following group-theoretic analogy[1] between a prime p and a knot K:

$$\begin{aligned} \text{monodromy over } p &\longleftrightarrow \text{meridian around } K \\ \text{Frobenius auto. over } p &\longleftrightarrow \text{longitude around } K. \end{aligned} \tag{1.1.2}$$

Moreover, we observe the analogy between a p-adic field $\mathbb{Q}_p$ and the boundary of the tubular neighborhood V_K of K:

$$\begin{aligned} \mathrm{Spec}(\mathbb{Q}_p) &\longleftrightarrow \partial V_K \\ \mathrm{Gal}(\mathbb{Q}_p(l)/\mathbb{Q}_p) = \langle x, y \mid x^{p-1}[x^{-1}, y^{-1}] = 1 \rangle &\longleftrightarrow \pi_1(\partial V_K) = \langle x, y \mid [x, y] = 1 \rangle, \end{aligned} \tag{1.1.3}$$

where $\mathbb{Q}_p(l)$ is the maximal pro-l extension of $\mathbb{Q}_p$.

[1] Strictly speaking, a prime ideal (p) generated by p is an analog of a knot K and a prime number p itself is an analog of a 'Seifert surface' spanning (p) (cf. [Kap96, Mor02b, Rez00, Sik01]).

https://doi.org/10.1112/S0010437X03000137 Published online by Cambridge University Press

We define an integer $l_{i,j}$ by the relation $p_i^{-1} \equiv g_j^{l_{i,j}} \bmod p_j$ for $1 \leqslant i \neq j \leqslant n$ and we then have

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

In view of the analogy (1.1.2), we call $l_{i,j} \bmod m$ the *linking number* mod m of p_i and p_j and denote it by $\mathrm{lk}_m(p_i, p_j)$ (cf. Example 1.3.1 below).

1.2 The Milnor $\overline{\mu_m}$-invariant

Let F be the free pro-l group on the words $x_1, \ldots, x_n$ representing $\tau_1, \ldots, \tau_n$ in the Galois group $G_S(l)$, respectively, and let $\mathbb{Z}/m\mathbb{Z}[[X_1, \ldots, X_n]]_{\mathrm{nc}}$ be the formal power series ring over $\mathbb{Z}/m\mathbb{Z}$ in n non-commuting variables $X_1, \ldots, X_n$. Recall that $m = l^e$ is a fixed power of l dividing all $p_i - 1$, $1 \leqslant e \leqslant e_S$. The Magnus embedding $M_m : F \longrightarrow (\mathbb{Z}/m\mathbb{Z}[[X_1, \ldots, X_n]]_{\mathrm{nc}})^\times$ over $\mathbb{Z}/m\mathbb{Z}$ is given by

$$M_m(x_i) = 1 + X_i, \quad M_m(x_i^{-1}) = 1 - X_i + X_i^2 - \cdots$$

for $1 \leqslant i \leqslant n$ and each element f of F has the Magnus expansion over $\mathbb{Z}/m\mathbb{Z}$,

$$M_m(f) = 1 + \sum_I \epsilon_I(f)_m X_I,$$

where I ranges over all multi-indices $I = (i_1 \cdots i_r)$ and $X_I = X_{i_1} \cdots X_{i_r}$for $|I| := r \geqslant 1$. In terms of the pro-l Fox free differential calculus [Iha86], the Magnus coefficient $\epsilon_I(f)_m$ is given by

$$\epsilon_I(f)_m = \epsilon_{\mathbb{Z}_l[[F]]}\left(\frac{\partial^r f}{\partial x_{i_1} \cdots \partial x_{i_r}}\right) \bmod m.$$

We then set, for a multi-index $I = (i_1 \cdots i_r)$,

$$\mu_m(I) = \epsilon_{I'}(y_{i_r})_m$$

where $I' = (i_1 \cdots i_{r-1})$ and y_j is the element of F representing σ_j in $G_S(l)$. By convention, we set $\mu_m(I) = 0$ for $|I| = 1$.

For a multi-index I, $1 \leqslant |I| \leqslant l^{e_S}$, we define $\Delta(I)$ to be the ideal of $\mathbb{Z}/m\mathbb{Z}$ generated by the binomial coefficients $\binom{l^{e_S}}{t}$ and $\mu_m(J)$, where $1 \leqslant t \leqslant |I|$ and J ranges over all cyclic permutations of proper subsequences of I. We then define the *Milnor* $\overline{\mu_m}$*-invariant* by

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

Our fundamental assertion, which refines Theorem 3.1.5 of [Mor02a], is the following.

Theorem 1.2.1. *Let I be a multi-index with $2 \leqslant |I| \leqslant l^{e_S}$. Then, $\overline{\mu_m}(I)$ is an invariant of the Galois group $G_S(l)$.*

Proof. Let $I = (i_1 \cdots i_r)$, $2 \leqslant r \leqslant l^{e_S}$, and $I' = (i_1 \cdots i_{r-1})$. As in Theorem 3.1.5 of [Mor02a], it suffices to show that $\overline{\mu_m}(I)$ is not changed under the following operations:

1) y_{i_r} is replaced by a conjugate;
2) some x_j is replaced by a conjugate;
3) y_{i_r} is multiplied by a product of conjugates of $x_j^{p_j-1}[x_j^{-1}, y_j^{-1}]$'s.

1) By comparing the coefficients of monomials on the both sides of the equation

$$M_m(x_j y_{i_r} x_j^{-1}) = (1 + X_j) M_m(y_i)(1 - X_j + X_j^2 - \cdots),$$

we have the congruence for any j

$$\epsilon_{I'}(x_j y_{i_r} x_j^{-1})_m \equiv \epsilon_{I'}(y_{i_r})_m$$

modulo the ideal for certain proper subsequences J of I'. This proves item 1.

https://doi.org/10.1112/S0010437X03000137 Published online by Cambridge University Press

2) Suppose that x_j is replaced by $\overline{x}_j = x_h x_j x_h^{-1}$ with $M_m(\overline{x}_j) = 1 + \overline{X}_j$. Then we have

$$X_j = (1 - X_h + X_h^2 - \cdots)\overline{X}_j(1 + X_h) = \overline{X}_j + (\text{terms involving } X_h\overline{X}_j \text{ or } \overline{X}_jX_h).$$

Thus, each time the factor X_j occurs in the expansion $M_m(y_{i_r}) = 1 + \sum_J \mu_m(Ji_r)X_J$, it is to be replaced by the above expansion and we finally reach the expansion of $M_m(y_{i_r})$ in $\overline{X}_1, \ldots, \overline{X}_n$, which we denote by $\overline{M}_m(y_{i_r})$. Then we see easily that the coefficient of $\overline{X}_{i_1} \cdots \overline{X}_{i_{r-1}}$ in $\overline{M}_m(y_{i_r})$ is of the form

$$\mu_m(I) + \sum_J \mu_m(Ji_r) \quad (J \text{ runs over certain proper subsequences of } I')$$

and it is congruent to $\mu_m(I)$ mod $\Delta(I)$. This proves item 2.

3) Firstly, we prove the following lemma which will also be used later on.

Lemma 1.2.2. *Let $J = (j_1 \cdots j_s)$ be a subsequence of I. Then we have, for $1 \leqslant j \leqslant n$,*

$$\epsilon_J(x^{p_j-1}[x_j^{-1}, y_j^{-1}])_m \equiv \begin{cases} \mu_m(j_2 \cdots j_s j_1), & j = j_1, \\ -\mu_m(J), & j = j_s, \\ 0, & \textit{otherwise}, \end{cases} \quad \text{mod } \Delta(J),$$

and so for any proper subsequence J of I we have $\epsilon_J(x^{p_j-1}[x_j^{-1}, y_j^{-1}]) \equiv 0$ mod $\Delta(I)$.

Proof of Lemma 1.2.2. First, note that $M_m(x_j^{p_j-1}) = (1 + X_j)^{l^{e_j}q_j} \equiv 1 +$ (terms of degree greater than s) mod $\Delta(J)$ by the definition of $\Delta(J)$. Next, we see that

$$\epsilon_J(x_jy_j)_m = \mu_m(Jj) \text{ if } j \neq i_1, \quad \epsilon_J(x_{i_1}y_{i_1})_m = \mu_m(Ji_1) + \mu_m(i_2 \cdots i_s i_1),$$
$$\epsilon_J(y_jx_j)_m = \mu_m(Jj) \text{ if } j \neq i_s, \quad \epsilon_J(y_{i_s}x_{i_s})_m = \mu_m(Ji_s) + \mu_m(J).$$

Since $M_m([x_j^{-1}, y_j^{-1}]) = 1 + (M_m(x_jy_j) - M_m(y_jx_j))M_m(x_j^{-1})M_m(y_j^{-1})$, we have

$$\epsilon_J([x_j^{-1}, y_j^{-1}]) \equiv \epsilon_J(x_jy_j)_m - \epsilon_J(y_jx_j)_m \equiv \begin{cases} \mu_m(j_2 \cdots j_s j_1), & j = j_1, \\ -\mu_m(J), & j = j_s, \\ 0, & \text{otherwise}. \end{cases} \quad \text{mod } \Delta(J),$$

Thus we get the first assertion. The second assertion follows from the definition of $\Delta(I)$ (it is here that cyclic permutations of the definition of $\Delta(I)$ are used). □

Now, let us show our assertion 3 in the theorem. By the formula of Fox's free derivative [Fox53, equation 3.2], we have

$$\epsilon_{I'}(x^{p_j-1}[x_j^{-1}, y_j^{-1}]y_{i_r}) = \epsilon_{I'}(y_{i_r})_m + \sum \epsilon_J([x_j^{-1}, y_j^{-1}])_m\mu_m(Ki_r) + \epsilon_{I'}(x^{p_j-1}[x_j^{-1}, y_j^{-1}])_m$$

where the sum is over partitions $I' = (J, K)$ with J and K non-empty. Hence, by Lemma 1.2.2, we obtain

$$\epsilon_{I'}(x_j^{p_j-1}[x_j^{-1}, y_j^{-1}]y_{i_r})_m \equiv \epsilon_{I'}(y_{i_r})_m \text{ mod } \Delta(I).$$

Similarly, we have $\epsilon_{I'}(y_{i_r}x_j^{p_j-1}[x_j^{-1}, y_j^{-1}])_m \equiv \epsilon_{I'}(y_{i_r})_m$ mod $\Delta(I)$ and the assertion 3 is proved. □

Remark 1.2.3. As the proof of Theorem 1.2.1 shows, the Milnor invariant is well defined with the smaller indeterminacy $\Delta^*(I)$, the ideal of $\mathbb{Z}/m\mathbb{Z}$ generated by $\binom{l^{e_S}}{t}$, $1 \leqslant t \leqslant |I| - 1$, and $\mu_m(J)$, J running over all cyclic permutations of proper subsequences of I. For example, $\Delta^*(ij) = 0$ while $\Delta(ij)$ may not be zero. However, the cyclic symmetry of the Milnor invariants holds only modulo $\Delta(I)$ (cf. Theorem 1.2.5(1) below), and further it is better work with $\Delta(I)$ in connection of the Massey products in the following section (cf. Definition 2.3.1 and Theorem 2.3.2). This is the reason that we introduced the milder indeterminacy $\Delta(I)$.

https://doi.org/10.1112/S0010437X03000137 Published online by Cambridge University Press

The following proposition shows that $\overline{\mu_m}(i_1\cdots i_r)$ depends only on the subset $\{p_{i_1},\dots,p_{i_r}\}$ of S. It justifies the notation used for the Milnor $\overline{\mu_m}$-invariant.

Proposition 1.2.4. *Let S' be a subset of S. We may assume that $S'=\{p_1,\dots,p_k\}$, $2\leqslant k<n$. Let $I=(i_1\cdots i_r)$ be a multi-index of integers with $1\leqslant i_1,\dots,i_r\leqslant k$. The two invariants $\overline{\mu_m}(I)$ and $\overline{\mu'_m}(I)$ are defined by means of the Galois groups $G_S(l)$ and $G_{S'}(l)$, respectively. Then we have $\overline{\mu_m}(I)=\overline{\mu'_m}(I)$.*

Proof. This is proved in the straightforward manner from the definition. □

As for the properties of $\overline{\mu_m}(i_1\cdots i_r)$ under the permutation of $i_1\cdots i_r$, we have the following theorem which can be seen as a generalization of the reciprocity law of Gauss and Rédei (cf. Examples 1.3.1 and 1.3.2 below).

Theorem 1.2.5. *Let r be an integer with $2\leqslant r\leqslant l^{e_S}$.*

1) *We have the cyclic symmetry*

$$\overline{\mu_m}(i_1\cdots i_r)=\overline{\mu_m}(i_2\cdots i_r i_1)=\cdots=\overline{\mu_m}(i_r i_1\cdots i_{r-1}).$$

2) *Let $I=(i_1\cdots i_s)$ and $J=(j_1\cdots j_t)$ be multi-indices with $s+t=r-1$, $s,t\geqslant 1$. Let Sh denote the set of all proper shuffles of I and J. Then we have the shuffle relation*

$$\sum_{H\in Sh}\overline{\mu_m}(Hk)\equiv 0 \ \mathit{mod}\ \mathit{g.c.d}\{\Delta(Hk)\mid H\in Sh\}.$$

Proof. 1) Let D be the two-sided ideal of $\mathbb{Z}/m\mathbb{Z}[[X_1,\dots,X_n]]_{\mathrm{nc}}$ consisting of elements $\sum_{|I|\geqslant 1}c_I X_I$ such that $c_I\equiv 0 \bmod \Delta(I)$ for $|I|\leqslant r$. Write $M_m(y_i)=1+\omega_i$, $\omega_i=\sum_I \mu_m(Ii)X_I$. Then we have, for $1\leqslant i\leqslant n$,

$$\begin{aligned}
M_m([x_i^{-1},y_i^{-1}]) &= 1+(M_m(x_iy_i)-M_m(y_ix_i))M_m(x_i^{-1})M_m(y_i^{-1})\\
&= 1+(X_i\omega_i-\omega_iX_i)(1-X_i+X_i^2-\cdots)(1-\omega_i+\omega_i^2-\cdots)\\
&= 1+(X_i\omega_i-\omega_iX_i)\\
&\quad\ +(\text{terms involving } X_jX_i\omega_i, X_j\omega_iX_i, X_i\omega_iX_j, \omega_iX_iX_j)\\
&\equiv 1+(X_i\omega_i-\omega_iX_i) \bmod D,
\end{aligned}$$

since Ii is a cyclic permutation of a proper subsequence of jiI, jIi, iIj, and Iij. In addition, $M_m(x_i^{p_i-1})\equiv 1 \bmod D$ by the definition of $\Delta(I)$ (cf. Remark 1.2.3). Hence we have

$$M_m(x_i^{p_i-1}[x_i^{-1},y_i^{-1}])\equiv 1+(X_i\omega_i-\omega_iX_i) \bmod D$$

and so $X_i\omega_i-\omega_iX_i\in D$ for $1\leqslant i\leqslant n$. Then, by looking at the coefficients of X_{iJ}, $|J|\leqslant r-1$, in the sum $\sum_{j=1}^n(X_j\omega_j-\omega_jX_j)\in D$, we obtain

$$\mu_m(Ji)\equiv\mu_m(iJ) \bmod \Delta(iJ)$$

which implies the cyclic symmetries.

2) It follows from a general theorem on the Magnus coefficients in [CFL58, Theorem 3.9]. □

A group-theoretic and arithmetic meaning of the refined Milnor invariants is given as follows (cf. [Mor02a, Theorem 3.1.7]).

Theorem 1.2.6. *Let r be an integer with $2\leqslant r\leqslant l^{e_S}$. We assume that $\mu_m(I)=0$ for $|I|\leqslant r-1$. Then the homomorphism $\pi:F\to G_S(l)$ in (1.1.1) induces the isomorphisms for $q\leqslant r$,*

$$F/F_{q,m}\simeq G_S(l)/G_S(l)_{q,m}.$$

https://doi.org/10.1112/S0010437X03000137 Published online by Cambridge University Press

Assume further that $\Delta(J) = 0$ for $|J| \leqslant r$. Then we have

$$\overline{\mu_m}(Ij) = 0 \text{ for } |I| \leqslant r-1 \Leftrightarrow p_j \text{is completely decomposed in } \mathbb{Q}(r,m)/\mathbb{Q},$$

where $\mathbb{Q}(q,m)$ is the field corresponding to the qth term $G_S(l)_{q,m}$ of the Zassenhaus filtration of $G_S(l)$ over $\mathbb{Z}/m\mathbb{Z}$ for $q \geqslant 1$.

Proof. Note that, for $f \in F$, $f \in F_{q,m}$ if and only if $\epsilon_I(f)_m = 0$ for $|I| < q$, $q \geqslant 2$. So, by our assumption, $y_i \in F_{r-1,m}$ and $[x_i^{-1}, y_i^{-1}] \in F_{r,m}$. In addition, $x_i^{p_i - 1} \in F_{r,m}$. Hence, π induces the isomorphisms $F/F_{q,m} \simeq G_S(l)/G_S(l)_{q,m}$ for $q \leqslant r$. Since $\Delta(J) = 0$ for $|J| \leqslant r$, we have $\overline{\mu_m}(Ij) = \mu_m(Ij) = \epsilon_I(y_i)_m$ for $|I| \leqslant r-1$. Hence we have

$$\begin{aligned} \overline{\mu_m}(Ij) = 0 \text{ for } |I| \leqslant r-1 &\Longleftrightarrow y_j \in F_{r,m} \\ &\Longleftrightarrow \sigma_j \in G_S(l)_{r,m} \\ &\Longleftrightarrow p_j \text{ is completely decomposed in } \mathbb{Q}(r,m)/\mathbb{Q}. \end{aligned} \qquad \square$$

Let $N_k(R)$ denote the group of $k \times k$ upper triangular unipotent matrices over a ring R. For a multi-index $I = (i_1 \cdots i_r)$, $2 \leqslant r < l^{e_S}$ such that $\Delta(I) \neq \mathbb{Z}/m\mathbb{Z}$, we define the map

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

by

$$\rho_I(f) = \begin{bmatrix} 1 & \epsilon\left(\dfrac{\partial f}{\partial x_{i_1}}\right)_m & \epsilon\left(\dfrac{\partial^2 f}{\partial x_{i_1}\partial x_{i_2}}\right)_m & \cdots & \epsilon\left(\dfrac{\partial^{r-1} f}{\partial x_{i_1}\cdots\partial x_{i_{r-1}}}\right)_m \\ & 1 & \epsilon\left(\dfrac{\partial f}{\partial x_{i_2}}\right)_m & \cdots & \epsilon\left(\dfrac{\partial^{r-2} f}{\partial x_{i_2}\cdots\partial x_{i_{r-1}}}\right)_m \\ & & \ddots & \ddots & \vdots \\ & 0 & & \ddots & \epsilon\left(\dfrac{\partial f}{\partial x_{i_{r-1}}}\right)_m \\ & & & & 1 \end{bmatrix} \bmod \Delta(I),$$

where we set $\epsilon(\alpha)_m = \epsilon_{\mathbb{Z}_l[[F]]}(\alpha) \bmod m$ for simplicity. The formula of Fox's free derivative [Fox53, equation 3.2] tells us that ρ_I gives a continuous homomorphism. We denote simply by $N(q)$ the qth term of the Zassenhaus filtration of $N_r((\mathbb{Z}/m\mathbb{Z})/\Delta(I))$ over $(\mathbb{Z}/m\mathbb{Z})/\Delta(I)$. The following theorem may be regarded as an analog of Murasugi's theorem [Mur85] which asserts that the Milnor invariants of a link are covering linkage invariants in certain nilpotent coverings.

Theorem 1.2.7.

1) *With the notation as above, the nilpotent representation ρ_I factors through the Galois group $G_S(l)$, which is also denoted by ρ_I,*

$$\rho_I : G_S(l) \longrightarrow N_r((\mathbb{Z}/m\mathbb{Z})/\Delta(I)).$$

If the indices $i_1, \ldots, i_{r-1}$ are distinct from each other, then ρ_I is surjective.

2) *Assume that $i_1, \ldots, i_{r-1}$ are distinct. Let K_q denote the subfield of $\mathbb{Q}_S(l)/\mathbb{Q}$ corresponding to the subgroup $\rho_I^{-1}(N(q))$ of $G_S(l)$. Then we have the following.*

   (a) *The field K_r is a finite Galois extension over $\mathbb{Q}$ unramified outside $p_{i_1}, \ldots, p_{i_{r-1}}$ with Galois group $\mathrm{Gal}(K_r/\mathbb{Q}) \simeq N_r((\mathbb{Z}/m\mathbb{Z})/\Delta(I))$.*

   (b) *The prime number p_{i_r} is completely decomposed in $K_{r-1}/\mathbb{Q}$ and the decomposition law of a prime divisor $\mathfrak{p}$ of p_{i_r} in K_{r-1} in the extension K_r/K_{r-1} is given by the refined Milnor invariant as follows. Let $\rho_{I,r-1} : \mathrm{Gal}(K_r/K_{r-1}) \xrightarrow{\sim} N(r-1)/N(r) \simeq (\mathbb{Z}/m\mathbb{Z})/\Delta(I)$ be the isomorphism induced by ρ_I and let $((K_r/K_{r-1})/\mathfrak{p}) = \sigma_{i_r}|_{K_r}$ be the Artin symbol of $\mathfrak{p}$ in*

K_r/K_{r-1}. Then, we have

$$\rho_{I,r-1}\left(\left(\frac{K_r/K_{r-1}}{\mathfrak{p}}\right)\right) = \overline{\mu_m}(I).$$

Proof. 1) By Lemma 1.2.2, we have $\rho_I(x_j^{p_j-1}[x_j^{-1}, y_j^{-1}]) \equiv 0 \bmod \Delta(I)$ and so ρ_I yields the representation of $G_S(l)$. For the second assertion, it suffices to note that the $\rho_I(x_{i_k})$'s $(1 \leqslant k \leqslant r-1)$ generate the whole $N_r((\mathbb{Z}/m\mathbb{Z})/\Delta(I))$.

2a) This follows from item 1 and $\rho_I(\tau_j) = 1_r$ for $j \neq i_1, \ldots, i_{r-1}$.

2b) Since $\mu_m(Ji_r) \equiv 0 \bmod \Delta(I)$ for any proper subsequence J of $(i_1 \cdots i_{r-1})$, $\rho_I(\sigma_{i_r}) \in N(r-1)$. This implies that p_{i_r} is completely decomposed in $K_{r-1}/\mathbb{Q}$. Furthermore, we have

$$\begin{aligned}\rho_{I,r-1}\left(\left(\frac{K_r/K_{r-1}}{\mathfrak{p}}\right)\right) &= \rho_{I,r-1}(\sigma_{i_r}|_{K_r}) \\ &= \epsilon\left(\frac{\partial^{r-1} y_{i_r}}{\partial x_{i_1} \cdots \partial x_{i_{r-1}}}\right)_m \mod \Delta(I) \\ &= \overline{\mu_m}(I).\end{aligned}$$

□

1.3 Examples

We give some examples of Milnor $\overline{\mu_m}$-invariants of low degree and their arithmetic interpretation.

Example 1.3.1 (Linking number). By definition, we have $\mu_m(12) = \mathrm{lk}_m(p_2, p_1)$. The similar computation as in Theorem 3.1.3 of [Mor02a] yields

$$\zeta_m^{\mu_m(12)} = \zeta_m^{\mathrm{lk}_m(p_2,p_1)} = \left(\frac{p_2}{p_1}\right)_m$$

where ζ_m is a suitable primitive mth root of 1 in $\mathbb{Q}_{p_1}$ and $(p_2/p_1)_m$ is the mth power residue symbol in the p_1-adic field $\mathbb{Q}_{p_1}$. Consider the case $m = 2$ and $p_1, p_2 \equiv 1 \bmod 4$ so that $\zeta_m = -1 \in \mathbb{Q}$ and $\Delta(12) = 0$. Then we see that the cyclic symmetry $\overline{\mu_2}(12) = \overline{\mu_2}(21)$ of Theorem 1.2.5(1) is nothing but the Gauss reciprocity for the Legendre symbol:

$$\left(\frac{p_2}{p_1}\right)_2 = \left(\frac{p_1}{p_2}\right)_2.$$

For $p_1, p_2 \equiv 3 \bmod 4$, we do not have the symmetry for the linking number mod 2, i.e. $\mu_2(12) \neq \mu_2(21)$, although the symmetry of $\overline{\mu_2}(ij)$ holds trivially by $\Delta(12) = \Delta(21) = \mathbb{Z}/2\mathbb{Z}$. As an example, let $p_1 = 5, p_2 = 29$. Then we have $\mathrm{lk}_2(5, 29) = \mathrm{lk}_2(29, 5) = 0$ so that the primes 5 and 29 are not linked modulo 2, but we also see that $\mathrm{lk}_4(5, 29) = \mathrm{lk}_4(29, 5) \equiv 2 \bmod 4$. Thus 5 and 29 may look as if they are linked to each other in $\mathbb{Z}/4\mathbb{Z}$ as shown in Figure 1.

Example 1.3.2 (Triple symbol). The triple Milnor invariant $\overline{\mu_m}(123)$ in $(\mathbb{Z}/m\mathbb{Z})/\Delta(123)$ is an invariant for the Galois group $\mathrm{Gal}(K_3/\mathbb{Q})$ where K_q are the Galois extensions over $\mathbb{Q}$ unramified outside p_1, p_2 defined in Theorem 1.2.7. Assume that $\mathrm{lk}_m(p_i, p_j) = \mu_m(ji) = 0$ for $1 \leqslant i \neq j \leqslant 3$ and that $p_i \equiv 1 \bmod l^2$ $(1 \leqslant i \leqslant 3)$ for $l = 2, 3$ so that we have $\Delta(123) = 0$. Moreover, we have $\mathrm{Gal}(K_3/\mathbb{Q}) = N_3(\mathbb{Z}/m\mathbb{Z})$ and K_2 is the bicyclic field k_1k_2 where k_i is the cyclic extension over $\mathbb{Q}$ of degree m unramified outside p_i, $i = 1, 2$. Since the inertia group over p_i generated by $\rho_{(123)}(\tau_i)$ has order m for $i = 1, 2$, K_3 is an unramified extension over K_2. By Theorem 1.2.7(2), for a prime divisor $\mathfrak{p}$ of p_3 in K_2, we have

$$\mathrm{Gal}(K_3/K_2) \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z}; \quad \left(\frac{K_3/K_2}{\mathfrak{p}}\right) \mapsto \mu_m(123).$$

Thus, as we showed in § 3.2 of [Mor02a], our Milnor invariant $\mu_m(123)$ gives a natural interpretation of the Rédei triple symbol $[p_1, p_2, p_3]$, which is defined in the case $m = 2$ such that $K_2 = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$

https://doi.org/10.1112/S0010437X03000137 Published online by Cambridge University Press

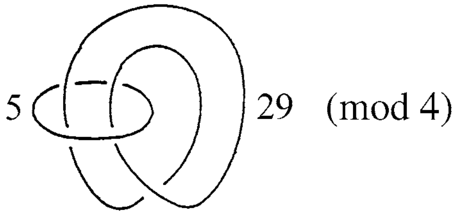

Figure 1.

and K_3 is the Galois extension of $\mathbb{Q}$ with dihedral Galois group $N_3(\mathbf{F}_2)$ of degree eight ([Réd38], see also [Fur80]). The cyclic symmetry and shuffle relation of Theorem 1.2.5 and Theorem 3.2.5 of [Mor02a] yield the following corollary immediately.

Corollary 1.3.3 [Réd38, Satz 2 and Satz 4]. *The Rédei triple symbol* $[p_1, p_2, p_3]$ *is invariant under any permutation of* p_1, p_2, p_3.

2. The Massey products in Galois cohomology and their connection with the Milnor invariants

In this section, following [Dwy75, Kra66, May69], we introduce the Massey products and recall some basic properties in the context of the profinite group cohomology, and then establish our main Theorem 2.3.2 giving the connection between the refined Milnor invariants in § 1 and certain Massey products in the cohomology of the Galois group $G_S(l)$.

2.1 The definition and some properties

Let G be a profinite group and let R be a commutative ring with identity on which G acts trivially. Let $C^*(G, R)$ be the complex of inhomogeneous cochains of G with coefficient in R, equipped with the coboundary operator d of degree one, and let the cohomology $H^*(G, R)$ be defined to be the homology of the complex $C^*(G, R)$. The graded module $A(G, R) = \bigoplus_{p \geqslant 0} C^p(G, R)$ has the structure of R-algebra by the cup product defined as

$$(a \cup b)(g_1, \dots, g_{p+q}) = a(g_1, \dots, g_p)b(g_{p+1}, \dots, g_{p+q})$$

for $a \in C^p(G, R), b \in C^q(G, R)$, and $g_i \in G$. Thus we have a differential graded R-algebra (DGA) $(A(G, R), d)$ satisfying

$$d(a \cup b) = da \cup b + (-1)^p a \cup db, \quad a \in C^p(G, R),\ b \in C^q(G, R).$$

Therefore, we can consider the Massey product structure on the DGA $A(G, R)$ according to the general procedure (cf. [May69]). However, we shall deal with only low (one- or two-) dimensional cohomology groups in the following discussion, and so we introduce here the Massey products only on $H^1(G, R)$. Note that our sign convention is different from that of [Kra66, May69]but the same as that of [Dwy75].

Definition 2.1.1. Let $r \geqslant 2$ and let $\alpha_1, \dots, \alpha_r \in H^1(G, R)$. The *rth Massey product* of $\alpha_1, \dots, \alpha_r$ is said to be defined if there is an array

$$A = \{a_{ij} \in C^1(G, R) \mid 1 \leqslant i < j \leqslant r + 1, (i, j) \neq (1, r + 1)\}$$

such that:

1) $a_{i,i+1}$ is a representative of α_i, $1 \leqslant i \leqslant r$;

2) $da_{ij} = \sum_{k=i+1}^{j-1} a_{ik} \cup a_{kj}$, $j \neq i+1$.

Such an array A is called a *defining system* for the product and the value of the product relative to A is defined to be the cohomology class of the 2-cocycle

3) $\sum_{k=2}^{r} a_{1k} \cup a_{k,r+1}$

and it is denoted by $\langle \alpha_1, \dots, \alpha_r \rangle_A$. The Massey product $\langle \alpha_1, \dots, \alpha_r \rangle$ is usually denoted for the subset of $H^2(G,R)$ of all $\langle \alpha_1, \dots, \alpha_r \rangle_A$ for some defining system A. The *indeterminacy* of $\langle \alpha_1, \dots, \alpha_n \rangle$ is defined to be the subset $\{a - b \mid a, b \in \langle \alpha_1, \dots, \alpha_r \rangle\}$. We also note that the defining system A is identified with the $(r+1) \times (r+1)$ upper triangular unipotent matrix, denoted also by A, over $C^1(G,R)$ with the (i,j) entry being a_{ij} for $1 \leqslant i < j \leqslant r+1$, where $(i,j) \neq (1, r+1)$ and the $(1, r+1)$ entry is zero. (See Proposition 2.1.5 below.)

We note that the basic properties of the Massey products in [Kra66] and [May69] (for singular cohomology) also hold for the profinite group cohomology, since we have isomorphisms for $G = \varprojlim G_i$, G_i being finite,

$$H^*(G,R) = \varinjlim H^*(G_i,R) = \varinjlim H^*(K(G_i,1),R)$$

where $K(G_i,1)$ is the Eilenberg–MacLane space.

We recollect some properties from [Kra66, Dwy75].

2.1.2. Let $f : G' \longrightarrow G$ be a homomorphism of profinite groups. Then if $\langle \alpha_1, \dots, \alpha_r \rangle$ is defined for $\alpha_i \in H^1(G,R)$ with defining system $A = (a_{ij})$, then so is $\langle f^*(\alpha_1), \dots, f^*(\alpha_n) \rangle$ with defining system $A^* = (f^*(a_{ij}))$, and $f^*(\langle \alpha_1, \dots, \alpha_r \rangle) \subset \langle f^*(\alpha_1), \dots, f^*(\alpha_r) \rangle$. If f is an isomorphism, the equality holds.

2.1.3. (cf. [Kra66, Lemma 20]). Assume that for any $\beta_1, \dots, \beta_s$, $s < r$, $\langle \beta_1, \dots, \beta_s \rangle$ is defined and $\langle \beta_1, \dots, \beta_s \rangle = 0$. Then the rth Massey product $\langle \alpha_1, \dots, \alpha_r \rangle$ is defined for $\alpha_i \in H^1(G,R)$ and $\langle \alpha_1, \dots, \alpha_r \rangle$ has no indeterminacy, i.e. it consists of a single element. For the case $r = 2$, the product is given by the cup product $\langle \alpha_1, \alpha_2 \rangle = \alpha_1 \cup \alpha_2$, and has no indeterminacy.

2.1.4. ([Kra66, Theorem 8]). Assume $\langle \alpha_1, \dots, \alpha_r \rangle$ is defined. Then $\langle \alpha_r, \dots, \alpha_1 \rangle$ is defined and $\langle \alpha_1, \dots, \alpha_r \rangle = (-1)^{r-1} \langle \alpha_r, \dots, \alpha_1 \rangle$.

A group-theoretic meaning of the Massey product is given as an obstruction for the lifting of a nilpotent representation. Let $N_k(R)$ be the group of $k \times k$ upper triangular unipotent matrices over R and $Z_k(R)$ the center of $N_k(R)$ as in Subsection 1.2, and set $\overline{N}_k(R) = N_k(R)/Z_k(R)$ so that for $A = (a_{ij})$ and $A' = (a'_{ij})$ in $N_k(R)$, $A \equiv A' \bmod Z_k(R)$ if and only if $a_{ij} = a'_{ij}$ for $(i,j) \neq (1,k)$. Suppose $A = (a_{ij})$ is a defining system for the Massey product $\langle \alpha_1, \dots, \alpha_r \rangle$, $\alpha_i \in H^1(G,R)$. Condition 2 of Definition 2.1.1 means that $\phi_A := (-a_{ij}) \bmod Z_{r+1}(R)$ defines a homomorphism $\phi_A : G \longrightarrow \overline{N}_{r+1}(R)$. Then we have the following.

Proposition 2.1.5. (cf. [Dwy75, Theorem 2.4]). *Let $\alpha_1, \dots, \alpha_r \in H^1(G,R)$. Then the correspondence $A \mapsto \phi_A$ gives a bijection between the set of defining systems A for the Massey product $\langle \alpha_1, \dots, \alpha_r \rangle$ and continuous group homomorphism $\phi = (\phi_{ij}) : G \longrightarrow \overline{N}_{r+1}(R)$ with $\phi_{i,i+1} = \alpha_i$ $(1 \leqslant i \leqslant r)$. Moreover, the value $\langle \alpha_1, \dots, \alpha_r \rangle_A = 0$ if and only if ϕ_A lifts to a homomorphism $G \longrightarrow N_{r+1}(R)$.*

https://doi.org/10.1112/S0010437X03000137 Published online by Cambridge University Press

Proof. The bijection follows from conditions 1 and 2 of Definition 2.1.1. To see the latter assertion, it suffices to note that $\langle \alpha_1, \ldots, \alpha_r \rangle_A$ corresponds to the group extension

$$1 \longrightarrow R = Z_{r+1}(R) \longrightarrow E \xrightarrow{\mathrm{pr}} G \longrightarrow 1$$

where $E = \{(g, u) \in G \times N_{r+1}(R) \mid \phi_A(g) = u \bmod Z_{r+1}(R)\}$. □

2.2 Stein's formula and the transgression

Let G be a finitely generated pro-l group with a minimal presentation

$$1 \longrightarrow N \longrightarrow F \xrightarrow{\pi} G \longrightarrow 1$$

where F is a free pro-l group on $x_1, \ldots, x_n$ and we set $\tau_i = \pi(x_i)$. Let l^{e_G} be the exponent of $G/G^{(2)}$ and we fix $m = l^e$ with $1 \leqslant e \leqslant e_G$ so that $H^1(F, \mathbb{Z}/m\mathbb{Z}) = H^1(G, \mathbb{Z}/m\mathbb{Z}) \simeq (\mathbb{Z}/m\mathbb{Z})^n$. In this subsection, we give a general formula bridging the Magnus coefficients of $f \in N$ (cf. Subsection 1.2) and the Massey products $\langle \alpha_1, \ldots, \alpha_r \rangle$, $\alpha_i \in H^1(G, \mathbb{Z}/m\mathbb{Z})$ via the transgression. Our formula is based on the following (pro-l version of) Stein's formula [Ste90].

Proposition 2.2.1. *Let $\psi = (\psi_{ij}) : F \longrightarrow N_{r+1}(\mathbb{Z}/m\mathbb{Z})$ be a continuous homomorphism. Then we have, for $1 \leqslant i < j \leqslant r+1$ and $f \in F$,*

$$\psi_{ij}(f) = \sum_{k=1}^{j-i} \sum_{c_1+\cdots+c_k=j-i} \sum_{I=(i_1\cdots i_k)} \psi_{i,i+c_1}(x_{i_1})\psi_{i+c_1,i+c_1+c_2}(x_{i_2})\cdots\psi_{j-c_k,j}(x_{i_k})\epsilon_I(f)_m$$

where $c_1, \ldots, c_k$ run over positive integers satisfying $c_1 + \cdots + c_k = j - i$ and $I = (i_1 \cdots i_k)$ over multi-indices $1 \leqslant i_1, \ldots, i_k \leqslant n$.

Proof. Consider the map $\psi' : F \to N_{r+1}(\mathbb{Z}/m\mathbb{Z})$ whose (i, j)-component is given by the right-hand side of the above formula. Then, as in the proof of Lemma 1.5 of [Ste90], we can see that ψ' gives a homomorphism. Since $\psi(x_i) = \psi'(x_i)$ for $1 \leqslant i \leqslant n$, we have $\psi = \psi'$. □

Recall that the *transgression* $tg : H^1(N, \mathbb{Z}/m\mathbb{Z})^G \to H^2(G, \mathbb{Z}/m\mathbb{Z})$ is defined as follows. For $a \in H^1(N, \mathbb{Z}/m\mathbb{Z})^G$, choose a 1-cochain $b : F \to \mathbb{Z}/m\mathbb{Z}$ such that $b|_N = a$. The value $db(f_1, f_2)$, $f_i \in F$, depends only on the cosets $f_1 \bmod N$ and $f_2 \bmod N$, and so there is a 2-cocycle $c \in C^2(G, \mathbb{Z}/m\mathbb{Z})$ such that $\pi^*(c) = db$. Then we set $tg(a) = c$. By the Hochschild–Serre sequence, tg is an isomorphism, and we let $tg^\vee : H_2(G, \mathbb{Z}/m\mathbb{Z}) \to H_1(N, \mathbb{Z}/m\mathbb{Z})_G$ be the dual of tg (Hopf's isomorphism).

Theorem 2.2.2. *With the notation as above, let $\alpha_1, \ldots, \alpha_r \in H^1(G, \mathbb{Z}/m\mathbb{Z})$ and let $A = (a_{ij})$ be a defining system for the Massey product $\langle \alpha_1, \ldots, \alpha_r \rangle$. Let $f \in N$ and set $\eta = (tg^\vee)^{-1}(f \bmod N^m[F, N])$. Then we have*

$$\langle \alpha_1, \ldots, \alpha_r \rangle_A(\eta) = \sum_{k=1}^{r} (-1)^{k+1} \sum_{c_1+\cdots+c_k=r} \sum_{I=(i_1\cdots i_k)} a_{1,1+c_1}(\tau_{i_1})\cdots a_{r+1-c_k,r+1}(\tau_{i_k})\epsilon_I(f)_m$$

where $c_1, \ldots, c_k$ run over positive integers satisfying $c_1 + \cdots + c_k = r$ and $I = (i_1 \cdots i_k)$ over multi-indices $1 \leqslant i_1, \ldots, i_k \leqslant n$.

Proof. Let $\phi_A : G \longrightarrow \overline{N}_{r+1}(\mathbb{Z}/m\mathbb{Z})$ be the homomorphism corresponding to A by Proposition 2.1.5. For $a \in C^*(G, \mathbb{Z}/m\mathbb{Z})$, we simply write a^* for $\pi^*(a)$ in the following. By (2.1.2), $A^* = (a^*_{ij})$ is a defining system for $\langle \alpha^*_1, \ldots, \alpha^*_r \rangle$ and $\pi^*(\langle \alpha_1, \ldots, \alpha_r \rangle_A) = \langle \alpha^*_1, \ldots, \alpha^*_r \rangle_{A^*} = \left[\sum_{k=2}^{r} a^*_{1k} \cup a^*_{k,r+1}\right]$. Since $H^2(F, \mathbb{Z}/m\mathbb{Z}) = 0$, there is a $b \in C^1(F, \mathbb{Z}/m\mathbb{Z})$ such that $db = \sum_{k=2}^{r} a^*_{1k} \cup a^*_{k,r+1}$. Hence we have $tg(b|_N) = \langle \alpha_1, \ldots, \alpha_r \rangle_A$, and the homomorphism $\phi_{A^*} = \phi_A \circ \pi$ corresponding to A^* lifts to the

https://doi.org/10.1112/S0010437X03000137 Published online by Cambridge University Press

homomorphism $\widetilde{\phi_{A^*}} : F \longrightarrow N_{r+1}(\mathbb{Z}/m\mathbb{Z})$ given by

$$\widetilde{\phi_{A^*}} = \begin{pmatrix} 1 & -a^*_{12} & -a^*_{13} & \dots & -a^*_{1r} & -b \\ 0 & 1 & -a^*_{23} & \dots & -a^*_{2r} & -a^*_{2,r+1} \\ \vdots & \ddots & \ddots & \dots & \vdots & \vdots \\ \vdots & & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & \dots & 0 & 1 & -a^*_{r,r+1} \\ 0 & \dots & \dots & 0 & 0 & 1 \end{pmatrix}.$$

Therefore, we have

$$\begin{aligned} \langle \alpha_1, \dots, \alpha_r \rangle_A(\eta) &= tg(b|_N)((tg^\vee)^{-1}(f \bmod N^m[F,N])) \\ &= b(f) \\ &= \sum_{k=1}^{r} (-1)^{k+1} \sum_{c_1+\cdots+c_k=r} \sum_{I=(i_1\cdots i_k)} a^*_{1,1+c_1}(x_{i_1}) \cdots a^*_{r+1-c_k,r+1}(x_{i_k}) \epsilon_I(f)_m \\ &= \sum_{k=1}^{r} (-1)^{k+1} \sum_{c_1+\cdots+c_k=r} \sum_{I=(i_1\cdots i_k)} a_{1,1+c_1}(\tau_{i_1}) \cdots a_{r+1-c_k,r+1}(\tau_{i_k}) \epsilon_I(f)_m \end{aligned}$$

where the third equality follows from Proposition 2.2.1. □

Corollary 2.2.3. *With the notation as above, assume $f \in F_{r,m} \cap N$. Then we have*

$$\langle \alpha_1, \dots, \alpha_r \rangle_A(\eta) = (-1)^{r+1} \sum_{I=(i_1\cdots i_r)} \alpha_1(\tau_{i_1}) \cdots \alpha_r(\tau_{i_r}) \epsilon_I(f)_m.$$

Proof. This follows from the fact that $\epsilon_I(f)_m = 0$ for $|I| < r$. □

2.3 The normalized Massey products and the Milnor $\overline{\mu_m}$-invariants

We first introduce the notion of a normalized Massey system following Turaev [Tur79]. We keep the same notation as in § 2.2. For an ideal $\mathfrak{a} \subset \mathfrak{a}'$, we denote by $\varphi^{\mathfrak{a}}_{\mathfrak{a}'}$ the homomorphism $C^*(G, (\mathbb{Z}/m\mathbb{Z})/\mathfrak{a}) \to C^*(G, (\mathbb{Z}/m\mathbb{Z})/\mathfrak{a}')$ induced by the natural map $(\mathbb{Z}/m\mathbb{Z})/\mathfrak{a} \to (\mathbb{Z}/m\mathbb{Z})/\mathfrak{a}'$.

Definition 2.3.1. A *normalized Massey system* $(\mathfrak{a}, a)$ for $(G; \tau_1, \dots, \tau_n)$ over $\mathbb{Z}/m\mathbb{Z}$ is a system of ideals $\mathfrak{a}(J)$ of $\mathbb{Z}/m\mathbb{Z}$ and 1-cochains $a(J) \in C^1(G, (\mathbb{Z}/m\mathbb{Z})/\mathfrak{a}(J))$, where J ranges over multi-indices of $|I| \geqslant 1$, which satisfies the following conditions:

1) $\mathfrak{a}(J)$ is the smallest ideal containing the ideal of $\mathbb{Z}/m\mathbb{Z}$ generated by $\binom{l^{e_G}}{t}$, $1 \leqslant t \leqslant |J|$, and all $\mathfrak{a}(J')$, J' running over all proper subsequences of J, and such that for $J = (j_1 \cdots j_s)$,
$$\sum_{k=2}^{s} \varphi^{\mathfrak{a}(j_1\cdots j_{k-1})}_{\mathfrak{a}(J)}(a(j_1 \cdots j_{k-1})) \cup \varphi^{\mathfrak{a}(j_k\cdots j_s)}_{\mathfrak{a}(J)}(a(j_k \cdots j_s))$$
is null-cohomologous (in particular, $\mathfrak{a}(1) = \cdots = \mathfrak{a}(n) = 0$);
2) this sum equals $da(I)$ in $C^2(G, (\mathbb{Z}/m\mathbb{Z})/\mathfrak{a}(I))$ (in particular, $da(i) = 0$); and
3) $a(j)(\tau_j) = 1$ for $1 \leqslant j \leqslant n$ and $a(J)(\tau_i) = 0$ for other cases.

It is easy to see by induction on $|J|$ that a normalized Massey system exists. For a multi-index $I = (i_1 \cdots i_r)$ with $r \geqslant 2$, we denote by $m(\mathfrak{a})(I)$ the ideal of $\mathbb{Z}/m\mathbb{Z}$ generated by $\binom{l^{e_G}}{t}$, $1 \leqslant t \leqslant |I|$, and all $\mathfrak{a}(I')$, I' taken over all proper subsequences of I, and by $m(a)(I)$ the cohomology class of the 2-cocycle

$$\sum_{k=2}^{r} \varphi_{m(\mathfrak{a})(I)}^{\mathfrak{a}(i_1\cdots i_{k-1})}(a(i_1\cdots i_{k-1})) \cup \varphi_{m(\mathfrak{a})(I)}^{\mathfrak{a}(i_k\cdots i_r)}(a(i_k\cdots i_r)) \quad (I = (i_1 \cdots i_r)).$$

The collection $(m(\mathfrak{a}), m(a))$ is called the *product* of a normalized Massey system $(\mathfrak{a}, a)$.

Let us go back to our arithmetic situation with G being the Galois group $G_S(l)$, $e_G = e_S$. We use the same notation as in § 1 which is consistent with that in Subsection 2.2. In order to obtain an analog of Turaev's formula for a link [Tur79], the normalized Massey product must be evaluated on a suitable second homology class η_i representing an analog of the 'boundary of tubular neighborhood' for a prime p_i. In view of the analogy (1.1.3), we define this class η_i as follows. First note that the local Galois group $G_i := \mathrm{Gal}(\mathbb{Q}_{p_i}(l)/\mathbb{Q}_{p_i})$ has the presentation $G_i = F_i/N_i$ where F_i is the free pro-l group generated by x_i, y_i and N_i is the closed subgroup generated normally by $r_i := x_i^{p_i-1}[x_i^{-1}, y_i^{-1}]$. Let $tg^{\vee} : H_2(G_i, \mathbb{Z}/m\mathbb{Z}) \xrightarrow{\sim} H_1(N_i, \mathbb{Z}/m\mathbb{Z})_{G_i} = N_i/N_i^m[N_i, F_i] \simeq \mathbb{Z}/m\mathbb{Z}$ be the dual of the transgression (Hopf's isomorphism) as before. Noting that $H_2(\mathrm{Spec}(\mathbb{Q}_{p_i}), \mathbb{Z}/m\mathbb{Z}) = H_2(G_i, \mathbb{Z}/m\mathbb{Z})$, we define the class η_i to be the image of the canonical generator $(tg^{\vee})^{-1}(r_i)$ of $H_2(G_i, \mathbb{Z}/m\mathbb{Z})$ under the map $H_2(G_i, \mathbb{Z}/m\mathbb{Z}) \to H_2(G_S(l), \mathbb{Z}/m\mathbb{Z})$. Of course, η_i is defined with coefficient $(\mathbb{Z}/m\mathbb{Z})/\mathfrak{b}$ for any ideal $\mathfrak{b}$ of $\mathbb{Z}/m\mathbb{Z}$.

Then our main result, which gives the connection between the normalized Massey products and the Milnor $\overline{\mu_m}$-invariants, is stated as follows.

Theorem 2.3.2. *Let $(\mathfrak{a}, a)$ be a normalized Massey system for $(G_S(l); \tau_1, \ldots, \tau_n)$. Let $I = (i_1 \cdots i_r)$ be a multi-index with $2 \leqslant r \leqslant l^{e_S}$ and let η_i be the class $(tg^{\vee})^{-1}(r_i)$ defined with coefficient $(\mathbb{Z}/m\mathbb{Z})/m(\mathfrak{a})(I)$. Then we have*

1) *$m(\mathfrak{a})(I) = \Delta(I)$; and*
2) *$m(a)(I)(\eta_{i_r}) = -m(a)(I)(\eta_{i_1}) \equiv (-1)^r \overline{\mu_m}(I) \bmod \Delta(I)$.*

Proof. Note that $\{a(1), \ldots, a(n)\}$ forms the $\mathbb{Z}/m\mathbb{Z}$-basis of $H^1(G_S(l), \mathbb{Z}/m\mathbb{Z})$, Kronecker dual to the monodromies $\{\tau_1, \ldots, \tau_n\}$. Let $J = (j_1, \ldots, j_s)$ be any subsequence of I $(1 \leqslant s \leqslant r)$. For $1 \leqslant p < q \leqslant r+1$, $(p, q) \neq (1, r+1)$, we set $a_{pq} = \varphi_{m(\mathfrak{a})(I)}^{\mathfrak{a}(i_p\cdots i_{q-1})}(a(i_p \cdots i_{q-1}))$. By conditions 1–3 of Definition 2.3.1, we see that $A = (a_{pq})$ forms a defining system of the product of $a(1), \ldots, a(n)$ over $(\mathbb{Z}/m\mathbb{Z})/m(\mathfrak{a})(J)$ and its value relative to A is given by $m(\mathfrak{a})(J)$ (concretely, a_{pq}'s are given by ρ_I in § 1.2 mod $m(\mathfrak{a})(J)$). By Theorem 2.2.2, we have

$$m(a)(J)(\eta_j) = (-1)^{r+1} \epsilon_J(x_j^{p_j-1}[x_j^{-1}, y_j^{-1}])_m \bmod m(\mathfrak{a})(J)$$

where η_j is the class $(tg^{\vee})^{-1}(r_j)$ with coefficient $(\mathbb{Z}/m\mathbb{Z})/m(\mathfrak{a})(I)$.

By Lemma 1.2.2, we have

$$\epsilon_J(x_j^{p_j-1}[x_j^{-1}, y_j^{-1}]) \equiv \begin{cases} \mu_m(j_2 \cdots j_s j_1), & j = j_1, \\ -\mu_m(j_1 \cdots j_{s-1} j_s), & j = j_s, \\ 0, & \text{otherwise.} \end{cases} \quad \bmod \Delta(J)$$

Hence, by the cycle relation 1 of Theorem 1.2.5, we have

$$m(a)(J)(\eta_{j_s}) = -m(a)(J)(\eta_{i_1}) = (-1)^s \mu_m(J) \bmod m(\mathfrak{a})(J) + \Delta(J). \qquad (2.3.3)$$

https://doi.org/10.1112/S0010437X03000137 Published online by Cambridge University Press

On the other hand, note that $\varphi_{\mathfrak{a}(J)}^{m(\mathfrak{a})(J)}(m(a)(J))$ is the cohomology class of the cocycle

$$\sum_{k=2}^{r} \varphi_{\mathfrak{a}(J)}^{\mathfrak{a}(j_1\cdots j_{k-1})}(a(j_1\cdots j_{k-1})) \cup \varphi_{\mathfrak{a}(J)}^{\mathfrak{a}(j_k\cdots j_s)}(a(j_k\cdots j_s)).$$

By the definition of $\mathfrak{a}(J)$ and using equation (2.3.3), we see by induction on $|J|$ that $\mathfrak{a}(J')$ is the ideal generated by $\Delta(J')$ and $\mu_m(J')$ for any proper subsequence J' of J, and hence $m(\mathfrak{a})(J) = \Delta(J)$. Taking J to be I in (2.3.3), we obtain the desired assertion. □

Theorem 2.3.2 is seen as a generalization of the well-known relation between the power residue symbol and the cup product [Koc70, Ser68] to the higher order operations.

Example 2.3.4.

1) (Linking number) The following is the well-known relation between the cup product and the linking number or power residue symbol:

$$(a(1) \cup a(2))(\eta_2) \equiv \mathrm{lk}_m(p_1, p_2) \bmod \Delta(12).$$

2) (Triple symbol) Assume that $\mathrm{lk}_m(p_i, p_j) = \mu_m(ji) = 0$ for $1 \leqslant i \neq j \leqslant 3$ and that $p_i \equiv 1 \bmod l^2$ $(1 \leqslant i \leqslant 3)$ for $l = 2, 3$ so that we have $\Delta(123) = 0$. Then we have

$$(a(12) \cup a(3) + a(1) \cup a(23))(\eta_1) \equiv \overline{\mu_2}(123) \bmod m.$$

This gives a cohomological interpretation of the Rédei triple symbol for the case $m = 2$.

Remark 2.3.5. In this paper, we have introduced the Massey products in terms of Galois cohomology which is group-theoretic and elementary. More geometrically, it may be natural to use the étale cohomology of $\mathrm{Spec}(\mathbb{Z}) \setminus S$. To define the Massey products on the étale cohomology, we can use the Čech cohomology construction, due to Verdier, via hypercoverings [AGV72].[2] Suppose in general that X is a scheme and let $\mathcal{R}$ be an étale sheaf of ring on X. Let $U_\bullet$ be the hypercovering of the étale site on X, and let $\mathcal{R}(U_\bullet)$ be the associated cochain complex. We then have the Alexander–Whitney product

$$\mathcal{R}(U_m) \times \mathcal{R}(U_m) \longrightarrow \mathcal{R}(U_{m+n})$$

on the cochains which equips $\mathcal{R}(U_\bullet) = \bigoplus_{n\geqslant 0} \mathcal{R}(U_n)$ the structure of a DGA. Thus, according to the general procedure (cf. Subsection 2.1), we can introduce the Massey products on $H^*(\mathcal{R}(U_\bullet))$. Since we have

$$H^*(X_{\text{ét}}, \mathcal{R}) \simeq \varinjlim H^*(\mathcal{R}(U_\bullet))$$

where the colimit is over the opposite category of the homotopy category of the hypercoverings $U_\bullet$ of X ([AGV72], see also [AM69, Fri82]), we obtain the Massey product structure on $H^*(X_{\text{ét}}, \mathcal{R})$. For our case where $X = \mathrm{Spec}(\mathbb{Z}) \setminus S$, $\mathcal{R} = \mathbb{Z}/m\mathbb{Z}$, we can use the Čech nerves for hypercoverings. Furthermore, the class η of a 'boundary of the tubular neighborhood' of a prime p is defined by the image of the canonical generator of $H_2(\mathrm{Spec}(\mathbb{Q}_p), \mathbb{Z}/m\mathbb{Z})$ (cf. § 2.2) under the natural map $H_2(\mathrm{Spec}(\mathbb{Q}_p), \mathbb{Z}/m\mathbb{Z}) \to H_2(\mathrm{Spec}(\mathbb{Z}) \setminus S, \mathbb{Z}/m\mathbb{Z})$.

Acknowledgements

I would like to thank M. Kapranov for enlightening communication on this topic. I thank T. Kohno for asking about the interpretation of my Milnor invariants in terms of Massey products. Finally, I am very grateful to J. Hillman for sending me his manuscript on algebraic invariants of links [Hil02] and for helpful communications.

[2] This construction was explained to the author by M. Kapranov.

https://doi.org/10.1112/S0010437X03000137 Published online by Cambridge University Press

References

AGV72 M. Artin, A. Grothendieck and J.-L. Verdier, *Théorie des topos et cohomologie etale des schémas*, Lecture Notes in Mathematics, vol. 270 (Springer, Berlin, 1972).

AM69 M. Artin and B. Mazur, *Etale homotopy*, Lecture Notes in Mathematics, vol. 100 (Springer, 1969).

CFL58 K. T. Chen, R. H. Fox and R. C. Lyndon, *Free differencial calculus, IV. The quotient groups of the lower central series*, Ann. Math. **68** (1958), 81–95.

Dwy75 W. G. Dwyer, *Homology, Massey products and maps between groups*, J. Pure Appl. Algebra **6** (1975), 245–275.

Fox53 R. H. Fox, *Free differential calculus. I: Derivation in the free group ring*, Ann. Math. **57** (1953), 547–560.

Fri82 E. M. Friedlander, *Etale homotopy of simplicial schemes*, Annals of Mathematical Studies, vol. 104 (Princeton University Press, 1982).

Fur80 Y. Furuta, *A prime decomposition symbol for a nonabelian central extension which is abelian over a bicyclic biquadratic field*, Nagoya Math. J. **79** (1980), 79–109.

Hil02 J. A. Hillman, *Algebraic invariants of links*, Series on Knots and Everything, vol. 32 (World Scientific, 2002).

Iha86 Y. Ihara, *On Galois representations arising from towers of coverings of* $\mathbf{P}^1 \setminus \{0, 1, \infty\}$, Invent. Math. **86** (1986), 427–459.

Kap96 M. Kapranov, *Analogies between number fields and 3-manifolds*, unpublished note (1996).

Koc70 H. Koch, *Galoissche theorie der p-Erweiterungen* (Springer, Berlin; VEB Deutscher Verlag der Wissenschaften, Berlin, 1970).

Kra66 D. Kraines, *Massey higher products*, Trans. Amer. Math. Soc. **124** (1966), 431-449.

Mas58 W. S. Massey, *Some higher order cohomology operations*, in *Symposium de topologia algebraica*, Mexico City, 1958, 145–154; *Higher order linking numbers*, J. Knot Theory and Its Ramifications **7** (1998), 393–414.

May69 J. P. May, *Matric Massey products*, J. Algebra **12** (1969), 533–568.

Maz65 B. Mazur, unpublished mimeographed note (circa 1965).

Mil57 J. Milnor, *Isotopy of links*, in *Algebraic Geometry and Topology, a symposium in honour of S. Lefschetz*, ed. R. H. Fox, D. S. Spencer and W. Tucker (Princeton University Press, Princeton, 1957), 280–306.

Mor00 M. Morishita, *Milnor's link invariants attached to certain Galois groups over* $\mathbf{Q}$, Proc. Japan. Academy **76** (2000), 18–21.

Mor01a M. Morishita, *Knots and primes, 3-manifolds and number fields* in *Algebraic number theory and related topics* (Japanese), Kyoto, December 2000, RIMS Report 1200 (2001), 103–115.

Mor01b M. Morishita, *Knots and primes, 3-manifolds and number fields*, in *A conference report 'Art of low dimensional topology VII'*, Kansai Seminar House, February 2001, 99–109.

Mor01c M. Morishita, *A theory of genera for cyclic coverings of links*, Proc. Japan. Academy **77** (2001), 115–118.

Mor02a M. Morishita, *On certain analogies between knots and primes*, J. Reine Angew. Math. **550** (2002), 141–167.

Mor02b M. Morishita, *Analogies between knots and primes, 3-manifolds and number fields* (2002), submitted.

Mor03 M. Morishita, *On capitulation problem for 3-manifolds*, in *Proc. 'Galois Theory and Modular Forms'*, ed. K. Hashimoto, K. Miyake and H. Nakamura, Developments in Mathematics (Kluwer Academic, Dordrecht, 2003), 305–313.

Mur85 K. Murasugi, *Nilpotent coverings of links and Milnor's invariant*, in *Low-dimensional topology*, London Mathematical Society Lecture Note Series, vol. 95 (Cambridge University Press, Cambridge, 1985), 106–142.

Por80 R. Porter, *Milnor's* $\overline{\mu}$*-invariants and Massey products*, Trans. Amer. Math. Soc. **275** (1980), 39–71.

https://doi.org/10.1112/S0010437X03000137 Published online by Cambridge University Press

Réd38 L. Rédei, *Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper, I*, J. Reine Angew. Math. **180** (1938), 1–43.

Rez00 A. Reznikov, *Embedded incompressible surfaces and homology of ramified coverings of three-manifolds*, Sel. Math. New Ser. **6** (2000), 1–39.

Ser68 J.-P. Serre, *Corps locaux* (Hermann, Paris, 1968).

Sik01 A. Sikora, *Analogies between group actions on 3-manifolds and number fields*, (2001), to appear.

Sta65 J. Stallings, *Homology and central series of groups*, J. Algebra **2** (1965), 170–181.

Ste90 D. Stein, *Massey products in the cohomology of groups with applications to link theory*, Trans. Amer. Math. Soc. **318** (1990), 301–325.

Tur79 V. G. Turaev, *Milnor's invariants and Massey products*, J. Soviet Math. **12** (1979), 128–137.

Wal76 J.-L. Waldspurger, *Entrelacements sur* Spec($\mathbf{Z}$), Bull. Sci. Math. **100** (1976), 113–139.

Masanori Morishita morisita@kenroku.kanazawa-u.ac.jp
Department of Mathematics, Faculty of Science, Kanazawa University, Kakuma-machi, Kanazawa, Ishikawa, 920-1192, Japan

https://doi.org/10.1112/S0010437X03000137 Published online by Cambridge University Press