Milnor Invariants and Multiple Residue Symbols

Michael Jemison

August 6, 2012

1 Introduction

We will explore the analogy between Milnor Invariants and Multiple Residue Symbols. This builds on the analogy between link groups and Galois groups with restricted ramification. We closely follow the flow of argument and a large chunk of the notation laid out in chapter 7 and chapter 8 of Morishita's 'Knots and Primes' ([Mo12]). Many proofs are omitted, even of non-trivial theorems. The aim of this expository paper is to briefly tell the story of an interesting analogy, without necessarily getting bogged down in the details.

2 Brief Summary of the Analogy between Link Groups and Galois Groups with Restricted Ramification

We have the following theorem about quotients of the link group by the lower central series.

Theorem 1 (See [Mo12] Theorem 7.1) For each $d \in \mathbb{N}$, there exists $y_i^{(d)} \in F$ such that

$$G_L/G_L^{(d)} =< x_1, ..., x_r | [x_1, y_1^{(d)}] = \cdots = [x_r, y_r^{(d)} = 1, F^{(d)} = 1 >$$
$$y_i^{(d)} = y_i^{(d+1)} \ mod \ F^{(d)}$$

where $y_i^{(d)}$ is a word representing a longitude β_i of K_i in $G_L/G_L^{(d)}$. We also have

$$\beta_j = \prod_{i \neq j} \alpha_i^{lk(K_i, K_j)} \ mod \ G_L^{(2)}$$

♣

The following theorem suggests an analogy between the theorem on links above and the following theorem on the Galois groups pro-l extension of p-adic rationals. But first we must fix some definitions. We fix a prime number l and a set $S = \{p_1, ..., p_r\} \subset \mathbb{Z}$ of primes that are all congruent to 1 mod l. Consider the extension $lim_{\to i} k_i =: \mathbb{Q}_S(l)$, where the limit is taken over all $k_i/\mathbb{Q} \subset \overline{Q}$ (fix an algebraic closure of $\mathbb{Q}$) such that the degree of the extension over $\mathbb{Q}$ is a power of l and unramified outisde of S and the infinite primes. We call $\mathbb{Q}_S(l)$ the maximal pro-l extension of $\mathbb{Q}$ unramified outside of S and the infinite primes. Set $G_S(l) = Gal(\mathbb{Q}_S(l), \mathbb{Q})$. Further, fix e_S to be the max exponent e such that all of the p_i are still congruent to 1 mode 1^e. Set $m = l^e$.

Further fix an algebraic closure of $\mathbb{Q}_{p_i}$ and analogously define $\mathbb{Q}_{p_i}(l)$, to be the maximal pro-l extension of $\mathbb{Q}_{p_i}$. It can be shown ([Mo12]), that

$$\mathbb{Q}_{p_i}(l) = \mathbb{Q}_{p_i}(\xi_{l^n}, (p_i)^{l^{-n}} | n \geq 1)$$

(where ξ_{l^n} denotes a primitive m^{th} root of unity). Consider the Galois group $G_{\mathbb{Q}_{p_i}(l)} := (Gal(\mathbb{Q}_{p_i}(l)/\mathbb{Q}_{p_i})$. Then $G_{\mathbb{Q}_{p_i}(l)}$ has generators τ_i called the monodromy and σ_i called the Frobenius automrphism defined as follows :

$$\tau_i(\xi_{l^n}) = \xi_{l^n}$$
$$\tau_i((p_i)^{l^{-n}}) = \xi_{l^n}(p_i)^{l^{-n}}$$

and

$$\sigma_i(\xi_{l^n}) = \xi_{l^n}^{p_i}$$
$$\sigma_i(p_i)^{l^{-n}} = (p_i)^{l^{-n}}$$

with relation

$$\tau_i^{p_i - 1}[\tau_i, \sigma_i] = 1$$

Choose embeddings $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}_{p_i}}$. These embeddings give rise to an embedding on pro-l extensions $\mathbb{Q}_S(l) \to \mathbb{Q}_{p_i}(l)$ and thus to a homomorphism on the Galois groups $\eta_i : Gal(\mathbb{Q}_{p_i}(l)/\mathbb{Q}_{p_i}) \to G_S(l)$. Let the images of the Frobenius and monodromy isomorphisms under η_i continue to be labeled by τ_i and σ_i. Let F denote the free group on words $x_1, ..., x_r$. Then let $\widehat{F}(l)$ be the projective limit taken over all quotients of F by subgroups of index equal to a power of l. Finally before giving the theorem, we define the m^{th} power residue symbol for $\mathbb{Q}_{p_i}$. When $\mathbb{Q}_{p_i}((a)^{1/m}/\mathbb{Q}_{p_i})$ is unramified, the m^{th} power residue is given by

$$(\frac{a}{p})_n := \frac{\sigma(a^{1/m})}{a^{1/m}}$$

where σ is the Frobenius map. We have the following theorem:

Theorem 2 The pro-l group $G_S(l)$ has the following presentation:

$$G_S(l) =< x_1, ..., x_r | x_1^{p_1-1}[x_1, y_1] = \cdots = x_r^{p_r-1}[x_r, y_r] = 1 >$$

where $y_i \in \widehat{F}(l)$ is the pro-l word representing σ_i. Define lk$(p_i, p_j) \in \mathbb{Z}_l$ and lk$_m(p_i, p_j) \in \mathbb{Z}/m\mathbb{Z}$ by

$$\sigma_j = \prod_{i \neq j} \tau_i^{lk(p_i,p_j)} \ mod \ G_S(l)^{(2)}$$

$$lk_m(p_i, p_j) := lk(p_i, p_j) \ mod \ m$$

And we have

$$\xi_m^{lk(p_i,p_j)} = (\frac{p_i}{p_j})_m$$

3 The Fox Free Differential Calculus

Consider a commutative ring R and group G. Then we have a group algebra $R[G]$ and the natural augmentation map $R[G] \to R$ which will be denoted by $\epsilon_{R[G]}$. By $\mathbb{Z} << X_1, ..., X_r >>$ we denote the formal power series in non-commuting variables $X_1, ..., X_r$ over $\mathbb{Z}$. The degree, denoted $deg(f)$, of a power series $f = \Sigma a_{i_1...i_n} X_{i_1}...X_{i_n}$ is the smallest n such that the coefficient $a_{i_1...i_n} \in \mathbb{Z}$ is non-zero.

Consider the free group F on letters $x_1, ..., x_r$. We have a homomorphism $M : F \to \mathbb{Z} << X_1, ..., X_r >>^{\times}$ defined by

$$x_i \to 1 + X_i$$

and

$$x_i^{-1} \to 1 - X_i + X_i^2 - ...$$

Theorem 3 M is injective.

We call M the magnus embedding. Given any $f \in \mathbb{Z}[F]$ we have a Magnus expansion given by $M(f) = \epsilon_{\mathbb{Z}[F]}(f) + \Sigma_{I=(i_1...i_n), 1 \leq i_1,...,i_n \leq r} \mu(I, f) X_I$, where $X_I = X_{i_1}...X_{i_n}$. The coefficients $\mu(I, f)$ are the Magnus coefficients. We have a theorem:

Theorem 4 For any $f \in \mathbb{Z}[F]$, there exists f_i uniquely for each i between 1 and r such that $f = \epsilon_{\mathbb{Z}[F]}(f) + \Sigma_{i=1}^r f_i(x_i - 1)$.

We see that f_j is the Fox free derivative of f with respect to x_j and we set $f_j = \frac{\partial f}{\partial x_j}$. The Fox free derivative satisfies the usual properties one would except from a sort of derivative. These are captured in the following theorem:

Theorem 5 The Fox free derivative $\partial/\partial x_j : \mathbb{Z}[F] \to \mathbb{Z}[F]$ satisfies the following properties:

$$(1)\frac{\partial x_i}{\partial x_j} = \delta_{ij}$$

$$(2)\frac{\partial (f+g)}{\partial x_j} = \frac{\partial f}{\partial x_j} + \frac{\partial g}{\partial x_j}$$

$$(3)\frac{\partial af}{\partial x_j} = a\frac{\partial f}{\partial x_j}, f, g \in \mathbb{Z}[F], c \in \mathbb{Z}$$

$$(4)\frac{fg}{\partial x_j} = \frac{\partial f}{\partial x_j}\epsilon_{\mathbb{Z}[F]}(g) + f\frac{\partial g}{\partial x_j} f, g \in \mathbb{Z}[F]$$

$$(5)\frac{\partial f^{-1}}{\partial x_j} = -f^{-1}\frac{\partial f}{\partial x_j} f \in F$$

We inductively define the higher derivatives:

$$\frac{\partial^n f}{\partial x_{i_1} ... x_{i_n}} := \frac{\partial}{\partial x_{i_1}}(\frac{\partial^{n-1} f}{\partial x_{i_2} ... x_{i_n}})$$

We also write $D_I(f)$, where $I = (i_1, ..., i_n)$.

Theorem 6 For $f, g \in \mathbb{Z}[F]$ and $I = (i_1, ..., i_n)$ we see that $\mu(I; f) = \epsilon_{\mathbb{Z}[F]}(D_I(f))$ and $\mu(I; fg) = \Sigma_{I=JK}\mu(J; f)\mu(K; g)$ where the sum is taken over all pairs (J,K) such that JK=I.

We have the following theorem relating lower central series and the degree of the image of the Magnus embedding:

Theorem 7 For $d \geq 2$ we have $F^{(d)} = \{f \in F | deg(M(f) - 1) \geq d\}$

Now we define the shuffle and discuss the shuffle relation among Magnus coefficients. Let $I = (i_1, ..., i_n)$ and $J = (j_1, ..., j_n)$ be a pair of multi-indices. A pair of sequences of integers $((f(1), ..., f(n)), (g(1), ..., g(m))$ is denoted the shuffle of I and J if both sequences are increasing and bounded above and below by m+n and 1, respectively and there exists a multi-index $H = (h_1, ..., h_l)$ such that

$$h_{f(s)} = i_s \ \ (s = 1, ..., n)$$

$$h_{g(t)} = j_t \ \ (t = 1, ..., m)$$

and such that for any $a = 1, ..., l$ there exists s or t such that $a = f(s)$ or $a = g(t)$. The index H is called the result of a shuffle. We set $Sh(I, J)$ to denote the set of results of shuffles of I and J. We let $PSh(I, J)$ denote the set of results of shuffles (f, g) such that $f(s) \neq g(t)$ for any pair (s, t) such that $1 \leq s \leq n$ and $1 \leq t \leq m$. We have the following theorem:

Theorem 8 For multiple indices I and J and $f \in F$, we see

$$\mu(I; f)\mu(J; f) = \Sigma_{H \in Sh(I,J)}\mu(H; f)$$

4 Milnor Invariants

Let L be a link with components $K_1, ..., K_r$ in S^3. Let G_L be the link group of L. Let $y_i^{(d)}$ be the word representing a longitude β_i of K_i in $G_L/G_L^{(d)}$ from above. Consider the Magnus expansion

$$M(y_i^{(d)}) = 1 + \Sigma_{I=(i_1,...,i_n),1 \leq i_1,...,\leq r}\mu^{(d)}(Ii)X_I$$

Theorem 7 implies for that large d, $\mu^{(d)}(I)$ is independent of d. So we set $\mu(I) = \mu^{(d)}(I)$ for sufficiently large d. We say that $\mu(I)$ is the Milnor number. We define the ideal $\Delta(I)$ to be the ideal of $\mathbb{Z}$ with generators consisting of the $\mu(J)$ as J runs over the cyclic permutations of proper subsequences of I, when $|I| \geq 2$. (When $|I| = 1$, we define $\mu(I)$ to be 0.) The Milnor $\overline{\mu}$ invariant is defined as $\mu(I) \ mod \ \Delta(I)$.

Theorem 9 (1) $\overline{\mu}(ij) = lk(K_i, K_j) \ (i \neq j)$.
(2) If $2 \leq |I| \leq d$, $\overline{\mu}(I)$ is a link invariant of L.
(3) For indices I and J and i between 1 and r we have

$$\Sigma_{H \in PSh(I,J)}\overline{\mu}(Hi) = 0 \ mod \ g.c.d. \ \{\Delta(Hi)|H \in PSh(I, J)\}$$

(4) $\overline{\mu}(I)$ is invariant under cyclic permutations of the index I. For a multi-index $I = (i_1, ..., i_n)$ consider the map $\rho_I : F \to N_n(\mathbb{Z}/\Delta(I))$ from the free group F to the group of $n \times n$ unipotent upper-triangular matrices with entries in $\mathbb{Z}/\Delta(I)$, given by $(\rho_I(f))_{j,k} = \epsilon(\frac{\partial^{i+j}f}{\partial x_{i_j}...x_{i_{j+k}}}) \ mod \ \Delta(I)$ for $j < k \leq n$.

Proof: We only comment on the proof of (2). It can be shown (See [Mo12] Remark 7.2) that if L and L' are isotopic links then $G_L/G_L^{(d)}$ and $G_{L'}/G_{L'}^{(d)}$ are isomorphic

through a map such that for given pairs (α_i, β_i) and (α'_i, β'_i) of meridians and longitudes of knot components in L and L', (α_i, β_i) is taken to $(\gamma\alpha'_i\gamma^{-1}, \gamma\beta'_i\gamma^{-1})$. Thus in order to show (2) it is enough to show:
(a) $\overline{\mu(I)}$ is unchanged if $y_{i_n}^{(d)}$ is replaced by a conjugate.
(b) $\overline{\mu(I)}$ is unchanged if x_i is switched out by a conjugate.
(c) $\overline{\mu(I)}$ is unchanged if $y_{i_n}^{(d)}$ is multiplied by a conjugate of $[x_i, y_i^{(d)}]$.
(d) $\overline{\mu(I)}$ is unchanged if y_{i_n} is multiplied by an element of $F^{(d)}$.
The proof of (1) follows quickly by Theorem 1. Indeed, we have that $\beta_j \equiv \prod_{i\neq j} \alpha_i^{lk(K_i,K_j} mod G_L^{(2)}$. Thus we see from the Magnus embedding

$$M(y_i^{(d)}) = 1 + \Sigma_{i\neq j} lk(K_i, K_j)X_i + HigherOrderTerms$$

We see immediately that $\overline{\mu}(ij) = \mu(ij) = lk(K_i, K_j)$.

The proof of (3) follows quickly from Theorem 8. Observe that we have

$$\mu(Ii)\mu(Ji) = \Sigma_{H\in Sh(I,J)}\mu(Hi)$$

We have that LHS $\equiv 0 \ mod \ g.c.d. \ \{\Delta(Hi)|H \in PSh(I, J)\}$. However $\mu(Hi)$ on the RHS is congruent to 0 when H is not a result of a proper shuffle. The claim follows.

We now show (4) in full detail. The argument follows that of $[Mo12]$. Set k strictly greater than $n = |I|$. Project L onto a plane and divide each component K_i into arcs $\alpha_{i1}, ..., \alpha_{i\lambda_i}$ Let $\overline{F}$ be the free group on generators x_{ij} $1 \leq i \leq n$, $1 \leq j \leq \lambda_i$. It follows from Mo12 chapter 2, that we have the following relation from the Wirtinger presentation

$$\prod_{i=1}^{r}\prod_{j=1}^{\lambda_i} z_{ij} r_{ij} z_{ij}^{-1} = 1$$

Consider $z_i = \eta_k(z_i\lambda_i)$. Then as $\eta_k(r_{ij}) = 1 mod F^{(d)}$ $(1 \leq j < \lambda_i)$ and $\eta_k(r_{i\lambda_i} = [x_i, y^{(d)}] mod F^{(d)}$, we have by Theorem 7 that

$$\prod_{i=1}^{r} z_i [x_i, y_i^{(d)} z_i^{-1} \in F^{(d)}$$

. Let K be the 2 sided ideal defined by

$$K := \{\Sigma_I c_I X_I \in \mathbb{Z} << X_1, ..., X_r >> |c_I = 0 mod \Delta(I), |I| \leq k\}$$

Consider the Magnus embeddings $M(y_i^{(d)}) = 1 + H_i$, where the H_i are higher order terms. By definition, $X_jX_iH_i$, $X_jH_iX_i$, $X_iH_iX_j$, $H_iX_iX_j$ all belong to K. We observe

$$M(z_i[x_i, y_i^{(d)}]z_i^{-1}) = 1 + M(z_i)([M(x_i), M(y_i^{(d)}](M(x_i^{-1}M(y_i^{(d)^{-1}}M(z_i^{-1})$$

$$= 1 + M(z_i)(X_iH_i - H_iX_i)M(x_i^{-1})M(y_i^{(d)^{-1}})M(z_i^{-1}) \equiv 1 + X_iH_i - H_iX_i \ mod \ K$$

Then Theorem 8 implies that $\Sigma_{i=1}^r(X_iH_i - H_iX_i \in K$. The coefficients on X_{iJ} is $\mu(Ji) - \mu(iJ)$ so we see that $\mu(Ji) \equiv \ \mu(iJ) \ mod \ \Delta(iJ)$. ♣

Now we come to our final theorem on Milnor invariants:

Theorem 10 (1) The homomorphism ρ_I factors through the link group G_L. We have surjectivity if the first $n-1$ indices of I are distinct.
(2) Suppose that the first $n-1$ indices of I are distinct. Then if $X_I \to X_L$ is the Galois covering corresponding to $Ker(\rho_I)$, with Galois group $Gal(M_I/S^3) = N_n(\mathbb{Z}/\Delta(I))$. In the case that $\Delta(I)$ is non-trivial, the Fox completion $M_I \to S^3$ of $X_I \to X_L$ satisfies that $M_I \to S^3$ is a Galois covering with ramification over the link $K_{i_1} \cup ... \cup K_{i_{n-1}}$. Let β_{i_n} be a longitude of K_{i_n}, then we have that $\rho_I(\beta_{i_n}$ is zero off the diagonal and away from $\rho_I(\beta_{i_n})_{(1,n)} = \overline{\mu}$. As a consquence, we see that $\overline{\mu} = 0$ is equivalent to K_{i_n} being completely decomposed in $M_I \to S^3$.

5 Extension to the Profinite Calculus

Per usual, the 'primes' side is 'larger' than the knots side. This time this manifests itself in that we must resort to a more 'massive' profinite Fox free differential calculus. Towards developing this end we have a theorem:

Theorem 11 We have an isomorphism of topological $\mathbb{Z}_l$ algebras $\mathbb{Z}_1[[\widehat{F}(l)]] \cong \mathbb{Z}_l << X_1, ..., X_r >>$ which restricts to the Magnus embedding on $\mathbb{Z}[[F]]$. $\widehat{M}$ is denoted the pro-l Magnus isomorphism.

We have a pro-l Magnus expansion and pro-l Magnus coefficients:

$$\widehat{M}(f) = \epsilon(f) + \Sigma_{I=(i_1,...,i_n),1 \leq i_1,...,i_n \leq r}\widehat{\mu}(I, f)X_I$$

Theorem 12 For $f \in \mathbb{Z}_l[[\widehat{F}(l)]]$ there exists uniquely $f_j \in \mathbb{Z}_l[[\widehat{F}(l)]]$ for each i between 1 and r such that

$$f = \epsilon(f) + \Sigma_{i=1}^r f_i(x_i - 1)$$

We say that f_j is the pro-l Fox free derivative of f w.r.t. x_j and set $\partial f/\partial x_j$.

The pro-l Fox derivative $\partial/\partial x_j : \mathbb{Z}_l[[\widehat{F}(l)]] \to \mathbb{Z}_l[[\widehat{F}(l)]]$ restricts to the ordinary Fox derivative on $\mathbb{Z}[F]$. It is no surprise that the pro-l Fox derivative satisfies the same linearity and Leibniz like rules as the Fox derivative. We also define higher pro-l derivatives in the same way we defined ordinary higher Fox derivatives, and are denoted by the same 'D_I' notation. We also have direct generalizations of Theorems 6-8 to the pro-l case.

Now tensoring with $\mathbb{Z}/m\mathbb{Z}$ for $m = l^e$ for some fixed $e \geq 1$ we have the mod m Magnus isomorphism $M_m : \mathbb{Z}/m\mathbb{Z}[[\widehat{F}(l)]] \cong \mathbb{Z}/m\mathbb{Z} << X_1, ..., X_r >>$

6 Arithmetic Invariants

We again fix a prime number l and a set $S = \{p_1, ..., p_r\} \subset \mathbb{Z}$ of primes that are all congruent to 1 mod l. Further, fix e_S to be the max exponent e such that all of the p_i are still congruent to 1 mode 1^e. Fix $m = l^e$.

Recall that by Theorem 2 we have that $G_S(l) =< x_1, ..., x_r | x_i^{p_i - 1}[x_i, y_i] = 1, 1 \leq i \leq r >$. Consider the pro-l Magnus expansion

$$\widehat{M}(y_i) = 1 + \Sigma \widehat{\mu}(Ii) X_I$$

By the analogue of the Theorem 7, we have that $\widehat{\mu}(Ii) = \epsilon(D_I(y_i))$. From the mod m Magnus expansion we also can consider $\mu_m = \widehat{\mu}(I) \ mod \ m$. For an index I satisfying $1 \leq |I| \leq l^{e_S}$, let $\Delta_m(I)$ be the ideal of $\mathbb{Z}/m\mathbb{Z}$ with generators $\binom{l^{e_S}}{t}$ $(1 \leq t < |I|)$ and $\mu_m(J)$ for J a proper subsequence of I or a permutation thereof. The Milnor $\widehat{\mu}$ invariant is given by $\widehat{\mu}_m(I) := \mu_m(I) \ mod \ \Delta_m(I)$. We have the following analogy to Theorem 11:

Theorem 13 (1) $\xi_m^{\mu_m(ij)} = (\frac{p_j}{p_i})_m$ where ξ_m is the primitive m^{th} root of unity satisfying $\xi_m^{l^s} = \xi_{l^n}^{l^s} = \xi_{l^{n-s}}$
(2) $\widehat{\mu}_m(I)$ depends on just S and I, when $2 \leq |I| \leq l^{e_S}$.
(3) Fix r between 2 and l^{e_S}. Then for indices I and J with $|I| + |J| = r - 1$ we have

$$\Sigma_{H \in PSh(I,J)} \widehat{\mu}_m(Hi) = 0 \ mod \ g.c.d. \ \{\Delta(Hi) | H \in PSh(I, J)\}$$

Proof: We only pause here to note that not only the statement of Theoren 12 mirrors the statement of Theorem 9, but the method of proof does as well. Observe that (2) is proved (in [Mo12]) by showing that $\overline{\mu(I)}_m$ independent of the choices of monodromy over p_i and the Frobenius automorphism over p_i. The argument boils down to showing:
(a) $\overline{\mu(I)}_m$ is unchanged if y_{i_n} is switched out by a conjugate.
(b) $\overline{\mu(I)}_m$ is unchanged if x_i is switched out by a conjugate.
(c) $\overline{\mu(I)}_m$ is unchanged if y_{i_n} is multiplied by a conjugate of $x_i^{p_i - 1}[x_i, y_i]$. It is worth remarking that the methods of proof of (1) and (3) also mirror that of (1) and (3) in

Theorem 10. ♣

Consider the group homomorphism $\rho_{m,I} : \widehat{F}(l) \to N_n(\mathbb{Z}/m\mathbb{Z}/\Delta_m(I)$ from the pro-l free group on r generators to the group of upper triangular matrices with entries in $\mathbb{Z}/m\mathbb{Z}/\Delta_m(I)$ by $(\rho_{(m,I)})_{j,k} = \epsilon(\frac{\partial^{k-1} f}{\partial x_{i_j} \ldots x_{i_k}})$. We have our final theorem:

Theorem 14 (1) The homomorphism $\rho_{(m,I)}$ factors through the Galois group $G_S(l)$. We have surjectivity if the first $n-1$ indices of I are distinct.
(2) Suppose that the first $n-1$ indices of I are distinct. Let $k_{(m,I)}$ be the extension over $\mathbb{Q}$ corresponding to $Ker(\rho_{(m,I)})$. Then $k_{(m,I)}$ is Galois and ramified over the primes $p_{i_1}, ..., p_{i_n}$ such that $Gal(k_{(m,I)}/\mathbb{Q}) = N_n(\mathbb{Z}/\Delta_m(I))$. The Frobenius automorphism σ_{i_n} over p_{i_n} satisfies $\rho_{(m,I)}(\sigma_{i_n})$ that $\rho_I(\beta_{i_n}$ is zero off the diagonal and away from $\rho_I(\beta_{i_n})_{(1,n)} = \overline{\mu}$. As a consquence, we see that $\overline{\mu}_m = 0$ is equivalent to p_{i_n} being completely decomposed in $k_{(m,I)}/\mathbb{Q}$. Further the results stated here suggest an analogy between Milnor numbers $\mu(i_1...i_n)$ and $l - adic$ Milnor numbers $\widehat{\mu}$ suggest that these share an analogous relationship. In addition, the Milnor invariants $\overline{\mu}$ seem to share an analogous relationship with the mod m Milnor invariants $\overline{\mu}_m$ as evidenced in Theorems 13 and 9. We see that the Chapter 5 of [Mo12] establishes the analogy between the decomposition groups of knots and the decomposition groups of primes. Theorems 14 and 10 enrichen this analogy. It is fitting that the results on the 'knots' side of things rest can be shown with the Fox free differential calculus and that the results on the 'primes' can be shown with the pro-l Fox differential calculus using analogous methods. The analogy is thus made much deeper since the analogous theorem statements have even similar methods of argument.

The following source was not cited but was used for clarification:
M. Morishita, Milnor invariants and Massey products for prime numbers. Compositio Math. (2004) 69-83