Davenport - Hasse の持ち上げ定理とその行列類似.

金井さん（新潟大）

§1

$p^r \equiv 1 \mod e$

$$
\begin{tikzcd}
 & \boxed{\text{Gaussian periods } \eta_r(i)} \arrow[rr, <->, "\mathcal{F}"] \arrow[d, squiggly] & & \boxed{\text{Gauss sums } G_r^*(\chi^i)} \arrow[d, squiggly] & \mathbb{F}_{p^r} \rightsquigarrow \mathbb{F}_{p^{rn}} \arrow[l] \\
\text{Today} \arrow[r] & \boxed{\text{Multi. matrix } C_r} \arrow[rr, <->] \arrow[dr, <->] & & \boxed{\text{Jacobi sums } J_r^*(\chi^i,\chi^j)} \arrow[dl, <->] & \\
 & & \boxed{\text{Diophantine sys. w.r.t. } p^r} & &
\end{tikzcd}
$$

$$J_r^*(\chi^i,\chi^j) = \frac{G_r^*(\chi^i)\,G_r^*(\chi^j)}{G_r^*(\chi^{i+j})}$$

▨ Gauss sums & Jacobi sums.

- reciprocity law [Gauss]
- $\mathbb{F}_{p^r}$ - rat'l point of Fermat variety [Weil]
  $X_1^m + \cdots + X_d^m = 0$.

Using DH thm. for Jacobisums.

Today

- DH thm. and its matrix analogue.

Notation

$e \geq 2$, $p^r \equiv 1 \pmod e$ $\quad p^r = ef + 1$

$\mathbb{F}_{p^n}^\times = \langle \gamma \rangle$

$\zeta_n := e^{\frac{2\pi i}{n}}$

$$\chi : \mathbb{F}_{p^r} \longrightarrow \mathbb{C} \quad : \text{Character of order } e$$
$$\gamma \longmapsto \zeta_e$$
$$0 \longmapsto 0$$

K : a field with $\mathrm{char}(K) = 0$

Definition

$$\mathrm{Tr}: \mathbb{F}_{p^r} \longrightarrow \mathbb{F}_p$$
$$\alpha \longmapsto \sum_{j=0}^{r-1} \alpha^{p^j}$$

$\eta_r(i) := \sum_{j=0}^{f-1} \zeta_p^{\mathrm{Tr}(\gamma^{ej+i})} \in \mathbb{Q}(\zeta_p)$: Gaussian periods of degree e for $\mathbb{F}_{p^r}$

$G_r^*(\chi^i) := \sum_{\alpha \in \mathbb{F}_{p^r}^\times} \chi^i(\alpha) \zeta_p^{\mathrm{Tr}(\alpha)} \in \mathbb{Q}(\zeta_e, \zeta_p)$: Gaussian sums

$J_r^*(i,j) := J_r^*(\chi^i, \chi^j) := \sum_{1 \neq \alpha \in \mathbb{F}_{p^r}^\times} \chi^i(\alpha)\chi^j(1-\alpha) \in \mathbb{Q}(\zeta_e)$: Jacobi sums

Facts

- $J_r^*(i,j) = \dfrac{G_r^*(\chi^i)\, G_r^*(\chi^j)}{G_r^*(\chi^{i+j})} \qquad (i+j \neq 0)$

- $|G_r^*(\chi^i)| = \begin{cases} \sqrt{p^r} & (i \neq 0) \\ 0 & (i = 0) \end{cases}$

$\rightsquigarrow \ |J_r^*(i,j)| = \sqrt{p^r} \qquad (i, j, \ i+j \neq 0)$

Theorem [Davenport - Hasse '35]

- $G_{nr}^*(\chi'^i) = (-1)^{n-1} G_r^*(\chi^i)^n$

- $J_{nr}^*(\chi'^i, \chi'^j) = (-1)^{n-1} J_r^*(\chi^i, \chi^j)^n$,

where

$$\chi' : \mathbb{F}_{p^{nr}} \xrightarrow{N_r} \mathbb{F}_{p^r} \xrightarrow{\chi} \mathbb{C}, \qquad i+j \neq 0,\ i \neq 0,\ j \neq 0.$$
$$\alpha \longmapsto \prod_{j=0}^{r-1} \alpha^{p^j}$$

$$\eta_r : \mathbb{Z}/e\mathbb{Z} \longrightarrow \mathbb{C}$$
$$\bar{i} \longmapsto \eta_r(i)$$

$$G_r^* : \widehat{\mathbb{Z}/e\mathbb{Z}} \longrightarrow \mathbb{C}$$
$$\chi^i \longmapsto G_r^*(\chi^i)$$

G : fin. ab. group

- $\mathcal{F} : \mathcal{L}^2(G) \longrightarrow \mathcal{L}^2(\hat{G})$
  $f \longmapsto \hat{f} = \sum_{x \in G} f(x)\overline{\chi(x)}$

  Vect. sp.
  all $\mathbb{C}$-valued funct. on G

  Then $\widehat{f*g} = \hat{f} \cdot \hat{g}$ (convolution)

  $f*g\,(i) = \sum_{k_1+k_2=i} f(k_1)\,g(k_2)$

Facts

- $(\mathcal{F}(\eta_r))(\chi^i) = G_r^*(\chi^{-i})$
- $(\mathcal{F}^{-1}(G_r^*))(i) = \eta_r(-i)$

Theorem [Davenport - Hasse : dual form]

$$\eta_{nr}(i) = (-1)^{n-1}\,\eta_r^{(n)}(i)$$ n回のconvolution

Definition

- $Cyc_r(i,j) := \#\left\{ (r_1, r_2) \;\middle|\; \begin{matrix} 0 \le r_1, r_2 \le f-1 \\ 1 + \gamma^{er_1+i} \equiv \gamma^{er_2+j} \bmod p^r \end{matrix} \right\}$: cyclotomic numbers of order e for $\mathbb{F}_{p^r}$

- $C_r := \left[Cyc_r(i,j)\;\; D_i f \right]_{0 \le i,j \le e-1}$, where

  $D_i := \delta_{0,i}$ (resp. $\delta_{\frac{e}{2},i}$) if f : even (resp. f : odd) : multiplication matrix of $\eta_r(i)$'s

Facts

- $(-1)^{fa} \sum_{i=0}^{e-1} \sum_{j=0}^{e-1} \mathrm{Cyc}_r(i,j) \zeta_e^{ai+bj} = J_r^*(a,b)$.

- $\eta_r(i)\eta_r(i+l) = \sum_{m=0}^{e-1} C_r[l,m]\,\eta_r(i+m)$

Remark

C_r has eigenvalues $\eta_r(i)$

$\rightsquigarrow P_{e,r}(X) := \prod_{i=0}^{e-1} (X - \eta_r(i)) \in \mathbb{Z}[X]$

Example

$P_{3,r}(X) = X^3 - 3p^r X - p^r c$

$$\begin{cases} 4p^r = c^2 + 27d^2 \\ c \equiv 1 \mod 3 \quad c \nmid d \end{cases}$$

Main theorem [Hoshi - K' 22]

$C_{nr} = (-1)^{n-1} C_r^{\boxed{(n)}}$ §2, 3 で def.

§2

Ref

- Multiplication matrices, Thaine '04.

K/k : cyclic ext. $\xrightarrow{\text{+ some cond.}}$ $A \overset{[a_{ij}]}{=}$: multiplication matrix for θ_i's is defined by

$(K = k(\theta_i)_{i=0,1,\dots,e-1})$

$\uparrow$ $\theta_0, \dots, \theta_{e-1}$ is basis of K/k

$$\theta_0 \theta_i = \sum_{j=0}^{e-1} a_{ij} \theta_j$$

Theorem [Thaine '04]

$k(\theta_i)/k$: cyclic ext. degree e $\overset{\text{iff}}{\Longleftrightarrow}$

① $a_{i,j} = a_{-i,\, j-i}$

② $A(K^{-i}AK^i) = (K^{-i}AK^i)A \quad (0 \le i \le e-1)$,

where $K = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 1 & & & 0 \end{pmatrix}$.

③ $P(X) = \prod (X - \theta_i)$ is irreducible $/ k$

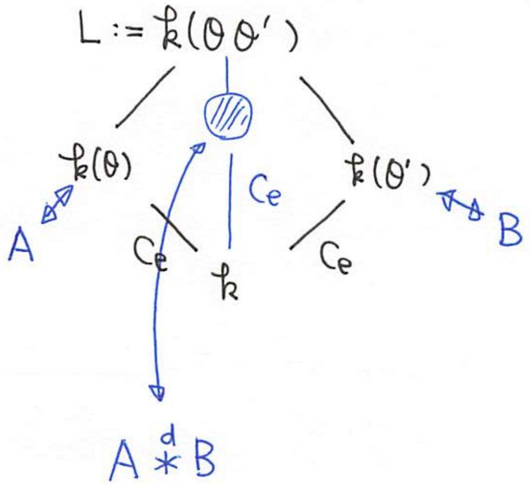
Remark

C_r satisfies ①, ② and

- $\displaystyle\sum_{k=0}^{e-1} a_{ik} = f - p^r D_i$
- $\displaystyle\sum_{k=0}^{e-1} a_{k,j} = \begin{cases} -1 & (j=0) \\ 0 & (j \neq 0) \end{cases}$

$\vdots$

■ Thaine's observation.



$Gal(L/k) \simeq C_e \times C_e \geq H$: e次部分群.

§3

Definition

For $A, B \in Mat_e(K)$, $d \in \mathbb{Z}/e\mathbb{Z} \setminus \{0\}$, we define

$$A \overset{d}{*} B := \left[\sum_{s=0}^{e-1} \sum_{t=0}^{e-1} A[s,t]\, B[ds+i,\, dt+j] \right]_{0 \leq i, j \leq e-1}.$$

Remark

" $\overset{d}{*}$ " is distributive.

In general,

- $A \overset{d}{*} B \neq B \overset{d}{*} A$
- $A \overset{d}{*} (B \overset{d_2}{*} C) \neq (A \overset{d_1}{*} B) \overset{d_2}{*} C$.

Proposition 1 [Hoshi - K]

For $d \in (\mathbb{Z}/e\mathbb{Z})^\times$,

$$B \overset{d}{*} A\,[i, \delta] = A \overset{d^{-1}}{*} B\,[-d^{-1}i, -d^{-1}\delta].$$

In particular, $A \overset{-1}{*} B = B \overset{-1}{*} A$.

Proposition 2 [Hoshi - K]

For $d_1 \in \mathbb{Z}/e\mathbb{Z} \setminus \{0\}$, $d_2 \in (\mathbb{Z}/e\mathbb{Z})^\times$

$$A \overset{d_1}{*} (B \overset{d_2}{*} C) = (A \overset{-d_2^{-1}d_1}{*} B) \overset{d_2}{*} C$$

In particular

$$A \overset{d_1}{*} (B \overset{-1}{*} C) = (A \overset{d_1}{*} B) \overset{-1}{*} C.$$

$\rightsquigarrow$ We can define $A^{(n)}$ as $A^{(n)} := A \overset{-1}{*} A \overset{-1}{*} \cdots \overset{-1}{*} A$.

Definition

For $f, g \in \mathcal{L}^2(\mathbb{Z}/e\mathbb{Z})$, $d \in \mathbb{Z}/e\mathbb{Z} \setminus \{0\}$, we define

$$f \overset{d}{*} g\,(i) = \sum_{s=0}^{e-1} f(s)g(ds+i).$$

Remark

$d = -1 \Rightarrow \overset{-1}{*} = *$ (usual convolution)

- $\overset{-1}{*}$ is commutative & associative

$\rightsquigarrow$ we can define $f^{(n)}(i) := (\underbrace{f \overset{-1}{*} \cdots \overset{-1}{*} f}_{})(i)$.

Corollary

$$\eta_r^{(n)}(i)\,\eta_i^{(n)}(i+l) = \sum_{m=0}^{e-1} C_r^{(n)}[l, m]\,\eta_r^{(n)}(i+m). \quad \cdots\cdots ✪$$

§4

Main result

$$C_{nr} = (-1)^{n-1} C_r^{(n)}.$$

(proof)

By DH-thm dual form & ⊛, $(-1)^{n-1} C_{nr}$ and $C_r^{(n)}$ have the same eigenvalues $\eta_r^{(n)}(i)$ and eigenvecor $T_i := \begin{pmatrix} \eta_r^{(n)}(i) \\ \vdots \\ \eta_r^{(n)}(i-1) \end{pmatrix}$

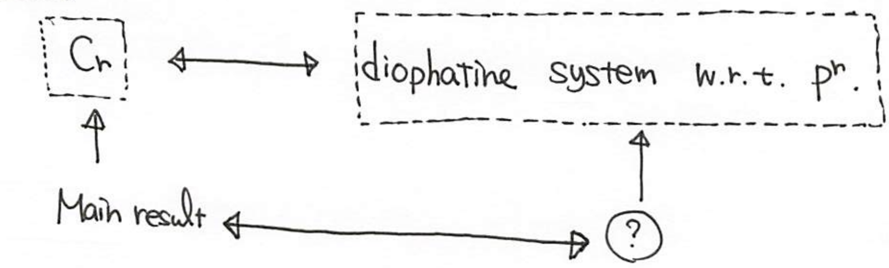
Then $P := (T_0, \cdots, T_{e-1})$ is invertible by [Baumert-Williams-Word '82].

$$\rightsquigarrow \quad P^{-1}(-1)^{n-1} C_{nr} P = \begin{pmatrix} \eta_r^{(n)}(0) & & \\ & \ddots & \\ & & \eta_r^{(n)}(e-1) \end{pmatrix} = P^{-1} C_r^{(n)} P.$$

$$\because \quad C_{nr} = (-1)^{n-1} C_r^{(n)}$$

□

§5



e.g. $e = 3$.

$$C_r = C_r(p, c, d) = \begin{pmatrix} A-f & B-f & C-f \\ B & C & D \\ C & D & B \end{pmatrix}$$

$$A = \frac{1}{9}(p^r + c + 8), \qquad C = \frac{1}{18}(2p^r - c - 9d - 4)$$

$$B = \frac{1}{18}(2p^r - c + 9d - 4), \qquad D = \frac{1}{9}(p^r + c + 1),$$

where $c, d \in \mathbb{Z}$ given as the integral solution of

$$\begin{cases} 4p^r = c^2 + 27d^2 \\ c \equiv 1 \bmod 3 \quad c \nmid d \end{cases}$$

By Main thm

$$C_{nr} = (-1)^{n-1} C_r(p, c, d)^{(n)}$$

$$= C_r(p^n, c^{(n)}, d^{(n)}),$$

where $c^{(n)}, d^{(n)}$ can be obtained as a form of degree n in c, d.

(e.g. $n = 2$

$$c^{(2)} = \frac{1}{2}(-c^2 + 27d^2), \quad d^{(2)} = -cd.$$)

$$p^{nr} = \left(\frac{c^2 + 27d^2}{4} \right)^n = \frac{(c^{(n)})^2 + 27(d^{(n)})^2}{4}$$

$\rightsquigarrow$ We can construct multiplicative quad. forms $q(X)$ on alg. var V.

$\overset{\text{def}}{\Longleftrightarrow}$ [Hoshi'05] $V \subseteq \mathbb{A}^n(K)$: alg. var $/K$.

$\exists \varphi : K^n \times K^n \longrightarrow K^n$ such that

- $\varphi(V \times V) \subset V$
- $q(X)\, q(Y) = q(\varphi(X, Y))$.

Remark [Hurwitz '98]

$\mathrm{Char}(K) \neq 2$.

$q(X) = \sum_{i=1}^{n} x_i^2$ is multiplicative $\mathbb{A}^n(K) \Rightarrow n = 1, 2, 4, 8$

Theorem [Hashi - K '22 ?]

Assume that

$$e = \ell \quad : \text{odd prime}$$

$$\mathrm{Gal}(K(\zeta_\ell)/K) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times$$

$V \subset \mathbb{A}_K^\ell$: alg. var $/K$ defined by

$$V : \quad f_n(X) = 0 \quad (n = 0, 1, \cdots, \tfrac{\ell-1}{2} - 1),$$

where

$$f_n(X) := \sum_{i=0}^{\ell-1} x_i x_{i+n} - \sum_{i=0}^{\ell-1} x_i x_{i+(n+1)}$$

Then $q(X) := f_0(X)$ is multiplicative on V. for some φ.

Question

For given $q(X)$, is there a V : alg. var $/K$ for which $q(X)$ is multiplicative ?

(V と φ を与えよ.)