数理解析研究所講究録
第617巻 1987年 193-205

Non congruence subgroup の Hecke 作用素

東大理 寺杣友秀.
(Tomohide Terasoma)

§1 Reimann 面の分岐の様子.

E を. E: $y^2 = x(x-1)(x-p)$ (p は odd, $\in \mathbb{N}$, $p \geq 5$) で定義される elliptic curve とする。

Lemma 1 E は $\mathbb{P}^1$ 上の $\{0, 1, \infty\}$ 以外で不分岐な covering として表わされる。

Proof これは Belyi によってさらに一般化された形で知られているが. ここではその具体的な形の1つをあげてみよう。$E \to \mathbb{P}^1$ を (x, y) を x に送る morphism と考えると. これは. $X \supset \{0, 1, \infty, p\}$ 以外で不分岐な covering であるから. $f: X = \mathbb{P}^1 \longrightarrow Y = \mathbb{P}^1$ なる map で. $f^{-1}(\{0, 1, \infty\}) \supset \{0, 1, \infty, p\}$ であり. f は $\{0, 1, \infty\} \subset Y$ 以外で不分岐なるものを構成すればよい。それには

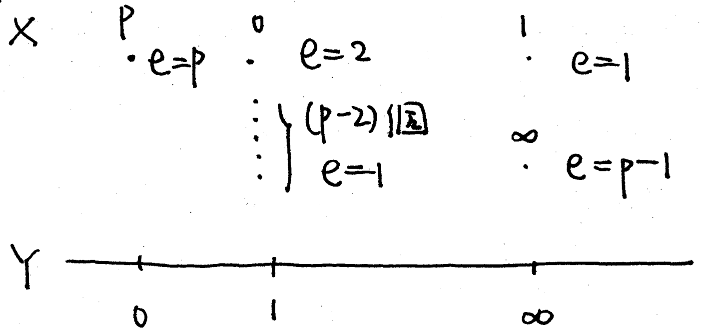
$$\begin{array}{ccc} \mathbb{P}^1 & \longrightarrow & \mathbb{P}^1 \\ \uplus & & \uplus \\ x & \longmapsto & f(x) \end{array}, \quad f(x) = \frac{1}{p^p}(x-1)^{-1}(x-p)^p$$

とすれば十分である。これから合わせて. $E \longrightarrow X \longrightarrow Y$ によってもとめる covering を得る。 Q.E.D.

さて次にE/YのGalois closureを求める。bを$Y^0=Y-\{0,1,\infty\}$の点とすると、$E_b:=b$におけるEのfiberには、$\pi_1(Y^0,b)$が作用する。それを、$\pi_1(Y^0,b)\longrightarrow \mathrm{Aut}(E_b)$として、このKernelに対応する$Y$のcoveringが求めるGalois closureである。$X_b:=b$におけるXのfiberとする。この時、$\# X_b=p$である。

<u>Lemma 2</u>　$\pi_1(Y^0,b)\longrightarrow \mathrm{Aut}(X_b)$は全射である。すなわち$X/Y$のGalois closureの$Y$上のGalois群は、$p$次対称群$\mathfrak{S}_p$である。

<u>Proof</u>　分岐点の様子は下の図の様になる。



ここでeは、そこでの分岐指数を表わす。これから上のmapの像は、$\mathbb{Z}/p$, $\mathbb{Z}/2$, $\mathbb{Z}/(p-1)$を含む。対称群の性質より、これは、必ず$\mathfrak{S}_p$を生成する。　Q.E.D.

さて次にいくつかの群を定義する。

$H_2 = \{ f \in Aut(\{-p, \cdots, -1, 1, \cdots, p\}) \mid f(-x) = -f(x) \ (\forall x \in \{\pm p, \cdots p\}) \}$

$H_1 = \{ f \in H_2 \mid f(1) = 1 \}$

また $H_2 \xrightarrow{p} \mathfrak{S}_p = Aut(\{1, \cdots, p\})$ を $f \longmapsto f$ (modulo sign) で定義し、そのKernelをVとおく。この時

$$0 \longrightarrow V \longrightarrow H_2 \xrightarrow{p} \mathfrak{S}_p \longrightarrow 0 \quad (\text{exact})$$

となる。さてEのY上のGalois closureをM，XのY上のGalois closureをLと書く。この時Reimann面のcoveringの関係は、図の様になる。

$$\begin{tikzcd}
L \arrow[d] & L \cdot E \arrow[l] \arrow[d] & M \arrow[l] \\
X \arrow[d] & E \arrow[l] & \\
Y. & &
\end{tikzcd}$$

<u>Theorem 3</u>　上の図に対して、群の包含関係は下の図の様になる。

$$\begin{tikzcd}
V \arrow[d] & H_1 \cap V \arrow[l] \arrow[d] & 1 \arrow[l] \\
p^{-1}(\mathfrak{S}_{p-1}) \arrow[d] & H_1 \arrow[l] & \\
H_2. & &
\end{tikzcd}$$

Proof 証明は難しくないが. 省略する。

§2 群論的解釈.

$Y-\{0,1,\infty\}\cong\mathfrak{H}/\Gamma(2)$ である。ここで. 上半空間 $\mathfrak{H}=\{z\in\mathbb{C}\mid \mathrm{Im}\,z>0\}$ に $\Gamma(2)=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL(2,\mathbb{Z})\;\middle|\;\begin{pmatrix}a&b\\c&d\end{pmatrix}\equiv 1\ (\mathrm{mod}\,2)\right\}$ は. 1次分数変換で作用するものとする。$\Gamma(2)/\pm1$ は. $\mathfrak{H}$ に fixed-point free に作用するので. $\pi_1(Y-\{0,1,\infty\},b)\cong\Gamma(2)/\pm1$ である。$Y\cong\mathfrak{H}/\Gamma(2)$ を. $Y\ni 0$ と 0-cusp, $Y\ni\infty$ と $i\infty$ cusp, が対応する様にとれば. $A=\begin{pmatrix}1&2\\0&1\end{pmatrix}$ の $\mathrm{Aut}(X_b)$ における image が. $(2,\cdots,p)$ と conjugate, $B=\begin{pmatrix}1&0\\2&1\end{pmatrix}$ の image が $(1,\cdots,p)$ と conjugate となる。他方. $AB^{-1}=\begin{pmatrix}-3&2\\-2&1\end{pmatrix}\in\{1\text{-cusp の stabilizer}\}$ なので AB^{-1} は $(1,2)$ と conjugate であるとしてよい。以上の事から適当な番号のつけかえ(X_b の)によって

$$\begin{array}{ccc}
\pi_1(Y-\{0,1,\infty\}) & \longrightarrow & \mathrm{Aut}(X_b)\\
\downarrow\cong & & \downarrow\cong\\
\Gamma(2)/\pm1 & \xrightarrow{\ \varphi\ } & \mathfrak{S}_p
\end{array}$$

$$\alpha=A^{-1}=\begin{pmatrix}1&-2\\0&1\end{pmatrix}\longmapsto(2,\cdots,p)^{-1}$$

$$\beta=AB^{-1}=\begin{pmatrix}-3&2\\-2&1\end{pmatrix}\longmapsto(1,2)$$

$$\gamma=B=\begin{pmatrix}1&0\\2&1\end{pmatrix}\longmapsto(1,\cdots,p)$$

なる様に対応しているとしてよい。

Proposition 1 適当に. $E_\ell=\{\pm1,\cdots,\pm p\}$ と同一視すれば.

i) $E_\ell \ni \pm i \longmapsto i\in X_\ell$ となり.

ii) $\pi_1(Y-\{0,1,\infty\}) \xrightarrow{\varphi} \mathrm{Aut}(E_\ell)$ が.

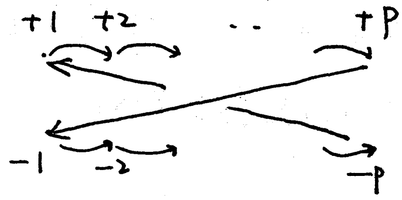
$$\alpha^{-1} \longmapsto (2,\cdots,p)^{\sim}$$

$$\beta \longmapsto (1,2)^{\sim}$$

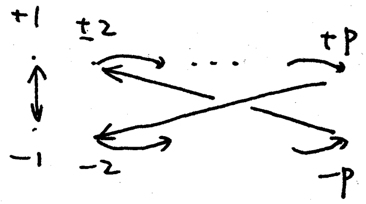
$$\gamma \longmapsto (1,\cdots,p)^{\sim}$$

なる map で与えるとしてよい。ここで. $(1,\cdots,p)^{\sim}$, $(1,2)^{\sim}$, $(1,\cdots,p)^{\sim}$ は.

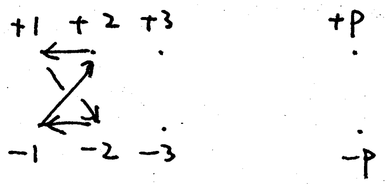
$(1,\cdots,p)^{\sim}$:



$(2,\cdots,p)^{\sim}$



$(1.2)^{\sim}$



なる置換である。

Proof まず $(1,\cdots,p)^{\sim}$ は E_ℓ に作用する。これは. X_ℓ でみると. $(1,\cdots,p)$ であり. また. $\{\pm1,\cdots,\pm p\}$ に transitive に作用

する。$(2,\cdots,p)^{\sim}$ は x_ℓ で見ると. $(2,\cdots,p)$ で. $\{\pm 2,\cdots,\pm p\}$ に transitive に作用する。また. $(1,\cdots,p)^{\sim}(2,\cdots,p)^{\sim -1}$ は. $\{\pm 1,\pm 2\}$ に transitive に作用し. $\{\pm 3,\cdots,\pm p\}$ に trivial に作用するので. これらの事を考え合わせて. 図の様な置換をひきおこしてると得ない。 Q.E.D.

± 2. 前§の記号での $\pi_1(Y-\{0,1,\infty\})\cong\Gamma(2)/\pm 1 \twoheadrightarrow H_2$ なる map 及び ℓ を奇素数とした時の自然な map $\Gamma(2)/\pm 1 \twoheadrightarrow PSL(2,\mathbb{F}_\ell)$ を合わせ. $f:\pi_1(Y-\{0,1,\infty\})\longrightarrow H_2\times PSL(2,\mathbb{F}_\ell)$ なる map を得る。以後 p は5以上の自然数とする。

<u>Proposition 2</u> $\ell>p$, $(\ell,p-1)=1$ のもとで. f は全射である。

<u>Proof</u> 各 factor へは surjective へ行くので. $\mathrm{Im}f\cap H_2\times\{e\}=H_2\times\{e\}$ を言えば十分である。まず $\mathrm{Im}f\cap H_2\times\{e\}\xrightarrow{\pi}\mathfrak{S}_n$ が全射であることを言おう。今. $A=\begin{pmatrix}1&2\\0&1\end{pmatrix}$ は π によって. $(2,\cdots,p)$ へ行くので. $A^\ell=\begin{pmatrix}1&2\ell\\0&1\end{pmatrix}$ は. $(2,\cdots,p)^\ell$ へ行く これは. order $(p-1)$ の元である。$B=\begin{pmatrix}1&0\\ &1\end{pmatrix}$ は π によって. $(1,\cdots,p)$ へ行くので. B^ℓ の π による image の order は. p である。また. $(AB^{-1})^\ell\equiv 1\ (\ell)$ であり. π による image は. order 2

であるので．$\mathrm{Im} f \cap H_2 \times \{e\} \longrightarrow \mathfrak{S}_p$ の image は．order p, $p-1$, 2 の元を含み全射となる。また． $A^{(p-1)\ell}$．$B^{p\ell}$ の imag は．± 1 のみを交換し．他は fix するので．$\mathrm{Im} f \cap H_2 \times \{e\} = H_2 \times \{e\}$ を得る。

Q.E.D.

さて以下 $\Gamma(2)/\pm 1$ を略して $\tilde{\Gamma}(2)$ と書く。今 $\tilde{\Gamma}(2) \xrightarrow{\varphi} H_2$ とおき、$\varphi^{-1}(H_1) = G$ とおく。 Main theorem は次の Theorem である。

<u>Theorem 3</u> ℓ を奇素数で $\ell > p$，$\ell \equiv 1\ (p)$ ，$\ell \not\equiv 1\ (p-1)$ ，$(\ell, p-1) = 1$ とする。この時．

$$\# \left(G \Big/ \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} G \begin{pmatrix} \ell^{-1} & 0 \\ 0 & 1 \end{pmatrix} \cap G \right) = 2p(\ell+1)$$

である。

<u>Remark</u> G がもし congruence subgroup なら．ほとんどすべての ℓ について $\# \left(G \Big/ \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} G \begin{pmatrix} \ell^{-1} & 0 \\ 0 & 1 \end{pmatrix} \cap G \right) = \ell+1$ なので．G は．congruence subgroup でない事がわかる。

<u>Proof</u> $\# \left(G \Big/ \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \tilde{\Gamma}(2) \begin{pmatrix} \ell^{-1} & 0 \\ 0 & 1 \end{pmatrix} \cap G \right) = \ell+1$ と．

$$\# \left(\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \tilde{\Gamma}(2) \begin{pmatrix} \ell^{-1} & 0 \\ 0 & 1 \end{pmatrix} \cap G \Big/ \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} G \begin{pmatrix} \ell^{-1} & 0 \\ 0 & 1 \end{pmatrix} \cap G \right) = 2p$$

を示せばよい。自然な map

$$G/\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}\tilde{\Gamma}(2)\begin{pmatrix} \ell^{-1} & 0 \\ 0 & 1 \end{pmatrix}\cap G \hookrightarrow \tilde{\Gamma}(2)/\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}\tilde{\Gamma}(2)\begin{pmatrix} \ell^{-1} & 0 \\ 0 & 1 \end{pmatrix}\cap \tilde{\Gamma}(2)$$

が全射となる事は．Propositionの全射性の結論である。ゆえにあとは．次のPropositionを示す事に帰着される。

<u>Proposition 4</u> 記号．仮定は定理のものとする。自然なmap

$$\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}\tilde{\Gamma}(2)\begin{pmatrix} \ell^{-1} & 0 \\ 0 & 1 \end{pmatrix}\cap G \Big/ \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}G\begin{pmatrix} \ell^{-1} & 0 \\ 0 & 1 \end{pmatrix}\cap G$$
$$\longrightarrow \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}\tilde{\Gamma}(2)\begin{pmatrix} \ell^{-1} & 0 \\ 0 & 1 \end{pmatrix}\Big/\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}G\begin{pmatrix} \ell^{-1} & 0 \\ 0 & 1 \end{pmatrix} \cong H_2/H_1$$

は全射である。

<u>Proof</u>の概略．　ψを．$\psi(A^\ell)=A$，$\psi(B)=B^\ell$（ここで．$A=\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$，$B=\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$）として定義する。$\tilde{\Gamma}(2)\xrightarrow{\overline{\varphi}}H_2/H_1\cong\{\pm1,\cdots\pm p\}$とした時．任意の$j\in\{\pm1,\cdots\pm p\}$について次の様な性質を満たすword $F(A,B)$が存在すればよい。

$$\begin{cases} \overline{\varphi}(F(A^\ell,B))=1 \\ \overline{\varphi}(\psi(F(A,B^\ell))=j \end{cases}$$

この様なFを実際に構成することにより．このProofを得る。この部分については．組み合わせ論的な考察を必要とし．一連の結果の本質的な部分であるが．かなり長い考察を必要とするので．証明を省きます。くわしくは．あとに出る論文を見て下さい。　Q.E.D.

§3 Correspondence に関する結果.

ここで下の correspondence を考える。(l を素数とする。)

$$
\begin{tikzcd}
& \mathfrak{h}/\begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix} G \begin{pmatrix} l^{-1} & 0 \\ 0 & 1 \end{pmatrix} \cap G \arrow[dl, "p"'] \arrow[dr, "q"] & \\
\mathfrak{h}/G & & \mathfrak{h}/G.
\end{tikzcd}
$$

§2 の main theorem より. $l>p$, $l\equiv 1\ (p)$, $l\not\equiv 1\ (p-1)$, $(l.p-1)=1$ の時 $\deg p = \deg q = 2p(l+1)$ であることがわかっていた。今 $\mathfrak{h}/G$ の compact化 $(\mathfrak{h}/G)^*$ は $E: y^2 = x(x-1)(x-p)$ と同型であるから. この correspondence q_*p^* は. $H^1(E.\mathbb{Q})$ の自己準同型をひきおこす。これを $T(l)$ と書く。今. 自然な map $\mathfrak{h}/G \to \mathfrak{h}/\Gamma(2)$ から induce される map を τ. とする。$\mathfrak{h}/\Gamma(2)$ 上には上と同様

$$
\begin{tikzcd}
& \mathfrak{h}/\begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix} \Gamma(2) \begin{pmatrix} l^{-1} & 0 \\ 0 & 1 \end{pmatrix} \cap \Gamma(2) \arrow[dl, "\bar{p}"'] \arrow[dr, "\bar{q}"] & \\
\mathfrak{h}/\Gamma(2) & & \mathfrak{h}/\Gamma(2)
\end{tikzcd}
$$

なる map を得るが. このグラフを考える。

$$
\Gamma_{\bar{p},\bar{q}} = \mathfrak{h}/\begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix} \Gamma(2) \begin{pmatrix} l^{-1} & 0 \\ 0 & 1 \end{pmatrix} \cap \Gamma(2) \xrightarrow{(\bar{p},\bar{q})} \mathfrak{h}/\Gamma(2) \times \mathfrak{h}/\Gamma(2)
$$

さらに (p,q) のグラフを $\Gamma_{p,q}$ とする。

$$
\Gamma_{p.q} = \mathfrak{h}/\begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix} G \begin{pmatrix} l^{-1} & 0 \\ 0 & 1 \end{pmatrix} \cap G \xrightarrow{(p.q)} \mathfrak{h}/G \times \mathfrak{h}/G.
$$

Proposition 1. 下の commutative diagram は fiber product である。

$$\begin{tikzcd}
\Gamma_{p,q}^* \arrow[r] \arrow[d] & (\mathfrak{h}/G)^* \times (\mathfrak{h}/G)^* \cong E \times E \arrow[d, "\tau\times\tau"] \\
\Gamma_{\bar p,\bar q}^* \arrow[r] & (\mathfrak{h}/\Gamma(2))^* \times (\mathfrak{h}/\Gamma(2))^*
\end{tikzcd}$$

Proof 上は commutative なので、下の可換図式が得られる。

$$\begin{tikzcd}
\Gamma_{p,q}^* \arrow[dr, "\beta"] \arrow[ddr, bend right] \arrow[drrr, bend left, "p"] & & & \\
& \Gamma_{\bar p,\bar q}^* \times_{(\mathfrak{h}/\Gamma(2))^{*2}} (E\times E) \arrow[r] \arrow[d, "\alpha"] & E\times E \arrow[r, "pr_1"] \arrow[d, "\tau\times\tau"] & E \arrow[d, "\tau"] \\
& \Gamma_{\bar p,\bar q} \arrow[r] \arrow[rr, bend right, "\bar p"'] & (\mathfrak{h}/\Gamma(2))^* \times (\mathfrak{h}/\Gamma(2))^* \arrow[r] & (\mathfrak{h}/\Gamma(2))^*
\end{tikzcd}$$

まず $\deg\tau = 2p$ なので、$\deg\alpha = \deg(\tau\times\tau) = (2p)^2$.
$\Gamma_{p,q}^* \to E\times E$ は injective なので β も injective。また
$\Gamma_{p,q}^*$, $\Gamma_{\bar p,\bar q}^*$ 共に既約で、$\tau\circ p$ が finite なので $\alpha\circ\beta$ も finite。
さらに上の可換図式から、$\deg(\beta\circ\alpha)\cdot\deg\bar p = \deg p\cdot\deg\tau$.
ここで $\deg\bar p = \ell+1$ は良く知られている。$\deg p = 2p(\ell+1)$, $\deg\tau$
$= 2p$ を代入して、$\deg(\beta\circ\alpha) = (2p)^2 = \deg\alpha$. ゆえに β は surjective.

<u>Corollary 2</u>　ℓ. pを今までの通りとする。この時.
$T(\ell) \mid H^1(E, \mathbb{Q}) = 0$ となる。

<u>Proof</u>　前のでは. $E \longrightarrow E/\pm 1 \ \mathbb{P}^1$
$\tau \searrow h_y / \Gamma(2)$

とfactorするので. $\Gamma_{p.q^*} \cong \Gamma_{p.-p^*}$となる。ここで$-q = ((-1)$倍$\mathrm{map}) \circ q$であるまたcorrespondenceとして$H^1$上に$(-1)$倍mapは$-1$として作用するので　$q_* p^* = -((-q)_* p^*)$. これから. 上の等式を得る。　　　　　　　　Q.E.D.

<u>Corollary 3.</u>　$\Gamma_{p.q^*} \ (\mathrm{mod}\ \ell)$は次の様になる。

$$\Gamma_{p.q^*} \ (\mathrm{mod}\ \ell) = H + {}^tH$$
$$H = F + (-F) + C.$$

ここでFは　$E(\mathrm{mod}\ \ell)$のFrobeniusのgraph. Cはほとんどすべてのℓについて既約なdivisorで(-1)倍でstable。

<u>Proof</u>　$\Gamma_{p.q^*} \ (\mathrm{mod}\ \ell) = (\tau \times \tau \ (\mathrm{mod}\ \ell))^{-1}(F) + (\tau \times \tau \ (\mathrm{mod}\ \ell))^{-1}({}^tF)$
で.　$(\tau \times \tau \ (\mathrm{mod}\ \ell))^{-1}(F) = H$とおくと.

$$H = \{(x.y) \in (E \times E)\ (\mathrm{mod}\ \ell) \mid \tau(x)^{\ell} = \tau(y)\}$$
$$= \{(x, y) \mid \tau(x^{\ell}) = \tau(y)\}$$

さらに $H' = \{(x,u) \in (E\times E)(\mathrm{mod}\,\ell) \mid \tau(x)=\tau(u)\}$

とおけば、$H' \ni (x,u) \longmapsto (x, u^\ell) \in H$ が define される。

$$\begin{tikzcd} H' \arrow[r] \arrow[dr] & H \arrow[d] \\ & (\mathfrak{H}/\Gamma(2)^*)(\mathrm{mod}\,\ell) \end{tikzcd}$$

$$\deg pr_1|_H = (\deg pr_1|_F) \times (2p)^2 = (2p)^2$$

$$\deg pr_2|_H = \ell(2p)^2$$

$\deg pr_1|_{H'} = (2p)^2$, $\deg pr_2|_{H'} = \ell(2p)^2$. だから、$H' \hookrightarrow H$ であれば、$H' \cong H$ となる。

$$\begin{tikzcd} H' \arrow[r, "\beta"'] \arrow[d, "\alpha"'] & H \arrow[d] \\ E & E\times E \arrow[l, "pr_1"] \end{tikzcd}$$

しかし左の図で α は separable, β は purely inseparable なので、β は injective でなくてはいけない。

他方、$H' = (\mathfrak{H}/G)^* \times_{(\mathfrak{H}/\Gamma)^*} (\mathfrak{H}/G)^*$ mod ℓ である。一般に次の Lemma が知られている。

<u>Lemma 4</u> $\Gamma_1, \Gamma_2 \subset \Gamma \subseteq SL(2,\mathbb{Z})$ a finite index の subgroup とすると、$(\mathfrak{H}/\Gamma_1)^* \times_{(\mathfrak{H}/\Gamma)^*} (\mathfrak{H}/\Gamma_2)^*$ の normalization $\cong \coprod_{\Gamma_1\backslash\Gamma/\Gamma_2 \ni g} (\mathfrak{H}/\Gamma_1 \cap g\Gamma_2 g^{-1})^*$ となる。

<u>proof</u> 略.

今この Lemma を使うと

$$(\mathfrak{h}_y/G)^* \times_{(\mathfrak{h}_y/\Gamma(2))^*} (\mathfrak{h}_y/G)^* \text{ の normalization}$$

$$\cong \coprod_{G\backslash\Gamma(2)/G} (\mathfrak{h}_y/G \cap gGg^{-1})^*$$

$$\cong \coprod_{H_1\backslash H_2/H_1} (\mathfrak{h}_y/G \cap gGg^{-1})^*$$

で．$H_1\backslash\{\pm i \mid i=1,\cdots,p\} = \{+1\}\cup\{-1\}\cup\{\pm 2,\cdots,\pm p\}$ となり．これは．l に independent であるから．ほとんどすべての l について既約成分は3つである。F と $-F$ は明らかにその異なる成分であるから．残りの1つは．ほとんどすべての l について既約である。

Q.E.D.