CONGRUENCE MODULES IN IWASAWA THEORY

JACOB SWENBERG

Abstract. In this short note, we define congruence modules and discuss their basic properties. We also outline a result of Ohta which describes the congruence module attached to a certain exact sequence arising from a limit of cohomology groups of modular curves. We finish by discussion Ohta's application of these results to Iwasawa theory.

Contents

1. Algebraic preliminaries

1.1. Congruence modules.

Let R be an integral domain with field of fractions F. Let

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

be a short exact sequence of flat R-modules. We write $A_F := F \otimes_R A$, and similarly define B_F and C_F. We may identify A with its image in A_F by flatness. Then the exact sequence

$$0 \to A_F \xrightarrow{\iota_F} B_F \xrightarrow{\pi_F} C_F \to 0$$

is split, so we may choose a section $s : C_F \to B_F$ of π_F.

Definition 1.1. The *congruence module* (attached to the above situation) is

$$\mathcal{C}(\pi, s) = C/\pi(B \cap s(C)).$$

Note that for all $\beta \in B_F$, we have $\beta - s(\pi_F(\beta)) \in \ker \pi_F$. We may then define an F-linear map $t : B_F \to A_F$ by the property that for all $\beta \in B_F$,

$$\iota_F(t(\beta)) + s(\pi_F(\beta)) = \beta.$$

Note that $t \circ \iota_F = 1_{A_F}$ is the identity. In particular, $A \subseteq t(B).$, and $t(B_F) = A_F$. Furthermore, for all $\xi \in C_F$, we have

$$\iota_F(t(s(\xi))) = s(\xi) - s(\pi_F(s(\xi))) = s(\xi) - s(\xi) = 0.$$

Lemma 1.2. *We have an isomorphism*

$$\phi : \mathcal{C}(\pi, s) \cong t(B)/A$$

defined as follows: let $[c] \in \mathcal{C}(\pi, s)$*, where* $c \in C$*. Choose any* $b \in B$ *with* $\pi(b) = c$*, and set* $\phi[c] = [t(b)]$*.*

Proof. We first show this is well-defined. Let $c, c' \in C$ and $b, b' \in B$ be such that $[c'] = [c] \in \mathcal{C}(\pi, s)$, $\pi(b) = c$, and $\pi(b') = c'$. Then there exists $c_0 \in C$ such that $s(c_0) \in B$ and $c' - c = \pi_F(s(c_0))$. Then

$$\pi(b' - b) = \pi(s(c_0)),$$

so $b' = b + s(c_0) + \iota(a)$ for some $a \in A$. Then

$$t(b') = t(b) + t(s(c_0)) + t(\iota(a)) = t(b) + a.$$

Then $[t(b')] = [t(b)] \in t(B)/A$. Furthermore, ϕ is clearly R-linear and surjective.

We now show ϕ is injective. Suppose that $\phi[c] = 0$ for some $c \in C$. Then there exists $b \in B$ and $a \in A$ such that $\pi(b) = c$ and $t(b) = a$. Then

$$\iota(a) = \iota_F(a) = \iota_F(t(b)) = b - s(\pi_F(b)) = b - s(\pi(b)).$$

In particular, $s(\pi(b)) \in B$, so

$$c = \pi(b) = \pi(s(\pi(b)) \in \pi(B \cap s(C)).$$

This completes the proof. ∎

Example 1.3. Let G be a group, and let X be a set on which G acts. Then we may consider the free abelian group $\mathbb{Z}[X]$ on X as a $\mathbb{Z}[G]$-module. We have a natural G-equivariant map $\deg : \mathbb{Z}[X] \to \mathbb{Z}$ given by $\sum_{x \in X} n_x x \mapsto \sum_{x \in X} n_x$. Let $\mathbb{Z}[X]_0$ denote the kernel of this map. Then we have a short exact sequence

$$0 \to \mathbb{Z}[X]_0 \to \mathbb{Z}[X] \xrightarrow{\deg} \mathbb{Z} \to 0.$$

Given any element $x \in X$, we consider the element $N_G x = \sum_{g \in G} gx \in \mathbb{Z}[X]^G$. We then obtain a G-equivariant splitting $s_x : \mathbb{Q} \to \mathbb{Q}[X]$ of $\deg_{\mathbb{Q}} : \mathbb{Q}[X] \to \mathbb{Q}$ by $1 \mapsto \deg(N_G x)^{-1} N_G x$. This gives the congruence module

$$\mathcal{C}(\deg, s_x) = \mathbb{Z}/(\deg(\mathbb{Z}[X] \cap s_x(\mathbb{Q}))) = \mathbb{Z}/\deg\left(\sum_{y \in Gx} y\right) = \mathbb{Z}/|Gx|.$$

1.2. **Fitting ideals.** We refer the reader to the appendix of [2] for more details.

Definition 1.4. Let R be a commutative ring.

(1) Let A be an $(n \times m)$-matrix with coefficients in R. The *Fitting ideal* of A, denoted $\mathrm{Fitt}_R(A)$, is R if $m < n$, and otherwise is the ideal of R generated by the $n \times n$ minors of A.

(2) Let M be a finitely presented R-module, given by an exact sequence

$$R^m \xrightarrow{h} R^n \to M \to 0.$$

Then the *Fitting ideal* of M, denoted $\mathrm{Fitt}_R(M)$, is defined to be the fitting ideal of the matrix giving h.

2. Congruence modules attached to Eisenstein series

For a congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$, we denote by $X(\Gamma)$ the usual modular curve of level Γ. We use standard notation for the modular curves $X(N)$, $X_1(N)$, and $X_0(N)$, modular forms $M_k(\Gamma, R)$ and $S_k(\Gamma, R)$, and Hecke algebras $\mathfrak{H}_k(\Gamma, R)$ and $\mathfrak{h}_k(\Gamma, R)$. In particular, we denote $\mathrm{SL}_2(\mathbb{Z})$ by $\Gamma(1)$.

Let $k \geq 4$, and let p be a prime such that $k \not\equiv 0 \pmod{p-1}$. Then there is a short exact sequence

$$0 \to S_k(\Gamma(1), \mathbb{Z}_p) \to M_k(\Gamma(1), \mathbb{Z}_p) \to \mathbb{Z}_p \to 0,$$

where the last nonzero map takes $f \in M_k(\Gamma(1), \mathbb{Z}_p) \subseteq \mathbb{Z}_p[[q]]$ to its constant coefficient. Upon tensoring with $\mathbb{Q}_p$, the above sequence uniquely splits as $\mathfrak{H}_k(\Gamma(1), \mathbb{Q}_p)$-modules, with the image of $\zeta(1-k)/2 \in \mathbb{Q}_p$ given by the usual weight k Eisenstein series:

$$E_k := \frac{\zeta(1-k)}{2} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \in M_k(\Gamma(1), \mathbb{Z}_p).$$

As in [3], the congruence module attached to this situation is $\mathbb{Z}_p/\zeta(1-k)\mathbb{Z}_p$.

In [3], Ohta generalizes this result to a Λ-adic setting, considering several related exact sequences of Λ-adic objects, when Λ is the Iwasawa algebra. In Section 3, we describe some of Ohta's results.

3. Ohta's results

Let $p \geq 5$ be prime. Let N be a positive integer prime to p. We further assume that p does not divide $\varphi(N)$. Let $K \subseteq \mathbb{C}_p$ be a complete subfield, and let $\mathcal{O}_K$ denote its ring of integers with uniformizer π_K. We set

$$\mathscr{T} := \varprojlim_r H^1_{\text{ét}}(X_1(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p), \qquad \widetilde{\mathscr{T}} := \varprojlim_r H^1_{\text{ét}}(Y_1(Np^r)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p),$$

$$\mathscr{T}_{\mathcal{O}_K} := \mathscr{T} \widehat{\otimes}_{\mathbb{Z}_p} \mathcal{O}_K, \qquad \widetilde{\mathscr{T}}_{\mathcal{O}_K} := \widetilde{\mathscr{T}} \widehat{\otimes}_{\mathbb{Z}_p} \mathcal{O}_K.$$

On these modules, there are commuting continuous actions of $G_{\mathbb{Q}}$ and the adjoint Hecke operators $T^*(n)$ for n a positive integer, and $T^*(q,q)$ for positive integers q prime to N. As usual, we have Hida's idempotent $e^* := \lim_{n\to\infty} T^*(p)^{n!}$.

Let $\mathbb{Z}_{p,N} := \varprojlim_r \mathbb{Z}/Np^r\mathbb{Z}$. Let

$$\widetilde{\Lambda}_{\mathcal{O}_K} := \mathcal{O}_K[[\mathbb{Z}_{p,N}^\times]] = \varprojlim_r \mathcal{O}_K[(\mathbb{Z}/Np^r)^\times] \cong \mathcal{O}_K[(\mathbb{Z}/Np)^\times][[1+p\mathbb{Z}_p]],$$

$$\Lambda_{\mathcal{O}_K} := \mathcal{O}_K[[1+p\mathbb{Z}_p]] \cong \mathcal{O}_K[[T]], \qquad [1+p] \mapsto 1+T.$$

Here, for $a \in 1+p\mathbb{Z}_p$, we denote the corresponding element of $\Lambda_{\mathcal{O}_K}$ by $[a]$. Then $\mathscr{T}_{\mathcal{O}_K}$ and $\widetilde{\mathscr{T}}_{\mathcal{O}_K}$ are modules over $\widetilde{\Lambda}_{\mathcal{O}_K}$, and hence over $\Lambda_{\mathcal{O}_K}$. By [1, Theorem 3.1], the modules $\mathscr{T}^{\mathrm{ord}}_{\mathcal{O}_K} := e^* \mathscr{T}_{\mathcal{O}_K}$ and $\widetilde{\mathscr{T}}^{\mathrm{ord}}_{\mathcal{O}_K} := e^* \widetilde{\mathscr{T}}_{\mathcal{O}_K}$ are free of finite rank over $\Lambda_{\mathcal{O}_K}$.

Furthermore, let $\mathfrak{h}^{\mathrm{ord}}_{\mathcal{O}_K}$ (resp. $\mathfrak{H}^{\mathrm{ord}}_{\mathcal{O}_K}$) denote the subalgebra of $\mathrm{End}_{\mathcal{O}_K}(\mathscr{T}^{\mathrm{ord}}_{\mathcal{O}_K})$ (resp. $\mathrm{End}_{\mathcal{O}_K}(\widetilde{\mathscr{T}}^{\mathrm{ord}}_{\mathcal{O}_K})$) generated by $T^*(n)$ and $T^*(q,q)$. These are Hida's *universal ordinary Hecke algebras*, and they act on the spaces $S^{\mathrm{ord}}(\Lambda_{\mathcal{O}_K})$ and $M^{\mathrm{ord}}(\Lambda_{\mathcal{O}_K})$ of ordinary $\Lambda_{\mathcal{O}_K}$-adic cusp forms and modular forms, respectively, via $T^*(n) \mapsto T(n)$ and $T^*(q,q) \mapsto T(q,q)$. Furthermore, these Hecke algebras are $\widetilde{\Lambda}_{\mathcal{O}_K}$-algebras, where for $a \in \mathbb{Z}_{p,N}^\times$, the element $[a] \in \widetilde{\Lambda}_{\mathcal{O}_K}$ acts as $T^*(a,a)$.

We introduce some characters.

- Let $\chi : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ be the usual p-adic cyclotomic character.
- Let $\omega : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ be the Teichmüller character, which factors through the unique section $(\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$.
- Let $\kappa : \mathbb{Z}_p^\times \to 1 + p\mathbb{Z}_p$ be defined by $\kappa(a) = a\omega(a)^{-1}$.
- Let u, v be positive integers such that $uv =\in \{N, Np\}$, and $p \nmid v$. Let θ and ψ be Dirichlet characters of modulus u and v, respectively, such that $\theta\psi(-1) = 1$.
- We assume that (θ, ψ) is not *exceptional*. We say that (θ, ψ) is *exceptional* if $\theta|_{(\mathbb{Z}/p\mathbb{Z})^\times} = \omega^{-1}$ and $(\theta\omega\psi^{-1})(p) = 1$.
- We henceforth assume that K is a finite extension of $\mathbb{Q}_p$ containing the values of θ and ψ.

We will also use a certain twist of the Kubota-Leopoldt p-adic L-function L_p. Namely, there exists $g_{\theta\omega^2} \in Q(\Lambda_{\mathcal{O}_K})$ such that the following hold:

- If $\theta\omega^2 = 1$, then $g_1 \in ((1+T) - (1+p)^2)^{-1}\Lambda_{\mathbb{Z}_p}$. Otherwise, $g_{\theta\omega^2} \in \Lambda_{\mathcal{O}_K}$.
- For any finite order character $\epsilon : 1 + p\mathbb{Z}_p \to \overline{\mathbb{Q}_p}^\times$ and any positive integer s, we have
$$g_{\theta\omega^2}(\epsilon(1+p)(1+p)^s - 1) = L_p(-1-s, \theta\omega^2\epsilon).$$

We also recall the definition of the Λ-*adic Eisenstein series attached to* (θ, ψ):
$$\mathcal{E} := \mathcal{E}(\theta, \psi) := \delta(\psi) g_{\theta\omega^2} + \sum_{n \geq 1} \left(\sum_{d|n,\, p\nmid d} \theta(d)\psi(n/d)d[\kappa(d)] \right) q^n \in Q(\Lambda_{\mathcal{O}_K}) + q\Lambda[[q]].$$
Here, $\delta(\psi) = 0$ unless $\psi = 1$ is the trivial character, in which case $\delta(\psi) = 1/2$.

Definition 3.1. The *Eisenstein ideal* (associated to (θ, ψ)) is
$$\widetilde{I} := \widetilde{I}(\theta, \psi) := \mathrm{Ann}_{\mathfrak{H}^{\mathrm{ord}}_{\mathcal{O}_K}}(\mathcal{E}(\theta, \psi)).$$
The *Eisenstein maximal ideal* is
$$\widetilde{\mathfrak{m}} := (\widetilde{I}, \pi_K, T).$$
We denote the images of $\widetilde{I}$ and $\widetilde{\mathfrak{m}}$ under the surjection $\mathfrak{H}^{\mathrm{ord}}_{\mathcal{O}_K} \to \mathfrak{h}^{\mathrm{ord}}_{\mathcal{O}_K}$ by I and $\mathfrak{m}$, respectively.

For $(\theta, \psi) \neq (\omega^{-2}, 1)$, we let
$$A_{\theta,\psi} := \left(\prod_{\substack{d|N \\ d\nmid \mathrm{cond}(\theta\psi^{-1})}} ([\kappa(d)] - (\theta\omega^2\psi^{-1})^{-1}(d)\kappa(d)^{-2} \right) g_{\theta\omega^2\psi^{-1}}.$$

We now can state part of the main result of [3].

Theorem 3.2. [3, Theorem 1.5.5] *There is an exact sequence of $\Lambda_{\mathcal{O}_K}$-modules*
$$0 \to (\mathscr{T}^{\mathrm{ord}}_{\mathcal{O}_K})_{\widetilde{\mathfrak{m}}} \to (\widetilde{\mathscr{T}}^{\mathrm{ord}}_{\mathcal{O}_K})_{\widetilde{\mathfrak{m}}} \to \Lambda_{\mathcal{O}_K} \to 0.$$
Upon tensoring with $Q(\Lambda_{\mathcal{O}_K})$, this sequence splits uniquely as modules over $(\mathfrak{H}^{\mathrm{ord}}_{\mathcal{O}_K})_{\widetilde{\mathfrak{m}}}$, with associated congruence module isomorphic to
$$\begin{cases} \Lambda_{\mathcal{O}_K}/(A_{\theta,\psi}), & (\theta, \psi) \neq (\omega^{-2}, 1), \\ 0 & \textit{else.} \end{cases}$$

4. Connections to Iwasawa Theory

Ohta uses their results, combined with methods of Kurihara and Harder–Pink, to construct "large" unramified abelian p-extensions of cyclotomic $\mathbb{Z}_p$-extensions of some abelian number fields.

We set up some more notation:

- Let $\mathcal{O}$ be the extension of $\mathbb{Z}_p$ generated by the values of $\theta\psi^{-1}$.
- Let F be the fixed field of the intersection of the kernels of $\theta\omega$ and ψ.
- Let F_∞ be the cyclotomic $\mathbb{Z}_p$ extension of F.
- Let $\Delta := \mathrm{Gal}(F/\mathbb{Q})$ and let $\Gamma := \mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$. We know that $\mathrm{Gal}(F_\infty/\mathbb{Q}) \cong \Delta \times \Gamma$.
- We define
$$F_{\theta\omega^2\psi^{-1}}(T) := g_{\theta\omega^2\psi^{-1}}((1+p)^{-1}(1+T)^{-1} - 1).$$
Then
$$F_{\theta\omega^2\psi^{-1}}((1+p)^s - 1) = L_p(s, \theta\omega^2\psi^{-1}).$$
- We define
$$B_{\theta,\psi}(T) := \left(\prod_{\substack{d \mid N \\ d \nmid \mathrm{cond}(\theta\psi^{-1})}} ([\kappa(d)] - (\theta\omega\psi^{-1})(d)d \right) F_{\theta\omega^2\psi^{-1}}.$$

Ohta uses the Galois representation coming from $(\mathscr{T}^{\mathrm{ord}}_{\mathcal{O}_K})_{\widetilde{\mathfrak{m}}}$ to construct an abelian pro-p extension L/F_∞. Ohta then proves the following Theorem:

Theorem 4.1. [3, Theorem A.1.13] *We have*
$$\mathrm{Fitt}_{\Lambda_{\mathcal{O}}}(\mathrm{Gal}(L/F_\infty)) \subseteq B_{\theta,\psi}\Lambda_{\mathcal{O}},$$
$$\mathrm{char}_{\Lambda_{\mathcal{O}}}(\mathrm{Gal}(L/F_\infty)) \subseteq B_{\theta,\psi}\Lambda_{\mathcal{O}}.$$

References

[1] Haruzo Hida. Galois representations into $\mathrm{GL}_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms. *Invent. Math.*, 85(3):545–613, 1986.

[2] B. Mazur and A. Wiles. Class fields of abelian extensions of **Q**. *Invent. Math.*, 76(2):179–330, 1984.

[3] Masami Ohta. Congruence modules related to Eisenstein series. *Ann. Sci. École Norm. Sup. (4)*, 36(2):225–269, 2003.