Massey Products and Ideal Class Groups

Number Theory seminar at MPI

Romyar T. Sharifi

August 27, 2003

Cup products in Galois cohomology:

p prime number, $n \geq 1$.

K field, Ω Galois extension of K, $G_{\Omega/K} = \mathrm{Gal}(\Omega/K)$.

Cup products:

$$H^1(G_{\Omega/K}, \mathbf{Z}/p^n\mathbf{Z}) \otimes H^1(G_{\Omega/K}, \mathbf{Z}/p^n\mathbf{Z}) \xrightarrow{\cup} H^2(G_{\Omega/K}, \mathbf{Z}/p^n\mathbf{Z}).$$

Let $\chi_1, \chi_2 \in \mathrm{Hom}(G_{\Omega/K}, \mathbf{Z}/p^n\mathbf{Z})$. Their cup product is represented by the cocycle

$$(\chi_1 \cup \chi_2)(\sigma, \tau) = \chi_1(\sigma)\chi_2(\tau),$$

for $\sigma, \tau \in G_{\Omega/K}$.

The cup product is the obstruction to the existence of a homomorphism $\rho\colon G_{\Omega/K} \to GL_3(\mathbf{Z}/p^n\mathbf{Z})$ with

$$\rho(\sigma) = \begin{pmatrix} 1 & \chi_1(\sigma) & \kappa(\sigma) \\ 0 & 1 & \chi_2(\sigma) \\ 0 & 0 & 1 \end{pmatrix}$$

for some map $\kappa\colon G_{\Omega/K} \to \mathbf{Z}/p^n\mathbf{Z}$.

Precisely, if ρ exists, then

$$d\kappa(\sigma, \tau) = \kappa(\sigma) + \kappa(\tau) - \kappa(\sigma\tau) = -(\chi_1 \cup \chi_2)(\sigma, \tau).$$

Massey products:

We define Massey products inductively. Two-fold Massey products are cup products, and 1-fold are trivial.

So let $r \geq 3$, and choose $\chi_1, \ldots, \chi_r \in \mathrm{Hom}(G_{\Omega/K}, \mathbf{Z}/p^n\mathbf{Z})$.

Let $T_{r+1}(n)$ denote the subgroup of upper-triangular unipotent matrices in $GL_{r+1}(\mathbf{Z}/p^n\mathbf{Z})$, and let $Z_{r+1}(n)$ denote its center.

Assume that there exists a homomorphism

$$\bar{\rho}\colon G_{\Omega/K} \to T_{r+1}(n)/Z_{r+1}(n)$$

with

$$\bar{\rho}(\sigma)_{i,i+1} = \chi_i(\sigma)$$

for $1 \leq i \leq r$.

Set

$$\kappa_{i,j}(\sigma) = \bar{\rho}(\sigma)_{i,j+1}$$

for $1 \leq i \leq j \leq r$ and $(i,j) \neq (1,r)$.

Then the r-fold Massey product

$$(\chi_1, \ldots, \chi_r) \in H^2(G_{\Omega/K}, \mathbf{Z}/p^n\mathbf{Z})$$

is represented by the cocycle

$$(\sigma, \tau) \mapsto \sum_{i=1}^{r-1} \kappa_{1,i}(\sigma)\kappa_{i+1,r}(\tau).$$

This cocycle is the obstruction to lifting $\bar{\rho}$ to $\rho\colon G_{\Omega/K} \to T$.

For example, if $r = 3$, then

$$\bar{\rho} = \begin{pmatrix} 1 & \chi_1 & \kappa_{1,2} & * \\ 0 & 1 & \chi_2 & \kappa_{2,3} \\ 0 & 0 & 1 & \chi_3 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

and the cocycle is

$$(\sigma, \tau) \mapsto \chi_1(\sigma)\kappa_{2,3}(\tau) + \kappa_{1,2}(\sigma)\chi_3(\tau).$$

There is an inherent ambiguity in the definition of the Massey product arising from the choices in the classes of maps $\kappa_{i,j}$, i.e., the choice of defining system. For example, $\kappa_{1,2}$ is defined only up to a cocycle, since it must satsify $d\kappa_{1,2} = \chi_1 \cup \chi_2$. So (χ_1, χ_2, χ_3), for instance, is well-defined only as an element of

$$H^2(G_{\Omega/K}, \mathbf{Z}/p^n\mathbf{Z})/(\chi_1 \cup H^1(G_{\Omega/K}, \mathbf{Z}/p^n\mathbf{Z}) + H^1(G_{\Omega/K}, \mathbf{Z}/p^n\mathbf{Z}) \cup \chi_3).$$

We will be interested in Massey products of the form $(\chi_1, \ldots, \chi_1, \chi_r)$. In this case, we can reduce the ambiguity in the definition to shorter Massey products of the same form (with χ_r replaced by an arbitrary character).

Massey products with coefficients in roots of unity:

Now assume that $\operatorname{char} K \neq p$ and $\mu_{p^n} \subset K$.

Fix positive integers $m \leq n$ and $k \leq p^{n+m-1} - 1$.

Note that

$$H^1(G_{\Omega/K}, \mu_{p^m}) \cong (K^\times \cap \Omega^{\times p^m})/K^{\times p^m}.$$

Assume given $a \in K^\times \cap \Omega^{\times p^n}$ with $a \notin K^{\times p}$ and $b \in K^\times \cap \Omega^{\times p^m}$.

We will consider $(k+1)$-fold Massey products of the form $(\chi_a, \ldots, \chi_a, \chi_b)$, where χ_a and χ_b denote the Kummer characters associated to a and b, respectively.

These will take values in a to-be-defined quotient of $H^2(G_{\Omega/K}, \mu_{p^m}^{\otimes(k+1)})$ and are denoted by $(a, b)^{(k)}_{p^m,\Omega/K}$.

Operators: Let G be a cyclic group of order p^n, and let σ generate G. Define

$$D^{(k)} = D_\sigma^{(k)} = (-1)^k \sum_{i=k}^{p^n-1} \binom{i}{k} \sigma^{i-k} \in \mathbf{Z}[G].$$

For $j \leq k$, we have

$$(\sigma - 1)^j D^{(k)} \equiv D^{(k-j)} \bmod p^m \mathbf{Z}[G].$$

Note that $D^{(0)}$ is the norm element of $\mathbf{Z}[G]$.

To obtain an acceptable formula for the Massey products and to reduce the ambiguity in their definition, we restrict the allowable choices of defining systems.
Let $\alpha^{p^n} = a$, let $L = K(\alpha)$, set $G = G_{L/K}$, and let σ be a generator.
Let $\zeta = \alpha^{\sigma-1} \in \mu_{p^n}$. Note: ζ is primitive.
We will assume that $b = N_{L/K} y$ for some $y \in L^\times$ and that $D^{(k-1)} y \in \Omega^{\times p^m}$.
Let us denote the group of such b by $U_{m,n}^{(k)}(a)$, and the set of such y for a given b by $V_{m,n}^{(k)}(a,b)$.

Given $y \in V_{m,n}^{(k)}(a,b)$ and a lift of σ to $G_{\Omega/K}$, we construct a homomorphism

$$\rho \colon G_K \to T_{k+2}(m)$$

from the absolute Galois group G_K of K with reduction inducing a defining system

$$\bar{\rho} \colon G_{\Omega/K} \to T_{k+2}(m)/Z_{k+2}(m)$$

of the k-fold Massey product $(a,b)_{p^m,\Omega/K}^{(k)} \otimes \zeta_m^{\otimes -(k+1)}$, where $\zeta_m = \zeta^{p^{n-m}}$.
Let $[x]$ denote the class of $x \in \Omega^\times$ in $H^1(G_\Omega, \mu_{p^m}) \cong \Omega^\times / \Omega^{\times p^m}$.
The induced character $\rho_{1,k+2} \colon G_\Omega \to Z_{k+2}(m) \cong \mu_{p^m}$ (via ζ_m) equals $[D^{(k)} y]$.

Theorem 1. *The map $\bar{\rho}$ provides a defining system for $(a,b)^{(k)}_{p^m,\Omega/K}$ with associated cohomology class given by*

$$\mathrm{Tra}_\Omega\,[D^{(k)}y] \otimes \zeta_m^{\otimes k} \in H^2(G_{\Omega/K}, \mu_{p^m}^{\otimes(k+1)}),$$

with Tra_Ω *the transgression map*

$$\mathrm{Tra}_\Omega\colon H^1(G_\Omega, \mu_{p^m})^{G_{\Omega/K}} \to H^2(G_{\Omega/K}, \mu_{p^m}).$$

The proof involves an interesting comparison between exact sequences in non-abelian cohomology associated to

$$0 \to Z_{k+2}(m) \to T_{k+2}(m) \to T_{k+2}(m)/Z_{k+2}(m) \to 0$$

and the sequence of base terms in the Hochschild-Serre spectral sequence in which Tra_Ω arises.

Let

$$P^{(k)}_{m,n}(a) = \langle \mathrm{Tra}_\Omega\,[D^{(k)}y] \mid b \in U^{(k)}_{m,n}(a), y \in V^{(k)}_{m,n}(a,b)\rangle.$$

Theorem 2. *For $b \in U^{(k)}_{m,n}(a)$ and $y \in V^{(k)}_{m,n}(a,b)$, define the $(k+1)$-fold Massey product of a and b to be*

$$(a,b)^{(k)}_{p^m,\Omega/K} = \mathrm{Tra}_\Omega\,[D^{(k)}y] \otimes \zeta_m^{\otimes k} \pmod{P^{(k-1)}_{m,n}(a) \otimes \mu_{p^m}^{\otimes k}}.$$

This definition depends only upon K, Ω, m, n, k, a, and b.

Proof. We illustrate independence from the choice of y. If $y, y' \in V^{(k)}_{m,n}(a,b)$, then $y' = yz^{\sigma-1}$ for some $z \in L^\times$, and

$$D^{(k)}y' \equiv D^{(k)}yD^{(k-1)}z \bmod L^{\times p^m}.$$

Similarly, $D^{(k-2)}z \in \Omega^{\times p^m}$, so

$$\mathrm{Tra}_\Omega[D^{(k-1)}z] \in P^{(k-1)}_{m,n}(a).$$

□

Massey Products with restricted ramification:

Now: K is a number field containing μ_{p^n}.

S set of primes including those above p and all real archimedean places.

Ω the maximal extension of K unramified outside S.

$G_{K,S} = G_{\Omega/K}$, and G, L, σ as before.

$A_{K,S}$ the p-part of the S-class group of K, the quotient of p-part of the class group A_K by the prime ideals in S.

Note that there is a natural injection

$$A_{K,S}/p^m A_{K,S} \hookrightarrow H^2(G_{K,S}, \mu_{p^m})$$

As defined, $P^{(k)}_{m,n}(a)$ is actually a subgroup of $A_{K,S} \otimes \mu_{p^m}^{\otimes k}$.

Let $I_{F,S}$ denote the S-ideal group of F/K.

For $\mathfrak{X} \in I_{F,S}$, let $[\mathfrak{X}]$ denote its class in $A_{K,S}/p^m A_{K,S}$.

Theorem 3. *Let k and m be positive integers with $k < p^{n-m}(p-1)$. If $k \geq 2$, assume that at most one prime in S does not split completely in L. Let $b \in U^{(k)}_{m,n}(a)$ and $y \in V^{(k)}_{m,n}(a,b)$. Let L' denote the subfield of L of degree p^{n-m} over K. Then we may write*

$$y\mathcal{O}_{L,S} \equiv \mathfrak{A}^{(\sigma-1)^k}\mathfrak{B} \bmod p^m I_{L,S},$$

with $\mathfrak{A} \in I_{L,S}$ and $\mathfrak{B} \in I_{L',S}$, and we have

$$(a,b)^{(k)}_{p^m,\Omega/K} = -[N_{L/K}\mathfrak{A}] \otimes \zeta_m^{\otimes k} \pmod{P^{(k-1)}_{m,n}(a) \otimes \mu_{p^m}^{\otimes k}}.$$

Iwasawa Theory:

K a number field and $K_n = K(\mu_{p^n})$ for $n \leq \infty$.

L_∞ a $\mathbf{Z}_p$-extension of K_∞ unramified outside S.

$X_{K,S}$ (resp., $X_{L,S}$) the Galois group of the maximal unramified pro-p abelian extension of K_∞ (resp., L_∞) in which all primes above those in S split completely.

There exists a sequence of elements $a = (a_n)$ for n sufficiently large and a nondecreasing sequence (l_n) with infinite limit and $l_n \leq n$ for all n, such that $a_n \in K_n^\times \cap \Omega^{\times p^{l_n}}$, $a_n \notin K_n^{\times p}$, with

$$a_{n+1}a_n^{-1} \in K_{n+1}^{\times p^{l_n}}$$

and such that, setting $\alpha_n^{p^{l_n}} = a_n$ and $L_n = K_n(\alpha_n)$, we have $L_\infty = \cup L_n$.

Let m_n be a sequence with $k \leq p^{l_n - m_n}(p-1)$ for n sufficiently large, and let

$$P_\infty^{(k)}(a) = \lim_{\leftarrow} P_{m_n,l_n}^{(k)}(a_n) \leq X_{K,S}.$$

$G = G_{L_\infty/K_\infty}$, $\Lambda = \mathbf{Z}_p[[G_{K_\infty/K}]]$, I_G the augmentation ideal of $\mathbf{Z}_p[[G]]$.

Theorem 4. *Assume that every prime above S in K_∞ other than v splits completely in L_∞ and that v does not split. We have a canonical isomorphism of pro-p groups,*

$$I_G^k X_{L,S}/I_G^{k+1}X_{L,S} \cong (I_G/I_G^2)^{\otimes k} \otimes_{\mathbf{Z}_p} X_{K,S}/P_\infty^{(k)}(a),$$

which is an isomorphism of Λ-modules if L_∞/K is Galois.

Note: I_G/I_G^2 is noncanonically isomorphic to $\mathbf{Z}_p$ as a $\mathbf{Z}_p$-module.

The theorem holds with $k = 0$ by the assumption, with $P_\infty^{(0)}(a) = 0$.

Theorem 4 tells us that Massey products determine the structure of the graded quotients of $X_{L,S}$ with respect to the augmentation filtration.

Examples:

Let p be even, $K = \mathbf{Q}(\mu_p)$, and $K_n = \mathbf{Q}(\mu_{p^n})$ for $n \leq \infty$.

Let S consist of the unique prime above p.

Note that $A_{K,S} = A_K$ and $X_{K,S} = X_K$, with X_K the Galois group of the maximal unramified pro-p abelian extension of K_∞.

Let T be the group of integer sequences $t = (t_n)$ with

$$t_{n+1} \equiv t_n \bmod p^{n-1}(p-1).$$

For $t \in T$, we may define a sequence of cyclotomic p-units$\lambda_t = (\lambda_{t,n})$, where

$$\lambda_{t,n} = \prod_{\substack{i=1 \\ (i,p)=1}}^{p^n-1} (1-\zeta_n^i)^{i^{t_n-1}}.$$

Then

$$\lambda_{t,n+1}\lambda_{t,n}^{-1} \in K_{n+1}^{\times p^n}.$$

Let L_∞ be any totally ramified $\mathbf{Z}_p$-extension of K_∞ defined by some such sequence λ_t (with t_1 odd).

Set $\mathcal{G} = \mathrm{Gal}(L_\infty/\mathbf{Q})$. Let $\Delta = \mathrm{Gal}(K/\mathbf{Q})$, let ω denote the Teichmüller character, and for $i \in T$, set

$$\epsilon_i = \frac{1}{p-1}\sum_{\delta\in\Delta} \omega(\delta)^{-i}\delta \in \mathbf{Z}_p[\Delta].$$

Proposition. *Assume that A_K has p-rank 1, and let r even be such that $A_K = \epsilon_{1-r}A_K$. If $(\lambda_{t,1}, \lambda_{r-t,1})^{(1)}_{p,\,\Omega/K} \neq 0$, then $X_{L,S} \cong X_K$ as $\mathbf{Z}_p[[\mathcal{G}]]$-modules.*

In particular, in this case $X_{L,S}$ is pseudo-null as a $\mathbf{Z}_p[[\mathcal{G}]]$-module (in the sense of Venjakob).

For $p = 37$, McCallum and I exhibited that the cup product is nontrivial on cyclotomic p-units (note $37 \mid B_{32}$). I have recently given a computable condition for the nontriviality of the cup product in terms of the operator U_p and the Eisenstein ideal in a certain Hecke algebra.

Corollary. *For $p = 37$ and $t \in T$ with $t \not\equiv 5, 27 \bmod 36$, we have isomorphisms of $\mathbf{Z}_p[[\mathcal{G}]]$-modules,*

$$X_{L,S} \cong X_K \cong \mathbf{Z}_p(s),$$

for some $s \in T$ with $s \equiv 5 \bmod 36$. If, furthermore, $t \not\equiv 31 \bmod 36$, then $X_L \cong \mathbf{Z}_p(s)$ as well.

$X_{L,S}$ can also have larger p-rank than X_K as well.

Proposition. *Assume that $X_K \cong \mathbf{Z}_p(s)$ for some $s \in T$. Let $t = 1 - 2s$. Then we have isomorphisms of Λ-modules,*

$$I_G^k X_{L,S} / I_G^{k+1} X_{L,S} \cong \mathbf{Z}_p(s + kt),$$

if $k = 0$ or 1, and for $k = 2$ if $3s \not\equiv -1 \bmod p - 1$.

Question: Is $X_{L,S}$ ever not pseudo-null as a $\mathbf{Z}_p[[\mathcal{G}]]$-module?
X_L (or $X_{L,S}$) is not pseudo-null $\Longleftrightarrow$ $X_{L,S}$ is not $\mathbf{Z}_p[[G]]$-torsion $\Longleftrightarrow$ $I_G^k X_{L,S} / I_G^{k+1} X_{L,S}$ is infinite for any k.
When A_K has p-rank 1, this is equivalent to: $P_\infty^{(k)}(a) = 0$ for all k $\Longleftrightarrow$ every "universal norm" in K_∞/K is a universal norm of p-units from L_∞. (Here, we allow elements in the $\mathbf{Z}_p$-completions of $K_n^\times$ and $L_n^\times$.)