Serre予想の証明： 帰納法の第一段階

田口 雄一郎 (九大数理)

1. Odlyzko bound
2. Mod 2, 3 表現の非存在
3. 半安定 Abel 多様体の非存在

序. 本稿では Serre 予想の特別の場合であり、帰納法による証明の第一段階となる、次の二つの定理を証明する。

定理 1. $p = 2, 3$ のとき、p の外で不分岐、連続、かつ既約な表現 $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ は存在しない。

定理 2. $p = 2, 3, 5, 7, 13$ のとき、$\mathbb{Q}$ 上の Abel 多様体 A であつて高々 p で半安定還元を持つ[1] ものは存在しない。

註. 定理 1 は Tate ([44], $p = 2$) と Serre ([38], $p = 3$) に依り、定理 2 は Schoof [32] に依る ([7] にも同様の結果がある)。定理 1 と類似の結果として [6] や [23] がある。Brueggeman [6] は $p = 5$ のとき、GRH[2] を仮定して、5 の外不分岐な既約表現 $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_5)$ の非存在を証明してゐるが、実は GRH が必要なのは “被約 Serre weight” が 6 の場合のみである ([23])。Serre weight が 6 の場合、ρ は半安定な重さ 2 の 5 進表現に持ち上がり、さらに ℓ 進表現系に延びる ([19])。Taylor [46] によりそれは高々 5 で半安定還元を持つ $\mathbb{Q}$ 上の Abel 多様体から来る事になるので、結局 Schoof の定理とその他諸々の「偉い」結果を合せると、定理 1 の $p = 5$ の場合 (mod 5 表現の非存在) が従ふ。

Schoof [32] は上の定理 2 以外にも次の事を証明してゐる：

定理 2′. $\mathbb{Q}$ 上の Abel 多様体 A であつて高々 11 で半安定還元を持つものは、level 11 の modular Jacobian $J_0(11)$ の冪と同種である。

定理 2″. $p = 2, 3, 5$ のとき、$\mathbb{Q}$ 上の Abel 多様体 A であつて p の外で良還元かつ p では馴潜在半安定還元[3] を持つものは存在しない。

[1] ここ及び以下で「高々 p で半安定還元を持つ」とは、p の外で良還元 (good reduction) を持ち p では半安定還元 (semi-stable reduction) を持つ事である。$\mathbb{Q}$ 上至る所良還元を持つ Abel 多様体は存在しない ([11]) ので、実際にはこの様な A は必ず p で悪還元を持つ事になる。

[2] ここ及び以下で、GRH と言つたら「全ての代数体の Dedekind zeta 函数に対する一般 Riemann 予想」の意。

[3] 「或る有限次拡大 $K/\mathbb{Q}$ であつて p で高々馴分岐 (tamely ramified) なもので基底変換すれば半安定還元を持つ」の意。文面の簡略化のため鋳造した語。

これらの定理は大雑把に言へば全て同じ原理で証明される。上の様な ρ や A があるとし、ρ や A の ℓ-等分点の群 $A[\ell]$ から生ずる Galois 拡大 $K/\mathbb{Q}$ を考へる (ℓ は適当な小さい素数)。ρ や A に課された条件から、$K/\mathbb{Q}$ にも制限がかかる。具体的には、$K/\mathbb{Q}$ の判別式 $d_{K/\mathbb{Q}}$ が上から押へられる (Tate や Fontaine の評価)。反対に下からは Odlyzko bound (§1) といふ判別式の絶対的な評価があり、これによると $K/\mathbb{Q}$ は非可解ではあり得ず、また、可解の場合には類体論などを使つて $K/\mathbb{Q}$ は非常に特殊なものに限られる事が示せる。その様な $K/\mathbb{Q}$ に対して、ρ は既約ではあり得ず、或いは $A[\ell]$ は (さらに $A[\ell^n]$ も)

$$0 \ \to \ (\mu_\ell \text{ たちの拡大}) \ \to \ A[\ell^n] \ \to \ (\mathbb{Z}/\ell\mathbb{Z} \text{ たちの拡大}) \ \to \ 0$$

の形、となり、これから矛盾が出る、といふ仕組みである。Fontaine による Abelian scheme/$\mathbb{Z}$ の非存在の証明 ([11]) もこの原理に依つてゐる。

謝辞. 「$R = T$ 勉強会」を主催して下さつたのみならず、宿の世話をし、バスの conductor の役を果たし、宴会を盛り上げ、なほかつ素晴らしい数々の講演をして下さつた安田正大さんと山下剛さんに心から敬意と謝意を表したいと思ひます。この小さい原稿を書いてみて、お二人がどれだけ膨大なエネルギーを注ぎ込んで講演の準備をして下さつたのか少しは想像できるやうな気がしました。またお二人は、この原稿の初稿及び第二稿を読んで多くの有益なコメントを下さいました (一々記しませんでしたが、その多くは本文中及び脚注に生かされてゐます)。深く感謝致します。服部新さんと三枝洋一さんには、群 scheme や fppf 層についての微妙な点に関して相談に乗つて頂きました。感謝致します。

1. Odlyzko bound. 実際に使はれるのは GRH を仮定しない、具体的な数値を与へる Odlyzko の表 ([26]) や Poitou の評価式 ([29]) だが、それを掲げる前に、理論的にスッキリしてゐる Serre による漸近評価 (GRH を仮定する) を紹介しよう (同様の発想の論文として Mestre [20] がある)。n 次拡大 $K/\mathbb{Q}$ に対しその判別式を $d_{K/\mathbb{Q}}$ とし、root discriminant を $d_K^{1/n} := |d_{K/\mathbb{Q}}|^{1/n}$ と書く。また、r_1, r_2 をそれぞれ K の実素点の個数、複素素点の個数とする。

定理 1.1 ([39]). 全ての代数体の Dedekind zeta に対する GRH を仮定する。このとき次の漸近評価が成り立つ :

$$\liminf_{n\to\infty} \left(\log d_K^{1/n} - a_1 \frac{r_1}{n} - a_2 \frac{2r_2}{n} \right) \ \geq \ 0,$$

ここに定数 a_1, a_2 は

$$\begin{cases} a_1 &= \log(8\pi)+\gamma+\pi/2 &= 5.372183..., \\ a_2 &= \log(8\pi)+\gamma &= 3.801387..., \end{cases}$$

($\gamma = 0.577215...$ は Euler 定数) である。特に総実 (乃至総虚) な K に限つて動かすと、$r_1 = n$ (乃至 $2r_2 = n$) だから、

$$\liminf_{n\to\infty} d_K^{1/n} \ \geq \ \begin{cases} 8\pi e^{\gamma+\pi/2} &= 215.332... \quad (K\text{: 総実}), \\ 8\pi e^{\gamma} &= 44.763... \quad (K\text{: 総虚}). \end{cases}$$

証明： 鍵になるのは Weil の明示公式 (explicit formula, [48]) である。これに現れる記号を説明するために、先づ K の Dedekind zeta の函数等式を思ひ出さう:

$$\zeta_K(s)G(s) \ = \ \zeta_K(1-s)G(1-s).$$

ここに $G(s)$ は Γ-因子:

$$G(s) := \ |d_{K/\mathbb{Q}}|^{s/2} g_1(s)^{r_1} g_2(s)^{r_2} \qquad \text{with} \quad \begin{cases} g_1(s) := \ \pi^{-s/2}\Gamma(\frac{s}{2}), \\ g_2(s) := \ (2\pi)^{-s}\Gamma(s). \end{cases}$$

函数等式の log 微分を取ると、

$$\frac{G'}{G}(s) + \frac{G'}{G}(1-s) \ = \ -\left(\frac{\zeta_K'}{\zeta_K}(s) + \frac{\zeta_K'}{\zeta_K}(1-s)\right).$$

これを直線 $s = 1/2 + it$ ($t \in \mathbb{R}$) 上で考へるので、

$$\Psi(t) := \ \frac{G'}{G}\left(\frac{1}{2}+it\right) + \frac{G'}{G}\left(\frac{1}{2}-it\right) \ = \ 2\mathrm{Re}\left(\frac{G'}{G}\left(\frac{1}{2}+it\right)\right)$$

とおき、さらに次の様に書き直す :

$$= \ \log|d_{K/\mathbb{Q}}| + r_1\Psi_1(t) + 2r_2\Psi_2(t),$$

ここに

$$\begin{cases} \Psi_1(t) := \ 2\mathrm{Re}\left(\frac{g_1'}{g_1}(\frac{1}{2}+it)\right) \ = \ -\log(\pi) + \mathrm{Re}\left(\psi(\frac{1}{4}+i\frac{t}{2})\right), \\ \Psi_2(t) := \ \mathrm{Re}\left(\frac{g_2'}{g_2}(\frac{1}{2}+it)\right) \ = \ -\log(2\pi) + \mathrm{Re}\left(\psi(\frac{1}{2}+it)\right), \end{cases}$$

$$\psi := \ \Gamma'/\Gamma.$$

さて **Weil の明示公式**[4] とは：

$$\sum_{\omega}\Phi(\omega)+\sum_{\mathfrak{p},m}\frac{\log N\mathfrak{p}}{N\mathfrak{p}^{m/2}}\left(F(\log N\mathfrak{p}^m)+F(-\log N\mathfrak{p}^m)\right)$$
$$=\ \Phi(0)+\Phi(1)+\frac{1}{2\pi}\int_{-\infty}^{\infty}\varphi(t)\Psi(t)dt,$$

ここに F, Φ, φ は資料函数で、

$F:\mathbb{R}$ 上の C^∞ 級急減少函数、
$\Phi(s):=\int_{-\infty}^{\infty}F(x)e^{(s-1/2)x}dx$,
$\varphi(t):=\Phi(1/2+it)$,

また、和 $\sum_\omega$, $\sum_{\mathfrak{p},m}$ はそれぞれ

$\omega:\zeta_K(s)$ の非自明零点、
$\mathfrak{p}:K$ の素イデアル、 $m:$整数 ≥ 1,

に亘る和である。

ここで $F\geq 0$, $\varphi\geq 0$ となる様に F を取ると、$\mathrm{Re}(\omega)=1/2$ ならば $\Phi(\omega)=\varphi(\mathrm{Im}(\omega))\geq 0$ である。そこで GRH を仮定すると「明示公式の左辺 ≥ 0」となるので

$$\Phi(0)+\Phi(1)+\frac{1}{2\pi}\int_{-\infty}^{\infty}\varphi(t)\left(\log|d_{K/\mathbb{Q}}|+r_1\Psi_1(t)+2r_2\Psi_2(t)\right)dt\ \geq\ 0.$$

以下 φ は常に $\frac{1}{2\pi}\int_{-\infty}^{\infty}\varphi(t)dt=1$ と正規化しておく。上の不等式の両辺を n で割り、F を (従つて Φ, φ も) 固定しておいて $n\to\infty$ とすると

$$\liminf_{n\to\infty}\left(\log d_K^{1/n}+\frac{r_1}{n}\int_{-\infty}^{\infty}\frac{\varphi(t)}{2\pi}\Psi_1(t)dt+\frac{2r_2}{n}\int_{-\infty}^{\infty}\frac{\varphi(t)}{2\pi}\Psi_2(t)dt\right)\ \geq\ 0.$$

ここで φ を Dirac の δ 函数に近づける (例へば $\varphi(t)=ce^{-bt^2}$ の形で $b\to\infty$ とする) と上の二つの $\int_{-\infty}^{\infty}$ は $\Psi_1(0)$, $\Psi_2(0)$ に近づくから、

$$\liminf_{n\to\infty}\left(\log d_K^{1/n}+\frac{r_1}{n}\Psi_1(0)+\frac{2r_2}{n}\Psi_2(0)\right)\ \geq\ 0.$$

[4] この公式自体は函数 $\frac{1}{2\pi i}\frac{\Lambda_K'}{\Lambda_K}(s)\Phi(s)$ を危険地帯 (critical strip) に於いて二通りに積分する事により得られる (ここに $\Lambda_K(s):=\zeta_K(s)G(s)$)。一つは、適当な有界長方形上で積分してその高さを $\to\infty$ とすると Cauchy の積分定理により $\sum_\omega\Phi(\omega)-\Phi(0)-\Phi(1)$ が出る。もう一つは、函数等式を用ゐてこれを $\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty}\frac{\Lambda_K'}{\Lambda_K}(s)\left(\Phi(s)+\Phi(1-s)\right)ds$ と書き換へると、$\frac{\Lambda_K'}{\Lambda_K}(s)=\frac{\zeta_K'}{\zeta_K}(s)+\frac{G'}{G}(s)$ の zeta 部分から $\sum_{\mathfrak{p},m}$ が現れ、gamma 部分から $\frac{1}{2\pi}\int\varphi(t)\Psi(t)dt$ が現れる。

定数 $\Psi_1(0), \Psi_2(0)$ を計算すると、それぞれ定理の $-a_1, -a_2$ になる。 □

さて、Serre 以前に Odlyzko [25] は、GRH を仮定せずに、次の評価を得てゐた[5] (Odlyzko に従つて「log を取らない版」で掲げておく) :

$$d_K^{1/n} \ > \ (60.1)^{r_1/n}(22.2)^{2r_2/n} \qquad (n \text{ が十分大のとき}).$$

その方法は基本的には上の明示公式を使ふものと同様「$d_K^{1/n}$ と $\zeta_K(s)$ の零点とを結び付ける」事であり、Stark[6] の方法 ([41]) の発展である。Odlyzko はさらに実用的な、次の様な表を得た :

n	$d_K^{1/n}$ (総実)	$d_K^{1/n}$ (総虚)
1	0.996	0.874
10	12.941	6.585
12	15.068	7.395
15	17.849	8.423
16	18.684	8.725
17	19.479	9.010
20	21.642	9.779
25	24.664	10.829
30	27.138	11.675
60	36.067	14.634
100	41.728	16.454
120	43.513	17.020
200	47.833	18.379
300	50.588	19.237
600	54.122	20.329
1000	55.966	20.895
10000	59.746	22.049
100000	60.582	22.308
1000000	60.691	22.348
10000000	60.702	22.352

これは [26] にある unconditional bound (GRH を仮定しない) の表の一部である。そこには GRH を仮定した場合の表もある。この表の読み方は、例へ

[5] Poitou は解説論文 [29] の中で次の評価を与へてゐる :
$\log d_K^{1/n} \ \geq \ \gamma + \log(4\pi) + r_1/n - 8.6n^{-2/3}$ (全ての $n \geq 1$ に対して),
$d_K^{1/n} \ > \ (60.8)^{r_1/n}(22.3)^{2r_2/n}$ (n が十分大のとき).

[6] Oldyzko は Stark の学生であつた。

ば $n = 60$ の行を見て「$n \geq 60$ のとき、K が総実ならば $d_K^{1/n} > 36.067$, K が総虚でも $d_K^{1/n} > 14.634$」等と読む (総虚の場合が一番評価が悪いので、実際は任意の K に対して右側の評価が成り立つ)。

判別式やそれに関連する諸物の評価に関する 1990 年頃までの「最近の状況」については Odlyzko の報告 [27] を参照されたい。

註. Odlyzko bound を改良出来たらいいなあとは誰しも思ふところだが、一般にはこれは絶望的と思はれる。しかし何らかの条件 (例へば $\mathrm{Gal}(K/\mathbb{Q}) \subset \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ なる K だけ動かすとか) の下で改良できないだらうか？虫が良過ぎるかしら？伊原 [16] には「至る所不分岐な無限次 Galois 拡大で殆ど完全分解する素点たちの寄与」を考慮に入れた判別式の評価 (定理 1.1 の改良) が与へられてゐるが、我々の文脈での応用は未だ見出されてゐない。

2. Mod 2, 3 表現の非存在. 前節では判別式の下からの評価 (Odlyzko bound) を紹介した。ここでは先づ判別式の上からの評価 (Tate bound) を紹介する。その原典は Tate [44] であるが、ここでは "被約 Serre weight" ごとに共役差積の付値を与へる公式 ([23]) を紹介する。問題は local だから、ρ は $\mathbb{Q}_p$ の絶対 Galois 群 D_p の表現としてよい。

$\rho : D_p \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ の Serre weight を $k(\rho)$ と書く (Serre weight の定義については [40], [13] を参照)。ρ の 被約 Serre weight $\tilde{k}(\rho)$ を

$$\tilde{k}(\rho) \ := \ \min\{k(\chi^{-\alpha} \otimes \rho) |\ \alpha \in \mathbb{Z}\}$$

と定義する (ここに χ は mod p 円分指標)。

$K/\mathbb{Q}_p$ を $\mathrm{Ker}(\rho)$ に対応する拡大とし、$\mathcal{D}_{K/\mathbb{Q}_p}$ をその共軛差積、$v_p(\mathcal{D}_{K/\mathbb{Q}_p})$ をその p 進付値とする ($v_p(p) = 1$ により正規化しておく)。これの上からの評価を問題とするのであるが、$K/\mathbb{Q}_p$ が馴分岐なら $v_p(\mathcal{D}_{K/\mathbb{Q}_p}) = 1 - 1/e$ (e は分岐指数) と分かつてゐるから、以下では ρ は (即ち $K/\mathbb{Q}_p$ は) 暴分岐 (wildly ramified) と仮定 する。暴分岐な ρ は I_p に制限すると

$$\rho|_{I_p} \ \sim \ \begin{pmatrix} \chi^{\beta} & * \\ 0 & \chi^{\alpha} \end{pmatrix} \qquad \text{with } * \neq 0,$$

の形であるから、これを

$$\rho|_{I_p} \ \sim \ \chi^{\alpha} \begin{pmatrix} \chi^{k-1} & * \\ 0 & 1 \end{pmatrix} \qquad \text{with } 2 \leq k \leq p,$$

と書き $k(\rho)$ の定義と較べると、

$$\tilde{k}(\rho) \ = \ \begin{cases} p+1 & (k = 2 \text{ かつ } \chi^{-\alpha} \otimes \rho \text{ が有限でないとき}) \\ k & (\text{その他}). \end{cases}$$

となる。

定理 2.1. $\rho : D_p \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ を暴分岐連続表現とし、$k := \tilde{k}(\rho)$ をその被約 Serre weight とする。このとき

$$v_p(\mathcal{D}_{K/\mathbb{Q}_p}) \;=\; \begin{cases} 1 + \frac{k-1}{p-1} - \frac{k-1+d}{(p-1)p^m} & \text{if } 2 \le k \le p, \\ 2 + \frac{1}{(p-1)p} - \frac{2}{(p-1)p^m} & \text{if } k = p+1. \end{cases}$$

ここに定数 d, m は

$$\begin{aligned} d :=&\; \gcd(\alpha, \beta, p-1), \\ p^m :=&\; (K/\mathbb{Q}_p \text{ の暴分岐指数}), \end{aligned}$$

とおいた。

証明 (sketch): $K/\mathbb{Q}_p$ を $\mathrm{Ker}(\rho)$ に対応する体とし、$K_1/K_0/\mathbb{Q}_p$ をそれぞれ $K/\mathbb{Q}_p$ の最大馴分岐/不分岐部分拡大とする。また、これらの Galois 群を $G = \mathrm{Im}(\rho) = \mathrm{Gal}(K/\mathbb{Q}_p)$, $H = \mathrm{Gal}(K/K_1) \simeq \left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)$, $\Delta = \mathrm{Gal}(K_1/K_0) \simeq \mathrm{Im}\left(\begin{smallmatrix} \chi^\beta & \\ & \chi^\alpha \end{smallmatrix}\right)$ とおく。馴分岐部分の共役差積の p 進付値は $1 - 1/|\Delta|$ と知れてゐるから、暴分岐部分だけが問題である。それを導手判別式積公式 ([35], 第 VI 章, §3, 命題 6 の系 2)

$$d_{K/K_1} \;=\; \prod_{\psi \in \widehat{H}} \mathfrak{f}_\psi$$

($\widehat{H}$ は H の既約指標全体の集合、$\mathfrak{f}_\psi$ は ψ の導手) により計算する。局所類体論により $U := \mathcal{O}_{K_1}^\times / (\mathcal{O}_{K_1}^\times)^p$ から H へ全射 $U \to H$ があるが、これは Δ-準同型である (Δ は U に Galois 群として自然に作用し、H には共役 $\left(\begin{smallmatrix} 1 & x \\ & 1 \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} \chi^\beta & \\ & \chi^\alpha \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & x \\ & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \chi^\beta & \\ & \chi^\alpha \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} 1 & \chi^{\beta-\alpha}x \\ & 1 \end{smallmatrix}\right)$ により作用する)。この作用の御蔭で、指標 $\psi \in \widehat{H}$ を U の指標と思つたときそれがどの $(1+\pi_1^c\mathcal{O}_{K_1})$ を経由するかが制限される (ここに π_1 は K_1 の素元)。簡単のため $d = 1$ と仮定すると、$2 \le k \le p$ のときは $\mathfrak{f}_\psi = (\pi_1^k)$. また、$k = p+1$ のときは (このとき自動的に $d = 1$ で)、全体の $1/p$ (即ち p^{m-1} 個) の ψ については $\mathfrak{f}_\psi = (\pi_1^2)$ 又は (1), 残り $(p^m - p^{m-1})$ 個が $\mathfrak{f}_\psi = (\pi_1^{p+1})$ となる (前者が peu ramifié の場合、後者が très ramifié の場合) ので、標記の $v_p(\mathcal{D}_{K/\mathbb{Q}_p})$ の値が出る。 □

この評価と Odlyzko bound とを組合せると、定理 1 より少し詳しく、次の結果が得られる ([23], 定理 1):

定理 2.2. p の外不分岐な既約表現 $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ の存在非存在の様子は、被約 Serre weight $k = \tilde{k}(\rho)$ の値によつて、以下の様になる：

$k\backslash p$	2	3	5	7	11	13	17	19	23	29	31
2	×	×	×	×	×	×	×	×	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$
3	×	×	×	×	×	×	×	×	f	f	f
4		×	×	×	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	f_{R}	f_{R}
5			×	×	×	×	×	×	f	f	f
6			$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	f_{R}	f_{R}	?	?	?
7				×	×	×	×	×	f	f	f_{R}
8				?	?	?	?	?	?	?	?
9					$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	f_{R}	f_{R}	f_{R}
10					?	?	?	?	?	?	?
11					$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	f_{R}	f_{R}	f_{R}
12					∃	∃	∃	∃	∃	∃	∃
13						f_{R}	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	f_{R}	f_{R}	f_{R}
14						?	?	?	?	?	?
15							f_{R}	f_{R}	f_{R}	f_{R}	f_{R}
16							∃	∃	∃	∃	∃
17							?	?	?	f_{R}	f_{R}
18							∃	∃	∃	∃	∃
19								?	?	?	?
20								∃	∃	∃	∃

この表に出て来る記号の意味は次の通り： 上の様な ρ は

- ×： 存在しない。
- $\times_{\mathrm{R}}$： GRH を仮定すると、 存在しない。
- f： 高々有限個しか存在しない。
- f_{R}： GRH を仮定すると、高々有限個しか存在しない。
- ∃： 存在する (保型形式から来るもの)。
- ?： 存在するかしないか不明。

註. 今、$N(\rho)=\varepsilon(\rho)=1$ の場合を考へてゐるから、

$$\rho \text{ が奇} \iff k \text{ が偶}$$

である。上の表は Serre 予想の帰結を無視して書いてあるが、それが解けた今となつては、k が偶数 ≤ 10 又は $k=14$ の部分は全て × である ($S_k(\mathrm{SL}_2(\mathbb{Z}))=0$ なので)。また、その他の部分も k が偶数ならば全て f である ($S_k(\mathrm{SL}_2(\mathbb{Z})$ は有限次元なので)。表の下半分で ∃ となつてゐるところは $f\in S_k(\mathrm{SL}_2(\mathbb{Z}))$ から来る $\bmod p$ 表現[7] である。

[7] [23] では $(k,p)=(12,23),(16,31)$ のところが ? となつてゐるが、これは $p=23,31$ がそれぞれ重さ 12, 16 の唯一の尖点形式 Δ_{12}, Δ_{16} の「例外素数」(即ち対応する $\bmod p$ 表現

さて、定理 1 を証明しよう。$G := \mathrm{Im}(\rho)$ とおき、$\mathrm{Ker}(\rho)$ に対応する体を K とする。

G が可解の場合 : Tate ([44]) と少し趣きを変へて、次の命題を使つて証明してみよう :

命題 2.3 ([42], §§21–22). $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ の可解かつ既約[8] な部分群 G は次のいづれかのタイプである :

(i) G は p と素な位数の巡回群と $\mathbb{Z}/2\mathbb{Z}$ との花輪積 (wreath product) の部分群であり、共役を除き次の形となる :

$$1 \ \to \ A \ \to \ G \ \to \ \mathbb{Z}/2\mathbb{Z} \ \to \ 1 \quad (\text{完全}), \qquad A \subset \begin{pmatrix} * & \\ & * \end{pmatrix}.$$

(ii) G の射影像 $\overline{G} := \mathrm{Im}(G \to \mathrm{PGL}_2(\overline{\mathbb{F}}_p))$ は次の短完全列を満たす :

$$1 \ \to \ \overline{A} \ \to \ \overline{G} \ \to \ \overline{H} \ \to \ 1,$$

ここに $\overline{A}$ は $(\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ の或る部分群と同型であり、$\overline{H}$ の $\overline{A}$ への共役作用は忠実である。従つて特に $\overline{G}$ は 2-群、対称群 S_4, 交代群 A_4, のいづれかである。

さらに、 $p = 2$ のときは (i) しか起こり得ない。

さて定理 1 の証明に戻る。

$p = 2$ のとき : このとき $G = \mathrm{Gal}(K/\mathbb{Q})$ は (i) 型なので、$K/\mathbb{Q}$ の或る部分体 F があつて、$F/\mathbb{Q}$ は 2 の外不分岐二次拡大、K/F は 2 の外不分岐奇数次 Abel 拡大、となる。そこで F は $\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{\pm 2})$ のいづれかであるが、いづれの場合も F の類数は 1 で、F の整数環 $\mathcal{O}_F$ の 2-進完備化の乗法群 $\mathcal{O}_F^\times$ は pro-2 群なので、類体論により、上の様な Abel 拡大 K/F は存在しない。

$p = 3$ のとき : G が (i) 型のとき、K は二次体 $F/\mathbb{Q}$ を含む。3 の外で不分岐な二次体は $F = \mathbb{Q}(\sqrt{-3})$ のみであり、その類数は 1 である。類体論を使つて F の 3 の外不分岐 Abel 拡大の可能性を調べる。F の整数環の 3-進完備化 $\mathcal{O}_{F,3}$ の乗法群の構造は

$$\mathcal{O}_{F,3}^\times \ \simeq \ (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}_3^{\oplus 2}.$$

ρ_Δ の像が $\mathrm{SL}_2(\mathbb{F}_p)$ を含まない) になつてゐるので「不明」と思つてしまつた故である。実際はその像は 3 次対称群と同型 ([37], §3) なので、ρ_Δ は既約である。この場をお借りして訂正させて頂きます。

[8] $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ の部分群 G が 既約 であるとは、包含写像 $G \hookrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ が群の表現として既約である事である。

相互写像を適用するとき $\mathbb{Z}/2\mathbb{Z}$ は大域単数 -1 により消えるから、3 の外不分岐 Abel 拡大 K/F であつて拡大次数が 3 と素なものは存在しない。

G が (ii) 型のとき、上の記号で、$\overline{H}$ は $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, S_3 のいづれかと同型であり、従つて $K/\mathbb{Q}$ は 2 次または 3 次の巡回部分体 $F/\mathbb{Q}$ を含む。$F/\mathbb{Q}$ が 3 次のとき、$F = \mathbb{Q}(\zeta_9)^+$ (= 9 分体の最大実部分体) であり、この体の類数は 1. また、

$$\mathcal{O}_{F,3}^{\times} \simeq (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}_3^{\oplus 3}$$

であり、$\mathbb{Z}/2\mathbb{Z}$ は大域単数 -1 により消えるから、3 の外不分岐 Abel 拡大 K/F であつて拡大次数が 3 と素なものは存在しない。$F/\mathbb{Q}$ が 2 次のとき、もし $\overline{H} \simeq \mathbb{Z}/2\mathbb{Z}$ なら (i) 型のときと同様。もし $\overline{H} \simeq S_3$ なら、その S_3-拡大を $E/\mathbb{Q}$ とすると、E の候補は二つのみで、それは $X^6 + 3$ の分解体であり ([18]), その類数は 1 で、

$$\mathcal{O}_{E,3}^{\times} \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times \mathbb{Z}_3^{\oplus 6}.$$

$\mathbb{Z}/2\mathbb{Z}$ は大域単数 -1 により消えるから、3 の外不分岐 Abel 拡大 K/E であつて拡大次数が 3 と素なものは存在しない。

G が非可解の場合： 定理 2.1 より

$$d_K^{1/n} < \begin{cases} 2^{2+1/2} < 5.657 & \text{if } p = 2, \\ 3^{2+1/6} < 10.809 & \text{if } p = 3. \end{cases}$$

一方 G が非可解ならば $n = [K : \mathbb{Q}] = |G| \geq 60$ だから §1 の Odlyzko bound の表より $d_K^{1/n} > 14.634$. これらの不等式は矛盾するから、この様な ρ は存在しない。 □

註. Tate [44] は Odlyzko bound でなく Minkowski bound を使つた (Odlyzko bound の使用を示唆したのは Serre [38] である)。Minkowski bound は所謂「数の幾何」で証明される (cf. [43], 第 5 章)。

省察. ここでは Tate 以来の色々な人々の工夫 (判別式の評価の改良や群論など) を動員して $\mathbb{Q}$ の GL_2-拡大についての具体的な議論から逃げてしまつたが、正直にやらうとすると結構泥沼にハマる。その様な議論を実際にやつてみると、Serre 予想が具体的に意味するところのものを体感出来る。[9]

一般化. Serre 予想は幾つかの一般化が提唱されてゐる。代表的なものとして次がある：

[9] このへんは山下さんが講演中に口走られた事の受け売りが含まれてゐますが、必ずしも正確に反映してをらず、責任は筆者にあります。

(1) 基礎体を $\mathbb{Q}$ から総実代数体に一般化する ([8]).
(2) 基礎体を $\mathbb{Q}$ から虚二次体に一般化する ([10], [34]).
(3) 群を GL_2 から GL_n に一般化する (基礎体は $\mathbb{Q}$ のまま) ([5], [4]).

(1) は総実代数体 F の 2 次元 mod p Galois 表現 $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ が Hilbert 保型形式から来るかといふ話である。現在のところ「$F/\mathbb{Q}$ が p で不分岐」といふ仮定の下で予想が定式化されてゐる。(2) は虚二次体 F の 2 次元 mod p Galois 表現 $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ の話である。この場合、対応させるべき相手としては、3 次元双曲空間の modular symbol 又は適当な群 (Bianchi modular 群) の cohomology 類を考へる。(3) は、今のところ基礎体は $\mathbb{Q}$ の場合のみ考へられてゐる。一般次元の mod p Galois 表現 $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\overline{\mathbb{F}}_p)$ の相手として、やはり適当な合同部分群 $\subset \mathrm{GL}_n(\mathbb{Z})$ の cohomology 類を考へる。

これらに関しても、Khare-Wintenberger に倣つて帰納法で証明しようとするならば、「第一段階」が必要である。現時点では次の結果が知られてゐる :

定理 2.4. (1) F が次の二次体のいづれかであるとき、$\{2, \infty\}$ の外不分岐既約 mod 2 表現 $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ は存在しない :

$$\mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{\pm 2}),\ \mathbb{Q}(\sqrt{\pm 3}),\ \mathbb{Q}(\sqrt{\pm 5}),\ \mathbb{Q}(\sqrt{\pm 6}).$$

(2) $F = \mathbb{Q}(\sqrt{-3})$ のとき、$\{3, \infty\}$ の外不分岐既約 mod 3 表現 $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbb{F}}_3)$ は存在しない。
(3) $n = 3, 4$ のとき、2 の外不分岐[10] 既約 mod 2 表現 $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\overline{\mathbb{F}}_2)$ は存在しない。

(1) は [24], [34] による (後者は前者の判別式の評価 (Tate bound の一般化) に全面的に依拠してゐる)。(2) は [34] に依るが、これは [21] の判別式の評価から容易に従ふ。(3) は [22] に依る。

註. [5], [4] では mod p 表現に "strict parity condition" なるものを課してゐるため、定理 2.4 の (3) により彼らの保型性予想の $n = 3, 4$, $p = 2$, $N = 1$ の場合は正しい事になる。しかし 2 次の Siegel 保型形式から来る 4 次元 mod 2 表現は必ずしもこの条件を満たさないのではないかと思ふので、(3) の様な結果を「$\{2, \infty\}$ の外不分岐」の場合に拡張する事は重要と思はれる。

3. 半安定 Abel 多様体の非存在. この節では Schoof の定理 (定理 2) を証明する。素数 p を固定する。ℓ を別の素数[11] とする。次の圏を考へる :

$\mathbf{G}_{p,\ell}$: $\mathbb{Z}[1/p]$ 上の有限平坦可換群 scheme であつて $\ell^{\text{冪}}$ 位数のものたち

[10] 無限素点でも不分岐 (つまり ρ(複素共役) $= 1$) と仮定する。
[11] [32] とは p と ℓ の役割を入れ換へた。

のなす圏

$\mathbf{D}_{p,\ell}$: $G \in \mathbf{G}_{p,\ell}$ であつて、全ての $\sigma \in I_p$ に対しその $G(\overline{\mathbb{Q}})$ への作用が $(\sigma-1)^2 = 0$ を満たすものたちのなす圏。

ここで、scheme S 上の (可換) 群 scheme とは、S 上の schemes の圏の中の (可換) 群対象の事、それが有限/平坦とは S-scheme として有限/平坦である事である。また、S 上の有限群 scheme G であつて構造層 $\mathcal{O}_G$ が $\mathcal{O}_S$ 上局所自由であるものに対し、その位数 (階数とも呼ぶ) とは $\mathrm{rank}_{\mathcal{O}_S}(\mathcal{O}_G)$ (その値は S の各連結成分上で一定) の事である。例へば A が $\mathbb{Z}[1/p]$ 上の Abel 多様体であつて p で半安定還元を持つとき、その ℓ^n-等分点の群 $A[\ell^n]$ は $\mathbf{D}_{p,\ell}$ の対象であり (cf. [12], 系 3.5.2)、その位数は ℓ^{2gn} ($g := \dim A$) である。

S 上の有限平坦可換群 scheme は S 上の fppf site 上の Abel 群の層とも思へ、fppf 層として考察した方が都合がよい事が多い (多くの文献でもさうしてゐる) ので、ここでも圏 $\mathbf{G}_{p,\ell}$, $\mathbf{D}_{p,\ell}$ を $\mathrm{Spec}(\mathbb{Z}[1/p])_{\mathrm{fppf}}$ 上の Abel 群の層のなす Abel 圏に埋め込んで考へる ($\mathbf{G}_{p,\ell}$, $\mathbf{D}_{p,\ell}$ はこの圏の充満部分圏になる)。実は $\mathbf{G}_{p,\ell}$ は拡大に関して閉ぢてをり、完全圏 (exact category) になる (cf. [9], §2, 特に Lemma 2.3; さらに $p \geq 3$ ならばこれらは Abel 圏にもなる (cf. [11], Th. 2; 本質的には Raynaud [30] に依る)). 従つてそこでの「拡大」や「単純対象 (simple object)」の概念が意味を持ち、$\mathrm{Ext}^1_{\mathbf{G}_{p,\ell}}(G,H)$ などの群が定義される (ここでは fppf 層としてのそれらを考へるが、群 scheme として考へても同じ事になる (cf. [28], III.17; [9], §2).

$\mathbb{Z}/\ell\mathbb{Z}$, μ_ℓ によりそれぞれ $\mathbb{Z}[1/p]$ 上の有限平坦群 schemes

$$\begin{aligned} \mathbb{Z}/\ell\mathbb{Z} = \mathrm{Spec}(\mathbb{Z}[1/p]^{\mathbb{Z}/\ell\mathbb{Z}}) &: \quad \text{“定” } \ell \text{ 次巡回群 scheme,} \\ \mu_\ell = \mathrm{Spec}(\mathbb{Z}[1/p][X]/(X^\ell - 1)) &: \quad \text{“1 の } \ell \text{ 乗根の群” scheme,} \end{aligned}$$

を表す。これらは $\mathbf{D}_{p,\ell}$ の単純対象である。$\mathbf{S}_{p,\ell}$ により $\mathbf{D}_{p,\ell}$ の単純対象の同型類の集合を表す。また、$\mathbf{A}_p$ により、$\mathbb{Q}$ 上の Abel 多様体であつて高々 p で半安定還元を持つものの圏を表す。

命題 3.1. p を固定する。次の二条件を満たす素数 $\ell \neq p$ が存在すれば高々 p でのみ半安定還元を持つ Abel 多様体は存在しない：

(i) $\mathbf{S}_{p,\ell} = \{\mathbb{Z}/\ell\mathbb{Z}, \mu_\ell\}$,
(ii) $\mathrm{Ext}^1_{\mathbf{G}_{p,\ell}}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z}) = 0$.

註. 上の条件 (i), (ii) のうち、大体の感じとして、条件 (i) は比較的成立し難い条件[12] で、条件 (ii) は比較的成立し易い条件[13] である。

[12] 例へば、代数体上の Abel 多様体の ℓ-等分点のなす群 scheme $A[\ell]$ は generic には単純と思はれる (楕円曲線なら実際さう ([36]) で、高次元でも多くの結果あり)。

[13] 実際 $\mathrm{Ext}^1_{\ell\text{-div.gp.}/\mathbb{Z}[1/p]}(\mu_{\ell^\infty}, \mathbb{Q}_\ell/\mathbb{Z}_\ell) = 0$ だから、μ_ℓ の $\mathbb{Z}/\ell\mathbb{Z}$ による拡大はもしあつた

証明： これは [11] の §3.4.3, §3.4.6 と似た方法で証明される。$A \in \mathbf{A}_p$ とし、$A[\ell^n]$ を考へる。(i) より $A[\ell^n]$ は各 gr が $\mathbb{Z}/\ell\mathbb{Z}$ または μ_ℓ である。(ii) より $0 \to \mathbb{Z}/\ell\mathbb{Z} \to G \to \mu_\ell \to 0$ の形の短完全列は分裂するから、この様な部分を $0 \to \mu_\ell \to G \to \mathbb{Z}/\ell\mathbb{Z} \to 0$ で置き換へて行く事により

$$\begin{aligned} 0 \to & M_n \to A[\ell^n] \to C_n \to 0, \\ & M_n \text{ は } \mu_\ell \text{ たちの拡大}, \quad C_n \text{ は } \mathbb{Z}/\ell\mathbb{Z} \text{ たちの拡大}, \end{aligned}$$

の形になる。$\mathbb{Z}_\ell$ 上では[14] これは $A[\ell^n]_{\mathbb{Z}_\ell}$ の connected-étale sequence

$$0 \to (A[\ell^n]_{\mathbb{Z}_\ell})^0 \to A[\ell^n]_{\mathbb{Z}_\ell} \to (A[\ell^n]_{\mathbb{Z}_\ell})^{\text{ét}} \to 0,$$

と一致してゐなければならないから、M_n も C_n も échelon n の truncated Barsotti-Tate group ([17], 定義 1.1) の筈で、 特に或る $r, s \geq 0$ があつて

$$M_n \text{ の位数} = \ell^{rn}, \quad C_n \text{ の位数} = \ell^{sn},$$

となる。ここで $\dim(A) = g$ ならば $s \leq g \leq r$ だが、$M_{n,\mathbb{Z}_\ell}$ は乗法型 (multiplicative type)[15] だから、双対を考へると M_n と C_n の役割が入れ換つて $r \leq g \leq s$ となるので、 $r = s = g$ である。ところで C_n は $\mathbb{Z}[1/p]$ 上 étale だから $G_{\mathbb{Q}}$ の $C_n(\overline{\mathbb{Q}})$ への作用は p の外不分岐で、C_n が $\mathbb{Z}/\ell\mathbb{Z}$ たちの拡大といふ事からこの作用は $\ell^{\text{冪}}$ 位数の或る商 $H_n = \mathrm{Gal}(K/\mathbb{Q})$ を経由する。故に $H_n^{\mathrm{ab}} := H_n/[H_n, H_n]$ は $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ の ℓ-part の商であり、特に巡回群である。ここで「非可換 ℓ 群は $(\mathbb{Z}/\ell\mathbb{Z})^{\oplus 2}$ と同型な商を持つ」(従つて H_n^{ab} が巡回群なら $H_n = H_n^{\mathrm{ab}}$ である) 事より H_n は abelian で、それ自身 $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ の ℓ-part の商になる。かくして C_n たちは n に依らない体 K $(\subset \mathbb{Q}(\zeta_p))$ 上一斉に constant になる。K の任意の有限素点 $\mathfrak{q} \nmid p$ を一つ取り、その剰余体を κ とすると、$(A/M_n)(\kappa) \supset C_n$ だから $(A/M_n)(\kappa)$ は ℓ^{gn} 個以上の点を持つ。A と A/M_n とは同種だから有限体上の有理点の個数は同じで、

$$\#A(\kappa) \ \geq \ \ell^{gn} \qquad \text{for all} \ \ n.$$

これは矛盾である。 □

次に $\mathrm{Ext}^1_{\mathbf{G}_{p,\ell}}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$ を計算する。

としても $\mathbb{Z}[1/p]$ 上の ℓ-divisible group には延びず、このような拡大の存在は有限のときの例外的なものである。有限のときは物事は微妙になり、補題 3.3 の証明中でも触れる様に、拡大の存在は 2 次の Bernoulli 数 $B_2 = 1/6$ と関係してゐる。

[14] 以下、基底変換 $(...) \otimes_{\mathbb{Z}[1/p]} \mathbb{Z}_\ell$ を $(...)_{\mathbb{Z}_\ell}$ で表す。

[15] ここでは「étale 群の Cartier 双対のこと」と理解されたい。詳しくは SGA3, Exp. IX, X 等を参照。

命題 3.2.

$$\dim_{\mathbb{F}_\ell} \mathrm{Ext}^1_{\mathbf{G}_{p,\ell}}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z}) \;=\; \begin{cases} 1 & \text{if } \frac{p^2-1}{24} \equiv 0 \pmod{\ell}, \\ 0 & \text{その他.} \end{cases}$$

上段の条件 $(p^2-1)/24 \equiv 0 \pmod{\ell}$ は次の条件を一言で言つたものである：

$$p \;\equiv\; \begin{cases} \pm 1 \pmod{\ell} & \text{if } \ell \geq 5, \\ \pm 1 \pmod{9} & \text{if } \ell = 3, \\ \pm 1 \pmod{8} & \text{if } \ell = 2. \end{cases}$$

この命題を証明するために先づ次を証明する：

補題 3.3. 次の自然な完全列がある：

$$0 \;\to\; \mathrm{Ext}^1_{\mathbf{G}_{p,\ell}}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z}) \;\to\; (\mathbb{Z}[1/p\ell, \zeta_\ell]^\times/\ell)_{\omega^2} \;\to\; (\mathbb{Q}_\ell(\zeta_\ell)^\times/\ell)_{\omega^2}.$$

(ここに Abel 群 X に対し X/ℓ は X 上の ℓ 倍 (or ℓ 乗) 写像の余核を表す。また $\omega : \Delta \to \mathbb{F}_\ell{}^\times$ は mod ℓ 円分指標であり、$(...)_{\omega^i}$ は Δ が ω^i 倍で作用する部分を表す。)

証明： 位相空間としての

$$\mathrm{Spec}(\mathbb{Z}[1/p]) \;=\; \mathrm{Spec}(\mathbb{Z}[1/pl]) \cup_{\mathrm{Spec}(\mathbb{Q}_\ell)} \mathrm{Spec}(\mathbb{Z}_\ell)$$

といふ貼合せに対し Mayer-Vietoris 完全列 ([31], 命題 2.4)[16] を適用して次の完全列[17] を得る：

$$(3.1)\;\; 0 \;\to\; \mathrm{Ext}^1_{\mathbb{Z}[1/p]}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z}) \;\to\; \mathrm{Ext}^1_{\mathbb{Z}[1/p\ell]}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z}) \;\to\; \mathrm{Ext}^1_{\mathbb{Q}_\ell}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$$

[16]一般には次の形：R を Noether 環、p を R の元、$\widehat{R}$ を R の p 進完備化とする。このとき、R 上の有限平坦群 schemes G, H に対し、次の自然な完全列がある：
$0 \to \mathrm{Hom}_R(G,H) \to \mathrm{Hom}_{\widehat{R}}(G,H) \times \mathrm{Hom}_{R[1/p]}(G,H) \to \mathrm{Hom}_{\widehat{R}[1/p]}(G,H)$
$\to \mathrm{Ext}^1_R(G,H) \;\to\; \mathrm{Ext}^1_{\widehat{R}}(G,H) \times \mathrm{Ext}^1_{R[1/p]}(G,H) \;\to \mathrm{Ext}^1_{\widehat{R}[1/p]}(G,H).$
これの背景にあるのは次の圏同値 (R-加群版は cf. [3], 定理 2.6) である：

$$(R \text{ 上の有限平坦群 schemes の圏}) \;\tilde{\to}\; (\text{三組 } (\widehat{G}, G, \theta) \text{ たちの圏}),$$

ここに $\widehat{G}$, G はそれぞれ $\widehat{R}$, $R[1/p]$ 上の有限平坦群 scheme, θ は両者の $\widehat{R}[1/p]$ 上での同一視、である。

[17]ここ及び以下で、可換環 R に対し Hom_R, Ext^1_R 等と書いたら、
・R 上の $\ell^{\text{冪}}$ 位数の有限平坦可換群 schemes のなす完全圏に於けるそれら、又は、
・$\mathrm{Spec}(R)_{\mathrm{fppf}}$ 上の Abel 群の層達のなす Abel 圏に於けるそれら、
を意味する (どちらで考へても同じになる)。従つて $\mathrm{Ext}^1_{\mathbb{Z}[1/p]} = \mathrm{Ext}^1_{\mathbf{G}_{p,\ell}}$ 等である。

ここで、$\mathrm{Ext}^1(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$ よりも $\mathrm{Ext}^1(\mathbb{Z}/\ell\mathbb{Z}, \mu_\ell)$ の方が計算しやすいので、$\mathbb{Z}[1/p\ell]$ や $\mathbb{Q}_\ell$ に ζ_ℓ を添加した環まで行つて同型 $\mu_\ell \simeq \mathbb{Z}/\ell\mathbb{Z}$ を選び、μ_ℓ と $\mathbb{Z}/\ell\mathbb{Z}$ の位置を交代する。同型 $\iota : \mu_\ell \xrightarrow{\sim} \mathbb{Z}/\ell\mathbb{Z}$ は Abel 群としての同型 $\mathrm{Ext}^1(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z}) \simeq \mathrm{Ext}^1(\mathbb{Z}/\ell\mathbb{Z}, \mu_\ell)$ を引き起こすが、$\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$ の作用は異なり、

$$\begin{aligned}\mathrm{Im}\left(\mathrm{Ext}^1_{\mathbb{Q}_\ell}(\mathbb{Z}/\ell\mathbb{Z}, \mu_\ell) \hookrightarrow \mathrm{Ext}^1_{\mathbb{Q}_\ell(\zeta_\ell)}(\mathbb{Z}/\ell\mathbb{Z}, \mu_\ell)\right) &= \mathrm{Ext}^1_{\mathbb{Q}_\ell(\zeta_\ell)}(\mathbb{Z}/\ell\mathbb{Z}, \mu_\ell)_{\omega^0} \\ &\simeq \mathrm{Ext}^1_{\mathbb{Q}_\ell(\zeta_\ell)}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})_{\omega^2}\end{aligned}$$

となつてゐる。$\mathrm{Ext}^1_{\mathbb{Z}[1/p\ell,\zeta_\ell]}(\mathbb{Z}/\ell\mathbb{Z}, \mu_\ell)$ についても同様。そこで

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}[1/p]}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Z}[1/p\ell,\zeta_\ell]}(\mathbb{Z}/\ell\mathbb{Z}, \mu_\ell)_{\omega^2} \to \mathrm{Ext}^1_{\mathbb{Q}_\ell(\zeta_\ell)}(\mathbb{Z}/\ell\mathbb{Z}, \mu_\ell)_{\omega^2}$$

なる完全列が出来る。右の二つの Ext^1 を調べるため、$\mathbb{Z}[1/p\ell, \zeta_\ell]$ 上及び $\mathbb{Q}_\ell(\zeta_\ell)$ 上で短完全列 $0 \to \mathbb{Z} \xrightarrow{\ell} \mathbb{Z} \to \mathbb{Z}/\ell\mathbb{Z} \to 0$ の $\mathrm{Ext}^{\cdot}(-, \mu_\ell)$ を取ると、

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[1/p\ell,\zeta_\ell]}(\mathbb{Z}, \mu_\ell) & \longrightarrow & \mathrm{Ext}^1_{\mathbb{Z}[1/p\ell,\zeta_\ell]}(\mathbb{Z}/\ell\mathbb{Z}, \mu_\ell) & \longrightarrow & \mathrm{Ext}^1_{\mathbb{Z}[1/p\ell,\zeta_\ell]}(\mathbb{Z}, \mu_\ell) \\
 & & \| & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[1/p\ell,\zeta_\ell]}(\mathbb{Z}, \mu_\ell) & \longrightarrow & \mathrm{Ext}^1_{\mathbb{Q}_\ell(\zeta_\ell)}(\mathbb{Z}/\ell\mathbb{Z}, \mu_\ell) & \longrightarrow & \mathrm{Ext}^1_{\mathbb{Q}_\ell(\zeta_\ell)}(\mathbb{Z}, \mu_\ell).
\end{array}$$

ここで、一般に R が整閉整域 $\ni 1/\ell$ であるとき (μ_ℓ は R 上 étale なので) $\mathrm{Ext}^1_R(\mathbb{Z}, \mu_\ell)$ は Galois cohomology 群 $H^1(R, \mu_\ell)$ (= étale 基本群 $\pi_1(\mathrm{Spec}\ R)$ の連続 cohomology 群) と標準的に同型であるから、上の図式全体の ω^2-part を取つたものに Snake lemma を適用すると、

$$\begin{array}{ccccccccc}
 & & & & \mathrm{Ker}(\alpha) & \xrightarrow{\simeq} & \mathrm{Ker}(\beta) & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mu_\ell & \longrightarrow & \mathrm{Ext}^1_{\mathbb{Z}[1/p\ell,\zeta_\ell]}(\mathbb{Z}/\ell\mathbb{Z}, \mu_\ell)_{\omega^2} & \longrightarrow & H^1(\mathbb{Z}[1/p\ell, \zeta_\ell], \mu_\ell)_{\omega^2} & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \\
0 & \longrightarrow & \mu_\ell & \longrightarrow & \mathrm{Ext}^1_{\mathbb{Q}_\ell(\zeta_\ell)}(\mathbb{Z}/\ell\mathbb{Z}, \mu_\ell)_{\omega^2} & \longrightarrow & H^1(\mathbb{Q}_\ell(\zeta_\ell), \mu_\ell)_{\omega^2} & \longrightarrow & 0
\end{array}$$

を得る。これと (3.1) を合せて

$$(3.2)\quad 0 \to \mathrm{Ext}^1_{\mathbf{G}_{p,\ell}}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z}) \to H^1(\mathbb{Z}[1/p\ell, \zeta_\ell], \mu_\ell)_{\omega^2} \to H^1(\mathbb{Q}_\ell(\zeta_\ell), \mu_\ell)_{\omega^2}$$

を得る。Kummer 完全列より

$$\begin{array}{ccccccc}
0 & \longrightarrow & (\mathbb{Z}[1/p\ell, \zeta_\ell]^\times/\ell) & \longrightarrow & H^1(\mathbb{Z}[1/p\ell, \zeta_\ell], \mu_\ell) & \longrightarrow & H^1(\mathbb{Z}[1/p\ell, \zeta_\ell], \mathbb{G}_m)[\ell] \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & (\mathbb{Q}_\ell(\zeta_\ell)^\times/\ell) & \longrightarrow & H^1(\mathbb{Q}_\ell(\zeta_\ell), \mu_\ell) & \longrightarrow & H^1(\mathbb{Q}_\ell(\zeta_\ell), \mathbb{G}_m)[\ell]
\end{array}$$

なる図式があるが、この右端に於いて

$$\begin{aligned} H^1(\mathbb{Z}[1/p\ell,\zeta_\ell],\mathbb{G}_m) &= \mathrm{Cl}(\mathbb{Z}[1/p\ell,\zeta_\ell]) \quad \text{(ideal 類群)},\\ H^1(\mathbb{Q}_\ell(\zeta_\ell),\mathbb{G}_m) &= 0 \qquad\qquad \text{(Hilbertsche Satz 90)}, \end{aligned}$$

である。ここで

$$\mathrm{Cl}(\mathbb{Z}[1/p\ell,\zeta_\ell]) = \mathrm{Cl}(\mathbb{Z}[\zeta_\ell])/\langle p\ell \text{ を割る素 ideal を含む類}\rangle.$$

また、Herbrand の定理 ([47], 定理 6.17) と $\ell\nmid B_2=1/6$ といふ事と鏡映定理 (Spiegelungssatz; [47], 定理 10.9) により $\mathrm{Cl}(\mathbb{Z}[\zeta_\ell])[\ell]$ の ω^2-part は 0 である。故に $\mathrm{Cl}(\mathbb{Z}[1/p\ell,\zeta_\ell])[\ell]_{\omega^2}$ も 0. そこで (3.2) の $H^1\to H^1$ を $(\mathbb{Z}[1/p\ell,\zeta_\ell]^\times/\ell)_{\omega^2}\to(\mathbb{Q}_\ell(\zeta_\ell)^\times/\ell)_{\omega^2}$ で置き換へる事が出来、所期の結果を得る。 □

次に補題 3.3 から命題 3.2 を導く。ここでは $\ell\geq 5$ の場合だけ証明する ($\ell=2,3$ でも大体同様)。補題 3.3 の短完全列

$$0 \to \mathrm{Ext}^1_{\mathbf{G}_{p,\ell}}(\mu_\ell,\mathbb{Z}/\ell\mathbb{Z}) \to (\mathbb{Z}[1/p\ell,\zeta_\ell]^\times/\ell)_{\omega^2} \xrightarrow{\alpha} (\mathbb{Q}_\ell(\zeta_\ell)^\times/\ell)_{\omega^2}$$

の右の二項をそれぞれ計算する。結果は

(1) $\dim(\text{中央}) = \begin{cases} 2 & \text{if } p\equiv\pm1 \pmod\ell,\\ 1 & \text{その他}, \end{cases}$

(2) $\dim(\text{右端})=1$,

(3) α は全射、

となる (これらは全て $\ell=2,3$ のときは微妙にズレて来る)。このうち (2) は容易であり、(3) は、$\ell\geq 5$ ならば $\mathbb{Z}[1/\ell,\zeta_\ell]$ の円単数の ω^2-part が既に $(\mathbb{Q}_\ell(\zeta_\ell)^\times/\ell)_{\omega^2}$ に全射に写る事 ([47], 定理 8.25)[18] から従ふ。あとは (1) だけ示せばよい。

Δ-加群の完全列

$$0\to\mathbb{Z}[1/\ell,\zeta_\ell]^\times\to\mathbb{Z}[1/p\ell,\zeta_\ell]^\times\xrightarrow{v}\mathbb{Z}^{S_p}\to\mathrm{Cl}(\mathbb{Z}[1/\ell,\zeta_\ell])\to\mathrm{Cl}(\mathbb{Z}[1/p\ell,\zeta_\ell])\to 0$$

がある。ここに $S_p=\{\mathfrak{p}|p\}$ は p 上にある $\mathbb{Q}(\zeta_\ell)$ の素点の集合、$\mathbb{Z}^{S_p}=\mathrm{Map}(S_p,\mathbb{Z})$ であり、これらには $\Delta=\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$ が自然に作用する。v は $x\in\mathbb{Z}[1/p\ell,\zeta_\ell]^\times$ に対し各素点 $\mathfrak{p}|p$ での付値を対応させる写像である。これに

[18] 「$((\text{局所単数})_{\omega^i}:(\text{円単数})_{\omega^i})=\ell^{L_\ell(1,\omega^i)}$」といふ形の定理 ($L_\ell(1,\omega^i)$ は ℓ 進 L 函数の 1 での値)。これと $L_\ell(1,\omega^2)\equiv L_\ell(-1,\omega^2)=-(1-\ell)B_2/2\not\equiv 0 \pmod\ell$ より全射性が従ふ。この議論から分かる様に、$i=2$ 以外では全射になるとは限らない。

$\otimes\mathbb{Z}_\ell$ して ω^2-part を見る。Herbrand の定理より $(\mathrm{Cl}(\mathbb{Z}[1/\ell,\zeta_\ell])\otimes\mathbb{Z}_\ell)_{\omega^2}=0$. この項より左側の短完全列は $((\mathbb{Z}_\ell^{S_p})_{\omega^2}$ は自由加群なので) 分裂するから、これを mod ℓ して

$$0 \ \to\ (\mathbb{Z}[1/\ell,\zeta_\ell]^\times/\ell)_{\omega^2} \ \to\ (\mathbb{Z}[1/p\ell,\zeta_\ell]^\times/\ell)_{\omega^2} \ \to\ (\mathbb{F}_\ell{}^{S_p})_{\omega^2} \ \to\ 0 \qquad \text{(完全)}.$$

$\mathbb{Z}[1/\ell,\zeta_\ell]^\times$ の構造はよく分かつてゐる (cf. [47], 命題 8.13) ので、左端の括弧の中身は $\mathbb{F}_\ell[\Delta]$-加群として $\mu_\ell\times\mathbb{F}_\ell[\Delta/\langle-1\rangle]$ と同型である事が分かり、従つてその ω^2-part は 1 次元である事が分かる。

右端の S_p は Δ-集合として $\Delta/\langle p\rangle$ と同一視出来るので、

$$\dim_{\mathbb{F}_\ell}(\mathbb{F}_\ell{}^{S_p})_{\omega^i} \ =\ \begin{cases}1 & \text{if } \omega^i(p)=1,\\ 0 & \text{if } \omega^i(p)\neq 1,\end{cases}$$

特に

$$\dim_{\mathbb{F}_\ell}(\mathbb{F}_\ell{}^{S_p})_{\omega^2} \ =\ \begin{cases}1 & \text{if } p\equiv\pm1,\\ 0 & \text{if } p\not\equiv\pm1,\end{cases}$$

となり、(1) が従ふ。 □

次に $\mathbf{D}_{p,\ell}$ の単純対象の集合 $\mathbf{S}_{p,\ell}$ が $\{\mathbb{Z}/\ell\mathbb{Z},\mu_\ell\}$ となるための判定条件を与へる。

補題 3.4. *R は $\mathbb{Q}$ の整閉な部分環で $\ell\notin R^\times$ なるものとする。G は R 上の $\ell^{\text{冪}}$ 位数の有限平坦群 scheme とし、$K=\mathbb{Q}(G(\overline{\mathbb{Q}}))$ とおく。もし G が単純かつ $[K(\zeta_\ell):\mathbb{Q}(\zeta_\ell)]=\ell^{\text{冪}}$ ならば G は R 上の群 scheme として $\mathbb{Z}/\ell\mathbb{Z}$ または μ_ℓ と同型である。*

証明: $G(\overline{\mathbb{Q}})$ は単純 $\mathbb{F}_\ell[G_\mathbb{Q}]$-加群[19]だから、もし $\mathrm{Gal}(K(\zeta_\ell)/\mathbb{Q}(\zeta_\ell))$ が $\ell^{\text{冪}}$ ならばそれは $G(\overline{\mathbb{Q}})$ 全体を固定する。故に $G_\mathbb{Q}$ の $G(\overline{\mathbb{Q}})$ への作用は $\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$ を経由する。即ち、その作用は mod ℓ 円分指標 $\omega:G_\mathbb{Q}\to\mathbb{F}_\ell{}^\times$ の或る冪 ω^k で書かれる。よつて $G(\overline{\mathbb{Q}})$ の単純性より G の位数 $=\ell$. Tate-Oort の定理 (以下に復習する) により G は $\mathbb{Z}/\ell\mathbb{Z}$, μ_ℓ, またはそれらの ℓ で不分岐な指標 ψ による捻り、のどれかと同型である。即ち $\omega^{k-\epsilon}$ $(\epsilon=0,1)$ は ℓ でも不分岐、従つて至る所不分岐。Minkowski の定理により $k=\epsilon$, $\psi=1$, となり、結局 $G\simeq\mathbb{Z}/\ell\mathbb{Z}$ or μ_ℓ となる。 □

[19] G が単純より G は ℓ 倍で消える。もし $G(\overline{\mathbb{Q}})$ が (従つて $G\otimes\mathbb{Q}$ が) 非自明な部分群を持てばその Zariski 閉包 in G は非自明な部分群になる。

定理 3.5 (Oort-Tate [45]). $K/\mathbb{Q}$ を有限次拡大とし、R を整閉整域 $\subset K$ であつてその分数体が K となるものとする。S_ℓ により、$(\ell) \in \mathrm{Spec}(\mathbb{Z})$ の上にある点の集合 $\subset \mathrm{Spec}(R)$ を表す。このとき次の一対一対応がある：

$$\{\text{位数 } \ell \text{ の有限平坦群 scheme } G/R \text{ の同型類}\}$$
$$\overset{1:1}{\longleftrightarrow} \{\text{組 } (\psi, (n_v)_{v\in S_\ell}) \text{ であつて次の (i), (ii) を満たすもの}\}$$

(i) ψ は idèle 類の指標 $\psi : C_K \to \mathbb{F}_\ell{}^\times$ であつて $\mathrm{Spec}(R) \smallsetminus S_\ell$ で不分岐；
(ii) $(n_v)_{v\in S_\ell}$ は 整数 $0 \le n_v \le v(\ell)$ の族であつて、各 $v \in S_\ell$ について

$$\psi_v(u) = N_{k_v/\mathbb{F}_\ell}(u \pmod{\ell})^{-n_v}, \qquad u \in U_v$$

を満たす (ここで、素点 $v \in S_\ell$ と対応する正規付値 $v : K_v^\times \twoheadrightarrow \mathbb{Z}$ とを同じ文字 v で表した)。

特に $R = \mathbb{Z}_{(\ell)}$ のとき、上の様な G は $\mathbb{Z}/\ell\mathbb{Z}$ または μ_ℓ と同型である (事が、上の対応 $G \mapsto (\psi^G, (n_v^G))$ の中身を見ると分かる)。

次に、単純な $G \in \mathbf{G}_{p,\ell}$ から生ずる拡大の分岐を評価する。ここで分岐群の最大 upper break $u_{L/K}$ について 復習しておくと便利[20] である。一般に L/K が完備離散付値体の Galois 拡大であるとき、その Galois 群 $G = \mathrm{Gal}(L/K)$ には上付き分岐 filtration $(G^u)_{u\in\mathbb{Q}_{\ge 0}}$ が入る ([1], [2]; 剰余体が完全のときは [35] 等)。剰余体が完全のとき

$$\begin{aligned}(\text{Abbes-Saito の } G^u) &= (\text{Corps Locaux [35] の } G^{u-1})\\ &= (\text{Fontaine [11] の } G^{(u)})\end{aligned}$$

となつてゐる。L/K が (必ずしも Galois でない) 代数拡大のとき、G をその Galois 閉包の Galois 群として、

$$u_{L/K} := \sup\{u \mid G^u \neq 1\} \qquad \in [0, \infty]$$

とおく。上付き分岐 filtration G^u は「商と両立する」から、この $u_{L/K}$ は体の合成 L_1L_2/K に関し次の性質を持つ：

$$u_{L_i/K} \le u \text{ for } i = 1, 2 \implies u_{L_1L_2/K} \le u. \tag{3.3}$$

[20] Schoof は [32] の命題 5.1 の証明で $G \times G_p \times V(\rho)$ 等といふ妙な直積群 scheme を考へてゐるが、これは有限平坦群 scheme G から来る拡大と $p^{1/\ell}, \zeta_p$ を添加する拡大との合成体の判別式を評価するためで、以下の (3.3) と (3.4) を知つてゐればこの様な議論は要らない。

また、L/K が有限次かつ $\mathcal{O}_L/\mathcal{O}_K$ が単生 (monogenic)[21] のとき、その共役差積 $\mathcal{D}_{L/K}$ と $u_{L/K}$ との間には次の関係が知られてゐる ([1], 補題 6.6; [11], 命題 1.3):

$$v_K(\mathcal{D}_{L/K}) \;=\; u_{L/K} - i_{L/K}. \tag{3.4}$$

ここに v_K は K の正規付値、$i_{L/K}$ は最大 lower break, 即ち

$$i_{L/K} := \max\{i|\ G_{(i)} \neq 1\} \;=\; \max\{v_K(\pi - \pi')\}$$

である (ここに $G_{(i)}$ は Fontaine 式の下付き分岐 filtration で、
$G_{(i)} = (\text{Corps Locaux の } G_{ei-1})$, e は L/K の分岐指数。また、右の max は、$\mathcal{O}_L$ を $\mathcal{O}_K[X]/(f(X))$ と表示したときの多項式 $f(X)$ の相異なる二つの根 π, π' を動かすときの最大)。

補題 3.6. $G \in \mathbf{G}_{p,\ell}$ に対し $K = \mathbb{Q}(G(\overline{\mathbb{Q}}))$ とおく。
(1) $K/\mathbb{Q}$ は $\{p, \ell, \infty\}$ の外不分岐。
(2) $\ell G = 0$ ならば $u_{K_\lambda/\mathbb{Q}_\ell} \leq 1 + \frac{1}{\ell-1}$, $v_\ell(\mathcal{D}_{K/\mathbb{Q}}) < 1 + \frac{1}{\ell-1}$.
(3) $\ell G = 0$ かつ $G \in \mathbf{D}_{p,\ell}$ ならば $K(p^{1/\ell})/\mathbb{Q}(p^{1/\ell})$ は p でも不分岐。

証明： (1) は群 scheme についての標準的知識 (e.g. [45], 補題 5).
(2) は Fontaine の定理 ([11], 命題 1.7, 補題 1.8; Abbes-Saito 理論を使つた別証明 (剰余体一般の完備離散付値環上の場合をも含む) は [14], 系 9; (群 scheme でなく) $\mathbb{Q}_\ell$ の有限次拡大の半安定表現の部分商の場合は [15] の主定理を参照)。
(3) このとき $G(\overline{\mathbb{Q}})$ は $\mathbb{F}_\ell$-vector space で、$(\sigma - 1)^2 = 0$ for $\sigma \in I_p$ より、I_p の $G(\overline{\mathbb{Q}})$ への作用は $\begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}$ の形。故に $K/\mathbb{Q}$ の p での分岐指数は ℓ を割る。よつて $K(p^{1/\ell})/\mathbb{Q}(p^{1/\ell})$ は p で不分岐である。 □

これら二つの補題より、$\mathbf{D}_{p,\ell}$ の単純対象に関する次の判定条件が得られる:

命題 3.7. $F := \begin{cases} \mathbb{Q}(\zeta_p) & \text{if } \ell | p-1, \\ \mathbb{Q} & \text{その他,} \end{cases}$ とおく。組 (p, ℓ) に対し次の条件 $(\mathrm{D}_{p,\ell})$ が成り立つならば $\mathbf{S}_{p,\ell} = \{\mathbb{Z}/\ell\mathbb{Z}, \mu_\ell\}$ である。

[21] $\mathcal{O}_L$ が $\mathcal{O}_K$-代数として一元で生成される事。剰余体の拡大が分離的ならばいつでも単生である ([35], 第 III 章, §6, 命題 12)。

$$(\mathrm{D}_{p,\ell})\begin{cases}\text{任意の Galois 拡大 } L/\mathbb{Q} \text{ に対し、二条件}\\ \text{(i) } L \text{ は } F(\zeta_{2\ell}, p^{1/\ell}) \text{ を含み、かつこの拡大は } \ell \text{ の外不分岐、}\\ \text{(ii) } v_\ell(\mathcal{D}_{L/\mathbb{Q}}) < 1 + \frac{1}{\ell-1},\\ \text{が成り立つならば } [L:\mathbb{Q}(\zeta_\ell)] = \ell^{\text{冪}}.\end{cases}$$

註. $(\mathrm{D}_{p,\ell})$ の仮定 (i) は特に $L/\mathbb{Q}$ の p での分岐指数 $= \ell$ である事を含む。従つて (i), (ii) より, $d_L^{1/n} < p^{1-1/\ell} \cdot \ell^{1+1/(\ell-1)}$ が従ふ。

証明： $G \in \mathbf{D}_{p,\ell}$ は単純とする。$L := F(G(\overline{\mathbb{Q}}), \zeta_{2\ell}, p^{1/\ell})$ とおくと、補題 3.6 の (3) より $L/F(\zeta_{2\ell}, p^{1/\ell})$ は ℓ の外不分岐で、補題 3.6 の (2) より $u_{K_\lambda/\mathbb{Q}_\ell} \leq 1+\frac{1}{\ell-1}$. また、$\mathbb{Q}_\ell(\zeta_{2\ell})/\mathbb{Q}_\ell$, $\mathbb{Q}_\ell(p^{1/\ell})/\mathbb{Q}_\ell$ の upper breaks $u_{\mathbb{Q}_\ell(\zeta_{2\ell})/\mathbb{Q}_\ell}$, $u_{\mathbb{Q}_\ell(p^{1/\ell})/\mathbb{Q}_\ell}$ も $\leq 1+\frac{1}{\ell-1}$ だから $L_\lambda/\mathbb{Q}_\ell$ のもさう ; $u_{L_\lambda/\mathbb{Q}_\ell} \leq 1+\frac{1}{\ell-1}$. 上の等式 (3.4) により $v_\ell(\mathcal{D}_{L/\mathbb{Q}}) < 1 + \frac{1}{\ell-1}$. そこで $(\mathrm{D}_{p,\ell})$ を仮定すると $[L:\mathbb{Q}(\zeta_\ell)] = \ell^{\text{冪}}$. 故に補題 3.4 により $\mathbf{S}_{p,\ell} = \{\mathbb{Z}/\ell\mathbb{Z}, \mu_\ell\}$ が従ふ。 □

定理 2 の証明： 各 $p \in \{2,3,5,7,13\}$ に対し、命題 3.2 の条件 $p \not\equiv \pm 1 \pmod{\ell \text{ or } 9 \text{ or } 8}$ を満たす適当な $\ell\ (\neq p)$ を取つて条件 $(\mathrm{D}_{p,\ell})$ を確かめればよい。ℓ は小さいほうが $(\mathrm{D}_{p,\ell})$ を示しやすいから、

$$(p,\ell) \ = \ (2,3),(3,2),(5,2),(7,3),(13,2)$$

について $(\mathrm{D}_{p,\ell})$ を示す。ここでは (Serre 予想の証明に使ふ) $p=5$ の場合だけやる。

$(p,\ell) = (5,2)$ のとき、命題 3.7 の体 F は $F = \mathbb{Q}(\zeta_5)$ である。L を $(\mathrm{D}_{p,\ell})$ の様な体とする (即ち L は $F(\zeta_4, \sqrt{5}) = \mathbb{Q}(\zeta_{20})$ を含み、この拡大は 2 の外不分岐、かつ $v_2(\mathcal{D}_{L/\mathbb{Q}}) < 2$). すると

$$d_L^{1/n} < 5^{1/2} \cdot 2^2 = 8.944....$$

§1 の Odlyzko bound の表により $n = [L:\mathbb{Q}] \leq 16$, 従つて $L/\mathbb{Q}(\zeta_{20})$ は次数 ≤ 4 の Abel 拡大である。そこで類体論を使つて $\mathbb{Q}(\zeta_{20})$ の 2 の外不分岐な 3 次拡大があるかどうか調べる (因みに 2 の上にある $\mathbb{Q}(\zeta_{20})$ の素点はただ一つである)。先づ、この体の類数は 1 である。次に、

$$\mathbb{Z}_2[\zeta_{20}]^\times \ \simeq \ \mathbb{F}_4^\times \times (\text{pro-2})$$

であるが、右辺の $\mathbb{F}_4^\times$ は相互写像を適用するとき大域単数 $\varepsilon = (1+\sqrt{5})/2$ により消えるので、$\mathbb{Q}(\zeta_{20})$ の 2 の外不分岐 Abel 拡大は $2^{\text{冪}}$ 次のものしか存在しない。 □

Brumer-Kramer の方法. Brumer-Kramer [7] も Schoof の定理 (定理 2) の一部 ($p = 2, 3, 5, 7$ の場合) を証明してゐる。その方法は、一部重複する部分もあるが、趣を異にする部分もあり、それはそれで面白いので、要点だけ簡単に説明する。

まづ局所的な話から。K を完備離散付値体とし、その剰余体 k は標数 p の完全体とする。A を K 上の Abel 多様体、ℓ を素数 $\neq p$, $T_\ell(A)$ を A の ℓ 進 Tate 加群とする。I_K を惰性群 $\subset G_K$ とする。このとき、$T_\ell(A)$ への惰性作用の初動段階 (effective stage of inertia action on $T_\ell(A)$) とは、I_K が $A[\ell^n]$ に非自明に作用する様な最小の整数 n のこと、と定義する。この値を $i(A/K, \ell)$ と記す。

今、A は K 上半安定還元を持つとすると、$T_\ell(A)$ は次の様な filtration を持つ ([12], 命題 3.5[22]) :

$$V^\perp \ \subset \ V \ \subset \ T_\ell(A).$$

ここに

$$V = V(A) := \ T_\ell(A)^{I_K},$$
$$V^\perp = V^\perp(A) := \ (V(\check{A}) \text{ の、Weil 対合に関する直交補空間})$$

(ここに $\check{A}$ は A の双対 Abel 多様体)。これらについては次の解釈と性質が知られてゐる ([12], §2, §3) :

$\mathcal{A}$: A の Néron model/$\mathcal{O}_K$,

$\mathcal{A}_s^0$: $\mathcal{A}$ の special fiber の連結成分 $\ni 1$,

とすると、

$$0 \ \to \ \mathcal{T} \ \to \ \mathcal{A}_s^0 \ \to \ \mathcal{B} \ \to \ 0,$$
$$(\mathcal{T} \text{ は torus}/k, \ \mathcal{B} \text{ は Abel 多様体}/k).$$

の形の短完全列があるが、このとき

$V^\perp \ \simeq \ T_\ell(\mathcal{T})$,

$V/V^\perp \ \simeq \ T_\ell(\mathcal{B})$,

$(g-1)(T_\ell(A)) \ \subset \ V^\perp \quad$ for $g \in I_K$.

これより準同型

$$N : \ I_K \ \to \ \mathrm{Hom}(T_\ell(A)/V, V^\perp)$$
$$g \ \mapsto \ N_g := g - 1,$$

[22]そこの (ii) に "$V \subset V^\perp$" と書いてあるのは誤殖。

が得られ、Tate 加群上の表現

$$\rho:\ I_K\ \to\ \mathrm{GL}_{2g}(T_\ell(A))$$

は $T_\ell(A)$ の適当な基底 (分解 $T_\ell(A)\simeq V^\perp\oplus(V/V^\perp)\oplus(T_\ell(A)/V)$ と両立するもの) に関して

$$\rho\ \sim\ \begin{pmatrix}1_t & & N\\ & 1_{2a} & \\ & & 1_t\end{pmatrix}$$

の形 (ここに $t:=\dim(\mathcal{T})$, $a:=\dim(\mathcal{B})$) となる。A が良還元でない場合、N は写像として $\neq 0$ である。

補題 3.8. 記号は上の通りとし、$\bar{V}=V\pmod{\ell}$, $\bar{V}^\perp=V^\perp\pmod{\ell}$ をそれぞれ V, $V^\perp$ の $A[\ell]$ に於ける像とする。$\varphi:A\to A'$ を K 上定義された同種射とし、その核 κ は $\bar{V}^\perp\subset\kappa\subset\bar{V}$ を満たすものとする。このとき $i(A'/K,\ell)=i(A/K,\ell)+1$ が成り立つ。

これは、可換図式

$$\begin{array}{ccc} T_\ell(A)/V & \xrightarrow{\varphi_*} & T_\ell(A')/V' \\ {\scriptstyle \ell N_\sigma}\big\downarrow & & \big\downarrow{\scriptstyle N'_\sigma} \\ V^\perp & \xleftarrow[\varphi'_*]{} & V'^\perp \end{array}$$

に於いて、補題の仮定の下、φ_*, φ'_* が同型になる事から従ふ (ここに $\varphi':A'\to A$ は $\varphi:A\to A'$ の双対同種射、V', $V'^\perp$ はそれぞれ A' に対する V, $V^\perp$ の対応物)。

さて、大域に戻つて、$A/\mathbb{Q}$ は高々 p で半安定還元を持つ Abel 多様体とする。既に見た様に、p と ℓ $(\neq p)$ が小さいとき、拡大体 $L=\mathbb{Q}(A[\ell])$ は非常に特殊なもの (例へば $L\subset\mathbb{Q}(\mu_\ell,p^{1/\ell})$) に限られる (この辺は Schoof の議論と同様)。ℓ と p との関係に依つては、p の上にある L の素点 v は唯一つ (従つて $\mathrm{Gal}(L_v/\mathbb{Q}_p)\simeq\mathrm{Gal}(L/\mathbb{Q})$) といふ事が起こり得る。このとき $G_\mathbb{Q}$-安定な部分群 $\kappa\subset A[\ell]$ を、$\mathbb{Q}_p$ 上 (先の記号で) $\bar{V}^\perp\subset\kappa\subset\bar{V}$ となる様に取れ ($\bar{V}$ や $\bar{V}^\perp$ 自身を取ればよい)、この κ を核とする $\mathbb{Q}$-同種射 $\varphi:A\to A'$ がある。もし高々 p で半安定な $A/\mathbb{Q}$ があつたとすると、(次元を固定して考へればそれらは有限個だから) 予め $i(A/\mathbb{Q}_p,\ell)$ が最大になる様に A を選んでおけば、補題 3.8 により $i(A'/\mathbb{Q}_p,\ell)=i(A/\mathbb{Q}_p,\ell)+1$ となり、矛盾。かくして $A/\mathbb{Q}$ の非存在が言へる。

References

[1] A. Abbes and T. Saito, *Ramification of local fields with imperfect residue fields*, Amer. J. Math. **124** (2002), 879–920.

[2] A. Abbes and T. Saito, *Ramification of local fields with imperfect residue fields, II*, Doc. Math. Extra Vol. Kazuya Kato's fiftieth birthday (2003), 5–72

[3] M. Artin, *Algebraization of formal moduli, II. Existence of modifications*, Ann. of Math. **91** (1970) 88–135

[4] A. Ash, D. Doud and D. Pollack, *Galois representations with conjectural connections to arithmetic cohomology*, Duke Math. J. **112** (2002), 521–579

[5] A. Ash and W. Sinnott, *An analogue of Serre's conjecture for Galois representations and Hecke eigenclasses in the mod p cohomology of* $\mathrm{GL}(n, Z)$, Duke Math. J. **105** (2000), 1–24

[6] S. Brueggeman, *The nonexistence of certain Galois extensions unramified outside* 5, J. Number Theory **75** (1999), 47–52

[7] A. Brumer and K. Kramer, *Non-existence of certain semistable abelian varieties*, Manuscripta Math. **106** (2001), 291–304

[8] K. Buzzard, F. Diamond and F. Jarvis, *On Serre's conjecrure for mod ℓ Galois representations over totally real fields*, preprint, 2005, available at: `http://www.unet.brandeis.edu/~fdiamond/bdj12.pdf`

[9] F. Calegari and M. Emerton, *On the ramification of Hecke algebras at Eisenstein primes*, Invent. Math. **160** (2005), 97–144

[10] L. M. Figueiredo, *Serre's conjecture for imaginary quadratic fields*, Compositio Math. **118** (1999), 103–122

[11] J-M. Fontaine, *Il n'y a pas de variété abélienne sur* $\mathbb{Z}$, Invent. Math. **81** (1985), 515–538

[12] A. Grothendieck, *Modèles de Néron et monodromie*, in: Groupes de Monodromie en Géométrie Algébrique, I, Séminaire de Géométrie

Algébrique du Bois-Marie, 1967–1969, Dirigé par A. Grothendieck avec la collaboration de M. Raynaud et D. S. Rim. Lecture Notes in Math. **288**, Springer-Verlag, Berlin-New York, 1972

[13] 萩原啓, レベル 1 の Serre 予想, この報告集

[14] S. Hattori, *Ramification of a finite flat group scheme over a local field*, J. Number Theory **118** (2006), 145–154

[15] S. Hattori, *On a ramification bound of semi-stable torsion representations over a local field*, preprint

[16] Y. Ihara, *How many primes decompose completely in an infinite unramified Galois extension of a global field?* J. Math. Soc. Japan **35** (1983), 693–709

[17] L. Illusie, *Déformations de groupes de Barsotti-Tate, d'après A. Grothendieck*, Séminaire sur les pinceaux arithmétiques: La conjecture de Mordell (L. Szpiro, ed.), Exp. VI, pp. 151–198

[18] J. Jones, *Tables of number fields with prescribed ramification*, `http://math.asu.edu/~jj/numberfields/`

[19] C. Khare and J.-P. Wintenberger, *On Serre's conjecture for* 2*-dimensional mod p representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, preprint

[20] J.-F. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Math. **58** (1986), 209–232

[21] H. Moon, *Finiteness results on certain mod p Galois representations*, J. Number Theory **84** (2000), 156–165

[22] H. Moon, *On four-dimensional mod* 2 *Galois representations and a conjecture of Ash et al.*, Bull. K.M.S. **44** (2007), 173–176

[23] H. Moon and Y. Taguchi, *Refinement of Tate's discriminant bound and non-existence theorems for mod p Galois representations*, Kazuya Kato's fiftieth birthday, Doc. Math. 2003, Extra Vol., 641–654

[24] H. Moon and Y. Taguchi, *The non-existence of certain mod* 2 *Galois representations of some small quadratic fields*, Proc. Japan Acad. **84** (2008), 57–61

[25] A. M. Odlyzko, *Lower bounds for discriminants of number fields, II*, Tôhoku Math. J. **29** (1977), 209–216

[26] A. M. Odlyzko, *Discriminant bounds*, unpublished manuscript (1976), available at:
`http://www.dtc.umn.edu/~odlyzko/unpublished/index.html`

[27] A. M. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results*, Sém. Théor. Nombres Bordeaux **2** (1990), 119–141

[28] F. Oort, *Commutative group schemes*, Lecture Notes in Math. **15**, Springer-Verlag, Berlin-New York, 1966, vi+133 pp.

[29] G. Poitou, *Minorations de discriminants* (d'après A. M. Odlyzko), Sém. Bourbaki, 1975/76, Exp. 479, Lecture Notes in Math. **567**, Springer-Verlag, Berlin, 1977, pp. 136–153

[30] M. Raynaud, *Schémas en groupes de type* $(p, \ldots, p)$, Bull. Soc. Math. France **102** (1974), 241–280

[31] R. Schoof, *Abelian varieties over cyclotomic fields with good reduction everywhere*, Math. Ann. **325** (2003), 413–448

[32] R. Schoof, *Abelian varieties over* $\mathbb{Q}$ *with bad reduction in one prime only*, Compos. Math. **141** (2005), 847–868

[33] M. H. Şengün, *Serre's conjecture over imaginary quadratic fields*, Ph.D. Thesis, University of Wisconsin, 2008

[34] M. H. Şengün, *The non-existence of certain representations of the absolute Galois group of quadraticfields*, preprint, 2007

[35] J.-P. Serre, *Corps Locaus* (3^{e} éd.), 1980, Hermann, Paris

[36] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. *15* (1972), 259–331

[37] J.-P. Serre, *Congruences et formes modulaires (d'aprés H.P.F. Swinnerton-Dyer)*, Sém. Bourbaki 1971/72, n° **416**, in: Œuvres III, Springer-Verlag, 1986, pp. 74–88

[38] J.-P. Serre, Note 229.$_2$ on p. 710, Œuvres III, Springer-Verlag, 1986

[39] J.-P. Serre, *Minorations de discriminants*, Œuvres III, Springer-Verlag, 1986

[40] J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54**(1987), 179–230

[41] H. M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Invent. Math. **23** (1974), 135–152

[42] D.A. Suprunenko, *Matrix Groups*, A.M.S., Providence, 1976

[43] 高木貞治『代数的整数論』(岩波書店)

[44] J. Tate, *The non-existence of certain Galois extensions of* $\mathbb{Q}$ *unramified outside* 2, in: "Arithmetic geometry", pp. 153–156, Contemp. Math. **174** Amer. Math. Soc., Providence, RI, 1994

[45] J. Tate and F. Oort, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3**, 1970, 1–21

[46] R. Taylor, *Remarks on a conjecture of Fontaine and Mazur*, J. Inst. Math. Jussieu **1** (2002), 125–143

[47] L. Washington, *Introduction to Cyclotomic Fields* (2nd ed.), GTM **83**, Springer-Verlag, New York, 1997

[48] A. Weil, *Sur les "formules explicites" de la théorie des nombres premiers*, Comm. Lund (vol. dédié à Marcel Riesz), 252–265

〒 819-0395 福岡市西区元岡 744
九州大学大学院数理学研究院
Email address: taguchi@math.kyushu-u.ac.jp