Arithmetic of adjoint L-values.

Haruzo Hida*

Department of Mathematics, UCLA,
June 14, 2014

Abstract: We define congruence modules and differential modules of commutative rings. If the starting rings are local complete intersection, the annihilator of the congruence module is the characteristic ideal of differential modules. If applied to Hecke algebras and universal deformation rings, the differential modules are adjoint Selmer groups for modular Galois representation, while the size of congruence modules is given by adjoint L-values.

*Pune (India) lecture No.1 on June 14, 2014. The authors are partially supported by the NSF grants: DMS 0753991.

§1. Set up.

- W: the base ring which is a DVR over $\mathbb{Z}_p$ with finite residue field $\mathbb{F}$ for a prime $p > 2$ (though algebraic extension of $\mathbb{F}_p$ can be allowed as $\mathbb{F}$).
- For a local W-algebra A sharing same residue field $\mathbb{F}$ with W (i.e., $A/\mathfrak{m}_A = \mathbb{F}$), we write CL_A the category of complete local A-algebras R with $R/\mathfrak{m}_R = \mathbb{F}$ for its maximal ideal $\mathfrak{m}_R$. Morphisms of CL_A are local A-algebra homomorphisms. If A is noetherian, the full subcategory CNL_A of CL_A is made up of noetherian local rings.
- Fix $R \in CNL_A$. For a continuous R-module M with continuous R–action, define the module of continuous A–*derivations* by

$$Der_A(R, M) = \Big\{\delta : R \to M \in \mathrm{Hom}_A(R, M)\Big|$$
$$\delta\text{: continuous, } \delta(ab) = a\delta(b) + b\delta(a)\ (a, b \in R)\Big\}.$$

Here the A-linearity of a derivation δ is equivalent to $\delta(A) = 0$. The association $M \mapsto Der_A(R, M)$ is a covariant functor from the category $MOD_{/R}$ of continuous R-modules to modules MOD.

§2. Differentials.

The differential R-module $\Omega_{R/A}$ is defined as follows: The multiplication $a \otimes b \mapsto ab$ induces a A–algebra homomorphism $m : R\widehat{\otimes}_A R \to R$ taking $a \otimes b$ to ab. We put $I = \mathrm{Ker}(m)$, which is an ideal of $R\widehat{\otimes}_A R$. Then we define $\Omega_{R/A} = I/I^2$. It is an easy exercise to check that the map $d : R \to \Omega_{R/A}$ given by $d(a) = a \otimes 1 - 1 \otimes a \mod I^2$ is a continuous A–derivation.

- We have a morphism of functors:

$$\mathrm{Hom}_R(\Omega_{R/A}, ?) \to Der_A(R, ?) : \ \phi \mapsto \phi \circ d.$$

Proposition 1. *The above morphism of two functors $M \mapsto \mathrm{Hom}_R(\Omega_{R/A}, M)$ and $M \mapsto Der_A(R, M)$ is an isomorphism, where M runs over the category of continuous R–modules. In other words, for each A-derivation $\delta : R \to M$, there exists a unique R-linear homomorphism $\phi : \Omega_{R/A} \to M$ such that $\delta = \phi \circ d$.*

Give yourself a proof of this.

§3. Functoriality.

Corollary 1.
Let $\pi : R \twoheadrightarrow C$ be a surjective morphism in CL_W, and write $J = Ker(\pi)$. Then we have the following natural exact sequence:

$$J/J^2 \xrightarrow{\beta^*} \Omega_{R/A}\widehat{\otimes}_R C \longrightarrow \Omega_{C/A} \to 0.$$

Moreover if $A = C$, then $J/J^2 \cong \Omega_{R/A}\widehat{\otimes}_R C$.

We often write $C_1(\pi; C) := \Omega_{R/A}\widehat{\otimes}_R C$ (which is called the differential module of π).

Ay assumption, we have algebra morphism $A \to R \twoheadrightarrow C = R/J$. By the Yoneda's lemma, we only need to prove that

$$0 \to Der_A(C, M) \xrightarrow{\alpha} Der_A(R, M) \xrightarrow{\beta} \mathrm{Hom}_C(J/J^2, M)$$

is exact for all continuous C–modules M. The first α is the pull back map. Thus the injectivity of α is obvious.

§4. Proof.

The map β is defined as follows: For a given A-derivation $D : R \to M$, we regard D as a A-linear map of J into M. Since J kills the C-module M, $D(jj') = jD(j') + j'D(j) = 0$ for $j, j' \in J$. Thus D induces C-linear map: $J/J^2 \to M$. Then for $b \in A$ and $x \in J$, $D(bx) = bD(x)+xD(b) = bD(x)$. Thus D is C-linear, and $\beta(D) = D|_J$.

Now prove the exactness at the mid-term of the second exact sequence. The fact $\beta \circ \alpha = 0$ is obvious. If $\beta(D) = 0$, then D kills J and hence is a derivation well defined on $C = R/J$. This shows that D is in the image of α.

§5. The case $A = C$.

Now suppose that $A = C$. To show injectivity of β^*, we create a surjective C-linear map: $\gamma : \Omega_{R/A} \otimes C \twoheadrightarrow J/J^2$ such that $\gamma \circ \beta^* = \mathrm{id}$.

Let $\pi : R \to C$ be the projection and $\iota : A = C \hookrightarrow R$ be the structure homomorphism giving the A-algebra structure on R. We first look at the map $\delta : R \to J/J^2$ given by $\delta(a) = a - P(a) \mod J^2$ for $P = \iota \circ \pi$. Then

$$\begin{aligned} & a\delta(b) + b\delta(a) - \delta(ab) \\ &\qquad = a(b - P(b)) + b(a - P(a)) - ab - P(ab) \\ &\qquad\qquad = (a - P(a))(b - P(b)) \equiv 0 \mod J^2. \end{aligned}$$

Thus δ is a A-derivation. By the universality of $\Omega_{R/A}$, we have an R-linear map $\phi : \Omega_{R/A} \to J/J^2$ such that $\phi \circ d = \delta$. By definition, $\delta(J)$ generates J/J^2 over R, and hence ϕ is surjective. Since J kills J/J^2, the surjection ϕ factors through $\Omega_{R/A} \otimes_R C$ and induces γ. Note that $\beta(d \otimes 1_C) = d \otimes 1_C|_J$ for the identity 1_C of C; so, $\gamma \circ \beta^* = \mathrm{id}$ as desired.

§6. An algebra structure on $R \oplus M$ and derivation.

For any continuous R-module M, we write $R[M]$ for the R-algebra with square zero ideal M. Thus $R[M] = R \oplus M$ with the multiplication given by

$$(r \oplus x)(r' \oplus x') = rr' \oplus (rx' + r'x).$$

It is easy to see that $R[M] \in CNL_W$, if M is of finite type, and $R[M] \in CL_W$ if M is a p-profinite R-module. By definition,

$$\begin{aligned} &Der_A(R, M) \\ &\quad \cong \left\{ \phi \in \mathrm{Hom}_{A-alg}(R, R[M]) \middle| \phi \mod M = \mathrm{id} \right\}, \end{aligned}$$

where the map is given by $\delta \mapsto (a \mapsto (a \oplus \delta(a))$.

Note that $i : R \to R \widehat{\otimes}_A R$ given by $i(a) = a \otimes 1$ is a section of $m : R \widehat{\otimes}_A R \to R$. We see easily that $R \widehat{\otimes}_A R / I^2 \cong R[\Omega_{R/A}]$ by $x \mapsto m(x) \oplus (x - i(m(x)))$. Note that $d(a) = 1 \otimes a - i(a)$ for $a \in R$.

§7. Congruence modules.

We assume that A is a domain and R is a reduced finite flat A-algebra. Let $\phi : R \twoheadrightarrow A$ be an onto A-algebra homomorphism. Then the total quotient ring $\mathrm{Frac}(R)$ can be decomposed uniquely

$$\mathrm{Frac}(R) = \mathrm{Frac}(\mathrm{Im}(\phi)) \times X$$

as an algebra direct product. Write 1_ϕ for the idempotent of $\mathrm{Frac}(\mathrm{Im}(\phi))$ in $\mathrm{Frac}(R)$. Let $\mathfrak{a} = \mathrm{Ker}(R \to X) = (1_\phi R \cap R)$, $S = \mathrm{Im}(R \to X)$ and $\mathfrak{b} = \mathrm{Ker}(\phi)$. Here the intersection $1_\phi R \cap R$ is taken in $\mathrm{Frac}(R) = \mathrm{Frac}(\mathrm{Im}(\phi)) \times X$. First note that $\mathfrak{a} = R \cap (A \times 0)$ and $\mathfrak{b} = (0 \times X) \cap R$. Put

$$\begin{aligned} C_0(\phi; A) &= (R/\mathfrak{a}) \otimes_{R,\phi} \mathrm{Im}(\phi) \\ &\cong \mathrm{Im}(\phi)/(\phi(\mathfrak{a})) \cong A/\mathfrak{a} \cong R/(\mathfrak{a} \oplus \mathfrak{b}) \cong S/\mathfrak{b}, \end{aligned}$$

which is called the *congruence* module of ϕ but is actually a ring.

§8. Congruence proposition.

Write $K = \text{Frac}(A)$. Fix an algebraic closure $\overline{K}$ of K. Since the spectrum $\text{Spec}(C_0(\phi; A))$ of the congruence ring $C_0(\phi; A)$ is the scheme theoretic intersection of $\text{Spec}(\text{Im}(\phi))$ and $\text{Spec}(R/\mathfrak{a})$ in $\text{Spec}(R)$:

$$\text{Spec}(C_0(\lambda; A)) = \text{Spec}(\text{Im}(\phi)) \cap \text{Spec}(R/\mathfrak{a}),$$

we conclude that

Proposition 2. *Let the notation be as above. Then a prime $\mathfrak{p}$ is in the support of $C_0(\phi; A)$ if and only if there exists an A-algebra homomorphism $\phi' : R \to \overline{K}$ factoring through $R/\mathfrak{a}$ such that $\phi(a) \equiv \phi'(a) \mod \mathfrak{p}$ for all $a \in R$.*

Since ϕ is onto, we see $C_1(\phi; A) = \mathfrak{b}/\mathfrak{b}^2$. We could define $C_n = \mathfrak{b}^n/\mathfrak{b}^{n+1}$. Then $C(\phi; A) = \bigoplus_n C_n(\phi; A)$ is a graded algbera. If $\mathfrak{b}$ is principal, this is a polynomial ring $C_0(\phi; A)[T]$.

§9. Deformation of a character.

Let $F/\mathbb{Q}$ be a number field with integer ring O. We fix a set $\mathcal{P}$ of properties of Galois characters. Fix a continuous character $\overline{\rho}$: Gal$(\overline{\mathbb{Q}}/F) \to \mathbb{F}^\times$ with the property $\mathcal{P}$.

A character ρ : Gal$(\overline{\mathbb{Q}}/\mathbb{Q}) \to A^\times$ for $A \in CL_W$ is called a $\mathcal{P}$-deformation of $\overline{\rho}$ if $(\rho \mod \mathfrak{m}_A) = \overline{\rho}$ and ρ satisfies $\mathcal{P}$.

A couple $(R, \boldsymbol{\rho})$ (universal couple) made of an object R of CL_W and a character $\boldsymbol{\rho}$: Gal$(\overline{\mathbb{Q}}/F) \to R^\times$ satisfying $\mathcal{P}$ is called a *universal couple* for $\overline{\rho}$ if for any $\mathcal{P}$-deformation ρ : Gal$(\overline{\mathbb{Q}}/F) \to A^\times$ of $\overline{\rho}$, we have a unique morphism $\phi_\rho : R \to A$ in CL_W (so it is a local W-algebra homomorphism) such that $\phi_\rho \circ \boldsymbol{\rho} = \rho$. By the universality, if exists, the couple $(R, \boldsymbol{\rho})$ is determined uniquely up to isomorphisms.

§10. Groups algebra is universal.

For a p-profinite abelian group $\mathcal{G}$, consider the group algebra $W[[\mathcal{G}]] = \varprojlim_n W[\mathcal{G}/\mathcal{G}^{p^n}]$. For example, $\Lambda = W[[\Gamma]]$ ($\Gamma = 1 + p\mathbb{Z}_p$) is called the Iwasawa algebra and is isomorphihc to $W[[T]]$ by $1 + p \leftrightarrow t = 1 + T$. Fix an O-ideal $\mathfrak{c}$ prime to p and write $H_{\mathfrak{c}p^n}/F$ for the ray class field modulo $\mathfrak{c}p^n$. Then by Artin symbol, we can identify $\mathrm{Gal}(H_{\mathfrak{c}p^n}/F)$ with the ray class group $Cl_F(\mathfrak{c}p^n)$ (here n can be infinity). Let $C_F(\mathfrak{c}p^\infty)$ for the maximal p-profinite quotient of $Cl_F(\mathfrak{c}p^\infty)$. If $\overline{\rho}$ has prime-to-p conductor equal to $\mathfrak{c}$, we define a deformation ρ to satisfy $\mathcal{P}$ if ρ is unramified outside $\mathfrak{c}p$ and has prime-to-p conductor a factor of $\mathfrak{c}$. Then for the Teichmüller lift ρ_0 of $\overline{\rho}$ and the inclusion $\kappa : C_F(\mathfrak{c}p^\infty) \hookrightarrow W[[C_F(\mathfrak{c}p^\infty)]]$, the universality of the group algebra tells us

Theorem 1. *The couple* $(W[[C_F(\mathfrak{c}p^\infty)]], \rho_0\kappa_{\mathcal{G}})$ *(resp.* $(W[[C_F]], \rho_0\kappa)$ *for* $C_F := C_F(1)$*) is universal among all* $\mathcal{P}$*-deformations (resp. among everywhere unramified deformations).*

§11. Congruence modules for group algebras.

Let H be a finite p-abelian group. We have a canonical algebra homomorphism: $W[H] \to W$ sending $\sigma \in H$ to 1. This homomorphism is called the *augmentation* homomorphism of the group algebra. Write this map $\pi : W[H] \to W$. Then $\mathfrak{b} = \mathrm{Ker}(\pi)$ is generated by $\sigma - 1$ for $\sigma \in H$. Thus

$$\mathfrak{b} = \sum_{\sigma \in H} W[H](\sigma - 1)W[H].$$

We compute the congruence module and the differential module $C_j(\pi, W)$ $(j = 0, 1)$.

Corollary 2. *We have $C_0(\pi; W) \cong W/|H|W$ and $C_1(\pi; W) = H \otimes_{\mathbb{Z}} W$.*

Let $K := \mathrm{Frac}(W)$. Then π gives rise to the algebra direct factor $K\varepsilon \subset K[H]$ for the idempotent $\varepsilon = \frac{1}{|H|} \sum_{\sigma \in H} \sigma$. Thus $\mathfrak{a} = K\varepsilon \cap W[H] = (\sum_{\sigma \in H} \sigma)$ and $\pi(W(H))/\mathfrak{a} = (\varepsilon)/\mathfrak{a} \cong W/|H|W$.

§12. A farfetched proof of $C_1(\pi; W) = H \otimes_{\mathbb{Z}} W$. Consider the functor $\mathcal{F} : CL_W \to SETS$ given by

$$\mathcal{F}(A) = \mathrm{Hom}_{\mathrm{group}}(H, A^{\times}) = \mathrm{Hom}_{W\text{-alg}}(W[H], A).$$

Thus $R := W[H]$ and the character $\boldsymbol{\rho} : H \to W[H]$ (the inclusion: $H \hookrightarrow W[H]$) are universal among characters of H with values in $A \in CL_W$.

Then for any R-module X, consider $R[X] = R \oplus X$ with algebra structure given by $rx = 0$ and $xy = 0$ for all $r \in R$ and $x, y \in X$.

Define $\Phi(X) = \{\rho \in \mathcal{F}(R[X]) | \rho \mod X = \boldsymbol{\rho}\}$. Write $\rho(\sigma) = \boldsymbol{\rho}(\sigma) \oplus u'_\rho(\sigma)$ for $u'_\rho : H \to X$. Since

$$\begin{aligned}\boldsymbol{\rho}(\sigma\tau) \oplus u'_\rho(\sigma\tau) &= \rho(\sigma\tau) \\ &= (\boldsymbol{\rho}(\sigma) \oplus u'_\rho(\sigma))(\boldsymbol{\rho}(\tau) \oplus u'_\rho(\tau)) \\ &= \boldsymbol{\rho}(\sigma\tau) \oplus (u'_\rho(\sigma)\boldsymbol{\rho}(\tau) + \boldsymbol{\rho}(\sigma)u'_\rho(\tau)),\end{aligned}$$

we have $u'_\rho(\sigma\tau) = u'_\rho(\sigma)\boldsymbol{\rho}(\tau) + \boldsymbol{\rho}(\sigma)u'_\rho(\tau)$, and thus $u_\rho := \boldsymbol{\rho}^{-1}u'_\rho : H \to X$ is a homomorphism from H into X. This shows

$$\mathrm{Hom}(H, X) = \Phi(X).$$

§13. Proof continues.

Any W-algebra homomorphism $\xi : R \to R[X]$ with $\xi \mod X = \mathrm{id}_R$ can be aritten as $\xi = \mathrm{id}_R \oplus d_\xi$ with $d_\xi : R \to X$. Since $(r \oplus x)(r' \oplus x') = rr' \oplus rx' + r'x$ for $r, r' \in R$ and $x.x' \in X$, we have $d_\xi(rr') = rd_\xi(r') + r'd_\xi(r)$; so, $d_\xi \in Der_W(R, X)$. By universality of $(R, \boldsymbol{\rho})$, we have

$$\begin{aligned}\Phi(X) &\cong \{\xi \in \mathrm{Hom}_{W\text{-alg}}(R, R[X]) | \xi \mod X = \mathrm{id}\} \\ &= Der_W(R, X) = \mathrm{Hom}_R(\Omega_{R/W}, X).\end{aligned}$$

Thus taking $X = K/W$, we have

$$\begin{aligned}\mathrm{Hom}_W(H \otimes_{\mathbb{Z}} W, K/W) &= \mathrm{Hom}(H, K/W) \\ &= \mathrm{Hom}_R(\Omega_{R/W}, K/W) \\ &= \mathrm{Hom}_W(\Omega_{R/W} \otimes_{R,\pi} W, K/W).\end{aligned}$$

By taking Pontryagin dual back, we have

$$H \cong \Omega_{R/W} \otimes_{R,\pi} W = C_1(\pi; W).$$

§**14. Class number formula.** Let $\mathrm{Ind}_F^{\mathbb{Q}}\mathrm{id} = \mathrm{id} \oplus \chi$ and $H = C_F$. Then for Ω_F given basically by the regulator and some power of $(2\pi i)$,

$$|L(1,\chi)/\Omega_F|_p = \Big||C_F|\Big|_p.$$

We can identify $C_F^\vee = \mathrm{Hom}(C_F, \mathbb{Q}_p/\mathbb{Z}_p)$ with the Selmer group of χ given by

$$\mathrm{Sel}_{\mathbb{Q}}(\chi) := \mathrm{Ker}(H^1(\mathbb{Q}, V(\chi)^*) \to \prod_l H^1(I_l, V(\chi)^*))$$

for the inertia group $I_l \subset \mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$.

Theorem 2 (Class number formula)**.** *Assume that $F/\mathbb{Q}$ is a Galois extension and $p \nmid [F : \mathbb{Q}]$. For the augmentation homomorphism $\pi : W[C_F] \to W$, we have, for $r(W) = \mathrm{rank}_{\mathbb{Z}_p} W$,*

$$\left|\frac{L(1,\chi)}{\Omega_F}\right|_p^{r(W)} = |C_1(\pi; W)|^{-1}$$
$$= |C_0(\pi; W)|^{-1} = \Big||\mathrm{Sel}_{\mathbb{Q}}(\chi)|\Big|_p^{r(W)}$$

and $C_1(\pi; W) = C_F \otimes W$ and $C_0(\pi; W) = W/|C_F|W$.